

THE RIGHT BACKUP™
BackupAssist 

RECOVERY BIBLE



Table of Contents

Introduction	3
Full server recovery for physical servers	4
1 Physical to Physical, Bare-Metal Disaster Recovery BMDR	4
2 Physical to Virtual, Bare-Metal Disaster Recovery	12
Full server recovery for Hyper-V environments.....	25
3 Recover a Hyper-V Host and all guest VMs to new metal	25
4 Recover specific Hyper-V guest VM to the same host	34
5 Recover specific Hyper-V guest VM to different host.....	41
6 Rapid recovery of a VM from backup within minutes.....	48
File restore for physical machines	54
7 Point-in-time search, browse and restore of files and directories	54
8 Search, browse and restore past versions of a file across all backups	60
File restore for Hyper-V guest VMs.....	66
9 Point-in-time restore of files and directories on a VM from a host backup	66
10 Restore past versions of a file on a Guest VM from backups of the host	72
Exchange Server restore and recover	78
11 Recover entire Exchange Server from backup	78
12 Recover specific Exchange Database(s) from backup.....	82
13 Granular restore of emails from a backup of Exchange in a physical environment	86
14 Granular restore of emails from a backup of Exchange in Hyper-V environment	92
SQL Server restore and recovery	98
15 Full SQL Server recovery from a drive image or application backup.....	98
16 Point-in-time recovery of SQL databases	103
Restore without using BackupAssist	108
17 Restore from a drive image backup using WinRE.....	108
18 Restore from file replication backup.....	112
19 Restore from ZIP archiving backup	114
20 Restore a database from an SQL backup.....	119
Appendix	123
How to create a bootable recovery media	123
Creating a bootable backup.....	127

Introduction

Welcome to the BackupAssist Recovery Bible. This resource is created for our **BackupCare subscribers** and designed to provide a one-stop-shop for all the information you may need when performing a recovery. Think of it as a **Break in Case of Emergency** document.

How to use this guide

Save the Recovery Bible to your computer or print it out as your **go-to guide**.

Each type of **recovery scenario** is listed **in the index**, so locate the scenario that you want to perform and turn to that page. If you are viewing this document as a PDF, clicking on a scenario will take you to the first page of that scenario.

Still need help?

Should you need more assistance, please don't hesitate to email or call the BackupAssist Technical Support Team.

- ❖ Support Team phone: 812-206-4265 or +1-812-206-4265 (international)
- ❖ Support Team email: support@backupassist.com

This guide is designed to take the stress out of recoveries
by making them predictable and successful.

Full server recovery for physical servers

The scenarios in this section will guide you through the process of **recovering an entire server** (physical or virtual) using a **System Protection backup** and a bootable **RecoverAssist media**.

First, we explain how to use a bare-metal backup to recover a **physical server**, and then how to use a bare-metal backup to recover a **physical server to a Hyper-V VM**.

1 Physical to Physical, Bare-Metal Disaster Recovery BMDR

This scenario explains how to **perform a full server recovery**, which is often the easiest way to recover a physical server. For example, if a server or its drives need to be replaced due to a natural disaster, hardware failure or ransomware infection. This is also known as a bare-metal recovery.






In a nutshell: A full server recovery can seem daunting at first, but all you're doing is using a bootable media to start a server and open a recovery environment, which you will then use to locate a backup and recover the server.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.



Recovery requirements

To perform a full server recovery, you will need the items shown in Option 1 or Option 2.

Option 1: If your System Protection job does not use a bootable backup destination.

<p>Physical server to recover to</p>  <p>A new server or the original server. An original server should have new disks if recovering from ransomware.</p>	<p>Bare-metal server backup</p>  <p>Must be a System Protection backup made with Back up Entire System ticked in the Selections screen.</p>	<p>Bootable RecoverAssist media</p>  <p>This media is created using the Recover tab. See the RecoverAssist builder section in the appendix to learn more.</p>
--	--	---

Option 2: If your System Protection job uses a bootable backup destination.

<p>Physical server to recover to</p>  <p>A new server or the original server. An original server should have new disks if recovering from ransomware.</p>	<p>Bootable backup</p>  <p>A bootable backup is a bootable media that contains the backup you will need for the recovery.</p>	<p>Learn more</p> <p>When you create a System Protection bare-metal backup to an external USB drive, the drive will be made bootable, unless you un-tick Make media bootable on the Set up destination step. A bootable backup will boot a server into a recovery environment, without a separate boot media.</p>
--	---	--

Recovery checklist

Use this checklist to make sure the **disks and firmware** on the physical **server you are recovering to** are **compatible** with **your backup**.

<input type="checkbox"/>	<p>Each disk being recovered to is large enough.</p> <p>The server must have a physical disk/s the same size, or larger, than the physical disk/s that the backup was made from.</p> <p>If you backed up a 1TB drive and plan to recover to a 1TB drive, check the manufacturer's specifications as different models of the same size disk can have minor size differences.</p> <p>To avoid drive size issues, we recommend recovering to a larger drive.</p>
<input type="checkbox"/>	<p>The server being recovered to has enough disks.</p> <p>If the backup contains data from multiple disks, the server being recovered to must contain at least the same number of disks.</p>
<input type="checkbox"/>	<p>The server being recovered to has compatible firmware.</p> <p>Backups of servers that use BIOS cannot be restored to servers that use EFI, and backups of servers that use EFI cannot be restored to servers that use BIOS. Some EFI servers allow you to choose EFI or a legacy BIOS option when selecting the boot device.</p> <p>The bootable media and backup must both be created from either BIOS or EFI firmware.</p>
<input type="checkbox"/>	<p>The disks on the server being recovered to use a compatible disk format.</p> <p>A backup of a server that uses BIOS, may not work if you are recovering to a server that has disks formatted with Advanced Format (4k sectors).</p>

Recovery process

This section guides you through the process of recovering a server using a **System Protection** backup and **RecoverAssist**.

To perform a full server recovery:

1. **Attach the bootable media to the server.**

The media will be either a **bootable RecoverAssist media** or a **bootable backup media**.

2. **Start the server.**

When the server starts, it should **detect the bootable media** and **start the boot process**.

Understanding the boot process can help if any problems are encountered.

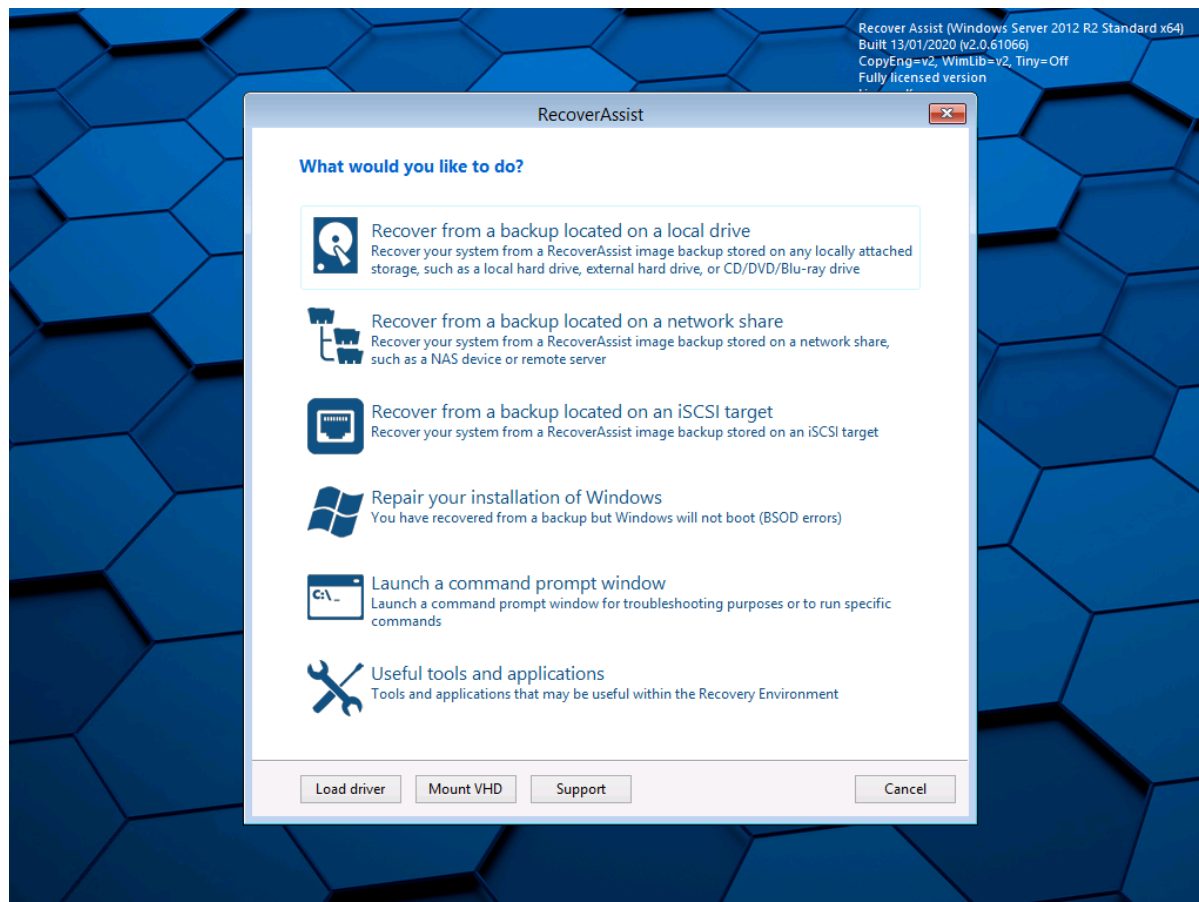


Boot process: Servers use firmware called **BIOS or EFI to access critical hardware**. When a server starts, this firmware checks the hardware and beeps once if the checks are successful. Additional beeps can indicate a hardware problem. Once a server has successfully checked its hardware, **it looks for an operating system**. BIOS and EFI are configured with a device order for the operating system's location. The **Bootable media must appear in this device order** before media that may load a failed operating system. To access the BIOS/ EFI settings, press the required function key, which will be displayed on screen. E.g. F8 or F12.

3. Wait for the RecoverAssist recovery environment to open.

When the server boots from the RecoverAssist media, you will see a progress bar then a blank screen or a Windows logo, depending on the operating system being recovered.

The **RecoverAssist recovery environment** will then load.



RecoverAssist includes a set of **useful tools** that **can help** if you encounter any problems. These tools are described at the end of this scenario.

4. Select a backup destination.

Select the destination your backups are stored on from one of the three options at the top of the RecoverAssist UI.

The options are:

- Recover from a backup located on a **local drive**.
- Recover from a backup located on a **network share**.
- Recover from a backup located on an **iSCSI target**.



BitLocker encrypted backups

System Protection backups to **local media** can be **encrypted** with BitLocker. RecoverAssist will prompt you for the **BitLocker password** if it finds an encrypted backup.

Enter the password used by the backup job to encrypt the backup. This is the password entered in the **Set up destination** step when the backup's job was created.

Considerations:

- Even though a BitLocker key can unlock a drive to create a backup, the password is required to perform a recovery.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

5. Configure the backup destination.

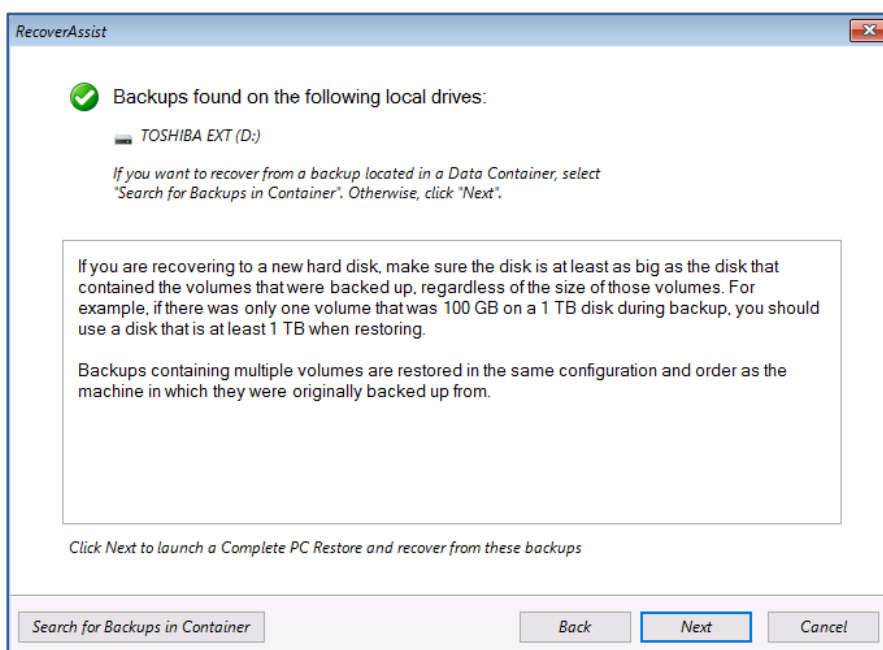
Provide the information required to access the destination you selected.

The following sections explain how to configure each backup destination.

To configure the **local drive** destination:

- Select **local drive** and RecoverAssist will scan all local drives for System Protection backups.

A confirmation dialog will confirm if any backups were found.



If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.

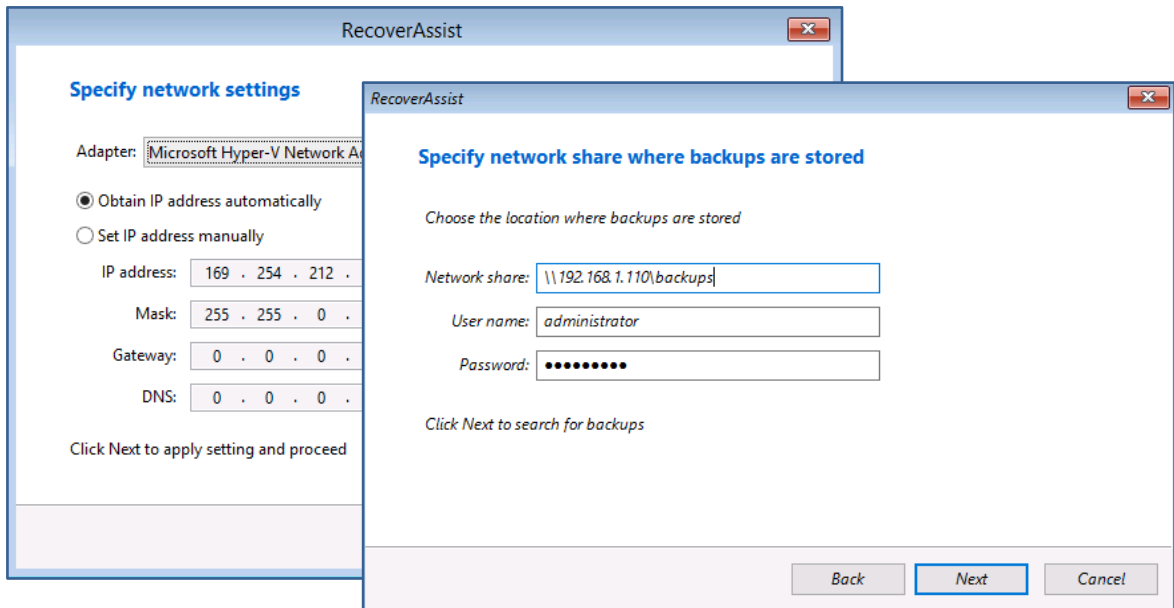
- Select **Next** to progress to the **Windows dialogs** explained below in step 6.

To configure the network share destination:

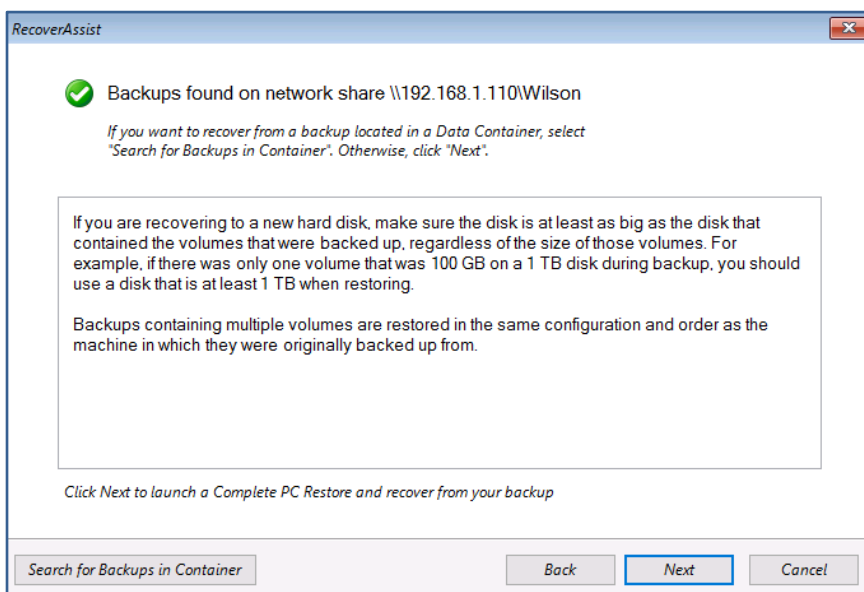
- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.

If you cannot find or configure the network adapter, you may need to manually load the network adapter drivers using the **Load driver** option on the **main RecoverAssist menu**.

- b) Use the **Specify network share where backups are stored** dialog to enter the DNS name or IP address of the share. Provide a **User name** and **Password** if the network share or NAS device is configured with authentication credentials.



Once the destination has been checked, a dialog will confirm if any backups were found. If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.



- c) Select **Next** then go to step 6, **confirm the selected backup**.

To configure the iSCSI target destination:

- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.

The screenshot shows the 'Specify network settings' dialog box in the RecoverAssist application. The title bar reads 'RecoverAssist'. The main heading is 'Specify network settings'. Below this, there is a dropdown menu for 'Adapter' set to 'Microsoft Hyper-V Network Adapter', with 'Refresh' and 'Apply' buttons to its right. Two radio buttons are present: 'Obtain IP address automatically' (selected) and 'Set IP address manually'. To the right of these radio buttons are refresh and cancel icons. Below the radio buttons are four text input fields: 'IP address' (169 . 254 . 168 . 245), 'Mask' (255 . 255 . 0 . 0), 'Gateway' (0 . 0 . 0 . 0), and 'DNS' (0 . 0 . 0 . 0). A checkbox labeled 'Dynamic' is checked next to the DNS field. At the bottom of the dialog, there is a 'Click Next to apply setting and proceed' instruction and three buttons: 'Back', 'Next', and 'Cancel'.

- b) Use the **Specify iSCSI target where backups are stored** dialog to enter the DNS name or IP address of the share.

Click **Search** and RecoverAssist will search for the iSCSI target. If an iSCSI target is found, its details are added to the **Target** section.

Provide a **User name** and **Password** if the iSCSI target is configured with authentication credentials.

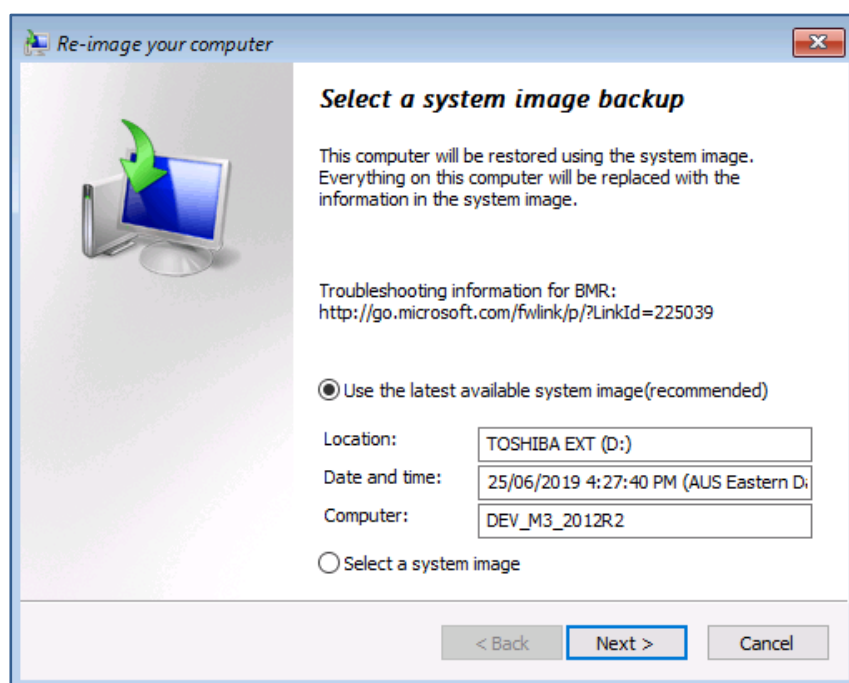
The screenshot shows the 'Specify iSCSI target where backups are stored' dialog box in the RecoverAssist application. The title bar reads 'RecoverAssist'. The main heading is 'Specify iSCSI target where backups are stored'. Below this, there is a sub-heading 'Choose the location where backups are stored'. There is a 'Portal' text input field containing 'DNS name or IP address of the iSCSI target' and a 'Search' button to its right. Below the 'Portal' field is a larger 'Target' text input field. Further down are 'Username' and 'Secret' text input fields, both with '[Optional]' placeholder text. At the bottom of the dialog, there is a 'Click Next to search for backups' instruction and a blue 'iSCSI Help' link with a question mark icon. At the very bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

- c) Once the destination has been checked, a final dialog will confirm if any backups were found. There are **no BitLocker** prompts or **Data Container** options as these features are not used with **iSCSI targets**.
- d) Select **Next** then go to step 6, **confirm the selected backup**.

6. Confirm the selected backup.

The **Select a system image backup** dialog will open and show the selected backup. This will be **the most recent backup**. The **date and time** field shows when the backup was created.

If multiple backups are available, the **Select a system image** option can be used to select a different backup.



If you choose, **Select a system image**, the next step will show a table with the most recent backup data. This is to confirm that this is the media you want to select the image from. When you click **Next**, you will be given the option **to select the backup** you want to recover from.

7. Start the Recovery process.

Confirm the two final Windows recovery dialogs:

- At the **Choose additional restore options** dialog, select **Next**.
- On the final screen, update the **Date** and **Time** if they are incorrect, and select **Finish**.

When you select **Finish**, the full server recovery will start.

8. Remove bootable media.

When the recovery starts, disconnect the bootable media from the server or the recovery environment will load when the server reboots.

Congratulations – your server is now being recovered.



Recovery support software

The following RecoverAssist recovery environment options can assist with a recovery.

Repair your installation of Windows

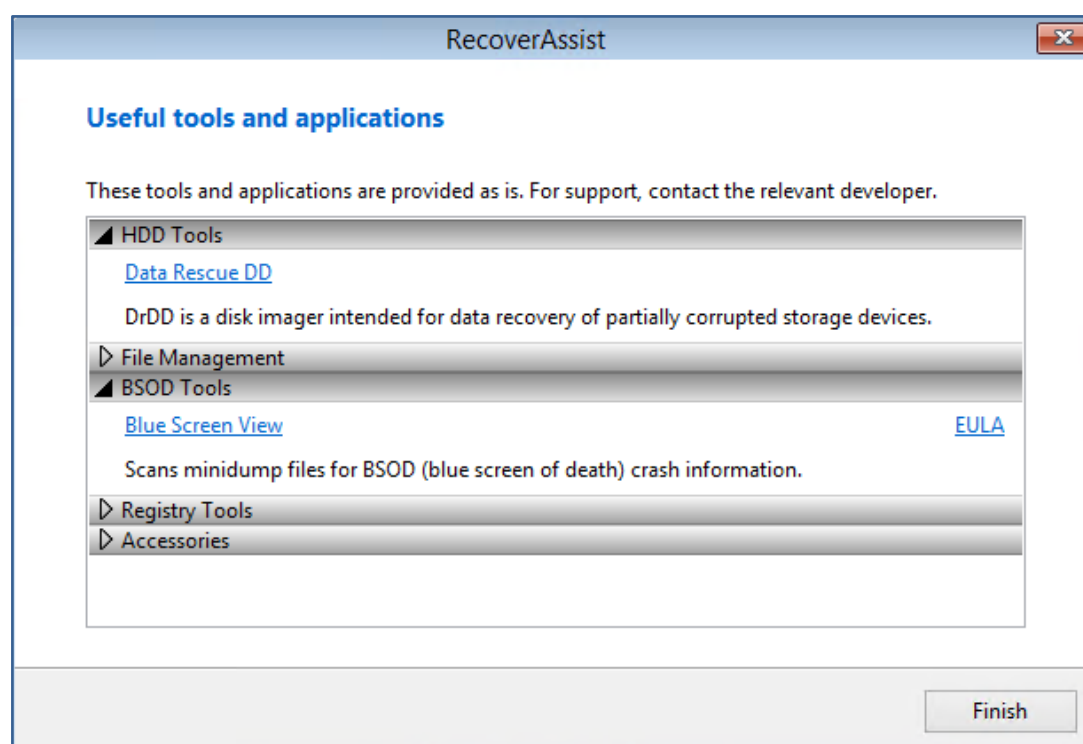
This option loads the **Windows Recovery Environment** and allows you to attempt a repair of the operating system if you encountered a bluescreen or Windows load failure. Using the **repair function** is not required for systems recovered within the RecoverAssist recovery environment.

Launch a command prompt window

This option launches a Windows **command prompt** so you can run the command-line tools included with RecoverAssist. The tools include diskpart.exe, bootsect.exe and regedit.exe.

Useful tools and applications

This option gives access to the applications and tools that you selected when you created your RecoverAssist media. These tools can be used to perform **diagnostics** and **troubleshoot** problems. Clicking on the name of an application will launch that application.



Additional options

The three buttons at the bottom of the Recovery environment give access to these features:

- **Load driver** - loads any **additional device drivers** that were included when creating the recovery environment.
- **Mount VHD** - mounts any VHD (e.g. a **Windows Backup image**). After mounting the VHD, you can access its files using a local drive letter. This is not used to mount Data Containers.

2 Physical to Virtual, Bare-Metal Disaster Recovery

Physical-to-Virtual (P2V) is the process of **recovering a physical server to a virtual machine (VM)**. This can be an ideal solution if you don't have the time or ability to source and install new hardware. A P2V recovery can also be used to migrate a physical server to a VM – a process known as virtualization.


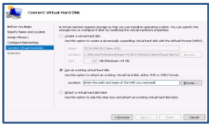




In a nutshell: A P2V recovery can seem daunting at first, but all you're doing is creating a new VM using a bootable ISO to start the server and open a recovery environment, which you will then use to locate a backup and recover the server.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform a P2V recovery, you will need:

<p>A Hyper-V Server</p>  <p>This is a Windows Server with the Hyper-V role running. The Hyper-V Server will give access to Hyper-V Manager.</p>	<p>Hyper-V Manager</p>  <p>Hyper-V Manager will be used to create a VM using the bootable ISO or DVD and then start that VM.</p>	<p>Bare-metal backup</p>  <p>Must be a System Protection backup created with Back up Entire System ticked in the Selections screen.</p>	<p>RecoverAssist media</p>  <p>An ISO or DVD accessible to the Hyper-V server. See the RecoverAssist builder section in the appendix to learn more.</p>
---	---	---	--

Recovery checklist

Before performing a recovery, check that:

<input type="checkbox"/>	<p>The size allocated to each virtual disk is large enough.</p> <p>When you create the VM, its virtual disk/s must be the same size, or larger, than the physical disk/s that the backup was made from. To avoid drive size issues, we recommend recovering to a larger drive.</p>
<input type="checkbox"/>	<p>The VM being recovered to has enough disks.</p> <p>If the backup contains data from multiple disks, the VM being recovered to must contain at least the same number of virtual disks.</p>
<input type="checkbox"/>	<p>The type of VM created is compatible with the backup and bootable media.</p> <p>When you create the VM, you will be prompted to select Generation 1 or 2. You must make the correct selection, based on the BIOS / EFI used by the server that was backed up.</p> <ul style="list-style-type: none"> • Select a Generation 1 VM if the Backup and Bootable media were from a BIOS server. • Select a Generation 2 VM if the Backup and Bootable media were from an EFI server. <p>The bootable media and backup must both be created from either BIOS or EFI firmware.</p>

Recovery process

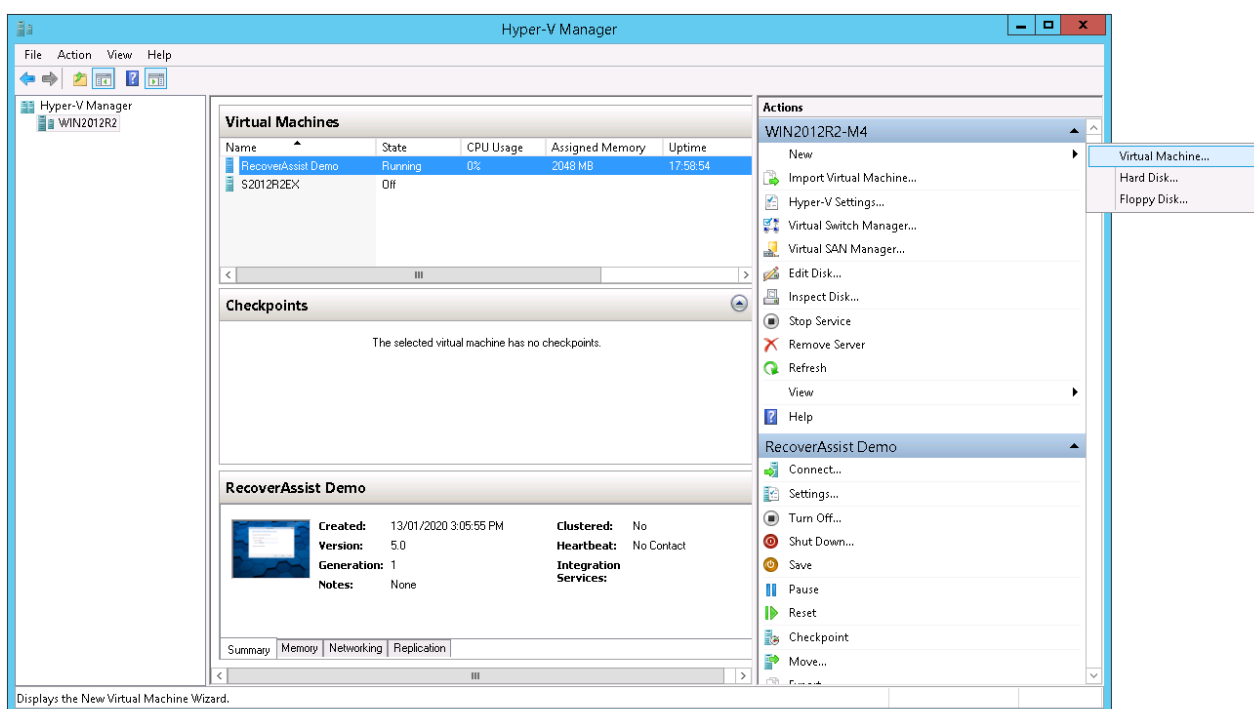
The section guides you through the process of recovering a physical server to a Hyper-V VM using a **System Protection** backup and a bootable **RecoverAssist media**.



Some of the steps in this scenario use the Microsoft **Hyper-V Manager** and **Server Manager**. To learn more about Hyper-V Manager and Server Manager, see Microsoft's online documentation.

To perform a physical to virtual (P2V) recovery:

1. Open the Hyper-V Server's **Hyper-V Manager** console.
2. Select **New** then **Virtual Machine...** from the **Actions** menu.



The **New Virtual Machine Wizard** will open and step you through the VM set up process.

3. Specify Name and Location.

Enter a Name for the VM into the field provided.

Check the **Location** where the VM will be created. To use a different location, tick **Store the virtual machine in a different location**, and **Browse** to and select the new location.

4. Specify Generation.

Select a **Generation 1 or 2** VM, and click **next**.

When selecting:

- Select a Generation 1 VM if the Backup and Bootable media were from a BIOS server.
- Select a Generation 2 VM if the Backup and Bootable media were from an EFI server.

5. Assign Memory.

Assign memory to the VM, and click **next**. The memory required will vary from system to system.

Ticking **Use Dynamic Memory for this virtual machine** means only the memory that is needed (from assigned memory) is used. This can result in the VM using less memory, though it may be less responsive.

6. Configure Networking.

Virtual network switches are set up in Hyper-V Manager and used to give VMs network access using the host's network adapter. You will need network access if the bootable media or backup are not stored on a local drive.

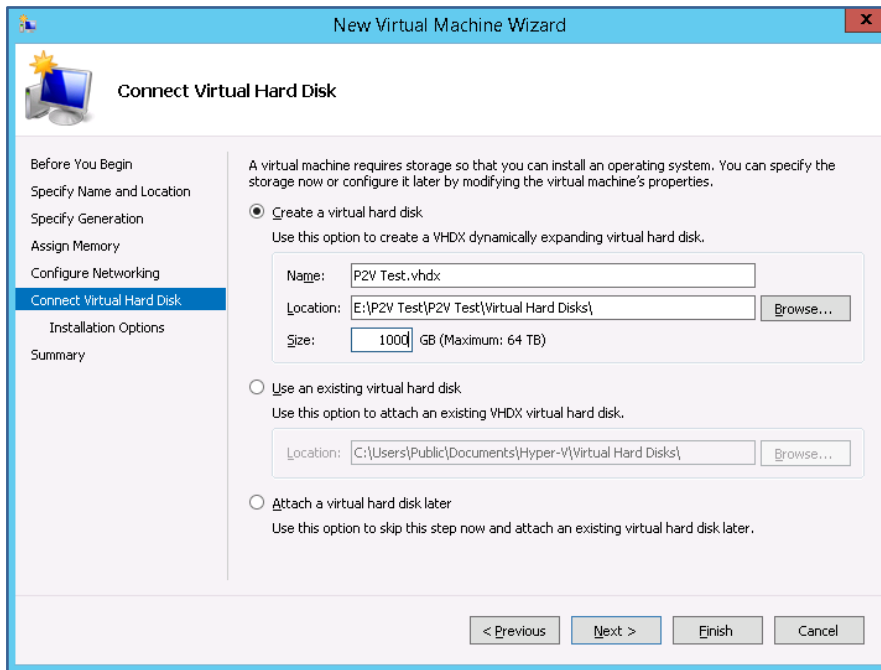
Select a Switch, and click **next**.



If there are multiple network cards on the physical host and not all of them are connected, make sure the **virtual switch** you select for your VM is using a **network card** that **is connected**.

7. Connect Virtual Hard Disk.

The virtual disks must be the **same size**, or larger, than the physical disk that the backup was made from.

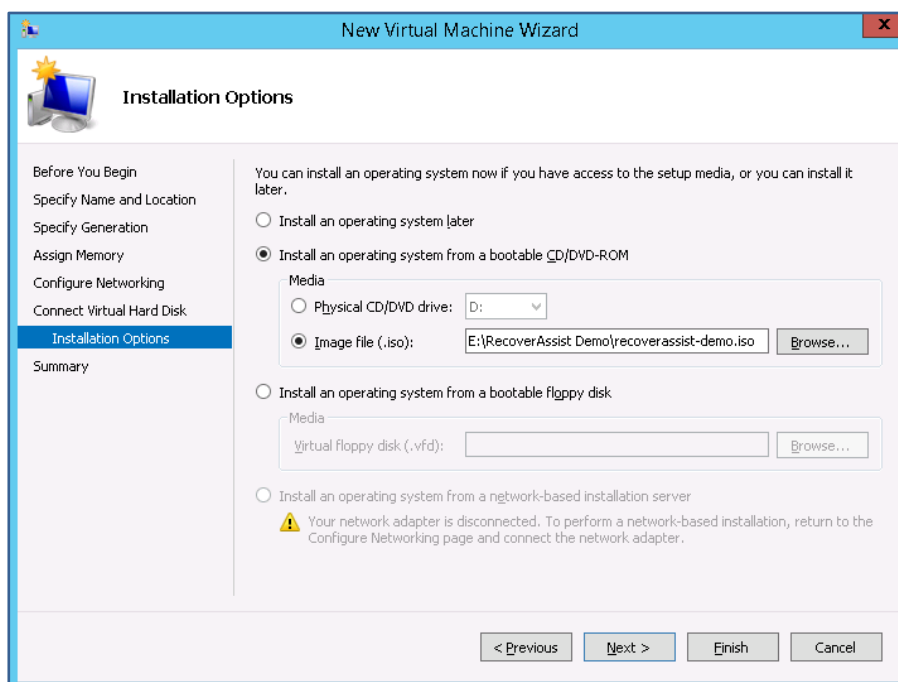


To add the virtual hard disk, complete the following steps:

- a) Select **Create a virtual hard disk**.
- b) Use the **Location** field if you want the VHD to be created in a different location to the default.
- c) Use the **Size** field to assign space to the virtual disk. The size of the virtual drive must be equal to or greater than the size of the hard disk that was backed up.
- d) Click **Next**.

8. Installation Options.

In this step, you will point the new VM to the bootable ISO to start the VM.



Review and complete the following steps:

- Choose **Install an operating system from a bootable CD/DVD-ROM**.
- Click **Image file (.iso)**.
- Browse to the **location of the RecoverAssist ISO** and select the ISO file.
- Click **Open**.
- Click **Next**.

If you used a **DVD or CD** for the bootable media, select **Physical CD/DVD drive**.

9. Summary.

Review the VM selections in the **Summary** step and select **Finish**.

The VM will now be created and added to the list of VMs in Hyper-V Manager.



If the VM **already has Windows Server installed**, you can set the VM to boot from a bootable media. To boot from an ISO, Connect to the VM and use the **Media** menu to **select Insert Disk** and then select the **bootable ISO**.

To boot from a CD, select the VM's **Settings**, and select the IDE or SCSI controller with the optical drive, then select the optical drive and click **Physical CD/DVD drive**. During the guest's start-up, press the **space bar** to boot from the attached media.

10. Right-click the VM and select **Start**.

11. Right-click the VM and select **Connect**.

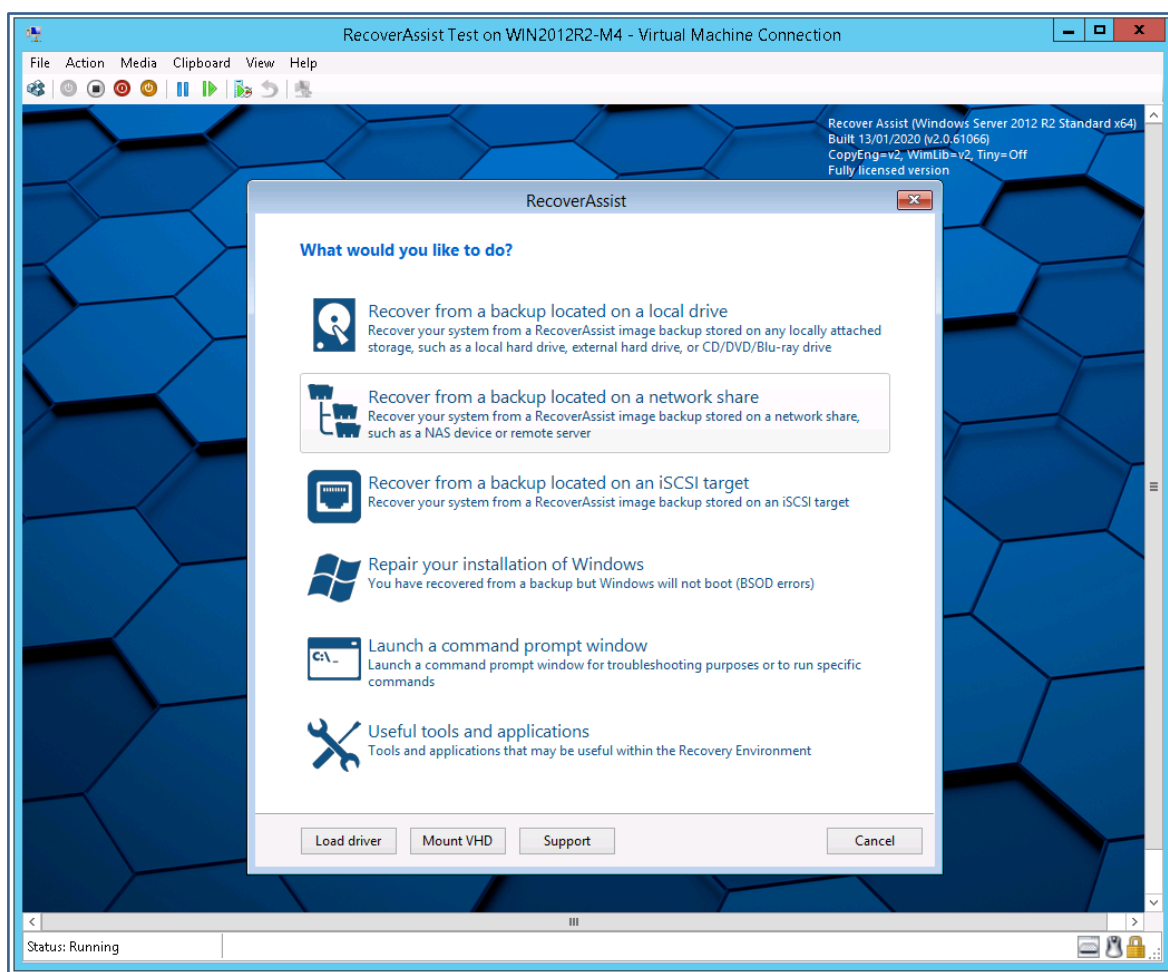
This will open a session so you can view what is happening in the VM.



If you receive the error, **An internal error occurred or the network path was not found**, the solution in this www.backupassist.com/blog/support/how-to-restore-a-server-2008-image-backup-to-a-new-hyper-v-vm-from-nas may help.

12. Wait for **RecoverAssist** recovery environment to open.

When the VM boots from the RecoverAssist media (ISO), you will see a progress bar then a blank screen or a Windows logo, depending on the operating system being recovered. The **RecoverAssist recovery environment** will then load.



RecoverAssist includes a set of **useful tools** that **can help** if you encounter any problems. These tools are described at the end of this scenario.

13. **Select a backup destination.**

Select the destination your backups are stored on from one of the three options at the top of the RecoverAssist UI.

The options are:

- Recover from a backup located on a **local drive**.
- Recover from a backup located on a **network share**.

- Recover from a backup located on an **iSCSI target**.



BitLocker encrypted backups

System Protection backups to **local media** can be **encrypted** with BitLocker. RecoverAssist will prompt you for the **BitLocker password** if it finds an encrypted backup. Enter the password used by the backup job to encrypt the backup.

Considerations:

- Even though a BitLocker key can unlock a drive to create a backup, the password is required to perform a recovery.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

14. Configure the backup destination.

Provide the information required to access the destination you selected.

The following sections explain how to configure each backup destination.

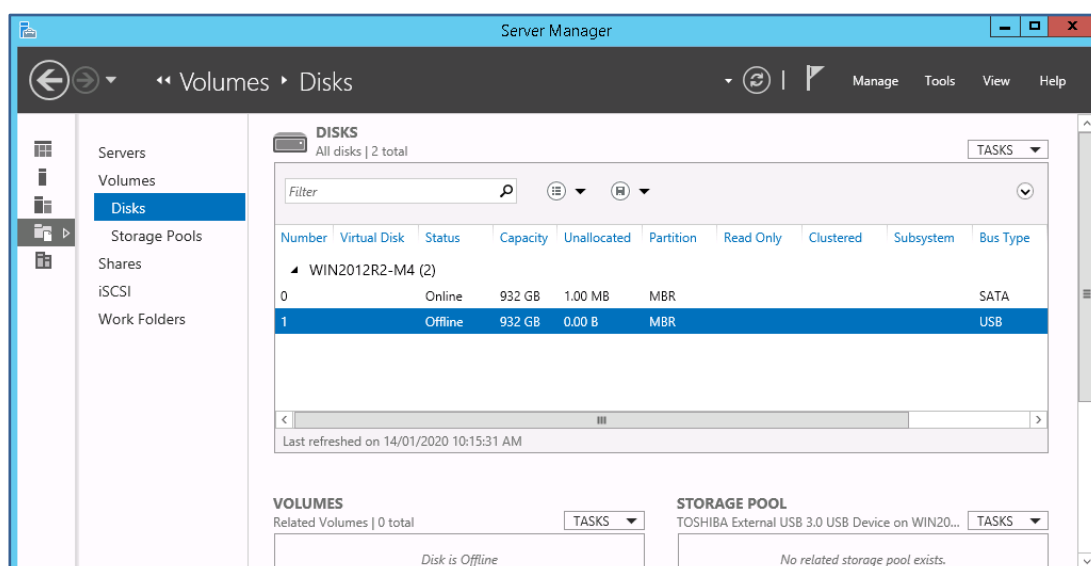
To configure the **local drive** destination:

Select **local drive** and **RecoverAssist will scan** all local drives **for System Protection backups**.

To give the VM access to an externally attached drive (e.g. External USB drive), you need to set up the attached drive as a pass-through disk.

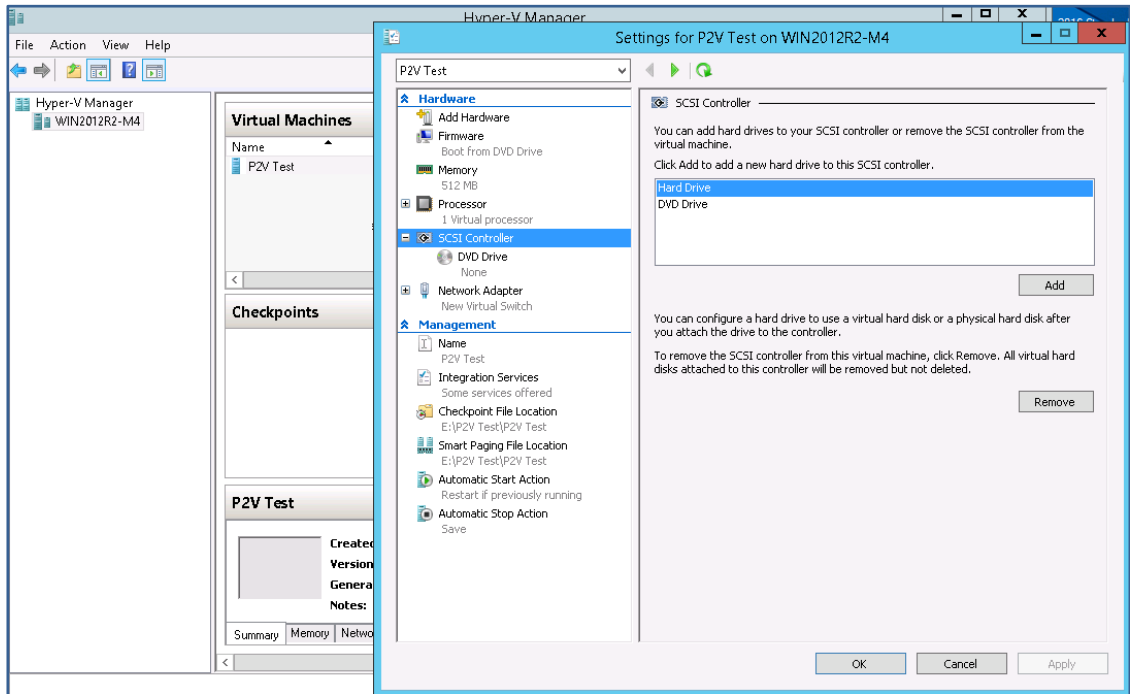
To set up a pass-through disk:

- Attach the drive** to the Windows Server running the Hyper-V Host.
- Open **Server Manager**.

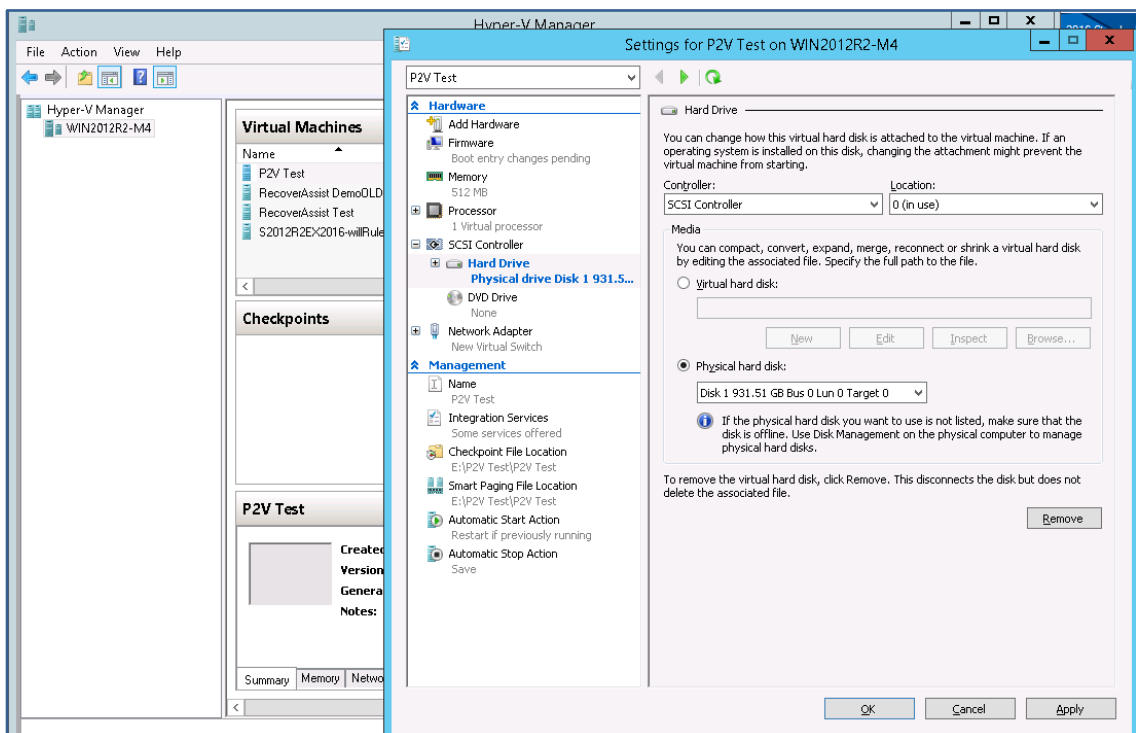


- Select **File and Storage Services** and click **Disks**.
- Right-click the attached drive and select **Take Offline**.
- Open **Hyper-V Manager**.

- f) Right-click the VM and select **Turn Off**.
- g) With the VM selected, click **Settings**.
- h) Select a free **IDE controller** or **SCSI controller**.
- i) Select **Hard Drive** and click **Add**.



- j) Click the **Physical Hard disk** radio button and click **OK**.



- k) Right-click the VM and select **Start**.

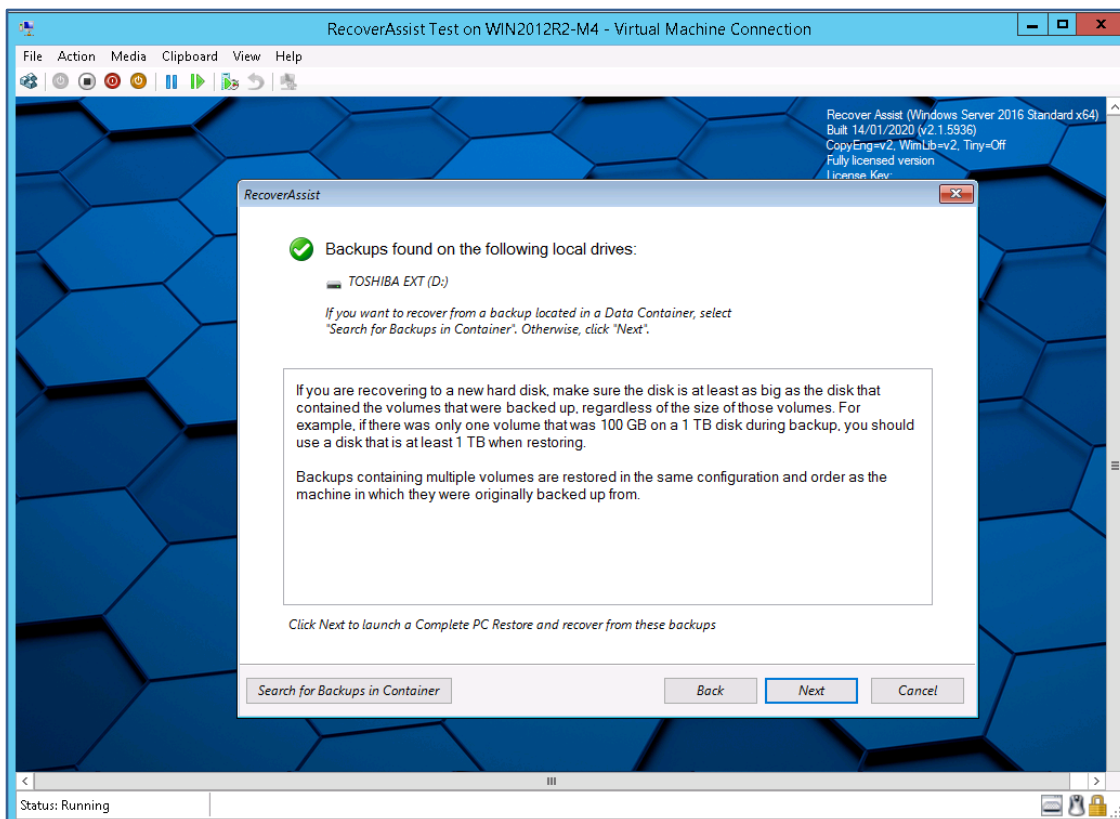
- l) Right-click the VM and select **Connect**.

This will open the VM and show the bootable RecoverAssist Environment load.

- m) Select **Recover from a backup located on a local drive**.

RecoverAssist will scan all local drives for System Protection backups.

A confirmation dialog will confirm if any backups were found.



If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.

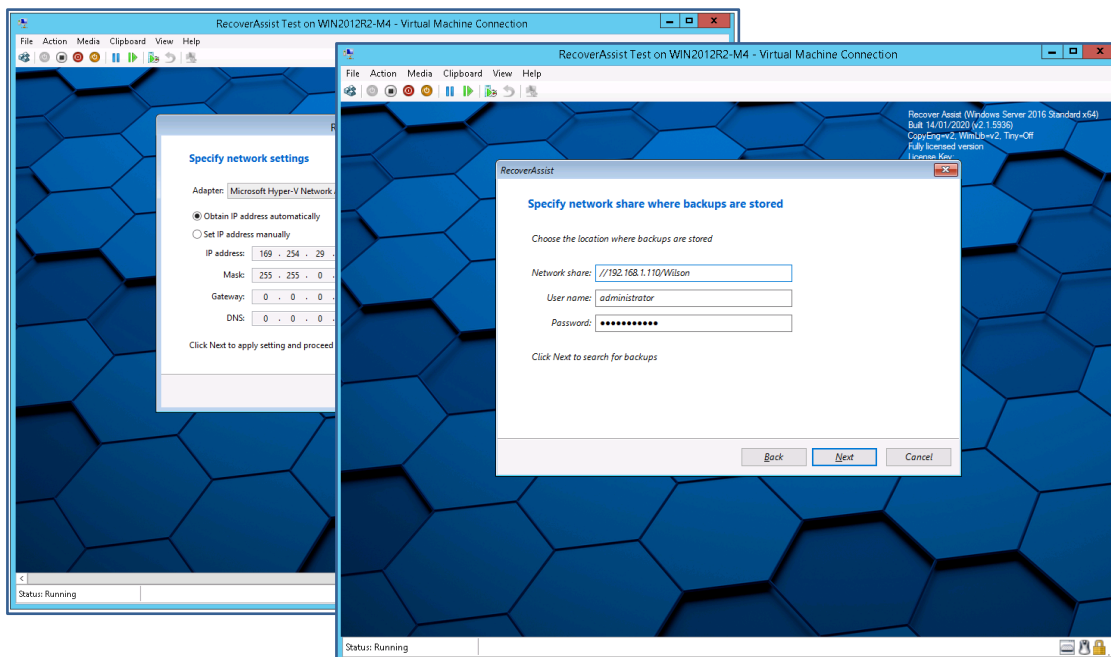
- n) Select **Next** then go to step 15, **confirm the selected backup**.

To configure the **network share destination**:

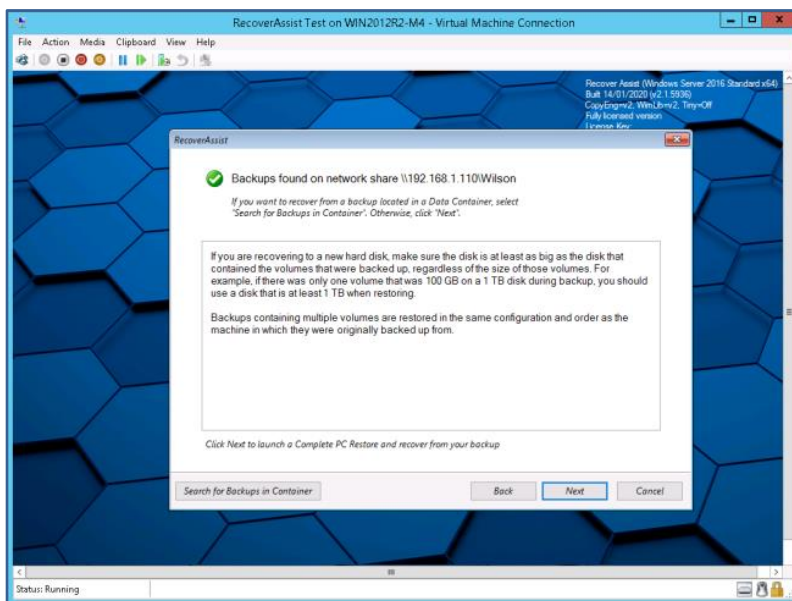
- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.

If you cannot find or configure the network adapter, you may need to manually load the network adapter drivers using the **Load driver** option on the **main RecoverAssist menu**.

- b) Use the **Specify network share where backups are stored** dialog to enter the DNS name or IP address of the share. Provide a **User name** and **Password** if the network location is configured with authentication credentials.



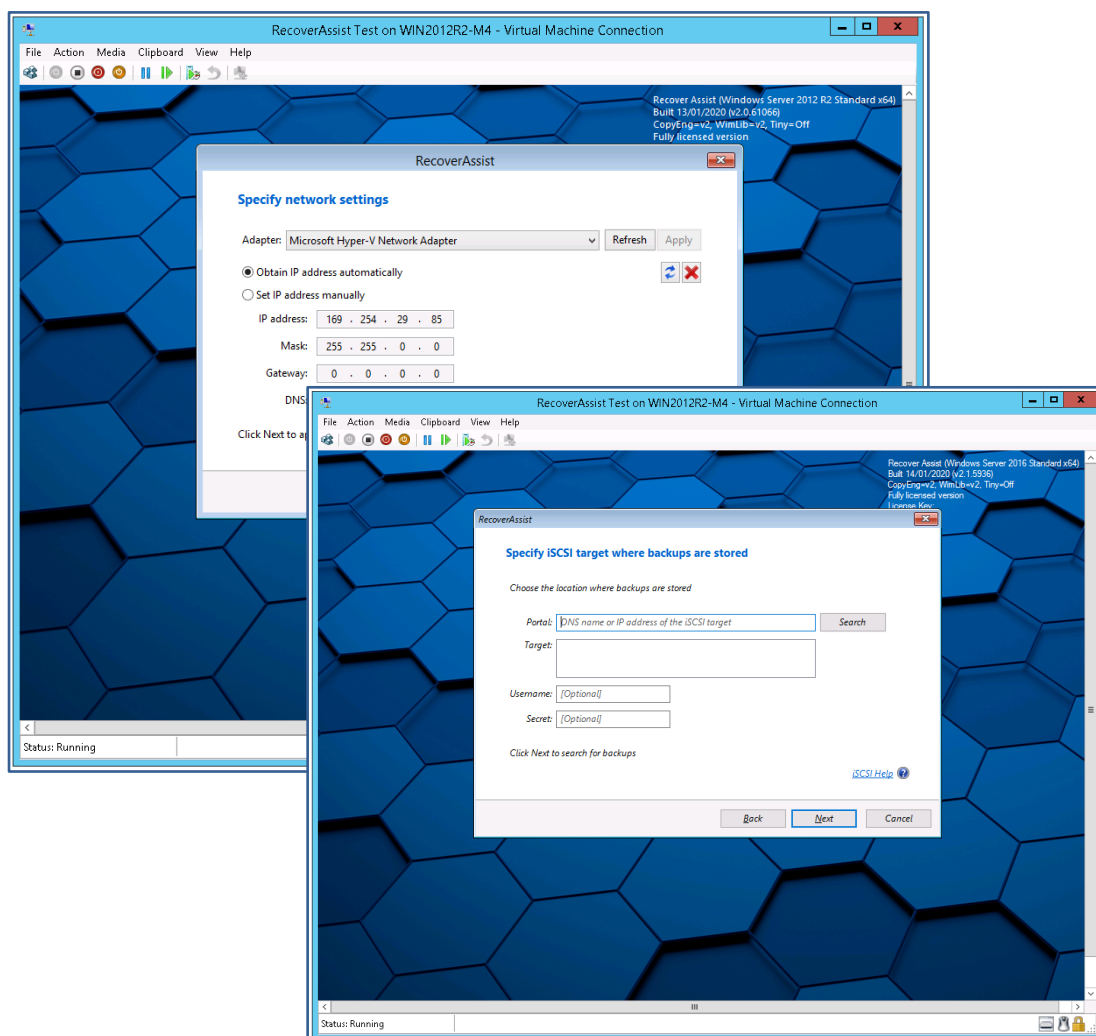
Once the destination has been checked, a dialog will confirm if any backups were found. If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.



- c) Select **Next** then go to step 15, **confirm the selected backup**.

To configure the iSCSI target destination:

- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.



- b) Use the **Specify iSCSI target where backups are stored** dialog to enter the DNS name or IP address of the share.

Click **Search** and RecoverAssist will search for the iSCSI target. If an iSCSI target is found, its details are added to the **Target** section.

Provide a **User name** and **Password** if the iSCSI target is configured with authentication credentials.

- c) Once the destination has been checked, a final dialog will confirm if any backups were found.

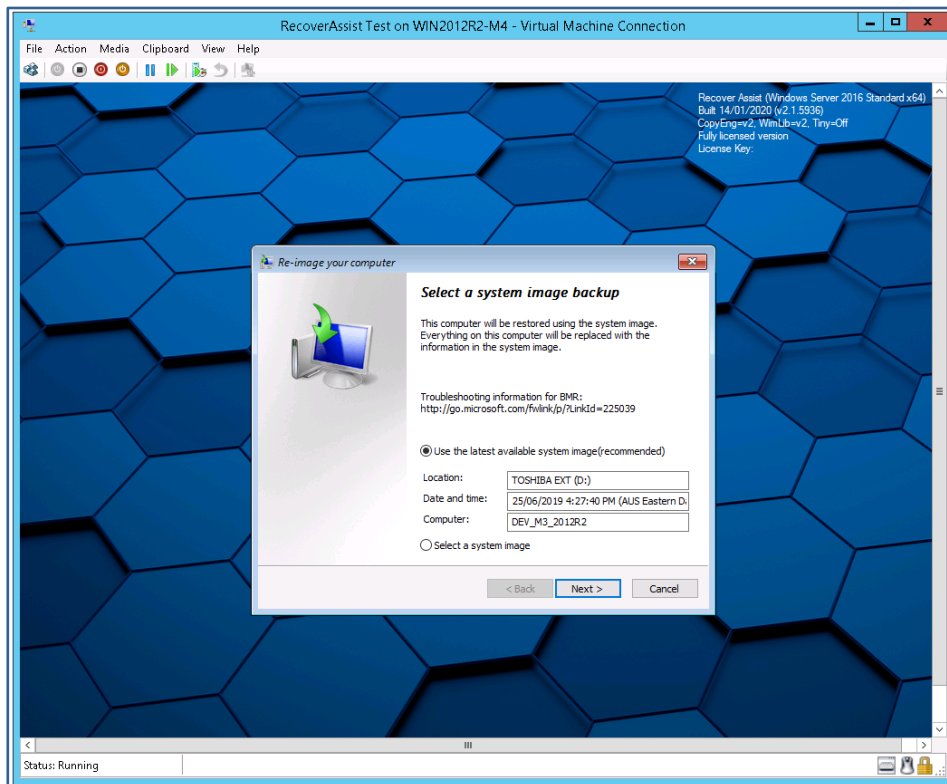
There are **no BitLocker** prompts or **Data Container** options as these features are not used with **iSCSI targets**.

- d) **Next** then go to step 15, **confirm the selected backup**.

15. Confirm the selected backup.

The **Select a system image backup** dialog will open and show the selected backup. This will be **the most recent backup**. The date the backup was created is shown in the **date and time** field.

If multiple backups are available, the **Select a system image** option will allow you to select a different backup.



16. Start the recovery process.

Confirm the two final Windows recovery dialogs:

- At the **Choose additional restore options** dialog, select **Next**.
- On the final screen, update the **Date** and **Time** if they are incorrect, and select **Finish**.

When you select **Finish**, the full server recovery will start.

17. Remove the bootable media.

When the recovery starts, disconnect the bootable ISO from the VM, or the recovery Environment will load again when the VM reboots.

To remove the bootable ISO:

- Select the VM in **Hyper-V Manager** and select **Settings**
- Select the **Controller** with the DVD/Drive. You will see the **ISO selected** under Media
- Click **None** then **Apply**.

Congratulations – your server is now being recovered to a VM.



Recovery support software

The following RecoverAssist recovery environment options can assist with a recovery.

Repair your installation of Windows

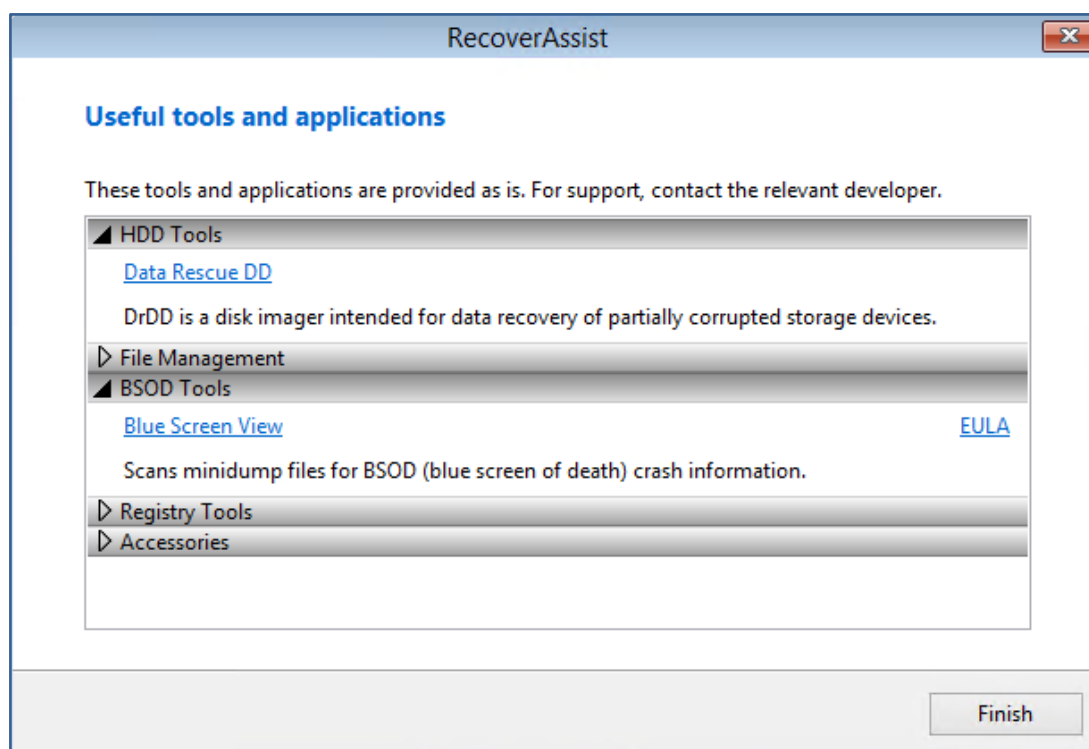
This option loads the **Windows Recovery Environment** and allows you to attempt a repair of the operating system if you encountered a bluescreen or Windows load failure. Using the **repair function** is not required for systems recovered within the RecoverAssist recovery environment.

Launch a command prompt window

This option launches a Windows **command prompt** so you can run the command-line tools included with RecoverAssist. The tools include diskpart.exe, bootsect.exe and regedit.exe.

Useful tools and applications

This option gives access to the applications and tools that you selected when you created your RecoverAssist media. These tools can be used to perform **diagnostics** and **troubleshoot** problems. Clicking on the name of an application will launch that application.



Additional options

The three buttons at the bottom of the Recovery environment give access to these features:

- **Load driver** - loads any **additional device drivers** that were included when creating the recovery environment.
- **Mount VHD** - mounts any VHD (e.g. a **Windows Backup image**). After mounting the VHD, you can access its files using a local drive letter. This is not used to mount Data Containers.

Full server recovery for Hyper-V environments

The scenarios in this section will guide you through the process of **recovering an entire Hyper-V Server** or individual VMs to the original or a different Hyper-V Server.

3 Recover a Hyper-V Host and all guest VMs to new metal

This scenario explains how to **perform a full Hyper-V Server recovery**, and check that the VMs are running after the recovery.




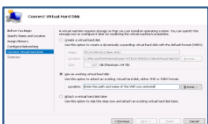


In a nutshell: A full Hyper-V Server recovery can seem daunting at first, but all you're doing is using a bootable media to start a server and open a recovery environment, which you will then use to locate a backup and recover the server.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.


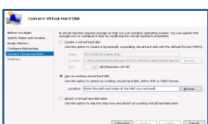

Recovery requirements

To perform a full Hyper-V Server recovery, you will need the items shown in Option 1 or Option 2.

Option 1: if your System Protection job does not use a bootable backup destination.

<p>A physical server</p>  <p>A new server or the original server. An original server should have new disks if recovering from ransomware</p>	<p>Hyper-V Manager</p>  <p>Hyper-V Manager will be used to check each VMs setting and then start each VM.</p>	<p>Bare-metal backup</p>  <p>Must be a System Protection backup created with Back up Entire System ticked in the Selections screen.</p>	<p>RecoverAssist media</p>  <p>This media is created using the Recover tab. See the RecoverAssist builder section in the appendix to learn more.</p>
---	---	--	--

Option 2: if your System Protection job uses a bootable backup destination.

<p>A physical server</p>  <p>A new server or the original server. An original server should have new disks if recovering from ransomware</p>	<p>Hyper-V Manager</p>  <p>Hyper-V Manager will be used to check each VMs setting and then start each VM.</p>	<p>Bare-metal backup</p>  <p>Must be a System Protection backup created with Back up Entire System ticked in the Selections screen.</p>	<p>Learn more</p> <p>System Protection bare-metal backups to external USB drives are made bootable, unless Make media bootable on the Set up destination step is unticked. A bootable backup can boot a server into a recovery environment, without a separate boot media.</p>
---	---	--	---

Recovery checklist

Use this checklist to make sure the **disks and firmware** on the physical **server you are recovering to** are **compatible** with **your backup**.

<input type="checkbox"/>	<p>Each disk being recovered to is large enough.</p> <p>The server must have a physical disk/s the same size, or larger, than the physical disk/s that the backup was made from.</p> <p>If you backed up a 1TB drive and plan to recover to a 1TB drive, check the manufacturer's specifications as different models of the same size disk can have minor size differences.</p> <p>To avoid drive size issues, we recommend recovering to a larger drive.</p>
<input type="checkbox"/>	<p>The server being recovered to has enough disks.</p> <p>If the backup contains data from multiple disks, the server being recovered to must contain at least the same number of disks.</p>
<input type="checkbox"/>	<p>The server being recovered to has compatible firmware.</p> <p>Backups of servers that use BIOS cannot be restored to servers that use EFI, and backups of servers that use EFI cannot be restored to servers that use BIOS. Some EFI servers allow you to choose EFI or a legacy BIOS option when selecting the boot device.</p> <p>The bootable media and backup must both be created from either BIOS or EFI firmware.</p>
<input type="checkbox"/>	<p>The disks on the server being recovered to use a compatible disk format.</p> <p>A backup of a server that uses BIOS, may not work if you are recovering to a server that has disks formatted with Advanced Format (4k sectors).</p>

Recovery process

This section guides you through the process of recovering a server using a **System Protection** backup and **RecoverAssist**.

To perform a full server recovery:

1. **Attach the bootable media to the server.**

The media will be either a **bootable RecoverAssist media** or a **bootable backup media**.

2. **Start the server.**

When the server starts, it should **detect the bootable media** and **start the boot process**.

Understanding the boot process can help if any problems are encountered.

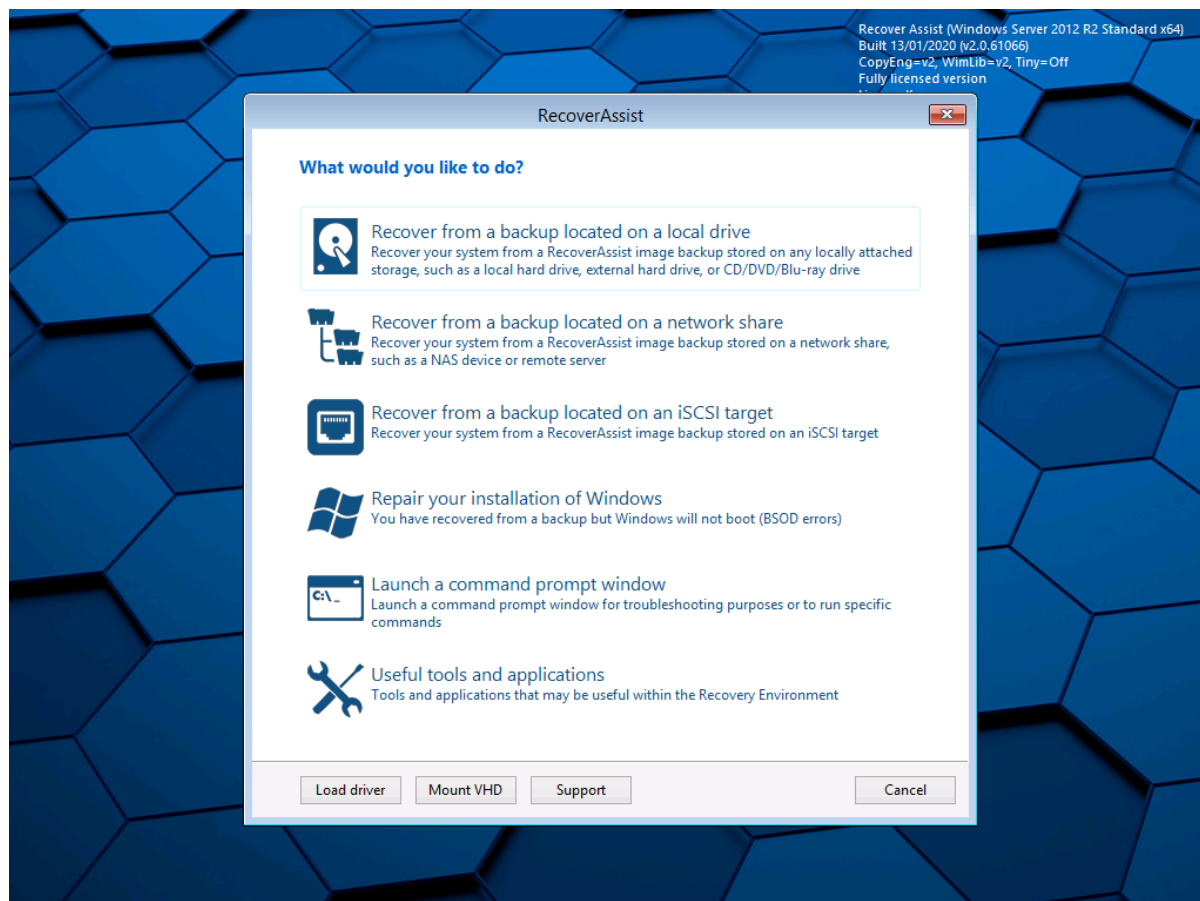


Boot process: Servers use firmware called **BIOS or EFI to access critical hardware**. When a server starts, this firmware checks the hardware and beeps once if the checks are successful. Additional beeps can indicate a hardware problem. Once a server has successfully checked its hardware, **it looks for an operating system**. BIOS and EFI are configured with a device order for the operating system's location. The **Bootable media must appear in this device order** before media that may load a failed operating system. To access the BIOS/EFI settings, press the required function key, which will be displayed on screen. E.g. F8 or F12.

3. Wait for the RecoverAssist recovery environment to open.

When the server boots from the RecoverAssist media, you will see a progress bar then a blank screen or a Windows logo, depending on the operating system being recovered.

The **RecoverAssist recovery environment** will then load.



RecoverAssist includes a set of **useful tools** that **can help** if you encounter any problems. These tools are described at the end of this scenario.

4. Select a backup destination.

Select the destination your backups are stored on from one of the three options at the top of the RecoverAssist UI.

The options are:

- Recover from a backup located on a **local drive**.
- Recover from a backup located on a **network share**.
- Recover from a backup located on an **iSCSI target**.



BitLocker encrypted backups

System Protection backups to **local media** can be **encrypted** with BitLocker. RecoverAssist will prompt you for the **BitLocker password** if it finds an encrypted backup.

Enter the password used by the backup job to encrypt the backup. This is the password entered in the **Set up destination** step when the backup's job was created.

Considerations:

- Even though a BitLocker key can unlock a drive to create a backup, the password is required to perform a recovery.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

5. Configure the backup destination

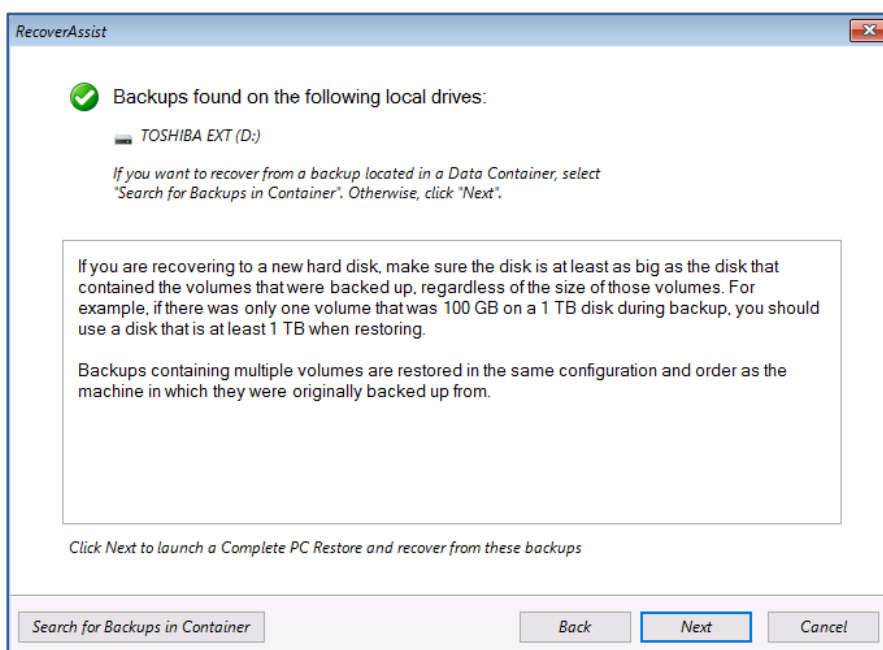
Provide the information required to access the destination you selected.

The following sections explain how to configure each backup destination.

To configure the **local drive** destination:

- Select **local drive** and RecoverAssist will scan all local drives for System Protection backups.

A confirmation dialog will confirm if any backups were found.



If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.

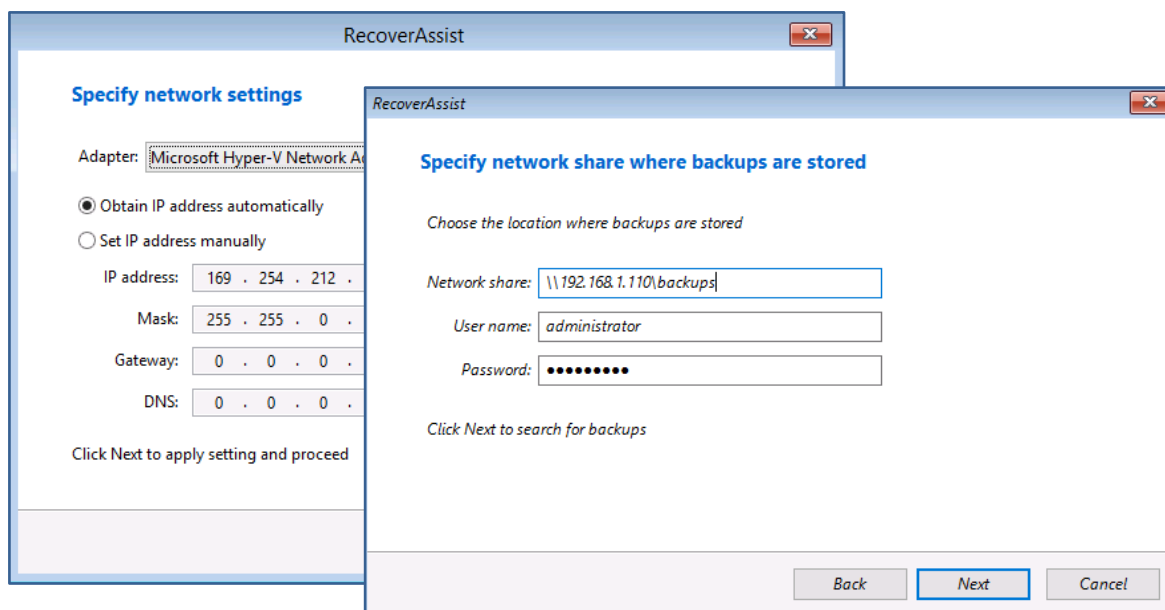
- Select **Next** to progress to the **Windows dialogs** explained below in step 6.

To configure the network share destination:

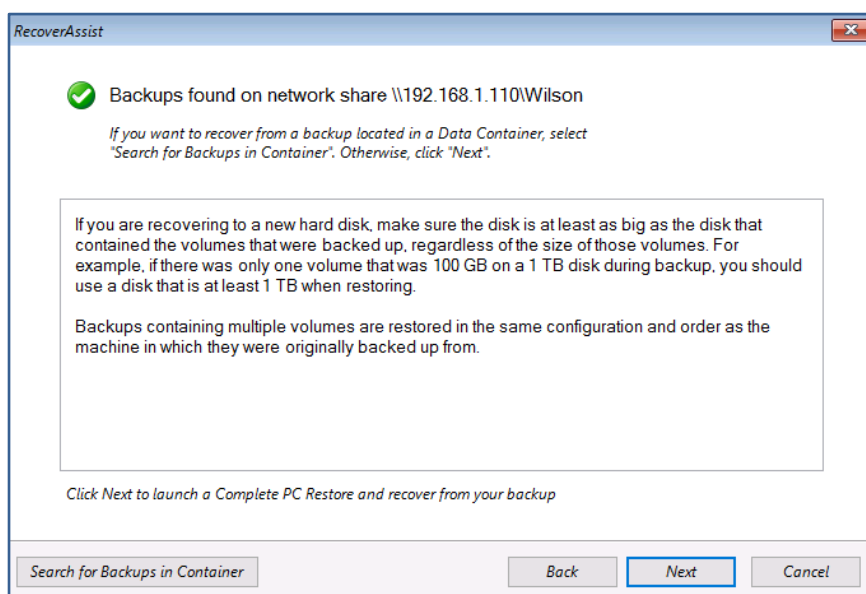
- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.

If you cannot find or configure the network adapter, you may need to manually load the network adapter drivers using the **Load driver** option on the **main RecoverAssist menu**.

- b) Use the **Specify network share where backups are stored** dialog to enter the DNS name or IP address of the share. Provide a **User name** and **Password** if the network share or NAS device is configured with authentication credentials.



Once the destination has been checked, a dialog will confirm if any backups were found. If the backups are in a **Data Container**, click the **Search for Backups in Container** button and set the location containing the backups.



- c) Select **Next** then go to step 6, **confirm the selected backup**.

To configure the iSCSI target destination:

- a) Use the **Specify network settings** dialog to provide the network adapter and IP information. Network drivers added to the RecoverAssist Builder are loaded as part of the boot process.

RecoverAssist

Specify network settings

Adapter: Microsoft Hyper-V Network Adapter Refresh Apply

Obtain IP address automatically Set IP address manually

IP address: 169 . 254 . 168 . 245

Mask: 255 . 255 . 0 . 0

Gateway: 0 . 0 . 0 . 0

DNS: 0 . 0 . 0 . 0 Dynamic

Click Next to apply setting and proceed

Back Next Cancel

- b) Use the **Specify iSCSI target where backups are stored** dialog to enter the DNS name or IP address of the share.

Click **Search** and RecoverAssist will search for the iSCSI target. If an iSCSI target is found, its details are added to the **Target** section.

Provide a **User name** and **Password** if the iSCSI target is configured with authentication credentials.

RecoverAssist

Specify iSCSI target where backups are stored

Choose the location where backups are stored

Portal: DNS name or IP address of the iSCSI target Search

Target:

Username: [Optional]

Secret: [Optional]

Click Next to search for backups

[iSCSI Help](#)

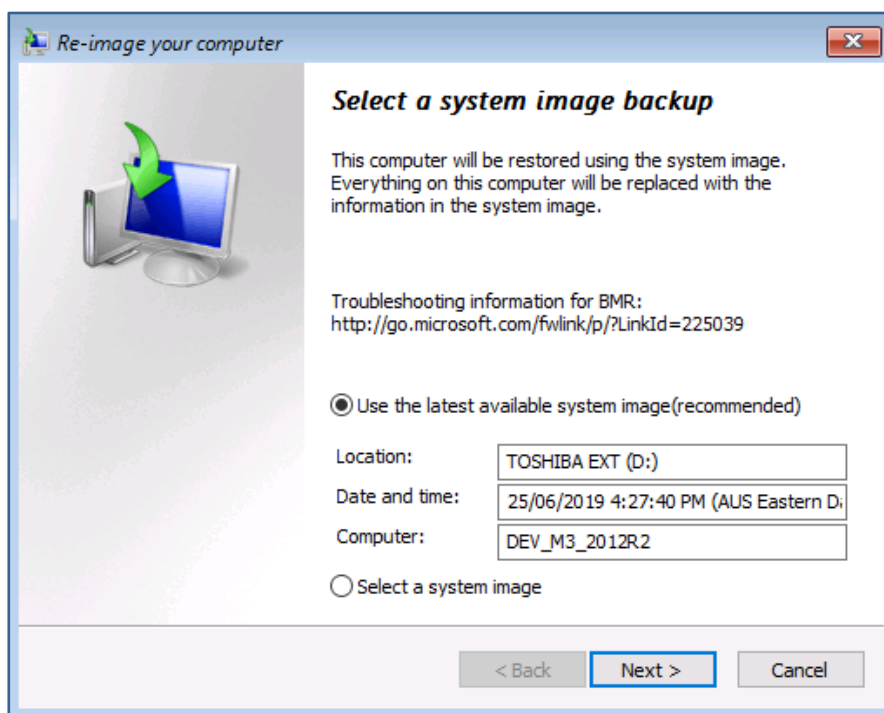
Back Next Cancel

- c) Once the destination has been checked, a final dialog will confirm if any backups were found. There are **no BitLocker** prompts or **Data Container** options as these features are not used with **iSCSI targets**.
- d) Select **Next** then go to step 6, **confirm the selected backup**.

6. Confirm the selected backup.

The **Select a system image backup** dialog will open and show the selected backup. This will be **the most recent backup**. The **date and time** field shows when the backup was created.

If multiple backups are available, the **Select a system image** option can be used to select a different backup.



you choose, **Select a system image**, the next step will show a table with the most recent backup data. This is to confirm that this is the media you want to select the image from. When you click **Next**, you will be given the option to **select the backup** you want to recover from.

7. Start the Recovery process.

Confirm the two final Windows recovery dialogs:

- At the **Choose additional restore options** dialog, select **Next**.
- On the final screen, update the **Date** and **Time** if they are incorrect, and select **Finish**.

When you select **Finish**, the full server recovery will start.

8. Remove bootable media.

When the recovery starts, disconnect the bootable media from the server or the recovery environment will load when the server reboots.

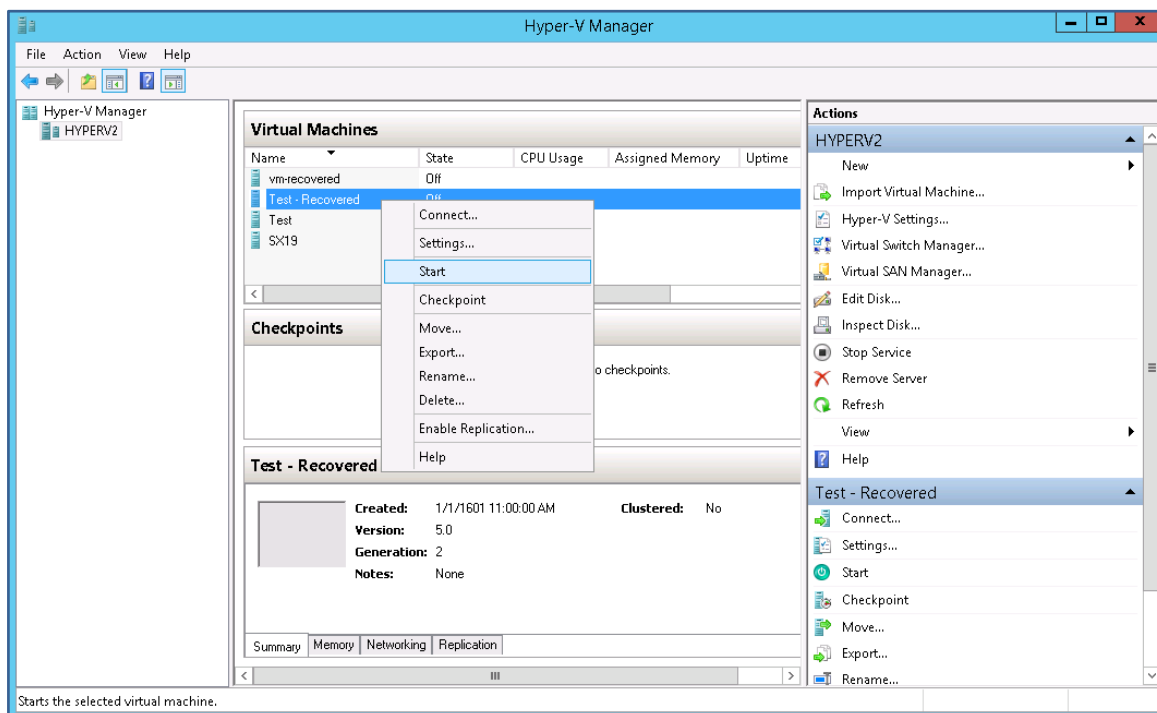
Now that the Hyper-V Server has been recovered, you can start the VMs.

9. **Log into the server.**

Use the administrator credentials for the server that was backed up and recovered.

10. **Open the Hyper-V Manager console.**

11. **Right-click each VM and select Start.**



If a VM does not start, select **Settings** and review the VMs configurations. Check that the memory and network adapter settings are compatible with the memory and network adapter set up on the physical host server.

Congratulations – your Hyper-V Server has been recovered.



Recovery support software

The following RecoverAssist recovery environment options can assist with a recovery.

Repair your installation of Windows

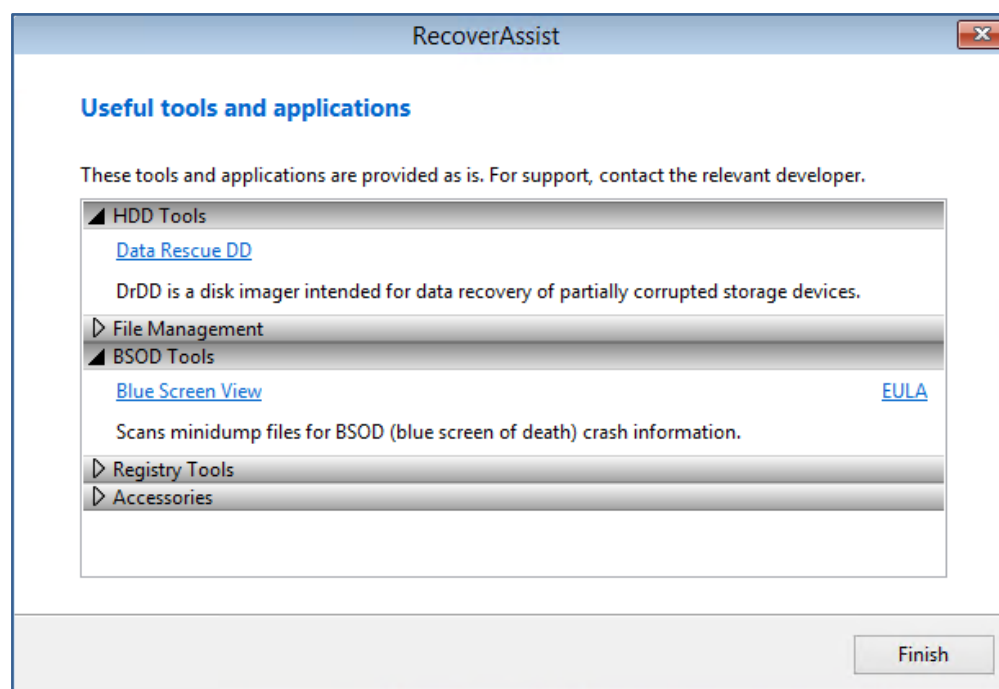
This option loads the **Windows Recovery Environment** and allows you to attempt a repair of the operating system if you encountered a bluescreen or Windows load failure. Using the **repair function** is not required for systems recovered within the RecoverAssist recovery environment.

Launch a command prompt window

This option launches a Windows **command prompt** so you can run the command-line tools included with RecoverAssist. The tools include diskpart.exe, bootsect.exe and regedit.exe.

Useful tools and applications

This option gives access to the applications and tools that you selected when you created your RecoverAssist media. These tools can be used to perform **diagnostics** and **troubleshoot** problems. Clicking on the name of an application will launch that application.



Additional options

The three buttons at the bottom of the Recovery environment give access to these features:

- **Load driver** - loads any **additional device drivers** that were included when creating the recovery environment.
- **Mount VHD** - mounts any VHD (e.g. a **Windows Backup image**). After mounting the VHD, you can access its files using a local drive letter. This is not used to mount Data Containers.

4 Recover specific Hyper-V guest VM to the same host

This scenario uses the **Recover tab's Full VM Recovery** option to recover a virtual machine (VM) to the host that it was backed up on, using a System Protection backup.


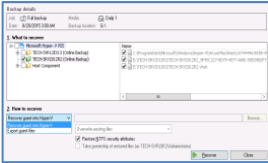
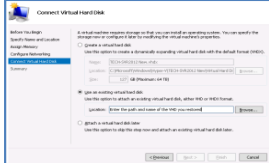
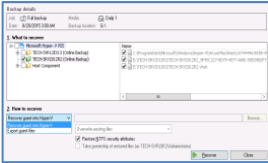
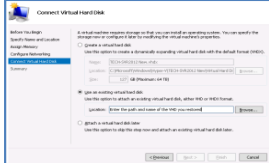
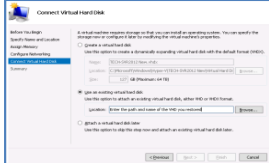


In a nutshell: In this scenario, you will choose a VM backup and recover that VM to a folder on the host server. You will then create a new VM using the recovered VM's .vhdx file. The new VM can then take over the functions of the VM that was backed up.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform a Full VM Recovery, you will need BackupAssist and:

 <h4>A VM backup</h4> <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the virtual machine.</p> <th data-bbox="608 896 1002 1261">  <h4>Integrated Restore Console</h4> <p>BackupAssist will use the Integrated Restore Console to recover the selected VM to a folder on the host.</p> <th data-bbox="1007 896 1414 1261">  <h4>Hyper-V Manager</h4> <p>Hyper-V Manager will be used to create a VM using the recovered VM's image file, and then start that new VM.</p> </th></th>	 <h4>Integrated Restore Console</h4> <p>BackupAssist will use the Integrated Restore Console to recover the selected VM to a folder on the host.</p> <th data-bbox="1007 896 1414 1261">  <h4>Hyper-V Manager</h4> <p>Hyper-V Manager will be used to create a VM using the recovered VM's image file, and then start that new VM.</p> </th>	 <h4>Hyper-V Manager</h4> <p>Hyper-V Manager will be used to create a VM using the recovered VM's image file, and then start that new VM.</p>
--	--	---

Recovery checklist

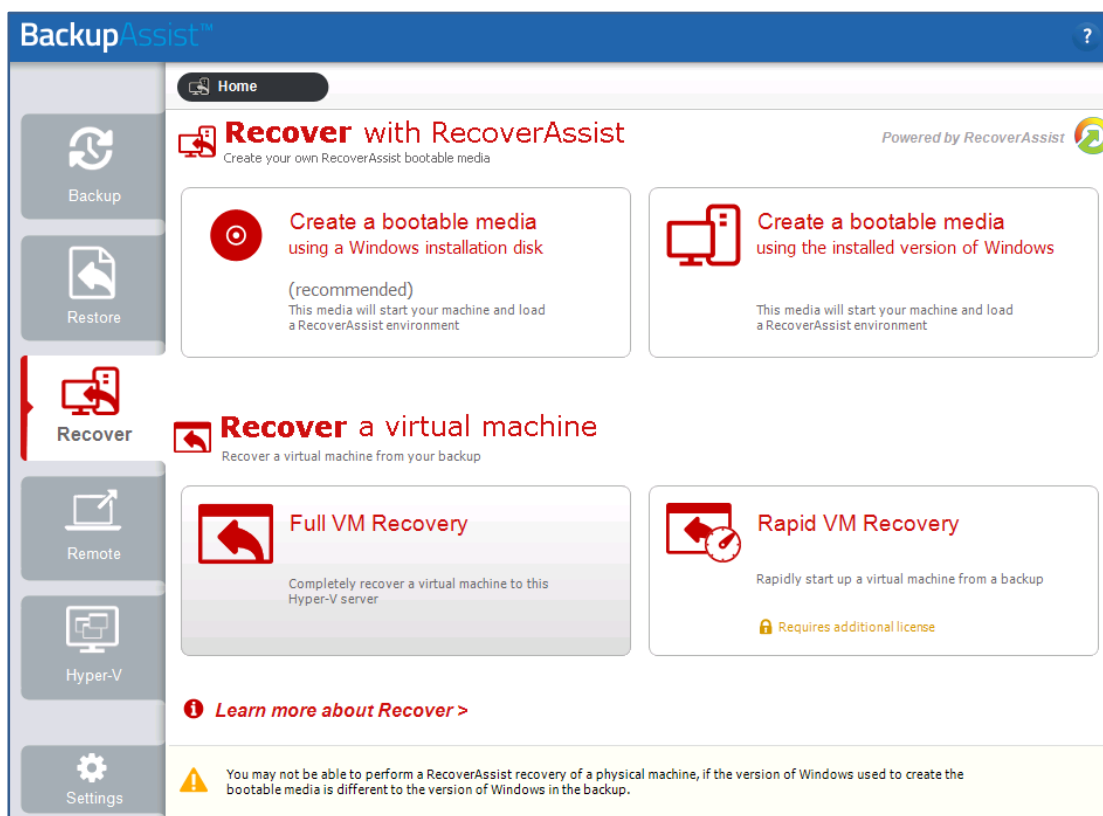
Use this checklist to make sure you have the required information:

<input type="checkbox"/>	The location on the Hyper-V Server that is large enough for the VM to be recovered to. For optimal performance, this folder should not be on the same drive as the operating system.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To recover a Hyper-V VM, follow these steps:

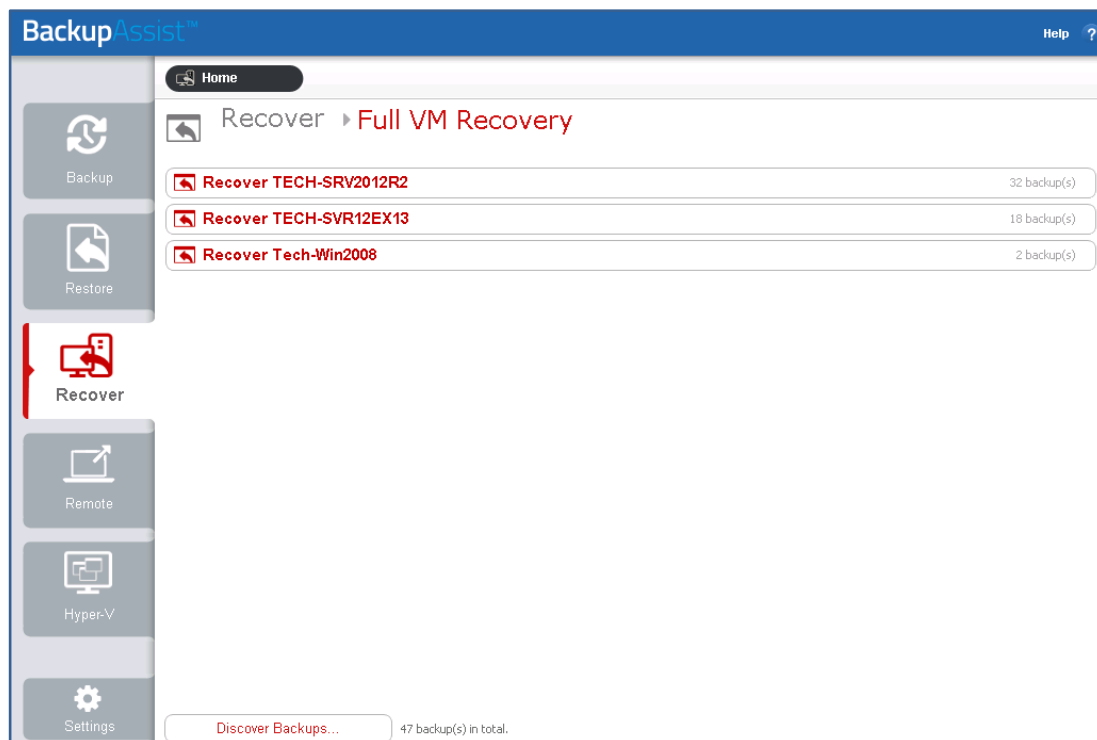
1. **Select BackupAssist's Recover tab.**
2. **Click Full VM Recovery.**



The **Full VM Recovery screen** will open and **display** all the **VMs** that have been backed up.

3. Select the VM.

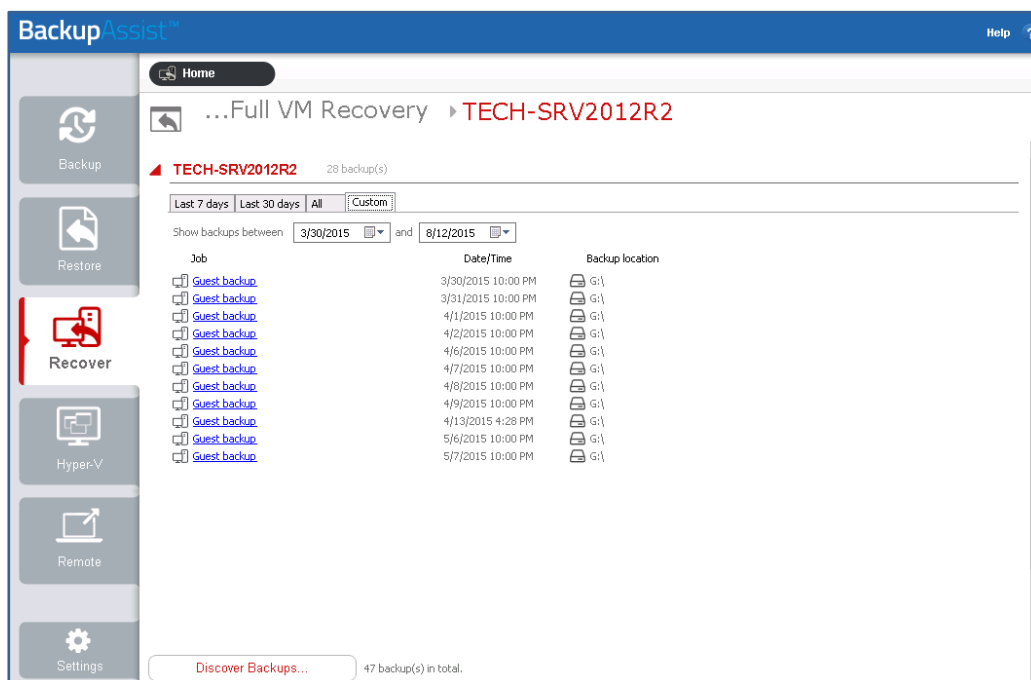
When you click on the VM that you want to recover, the screen will display all available backups of that VM.



4. Select a backup.

Select the backup that you want to recover the VM from.

The **tabs above a VM's backup list** can be used to **filter the backups shown**. If there are many backups, the filters can help locate the backup you need.

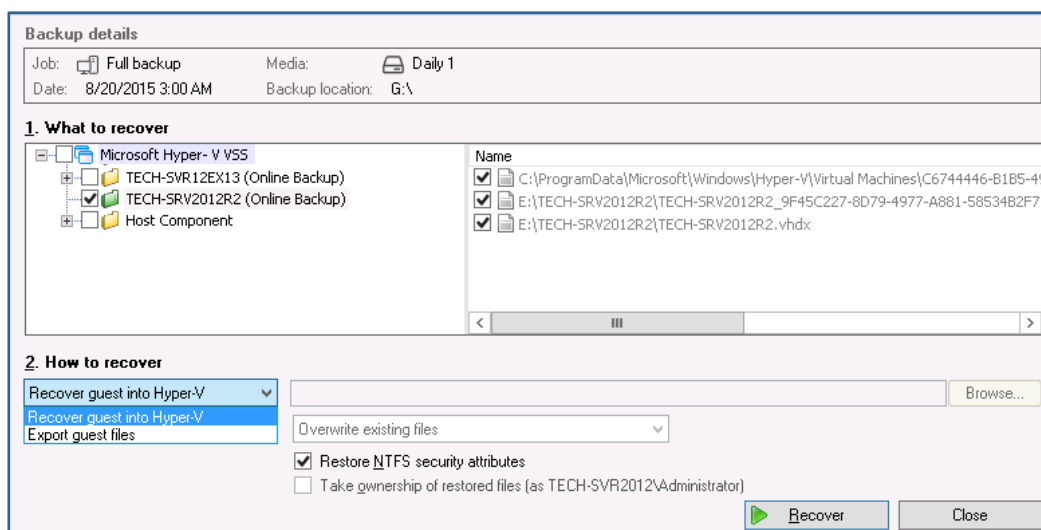


The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a date range and display backups for that period.

5. Select the VM in the backup.

When you select a backup, the **Integrated Restore Console** will **display the VMs** that were backed up. Use the **What to recover** pane to **tick the box** next to the **VM that you want to recover**. You can select more than one VM but they will share the restore settings used.



6. Set how to recover the VM.

The **How to recover** drop-down box is used to select the recovery method.

The recovery methods are:

- **Recover guest into Hyper-V** – this will recover the guest (VM) to its original location.
- **Export guest files** – this will copy the guest (VM) files to a selected location.

In this scenario, we will use the **Export guest files** option. This allows us to get a recovered copy of the VM running, while still having the original VM available for ongoing investigation if required.

7. Select the recovery destination.

Use the **Browse** button to **select a folder to restore the VM to**. This location must be large enough for the VM. For optimal performance, the operating system's drive should not be used because the VM will be run from this location.

8. Click the Recover button.

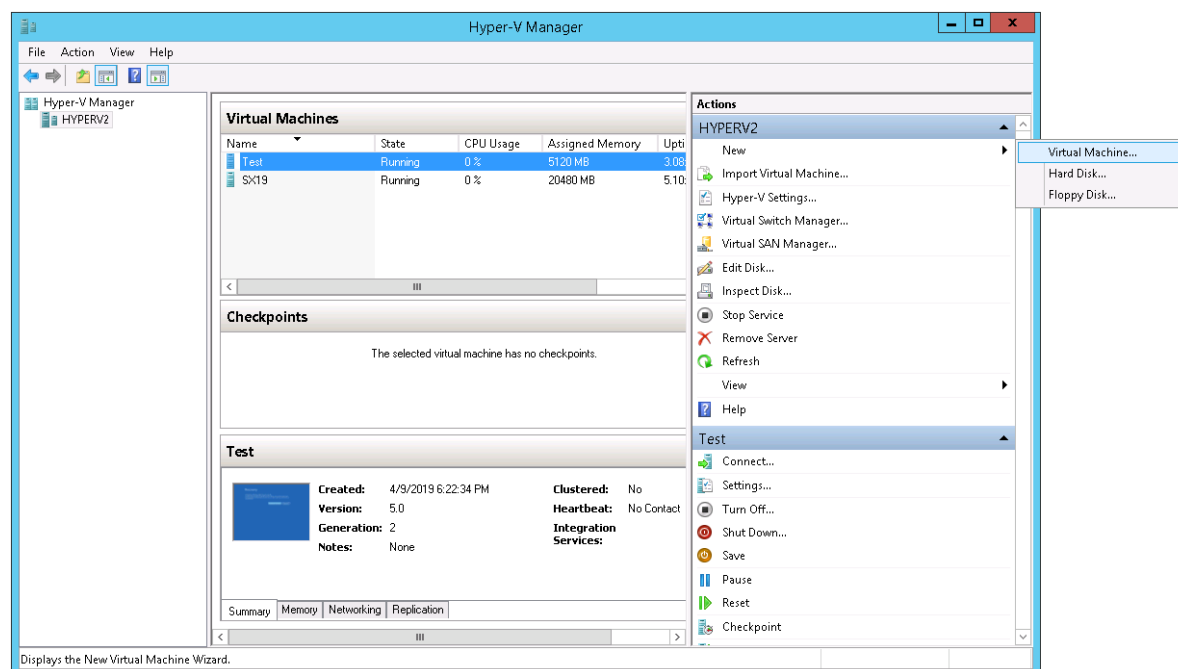
The recovery process will begin and the **Integrated Restore Console** will display its **progress**.

Select **Done** and **Close** when the recovery has finished.

We will now use the recovered VM's .vhdx file to create a new VM.

9. Open the Hyper-V Manager console.

10. Select **New** then **Virtual Machine...** from the **Actions** menu.

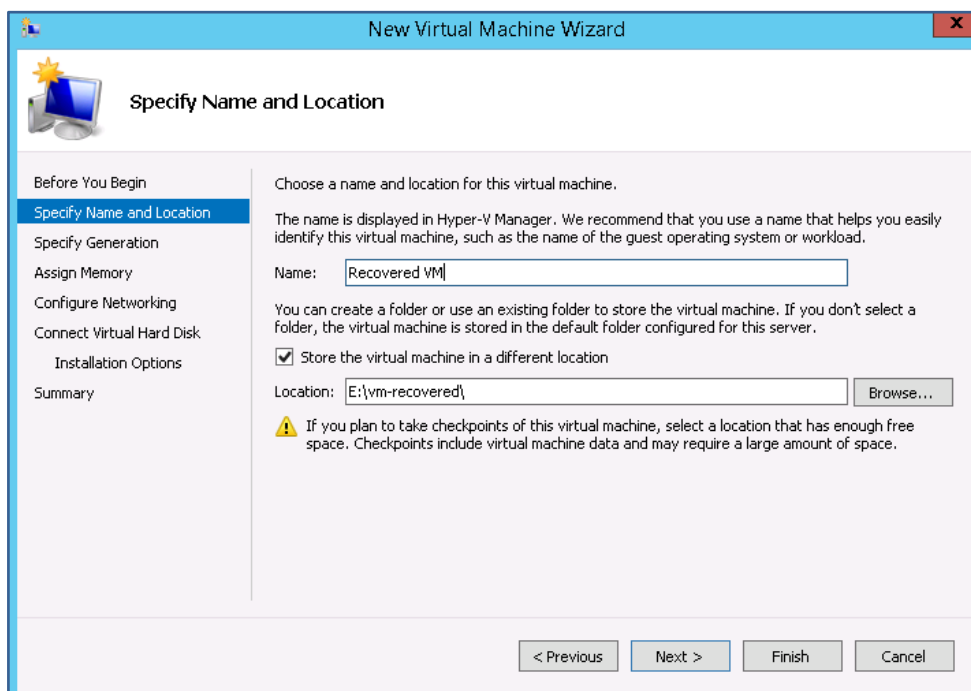


The **New Virtual Machine Wizard** will open and step you through the VM set up process.

11. Specify Name and Location.

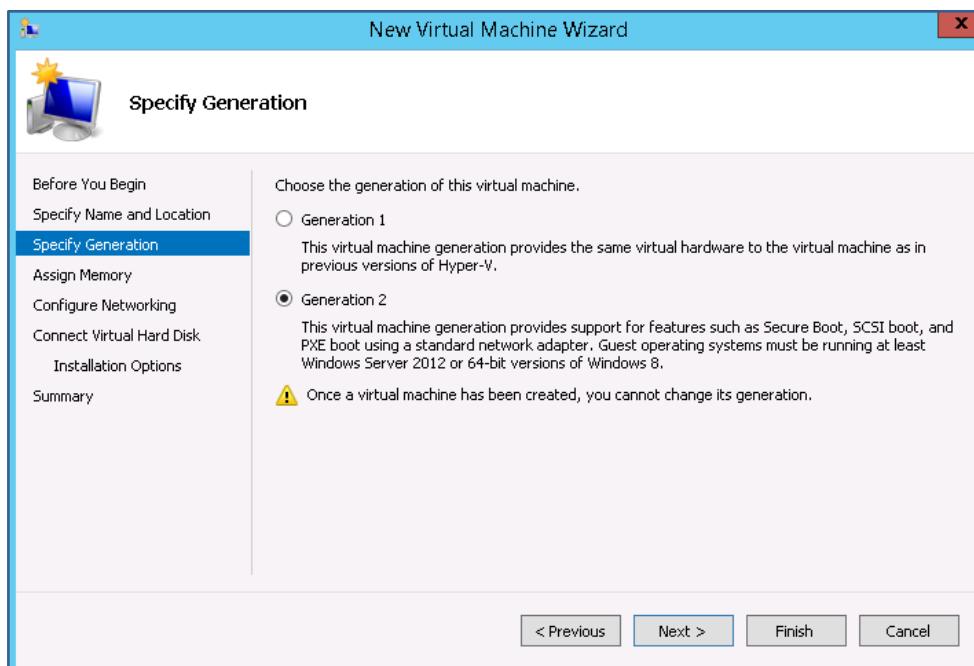
Enter a Name for the VM into the field provided.

Check the **Location** where the VM will be created. To use a different location, tick **Store the virtual machine in a different location**, and **Browse** to and select the new location.



12. Specify Generation.

Select a **Generation 1 or 2** VM, and click **next**.



When selecting:

- Select a Generation 1 VM if the Backup was from a BIOS server.
- Select a Generation 2 VM if the Backup was from an EFI server.

13. Assign Memory.

Assign Memory to the VM, and click **next**.

The memory required will vary from system to system.

Ticking **Use Dynamic Memory for this virtual machine** means only the memory that is needed (from the assigned memory) is used. This can result in the VM using less memory, though it may be less responsive.

14. Configure Networking

Virtual network switches are set up in Hyper-V Manager and used to give VMs access to the network using the host's network adapter.

Select a Switch, and click **next**.



If there are multiple network cards on the physical host and not all of them are connected, make sure the **switch** you select for your VM is using a **network card** that **is connected**.

15. Connect Virtual Hard Disk.

To add the virtual hard disk, complete the following steps:

- a) Select **Use an existing virtual hard disk**.
- b) Use the **Location** field to **Browse** to and select the recovered VM's .vhdx file. This is an image of the backed up VM. It will be located in **the Virtual Hard Disks** folder, inside the folder you recovered the VM to.
- c) Click **Next**.

The screenshot shows the 'New Virtual Machine Wizard' dialog box, specifically the 'Connect Virtual Hard Disk' step. The window title is 'New Virtual Machine Wizard' and it has a close button (X) in the top right corner. On the left side, there is a navigation pane with the following steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk' (which is highlighted in blue), and 'Summary'. The main area of the dialog contains the following text and controls:

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

There are three radio button options:

- Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.
This section includes a 'Name' field with the value 'vm-recovered.vhdx', a 'Location' field with the value 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\', and a 'Browse...' button. The 'Size' field is set to '127 GB (Maximum: 64 TB)'.
- Use an existing virtual hard disk
Use this option to attach an existing VHDX virtual hard disk.
This section includes a 'Location' field with the value 'E:\vm-recovered\Test\Virtual Hard Disks\Test.vhdx' and a 'Browse...' button.
- Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

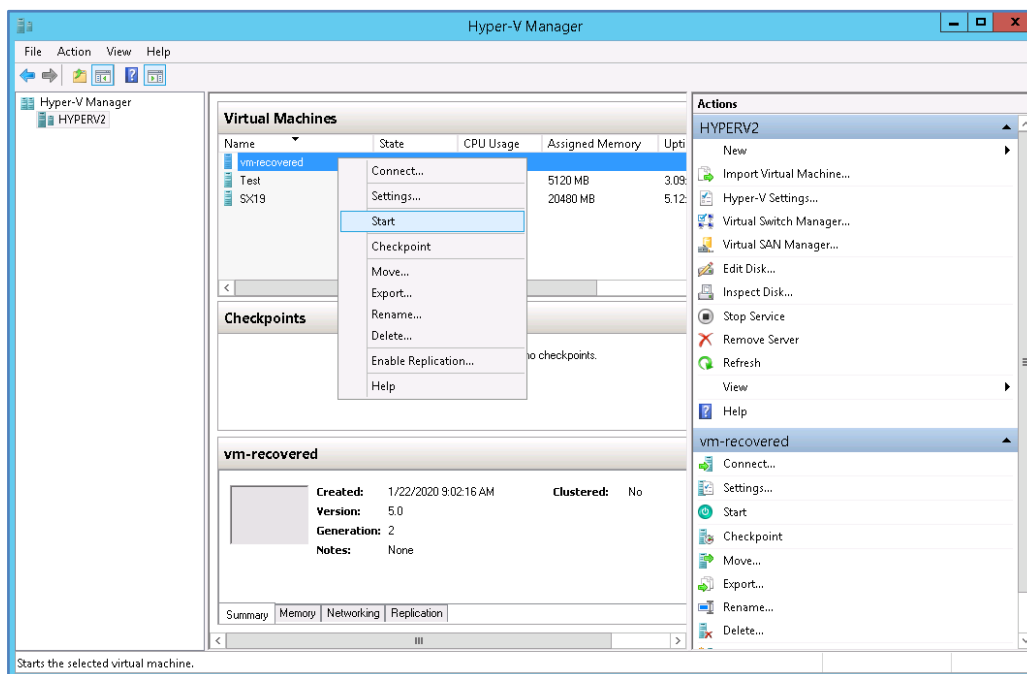
At the bottom of the dialog, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

16. Summary.

Review the VM selections in the **Summary** step and select **Finish**.

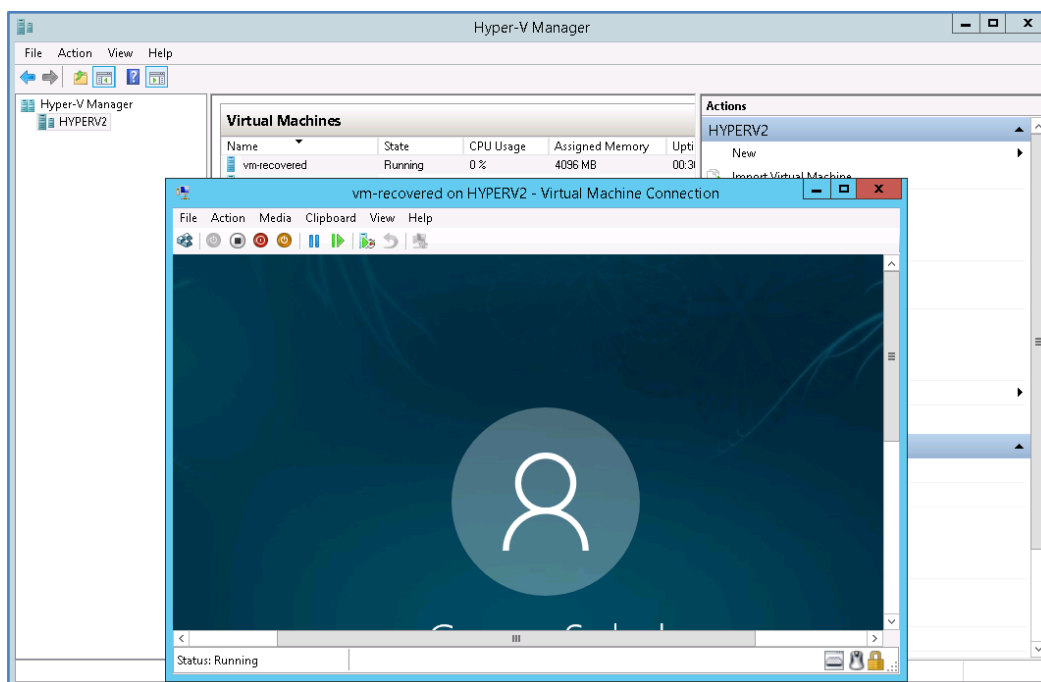
The VM will now be created and added to the list of VMs in Hyper-V Manager.

17. Right-click the new VM and select **Start**.



18. Right-click the VM and select **Connect**.

This will open a session so you can log into the VM.



Congratulations – your VM has been recovered.

5 Recover specific Hyper-V guest VM to different host

This scenario uses the **Recover tab's Full VM Recovery** option to recover a virtual machine (VM) to a Hyper-V Server that was not its original host. For example, if the VM's original host is not operational, it could be recovered to another Hyper-V Server.


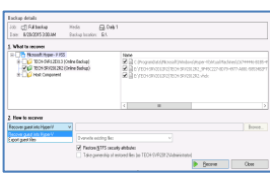
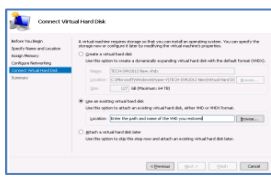


In a nutshell: In this scenario, you will use BackupAssist's Discover backup feature on a Hyper-V Server to locate another host's VM backup. You will then use that backup to recover the VM's files to a local drive and use those files to create a new VM.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform a Full VM Recovery, you will need BackupAssist and:

 <h4>A VM backup</h4>	 <h4>Integrated Restore Console</h4>	 <h4>Hyper-V Manager</h4>
<p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the Virtual Machine.</p>	<p>BackupAssist will use the Integrated Restore Console to recover the selected VM to a folder on the host.</p>	<p>Hyper-V Manager will be used to create a new VM using the recovered VM's image file, and then start that new VM.</p>

Recovery checklist

Use this checklist to make sure you have the required information:

<input type="checkbox"/>	An accessible backup of the VM. If the backup is in a network location, you will need the full path for the location.
<input type="checkbox"/>	The location on the Hyper-V Server that is large enough for the VM to be recovered to. For optimal performance, this folder should not be on the same drive as the operating system.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Recovery process

To recover a Hyper-V VM to a different host, follow these steps:

1. **Select BackupAssist's Recover tab.**
2. **Click Full VM Recovery.**

The **Full VM Recovery screen** will open and **display** all the **VMs** that have been backed up locally.

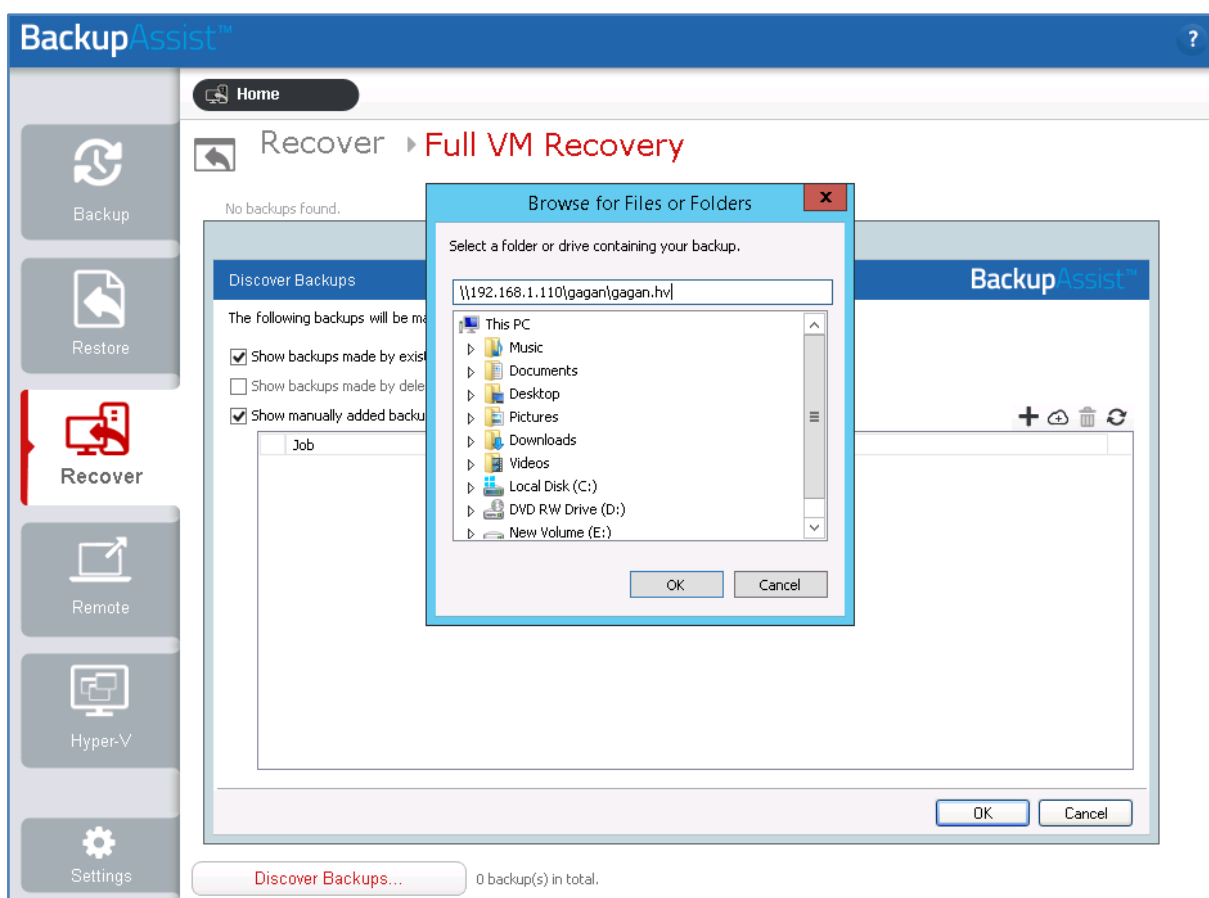
3. Locate the other hosts backup.

To locate the backup:

- a) Click **Discover Backups**.
- b) Click the **+** symbol.
- c) Enter or browse to the **location of the backup**.
- d) Select **OK**.

When you add the backup, it will appear in your **Discover Backups list**.

- e) Confirm that the backup is listed in the Discover Backups screen and Select **OK**.

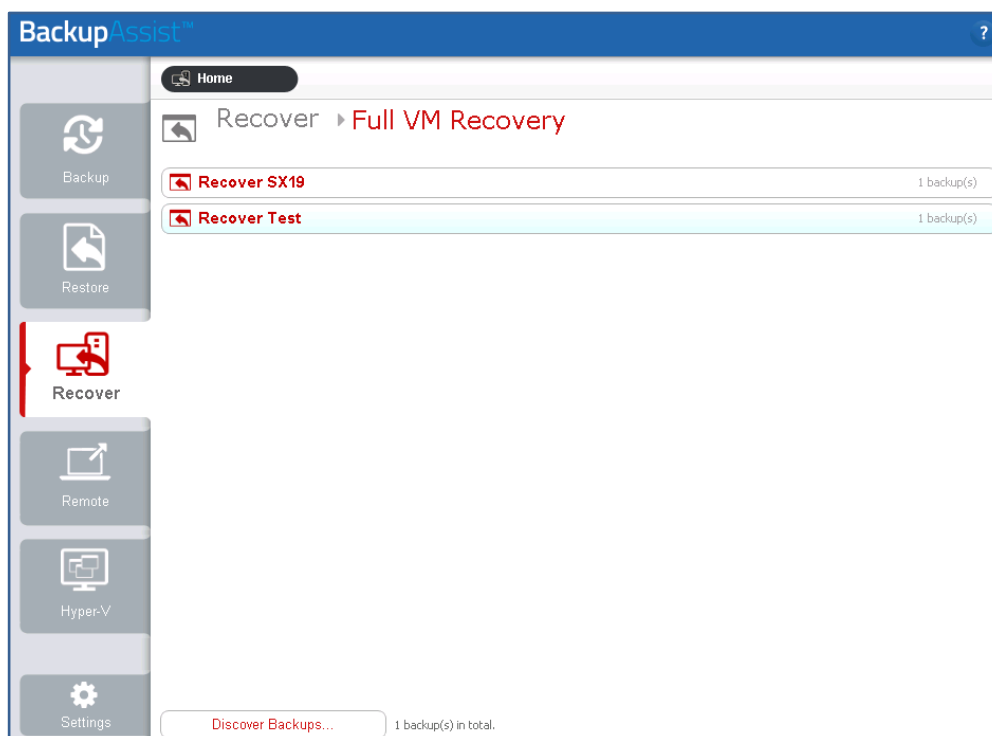


When the backup of the other Hyper-V host has been added to this host, each VM in the other host's backup will appear in the **Full VM Recovery** screen.

4. Select the VM.

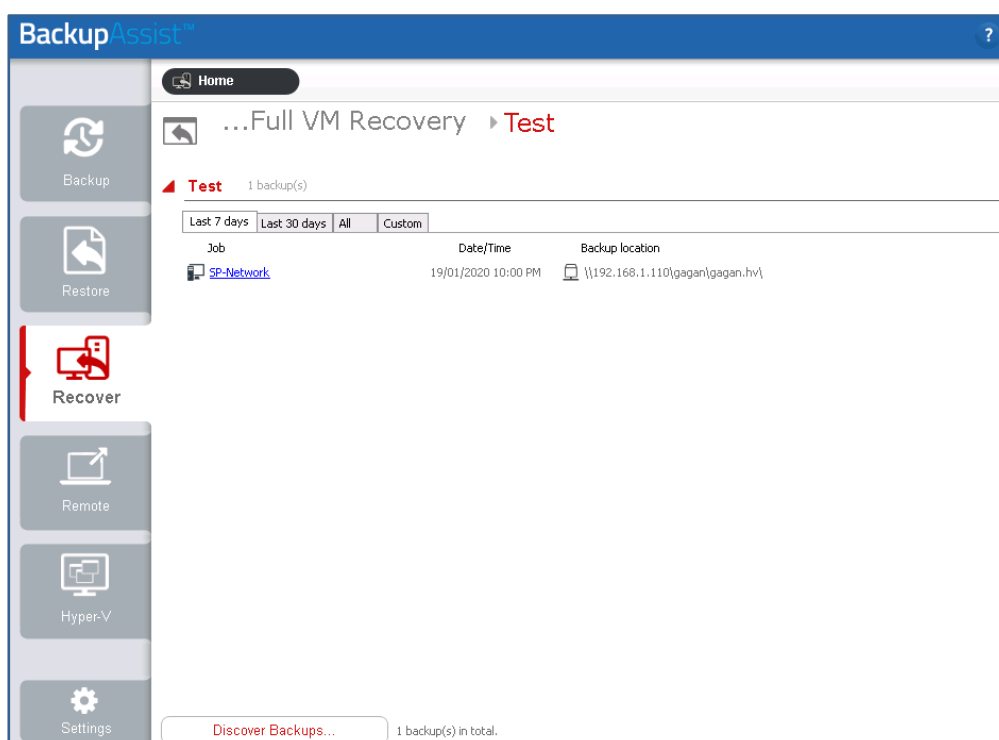
From the **Full VM Recovery screen**, select the **VM** that you want to recover.

When you click on the VM, the screen will display all available backups of that VM.



5. Select a backup.

Select the backup that you want to recover the VM from. The **tabs above a VM's backup** list can be used to **filter the backups** shown.

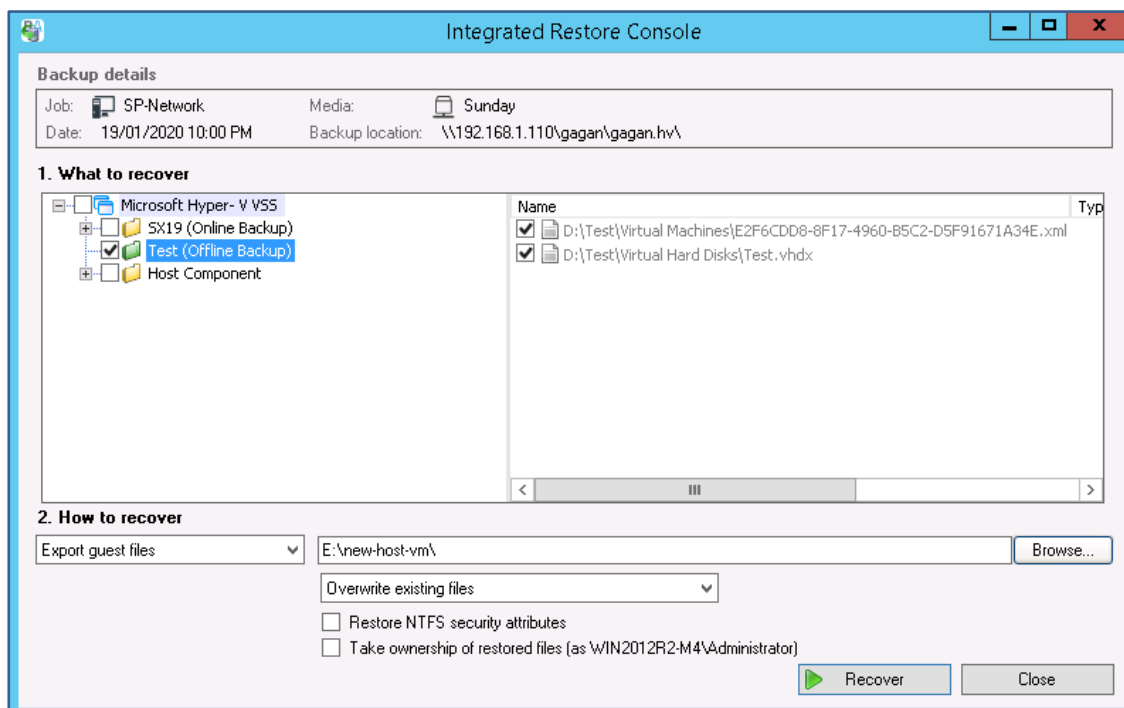


The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a date range and display backups for that period.

6. Select the VM in the backup.

The **Integrated Restore Console** will open the backup and **display the VMs** that were backed up.



Use the **What to recover** pane to **tick the box** next to the **VM that you want** to recover. You can select more than one VM but they will share the restore settings used.

7. Select how you want to recover the VM (guest).

The **How to recover** drop-down box is used to select the recovery method.

The recovery methods are:

- **Recover guest into Hyper-V** – recovers the guest to its original path on the new host.
- **Export guest files** – copies the guest files to a selected location.

In this scenario, we will use the **Export guest files** option. This allows you to get a recovered copy of the VM running, while still having the original VM available for ongoing investigation if required.

8. Select the recovery destination.

Use the **Browse** button to **select a folder to restore the VM to**. This location must be large enough for the VM. For optimal performance, the operating system's drive should not be used.

9. Click the Recover button.

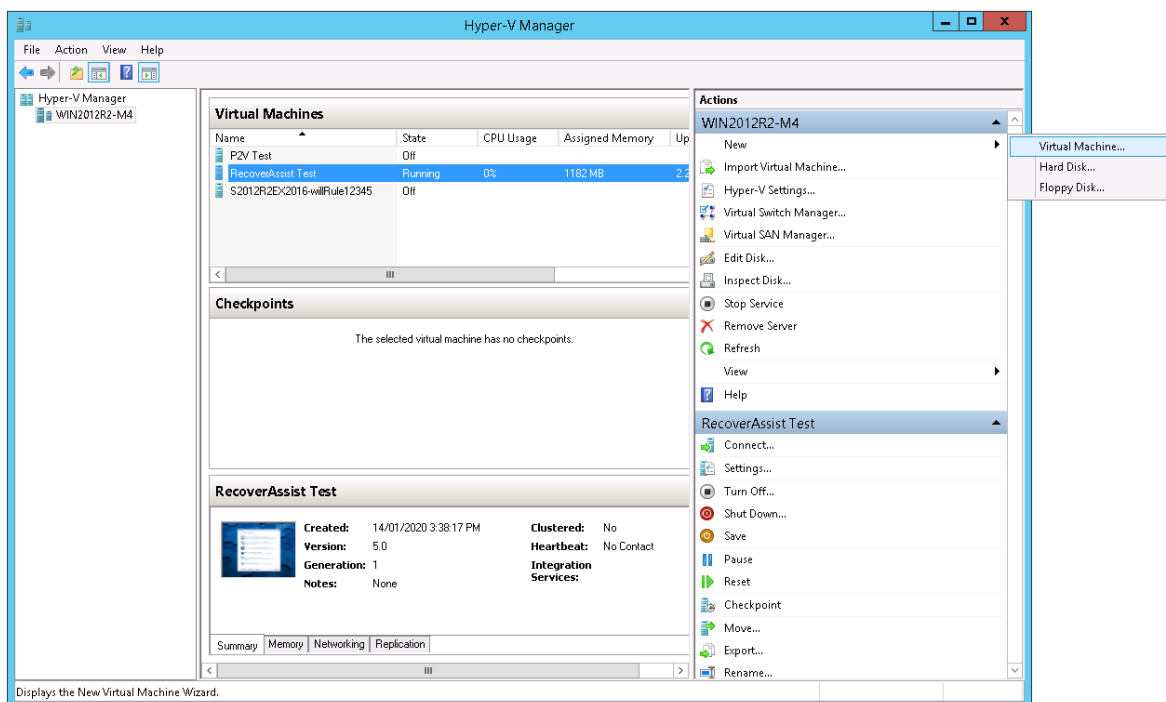
The recovery process will begin and the **Integrated Restore Console** will display its **progress**.

Select **Done** and **Close** when the recovery has finished.

We will now use the recovered VM's .vhdx file to create a new VM.

10. Open the Hyper-V Manager console.

11. Select **New** then **Virtual Machine...** from the **Actions** menu.

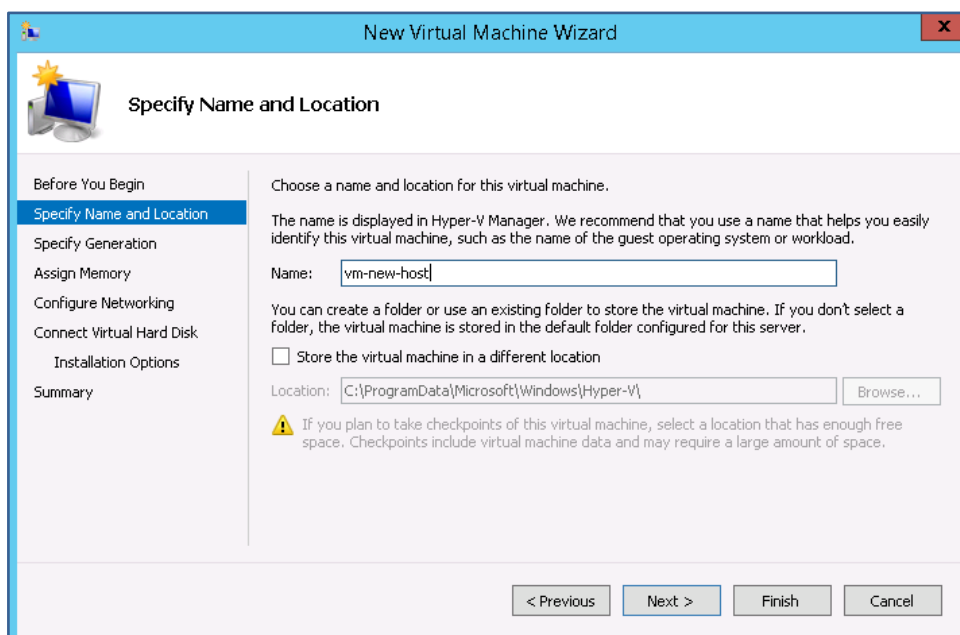


The **New Virtual Machine Wizard** will open and step you through the VM set up process.

12. **Specify Name and Location.**

Enter a Name for the VM into the field provided.

Check the **Location** where the VM will be created. To use a different location, tick **Store the virtual machine in a different location**, and **Browse** to and select the new location.



13. **Specify Generation.**

Select a **Generation 1 or 2** VM, and click **next**.

When selecting:

- Select a Generation 1 VM if the Backup was from a BIOS server.
- Select a Generation 2 VM if the Backup was from an EFI server.

14. Assign Memory.

Assign Memory to the VM, and click **next**.

The memory required will vary from system to system.

Ticking **Use Dynamic Memory for this virtual machine** means only the memory that is needed (from the assigned memory) is used. This can result in the VM using less memory, though it may be less responsive.

15. Configure Networking.

Virtual network switches are set up in Hyper-V Manager and used to give VMs access to the network using the host's network adapter.

Select a Switch, and click **next**.



If there are multiple network cards on the physical host and not all of them are connected, make sure the **switch** you select for your VM is using a **network card** that **is connected**.

16. Connect Virtual Hard Disk.

To add the virtual hard disk, complete the following steps:

- Select **Use an existing virtual hard disk**.
- Use the **Location** field to **Browse** to and select the recovered VM's .vhdx file. This is an image of the backed up VM. It will be located in **the Virtual Hard Disks** folder, inside the folder you recovered the VM to.

New Virtual Machine Wizard

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:
Location:
Size: GB (Maximum: 64 TB)

Use an existing virtual hard disk
Use this option to attach an existing VHDX virtual hard disk.

Location:

Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

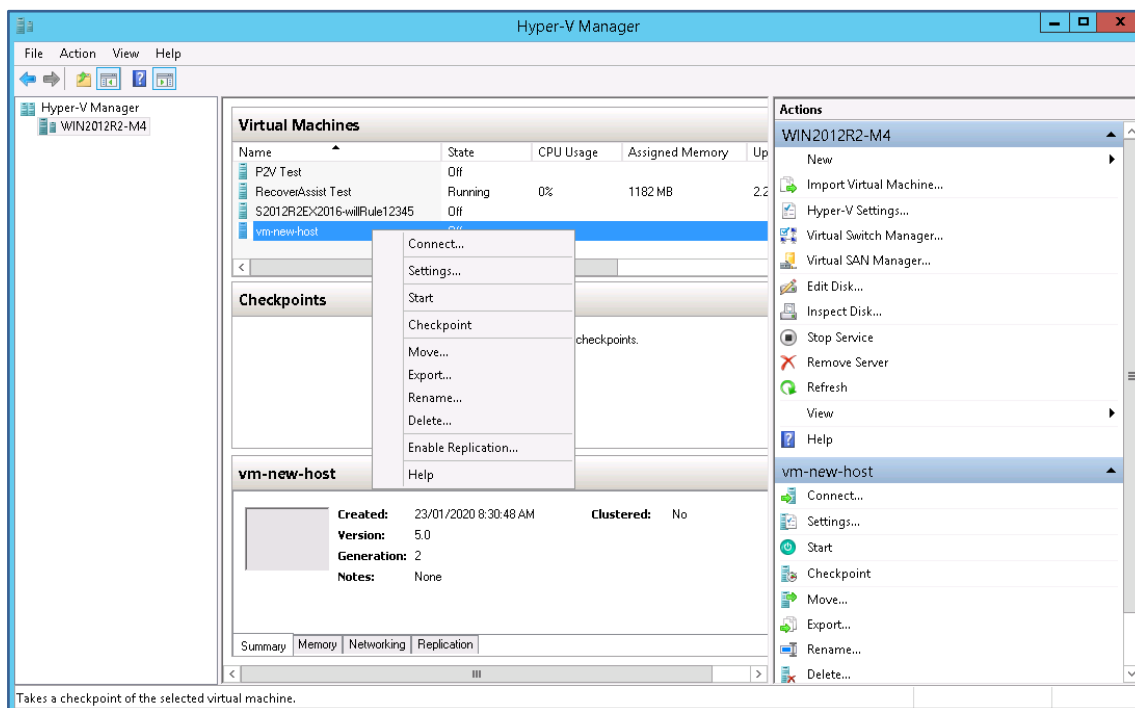
< Previous Next > Finish Cancel

c) Click **Next**.

17. Review the VM selections in the **Summary** step and select **Finish**.

The VM will be created and added to the list of VMs in Hyper-V Manager.

18. Right-click the new VM and select **Start**.



19. Right-click the VM and select **Connect**.

This will open a session so you can log into the VM.

Congratulations – your VM has been recovered on a new host.

6 Rapid recovery of a VM from backup within minutes

A Rapid VM Recovery gets a **guest up and running from its backup destination** in just a few minutes so the VM's functions can resume with minimal interruption. This **temporary solution** provides business continuity until a suitable time can be found to perform a Full VM Recovery.



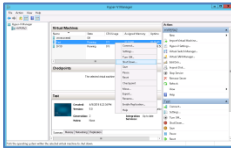


In a nutshell: In this scenario, you'll select a VM and its backup then, with a click of a button, BackupAssist will run that VM from the backup destination. The scenario will then explain how to fully recover that VM.

To make sure there are no surprises along the way, we will begin with a look at **what you will use** and **what information you will need**.

Recovery requirements

To perform a Full VM Recovery, you will use:

 <p>BackupAssist</p>	 <p>A Backup</p>	 <p>Windows Hyper-V Manager</p>
<p>BackupAssist will be used to select the VM and backup and start the rapid recovery.</p>	<p>You will need a System Protection, File Protection or File Archiving backup <u>on a local drive</u>.</p>	<p>Hyper-V Manager will be used to review and then start the VM that is being rapidly recovered.</p>

Recovery checklist

Use this checklist to make sure you have the required information:

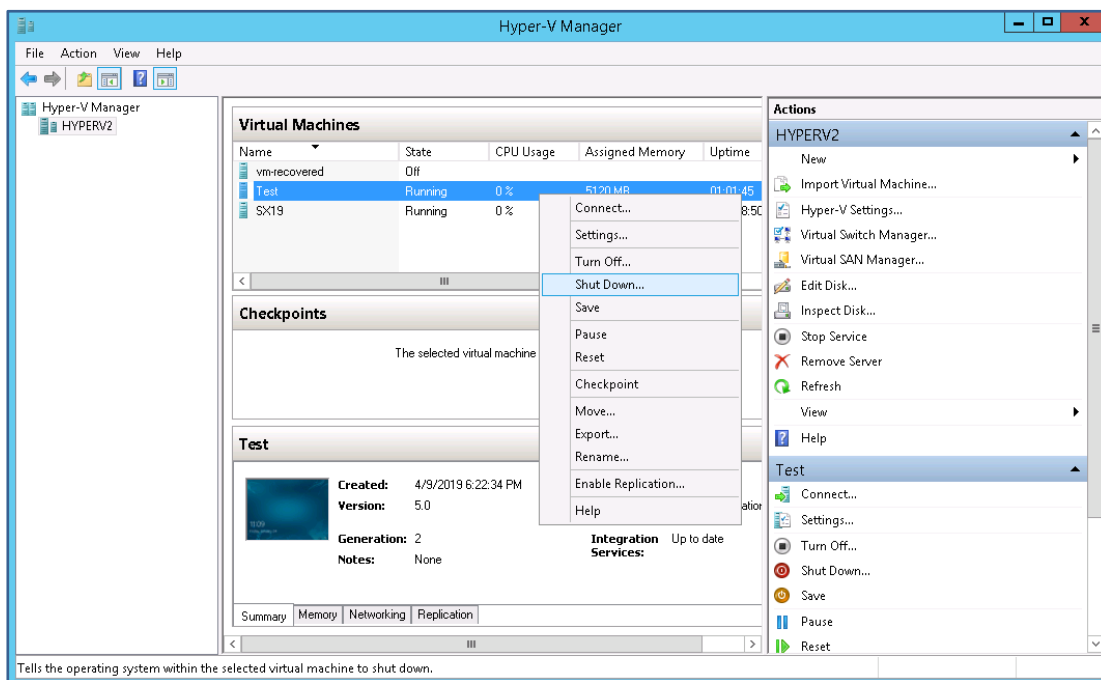
<input type="checkbox"/>	<p>The location on the Hyper-V Server that is large enough for the VM to be recovered to. For optimal performance, this folder should not be on the same drive as the operating system.</p>
<input type="checkbox"/>	<p>Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.</p>

Recovery process

To rapidly recover a Hyper-V VM, follow these steps:

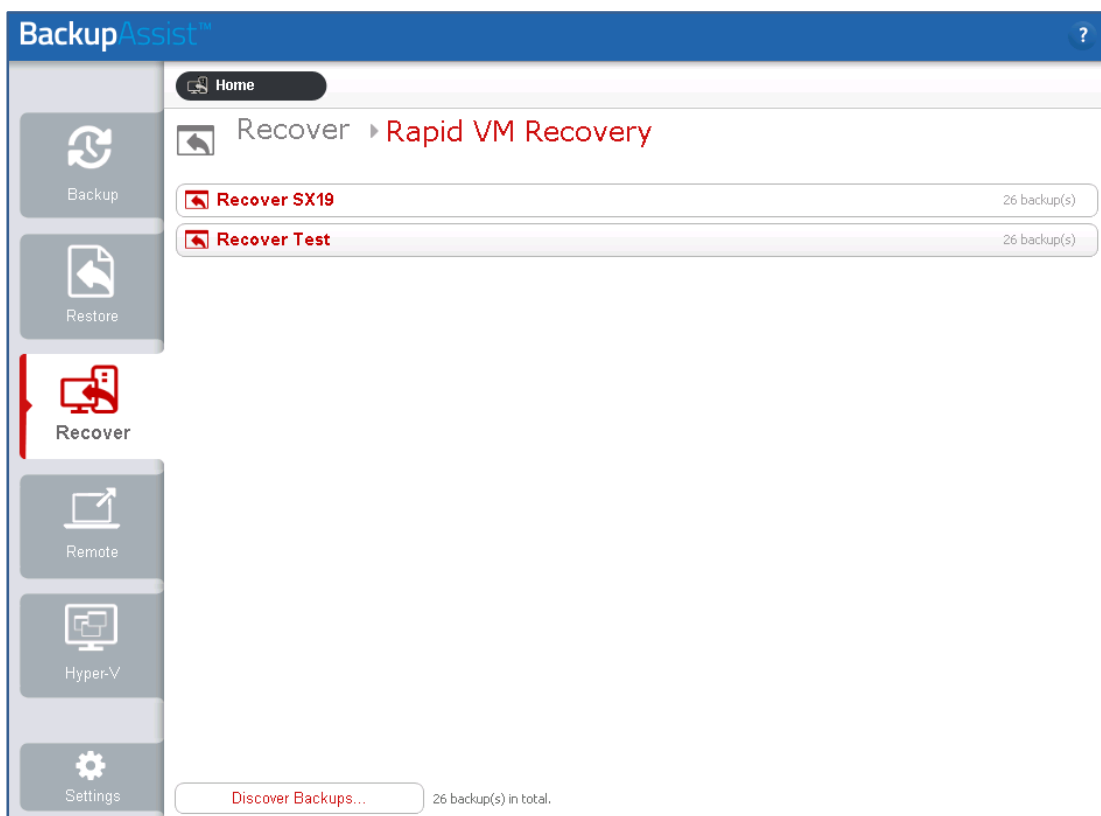
1. **Open Windows Hyper-V Manager.**
2. **Check that the VM you are rapidly recovering is not running.**

If the VM is running, right-click the VM and select **Turn Off**.



3. **Select BackupAssist's Recover tab.**
4. **Click Rapid VM Recovery.**

The **Rapid VM Recovery screen** will open and **display** all the **VMs** that have been backed up.

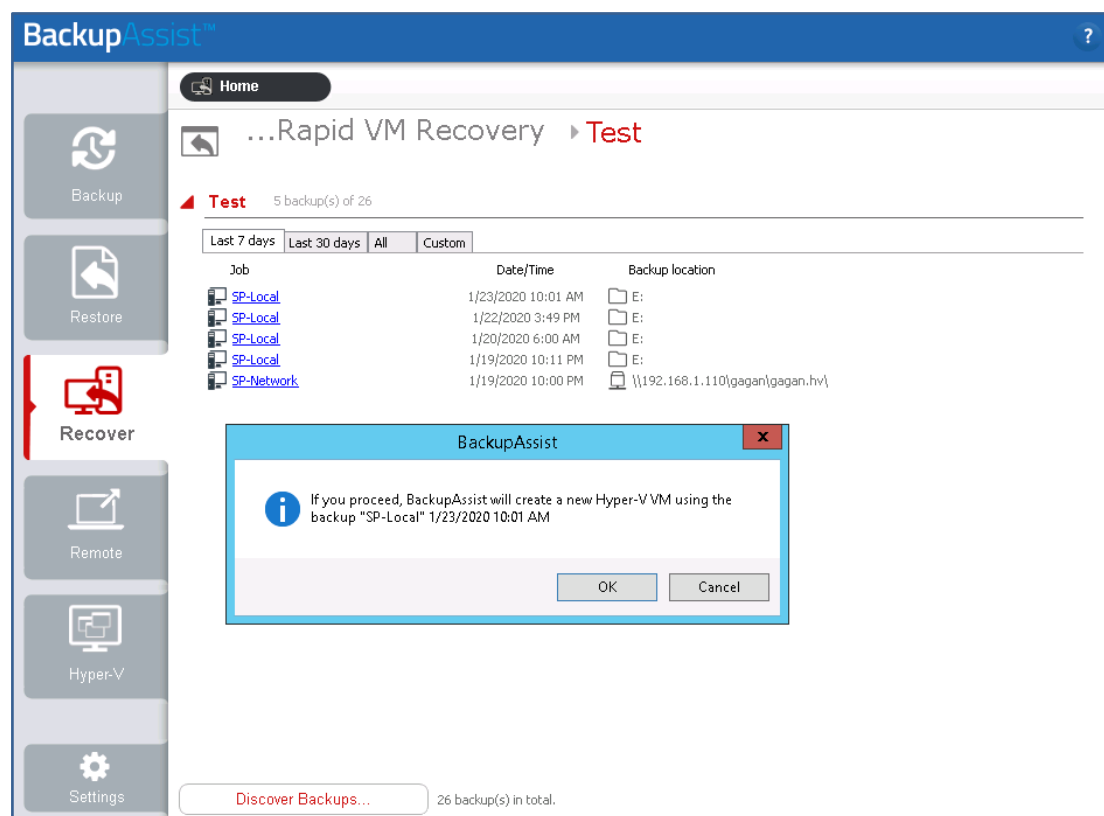


5. Select the guest.

Select the guest that you want to rapidly recover. When you make the selection, the screen will display all available backups of that guest.

6. Select the backup.

Select the backup you want to use. When you make the selection, a dialog will prompt you to confirm this backup.



The tabs above each volume's backup list can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

7. Select a location to store data changes.

While the Rapidly Recovered VM is running, the Hyper-V host will store and manage changes to the VM's data. **Select a folder on a local host drive** that can be used to store this data.

After you confirm the location, a message will advise you that the rapidly recovered VM has been created, and **show the name used** by the rapidly recovered VM in the Hyper-V Manager.

8. Review the guest configurations.

The VM's configurations will be the same as the VM had when it was backed up. These configurations should be reviewed, especially if the host has changed since the backup was created.

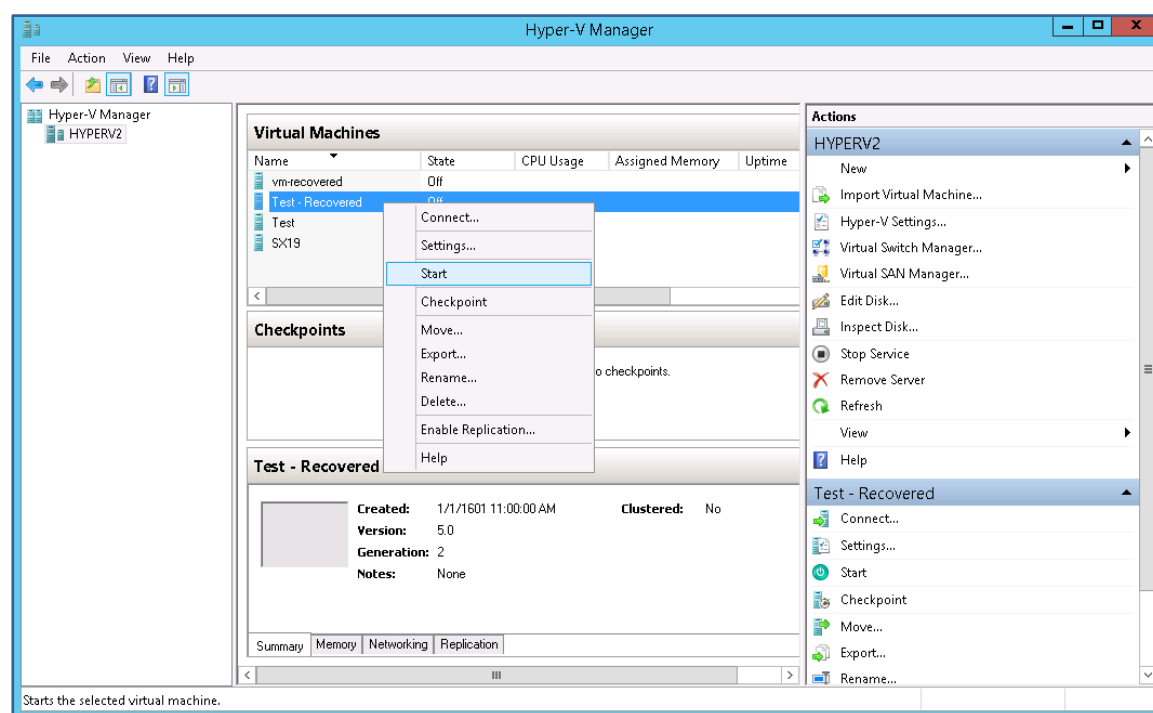
To review the VM's configurations:

- Open **Windows Hyper-V Manager**.
- Select the **VM**.
- Select **Settings** from the **Actions** menu.
- Review the settings, especially the **Memory**, **Hard Drive** and **Network Adapter** settings.

Check the guest has the appropriate configurations for the host and the required resources to run.

9. Start the rapidly recovered guest.

Use the Windows Hyper-V Manager **Actions** menu to **start the Hyper-V guest**.



To start the VM:

- Open **Windows Hyper-V Manager**.
- Right-click the VM** and select **Start**.

Congratulations – your VM has been rapidly recovered.

How to perform a Full VM recovery of the rapidly recovered VM.

Rapid VM Recovery is a **temporary solution** that provides **business continuity** until a suitable time can be found to perform a Full VM Recovery, which could take many hours.

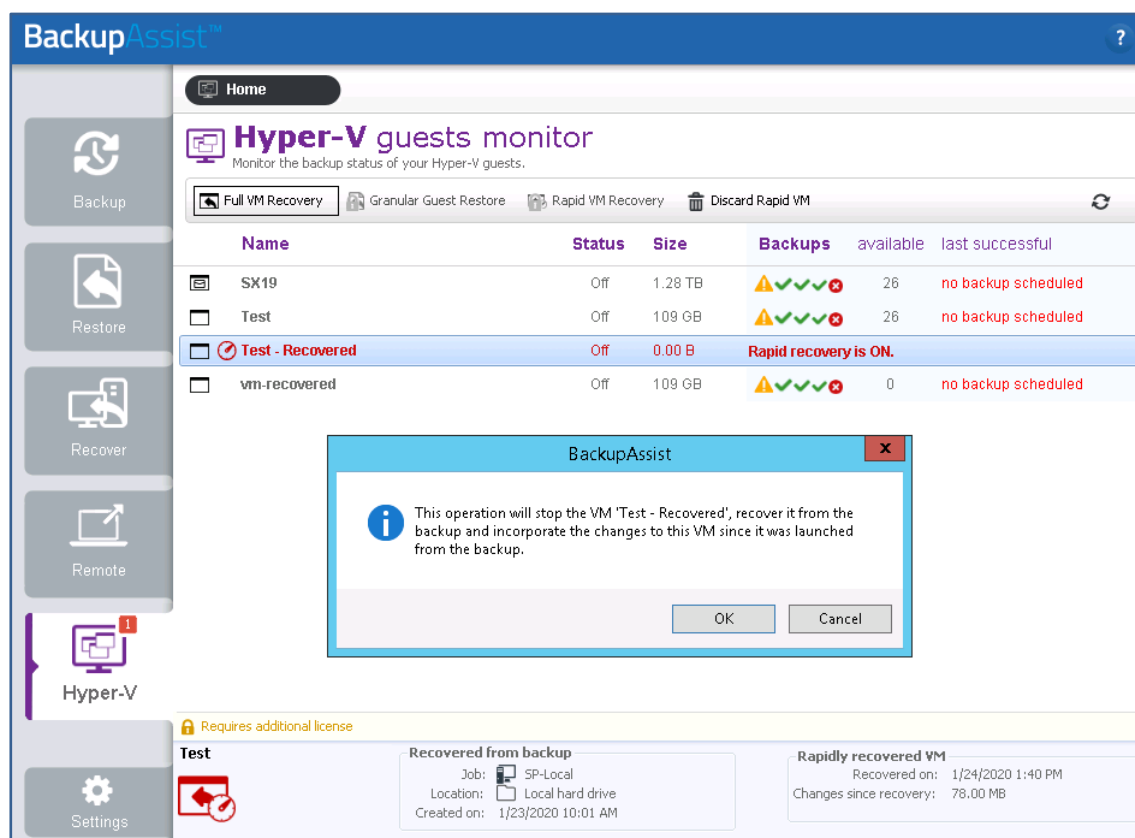
The full recovery results in a clean copy of the guest's data and includes all changes accumulated while the rapidly recovered guest was running.

Considerations:

- **Any data that changed** while the VM was rapidly recovered **will be included** in the full recovery.
- Before starting, ensure there is **enough space on the host** to recover the guest to.
- This process is a full recovery to the rapidly recovered guest, not to the original guest.

To fully recover a rapidly recovered VM:

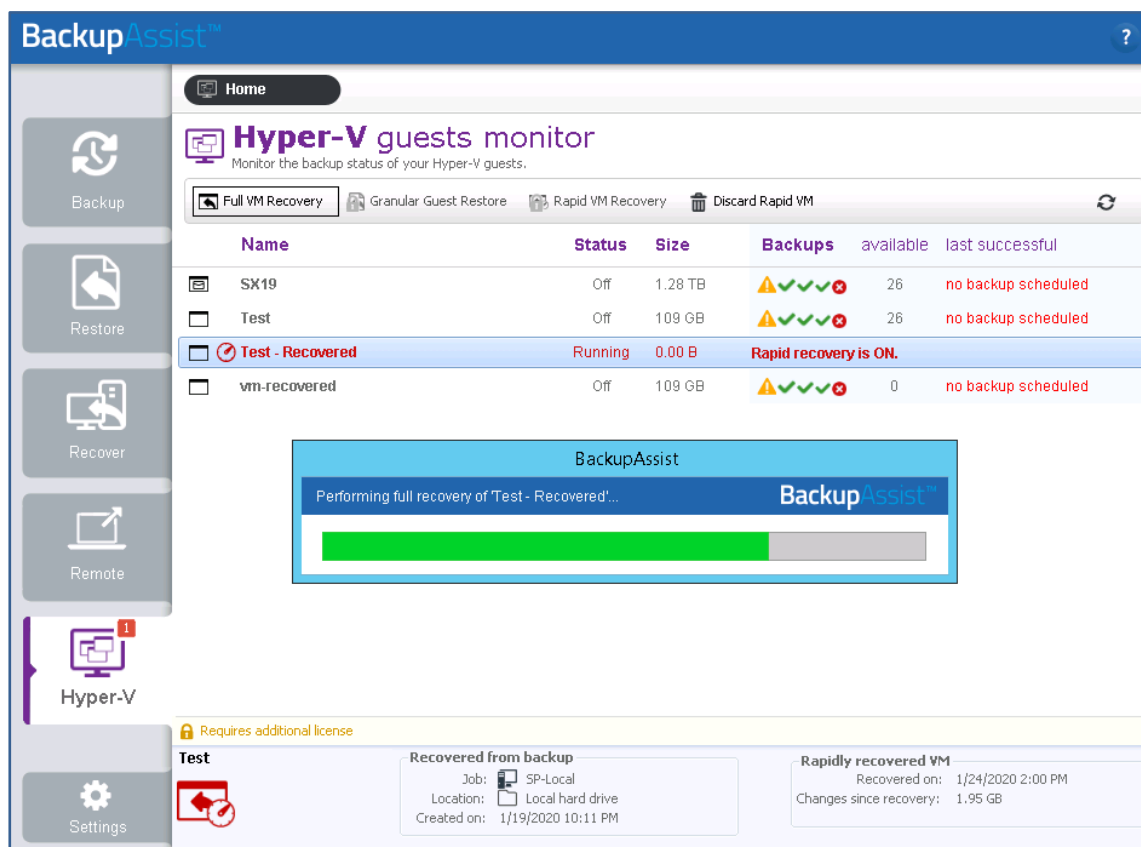
- Select the **Hyper-V tab**.
- Select the **rapidly recovered VM**.



- Select **Full VM Recovery** from the main menu.
- Select **OK** on the confirmation dialog to start the full recovery.
- Select a permanent location for the recovered VM.

The VM's virtual disks and configuration files will be recovered to this location.

f) Select **OK** and the **Full VM Recovery** process will **begin**.



A progress bar will appear while the recovery is in progress, and a confirmation message will appear once the recovery has been completed.

Congratulations – your rapidly recovered VM has been fully recovered.

Discarding a Rapidly Recovered VM

If you do not want to continue using the rapidly recovered VM or fully recover the rapid VM, you can discard it. This will discard any changes made to the VM's data since it was rapidly recovered, and remove the VM instance from the Hyper-V Manager.

To discard a rapid VM:

- Select the **Hyper-V tab**.
- Select the **Rapidly Recovered VM**.
- Select the **Discard Rapid VM button**.

When you select **Discard the Rapid VM**, you will be prompted to confirm that you want to **delete the VM data**.

File restore for physical machines

This section explains how to perform file and folder restores using BackupAssist's powerful backup filter and search features. The first scenario explains how to locate and restore a specific file to a point in time. The second scenario explains how to locate and restore different versions of the same file.

7 Point-in-time search, browse and restore of files and directories

This scenario uses the Restore tab's **Local and Network Files** option to restore files and folders to a point in time. The instructions for this scenario use a Cloud Backup to restore an old version of a word document from an Azure cloud container.

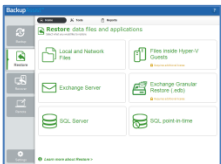

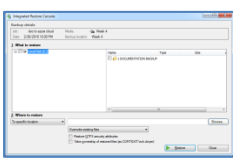


In a nutshell: In this scenario, you will choose a backup then locate the files you want and restore them to a selected location. The key is finding the backup with the files, so we'll use BackupAssist's **Filter** and **Search** functions for a fast, efficient outcome.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform a file and folder restore, you will need:

BackupAssist	Backups	Integrated Restore Console
 <p>BackupAssist will be used to select the type of restore required, and locate the backup and the files you want to restore.</p>	 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the data to be restored.</p>	 <p>BackupAssist will use the Integrated Restore Console to select the files and restore them to your chosen location.</p>

Restore checklist

Use this checklist to make sure you have the required information:

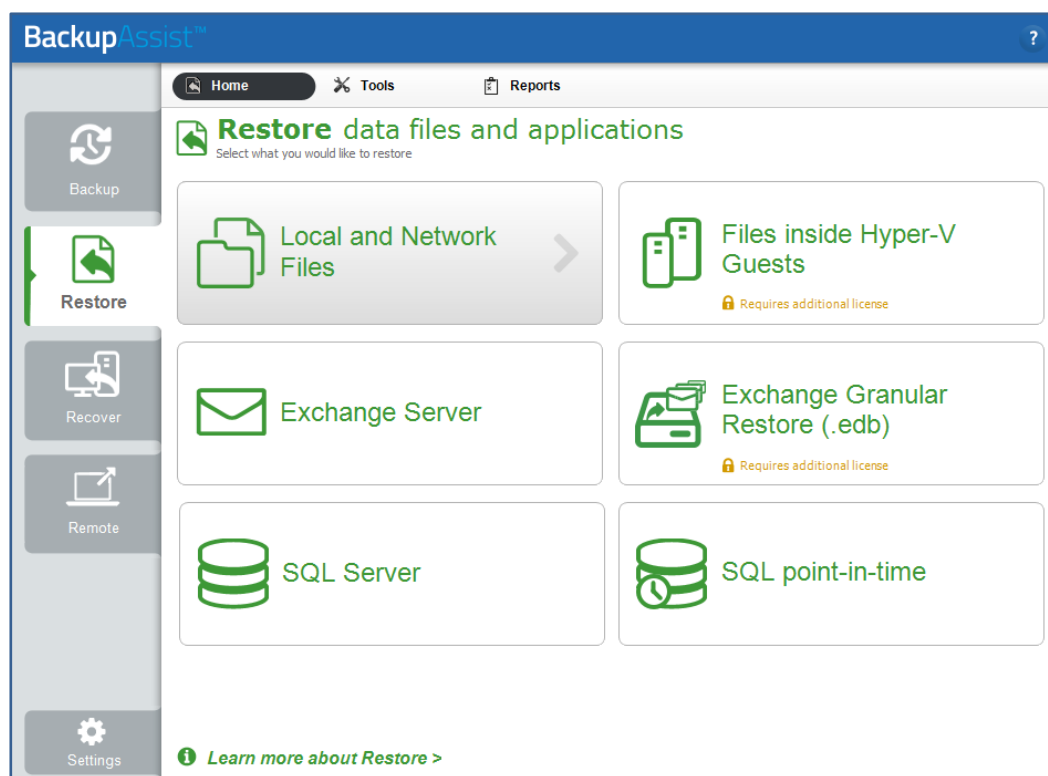
<input type="checkbox"/>	Details about the files you want to restore. For example, the file names and the dates that the files should be restored from.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore files and directories, follow these steps:

1. **Select BackupAssist's Restore tab.**

2. Select Local and Network Files.



This step starts the guided restore process and opens the **Local and Network Files** screen.

3. Locate the files that you want to restore.

The **Local and Network Files** screen shows the volumes backed up by this installation of BackupAssist. Click the arrow beside a volume to view backups of that volume.

- ❖ **If you know the backup** you want but there are dozens of backups listed, the **Filter** option can help you locate the right backup.

For example, if you want a backup of C: drive made in the previous week, you can select the **Last 7 days** tab to reduce the backups shown, making it easier to spot the one you want.

- ❖ **If you know the files** you want to restore, but don't know what backup they are in, you can use the **Search** options to find those files, and the backups they are in.

For example, if you want to restore the first version of a file, you can search all of the backups containing that file, then select the first backup that file appears in.

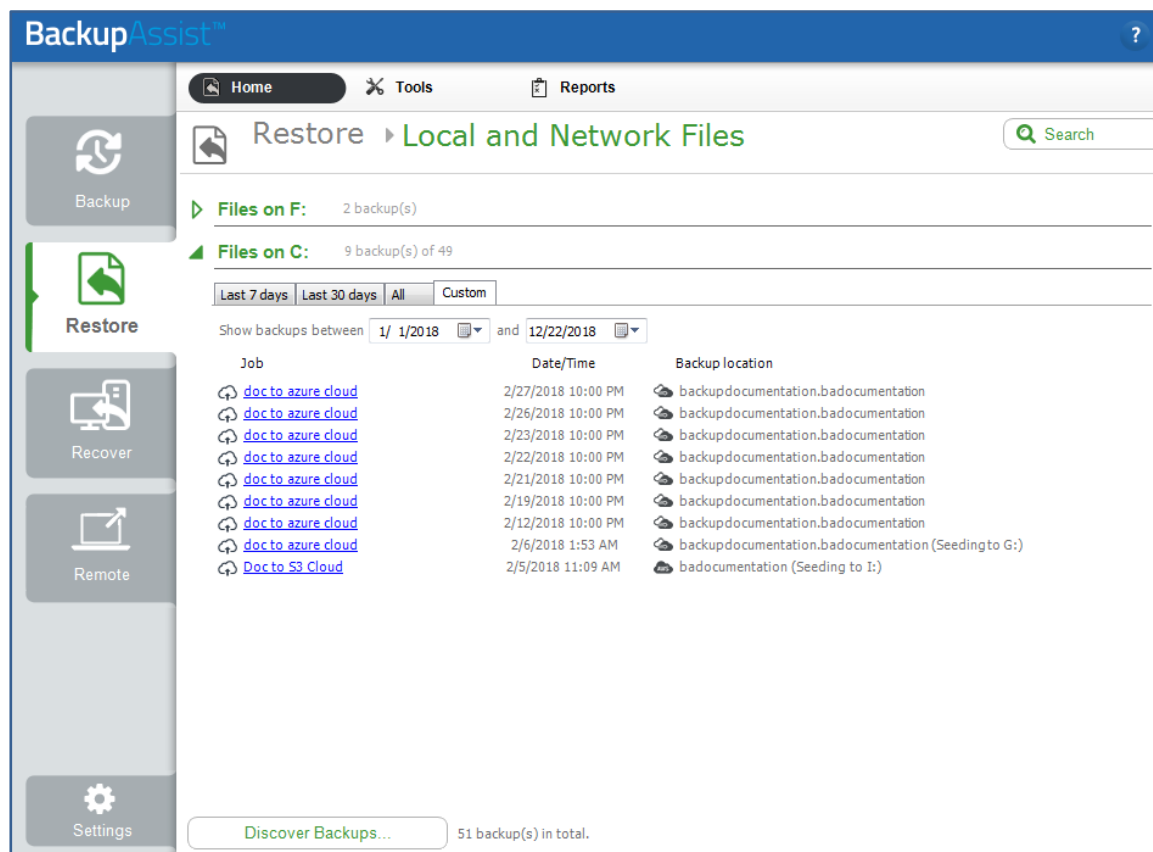
To Filter the backups.

The tabs above each volume are used to filter the list of backups shown.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.

In this screenshot, I want to restore an old version of a document from an Azure Cloud Backup, so I used the **Custom** tab to show the backups created in 2018.



To Search the backups

The **Search** button opens the **Search screen**, which allows you to locate files across all backups. The **Search** screen uses two sections to set the search criteria: **Backups** and **Search**.

Backups section

The **Backups** section is used to limit the set of backups that will be searched.

To limit the backups that will be searched:

- Use the **Blue link** next to **Jobs** to view all jobs that have run on this installation of BackupAssist. Deselecting a backup job will exclude any backups made by that job from a search.
- Use the **Backup date** and choose a date range. Only backups created between those dates will be included in the search.

Search section

The **Search** section is used to enter the criteria that will help you find a file or files.

The following search criteria are available:

- The **Search for** field will search the **text entered** for occurrences of that text within a file name. If you don't know the exact file name, put * before and after the part of the name you know.
- The **Created** and **Modified** options are used to search for files based on the date they were created or modified. This is different from the **Backups** section's date range, which only applies to the date a backup was created.

When you tick Created or Modified, the **blue link** can be used to set a time frame or context for the selected dates in the date field. For example **Before 4/8/2016**.

- The **Size** option allows you to include a file's size in the search criteria.
- **Limit results per backup** is an important setting, as it **limits** how many **items found** by the search will be shown. If the search results equal the limit, you should increase the limit and/or refine the search criteria so that all of the results are within the limit.

This screenshot shows the results of a search for a file with **data container** in its name, that was created before April 7, 2016. Each backup with files matching the criteria is listed.

The screenshot displays the BackupAssist interface. The main window is titled "...Local and Network Files > Search". The search criteria are as follows:

- Filter by:**
 - Jobs: 2 of 10 doc to azure cloud, seed-test-data-to-local
 - Backup date: between 1/ 2/2018 and 12/21/2018
- Search:** Completed in 00:00, Backups with results: 8
 - Search for: *data container* (e.g. report*.docx)
 - Created: Before 4/ 7/2016
 - Modified: Between 1/16/2020 and 1/16/2020
 - Size: Equal 10,000 bytes
 - Limit results per backup: 50

The search results list shows three backups:

1. doc to azure cloud @ 2/27/2018 10:00 PM Found files: 5, directories: 0
2. doc to azure cloud @ 2/26/2018 10:00 PM Found files: 5, directories: 0
3. doc to azure cloud @ 2/23/2018 10:00 PM Found files: 5, directories: 0

Below the list is a table of found files:

Name	Size	Created	Modified	Location
RESOURCE -Data containers.docx	420 B	3/18/2016 1:42 PM	1/13/2016 2:08 PM	C:\1 DOCUMENTATION BACKUP\Resources\
Data Containers.htm689160805v.20...	25.93 kB	3/18/2016 1:48 PM	3/4/2016 2:34 PM	C:\1 DOCUMENTATION BACKUP\Flare stuff\0 F
Data Containers.htm	25.93 kB	3/18/2016 1:46 PM	2/23/2016 2:33 PM	C:\1 DOCUMENTATION BACKUP\Flare stuff\0 F
Data Containers.htm	934 B	3/18/2016 1:48 PM	3/4/2016 2:35 PM	C:\1 DOCUMENTATION BACKUP\Flare stuff\0 F
Data Containers.htm	1.16 MB	3/18/2016 1:49 PM	3/4/2016 2:35 PM	C:\1 DOCUMENTATION BACKUP\Flare stuff\0 F

4. Select the backup.

From the **Local and Network Files** screen, click on the backup.

From the **Search results** list, select the **Restore button** next to the backup.

This will open the backup using the **Integrated Restore Console (IRC)**.



For encrypted backups

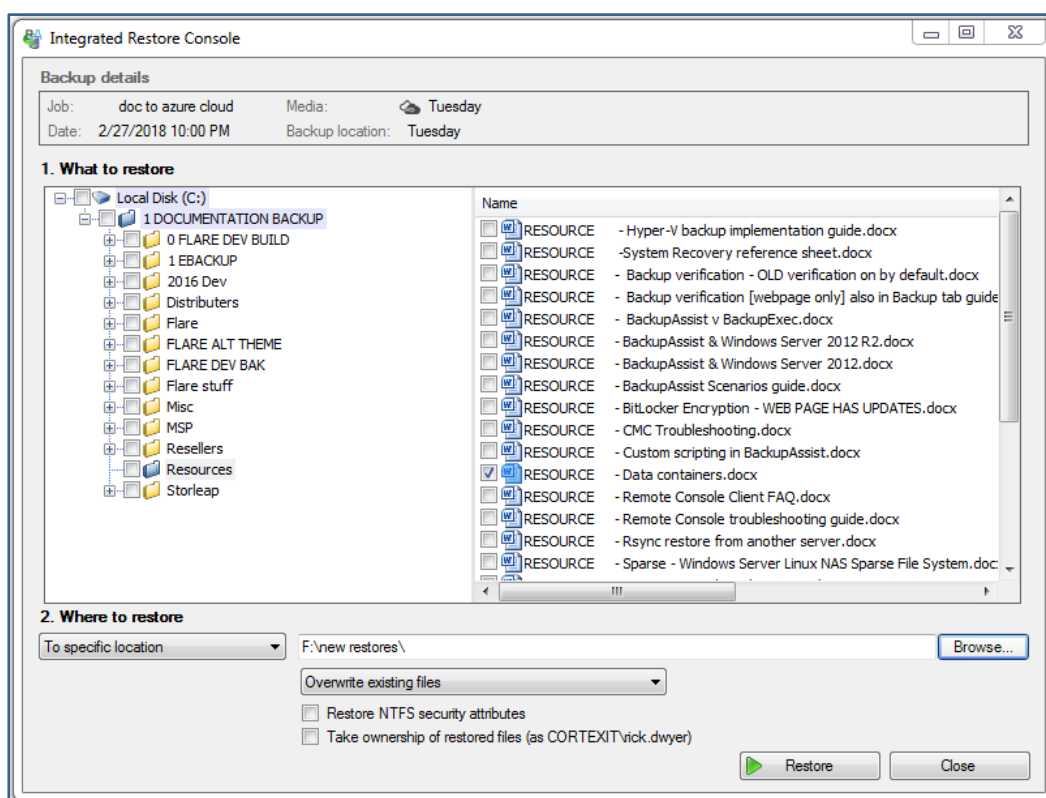
If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

5. Select the data.

Use the Integrated Restore Console to **select the files** and **folders** that you want to restore.



To locate and select the data:

- Use the **left pane** to browse through the folders.
- The **right pane** will display the contents of the folder selected in the left pane.
- **Tick the box** next to each file or folder you want to restore. If you tick a folder, all files and folders within it are selected.

6. Configure the restore settings.

Follow these steps to configure the restore options:

- Under **Where to restore** select **To original location** or **To Specific location**.

If you select **To original location** and there are files or folders present with the same names, the **Overwrite** rules will determine what files or folders are retained.

Selecting **To specific Location** can be an easier solution for file and folder restores, as you can further review what data you have and then copy it to a suitable location.

- b) Use the **Browse** button to locate and select the restore destination.
- c) The **Overwrite existing files** drop-down box is used to select the rule that will apply if a destination contains a file or folder with the same name as the file or folder being restored.
- **Overwrite existing files:** the restored files will overwrite files in the restore destination.
 - **Do not overwrite existing files:** the restored files will not overwrite files in the restore destination. This means the files will not be restored.
 - **Only overwrite older files:** if a file in the restore destination has changed since the backup was made it will not be overwritten.
- d) The **Restore NTFS security attributes** option.

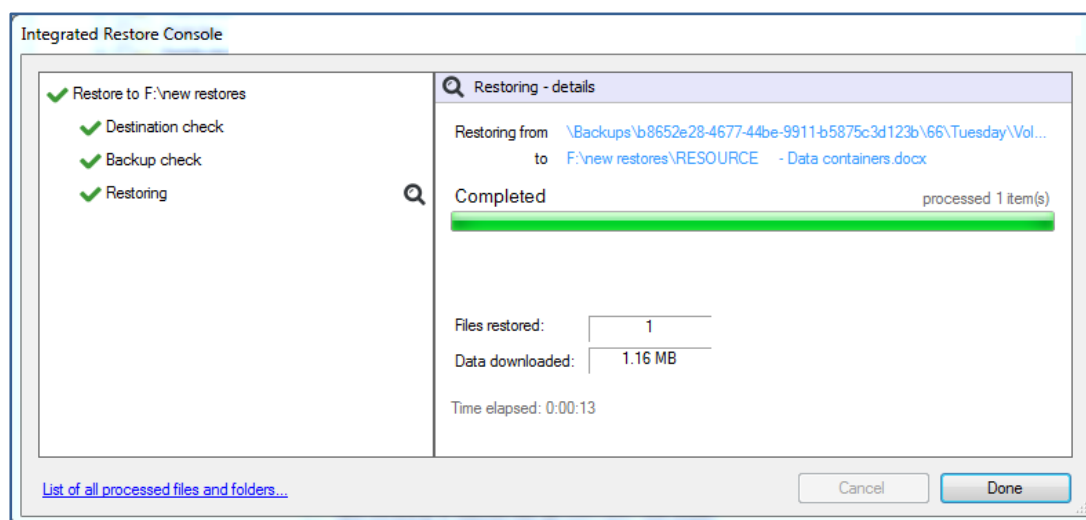
If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.

- e) The **Take ownership of restored files** option.

The **user** performing the restore needs **Write access** to the selected files or the restore will fail. This option gives the user Write access to the selected files. The user this applies to is shown to the right of the text box description.

7. Start the restore.

When you select the **Restore** button, the restore **process will begin**. The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.



List all processed files and folders.

Selecting this link will open notepad and display a list of the files restored, including their full path.

8. Select Done then Close.

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your files have been restored.

8 Search, browse and restore past versions of a file across all backups

This scenario uses the **Restore tab's Local and Network Files** option to restore different versions of a file. The instructions use a File Archiving backup to restore two versions of a file.

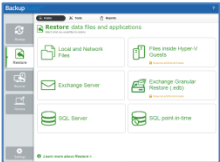

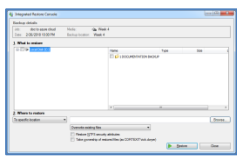


In a nutshell: In this scenario, you will search your backups to find specific versions of a file, and then restore those versions of the file to a selected location. The search process will use BackupAssist's powerful **Search** functions for a fast, efficient outcome.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform a file and folder restore, you will need:

BackupAssist	Backups	Integrated Restore Console
 <p>BackupAssist will be used to select the restore type, and search the backups for the files you want to restore.</p>	 <p>System Protection, File Protection, File Archiving or Cloud backup containing different versions of the file to be restored.</p>	 <p>BackupAssist will use the Integrated Restore Console to restore the selected files.</p>

Restore checklist

Use this checklist to make sure you have the required information:

<input type="checkbox"/>	Details about the files you want to restore. For example, the file names and the dates that the files should be restored from.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

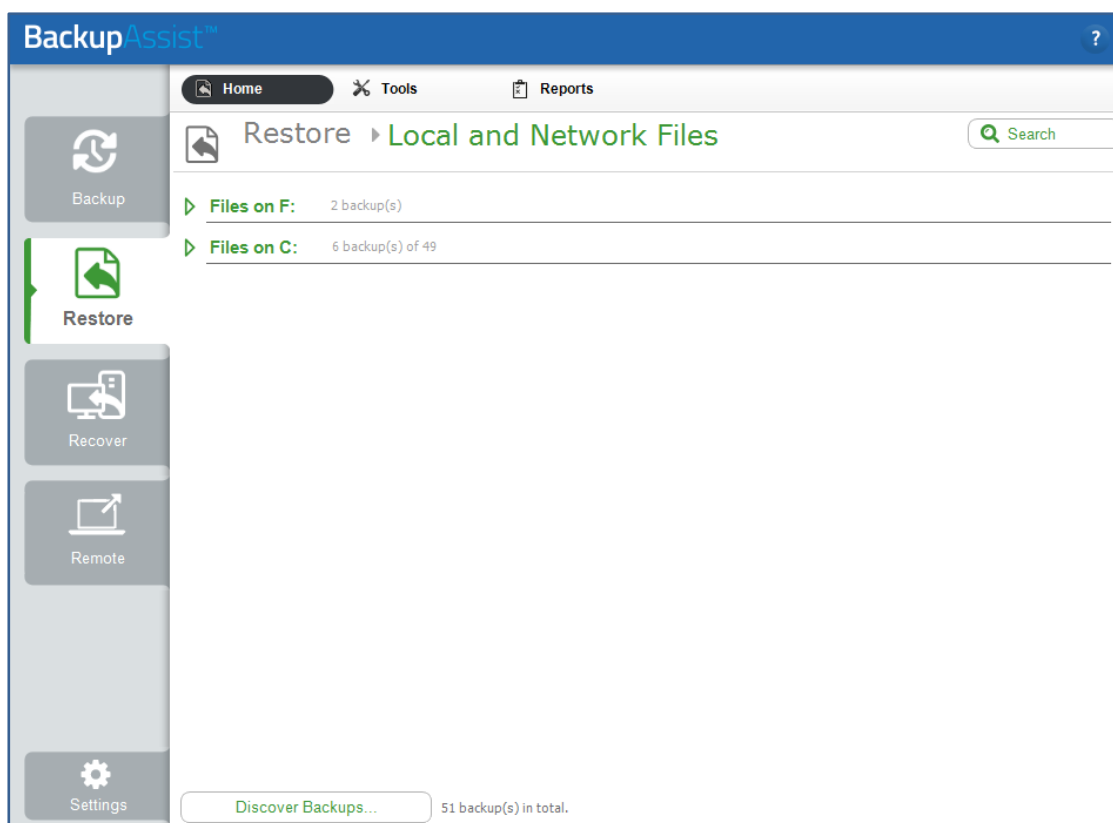
Restore process

To restore different versions of a file, follow these steps:

1. **Select BackupAssist's Restore tab.**
2. **Select Local and Network Files.**

This step starts the guided restore process and opens the **Local and Network Files** screen.

3. Select the Search button.



4. Locate the files that you want to restore.

Use the **Search** functions to search your backups for the **different versions** of the file you want to restore.

The **Search** screen uses two sections to set the search criteria: **Backups** and **Search**.

Backups section

The **Backups** section is used to limit the set of backups that will be searched.

To limit the backups that will be searched:

- Use the **Blue link** next to **Jobs** to view all jobs that have run on this installation of BackupAssist. Deselecting a backup job will exclude any backups made by that job from a search.
- Use the **Backup date** and choose a date range. Only backups created between those dates will be included in the search.

Search section

The **Search** section is used to enter the criteria that will help you find different versions of a file.

This screenshot shows the results of a search for all versions of a file called **history**, between October 1 and December 31. Each backup with files matching the criteria is listed.

The screenshot shows the BackupAssist™ web interface. The top navigation bar includes 'Home', 'Tools', and 'Reports'. The main content area is titled '...Local and Network Files > Search'. On the left sidebar, there are buttons for 'Backup', 'Restore', 'Recover', 'Remote', and 'Settings'. The main search area is divided into two sections: 'Backups' and 'Search'. The 'Backups' section shows a filter for 'Jobs: 1 of 10 FlarebackupNEW' and 'Backup date: between 11/ 7/2017 and 1/16/2020'. The 'Search' section shows a search for '*history*' with filters for 'Created: Between 10/ 1/2019 and 12/31/2019', 'Modified: Before 1/17/2020', and 'Size: Equal 10,000 bytes'. A 'Limit results per backup: 10' is also set. The search results show six backup entries, each with a 'Restore...' button.

The following search criteria are available:

- The **Search for** field will search the **text entered** for occurrences of that text within a file name. If you don't know the exact file name, put * before and after the part of the name you know.
- The **Created** and **Modified** options are used to search for files based on the date they were created or modified. This is different from the **Backups** section's date range, which only applies to the date a backup was created.

When you tick Created or Modified, the **blue link** can be used to set a time frame or context for the selected dates in the date field. For example **Before 4/8/2016**.

- The **Size** option allows you to include a file's size in the search criteria.
- **Limit results per backup** is an important setting, as it **limits** how many **items found** by the search will be shown. If the search results equal the limit, you should increase the limit and/or refine the search criteria so that all of the results are within the limit.

5. Select the backups.

In the screenshot below, the file searched for is called **history.htm**. This file is about 110k in size and contains BackupAssist's release notes. To find the different versions of this file, each backup is opened and checked for instances of **history.htm** with different modified dates.

Two versions of the file have been found. One was modified on 12/20/2019 and the other was Modified on 12/16/2019.

The screenshot displays the BackupAssist interface with search results for 'history.htm' files. The interface includes a sidebar with 'Backup', 'Restore', 'Recover', 'Remote', and 'Settings' buttons. The main area shows search results for four backup jobs. The first job is '1. FlarebackupNEW @ 1/6/2020 10:00 PM' and the fourth is '4. FlarebackupNEW @ 12/16/2019 10:00 PM'. Both show a table of files with columns for Name, Size, Created, Modified, and Location. In the first table, the 'history.htm' file modified on 12/20/2019 8:02 AM is highlighted with a red box. In the second table, the 'history.htm' file modified on 12/16/2019 11:25 AM is highlighted with a red box. A 'Restore...' button is visible next to each backup job.

To restore different versions of a file:

- Select the **Restore** button next to the backup containing the file you want to restore.
- Use the **Integrated Restore Console** to select the file and restore it. This process is documented below in step 6.
- Rename each restored file by adding a suffix to make it clear what version of the file was restored. For example, rename the **history.htm** file modified on 12.16 to **history-12.16.htm**.
- Repeat this process for each version of the file to be restored.

The Integrated Restore Console will not restore a file to a location that already has a file with the same name.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

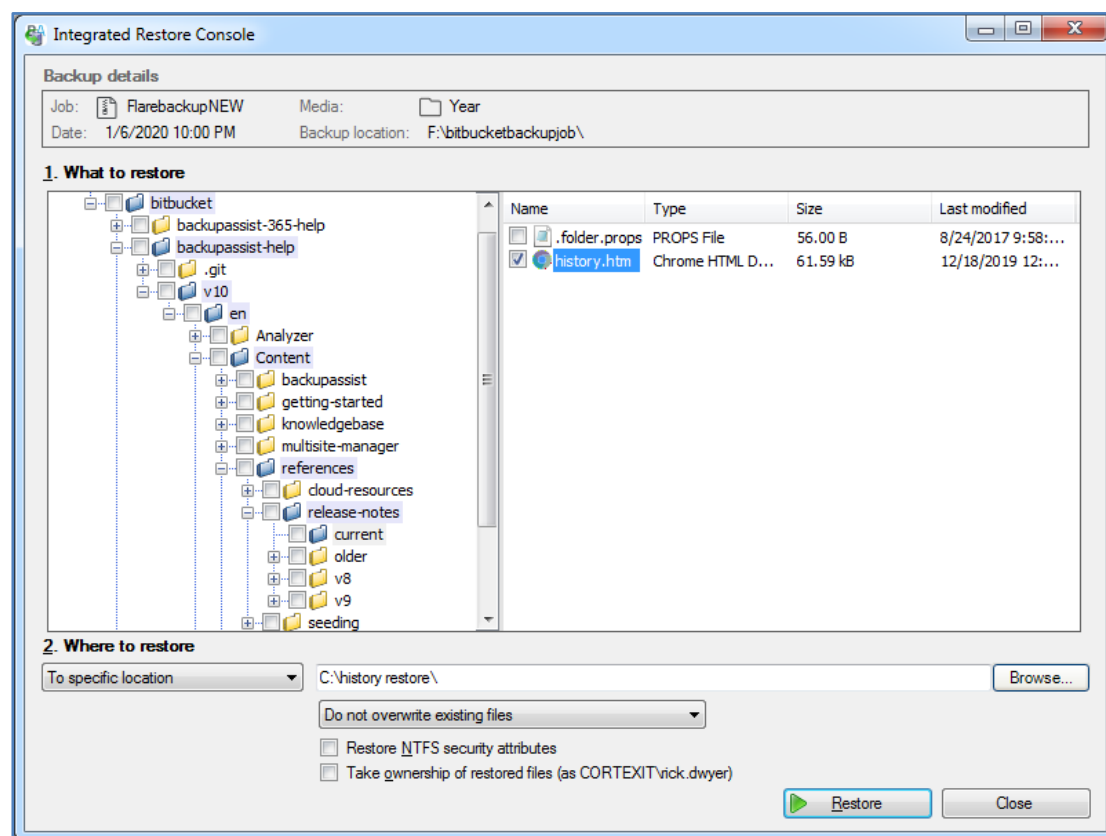
- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

6. Select the files.

Use the Integrated Restore Console to select and restore each version of the file. The location of the file can be seen in the Restore tab's **Location** field, when you view the search results.

To locate and select the file:

- Use the **left pane** to browse through the folders.
- The **right pane** will view the contents of the folder selected in the left pane.
- **Tick the box** next to each file or folder you want to restore. If you tick a folder, all files and folders within it are selected.



7. Configure the restore settings.

Follow these steps to configure the restore options:

- Under **Where to restore** select **To specific location**.
When restoring multiple versions of a file, create a new folder for the files to be restored too.
- Use the **Browse** button to locate and select the restore **destination**.
- Select **Do not overwrite existing files** so that each restored file will not overwrite other versions of the restored file.

Other restore options:

- **Restore NTFS security attributes.**

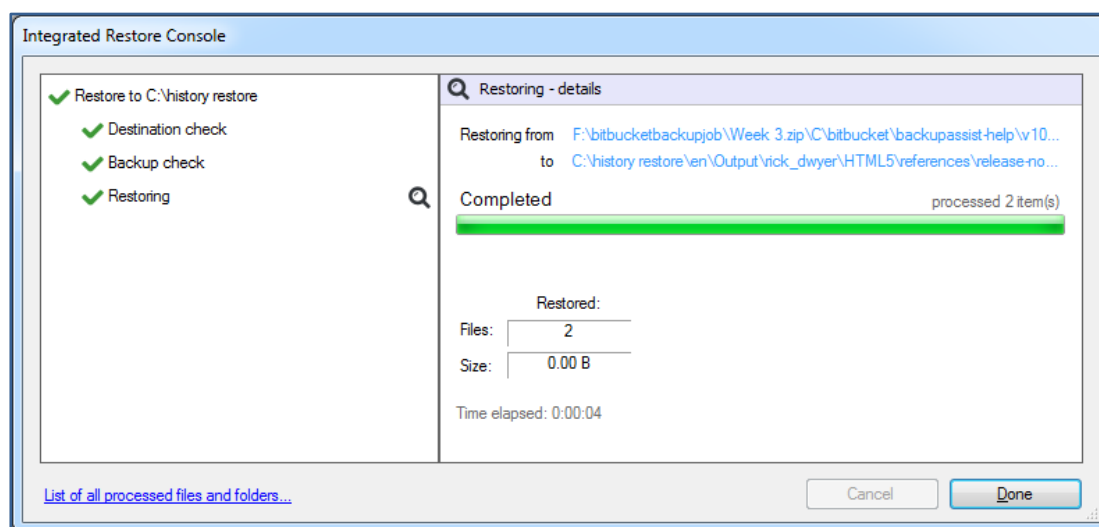
If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.

- **Take ownership of restored files.**

The **user** performing the restore **needs Write access** to the selected files or the restore will fail. This option gives the user Write access to the selected files. The user this applies to is shown to the right of the text box description.

8. Start the restore.

When you select the **Restore** button, the restore **process will begin**. The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.



List all processed files and folders.

Selecting this link on the progress window will open notepad and display a list of the files restored, including their full path.

Remember - the Integrated Restore Console will not restore a file to a location that already has a file with the same name.

Rename each restored file by adding a suffix to make it clear what version of the file was restored. For example, rename the **history.htm** file modified on 12.16 to **history-12.16.htm**.

Then restore the next version of the file.

9. Select Done then Close.

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your files have been restored.

File restore for Hyper-V guest VMs

This section explains **how to locate and restore files inside a VM**, using a Hyper-V host installation of BackupAssist. The **first scenario** explains how to locate and restore **specific files**. The **second scenario** explains how to locate and restore **different versions of the same file**.

9 Point-in-time restore of files and directories on a VM from a host backup

This scenario uses the **Restore tab's Files inside Hyper-V Guests** option to restore files inside a VM using a backup created by a host installation of BackupAssist. The instructions for this scenario use a System Protection Backup.


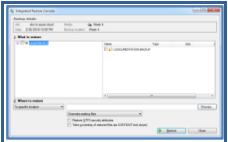



In a nutshell: In this scenario, you will choose a VM backup and the files to be restored, then restore those files to a selected location. Thanks to Hyper-V Granular Restore, this process will be as straight forward as a normal file restore.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To restore a VM's files from the host, you will need BackupAssist and:

Host backup of the VM	Integrated Restore Console	Hyper-V Advanced add-on
 <p>System Protection, File Protection, File Archiving or Cloud Backup of the host, that includes the VM.</p>	 <p>BackupAssist will use the Integrated Restore Console to restore the selected VM files to your chosen location.</p>	 <p>This add-on includes Hyper-V Granular Restore, which will give the Integrated Restore Console access to the VM's files.</p>

Important: To **Search** a VM backup, you need a **System Protection** or **File Protection** backup that was created with the **Catalog Hyper-V Guests** option ticked. To enable this option, **Edit** the backup job and select **Replication options** for File Protection and **Imaging options** for System Protection, and tick the box next to **Catalog Hyper-V Guests**.

Restore checklist

Use this checklist to make sure you have the required information:

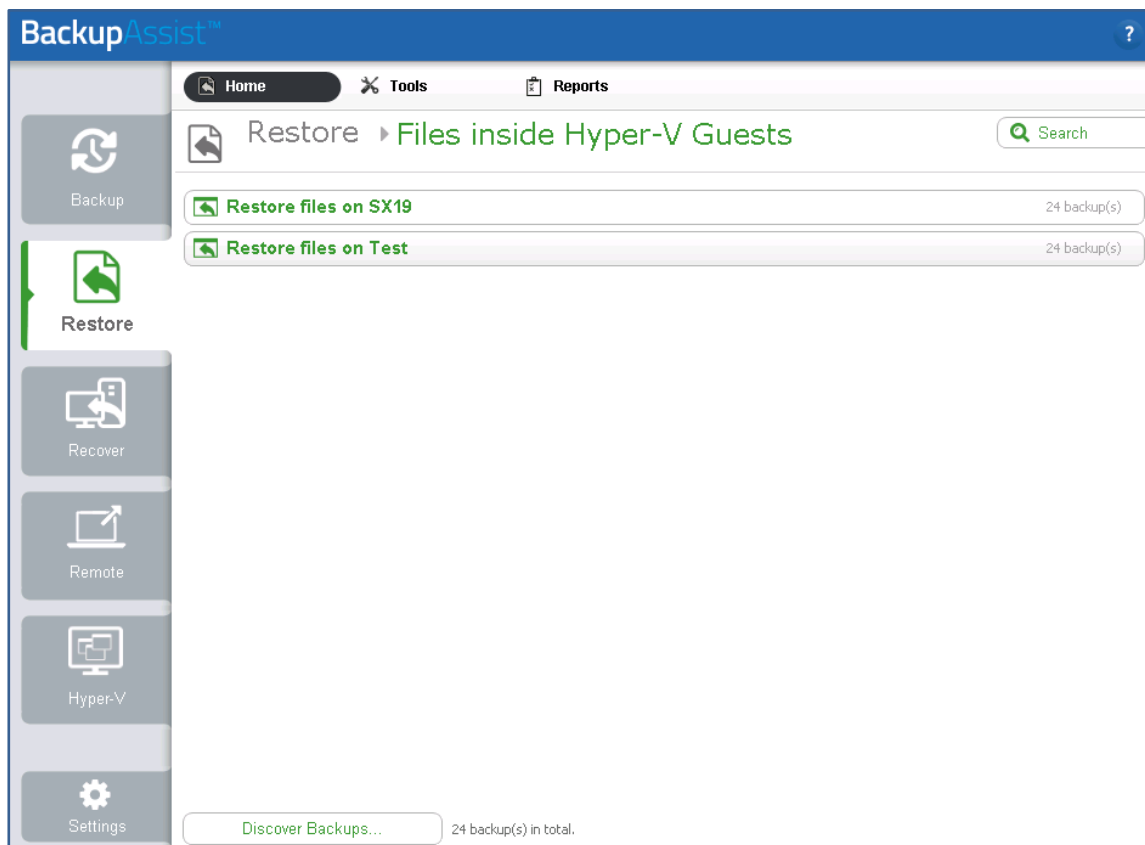
<input type="checkbox"/>	Details about the files you want to restore. For example, the file names and the dates that the files should be restored from.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore a VM's files from a host backup, follow these steps:

1. **Select BackupAssist's Restore tab.**
2. **Select Files inside Hyper-V Guests.**

Selecting **Files inside Hyper-V Guests** will display all the **VMs backed up** on the host.



3. **Select the VM with the files you want to restore.**

When you click on the VM, the screen will display all available backups of that VM.

4. **Locate the files that you want to restore.**

The **Files inside Hyper-V Guests** screen shows the backups of the VM you selected.

- ❖ **If you know the backup** you want but there are dozens of backups listed, the **Filter** option can help you locate the right backup.

For example, if you want a backup made in the previous week, you can select the **Last 7 days** tab to reduce the backups shown, making it easier to spot the one you want.

- ❖ **If you know the files** you want to restore, but don't know what backup they are in, you can use the **Search** options to find those files, and the backups they are in.

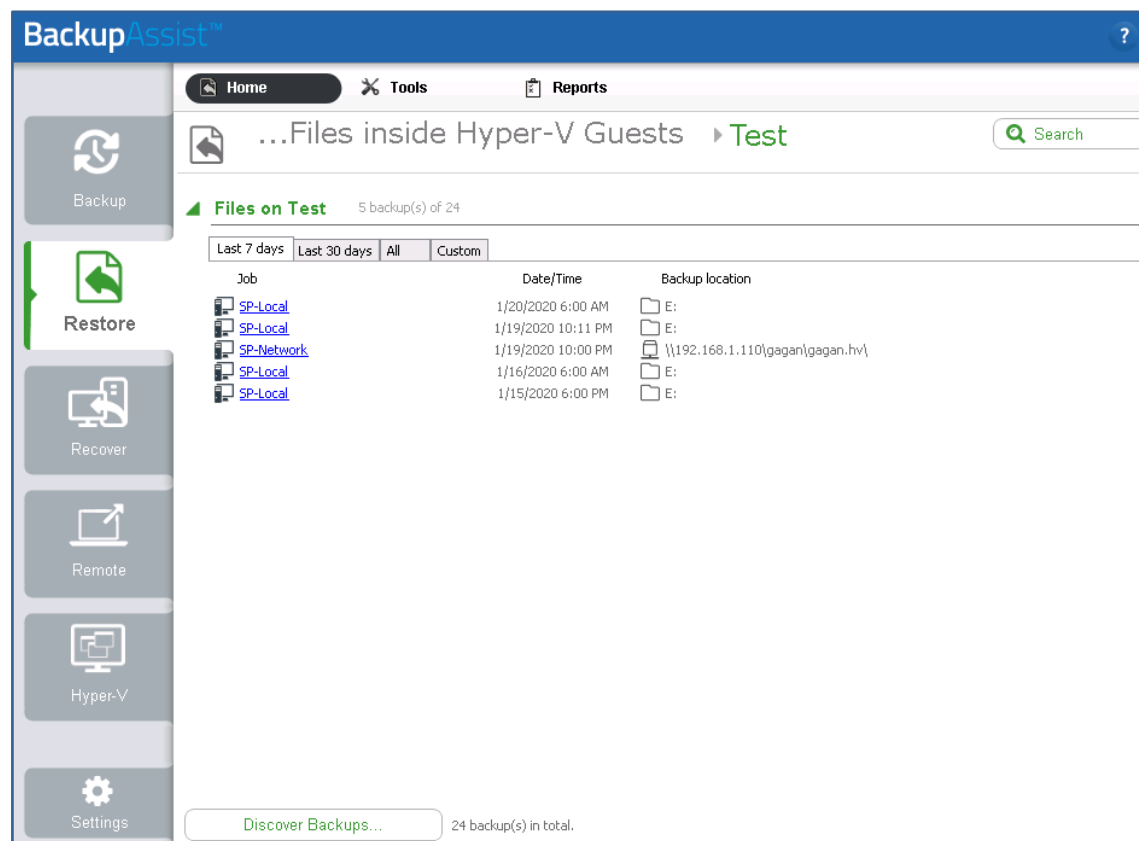
For example, if you want to restore the first version of a file, you can search all of the backups containing that file, then select the first backup that file appears in.

To Filter the backups.

The **tabs above a VM's backup list** can be used to **filter the backups shown**.

The tabs available are:

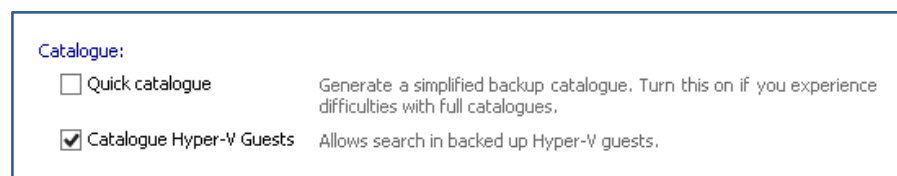
- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.



To Search the backups

To **Search a VM backup**, you must have a System Protection or File Protection backup job with the **Catalog Hyper-V Guests** option ticked.

To enable this option, **Edit** the backup job and select **Replication options** for File Protection and **Imaging options** for System Protection, and tick the box next to **Catalog Hyper-V Guests**.



The **Search button** opens the **Search screen**, which allows you to locate files across all backups.

The **Search** screen uses two sections to set the search criteria: **Backups** and **Search**.

Backups section

The **Backups** section is used to limit the set of backups that will be searched.

To limit the backups that will be searched:

- Use the **Blue link** next to **Jobs** to view all jobs that have run on this installation of BackupAssist. Deselecting a backup job will exclude any backups made by that job from a search.
- Use the **Backup date** and choose a date range. Only backups created between **those** dates will be included in the search.

Search section

The **Search** section is used to enter the criteria that will help you find a file or files.

The following search criteria are available:

- The **Search for** field will search the **text entered** for occurrences of that text within a file name. If you don't know the exact file name, put * before and after the part of the name you know.
- The **Created** and **Modified** options are used to search for files based on the date they were created or modified. This is different from the **Backups** section's date range, which only applies to the date a backup was created.

When you tick Created or Modified, the **blue link** can be used to set a time frame or context for the selected dates in the date field. For example **Before 4/8/2016**.

- The **Size** option allows you to include a file's size in the search criteria.
- **Limit results per backup** is an important setting, as it **limits** how many **items found** by the search will be shown. If the search results equal the limit, you should increase the limit and/or refine the search criteria so that all of the results are within the limit.

5. Select the backup.

From the **Files inside Hyper-V Guests** screen, click on the backup.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

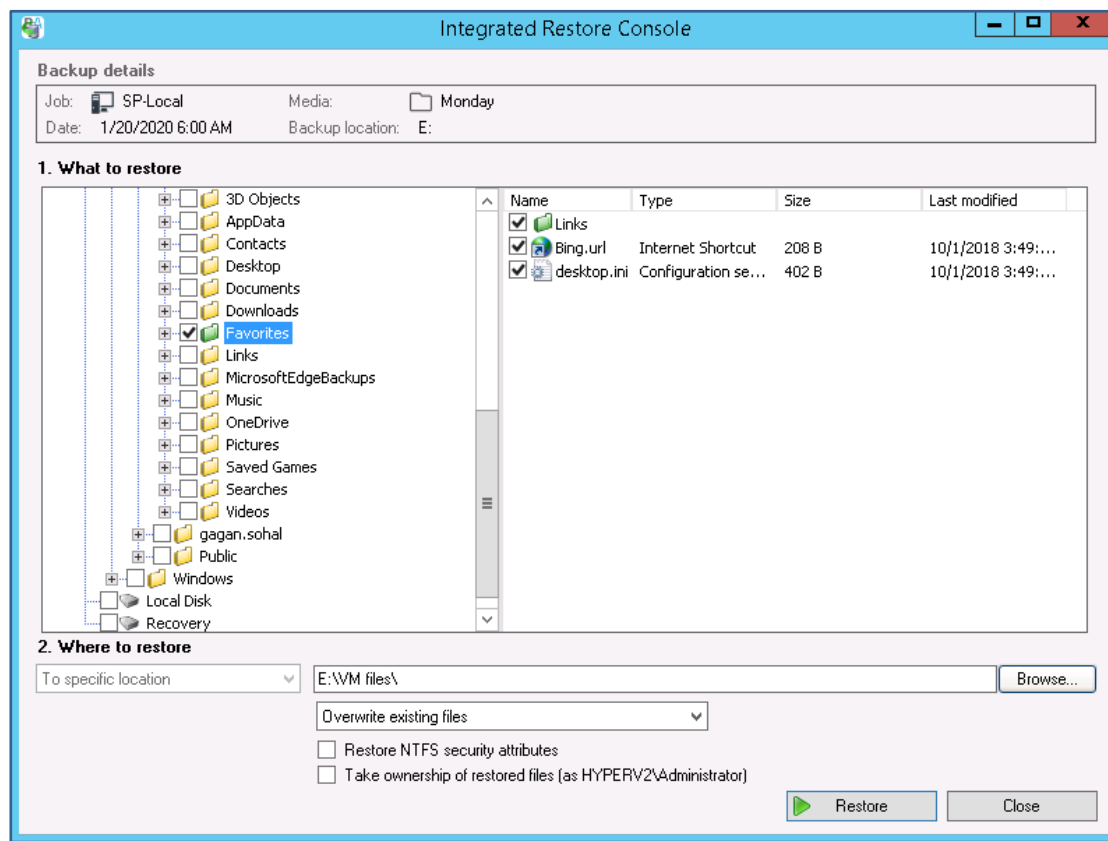
- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

If you performed a **Search**, select the **Restore button** next to the backup.

This will open the backup using the **Integrated Restore Console** (IRC).

6. Select the data.

Use the Integrated Restore Console to **select the files** and **folders** that you want to restore.



To locate and select the data:

- Use the **left pane** to browse through the folders.
- The **right pane** will display the contents of the folder selected in the left pane.
- **Tick the box** next to each file or folder you want to restore. If you tick a folder, all files and folders within it are selected.

7. Configure the restore settings.

Follow these steps to configure the restore options:

- Under **Where to restore** select **To original location** or **To Specific location**.

If you select **To original location** and there are files or folders present with the same names, the **Overwrite** rules will determine what files or folders are retained.

Selecting **To specific Location** can be an easier solution for file and folder restores, as you can further review what data you have and then copy it to a suitable location.

- Use the **Browse** button to locate and select the restore destination.
- The **Overwrite existing files** drop-down box allows you to select the rule that will apply if a destination contains a file or folder with the same name as the file or folder being restored.
 - **Overwrite existing files:** the restored files will overwrite files in the restore destination.

- **Do not overwrite existing files:** the restored files will not overwrite files in the restore destination. This means the files will not be restored.
- **Only overwrite older files:** if a file in the restore destination has changed since the backup was made it will not be overwritten.

d) The **Restore NTFS security attributes** option.

If you select this option, the NTFS security attributes the files had when they were backed up will be retained when the files are restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.

e) The **Take ownership of restored files** option.

The **user** performing the restore **needs Write access** to the selected files or the restore will fail. This option gives the user Write access to the selected files. The user this applies to is shown to the right of the text box description.

8. **Start the restore.**

When you select the **Restore** button, the restore **process will begin**. The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.

List all processed files and folders.

Selecting this link on the progress window will open notepad and display a list of the files restored, including their full path.

9. **Select Done then Close.**

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your files have been restored from the VM.

10 Restore past versions of a file on a Guest VM from backups of the host

This scenario uses the **Restore tab's Files inside Hyper-V Guests** option to restore different versions of a file inside a VM using backups made by a host installation of BackupAssist. The instructions for this scenario use a System Protection Backup.


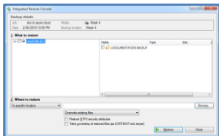



In a nutshell: In this scenario, you will choose the VM and the files to be restored, then restore those files to a selected location. The key is finding the backups containing the files, so we'll use BackupAssist's **Search** functions for a fast, efficient outcome.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To restore a VM's files from the host, you will need BackupAssist and:

<p>Host backups of the VM</p>  <p>System Protection, File Protection, File Archiving or Cloud Backups of the host, that includes the VM.</p>	<p>Integrated Restore Console</p>  <p>BackupAssist will use the Integrated Restore Console to restore the selected VM files to your chosen location.</p>	<p>Hyper-V Advanced add-on</p>  <p>This add-on includes Hyper-V Granular Restore, which will give the Integrated Restore Console access to the VM's files.</p>
---	---	---

Important: To **Search** a VM backup, you need a **System Protection** or **File Protection** backup that was created with the **Catalog Hyper-V Guests** option ticked. To enable this option, **Edit** the backup job and select **Replication options** for File Protection and **Imaging options** for System Protection, and tick the box next to **Catalog Hyper-V Guests**.

Restore checklist

Use this checklist to make sure you have the required information:

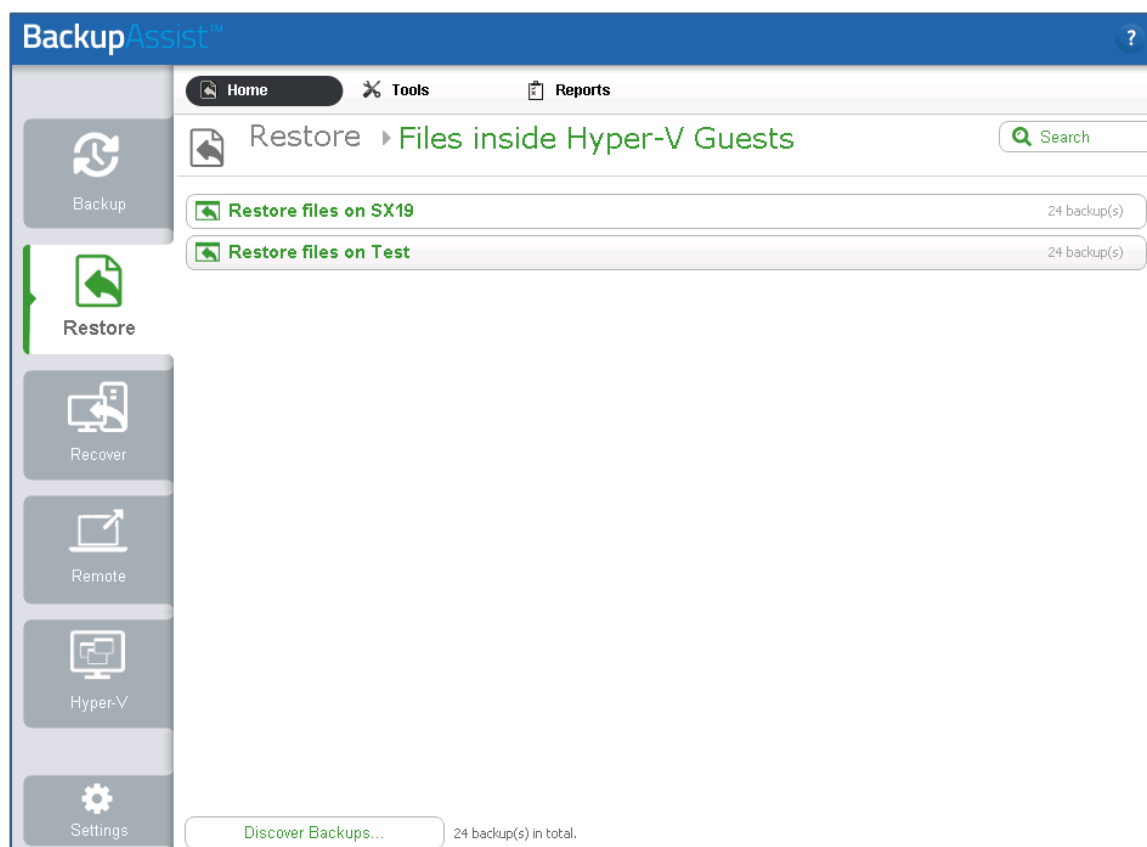
<input type="checkbox"/>	<p>Details about the files you want to restore. For example, the file names and the dates that the files should be restored from.</p>
<input type="checkbox"/>	<p>Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.</p>

Restore process

To restore a VM's files from a host backup, follow these steps:

1. **Select BackupAssist's Restore tab.**
2. **Select Files inside Hyper-V Guests.**

Selecting **Files inside Hyper-V Guests** will display all the **VMs backed up** on the host.



3. **Select the VM with the files you want to restore.**

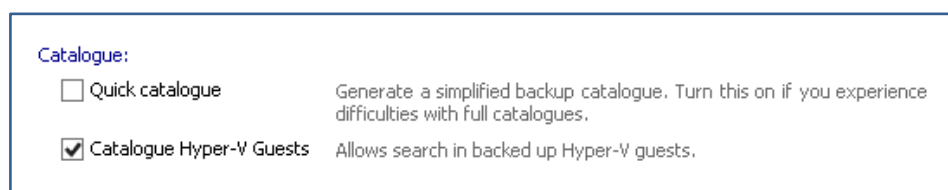
When you click on the VM, the screen will display all available backups of that VM.

4. **Select the Search button.**

If you know what backups have the file you want to restore, select each backup and restore the file as explained in step 6. If you want to search multiple backups for the file, use the **Search** button.

To **Search a VM backup** created by a host installation of BackupAssist, you must have a System Protection or File Protection backup created with the **Catalog Hyper-V Guests** option ticked.

To enable this option, **Edit** the backup job and select **Replication options** for File Protection and **Imaging options** for System Protection, and tick the box next to **Catalog Hyper-V Guests**.



5. **Locate the files that you want to restore.**

The **Search button** opens the **Search screen**, which allows you to locate files across all backups.

The **Search** screen uses two sections to set the search criteria: **Backups** and **Search**.

Backups section

The **Backups** section is used to limit the set of backups that will be searched.

To limit the backups that will be searched:

- Use the **Blue link** next to **Jobs** to view all jobs that have run on the host installation of BackupAssist. Deselecting a backup job will exclude any backups made by that job from a search.
- Use the **Backup date** and choose a date range. Only backups created between those dates will be included in the search.

Search section

The **Search** section is used to enter the criteria that will help you find different versions of a file.

This screenshot shows the results of a search for all versions of a file called **standard0043.log**. Two backups have been found with the file.

The screenshot displays the BackupAssist web interface. The top navigation bar includes 'Home', 'Tools', and 'Reports'. The left sidebar contains icons for 'Backup', 'Restore', 'Recover', 'Remote', 'Hyper-V', and 'Settings'. The main content area is titled '...Test > Search'. Under the 'Backups' section, it shows '2 of 2' backups and a note: 'A backup can only be searched if it was created with 'Catalogue Hyper-V Guests' enabled.' The 'Filter by' section includes a checked 'Jobs' filter for '1 of 1 SP-Local' and an unchecked 'Backup date' filter set to 'between 1/22/2020 and 1/23/2020'. The 'Search' section shows 'Completed in 00:00. Backups with results: 2'. The search criteria are: 'Search for: standard0043.log e.g. report*.docx', 'Created: Before 1/23/2020', 'Modified: Before 1/23/2020', 'Size: Equal 10,000 bytes', and 'Limit results per backup: 10'. A 'Search' button is present. The results list shows two entries: '1. TestSP-Local @ 1/23/2020 10:01 AM Found files: 1, directories: 0' and '2. TestSP-Local @ 1/22/2020 3:49 PM Found files: 1, directories: 0', each with a 'Restore...' button. At the bottom, there is a 'Discover Backups...' button and the text '26 backup(s) in total.'

The following search criteria are available:

- The **Search for** field will search the **text entered** for occurrences of that text within a file name. If you don't know the exact file name, put * before and after the part of the name you know.
- The **Created** and **Modified** options are used to search for files based on the date they were created or modified. This is different from the **Backups** section's date range, which only applies to the date a backup was created.

When you tick Created or Modified, the **blue link** can be used to set a time frame or context for the selected dates in the date field. For example **Before 4/8/2016**.

- The **Size** option allows you to include a file's size in the search criteria.
- **Limit results per backup** is an important setting, as it **limits** how many **items found** by the search will be shown. If the search results equal the limit, you should increase the limit and/or refine the search criteria so that all of the results are within the limit.

6. Select the backup.

In the screenshot below, the file searched for is called **standard0043.log**. To find the different versions of this file, each backup is opened and checked for instances of **standard0043.log** with different modified dates.

In the screenshot below, two versions of the file have been found.

The screenshot shows the BackupAssist interface with a search for 'standard0043.log'. The search criteria include 'Created: Before 1/23/2020', 'Modified: Before 1/23/2020', and 'Size: Equal 10,000 bytes'. The search results are displayed in two sections:

1. TestSP-Local @ 1/23/2020 10:01 AM Found files: 1, directories: 0

Name	Size	Created	Modified	Location
standard0043.log	33.96 kB	2/25/2019 11:44 AM	1/23/2020 1:57 PM	Local Disk\Users\gagan.sohal\Downloads

2. TestSP-Local @ 1/22/2020 3:49 PM Found files: 1, directories: 0

Name	Size	Created	Modified	Location
standard0043.log	33.90 kB	2/25/2019 11:44 AM	3/14/2019 10:49 AM	Local Disk\Users\gagan.sohal\Downloads

To restore different versions of a file:

- Select the **Restore** button next to the backup containing the file you want to restore.
- Use the **Integrated Restore Console (IRC)** to select the file and restore it. This process is documented below in step 7.
- Rename each restored file by adding a suffix to make it clear what version of the file was restored. For example, rename the **standard0043.log** file modified on 12.16 to **standard0043-12.16.log**.
- Repeat this process for each version of the file to be restored.

The IRC will not restore a file to a location that already has a file with the same name.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

7. Select the file.

Use the Integrated Restore Console to select and restore each version of the file. The location of the file can be seen in the **Search results Location field**, for that file.

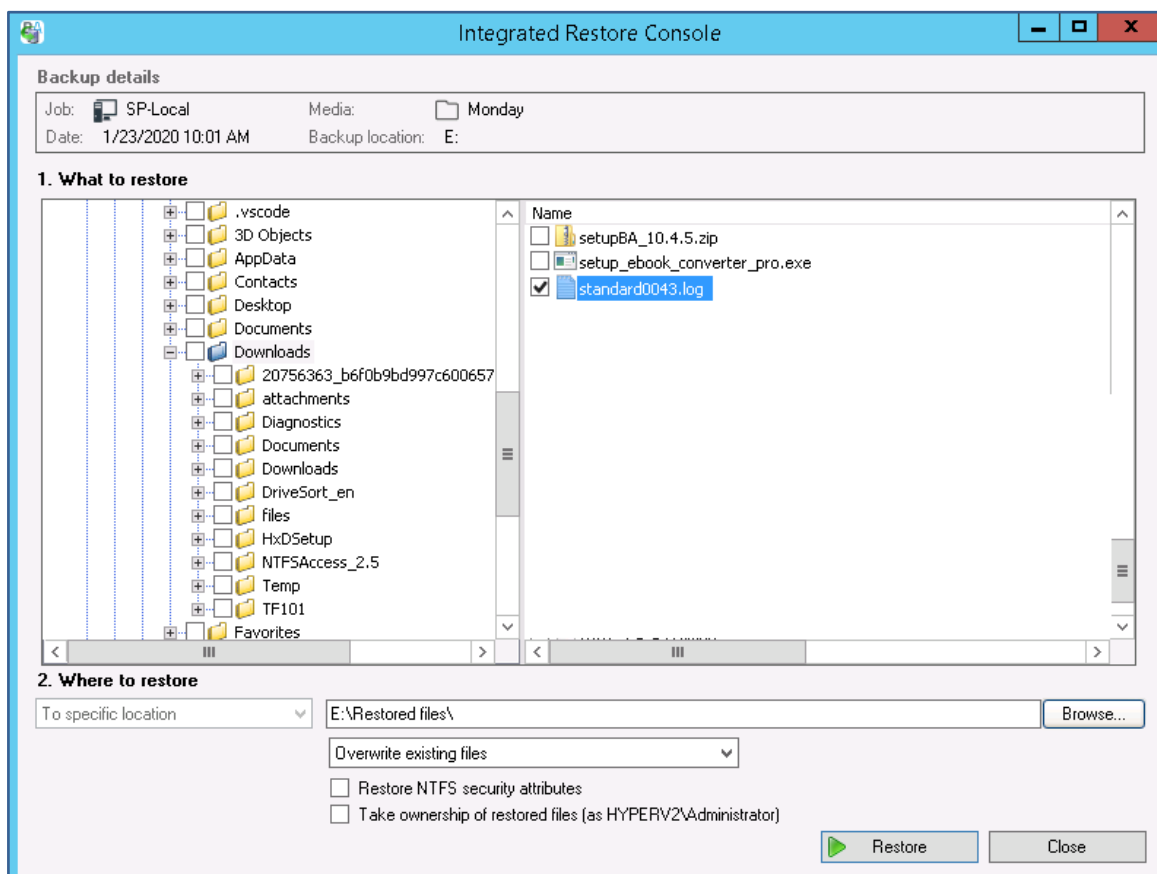
To locate and select the file:

- Use the **left pane** to browse through the folders.
- The **right pane** will view the contents of the folder selected in the left pane.
- **Tick the box** next to the file or folder you want to restore. If you tick a folder, all files and folders within it are selected.

8. Configure the restore settings.

Follow these steps to configure the restore options:

- Under **Where to restore** select **To original location** or **To Specific location**.



If you select **To original location** and there are files or folders present with the same names, the **Overwrite** rules will determine what files or folders are retained.

Selecting **To specific Location** can be an easier solution for file and folder restores, as you can further review what data you have and then copy it to a suitable location.

- b) Use the **Browse** button to locate and select the restore destination.
- c) The **Overwrite existing files** drop-down box is used to select the rule that will apply if a destination contains a file or folder with the same name as the file or folder being restored.

As noted in step 6, **each version of the file is renamed** by adding a suffix to make it clear what version of the file was restored. This means there will be no complications from the **Overwrite** option selected.

- d) The **Restore NTFS security attributes** option.

If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.

- e) The **Take ownership of restored files** option.

The **user** performing the restore **needs Write access** to the selected files or the restore will fail. This option gives the user Write access to the selected files. The user this applies to is shown to the right of the text box description.

9. **Start the restore.**

When you select the **Restore** button, the restore **process will begin**. The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.

List all processed files and folders.

Selecting this link on the progress window will open notepad and display a list of the files restored, including their full path.

10. **Select Done then Close.**

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your files have been restored.

Exchange Server restore and recover

11 Recover entire Exchange Server from backup

This scenario uses the **Restore tab's Exchange Server** option to restore an Exchange Server from a System Protection backup.

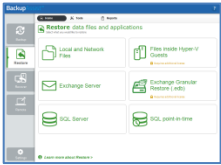

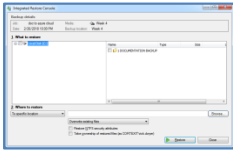


In a nutshell: In this scenario, you will choose an Exchange Server backup, select the Exchange Server application in that backup and run a restore, replacing the Exchange Server's files and database.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform an Exchange Server restore, you will need:

BackupAssist	A backup	Integrated Restore Console
 <p>BackupAssist will be used to select Exchange Server restore and locate the Exchange Server backup.</p>	 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the Exchange Server.</p>	 <p>BackupAssist will use the Integrated Restore Console to select and restore the Exchange Server.</p>

Recovery checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	If you are restoring a production Exchange Server, you should perform the restore at a time with minimal impact on the Exchange users and communicate the expected downtime.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore an Exchange Server, follow these steps:

1. **Open BackupAssist.**
2. **Select the Restore tab.**
3. **Select Exchange Server.**

This step starts the guided restore process and opens the **Exchange Server** screen.

4. Locate the backup you want to restore from.

The **Exchange Server** screen lists all of the Exchange Server backups.

The tabs along the top can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.

The screenshot shows the BackupAssist 10.5.1 application window. The main area displays the 'Exchange Server' backup list for a 'Local Exchange Server'. The interface includes a sidebar with 'Backup', 'Restore', 'Recover', 'Remote', and 'Settings' buttons. The main content area has tabs for 'Last 7 days', 'Last 30 days', 'All', and 'Custom'. Below the tabs is a table of backup jobs with columns for Job, Date/Time, and Backup location.

Job	Date/Time	Backup location
SP-Network	1/19/2020 6:00 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/15/2020 1:12 AM	E:\BackupAssist\FA-Local\
FA-Network	1/14/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/14/2020 1:13 AM	E:\BackupAssist\FA-Local\
FA-Network	1/13/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/13/2020 1:11 AM	E:\BackupAssist\FA-Local\
FA-Network	1/12/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/12/2020 1:10 AM	E:\BackupAssist\FA-Local\
FA-Network	1/11/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/11/2020 1:10 AM	E:\BackupAssist\FA-Local\
FA-Network	1/10/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/10/2020 1:09 AM	E:\BackupAssist\FA-Local\
FA-Network	1/9/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/8/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/7/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/6/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/5/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/4/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/3/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/2/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/1/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	12/31/2019 11:59 PM	\\192.168.1.110\Gagan\gagan.219\

At the bottom of the window, there is a 'Discover Backups...' button and a status message: '181 backup(s) in total.'

5. Select the backup

When you select the backup, it will be opened by the **Integrated Restore Console (IRC)**.



For encrypted backups

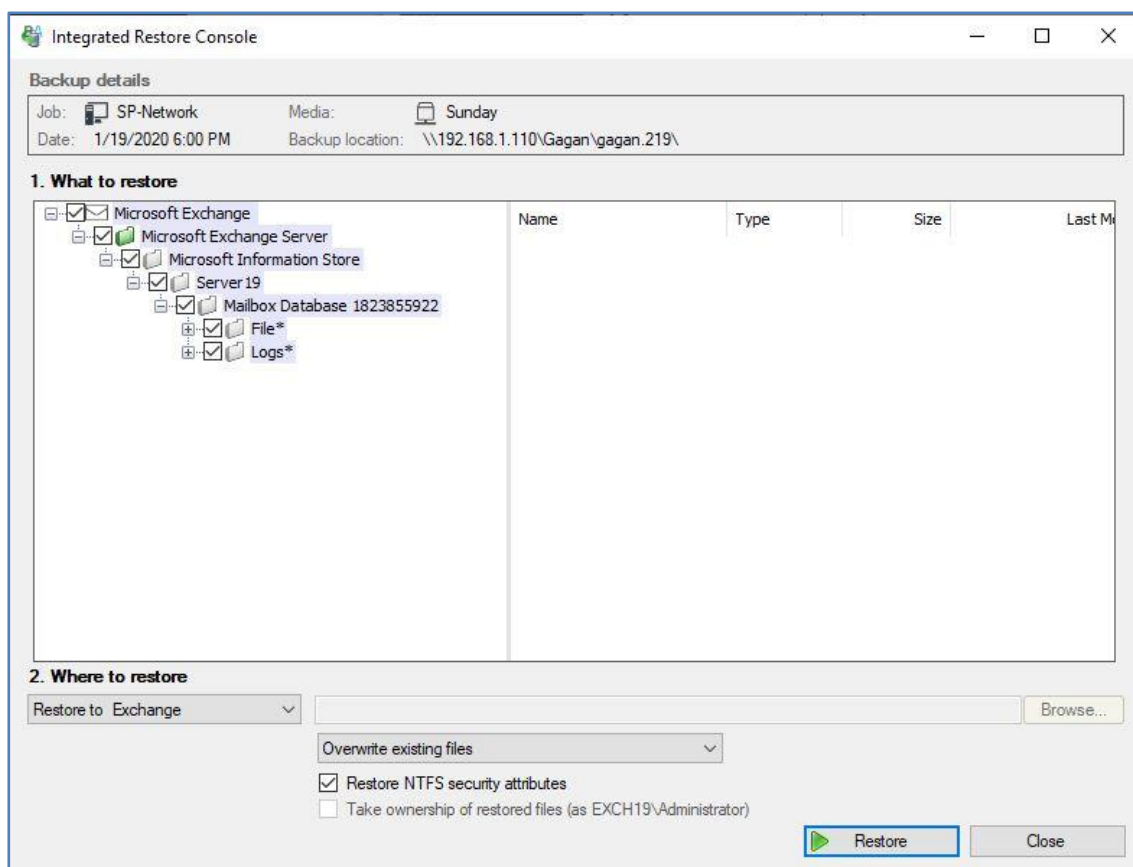
If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

6. Select the Exchange Server.

Use the Integrated Restore Console to **tick** the box next to **Microsoft Exchange**. This is the top box with the envelope icon. Ticking it will select all of the files required for an Exchange Server restore.



7. Configure the restore settings.

Follow these steps to configure the restore options:

- Under **Where to restore** leave **Restore to Exchange** selected.
- Leave **Overwrite existing files** selected.

When the Exchange Server's files are restored, they will replace the existing files.

- The **Restore NTFS security attributes** option.

If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.

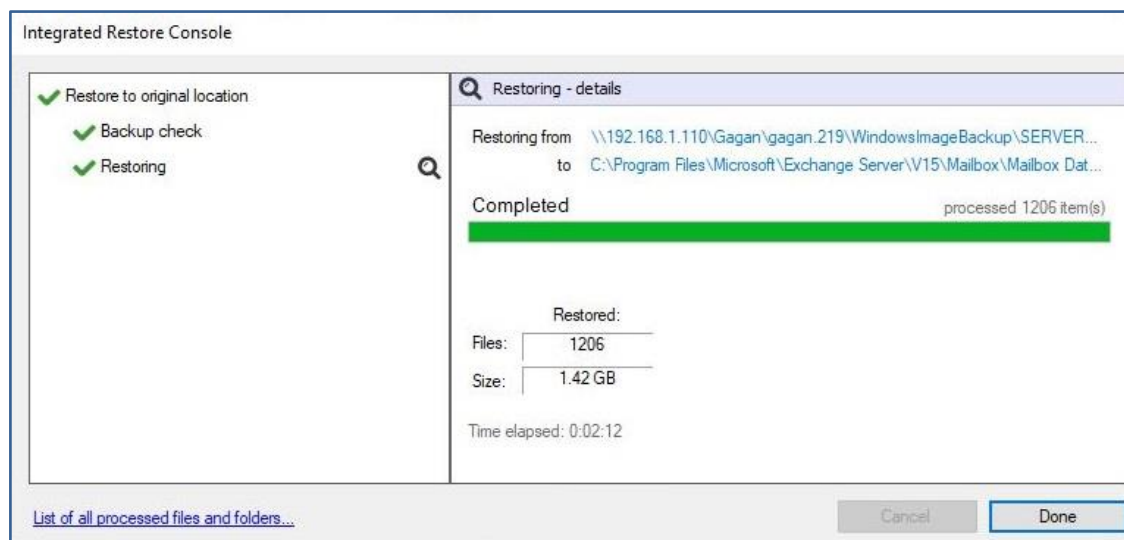
8. Start the restore.

When you select the **Restore** button, the Exchange Server restore **process will begin**.

BackupAssist will:

- Stop the Exchange Server.
- Restore the Exchange Server.
- Start the Exchange Server.

The Integrated Restore Console will display information about the restore and provide status updates as the job runs.



List all processed files and folders.

Selecting this link will open notepad and display a list of the files restored, including their full path.

9. Select Done then Close.

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your Exchange Server has been restored

12 Recover specific Exchange Database(s) from backup

This scenario uses the **Restore tab's Exchange Server** option to restore an Exchange Server database from a System Protection backup.

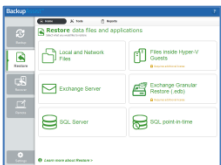

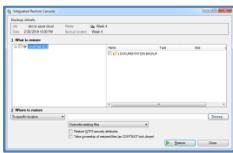


In a nutshell: In this scenario, you will choose an Exchange Server backup, select that Exchange Server's database file and restore that file to its original location. This will replace the current database, resolving any problems the database may have caused.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform an Exchange database restore, you will need:

BackupAssist	A backup	Integrated Restore Console
 <p>BackupAssist will be used to select Exchange Server restore and locate the Exchange Server backup.</p>	 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the Exchange Server.</p>	 <p>BackupAssist will use the Integrated Restore Console to select and restore the Exchange database.</p>

Recovery checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	If you are restoring a production Exchange Server, you should perform the restore at a time with minimal impact on the Exchange users and communicate the expected downtime.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore an Exchange database, follow these steps:

1. **Open BackupAssist.**
2. **Select the Restore tab.**
3. **Select Exchange Server.**

This step starts the guided restore process and opens the **Exchange Server** screen.

4. Locate the backup you want to restore from.

The **Exchange Server** screen lists all of the Exchange Server backups.

The tabs along the top can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.

Job	Date/Time	Backup location
SP-Network	1/19/2020 6:00 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/15/2020 1:12 AM	E:\BackupAssist\FA-Local\
FA-Network	1/14/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/14/2020 1:13 AM	E:\BackupAssist\FA-Local\
FA-Network	1/13/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/13/2020 1:11 AM	E:\BackupAssist\FA-Local\
FA-Network	1/12/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/12/2020 1:10 AM	E:\BackupAssist\FA-Local\
FA-Network	1/11/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/11/2020 1:10 AM	E:\BackupAssist\FA-Local\
FA-Network	1/10/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/10/2020 1:09 AM	E:\BackupAssist\FA-Local\
FA-Network	1/9/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/8/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/7/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/6/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/5/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/4/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/3/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/2/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/1/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	12/31/2019 11:59 PM	\\192.168.1.110\Gagan\gagan.219\

5. Select the backup

When you select the backup, it will be opened by the **Integrated Restore Console (IRC)**.



For encrypted backups

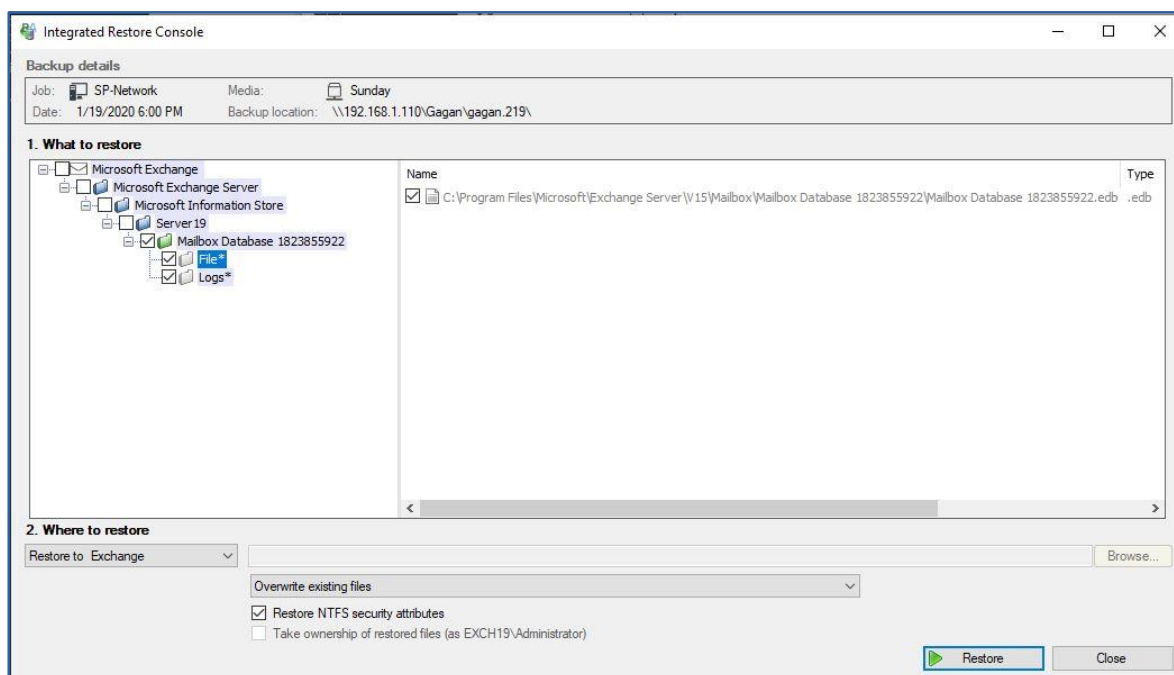
If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

6. Select the Exchange Server's database.

Use the Integrated Restore Console to **tick** the box next to **Mailbox Database**. This will select the .edb file and the database logs.



7. Configure the restore settings.

Follow these steps to configure the restore options:

- d) Under **Where to restore** leave **Restore to Exchange** selected.

This will restore the .edb file to its original location in the Exchange Server.

- e) Leave **Overwrite existing files** selected.

When the .edb file is restored, it will write over and replace the existing .edb file.

- f) The **Restore NTFS security attributes** option.

If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.



BackupAssist will automatically stop and start the Exchange services for the restore. However, if you restore the database to another location and want to manually copy it to replace the current database, you will need to stop the Exchange services first, and start the services after the database has been copied.

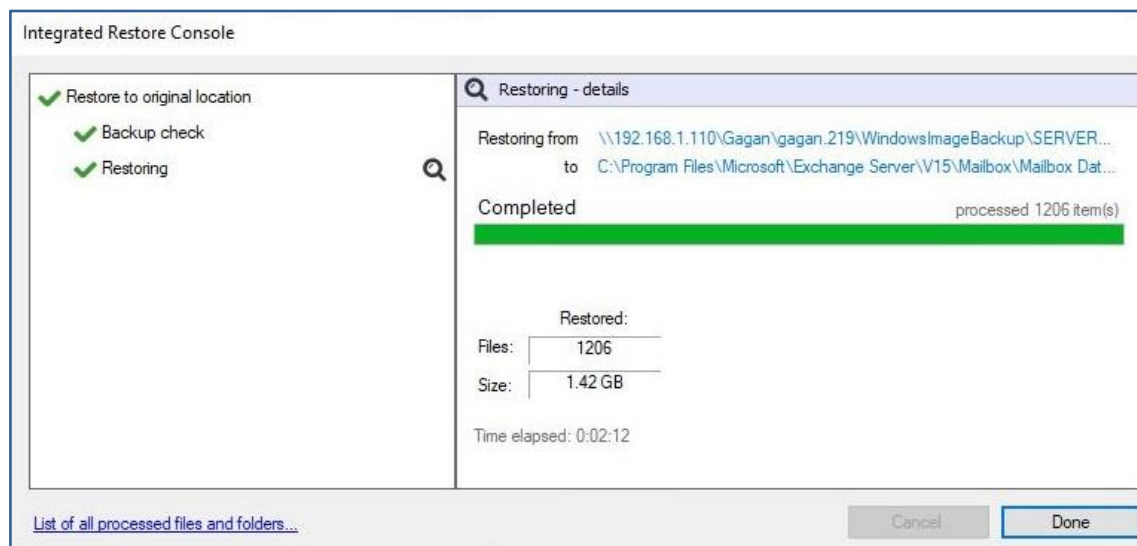
8. Start the restore.

When you select the **Restore** button, the restore **process will begin**.

BackupAssist will:

- Stop the Exchange Server.
- Restore the Exchange database.
- Start the Exchange Server.

The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.



List all processed files and folders.

Selecting this link on the progress window will open notepad and display a list of the files restored, including their full path.

9. Select Done then Close.

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

Congratulations – your Exchange database has been restored

13 Granular restore of emails from a backup of Exchange in a physical environment

This **scenario** uses **Exchange Granular Restore (EGR)** to restore **individual emails** from a System Protection backup.


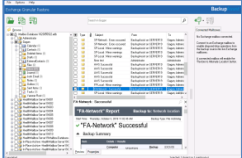
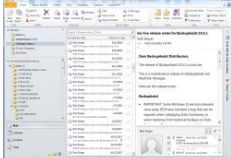


In a nutshell: In this scenario, you will open a backup using EGR, find some emails that need to be restored and export them to a PST file. This file will be given to the user who requested the restore, and they will open it in Outlook to view and access the emails.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To restore emails from an Exchange Server, you will need BackupAssist and:

A backup	Exchange Granular	Outlook
 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the Exchange Server.</p>	 <p>Exchange Granular Restore is used to locate and restore mail items, and requires the Exchange Granular add-on.</p>	 <p>An Outlook mail client will be used to review and copy the restored emails.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	<p>You will need information about the emails that are to be restored. For example, the date that the emails should be restored from, the name of the mailbox and search criteria that will help locate specific emails, like the Subject of an email.</p>
<input type="checkbox"/>	<p>Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.</p>

Restore process

To restore Exchange emails, follow these steps:

1. **Select the BackupAssist Restore tab.**
2. **Select Exchange Granular Restore (.edb).**

This step starts the guided restore process and opens the **Exchange Granular Restore** screen.

3. **Locate the backup you want to restore from.**

The **Exchange Granular Restore** screen shows the Exchange Servers backed up by this installation of BackupAssist.

The tabs above each volume's backup list can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.

Job	Date/Time	Backup location
SP-Network	1/19/2020 6:00 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Network	1/14/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/14/2020 1:13 AM	E:\BackupAssist\FA-Local\
FA-Network	1/13/2020 11:59 PM	\\192.168.1.110\Gagan\gagan.219\
FA-Local	1/13/2020 1:11 AM	E:\BackupAssist\FA-Local\

4. Select the backup

Click the **Backup** you want to restore from then **click the .edb file** that is listed under the backup, as shown in the screenshot above. The backup will open in **Exchange Granular Restore (EGR)**.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

5. Locate the emails that you want to restore.

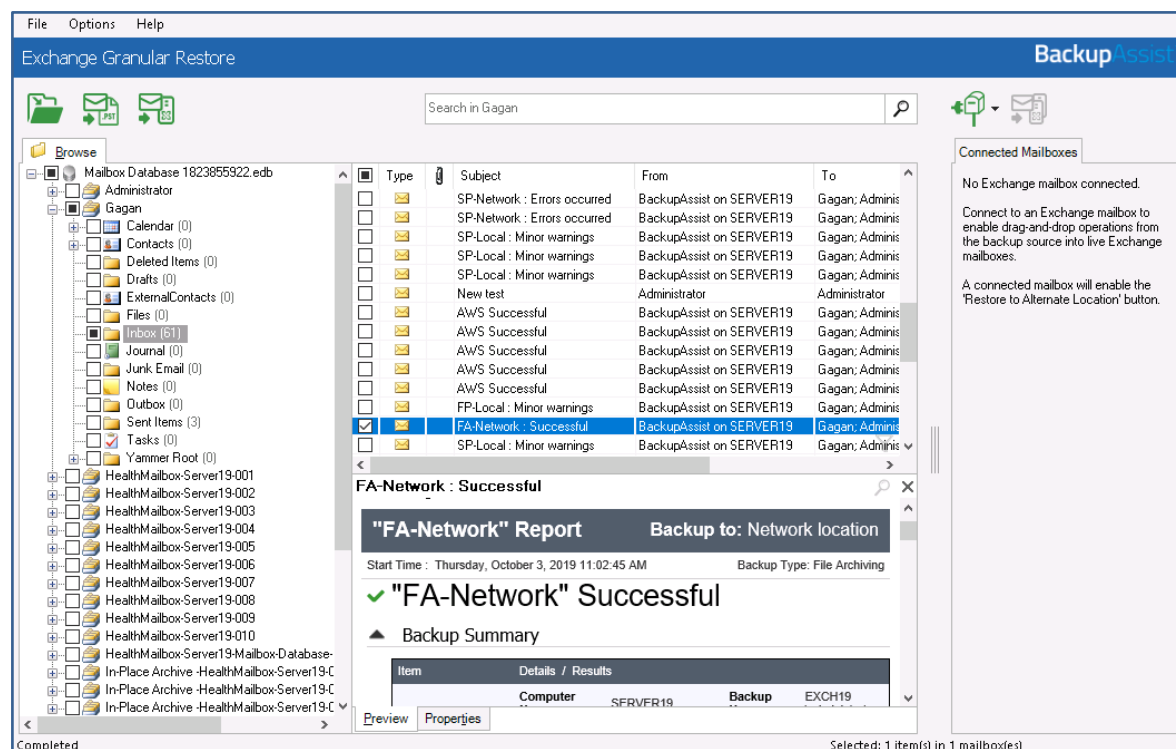
The Exchange Granular Restore console has a mail tree that you can **Browse** and **Search**. Both of these options will help locate, preview and select the emails that you want to restore.

Using Browse

Browsing for the emails you want to restore is **ideal** when you **know the email's location**.

To browse for the emails:

- Expand a mailbox and select one of its folders to show the individual emails inside it.
- Select an email to preview its contents in the pane below it.



Using Search

Searching for emails is **ideal** when you **do not know an email's location**.

To perform a search:

- If you know what mailbox** to search, **tick the box** next to that mailbox and its name will appear in the Search field. If you select multiple mailboxes, they will be listed in the **Search in...** field. Any expanded mailboxes are also added to the search by default.

The search feature will search the entire database unless you select a specific mailbox.

- Click the **Search field** to open the **Search dialog** and enter your search criteria.

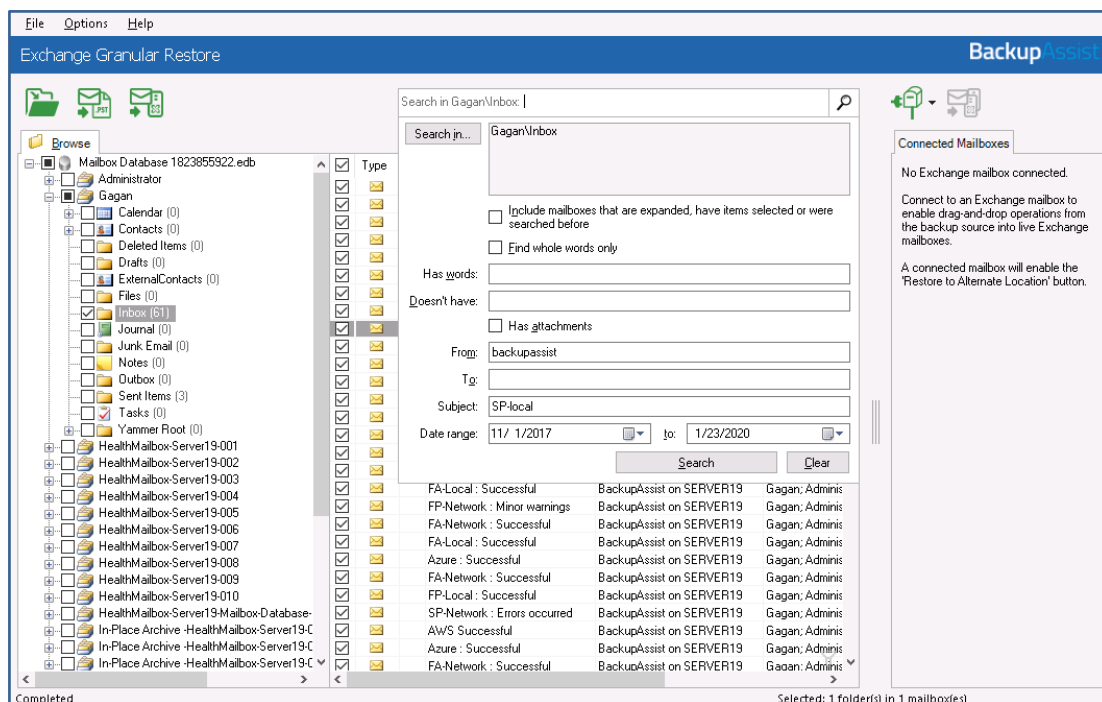
The option **Include mailboxes that are expanded, have items selected or were searched before** is ticked by default. Deselect this if you only want to search ticked mailboxes.

The following criteria can be used to perform a search:

- **Find whole words only**, select if you only want to search for emails with complete versions of any search words used.

- **Has words** - searches all parts of an email (body, Subject, etc.) for the words in this field.
- **Doesn't have** - searches for emails that do not have the words entered in this field.
- **Has attachments** - will search for emails with attachments.
- **From** - will search for words entered in the From: field.
- **To** - will search for words entered in the To: field.
- **Subject** - will search for words entered in the Subject: field.
- **Date range** - will search for emails created, sent or received between the selected dates.

c) Select the **search icon** to **start the search**.



A **new tab** will open with **matches** for your search.

If a search does not match any emails, review your search parameters and run another search.



If you want to **include emails** that are **no longer present** in user mailboxes, select the Options menu then click **display hidden deleted items** and **Display all items**. Deleted items from Exchange Server 2007 are stored in their original folders. Deleted items from Exchange 2010 and later are stored in the Deletions folder. These items can only be exported to a PST file.

6. Select the emails you want to restore.

Tick the box next to each email that you want to restore from the **Browse** pane.

If you performed a **search**, select each email listed in the search results. To restore **all items** listed **in the search** results, tick the Inbox. This will restore a copy of the mail account's inbox containing only the items listed in the search results.

7. Restore the selected emails.

There are three ways to restore emails: to their **original location**, to an **alternate location** and **Export to PST**.

Export to PST file is a good option as it **restores the emails to a file** that can be **given to the user** who requested the restore. The user can then open the PST file in their Outlook mail client.

To restore the emails to a PST file:

- Select the **Export to PST** file button.

This button will become active when emails or mailboxes have been selected.

- Confirm the **Personal Storage Table (PST)** format.

You can choose Unicode or ANSI encoding for the PST output file.

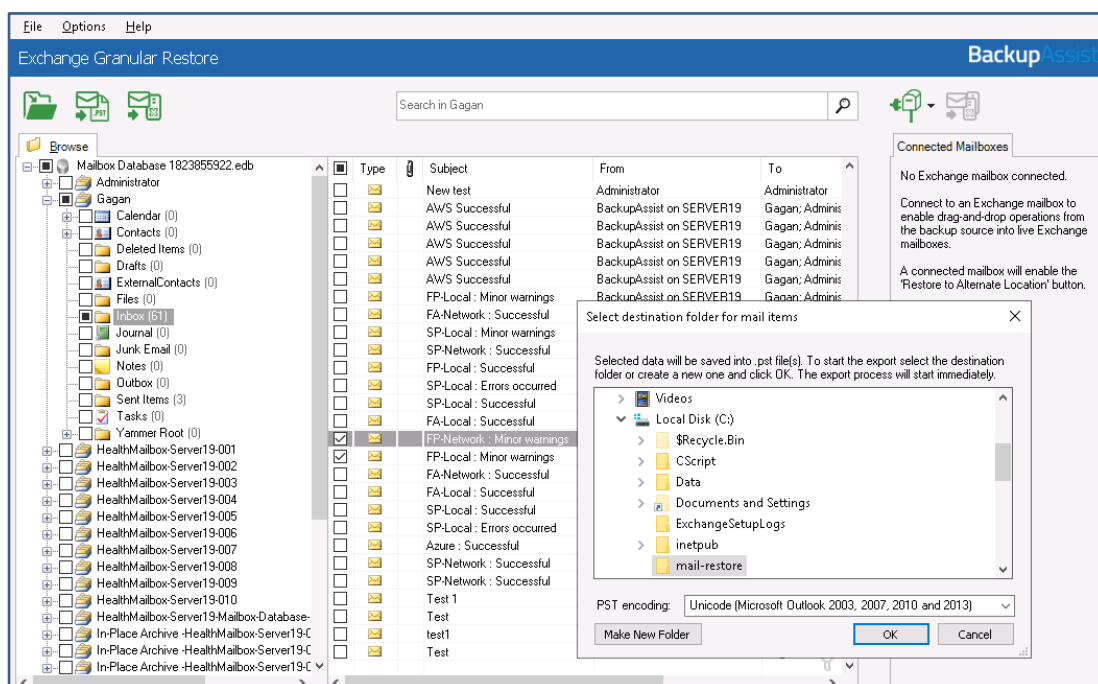
With large exports, there can be more than one PST file. Additional files are created automatically when the file size limit is reached. The limit depends on the output file encoding.

- For ANSI PST files, the size limit is 1 GB.
- For Unicode PST files, the size limit is 10 GB.
- A maximum of 15,000 messages can be restored into the PST file.

- Select the **destination**.

You will be asked to select a folder or create a new folder.

After selecting the new or existing folder, the export will begin.



A window will display the export's progress. The export can be canceled by clicking the **Stop Export** button.

The emails will be exported to a .pst file named: "Restore NNN <Mailbox Name>[VVV]. pst", where NNN is the current recovery session identifier and VVV is the volume number.

8. Open the PST file and access the emails.

The user who requested the restore can be given a copy of the PST file to open and access the emails. The user should follow these instructions.

To open a PST using an Outlook Client:

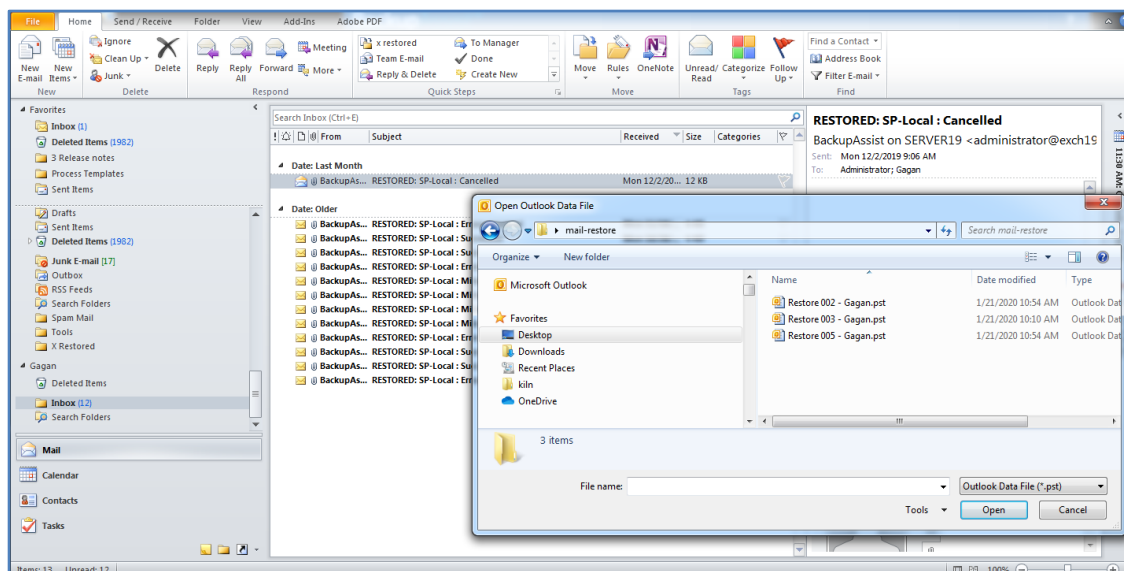
- Click **File** > **Open** and choose **Open Outlook Data File**.
- Browse** to the **PST file** that was exported.
- Select** the **PST file** and click **OK**.

The **PST file** will appear **in Outlook** as a container.

RESTORED will appear in the Subject line of each email restored. This is enabled by default and can be turned off by selecting **Options** > Add 'RESTORED' to exported item > No.

In the **screenshot below**, a PST has been restored and the contents of the PST appear with RESTORED next to each email.

Another PST is about to be selected and added to the Outlook client.



You can now:

- View and access the emails in Outlook.
- Drag-and-drop the emails from the PST to another folder in Outlook. These emails will be automatically synchronized with the live Exchange Server database.

Congratulations – your emails have been restored.

14 Granular restore of emails from a backup of Exchange in Hyper-V environment

This **scenario** restores **individual emails** from an Exchange Server running in a VM, from an installation of BackupAssist on a Hyper-V host. The scenario's instructions use a System Protection backup.


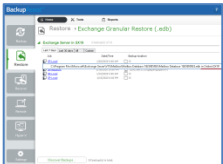
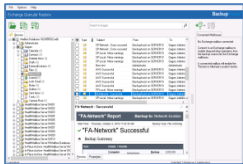
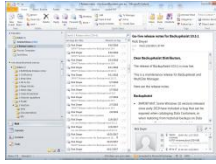


In a nutshell: In this scenario, you will open a backup, find the emails that need to be restored and export them to a PST file. This file will be given to the user who requested the restore, and they will open it in Outlook to view and access the emails.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To restore emails from a VM running Exchange, you will need BackupAssist and:

A backup	Hyper-V Granular	Exchange Granular	Outlook
 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the Exchange Server.</p>	 <p>Hyper-V Granular Restore will mount the Exchange VM so Exchange Granular Restore can access the mail database.</p>	 <p>Exchange Granular Restore is used to locate and restore mail items, and requires the Exchange Granular add-on.</p>	 <p>An Outlook mail client will be used to review and copy the restored emails.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	You will need information about the emails that are to be restored. For example, the date that the emails should be restored from, the name of the mailbox and search criteria that will help locate specific emails, like the Subject of an email.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore Exchange emails from a host backup, follow these steps:

1. **Select the BackupAssist Restore tab.**
2. **Select Exchange Granular Restore (.edb).**

This step starts the guided restore process and opens the **Exchange Granular Restore** screen.

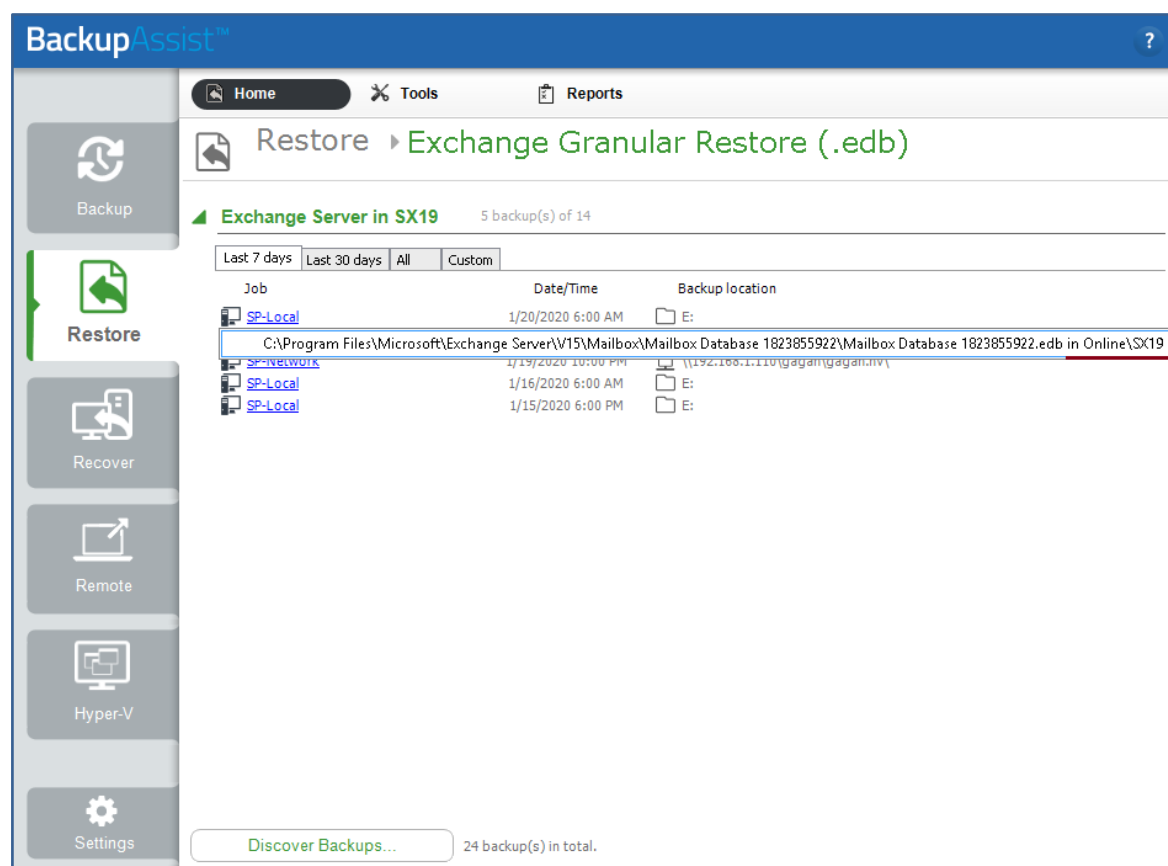
3. Locate the backup you want to restore from.

The **Exchange Granular Restore** screen shows the Exchange Servers backed up by this installation of BackupAssist.

The tabs above each volume's backup list can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.



4. Select the backup.

Click the **Backup** you want to restore from then **click** the **.edb file** that is listed under the backup.

Hyper-V Granular Restore

As shown in the screenshot above, at the end of the .edb file name is the name of the VM that was backed up.

When you select the file, Hyper-V Granular Restore will **work in the background to mount the VM** so that **Exchange Granular Restore** can open the .edb file.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

5. Locate the emails that you want to restore.

The Exchange Granular Restore console has a mail tree that you can **Browse** and **Search**. Both of these options will help locate, preview and select the emails that you want to restore.

Using Browse

Browsing for the emails you want to restore is **ideal** when you **know the email's location**.

To browse for the emails:

- Expand a mailbox and select one of its folders to show the individual emails inside it.
- Select an email to preview its contents in the pane below it.

The screenshot shows the Exchange Granular Restore console interface. On the left, a tree view shows the mailbox structure for 'Gagan', including folders like 'Calendar', 'Contacts', 'Deleted Items', 'Drafts', 'Files', 'Inbox', 'Journal', 'Notes', 'Outbox', 'Sent Items', 'Tasks', and 'Yammer Root'. The 'Inbox' folder is expanded, showing a list of emails. The selected email is 'FA-Network : Successful' with the subject 'FA-Network : Successful' and the body text 'FA-Network : Successful'. The preview pane shows the email details, including the start time 'Thursday, October 3, 2019 11:02:45 AM' and the backup type 'File Archiving'. The status is 'Successful'.

Using Search

Searching for emails is **ideal** when you **do not know an email's location**.

To perform a search:

- If you know what mailbox** to search, **tick the box** next to that mailbox and its name will appear in the Search field. If you select multiple mailboxes, they will be listed in the **Search in...** field. Any expanded mailboxes are also added to the search by default.

The search feature will search the entire database unless you select a specific mailbox.

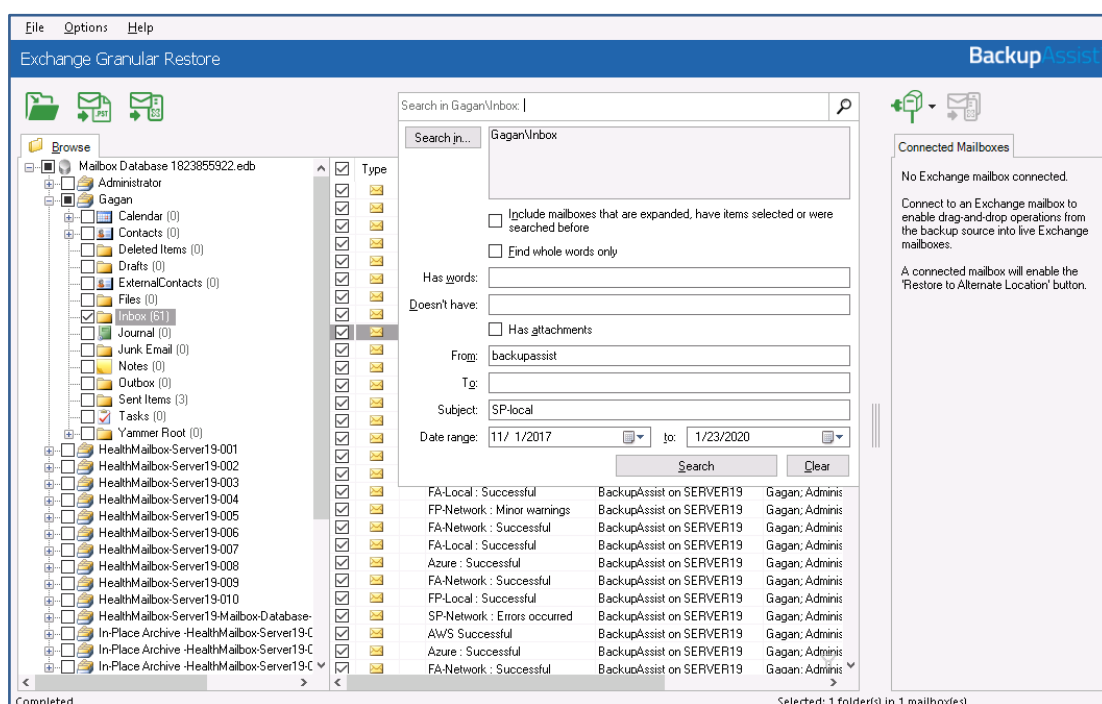
- b) Click the **Search field** to open the **Search dialog** and enter your search criteria.

The option **Include mailboxes that are expanded, have items selected or were searched before** is ticked by default. Deselect this if you only want to search ticked mailboxes.

The following criteria can be used to perform a search:

- **Find whole words only** - select if you only want to search for emails with complete versions of any search words used.
- **Has words** - searches all parts of an email (body, Subject, etc.) for the words in this field.
- **Doesn't have** - searches for emails that do not have the words entered in this field.
- **Has attachments** - will search for emails with attachments.
- **From** - will search for words entered in the From: field.
- **To** - will search for words entered in the To: field.
- **Subject** - will search for words entered in the Subject: field.
- **Date range** - will search for emails created, sent or received between the selected dates.

- c) Select the **search icon** to **start the search**.



A **new tab** will open with **matches** for your search.

If a search does not match any emails, review your search parameters and run another search.



If you want to **include emails** that are **no longer present** in user mailboxes, select the Options menu then click **display hidden deleted items** and **Display all items**. Deleted items from Exchange Server 2007 are stored in their original folders. Deleted items from Exchange 2010 and later are stored in the Deletions folder. These items can only be exported to a PST file.

6. Select the emails you want to restore.

Tick the box next to each email that you want to restore from the **Browse** pane.

If you performed a **search**, select each email listed in the search results. To restore **all items** listed **in the search** results, tick the Inbox. This will restore a copy of the mail account's inbox containing only the items listed in the search results.

7. Restore the selected emails.

There are three ways to restore emails: to their **original location**, to an **alternate location** and **Export to PST**. **Export to PST** file is a good option as it **restores the emails to a file** that can be **given to the user** who requested the restore. The user can then open the PST file in their Outlook mail client.

To restore the emails to a PST file:

- Select the **Export to PST** file button.

This button will become active when emails or mailboxes have been selected.

- Confirm the **Personal Storage Table (PST)** format.

You can choose Unicode or ANSI encoding for the PST output file.

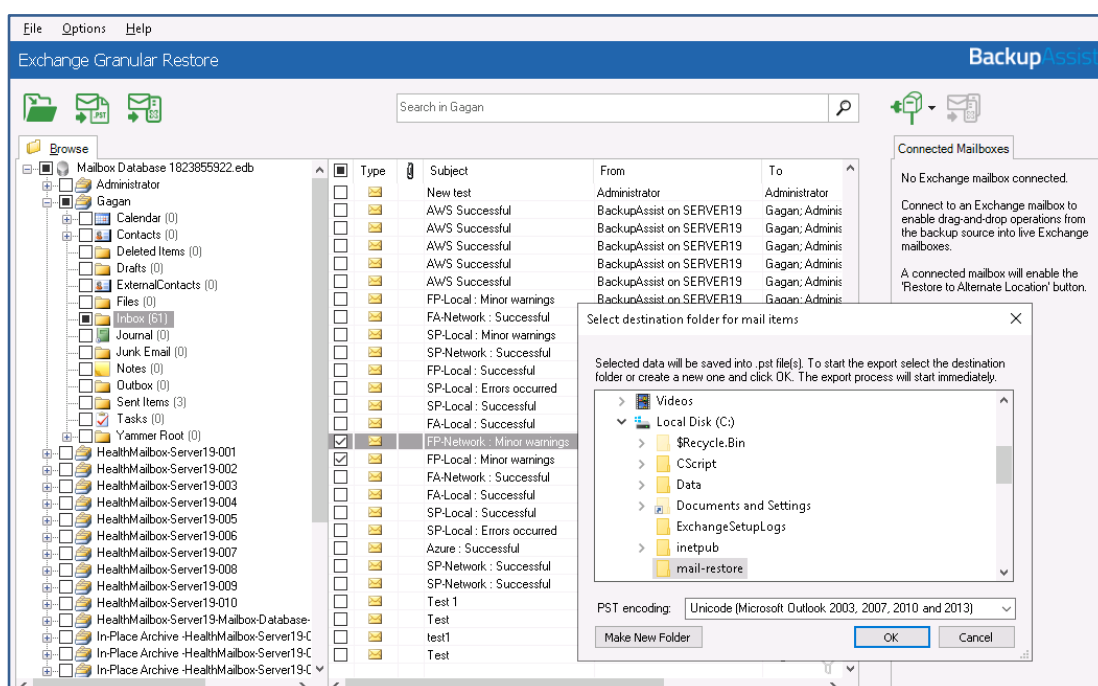
With large exports, there can be more than one PST file. Additional files are created automatically when the file size limit is reached. The limit depends on the output file encoding.

- For ANSI PST files, the size limit is 1 GB.
- For Unicode PST files, the size limit is 10 GB.
- A maximum of 15,000 messages can be restored into the PST file.

- Select the **destination**.

You will be asked to select a folder or create a new folder.

After selecting the new or existing folder, the export will begin.



A window will display the export's progress. The export can be canceled by clicking the **Stop Export** button.

The emails will be exported to a .pst file named: "Restore NNN <Mailbox Name>[VVV]. pst", where NNN is the current recovery session identifier and VVV is the volume number.

8. Open the PST file and access the emails.

The user who requested the restore can be given a copy of the PST file to open and access the emails. The user should follow these instructions.

To open a PST using an Outlook Client:

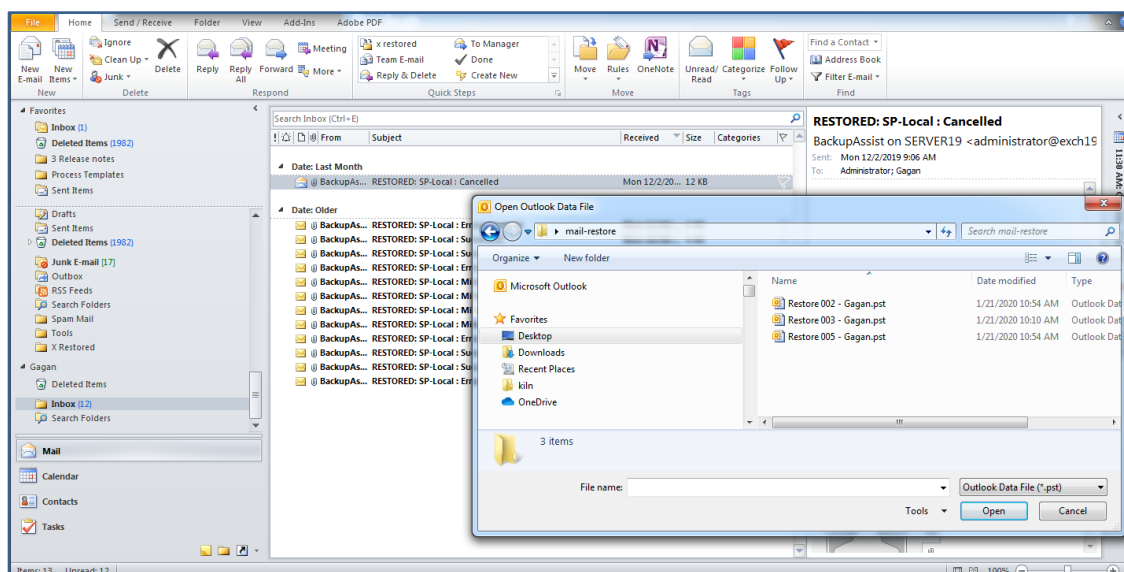
- d) Click **File > Open** and choose **Open Outlook Data File**.
- e) **Browse** to the **PST file** that was exported.
- f) **Select** the **PST file** and click **OK**.

The **PST file** will appear **in Outlook** as a container.

RESTORED will appear in the Subject line of each email restored. This is enabled by default and can be turned off by selecting **Options > Add 'RESTORED'** to exported item > No.

In the **screenshot below**, a PST has been restored and the contents of the PST appear with RESTORED next to each email.

Another PST is about to be selected and added to the Outlook client.



You can now:

- View and access the emails in Outlook.
- Drag-and-drop the emails from the PST to another folder in Outlook. These emails will be automatically synchronized with the live Exchange Server database.

Congratulations – your emails have been restored.

SQL Server restore and recovery

This section covers two common SQL recovery scenarios. The **first scenario** explains how to recover a **Full SQL Server** using the Integrated Restore Console. The **second scenario** explains how to restore an SQL **database to a specific point in time** using the SQL Restore Tool.

15 Full SQL Server recovery from a drive image or application backup

This scenario explains how to **recover an SQL Server** using a **System Protection backup** of either the full Windows Server or the SQL Server application.

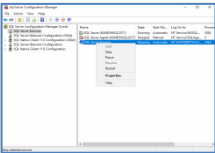

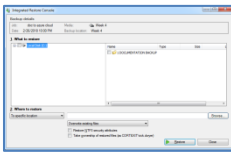


In a nutshell: In this scenario, you will stop an SQL Server, then use the Restore tab's SQL Server option to restore a copy of that SQL Server. After the restore, you will start the restored version of the SQL Server, which will resume its operations.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Recovery requirements

To perform an SQL Server recovery, you will need BackupAssist and:

SQL Configuration Manager	A backup	Integrated Restore Console
 <p>The SQL Server Configuration Manager is used to stop and start the SQL services for the restore.</p>	 <p>You will need a System Protection, File Protection, File Archiving or Cloud Backup of the SQL Server.</p>	 <p>BackupAssist will use the Integrated Restore Console to restore the SQL Server's files.</p>

Recovery checklist

Use this checklist to make sure you are ready to perform the recovery:

<input type="checkbox"/>	If you are recovering a production SQL Server, you should perform the recovery at a time that has minimal impact on SQL users and communicate the expected downtime.
<input type="checkbox"/>	Check that you have the passwords for any encrypted backups. BackupAssist Technical Support cannot retrieve a password if it is lost or forgotten.

Restore process

To restore an SQL Server, follow these steps:

1. Open the SQL Server Configuration Manager.

SQL Server Configuration Manager is an MMC Snap-On that can be **selected** from the **Start** menu.

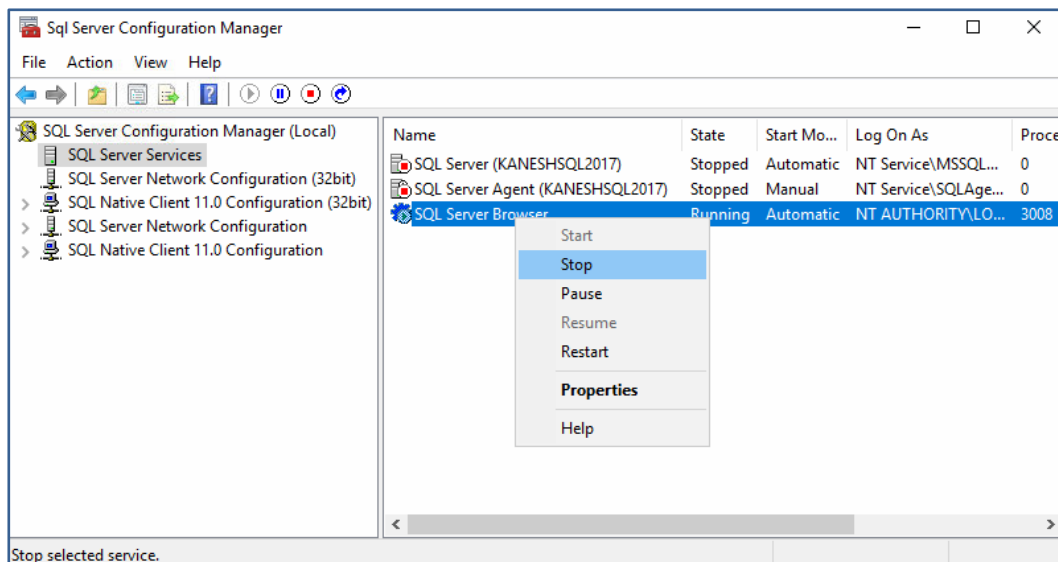
2. Select SQL Server Services.

SQL Server Services appears in the **Configuration Manager's left pane**.

3. Stop any running services.

Before you can restore an SQL Server from a backup, you first need to stop the SQL Server Services. The services are listed in the right pane.

To stop a service, **right-click the service name** and select **Stop**.

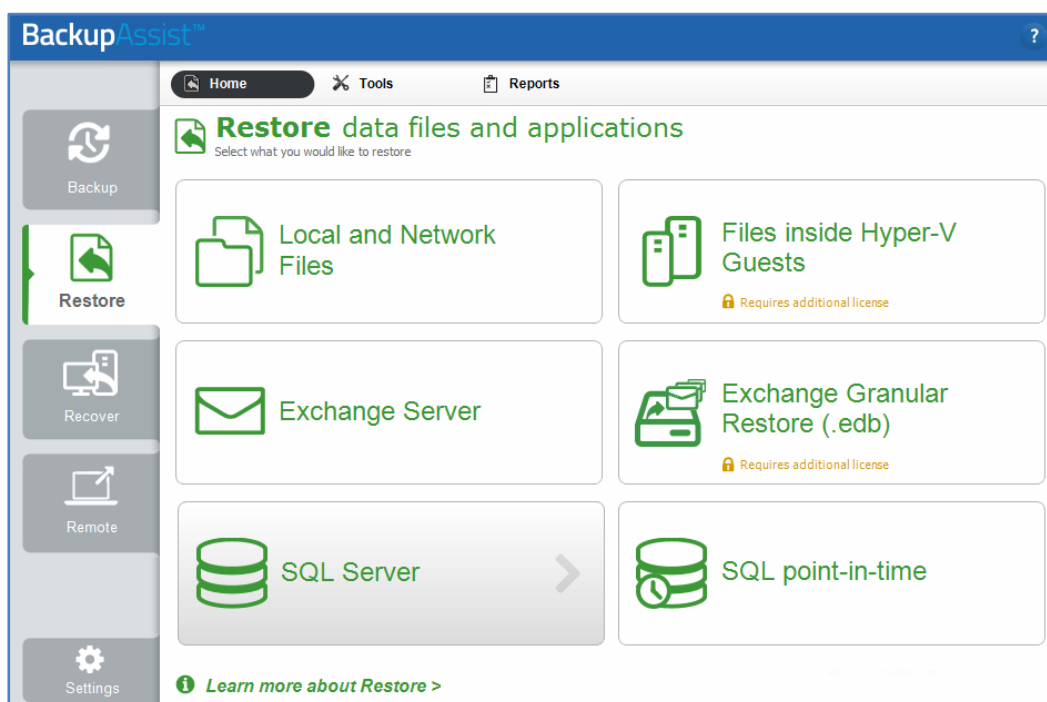


4. Open BackupAssist.

5. Select the Restore tab.

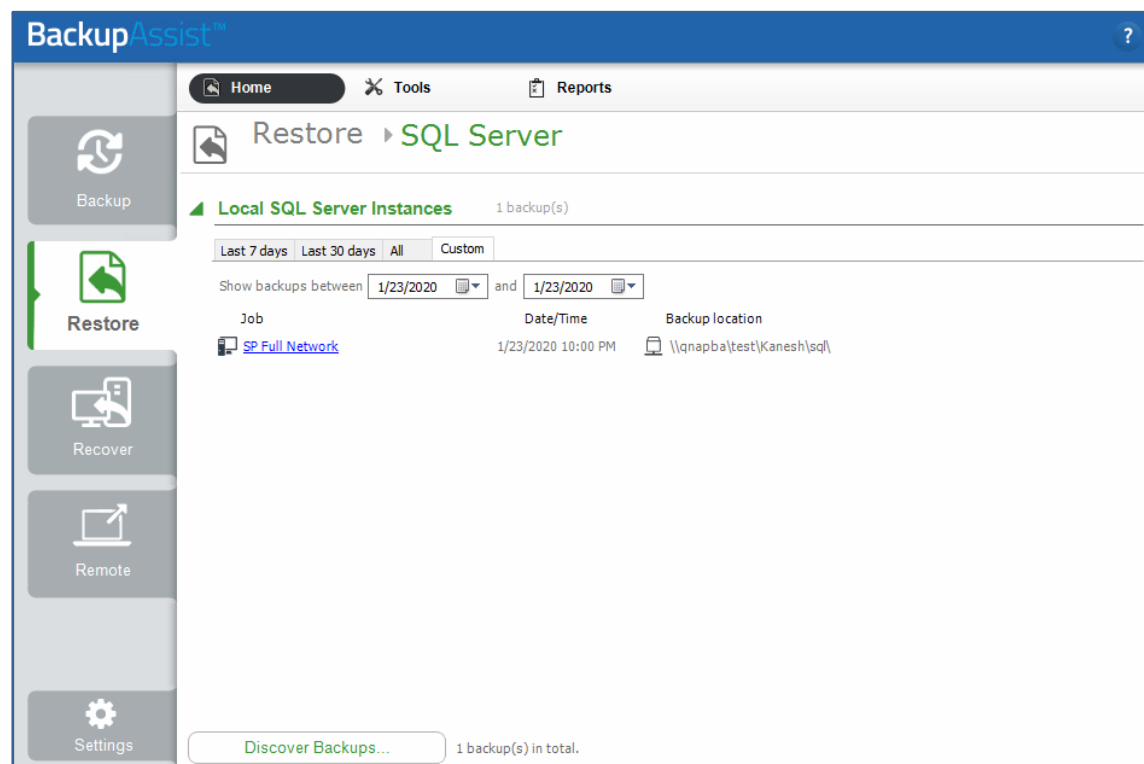
6. Select SQL Server.

This step starts the guided restore process and opens the **SQL Server** restore screen.



7. Select the backup

The SQL Server screen displays the SQL Server backups created by this installation of BackupAssist. Click the backup you want to restore from, and the **Integrated Restore Console (IRC)** will open that backup.



The tabs above each volume's backup list can be used to filter the backups shown. If there are many backups, the filters can help locate the backup you need.

The tabs available are:

- **Last 7 days** and **Last 30 days** - shows the backups within those ranges.
- **All** - shows all backups available.
- **Custom** - allows you to select a specific date range and display backups for that period.



For encrypted backups

If the backup is encrypted, you will be prompted to enter the encryption password. This is the password entered in the **Set up destination** step when the job was created.

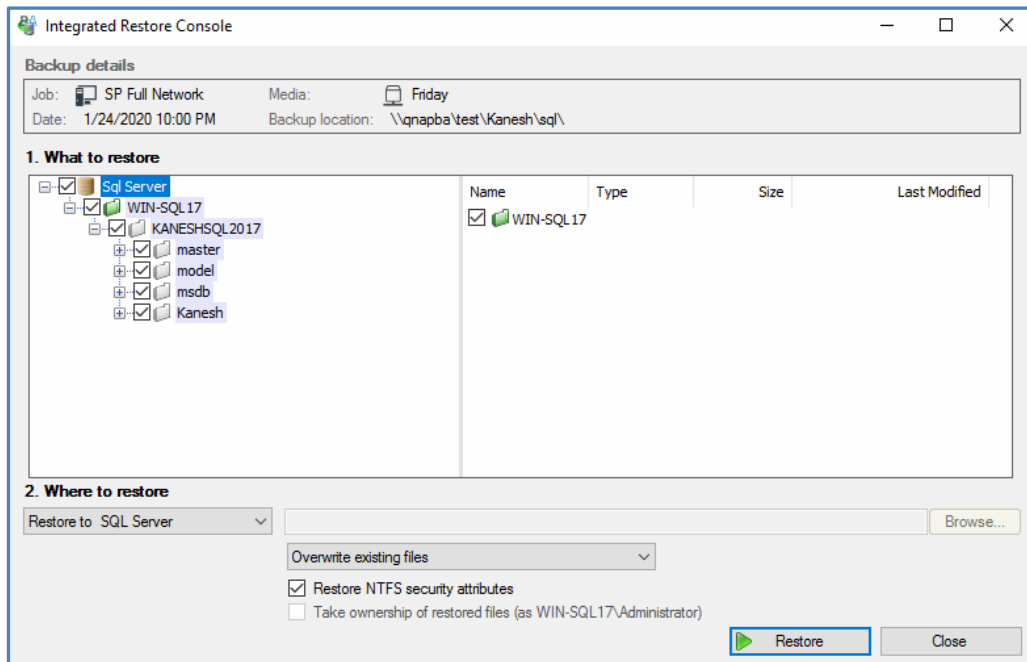
Considerations:

- If you used BitLocker, the password is required. A BitLocker key can only unlock a drive to create a backup.
- BackupAssist Technical Support cannot retrieve the password if it is lost or forgotten.

8. Select the SQL Server

The Integrated Restore Console will detect and display the SQL Server files in the backup. Even if the backup is of a full volume, only the SQL Server and the files needed to restore it are shown.

Tick the box next to the **SQL Server object**. This is the top tick box with the database icon.



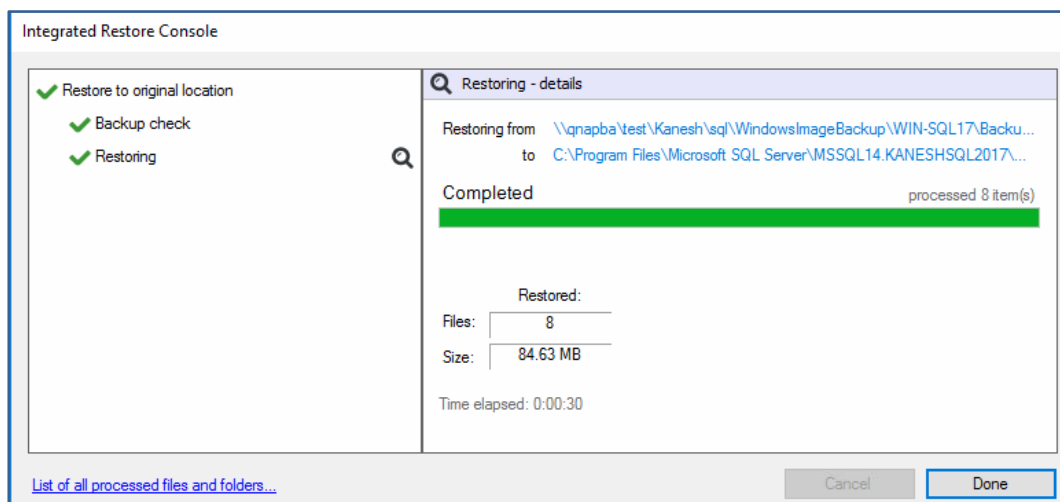
9. Review the restore destination and settings.

To review the destination and restore options:

- Check that **Where to restore** has **Restore to SQL Server** selected.
- Check that **Overwrite existing files** is selected. The restored files will overwrite files in the restore destination.
- The **Restore NTFS security attributes** option should be left ticked so that the security attributes the files had when they were backed up will be retained when the files are restored. The NTFS security attributes can be viewed in the **Security** tab on the file's **Properties**.
- The **Take ownership of restored files** option will not be selectable.

10. Start the restore.

When you select the **Restore** button, the restore **process will begin**. The Integrated Restore Console will display information about the restore job and provide status updates as the job runs.



List all processed files and folders.

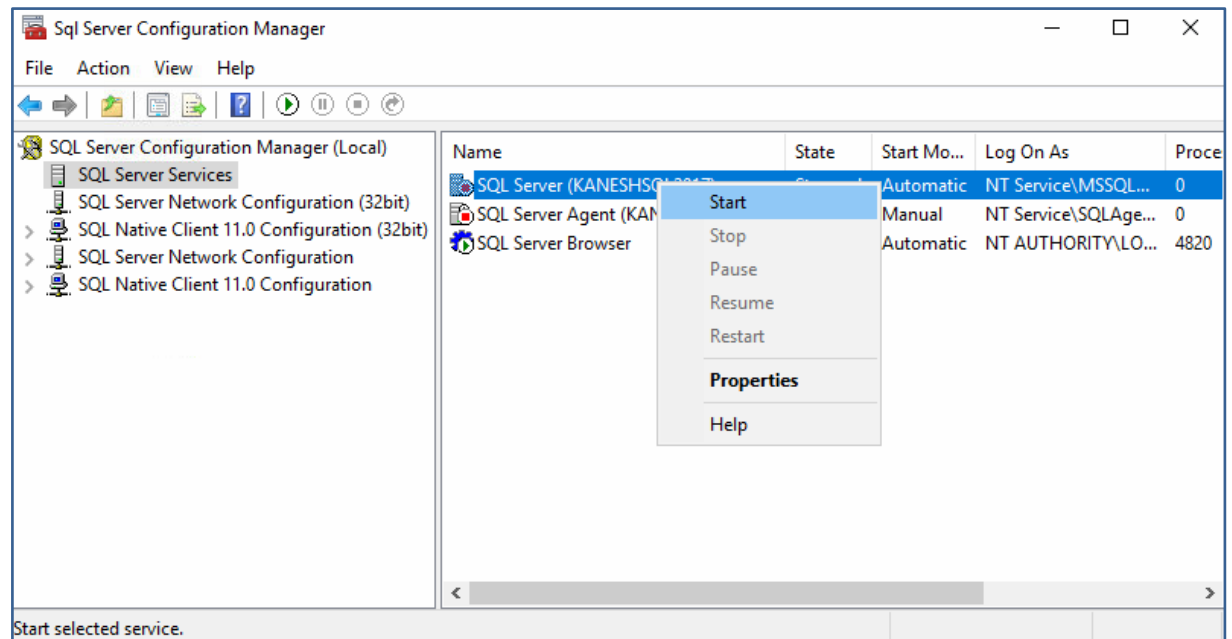
Selecting this link on the progress window will open notepad and display a list of the files restored, including their full path.

11. Select Done then Close.

Once the restore has finished, selecting **Done** then **Close** will return you to the BackupAssist UI.

12. Open the SQL Server Configuration Manager.

13. Select SQL Server Services.



14. Start the services for the SQL Server.

To start a service, **right-click the service name** and select **Start**.

Once the SQL Server is running, you can use **Microsoft SQL Management Studio** to review the tables and objects in the restored SQL Server.

Congratulations – your SQL Server has been recovered.

16 Point-in-time recovery of SQL databases

This scenario uses the **Restore tab's SQL point-in-time** option to restore an SQL database to a point just before it was corrupted. The instructions for this scenario use an SQL Protection backup to restore a user database.

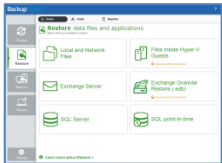

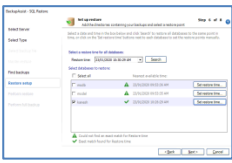


In a nutshell: In this scenario, you will use BackupAssist's **SQL Restore tool** to choose an **SQL Server**, then the **database** that is to be restored. You then select **the time** to restore the database to and restore it.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform an SQL database restore, you will need:

BackupAssist	SQL Protection backup	SQL Restore Tool
 <p>BackupAssist will be used to select SQL point-in-time and launch the SQL Restore tool.</p>	 <p>You will need an SQL Protection backup created using the Transactional scheme. This requires the SQL Continuous add-on.</p>	 <p>The SQL Restore tool restores databases from SQL Protection backups. This requires the SQL Continuous add-on.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the database restore:

<input type="checkbox"/>	<p>Know the point in time that you want to restore the database to. For example, if the database was corrupted, you can choose a point just before the corruption occurred.</p>
--------------------------	---

Restore process

To restore an SQL database, follow these steps:

1. **Select BackupAssist's Restore tab.**

2. **Select SQL point-in-time.**

This will open the **SQL Restore tool** and start the **guided restore process**.

3. **SQL Server Restore.**

This is the first step using the SQL Restore tool, and used to **locate the SQL Server** with the database you want to restore. You can **select a local or remote SQL Server**.

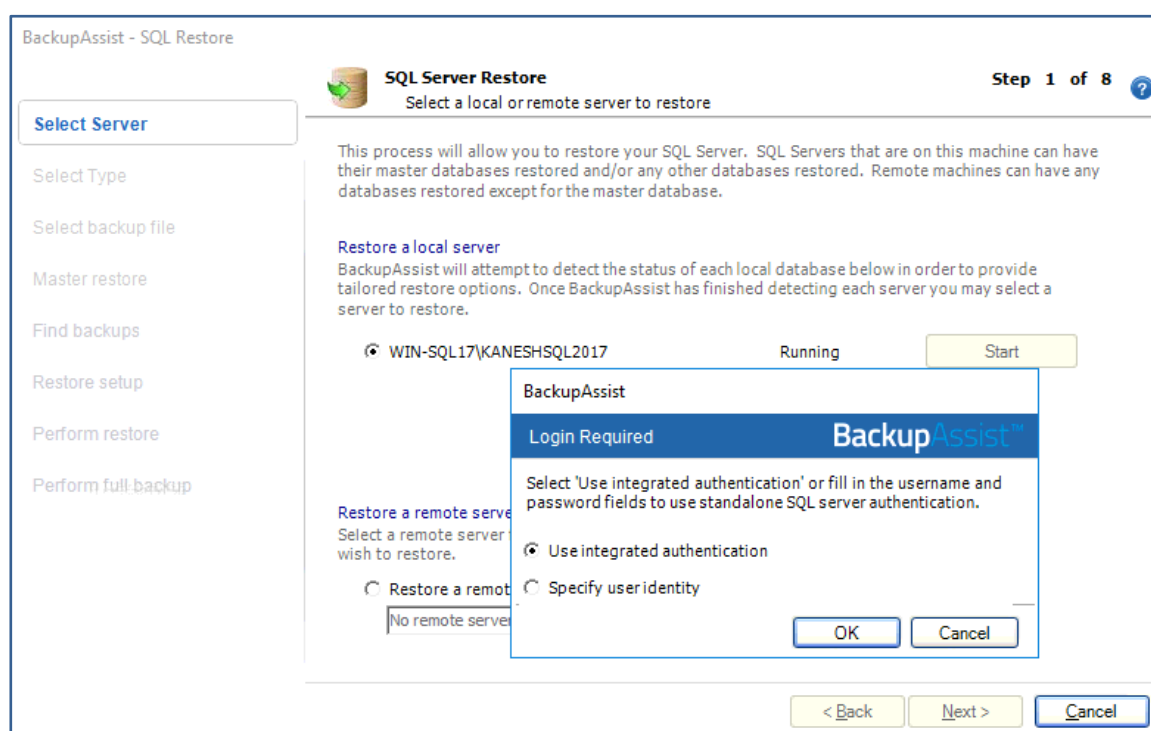
The **Restore a local Server** section lists the SQL servers on your local machine. If an SQL Server is present but not running, you can click **Start**. You can only restore to SQL servers that are running.

If you choose **Restore a remote server**, any remote SQL servers detected will appear in the drop-down list for selection. If a server is not shown, type its name or IP address into the drop-down field and click **Refresh**.

Select the server to restore to and click **Next**.

4. Server authentication.

When you select **Next** in the **SQL Server Restore** step, you will be prompted to provide **credentials** with access to the **selected SQL Server**.



There are two authentication options to choose from:

- **Use integrated authentication** will authenticate with the Backup user identity.
- **Specify user identity** will prompt you to enter credentials for another user account or an SQL Server user account.



The **authentication account** and the SQL Server's **service account** will both **need access to the backup** used for the restore.

Some SQL servers are configured to accept only SQL authentication.

Provide the appropriate logon credentials and click **Next**.

5. Select restore type.

This step determines the **type of database** that will be restored. **Master database recovery** will restore the system databases that the SQL Server uses to operate. **Selected databases** will restore user/business databases.

Tick **Selected databases** and click **Next**.



Master database recovery is for SQL recovery scenarios. Only select **Master database recovery** if your SQL database is damaged, missing or needs to be recreated. It is advised that you restore the master database before any other databases.

To restore the master database you need to have BackupAssist installed on the server itself.

6. Select your backup directory.

This step is used to **add or confirm** the location of your **SQL database backups**. If a backup is not listed, use the **Browse** field to type in the path of the backup or browse to it, then **click Add**.

You can locate and add multiple backups. All of these backups will be used to provide restore points.

Confirm that the backups you need are listed and click **Next**.

BackupAssist - SQL Restore

Select your backup directory Step 5 of 8

Add directories containing your database backups below.

Enter or browse to any directories containing backups for the SQL database you wish to restore. That server will then become available in the 'Select a server to restore:' box below.

Add directories containing backups:

C:\ProgramData\BackupAssist v 10\temp\sql\

Backups for server WIN-SQL17\KANESHSQL2017 have been found.

Click 'Next' to pick the restore times for the databases within the selected server.

< Back Next > Cancel

7. Set up restore.

This step is used to select the database and the point in time that it is to be restored to.

To set up the restore:

- Tick the **database** that you want to restore.
- Click the **Set restore time** button next to the database.

A dialog will display a calendar and the time range the database can be restored to on the day selected in the calendar. Selecting a different day will display the time ranges the database can be restored to from that day.

The **Select a time from within that range** field is used to select a specific point within the chosen range, to restore the database from.

- c) Use the calendar to select the **date** to recover the database from.
- d) Choose a **time range** from the list shown.
- e) Enter a point in time using the **Select a time from within that range** field.
- f) Click **OK**.
- g) Click **Next**.

The screenshot shows the BackupAssist - SQL Restore dialog. The main window is in the 'Set up restore' step. The 'Restore time' field is set to 23/01/2020 10:30:29 AM. The 'Select databases to restore' section shows 'kanesh' selected. A 'Select restore point' dialog is overlaid, showing a calendar for January 2020 with the 23rd selected, and a list of time ranges for the 'kanesh' database. The 'Select a time from within that range' field is set to 10:26:29 AM.



The **Restore time field** is used when you want to restore all of the databases. When you click **Search**, the backups closest to the selected time will appear next to each database and show the time that the backup was made. If the restore time specified is not available, a warning icon will appear by the database, and the closest available time will be displayed.

8. Restore selected databases.

Review the restore job settings and then select **Start restore** to restore the database.

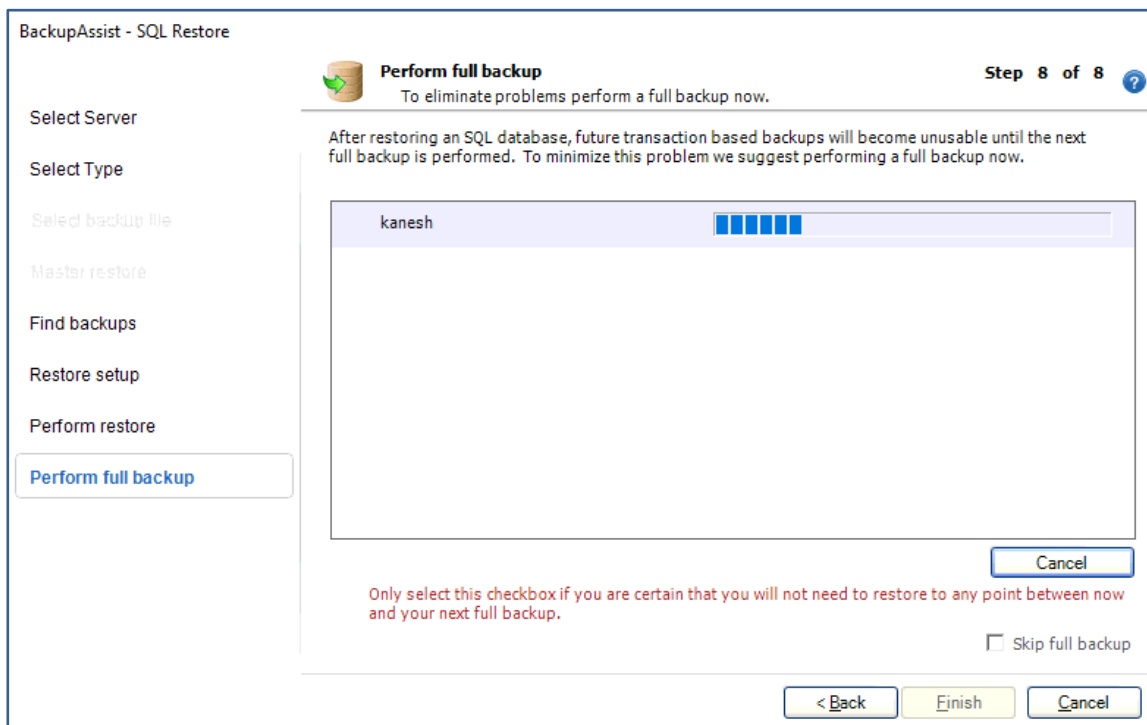
Click **Next** once the restore process has completed.

Congratulations – your database has been recovered.

9. Perform full backup.

After restoring an SQL database, future transaction log backups cannot be used to restore a database to a specific point in time until a full backup has run. It is recommended that you now run a full backup of the database that was restored.

Click **Start full backup**.



The backup will be stored in the same folder as the backup files you just restored from.

If your backup schedule includes a full back up as the next SQL backup, and you are certain you will not need to restore this database to a specific point in time between the restoration and the next full back up, you can check **Skip** the full backup and click **Finish**.

Restore without using BackupAssist

One of BackupAssist's strengths is its use of open formats for backups. This means that **if a server no longer uses BackupAssist, you can still restore** from a System Protection, File Protection or File Archiving backup. In this section, we look at how to restore from these backups without BackupAssist.

17 Restore from a drive image backup using WinRE

This scenario uses Windows Server Backup's Recovery Tool (**WinRE**) to **recover** files from a **System Protection** image backup.

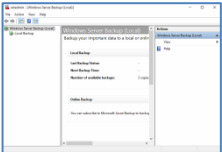



In a nutshell: If you haven't used WinRE, don't worry. It is a straightforward recovery tool that can detect and open System Protection backups. Then all you do is select the files to restore and where to restore them to.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform a WinRE restore, you will need:

Windows Server Backup	A System Protection backup
 <p>Windows Server Backup is included with Windows Server and launches the Recovery Tool (WinRE).</p>	 <p>A local System Protection backup. System Protection backups use .vhdx files, which are compatible with WinRE.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	Check that the backup location can be accessed by the Windows Server performing the recovery.
<input type="checkbox"/>	If the backup is in a Data Container , you will need to manually mount the Data Container so that Windows can access it and detect the backups.

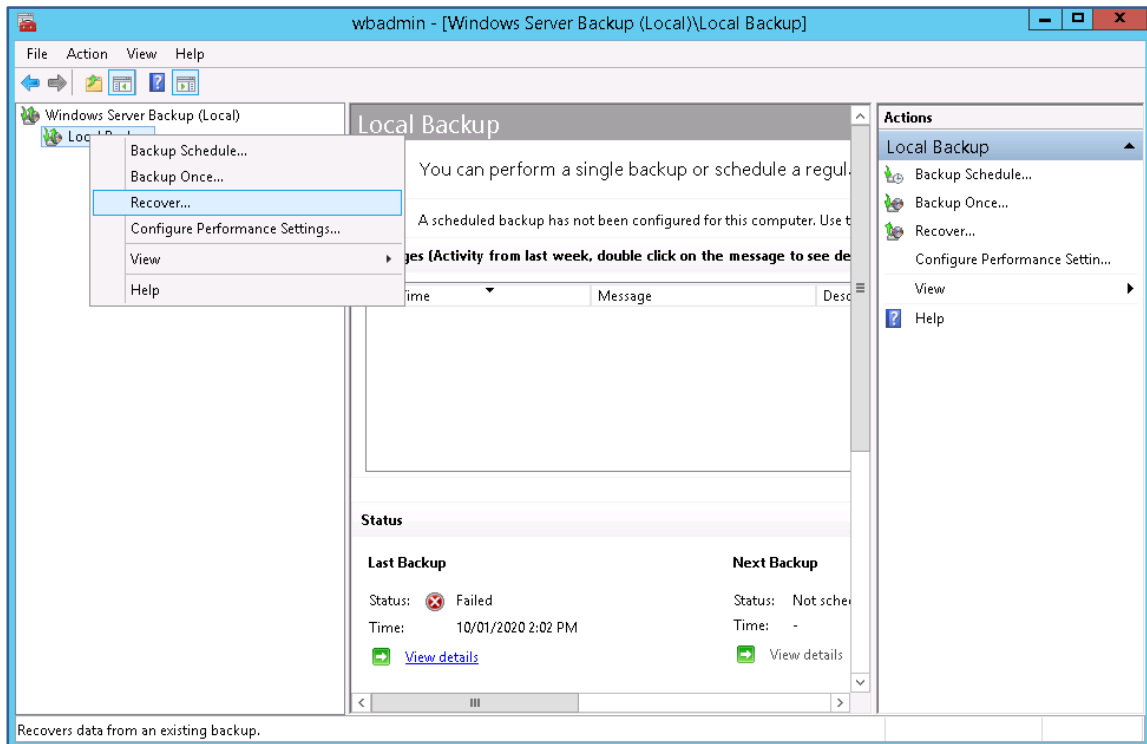
Restore process

To restore files, using WinRE, follow these steps:

1. **Type backup** into the **Search** field on the Windows desktop and **select Windows Server Backup**.
This will open Windows Server backup.

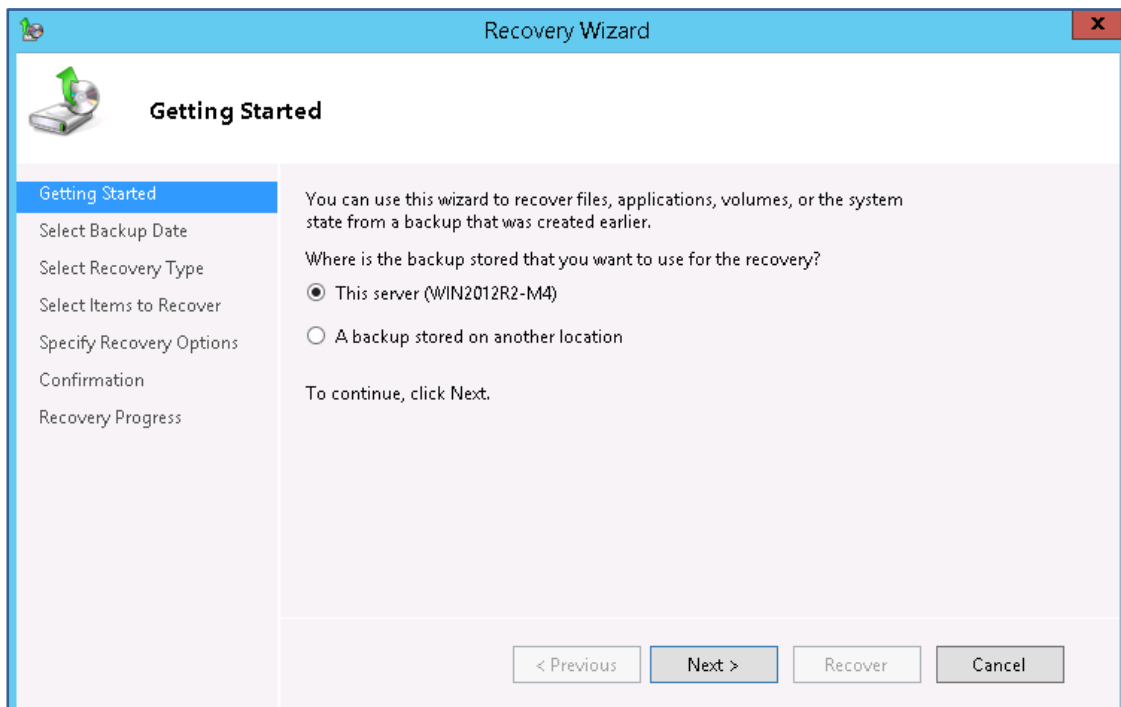
2. Right-click **Local Backup** and select **Recover...**

This will open the Windows Backup Recovery Wizard (WinRE).



3. Select the **backup**.

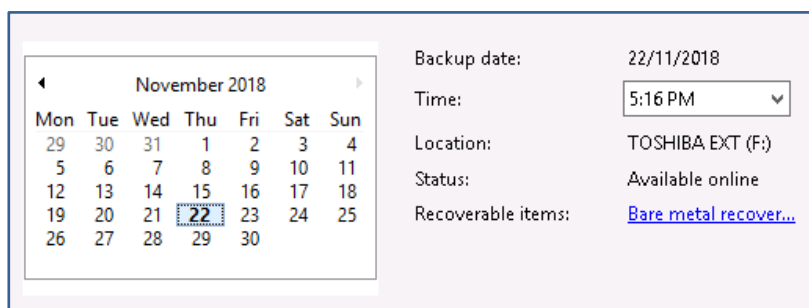
When WinRE starts, it scans the server for backups and displays them on the **Getting Started** screen. In this screenshot, it has detected a **System Protection backup** on a **local drive**.



Selecting **A backup stored on another location** allows you to select a local drive or provide the UNC for a remote shared folder. WinRE will scan the location provided for compatible backups.

4. Select Backup Date.

Use the **Calendar** to select a **backup date**. The **Time field** can be used to select different times if more than one recovery point is available for that day.



Backup date: 22/11/2018

Time: 5:16 PM

Location: TOSHIBA EXT (F:)

Status: Available online

Recoverable items: [Bare metal recover...](#)

5. Select Recovery Type.

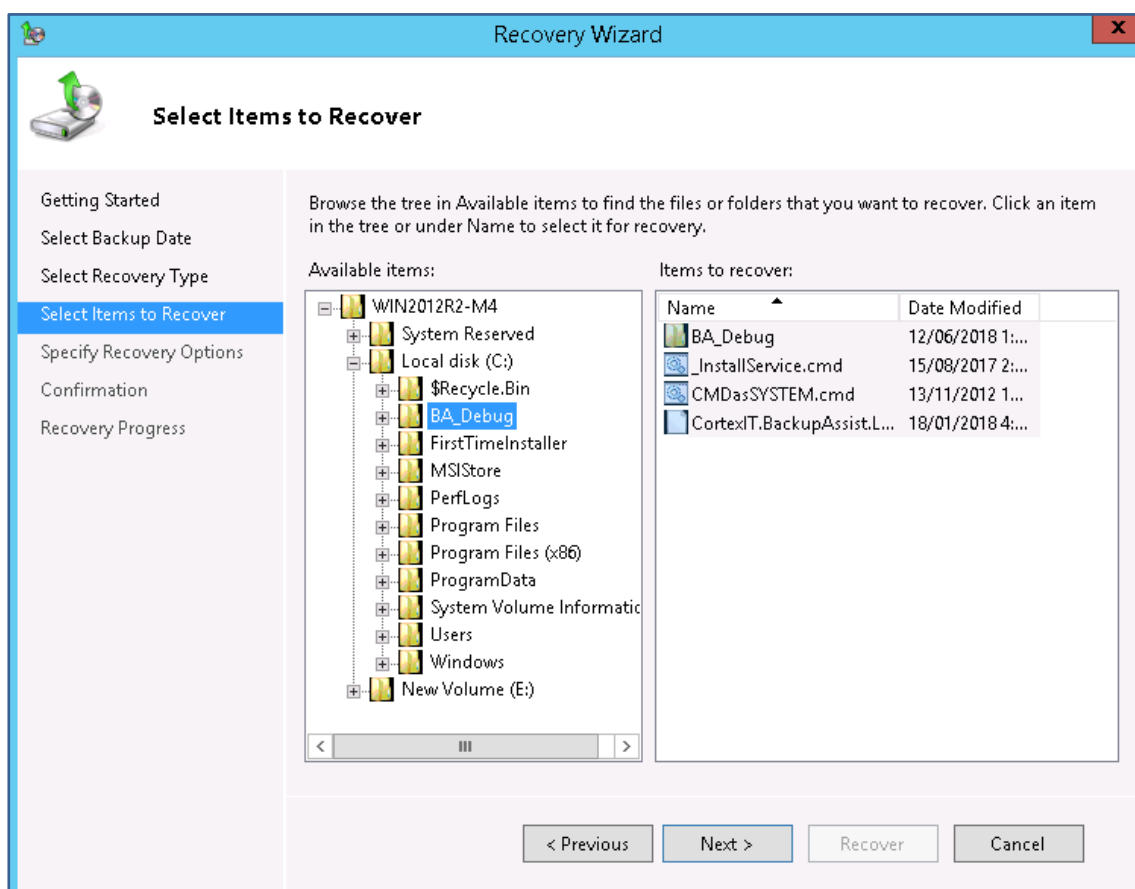
This step presents five recovery options: Files and Folders, Hyper-V, Volumes, Applications and System State. Each option includes descriptions of what it is used to restore.

In this scenario, **Files and folders** has been selected.

6. Select items to recover.

The options available in this step will depend on the Recovery Type.

In this screenshot, BackupAssist's **Debug folder** has been **selected**.



Recovery Wizard

Select Items to Recover

Getting Started

Select Backup Date

Select Recovery Type

Select Items to Recover

Specify Recovery Options

Confirmation

Recovery Progress

Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.

Available items:

- WIN2012R2-M4
 - System Reserved
 - Local disk (C:)
 - \$Recycle.Bin
 - BA_Debug
 - FirstTimeInstaller
 - MSIStore
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - System Volume Informati...
 - Users
 - Windows
 - New Volume (E:)

Items to recover:

Name	Date Modified
BA_Debug	12/06/2018 1:...
_InstallService.cmd	15/08/2017 2:...
CMDasSYSTEM.cmd	13/11/2012 1:...
CortexIT.BackupAssist.L...	18/01/2018 4:...

< Previous Next > Recover Cancel

7. Specify Recovery Options.

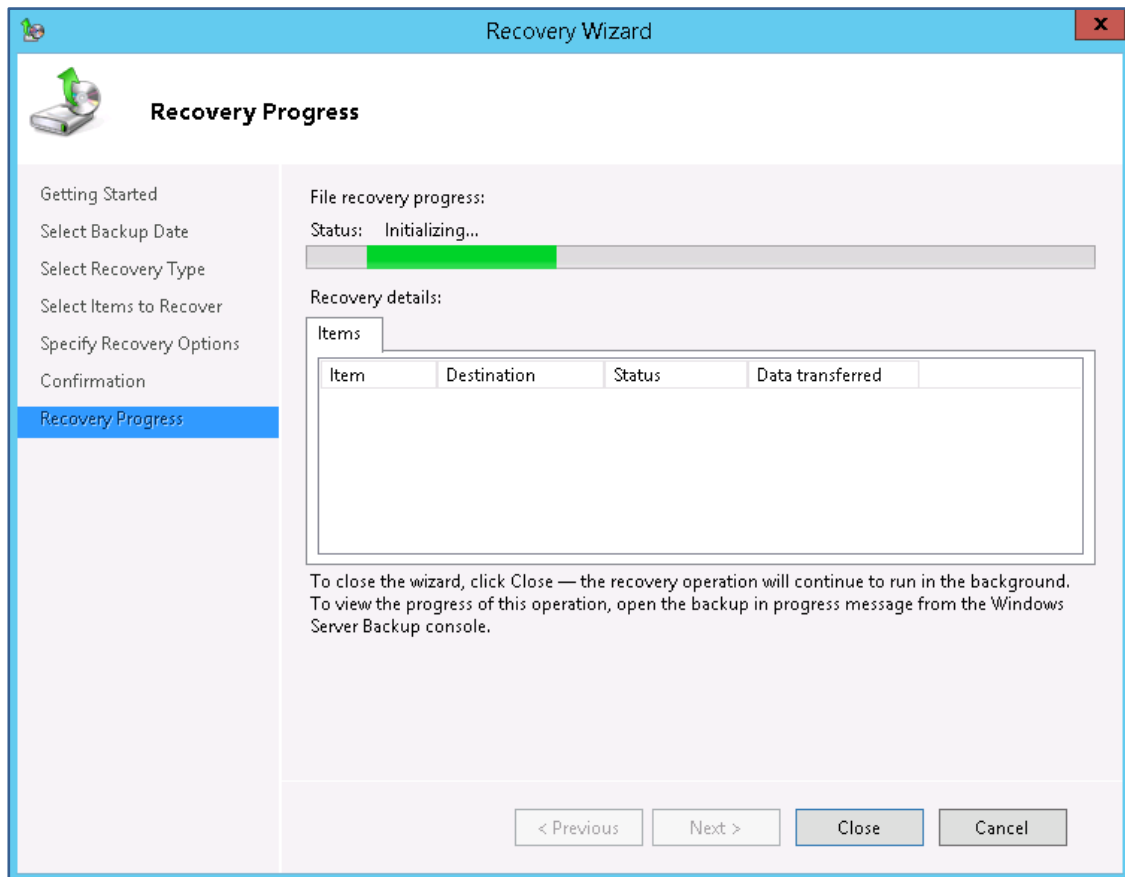
Choose where you want to recover your selections to.

In this scenario, **Another location** was selected and the location of a folder on the server's E: Drive entered.

8. Confirmation

Review the information you have provided.

When you are ready to recover the data, select **Recover**.



When the recovery has finished, it will list the items recovered.

Congratulations – your files have been recovered.

18 Restore from file replication backup

A BackupAssist **File Protection job replicates data** to a backup destination. This scenario restores files from a File Protection backup using Windows Explorer's copy function.

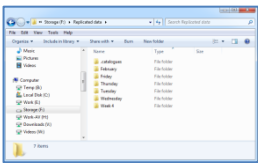



In a nutshell: In this scenario, you will use Windows to locate a File Protection backup that you want to restore from, select the files you want to restore, then copy and paste those files to another location.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform a file restore, you will need:

Windows Explorer	A File Protection backup
 <p>Windows Explorer will be used to locate the backup and to copy and paste the files that are needed.</p>	 <p>A File Protection backup in a location that can be accessed by the computer performing the restore.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	Check that the backup destination can be accessed by the server performing the restore.
<input type="checkbox"/>	If the backup destination is encrypted with BitLocker, you will first need to use BitLocker to unlock it.

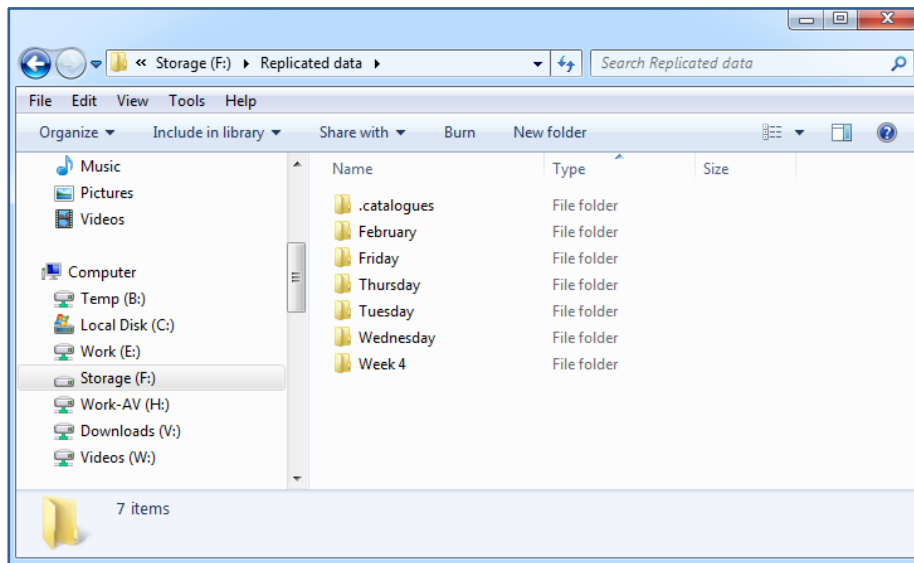
Restore Process

To restore files using Windows Explorer, follow these steps:

1. Use **Windows Explorer** to **Browse** to the **backup destination**.

The backup destination will show a set of folders that are used to store the backups. The folders will reflect the backup schedule used by the job that created the backups.

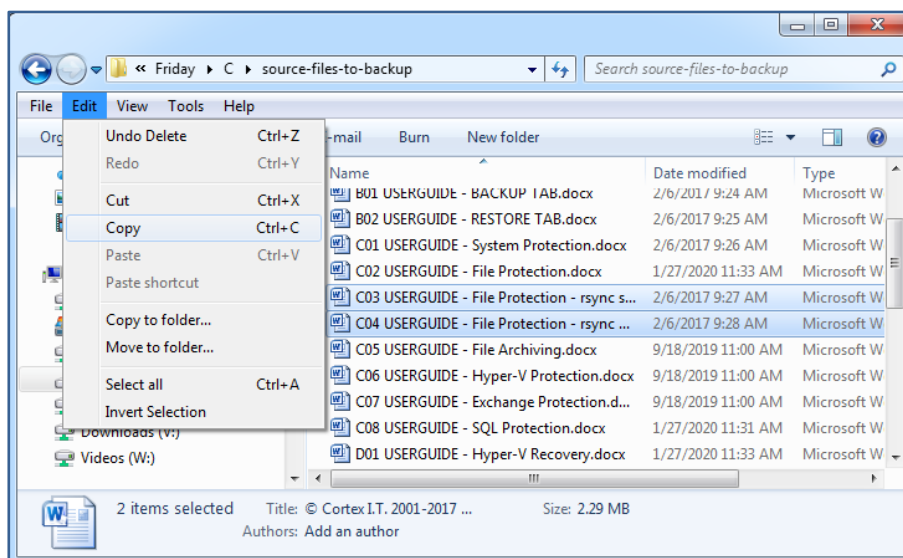
2. **Open the folder containing the backup.**



3. **Select the files** that you want to restore.

Hold down the Ctrl key to select multiple files.

4. **Select Edit** then **Copy** from the top menu.



5. **Browse** to the **location** you want to **restore** the files to.

6. Select **Edit** then **Paste** from the top menu.

Congratulations – your files have been restored.

19 Restore from ZIP archiving backup

BackupAssist File Archiving compresses data into a ZIP file as it is backed up. This scenario explains how to **restore files** from a **File Archiving backup** using **third-party** file archiving **software**.



In a nutshell: In this scenario, you will open a File Archiving backup's ZIP file using Windows or WinRAR archiving software, then identify the files you want and restore them to another location.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.



Restore requirements

The easiest way to open a ZIP file and view its contents is to open the file with Windows Explorer. However, many companies use third-party archiving software for additional functionality including ZIP encryption/decryption support. 7-ZIP and WinRAR and examples of popular archiving software.

This scenario explains how to restore from a ZIP file using:

- **WinRAR** – for users who have backups created using ZIP encryption. We will use WinRAR, as it can be used for free and is a good example of how most file archiving software works.
- **Windows Explorer** – for users who do not have archiving software and whose backups do not use ZIP encryption.

To perform a restore from a ZIP file, you will need:

Archiving software or Windows	A File Archiving backup
 <p>Third-party archiving software will be required if the backup was created using the ZIP encryption option.</p>	 <p>File Archiving backups use the .zip compression format, which is compatible with most file archiving software.</p>

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	If you want to use third-party archiving software, it needs to be installed on the server before you start. WinRAR can be downloaded and installed as a free trial version from https://www.rarlab.com/ .
<input type="checkbox"/>	If the backup destination is encrypted with BitLocker, you will first need to use BitLocker to unlock it. BitLocker protected File Archiving backups do not use ZIP encryption.

Restore process – using WinRAR

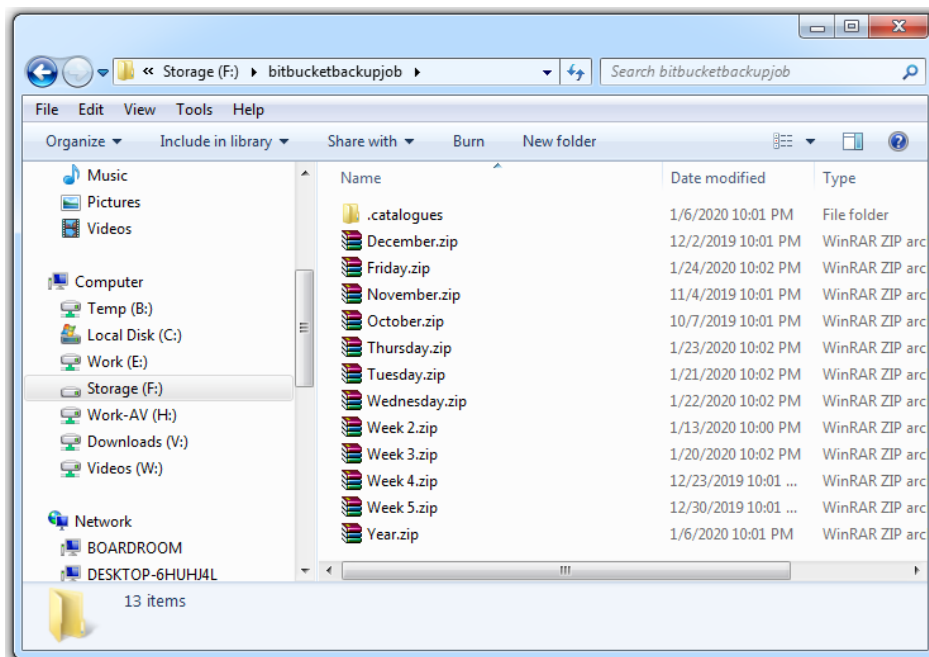
To restore files from a ZIP backup using WinRAR:

1. Use Windows Explorer to **Browse** to the **backup destination**.

The backup destination will contain a set of .zip backup files. The file names will reflect the backup schedule used by the job that created the backups.

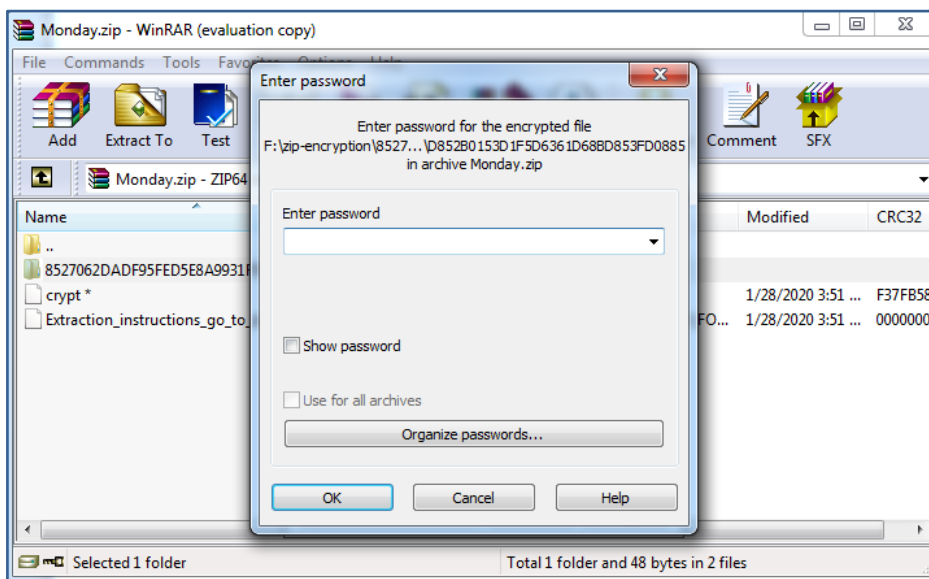
2. **Identify the backup** containing the files you want to restore.

The Date Modified column shows when the backup was created.



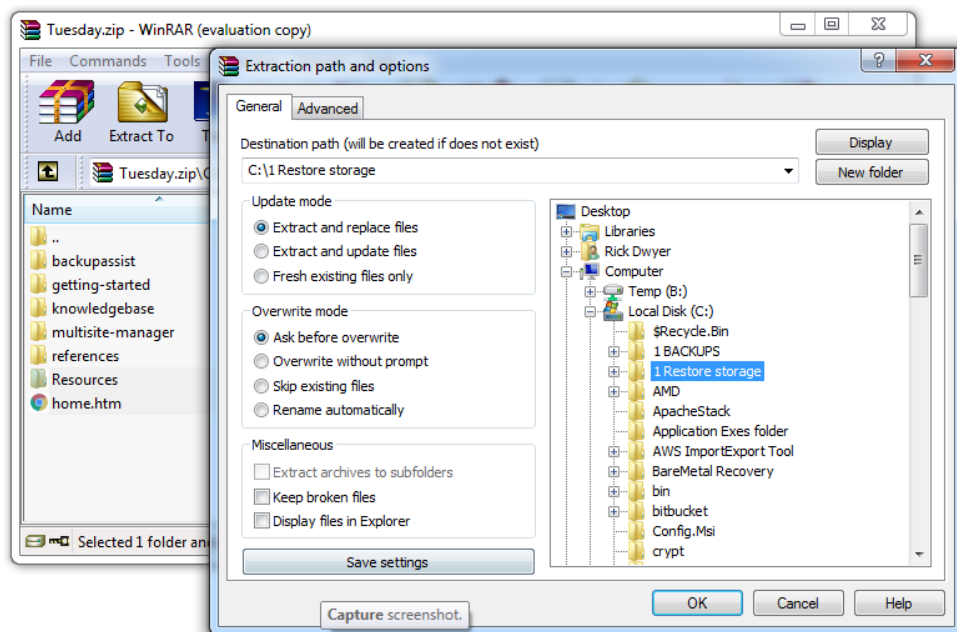
3. **Double-click the backup.**

WinRAR will open the backup. If the backup is encrypted, you will be prompted to enter the encryption password.

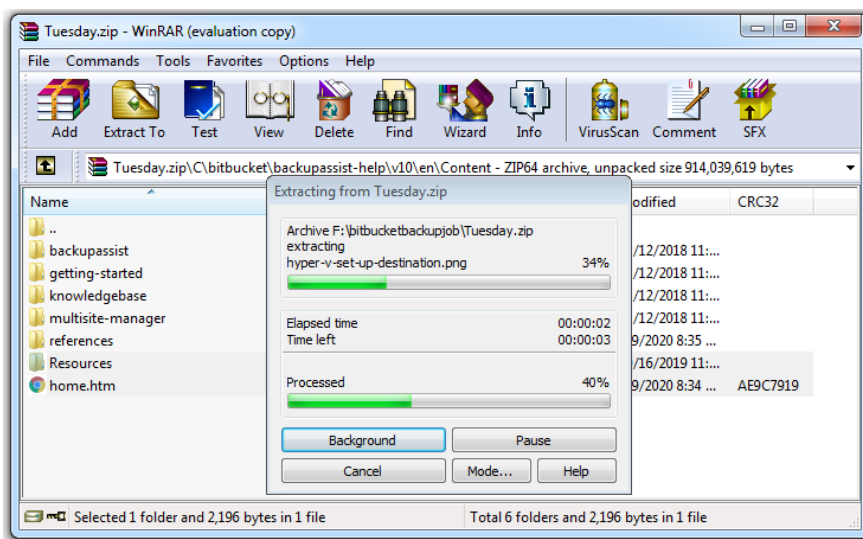


4. Select **Extract to**.

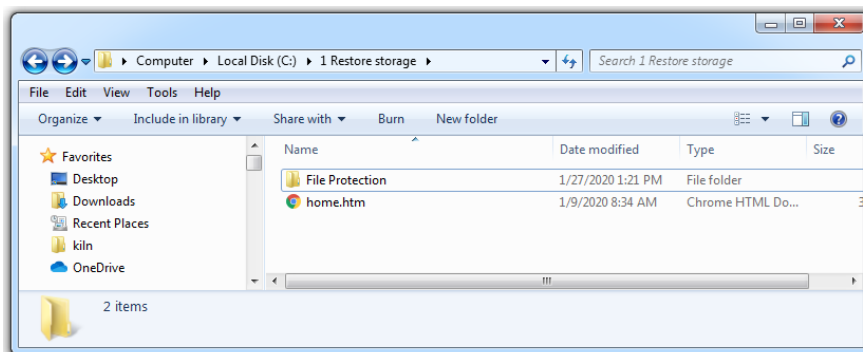
5. Select a **destination to restore (extract) the files to**.



6. Select **OK** and WinRAR will start extracting the files.



7. Once the files have been **extracted**, you can access them from the **restore location**.



Congratulations – your files have been restored.

Restore process – using Windows Explorer

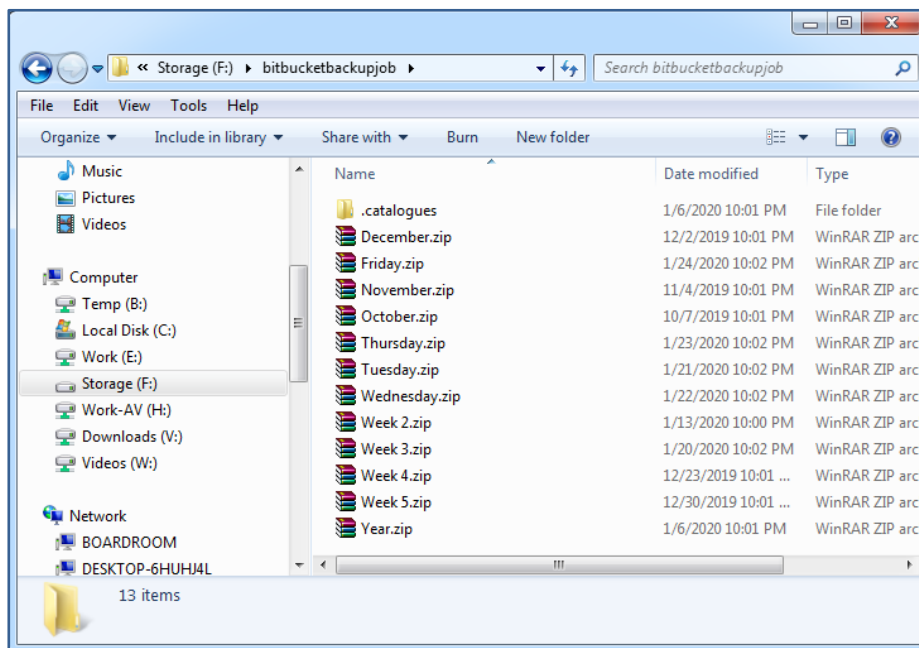
To restore files from a ZIP backup using Window Explorer:

1. Use Windows Explorer to **Browse** to the **backup destination**.

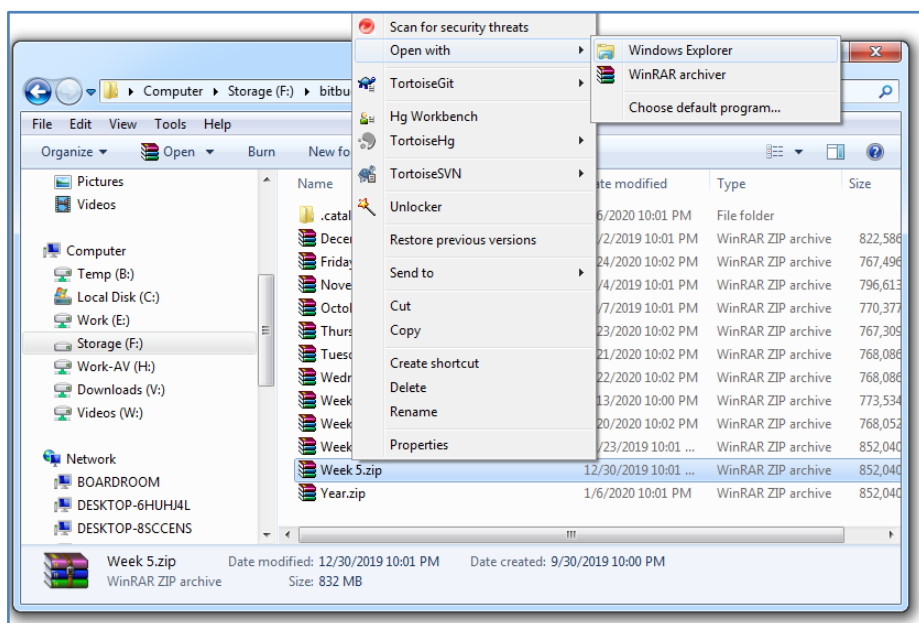
The backup destination will contain a set of .zip backup files. The file names will reflect the backup schedule used by the job that created the backups.

2. **Identify the backup** containing the files you want to restore.

The Date Modified column shows when the backup was created.

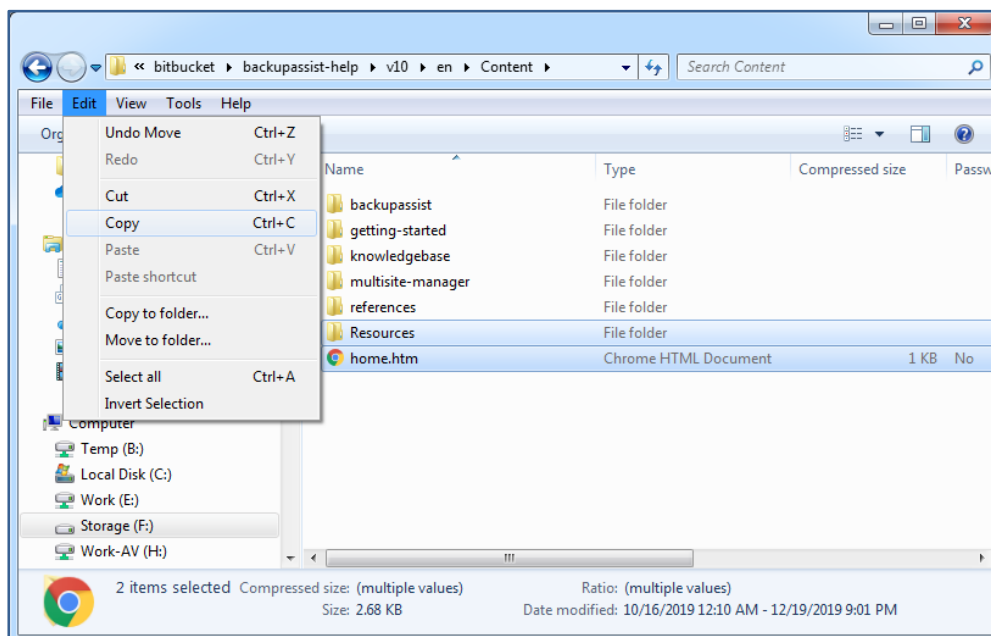


3. **Right-click** the backup and **select Open with Windows Explorer**.

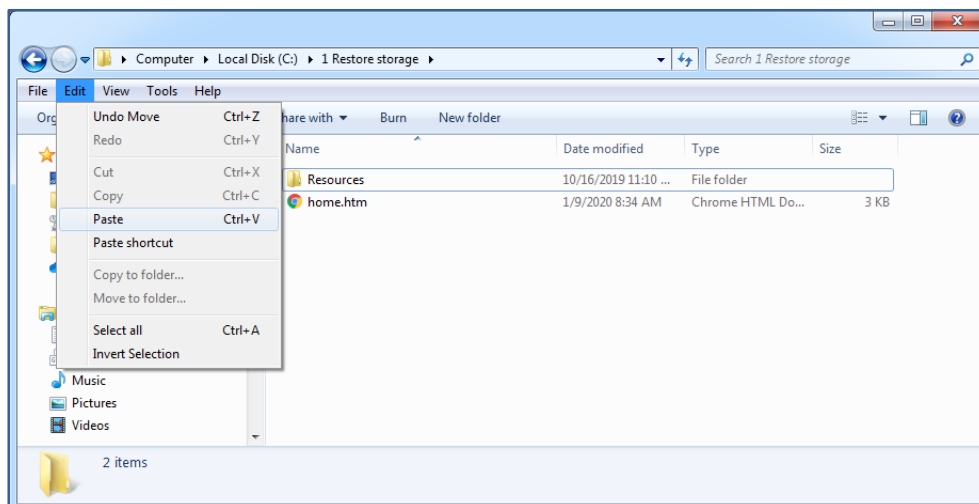


This will open the contents of the .zip file in Windows Explorer.

4. **Browse** to the **location of the files** you want to restore.
5. **Select the files** you want to restore.
Hold down the Ctrl key to select multiple files.
6. **Select Edit** then **Copy** from the top menu.



7. **Browse** to the **location** you want **to restore** the files to.
8. Select **Edit** then **Paste** from the top menu.



Congratulations – your files have been restored.

20 Restore a database from an SQL backup

This scenario uses **Microsoft SQL Server** Manager to **restore a database** from a BackupAssist **SQL Protection** backup.

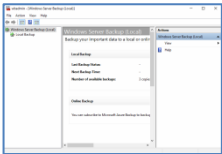



In a nutshell: If you haven't used Microsoft SQL Server Manager, don't worry. It has a simple restore process that you will use to locate an SQL Protection backup and select a restore point, which SQL Server Manager will use to restore the selected database.

To make sure there are no surprises along the way, we will begin with a look at **what you will need** and **what you should check**.

Restore requirements

To perform an SQL database restore, you will need:

<p>SQL Server Manager</p>  <p>Microsoft SQL Server Manager has a database restore option that can detect and use an SQL Protection backup.</p>	<p>SQL Protection backup</p>  <p>SQL Protection backups are saved to a local drive and require the SQL Continuous add-on.</p>	<p>Backup schemes</p> <p>SQL Protection backups created with the Transactional scheme can be used for a point-on-time restore.</p> <p>SQL Protection backups created with the Basic scheme can be used to restore from a daily backup.</p>
---	---	---

Restore checklist

Use this checklist to make sure you are ready to perform the restore:

<input type="checkbox"/>	<p>If you are recovering a production SQL Server, you should perform the recovery at a time that has minimal impact on SQL users and communicate the expected downtime.</p>
<input type="checkbox"/>	<p>Know the point in time that you want to restore the database to. For example, if the database was corrupted, you may choose a point just before the corruption occurred.</p>

Restore process

To restore a database using SQL Server Manager, follow these steps:

1. **Open Microsoft SQL Server Manager.**
2. **Connect to the SQL Server** you want to restore to.

Use the **Server name** field to select the server and select **Connect**.

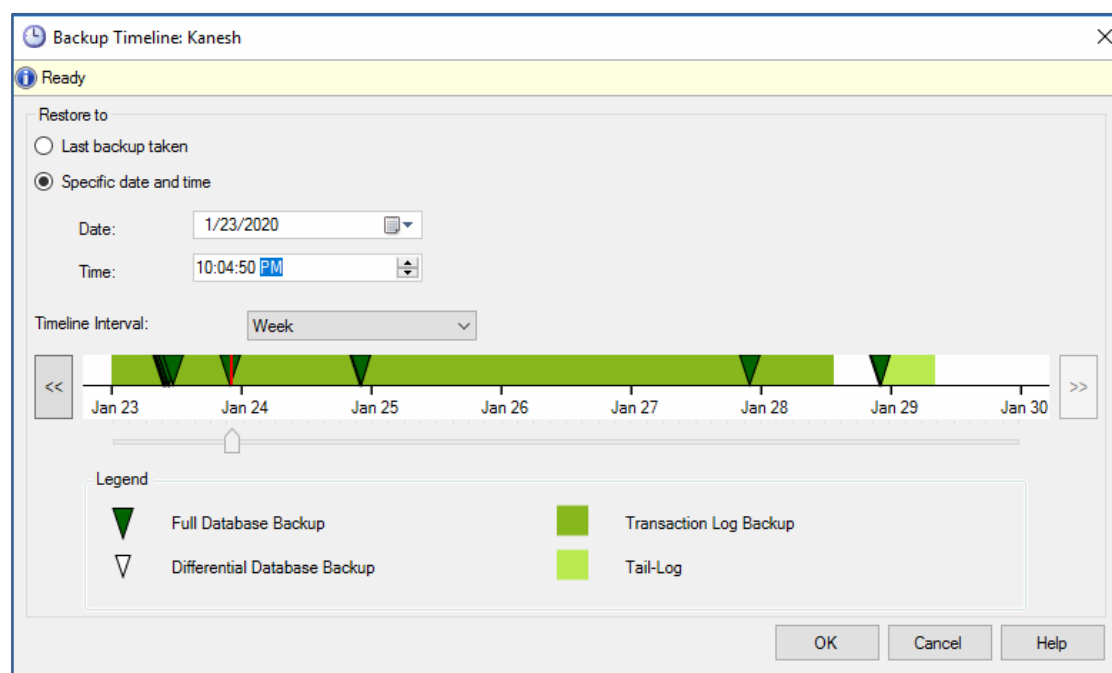
When you select the database, **Microsoft SQL Server Manager will scan** for backups of that database. This scan will detect any BackupAssist **SQL Protection backups** and **list** them in the **Backup sets to restore** section.

5. **Select Timeline.**

This will open the **Backup Timeline** screen.

6. **Choose a restore point.**

The Timeline screen is used to select a **Date** and **Time** to restore the database from.



Last backup taken

This option will use the last backup created for the database restore. The backup's date is shown in the **Date** and **Time** fields. This is ideal if you want to use the most recent backup possible.

Specific date and time

This option allows you to use the **Date** and **Time** fields to **select the time** you want to restore to and then see **what restore points are available**.

In the screenshot above, **Week** has been selected to show all restore options for the past week.

Restore points are shown as follows:

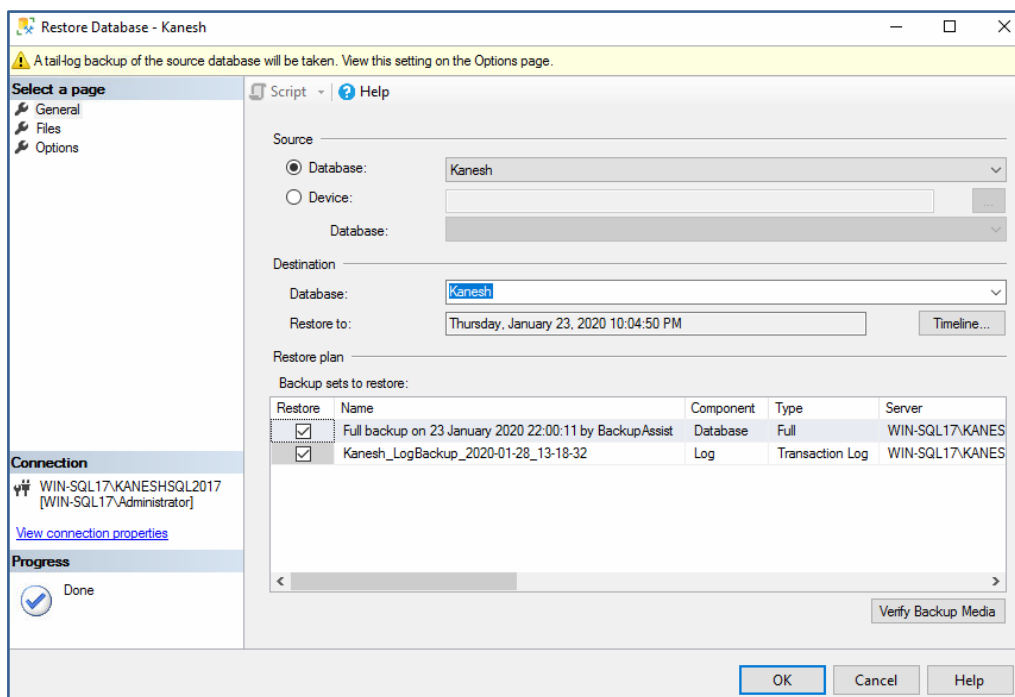
- ❖ SQL Protection backups created with the **Basic scheme** are shown as **dark green** triangles.
- ❖ SQL Protection backups created with the **Transactional scheme** are shown as **green blocks**.

7. **Confirm the selections.**

When you have selected the point to restore to, click **OK**.

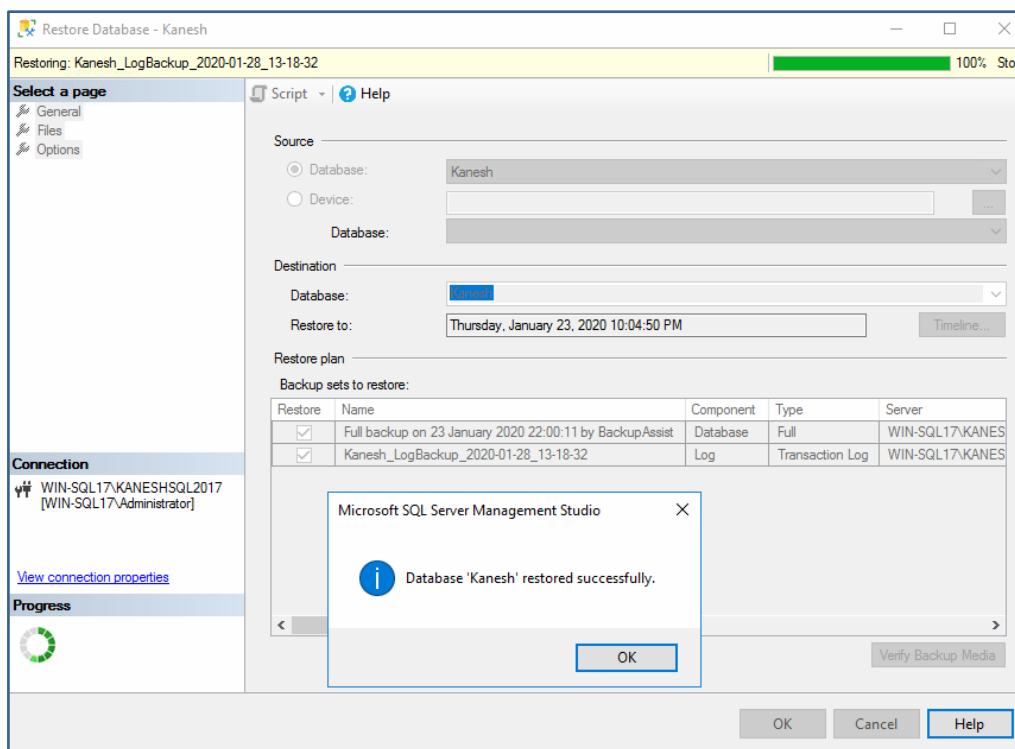
This will return you to the **Restore Database** screen.

The **Restore to** field will show the time selected, and the **Restore plan** fields show the backups and logs (for a Transactional scheme) that will be used.



8. Start the restore

Click **Ok** and the backup and log will be used **to restore the database** to the chosen point in time.



A confirmation message will appear when the restore has completed.

Congratulations – your database has been restored.

Appendix

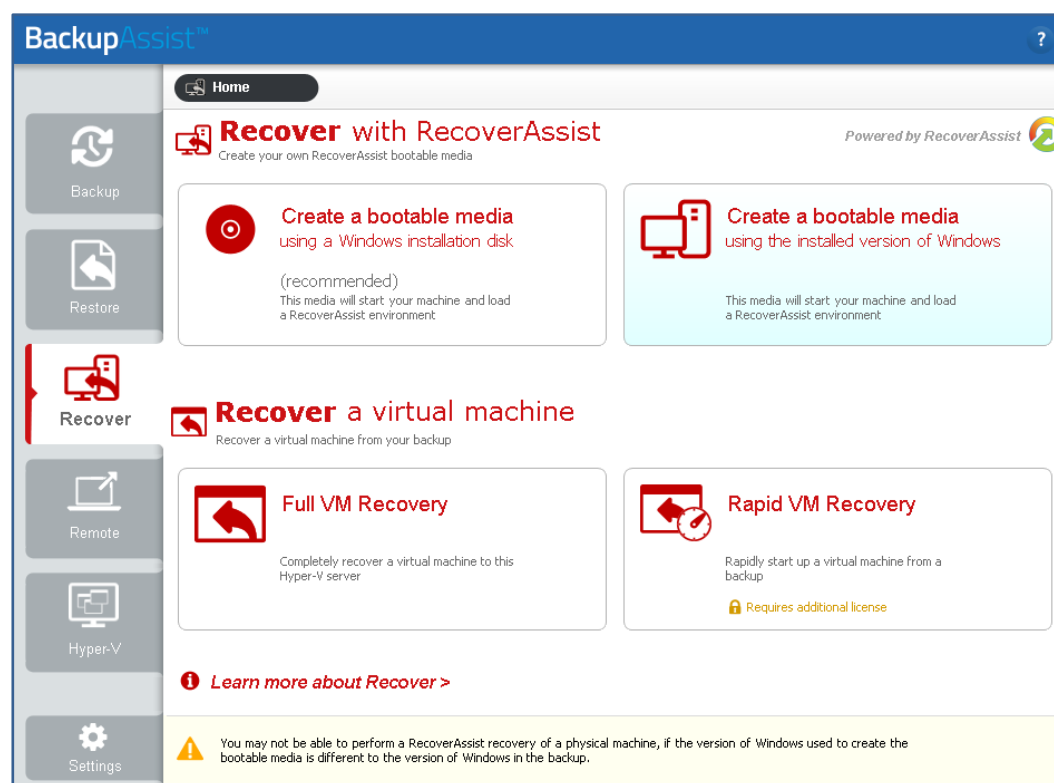
How to create a bootable recovery media

This section explains how to create a stand-alone bootable media. A standalone bootable media boots into the RecoverAssist environment and uses a System Protection bare-metal backup on separate media, to recover a server.

To create a bootable media, follow these steps:

1. **Select BackupAssist's Recover tab.**
2. **Select how you want to make the bootable media.**

Choose either **Create a bootable media using the installed version of Windows** or **Create a bootable media using a Windows installation disk**.



If you choose, **Create a bootable media using the installed version of Windows**, RecoverAssist will use the computer you are on, and its operating system, to create a bootable Recovery disk. If the operating system requires an install disk, this option will be greyed out and not selectable.

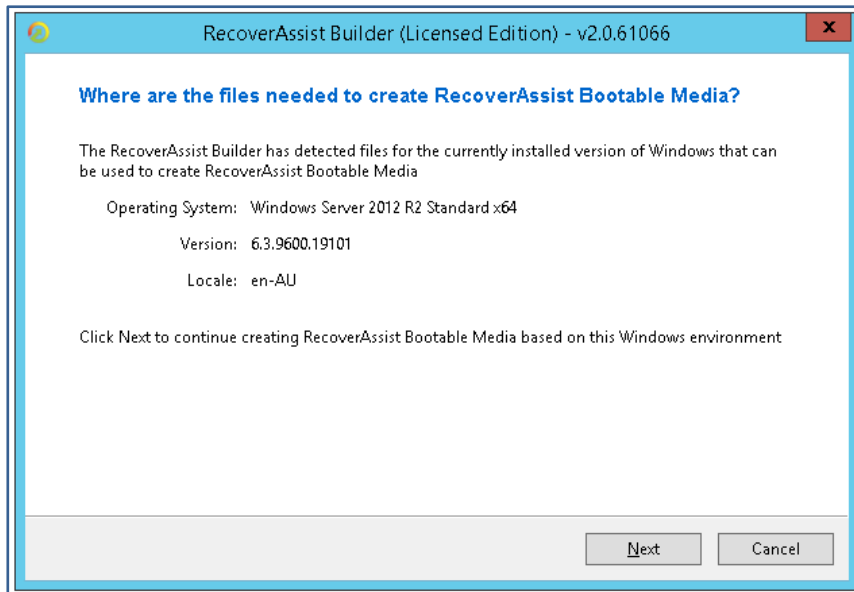
If you choose, **Create a bootable media using a Windows installation disk**, RecoverAssist will use a Windows operating system installation disk, to create a bootable Recovery Environment.



OEM installations of Windows and Windows installation media provided by system manufacturers may include altered system files that can cause RecoverAssist recovery environments to fail. BackupAssist recommends the use of a Microsoft issued install disk or ISO when building RecoverAssist recovery media.

3. Select or confirm the Operating System location.

When you make a selection in step 2, the RecoverAssist dialog will open. Confirm the Operating System or provide the location of the installation disk to be used, and click **Next**.

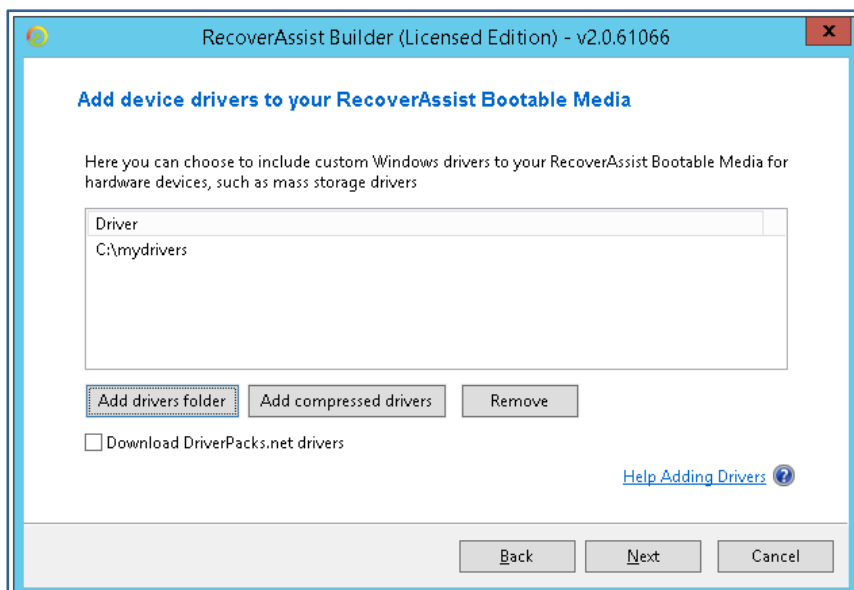


If you selected, **Create a bootable media using the installed version of Windows**, RecoverAssist will confirm the operating system details for the computer you are on.

If you selected, **Create a bootable media using a Windows installation disk**, RecoverAssist will try to detect the media. If it cannot, it will ask you to insert the Windows installation disk and select a drive letter from the drop-down list.

4. Add any device drivers to your RecoverAssist Bootable Media.

RecoverAssist lets you **add your own drivers** to the bootable media. These drivers may be required to give the recovery environment access to the backup location and the local hardware. Make your selections, and click **Next**.



RecoverAssist will automatically select the appropriate driver to be used during the boot process.

There are three ways to add drivers:

- **Add drivers folder** allows you to browse to the location of the drivers that you want to add to the recovery media. Drivers should be added in an unpacked state.
- **Add compressed drivers** will unpack any compressed drivers you select and add them to the recovery media.
- **Download DriverPacks.net** will download a recommended driver pack. The drivers will be automatically downloaded and added to the media during the media creation stage.

5. **Add any files/folders to your RecoverAssist Media.**

You can add your own **files and folders** to the bootable media and have them **available to use** when you are performing the recovery. Make your selections, and click **Next**.

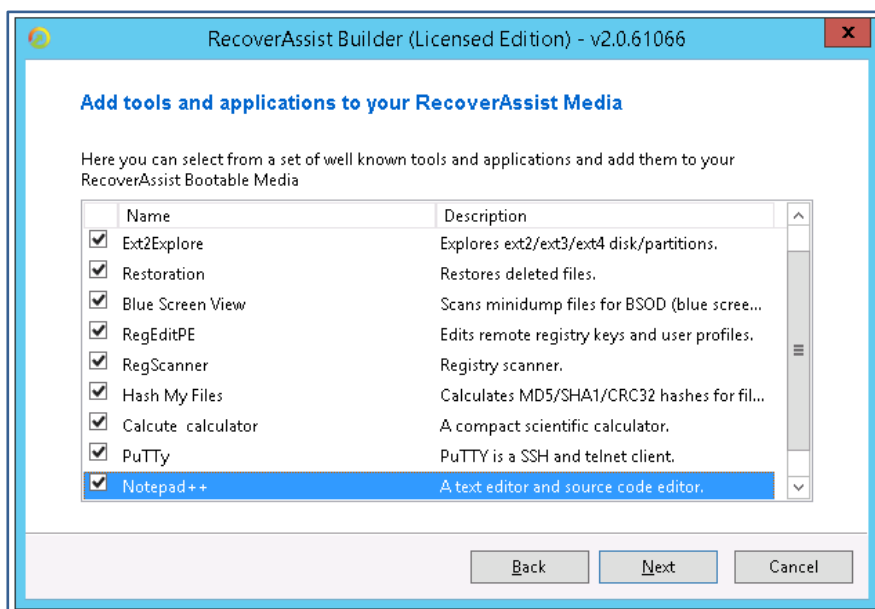
The files and folders will be added to the **UserFiles folder** in the **root directory**. You can also use this step to add drivers that you do not want to be loaded when the system boots.

6. **Add tools and applications to your RecoverAssist Media.**

This step displays a list of useful troubleshooting and support tools that you can choose from.

The applications you select will be **added to your recovery media** and made **available during a recovery**. Applications selected will be downloaded from BackupAssist and added to the media when it is created.

Tick the box next to the application and click **Next**.



7. **Choose what type of media to use for RecoverAssist.**

RecoverAssist can use **removable drives, ISO images or optical disks** as bootable media. You can also make a backup media bootable using the Bootable Backup Media option.

Bootable Backup Media

This option adds RecoverAssist to the backup media. A Bootable Backup Media can be used to boot into a RecoverAssist recovery environment and recover the server, without a separate boot disk. A warning will appear if RecoverAssist needs to format the backup media. If a format is required, all data on the drive, including any backups and backup history, will be lost.

Removable drive

This option will create the recovery image on a removable drive. A warning will advise that the removable drive will be formatted before it is written to. This means everything currently on the drive will be deleted.

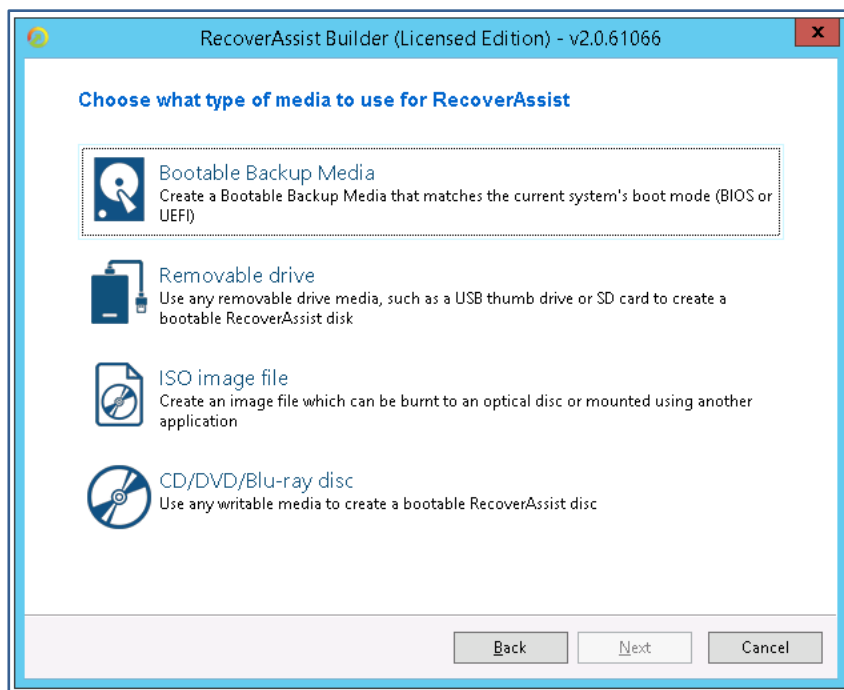
An ISO image file

This option will create an ISO image. Although the saved ISO image is not on a bootable media, it can be used to create a recovery image that can be saved to a bootable device at a later date.

CD/DVD/Blu-ray disc

This option will detect the optical drive on your computer and ask you to select the drive containing the optical media.

Make your selection, and click **Next**.



When you select **Next**, the bootable media creation will begin.

A progress bar will be displayed. Once it has completed, click **Finish**.

The bootable media has now been created.

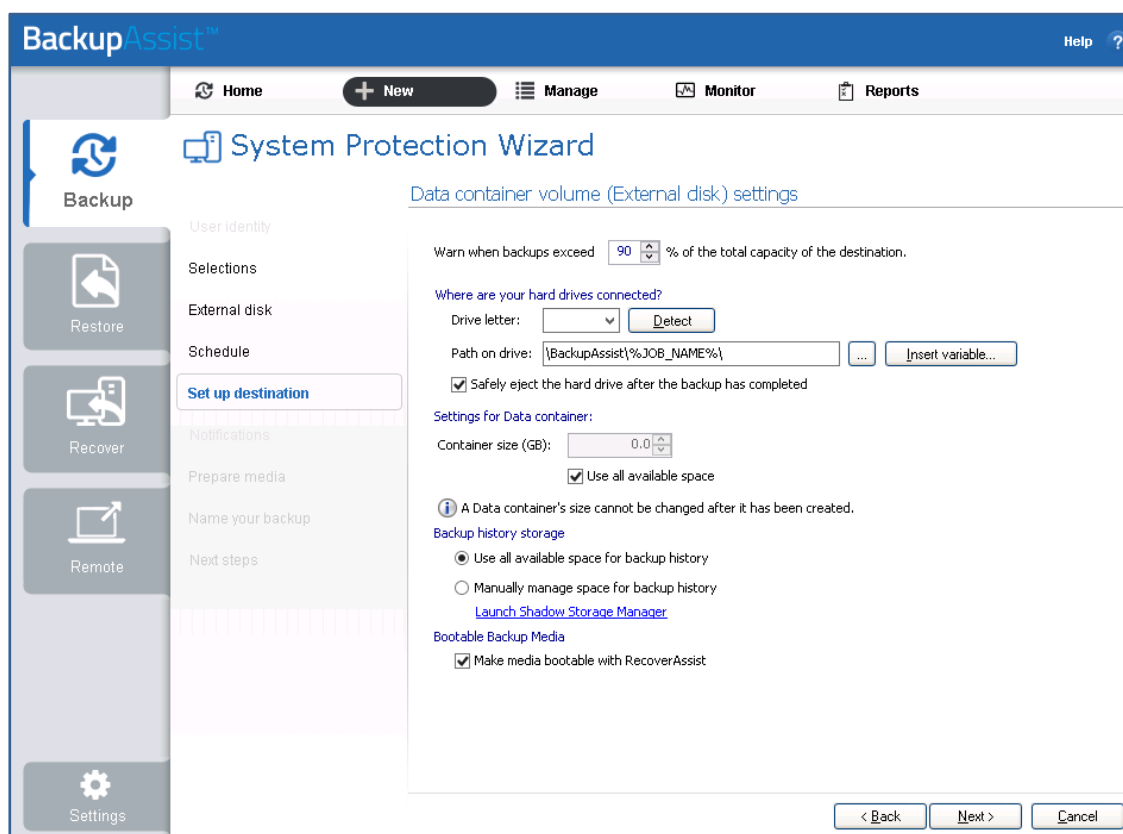


Any bootable RecoverAssist media created during the BackupAssist trial period will expire. The RecoverAssist media will need to be re-created once a BackupAssist license has been purchased. This must be done after you purchase a license.

Creating a bootable backup

If you create a **System Protection** bare-metal backup on an **external USB hard disk**, the media will be made into a **Bootable Backup Media**, which can boot a server into a recovery environment and recover the server, without a separate boot disk.

When you create the backup job, the **media will be made bootable by default**, unless you deselect the Make media bootable with RecoverAssist tick-box on the **Set up destination** step.



Creating a Bootable Backup Media

- Selecting **Prepare** on the **Prepare media** step will generate a **Destination Check Report**. This report will advise if the backup media could not be made bootable.
- If the media is an external USB hard disk, it will be **made bootable** the **first time** the backup **job runs**. This can make the first backup take longer than a normal backup.
- After you run the backup job, the **backup report's Recovery** section will **note if the backup media was made bootable** or if the boot information was updated.
- **If there are problems** making the media bootable, you can use the **Recover tab** to manually **make the backup media bootable**, or make a separate, standalone RecoverAssist media.

Considerations:

- If a **newer version of RecoverAssist** is released, it will be **applied to the media**.
- If a bootable media is created using a **trial version** of BackupAssist, it **will be updated if a license key is purchased**.
- If the **operating system** being backed up **changes**, the **bootable media will update** to support it.