

ActiveImage Protector 2022 Virtual Setup Guide

2nd Edition (October, 2023)



CONTENTS

1. Overview.....	3
1-1. Agentless and agent-based backup.....	3
1-2. Product Components	4
1-3. System Requirements.....	5
2. Preparatory Steps	7
2-1. Installation of HyperAgent	7
2-2. Configure HyperAgent settings.....	9
3. Product Activation.....	12
4. Configure backup settings and run backup tasks.....	13
4-1. Agent-based Backup	13
4-2. Agentless Backup.....	14
5. Restore	27
5-1. File / Folder Recovery.....	27
5-2. Restore a backup as a virtual machine (HyperRecovery).....	32
5-3. Zero Time Recovery (HyperRecovery LIVE!)	37
6. Image Management – Image Manager	42
6-1. Image Manager	42
6-2. Check for bootability of backups (BootCheck).....	43
6-3. Quick Verify	45
6-4. Consolidation	47
6-5. Archive Backups.....	49
6-6. MD5 Checksum.....	51
6-7. Delete Backup Files.....	53
6-8. Image Manager: Mount Image	54
6-9. Image Manager: Image Target Server.....	56
7. Virtualization	64
7-1. Migration from backup source to virtual environment.....	64
7-2. Migration from physical disk to virtual environment	69
8. Creates and maintains dormant virtual replicas.....	73
8-1. HyperStandby	73
8-2. HyperBoot	82
9. Remote Management Console.....	91
10. Reference	94

1. Overview

ActiveImage Protector is a data protection solution supporting various system environments, including physical and virtual machines and cloud environments. This set-up guide will show you how to install and configure ActiveImage Protector 2022 Virtual in on-premise virtual environments. We recommend you read this manual before using ActiveImage Protector 2022 to configure backups. Please visit our online help for more detailed information and limitations.

Online Help for Windows environments: https://webhelp.actiphyc.com/AIP/2022/en_US/

Online Help for Linux environments: https://webhelp.actiphyc.com/AIP/linux/2022/en_US/

1-1. Agentless and agent-based backup

ActiveImage Protector Virtual provides an agentless backup feature enabling you to back up virtual machines on specific hypervisors without installing ActiveImage Protector agents on your source hypervisor or virtual machines, as well as a traditional agent-based backup of virtual machines requiring the installation of ActiveImage Protector agents:

1. **Agentless backup:** ActiveImage Protector Virtual now provides HyperAgent, an agentless backup feature, selectable when backing up virtual machines on a hypervisor. HyperAgent backs up and restores virtual machines without the need to install ActiveImage Protector on either the host or guest machines.

There are several advantages to agentless backups:

- Since there is no need to install ActiveImage Protector agents on virtual machines, you don't have to waste time performing manual installations.
- The HyperAgent, installed on a remote machine, runs the tasks, minimizing CPU and memory resource consumption on host and guest machines.
- You get flexible support for virtual machines' guest operating systems (Windows Server 2003 and later OS).

2. **Agent-based backup:** Agent-based backup requires the installation of ActiveImage Protector agents on virtual machines in the same manner as in the physical environment. ActiveImage Protector installed on the virtual machines respectively backs up and restores the virtual machines.

There are several advantages to agent-based backups:

- Unified backup operation for physical and virtual environments.
- No need for administrative rights on the hypervisor host.
- Support for VMware vSphere RDM, Hyper-V path through disk configuration.

*When registering hypervisor with HyperAgent, you need Administrator's privilege.

1-2. Product Components

ActiveImage Protector Virtual is composed of the following product media and product keys.

1. Product media
 - a. Product media for ActiveImage Protector 2022 Windows: You use this product media to install ActiveImage Protector agents on Windows virtual machines and to install HyperAgent.
 - b. Product media for ActiveImage Protector 2022 Linux: You use this product media to install ActiveImage Protector agents on Linux virtual machines.

2. Product Key
 - a. Product Key for HyperAgent: You use this product key to install HyperAgent.
 - b. Product Key for installation of the product on virtual machines (agent-based): You use this product key to install the product on Windows / Linux virtual machines.

1-3. System Requirements

The following are the system requirements for ActiVImage Protector 2022 (Version 7.0.0.8643 for Windows, Version 7.0.0.8661 for Linux). Please ensure your computer meets these minimum system requirements before using ActiVImage Protector 2022. Please visit our Web site (<https://www.actiphy.com/global/support/system-requirements>) for the latest system requirements.

Windows Virtual Machine (agent-based), HyperAgent	
CPU	Pentium 4 or newer.
Main Memory (RAM)	2GB of RAM or greater.
Hard Disk	650MB of available disk space or greater.
DVD drive	Needed to install, boot, or start up the ActiVImage Protector boot environment.
Internet connection	Required for online activation of the product, issuing a license file and installation of the latest updates.
Supported OS	<ul style="list-style-type: none"> ▪ Windows Server 2022 ▪ Windows Server 2019 ▪ Windows Server 2016 ▪ Windows Server 2012 R2 ▪ Windows Server IoT 2019 / 2022 for Storage ▪ Windows Storage Server 2016 ▪ Windows Storage Server 2012 R2
Linux Virtual Machine (agent-based)	
CPU	Pentium 4 or newer. *Only x86_64 architecture is supported. *Secure Boot is not supported.
Main Memory (RAM)	2GB or above.
Hard Disk Space	2GB or more of available hard disk space is required at setup.
DVD-ROM Drive	Required to install the product and boot up the ActiVImage Protector Boot Environment.
Internet connection	Required for online activation of the product
Supported OS	<ul style="list-style-type: none"> ▪ Red Hat Enterprise Linux : 9.0 – 9.2 / 8.0 – 8.6 / 7.0 – 7.9 (x86_64) ▪ CentOS : 8.1 – 8.4 / 7.0 – 7.9 / 6.0 – 6.10 (x86_64) ▪ Oracle Linux : 9.0 – 9.2 / 8.1 – 8.6 / 7.0 – 7.9 (x86_64) ▪ AlmaLinux 9.0 – 9.2 / 8.3 – 8.8 ▪ MIRACLE LINUX 9.0 / 8.6 / 8.4 ▪ Rocky Linux 9.0 – 9.2 / 8.3 – 8.8 ▪ Amazon Linux 2 ▪ SUSE Linux Enterprise Server 15 / Desktop 15 ▪ openSUSE Leap 15 ▪ Ubuntu 18.04LTS / 20.04LTS / 22.04LTS ▪ Debian 9 – 12

Hypervisor	
Supported Hypervisor	<ul style="list-style-type: none">▪ Windows Server 2022 Hyper-V▪ Windows Server 2019 Hyper-V▪ Windows Server 2016 Hyper-V▪ Windows Server 2012/2012 R2 Hyper-V▪ VMware vSphere ESX[i] 6.0 / 6.5 / 6.7 / 7.0 / 8.0▪ Citrix Hypervisor 8.2▪ Proxmox VE 7.2-1▪ Nutanix Acropolis Hypervisor (AHV) 20190916.276 <p>*Agentless backup supports virtual machines configured on Hyper-V or VMware vSphere. Please use agent-based backup for the virtual machines configured on other hypervisors.</p> <p>*As for the supported backup source OS for HyperAgent (agentless backup), please refer to our knowledge base: https://enkb.actiphyc.com/?akb&p=3479</p>

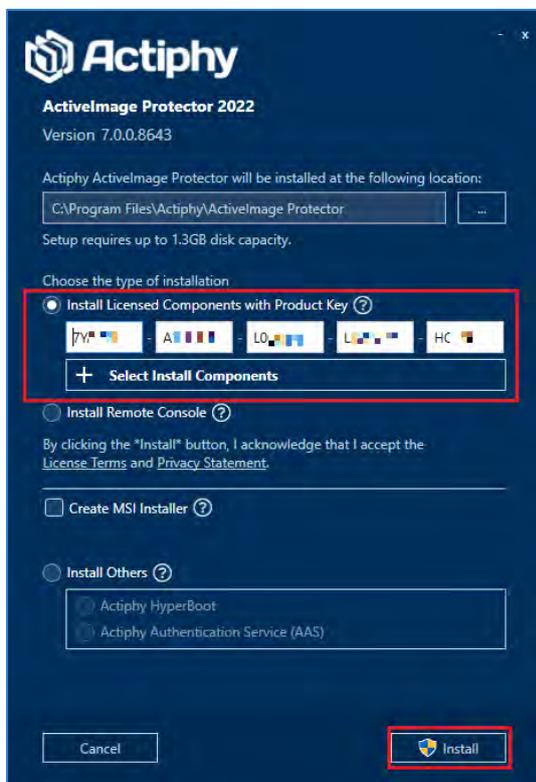
2. Preparatory Steps

Whether you use an agentless or agent-based backup, you must install "HyperAgent." Please install HyperAgent on a remote Windows server on the same network as the hypervisor host on which you have configured backup source virtual machines. Please install HyperAgent on one of the following:

1. A new Windows server.
2. An existing Windows NAS.
3. A Hyper-V host.
4. Windows virtual machines.

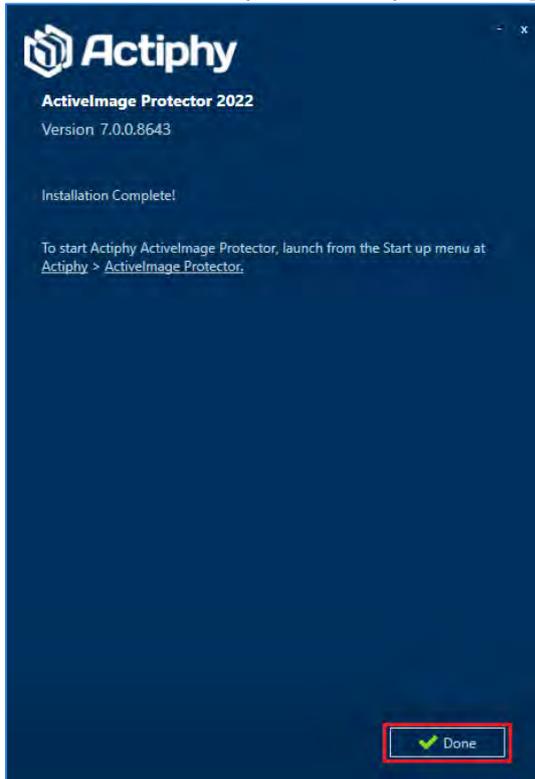
2-1. Installation of HyperAgent

1. Insert ActiImage Protector 2022 Windows product media into the media drive of your computer, and double-click on "Setup.exe" in the "Setup" folder to run the installer. Select **[Install Licensed Components with Product Key]** from the install wizard and enter the product key for "HyperAgent." Click **[Install]** to start the installation process.



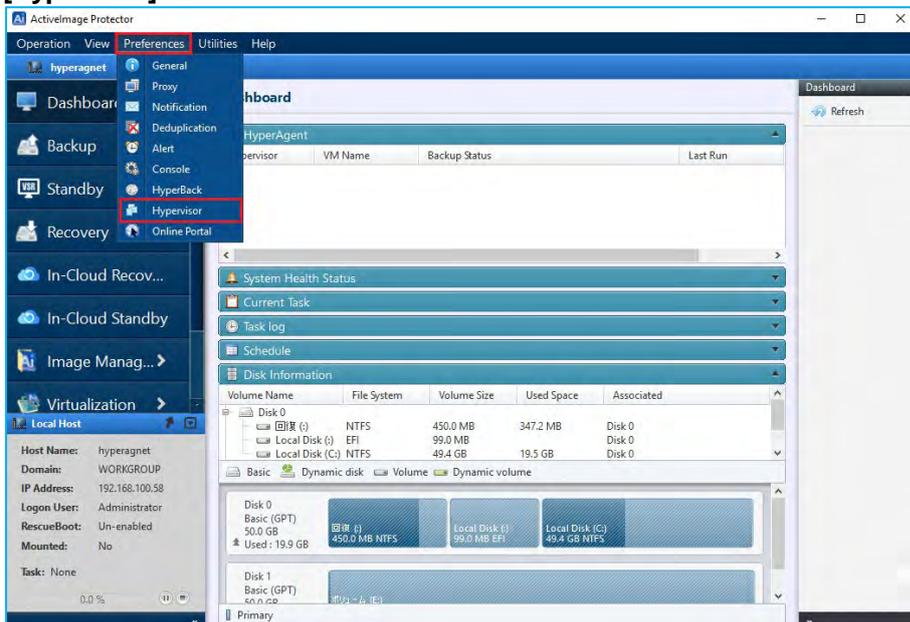
Preparatory Steps

2. When the installation process completes, click **[Done]**. You do not need to reboot your system after installation.

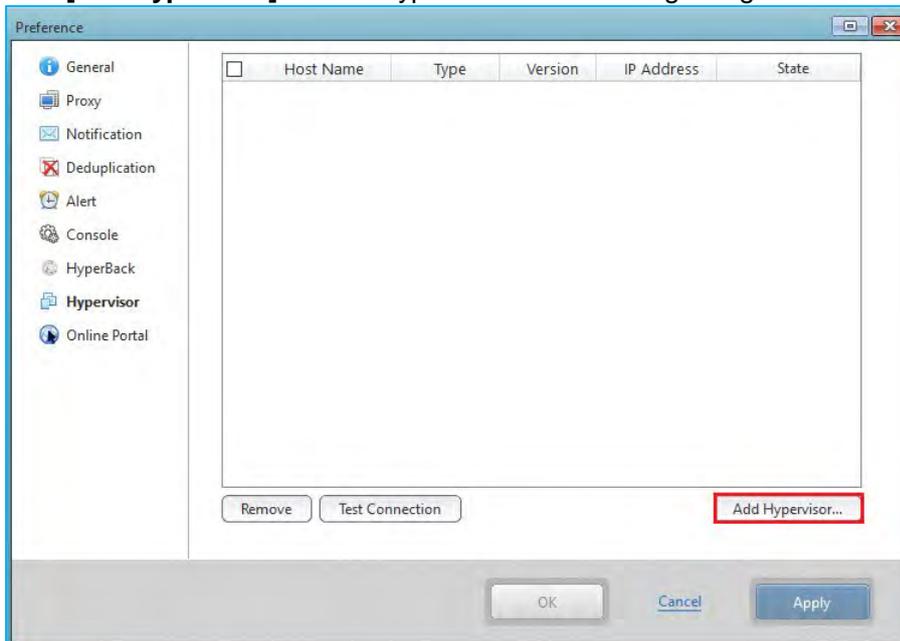


2-2. Configure HyperAgent settings

- Once you've completed the installation process, register the "hypervisor" on the backup source virtual machines you have configured. Next, start ActiImage Protector by clicking on the Windows Start menu and selecting **[ActiPhy]** → **[ActiImage Protector]**. Next, select **[Preference]** in the console menu and click **[Hypervisor]**.

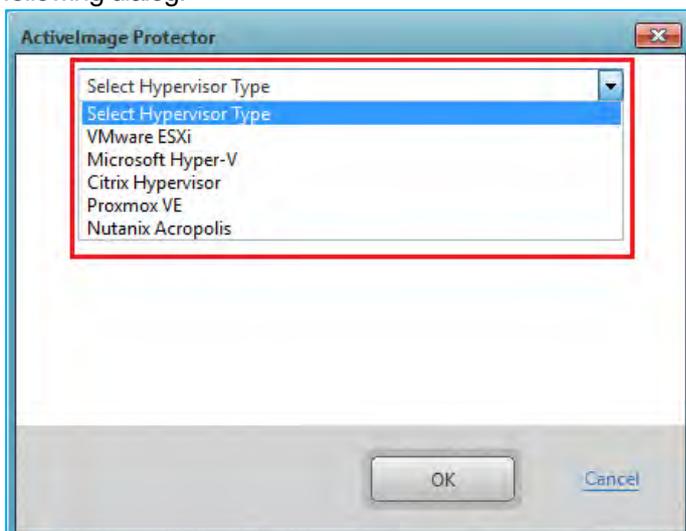


- Click **[Add Hypervisor]** to add a hypervisor in the following dialog.

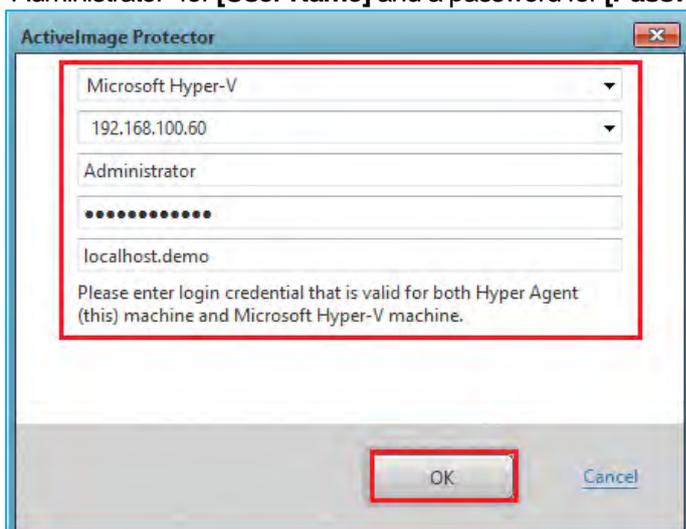


Preparatory Steps

3. Click on the "▼" icon on the right-hand side of the **[Select Hypervisor Type]**, and the hypervisors of the selected type are listed. Please select the hypervisor. Click **[Add Hypervisor]** to add a hypervisor in the following dialog.

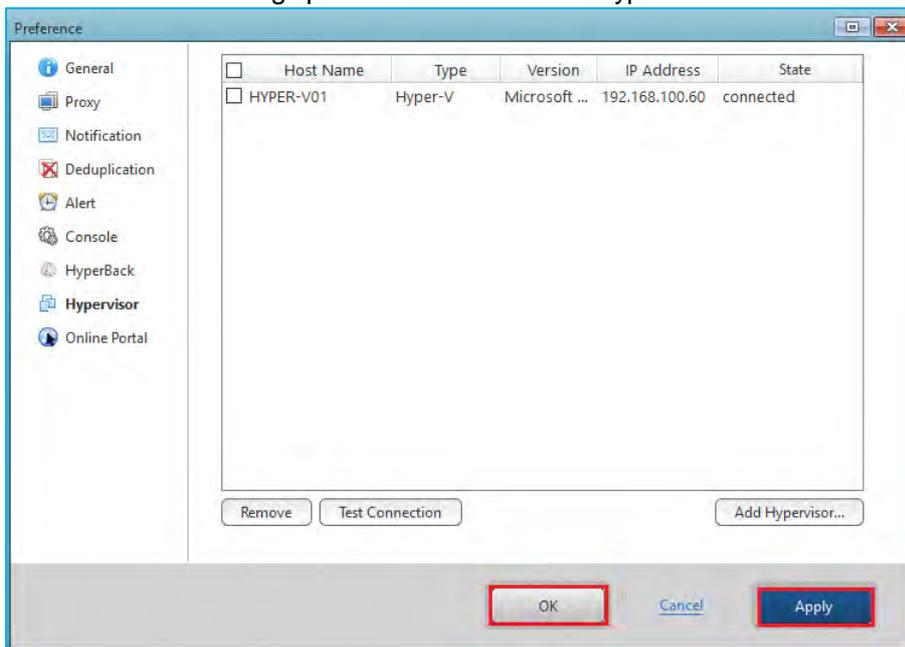


4. The example screen below shows that "Microsoft Hyper-V" is selected for **[Hypervisor Type]**, and the IP address "192.168.100.60" is specified for **[Host Name or IP address]**. In this case, we've entered "Administrator" for **[User Name]** and a password for **[Password]**. Click the **[OK]** button to continue.



Preparatory Steps

5. Please ensure you have established a connection to the hypervisor host, then click **[Apply]** and **[OK]**. Now that you have registered the hypervisor for HyperAgent, the agentless and agent-based backup features are selectable when backing up virtual machines on the hypervisor.



3. Product Activation

ActiveImage Protector supports three types of activation:

- Activating your product online.
- Actiphy Authentication Service (AAS).
- Using a license file.

The easiest method is to activate your product online using the Actiphy License Server.

If you need to activate ActiveImage Protector on a PC that doesn't have internet access, please use the Actiphy Authentication Service (AAS) or License File options to activate your product.

For detailed information on activating your product, please refer to the Activation Guide for your product on Actiphy's website:

- ActiveImage Protector 2022 Server
https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_server
- ActiveImage Protector 2022 Desktop
https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_desktop
- ActiveImage Protector 2022 Linux
https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_linux
- ActiveImage Protector 2022 Virtual
https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_virtual
- AAS Docker
https://www.actiphy.com/global/activation_guide/aas_docker/
- Remove license/bundle file:
https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_license_recovery_guide

4. Configure backup settings and run backup tasks

ActiveImage Protector Virtual now provides HyperAgent, an agentless backup feature, selectable when backing up virtual machines on the hypervisor, and the traditional agent-based backup of virtual machines requiring the installation of ActiveImage Protector.

4-1. Agent-based Backup

1. System environments that only support agent-based backups. Install ActiveImage Protector agents on virtual machines to backup the following system environments:

- Unified backup operation for physical/virtual environments.
- Agent-based backup supports the hypervisor, which agentless backup does not support.
- Domain controller, SQL Server, Exchange, Oracle, non-VSS-savvy database, etc., is deployed on the virtual machine configured on Hyper-V 2012/2012R2.
- Installation of ActiveImage Protector agents on virtual machines and configuration of basic settings.

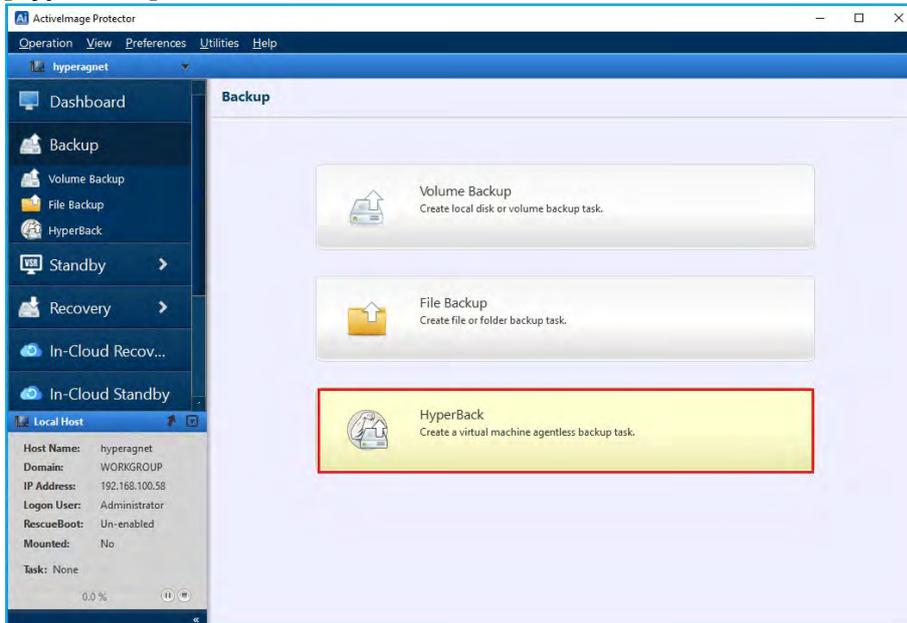
2. Please refer to the following setup guide for more detailed information on installing ActiveImage Protector agents on virtual machines and the configuration of backup/restore settings.

- ActiveImage Protector 2022 Server Setup Guide:
https://www.actiphly.com/global/setup_guide/actiphly_activeimage_protector_2022_server
- ActiveImage Protector 2022 Linux Setup Guide:
https://www.actiphly.com/global/setup_guide/actiphly_activeimage_protector_2022_linux

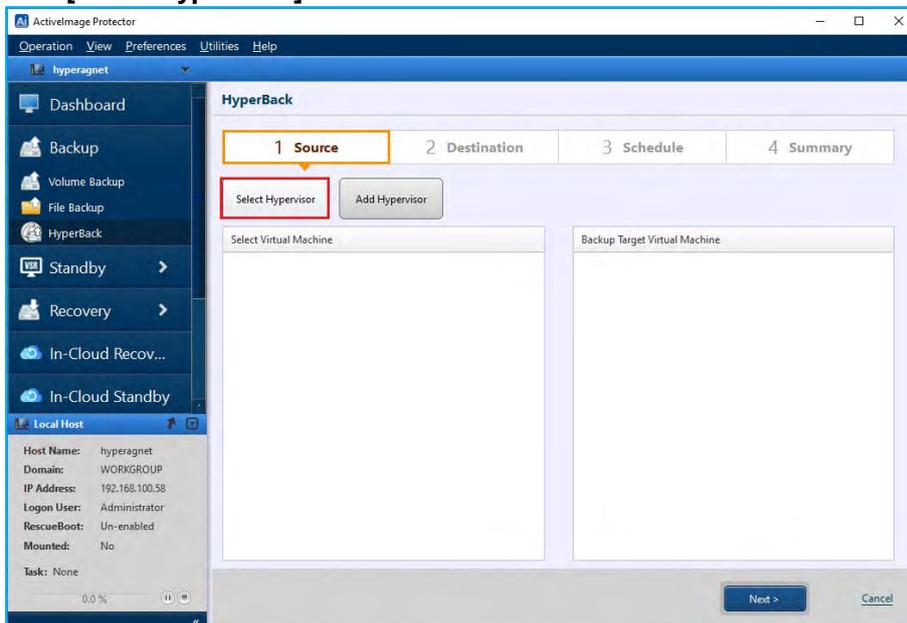
4-2. Agentless Backup

Use the following steps to configure the "agentless backup" settings.

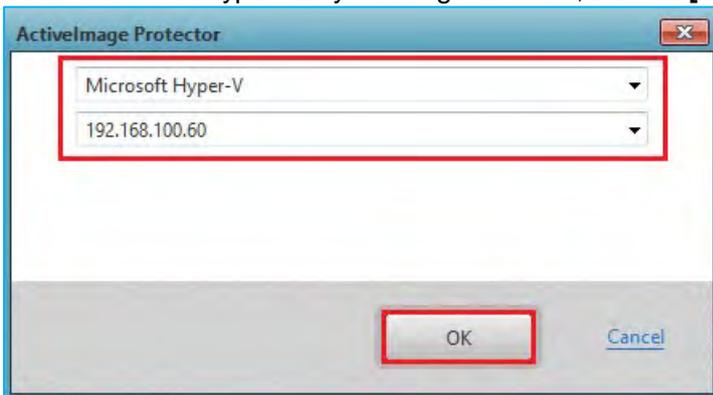
1. Launch ActiImage Protector by clicking on the Windows Start menu and then navigating to **[Actiphy]** → **[ActiImage Protector]**. Launch ActiImage Protector's console window and select **[Backup]** → **[HyperBack]** in the menu.



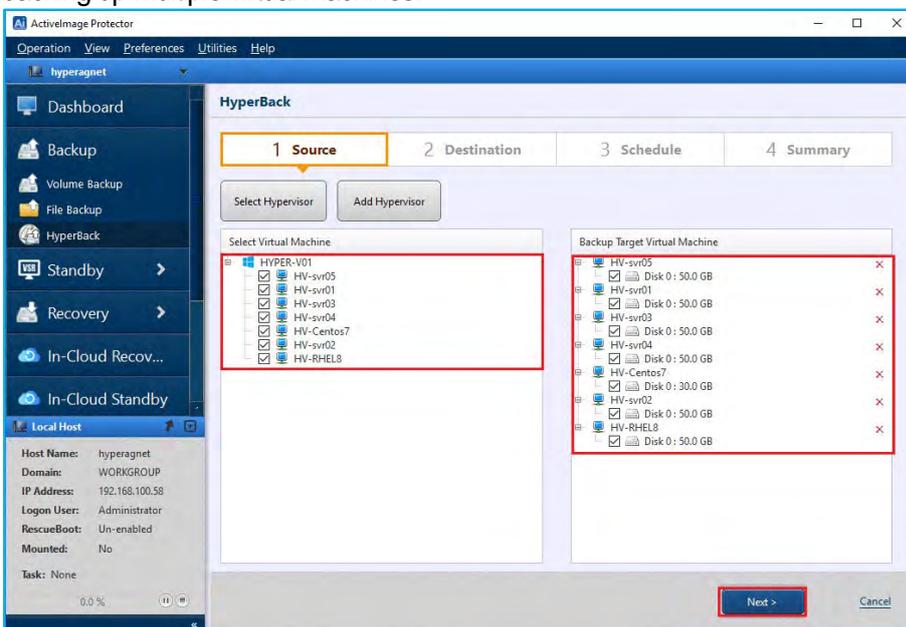
2. Click **[Select Hypervisor]**.



- 3. Select the source hypervisor you configured. Then, click the **[OK]** button.

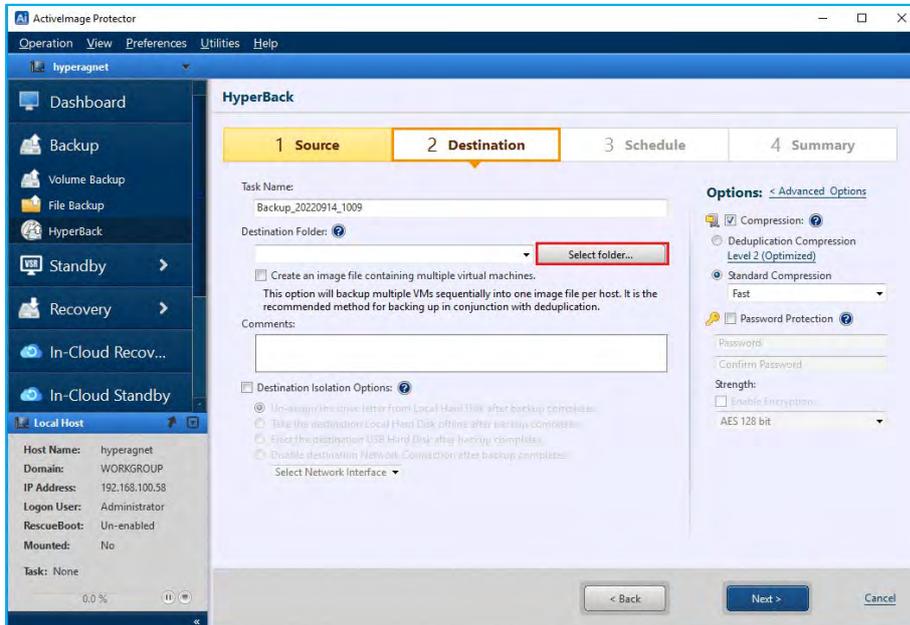


- 4. Enable the checkbox next to the virtual machine(s), which the system will add to the **[Backup Target Virtual Machine]** list. Then, click the **[Next]** button. By default, you may execute five backup tasks in parallel when backing up multiple virtual machines.

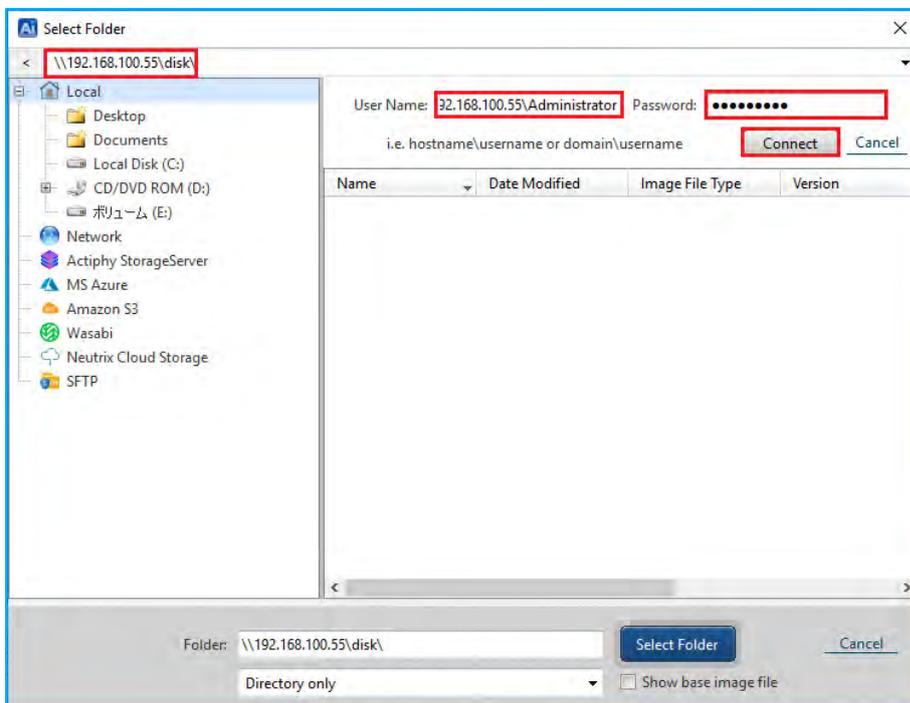


Configure backup settings and run backup tasks

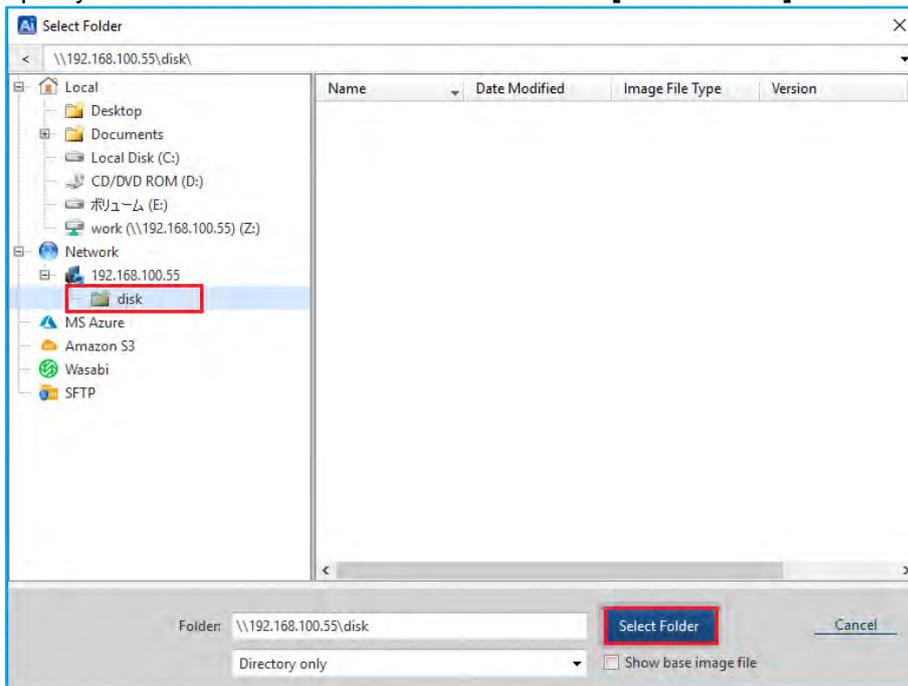
- Now, you should be on the **[2 Destination]** screen. From here, you can:
 - Enter the name of your backup task in the **[Task Name]** field.
 - For example, we've named our task "Backup_20220914_1009" in this step.
 - Select a destination folder to store your backup image. Click the **[Select Folder]** button to configure your destination folder, or click on the "▼" icon on the right-hand side of the **[Destination folder]** text box to select a location to save your backup.



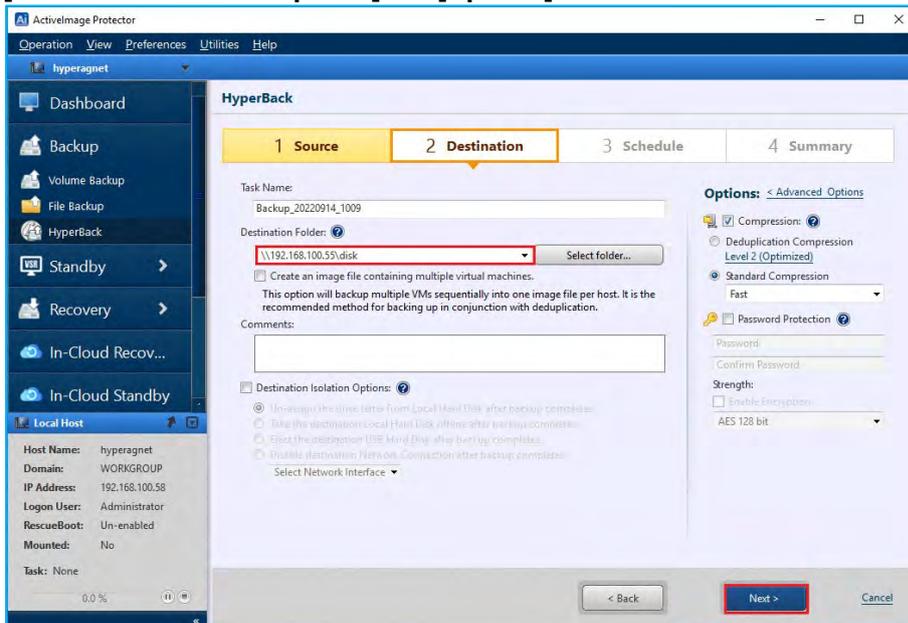
- Specify a shared folder for the destination storage and press the **[Enter]** key. Also, enter the destination folder's login credentials and click the **[Connect]** button. (In this screenshot, we're using "192.168.100.55\disk" as the destination folder and "192.168.100.55\Administrator" as the username). Click **[Connect]**.



Specify the shared folder for the destination and click **[Select Folder]**.



7. Ensure you have correctly filled in the **[Destination Folder]** field and click **[Next]**. We will review the **[Destination Isolation Options]** and **[Options]** sections later in this document.



Configure backup settings and run backup tasks

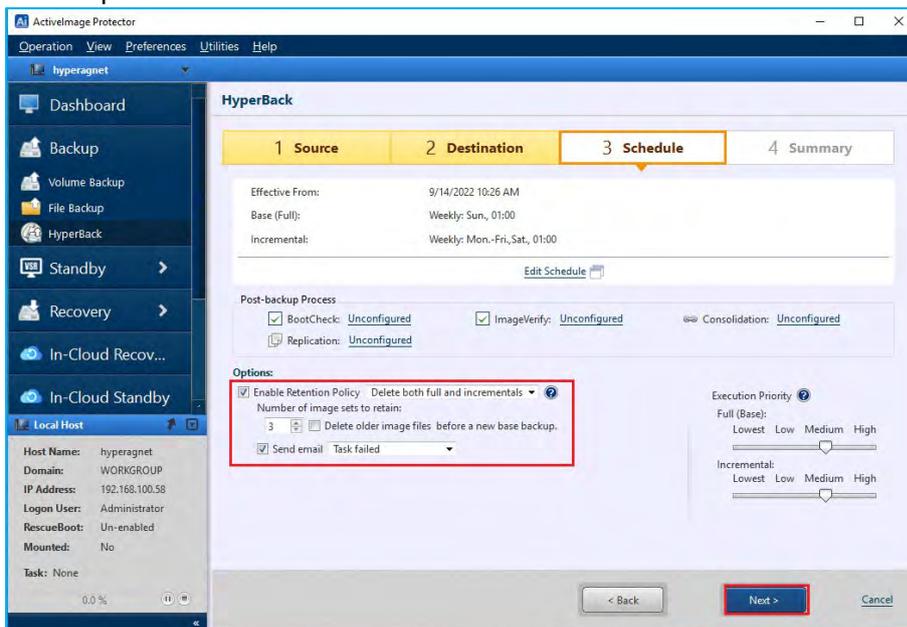
- Configure the backup schedule. The steps below show an example of configuring a schedule:
 - Select **[Schedule Backup]** for the Task Type and configure the Weekly backup schedule settings.
 - Set the Base backup schedule to **Weekly**.
 - Set the Incremental backup schedule to **Weekly**.
 - Set the Execute Time of the Base backup to **Sundays at 1:00 am**.
 - Set the Incremental Backup schedule to **Monday to Saturday at 1:00 am**.
 - After configuring all options, click the **[OK]** button.

The screenshot shows the 'Schedule Settings' dialog box for a backup task named 'Backup_20220914_1009'. The 'Effective Date/Time' is set from 2022/09/14 10:26 to 2023/09/14 10:26, with 'Not Specified' checked. The 'Base' section is configured with 'Weekly' frequency, 'Sun' selected, and 'Execute Time' of 01:00. The 'Incremental' section is also configured with 'Weekly' frequency, 'Mon' through 'Sat' selected, and 'Execute Time' of 01:00. The 'Multi-times' section is unselected, and 'One time only' is selected with 'Execute Time' of 01:00. The 'Add New Base' and 'Add New Incremental' links are visible at the bottom. The 'OK' button is highlighted with a red box.

- The following example shows how to set up a multi-scheduled backup:
 - Click the **[Add New Base]** link on the Schedule Settings page
 - Configure the settings for your additional schedule.
 - In addition to a weekly schedule, you can configure backups to occur on specific days, such as the month's second and fourth Fridays, using the **[Designate Specific Days]** option.

The screenshot shows the 'Schedule Settings' dialog box for a backup task named 'Backup_20220914_1009'. The 'Effective Date/Time' is set from 2022/09/14 10:26 to 2023/09/14 10:26, with 'Not Specified' checked. The 'Base' section is configured with 'Designate Specific Days' selected. The 'Month' is set to 1, and the 'Execute Time' is 00:00. A calendar grid shows the second and fourth Fridays of the month selected. The 'Incremental' section is configured with 'Weekly' frequency, 'Mon' through 'Sat' selected, and 'Execute Time' of 01:00. The 'Multi-times' section is unselected, and 'One time only' is selected with 'Execute Time' of 01:00. The 'Add New Base' link is highlighted with a red box. The 'OK' button is highlighted with a red box.

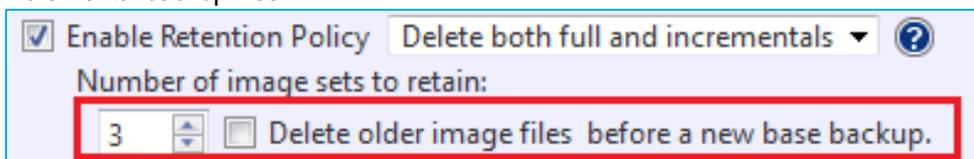
10. You can configure your **[Enable Retention Policy]** and **[Send Email]** settings on the **[Schedule]** tab. Then, click the **[Next]** button for the settings to take effect. We will cover details about Post-backup Process in the next chapter.



- **Enable Retention Policy**

The Retention Policy defines how many sets of backup files to retain before deletion. In this example, we've enabled the retention policy by checking the **[Enabling Retention Policy]** checkbox. We've also configured the program to keep the three most recent backups in the destination folder and delete any backups older than those. The default setting for the **[Number of image sets to retain]** field is 3.

Note: Each set of ActiImage Protector backup files consists of one base backup image and any associated incremental backup files.

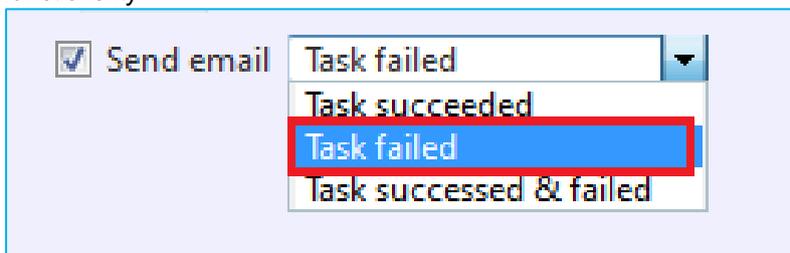


- **Send Email**

Enable this option to receive status emails for each task based on the task's completion status (i.e., **[Task succeeded]**, **[Task failed]**, **[Task succeeded or failed]**).

If you select the **[Task failed]** option, the system will only send you an email if the backup task fails.

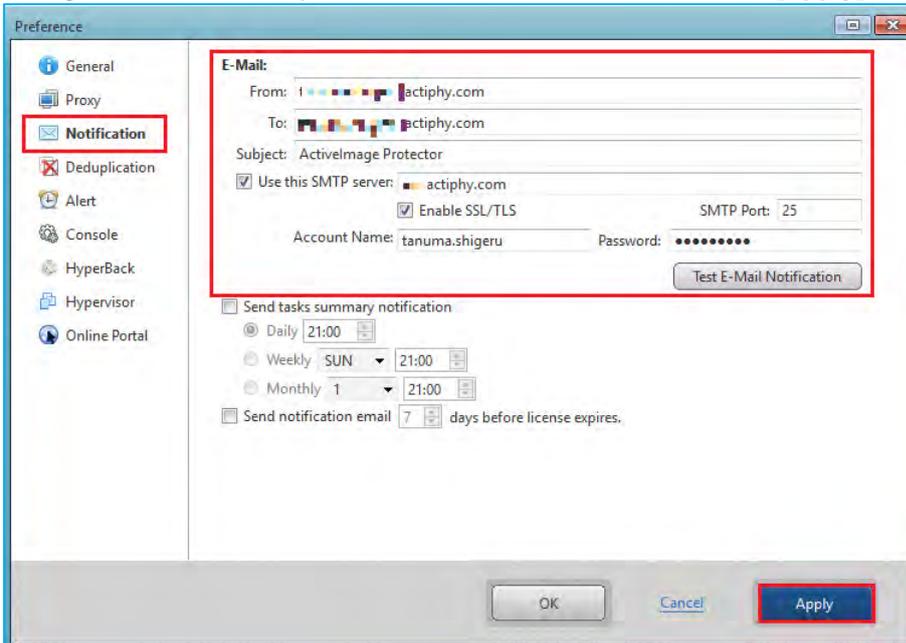
You must configure your email settings in **[Preference]** → **[Notification]** before using the **[Send Email]** functionality.



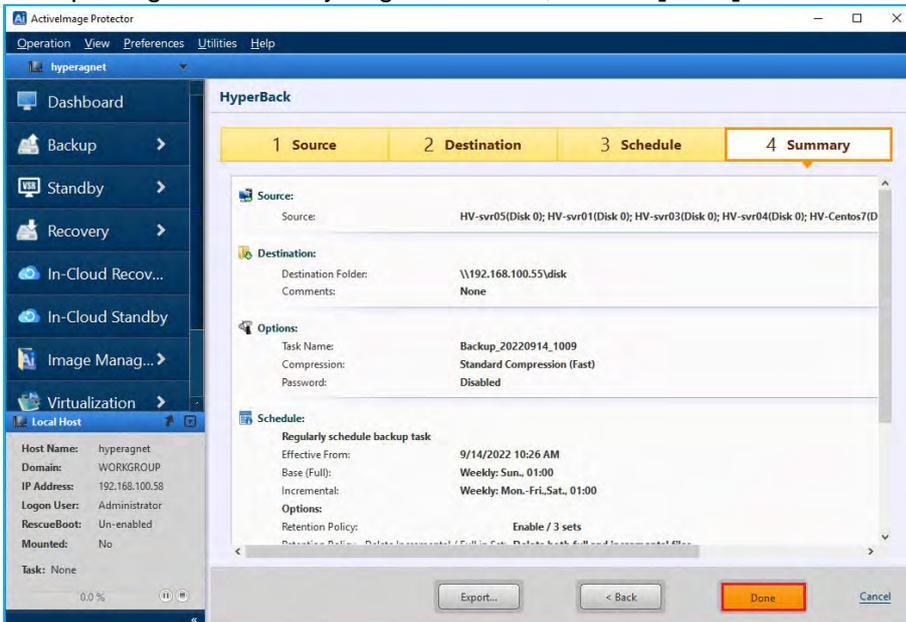
• **Email Setting**

To configure your email settings, go to **[Preferences]** → **[Notification]**.

After configuring your email settings, click the **[Test Email Notification]** button to ensure your email notification settings are correct. Once you have received the test email, click the **[Apply]** button to save your configuration.

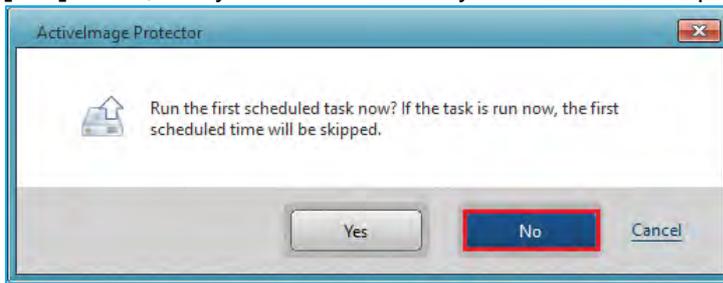


11. After setting up your backup schedule, you should see a summary of your configuration. Please review your backup configuration. If everything looks correct, click the **[Done]** button.

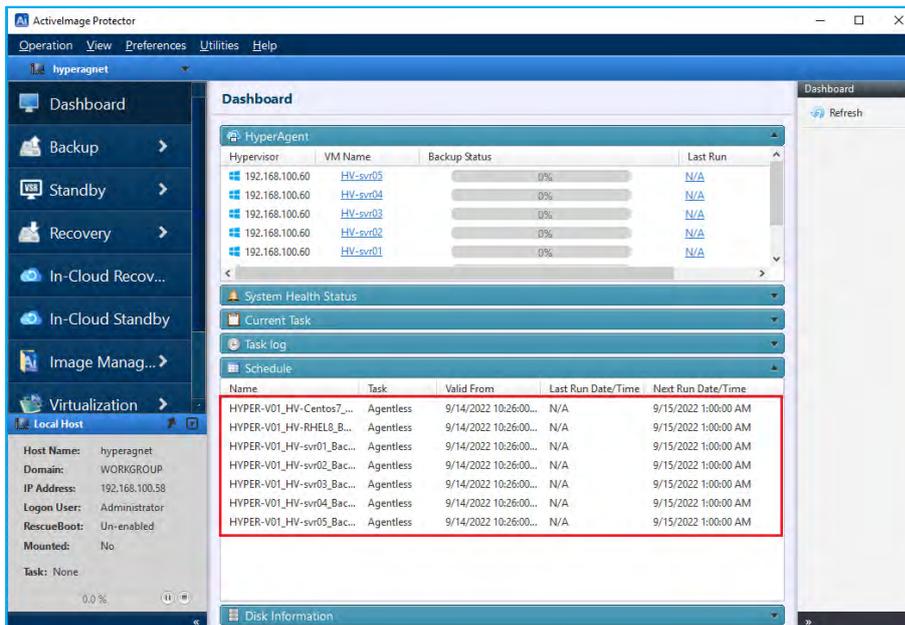


Configure backup settings and run backup tasks

12. Next, you'll see a dialog asking if you want to run the initial backup now. If you click the **[No]** button, the system will take you back to the Dashboard, and your initial backup will run according to your schedule. If you click the **[Yes]** button, the system will immediately run the initial backup and skip the first scheduled backup.



13. Go to **[Dashboard]** → **[Schedule]** to modify or monitor your scheduled tasks. Backup tasks will run according to the schedule.

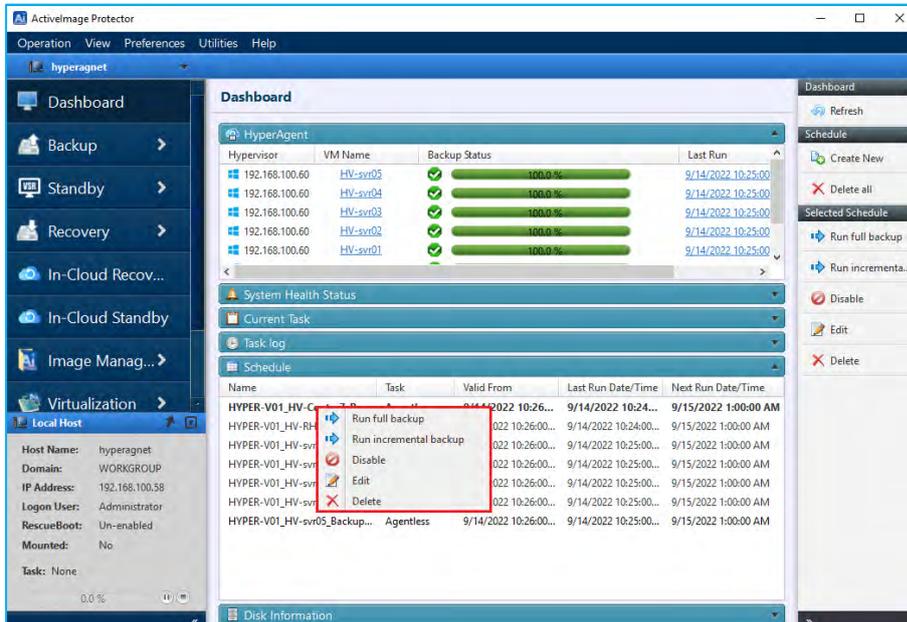


Name	Task	Valid From	Last Run Date/Time	Next Run Date/Time
HYPER-V01_HV-Centos7_...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-RHEL8_B...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-svr01_Bac...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-svr02_Bac...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-svr03_Bac...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-svr04_Bac...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM
HYPER-V01_HV-svr05_Bac...	Agentless	9/14/2022 10:26:00...	N/A	9/15/2022 1:00:00 AM

Configure backup settings and run backup tasks

14. If you right-click on the name of your schedule, you can use the drop-down menu to:

- Immediately run a full backup task.
- Immediately run an incremental backup task.
- Disable the schedule.
- Edit the schedule.
- Delete the schedule.



15. Option settings for HyperBack

Go to **[Preferences]** → **[HyperBack]** and configure the option settings for HypeBack.



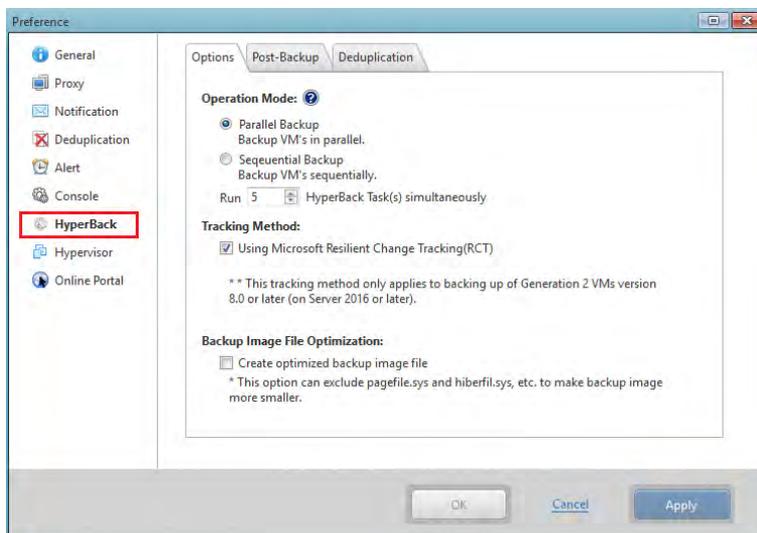
• Operation Mode

Select one of the two operation mode options, i.e., **[Parallel Backup]** or **[Sequential Backup]**.

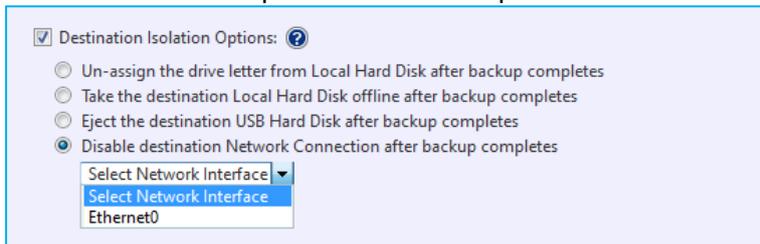
When **[Parallel Backup]** is enabled, specify the concurrently executable number of HyperBack tasks. If the system resources of your HyperAgent computer or your network resources are insufficient, we recommend you select **[Sequential Backup]**.

• Tracking Method

Enable the **[Using Microsoft Resilient Change Tracking (RCT)]** option for the change tracking method to take incremental backups. When this option is selected, the checkpoint does not remain after completing the processing. This tracking method can be applied only to the backups of Generation 2 VMs (Windows Server 2016 or later). If not, the system uses ActiPhy's proprietary tracking method to take incremental backups.



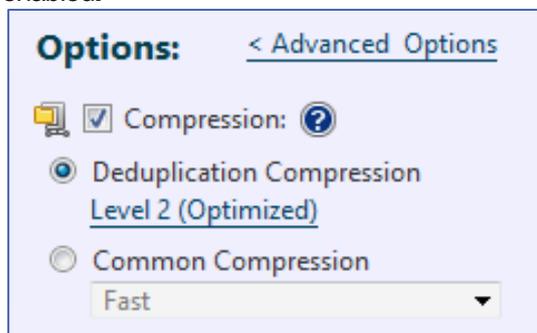
- Configure Destination Isolation Options settings. Enabling the **[Destination Isolation Options]** causes the system to disconnect network access to the backup image's storage drives or sets the destination disk offline once the backup task is complete. The **[Destination Isolation Options]** feature protects the backup storage location and the backups stored there from potential malware or ransomware attacks.



- Configure Option settings.

- Compression**

ActiveImage Protector provides two types of compression: **[Standard Compression]** and **[Deduplication Compression]**. The compression ratio differs depending on the type of compression you choose. The **[Standard Compression]** option will produce a backup image around 70% of the size of the backup source. The **[Deduplication Compression]** option will produce backup images around 50% of the size of the backup source. When selecting **[Deduplication Compression]**, **[Level 2 (Optimized)]** and **[Change temp file folder]** are enabled.

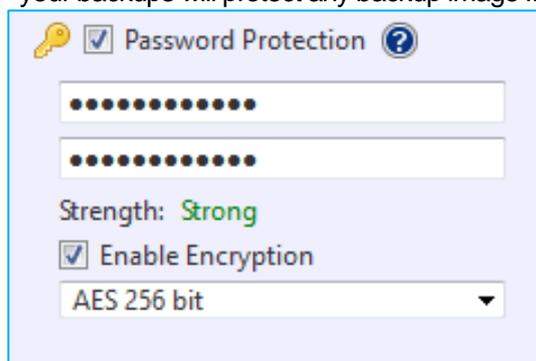


- Password Protection**

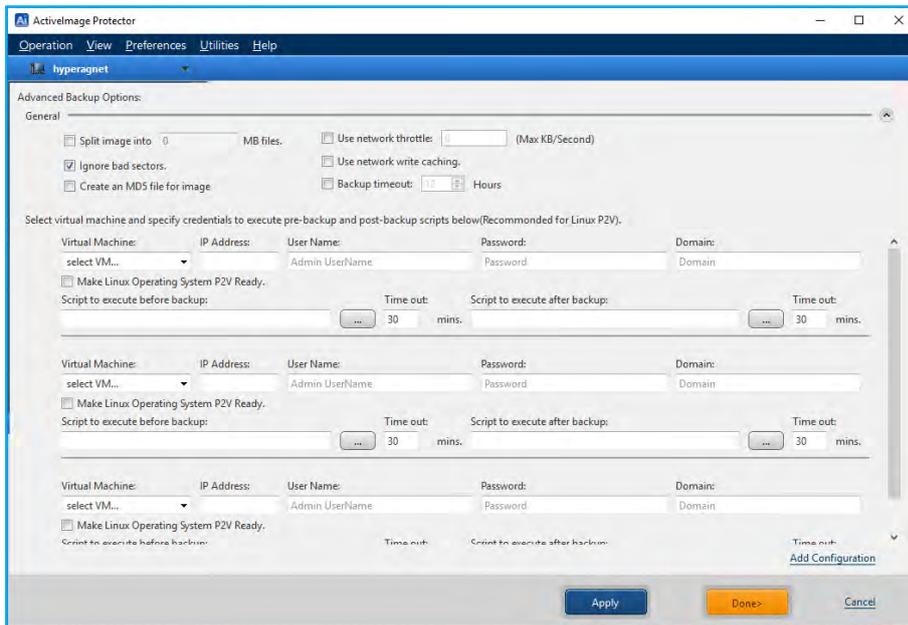
Enabling this option protects the backup image file by assigning a unique password. This additional security prevents anyone from mounting, exploring, or restoring the image file without a password.

- Enable Encryption**

There are three levels of encryption to choose from: "RCS," "AES128 bit", and "AES256 bit." Encrypting your backups will protect any backup image files you save to a remote location from cyber attacks.

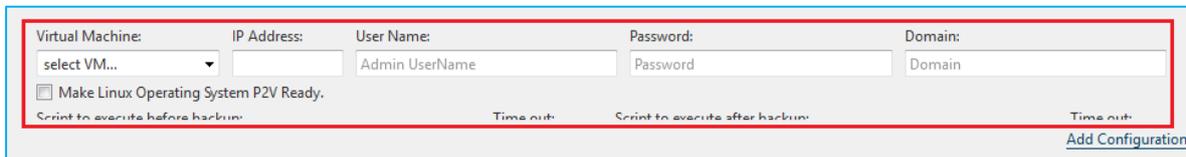


18. Advanced Backup Options. The Advanced Backup Options section contains **[Split image into xx MB files]**, **[Use network throttle xx (Max KB/Second)]**, **[Use network write caching]**, **[Make backup image file P2V ready]** and **[Scripting]**. The following describes **[Scripting]**.



• **[Scripting]**

You can write scripts to run before and after Activelmage Protector creates snapshots or backups. For example, when backing up non-VSS-savvy databases, you need to stop the service before starting the backup task to maintain the integrity of the data. Therefore, you can specify a script or batch file to stop the database service before Activelmage Protector takes a snapshot and then start it again once the backup is complete.

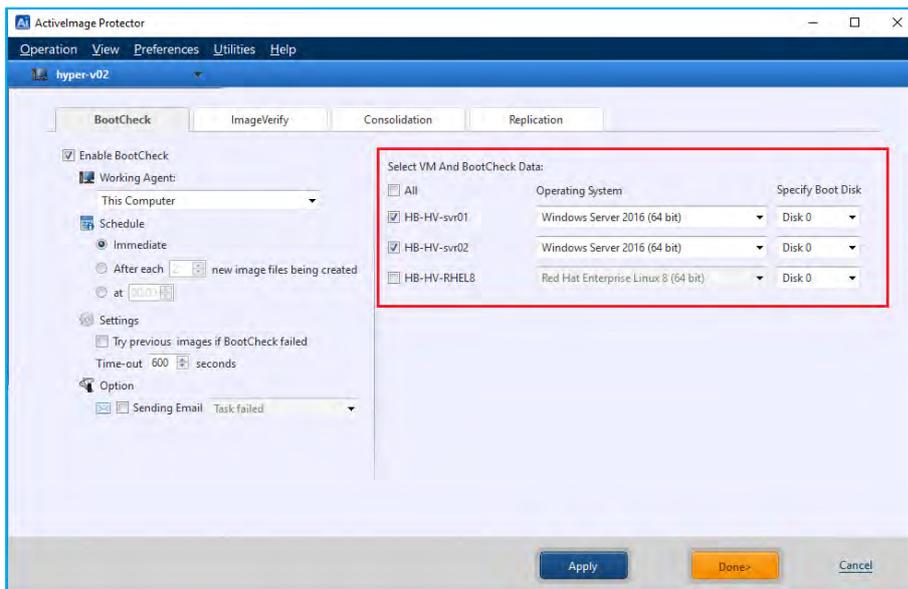


19. Post-backup Process. The Post-backup process is executed upon completion of a backup task or at a specified time. You can select an option for Post-backup Process, i.e., **[BootCheck]**, **[Image Verify]**, **[Consolidation]**, or **[Replication]**.

- **BootCheck**

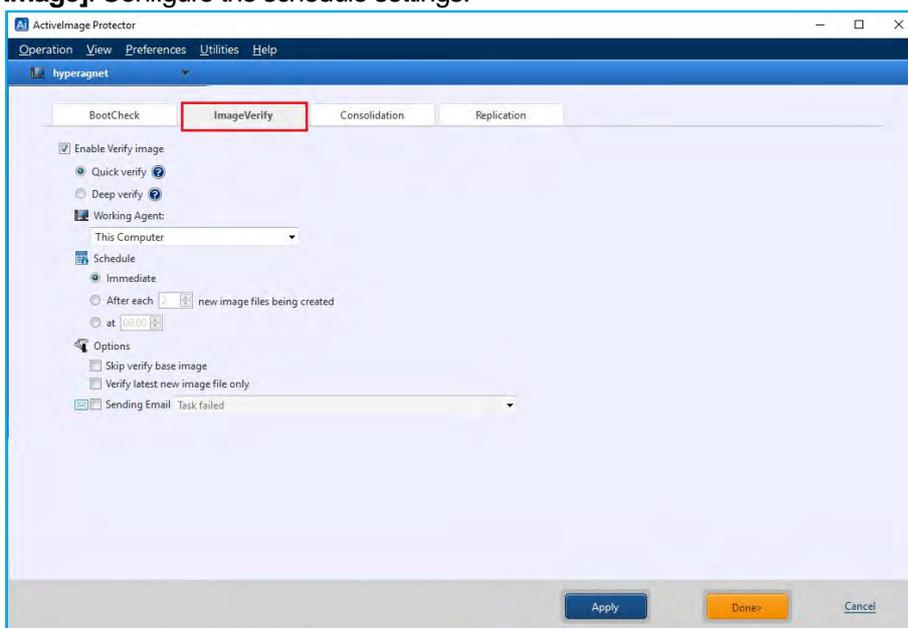
BootCheck quickly tests if a created backup of the system volumes can successfully boot on the selected hypervisor. First, click in the box to enable the **[Enable BootCheck]** option. Next, configure the Schedule settings, Sending Email options, etc.

Note: BootCheck does not support the backup of a Linux virtual machine; therefore, please do not check the checkbox for Linux virtual machine.



- **Image Verify**

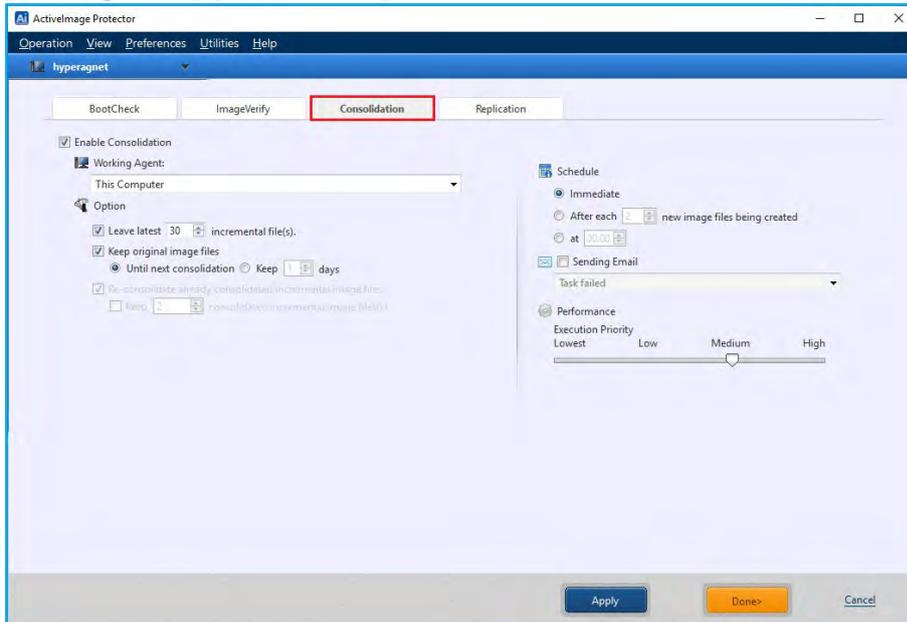
Specify the options and timing to start the ImageVerify process. Click in the box to enable the **[Enable Verify Image]**. Configure the schedule settings.



Configure backup settings and run backup tasks

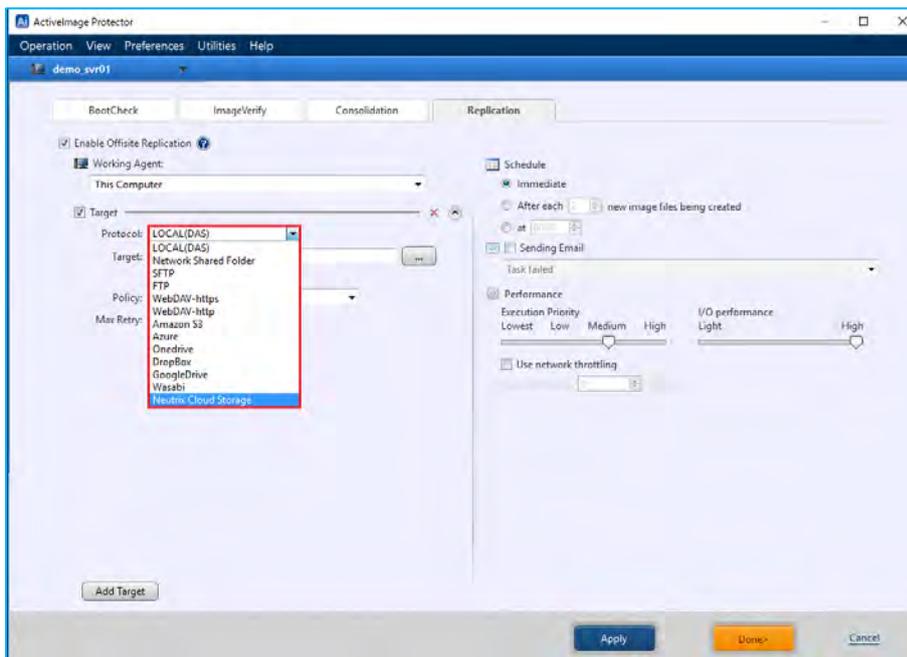
• Consolidation

You can schedule to consolidate the incremental backups into a single backup image set, reducing storage demands. Click in the box to enable the **[Enable Consolidation]** option. Configure the settings for **[Schedule]**, **[Sending Email]**, **[Performance]**, etc.



• Offsite Replication

The Replication feature enables you to replicate backup image files to an offsite storage share, including cloud storage. ActiveImage Protector Replication feature supports local storage, shared folder, WebDAV / FTP, Amazon S3, Azure Storage, OneDrive, Dropbox, Google Drive, Wasabi and Neutrix Cloud.

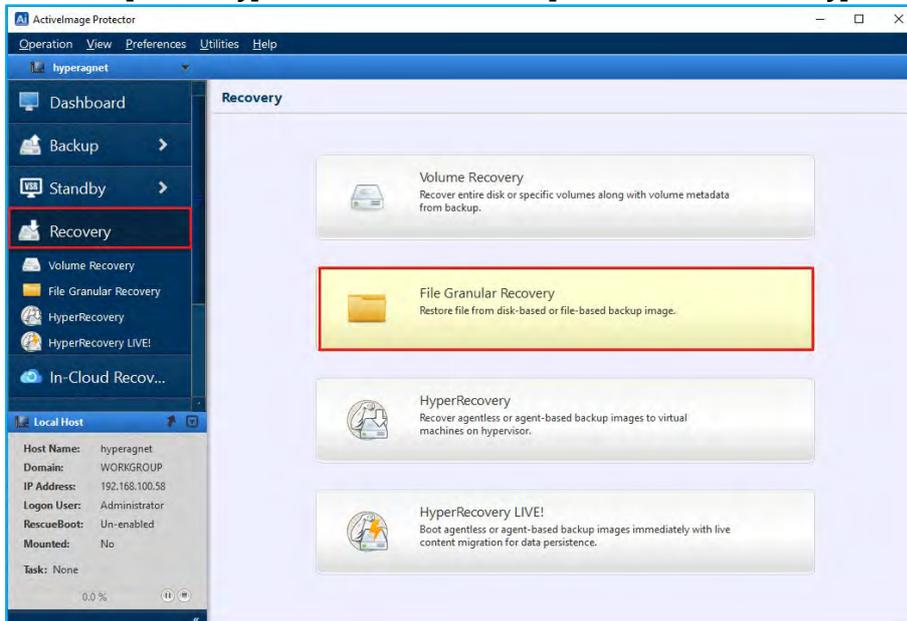


5. Restore

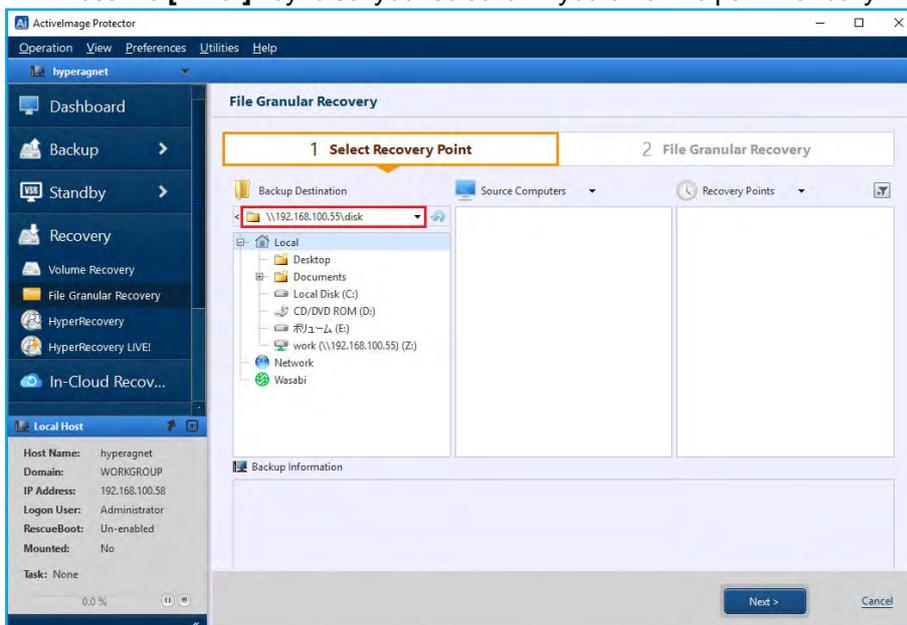
5-1. File / Folder Recovery

Please use the following steps to restore a specific file or folder from a disk backup image:

1. Select the **[Recovery]** menu. Next, click on the **[File Granular Recovery]** button.

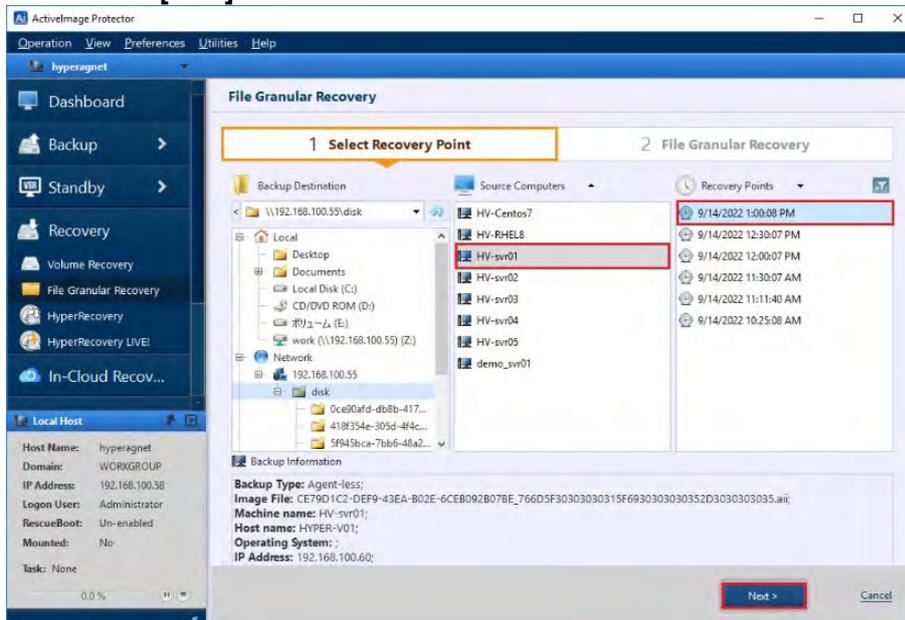


2. Click on the [▼] icon under **[Backup Destination]**.
 - Select the folder containing the backup image file from which you want to restore a file or folder.
 - You can also specify the path to the backup image. In this example, we're using "\\192.168.100.55\disk" as the folder containing our backup image.
 - Press the **[Enter]** key to set your selection if you enter the path manually.



Restore

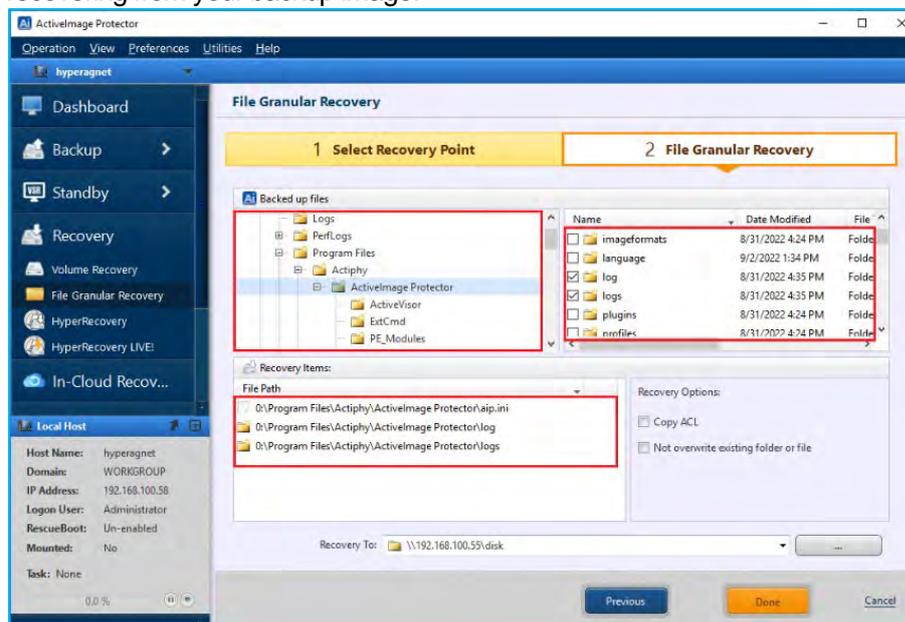
3. Activelmage Protector will populate the **[Source Computers]** list with all the images in the directory you specified.
 - Select the source computer from which you want to restore a file or folder in the list. Activelmage Protector will display information about your selected backup image and recovery point in the **[Backup Information]** section of the screen.
 - Click the **[Next]** button.



4. Now, click the checkbox next to each file or folder you want to restore in the **[Backed up files]** list. Activelmage Protector will list each item you've selected in the **[Recovery Items]** section of the page. Once you have selected all the files and folders you want to restore from the **[Backup up files]** list, you may choose the following recovery options:
 - Copy the Access Control List data for each file and folder by clicking on the checkbox next to **[Copy ACL]**.
 - Prevent Activelmage Protector from overwriting existing files during recovery by clicking on the checkbox next to **[Not overwrite existing folder or file]**.

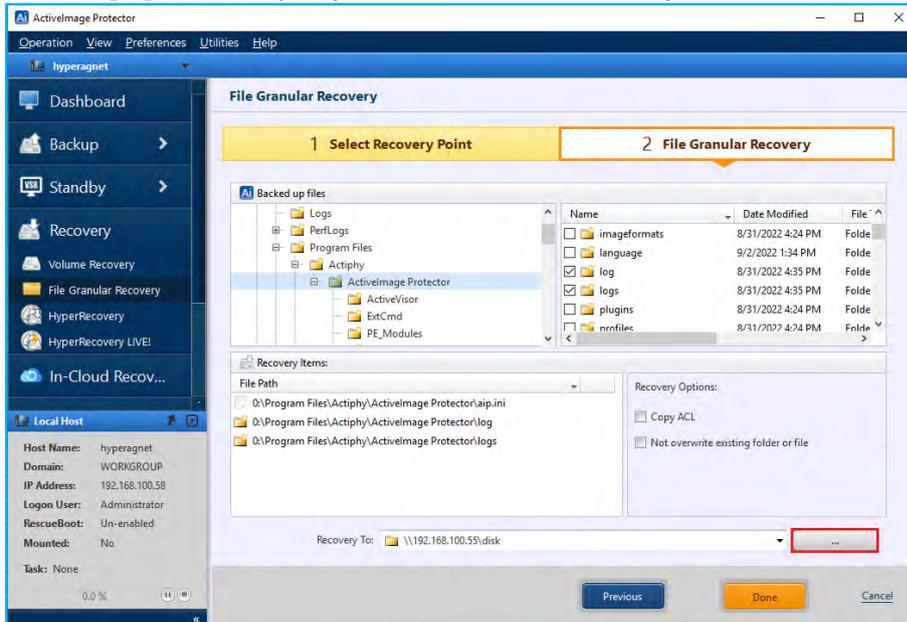
[Copy ACL] will copy the Access Control List data from the backup image to the recovered file or folder.

If **[Not overwrite existing folder or file]** is selected, Activelmage Protector will safely recover your selected files without overwriting existing files and folders. If you don't choose this option, Activelmage Protector will overwrite any files or folders on your computer that have the same name as the files and folders you are recovering from your backup image.

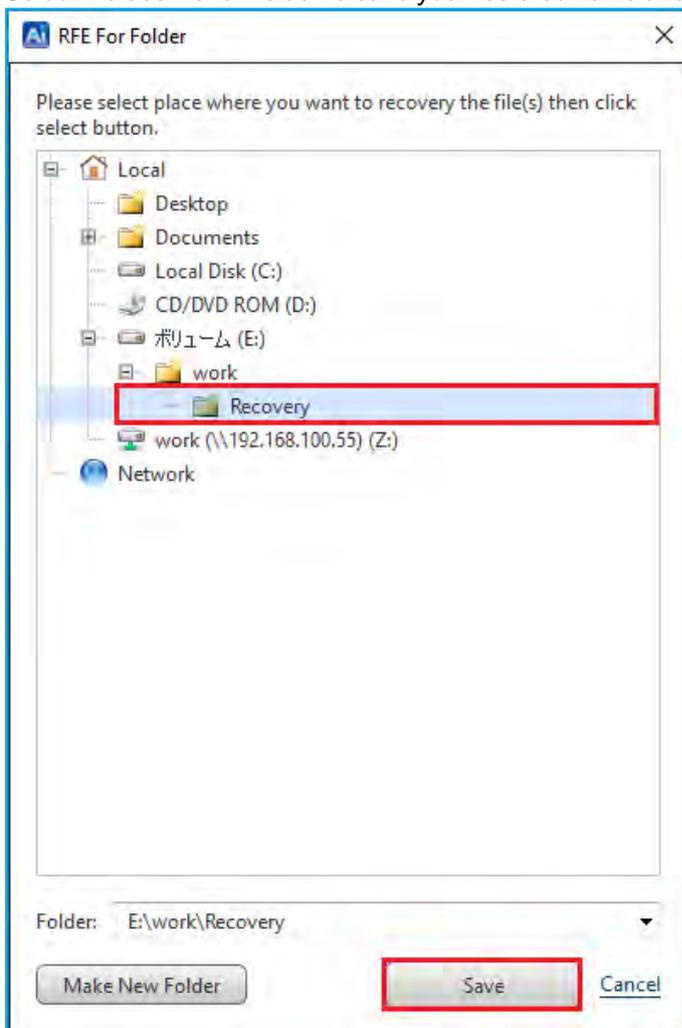


Restore

5. Click the [...] button to specify a destination folder to save your restored items.

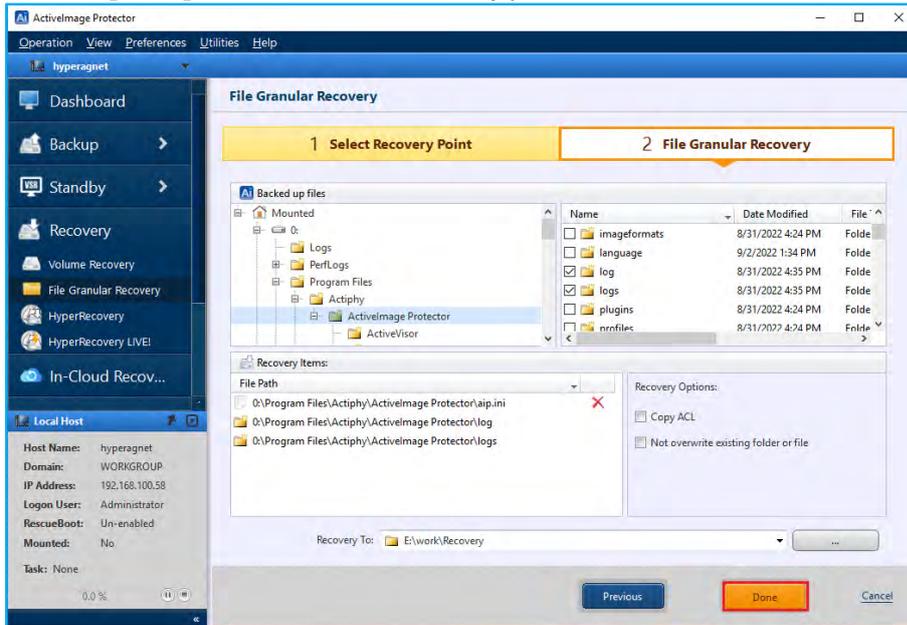


6. Select the destination folder to save your restored items and click **[Save]**.

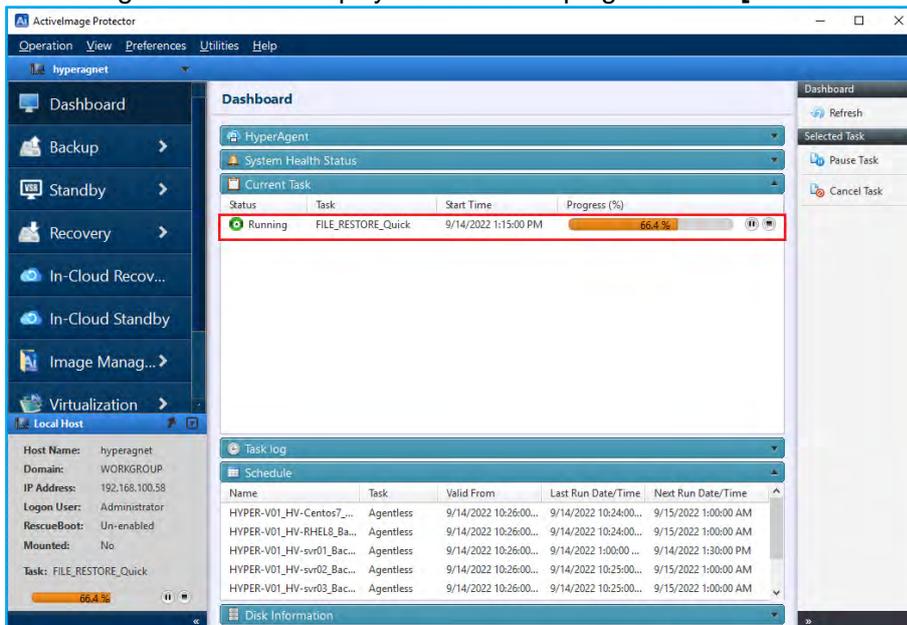


Restore

Click the **[Done]** button to start the recovery process.

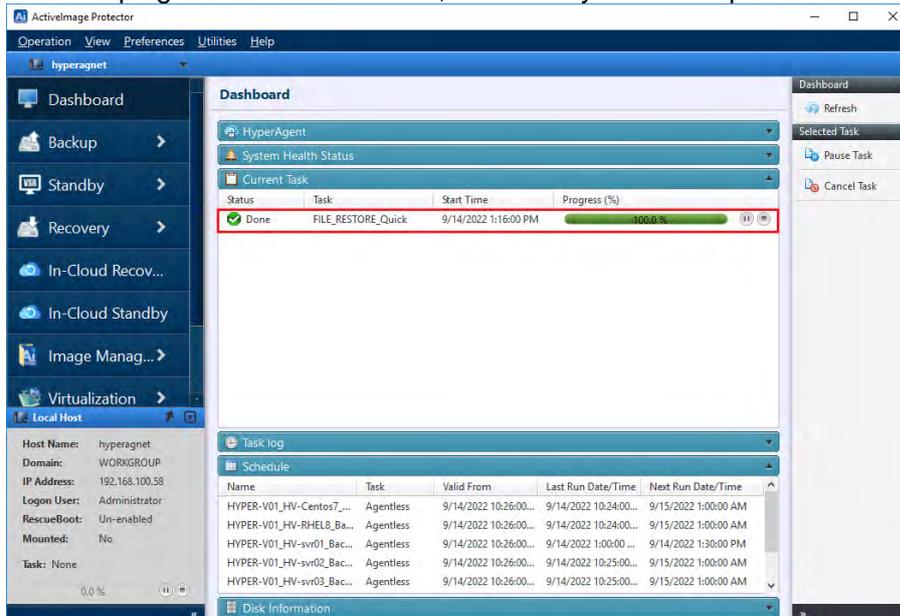


7. ActiVImage Protector will display the restoration progress in the **[Current Task]** section.

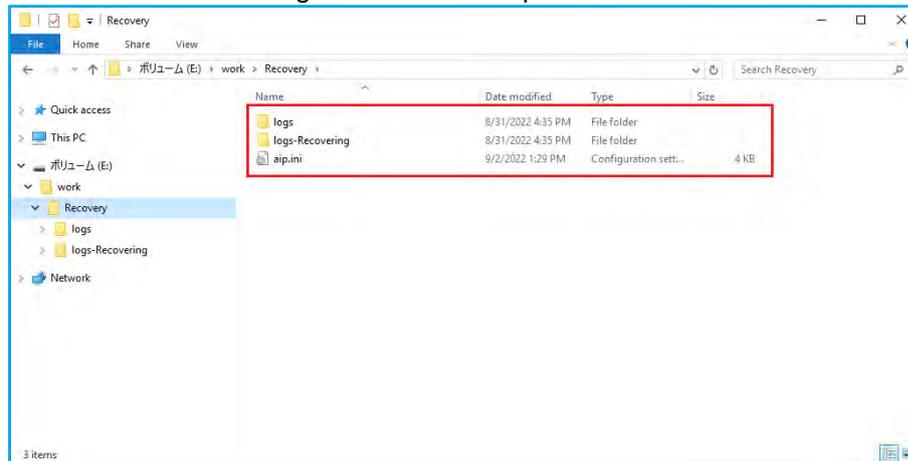


Restore

8. Once the progress bar reaches 100%, the recovery task is complete.



9. The restored files/folders get restored to the specified destination folder.



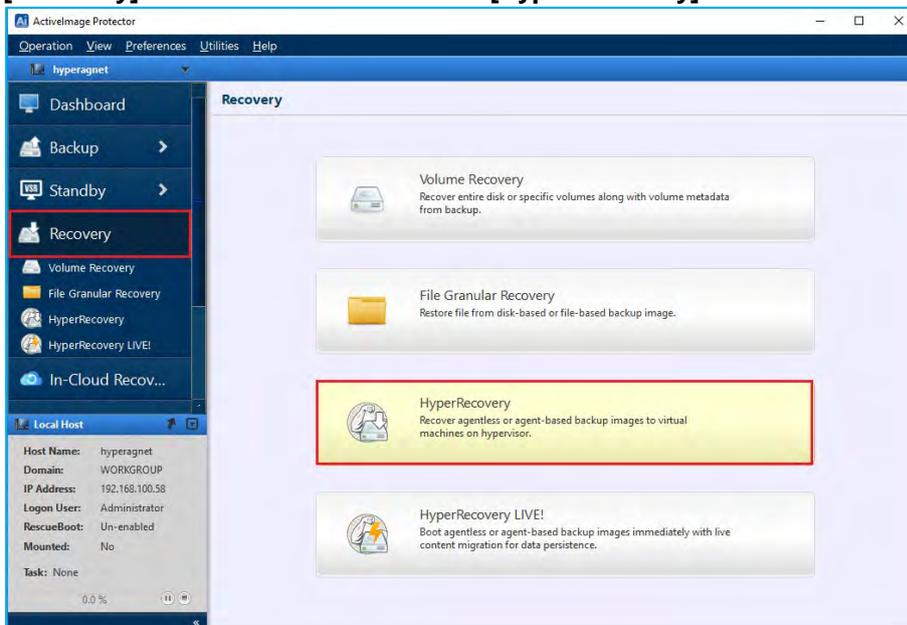
5-2. Restore a backup as a virtual machine (HyperRecovery)

Using HyperRecovery you can restore a backup image file as a virtual machine or virtual disk. The supported hypervisors are Microsoft Hyper-V and VMware vSphere vCenter.

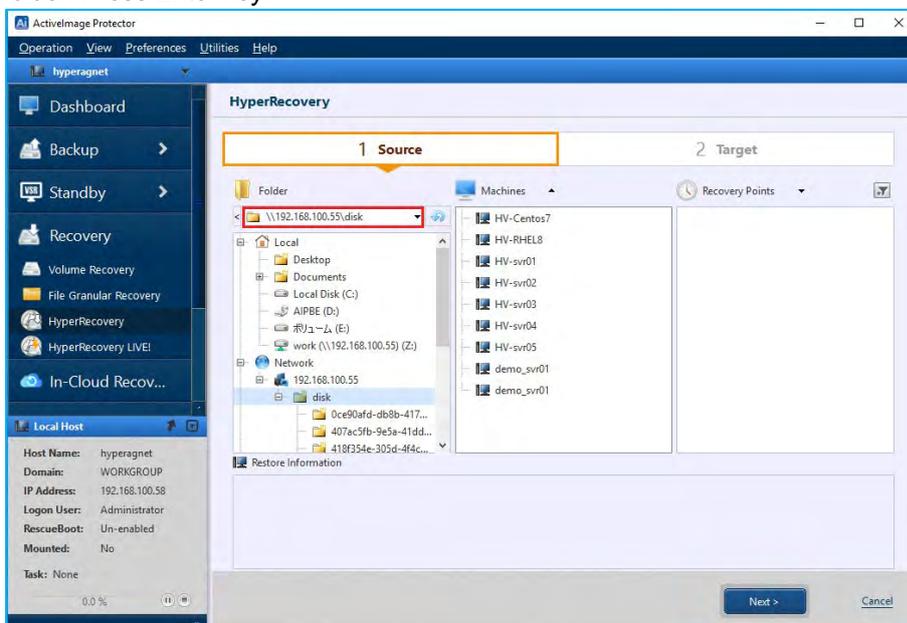
The example below shows the steps to restore as a virtual machine using HyperRecovery.

Note: HyperRecovery does not support restoring agent-based Linux backups with LVMs as virtual machines.

1. Start ActiImage Protector. Go to Windows Start menu - **[Actiphys]** → **[ActiImage Protector]**. Select **[Recovery]** in the console menu and click **[HyperRecovery]**.

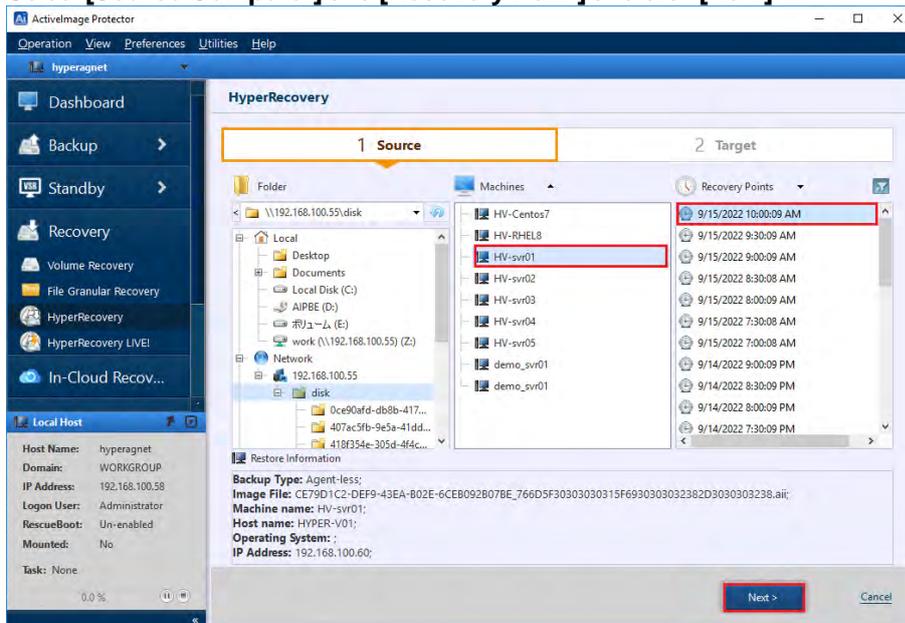


2. Select a folder containing backup image files. Click on the “▼” icon on the right-hand side of the **[Folder]** text box to select a location. In the following example we will specify “¥¥192.168.100.55¥¥disk”, a network shared folder. Press Enter key.

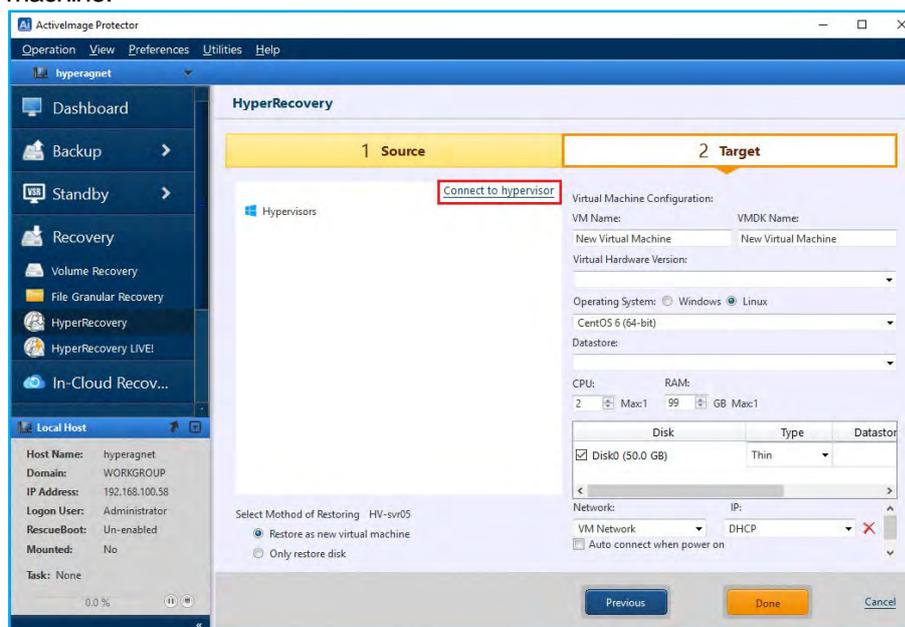


Restore

3. Select **[Source Computer]** and **[Recovery Point]** and click **[Next]**.

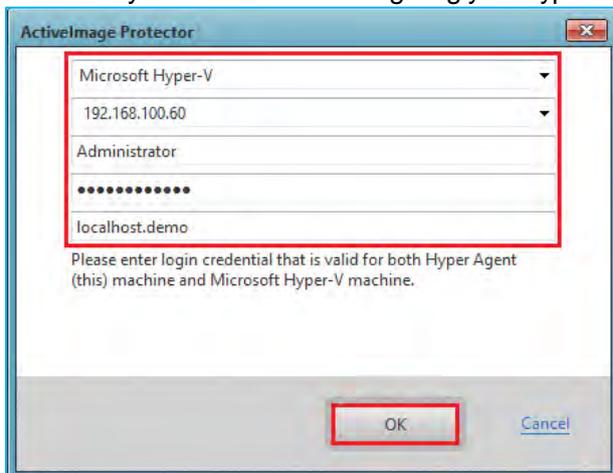


4. Click **[Connect to hypervisor]** to establish the connection to the hypervisor that will host the restored virtual machine.

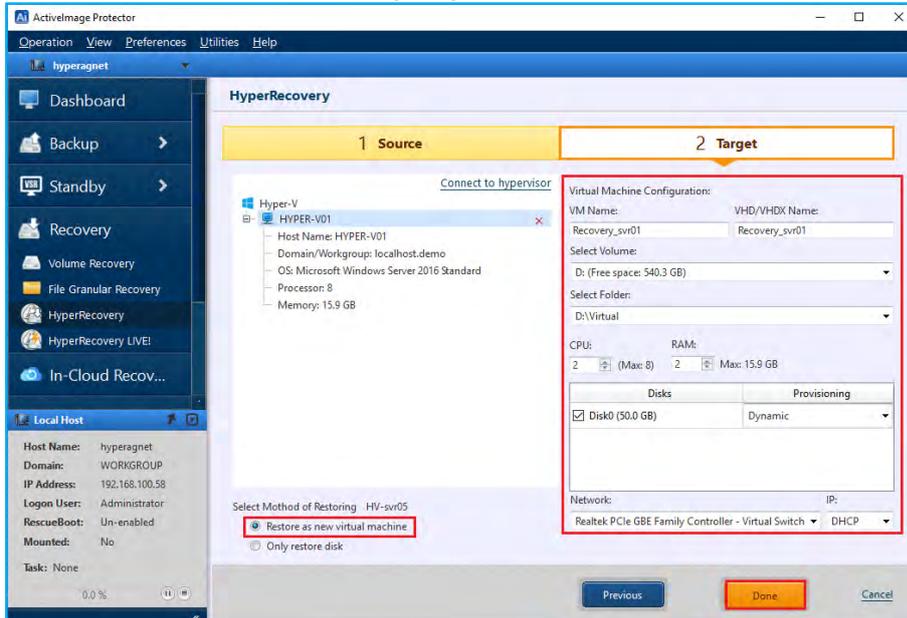


Restore

5. Select the hypervisor type, Microsoft Hyper-V or VMware vSphere (ESXi) and enter your credentials.
 - We have selected "Microsoft Hyper-V" as the hypervisor type in this example.
 - Enter the IP address or hostname of your Hyper-V host. We have entered "192.168.100.60".
 - Enter the username for the hypervisor. For example, "Administrator."
 - Enter the password for your hypervisor.
 - When you have finished configuring your hypervisor, click the **[OK]** button.

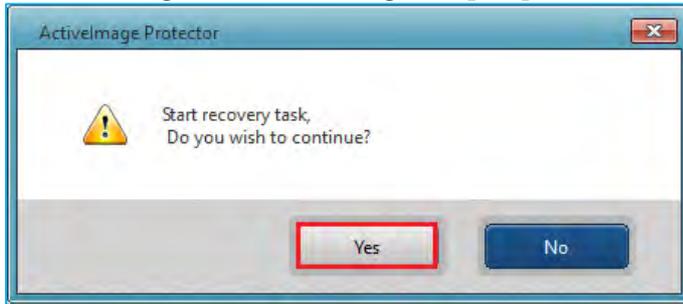


6. Configure the following settings to restore from a backup to a new virtual machine.
 - We have selected **[Restore as new virtual machine]** for **[Select Method of Restoring]**. Configure the following settings in **[Virtual Machine Configuration]**.
 - Enter **[VM Name]**. We have entered "Recovery_svr01" in this example.
 - Enter volume name. For example, "D:" for **[Select Volume]** and "Virtual" for **[Select Folder]**.
 - Enter **[CPU:]**, **[RAM:]** and **[Provisioning]**. We have entered "2" for **[CPU:]**, "2GB" for **[RAM:]** and "Dynamic" for **[Provisioning]**.
 - When you have finished configuring your virtual machine, click the **[Done]** button to start.

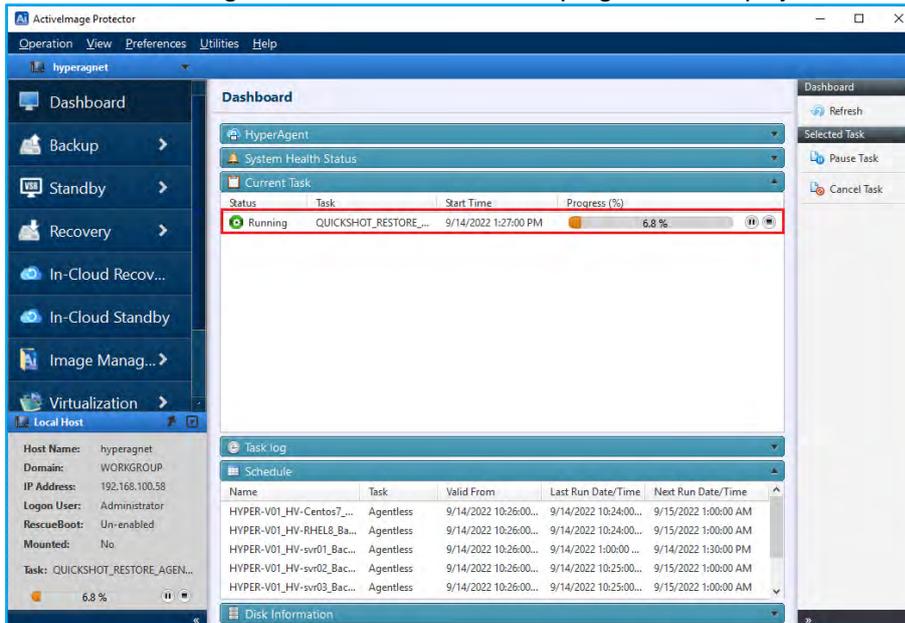


Restore

- In the following confirmation dialog, click **[Yes]**.

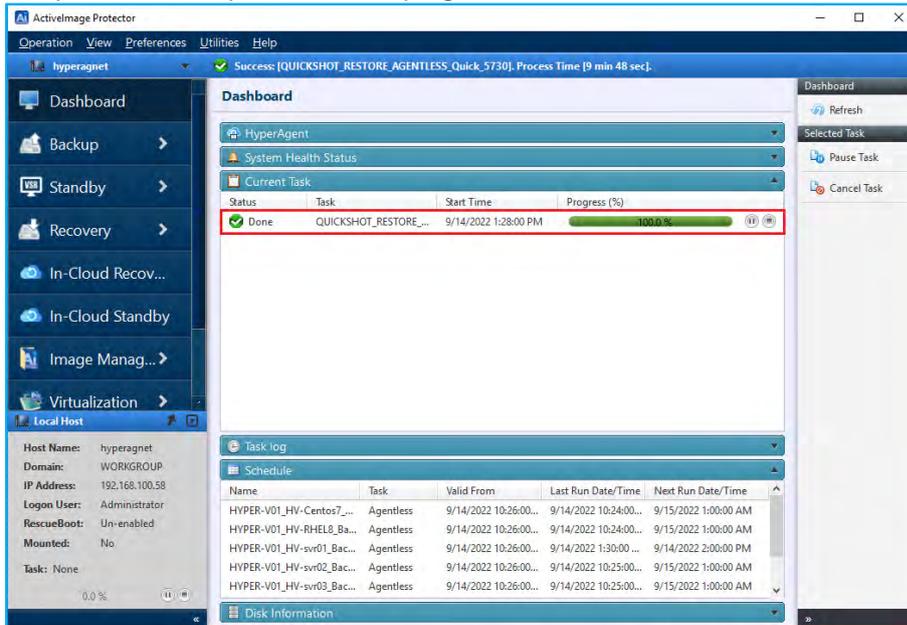


- The task for creating the virtual machine and the progress are displayed.

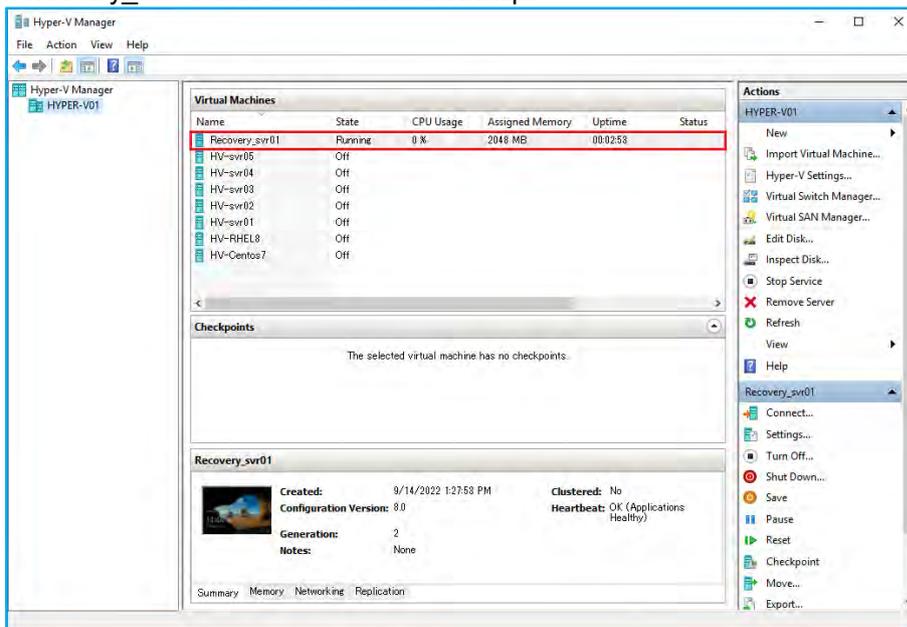


Restore

9. The process is complete when the progress reaches 100%.



10. You can manage the new virtual machine from Hyper-V Manager. In this example, a new virtual machine "Recovery_svr01" was created from a backup.

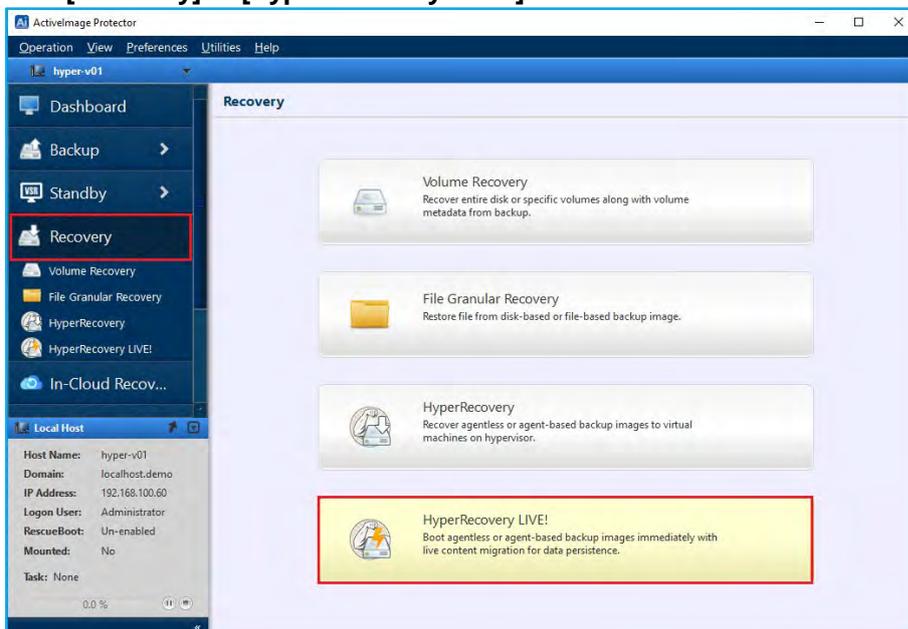


5-3. Zero Time Recovery (HyperRecovery LIVE!)

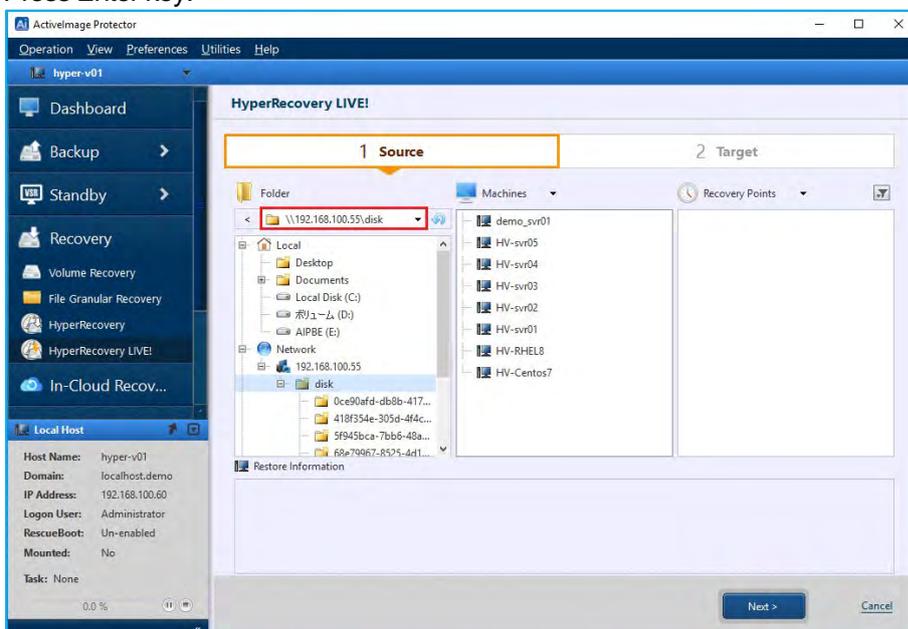
HyperRecovery LIVE! boots a virtual machine from a backup image file on a hypervisor and does a live migration of the system to a virtual machine in the background. The following explains how to use HyperRecovery LIVE! to do a live migration to a virtual machine.

Note: HyperRecovery LIVE! does not support migrations of Linux backup images.

1. Click **[Recovery]** → **[HyperRecovery LIVE!]**.

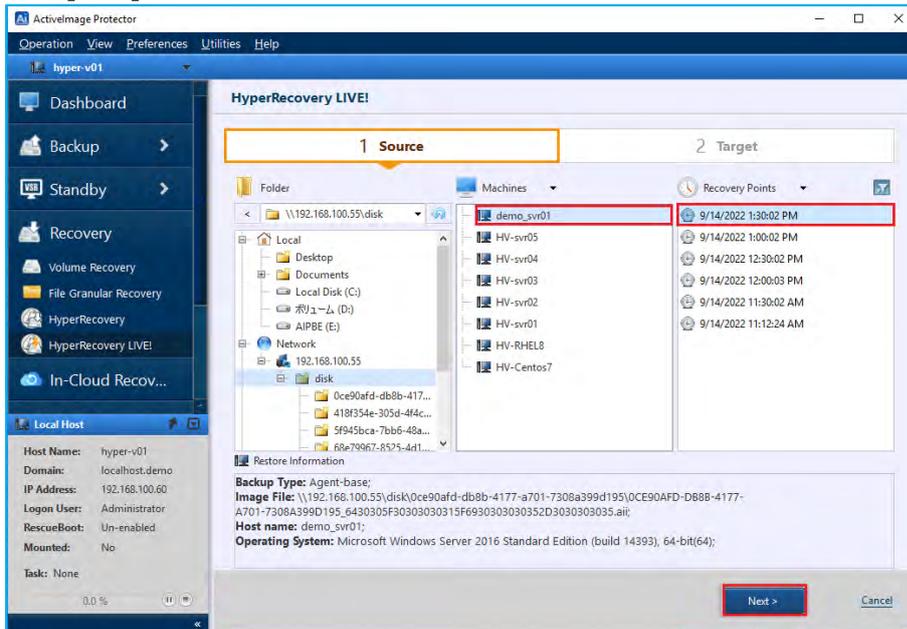


2. Select a folder containing the backup image files. In this example, we have selected the network shared folder \\192.168.100.55\disk. Click **[Select Folder]** or click on the “▼” icon on the right-hand side of the **[Destination folder]** text box to select a location. Press Enter key.

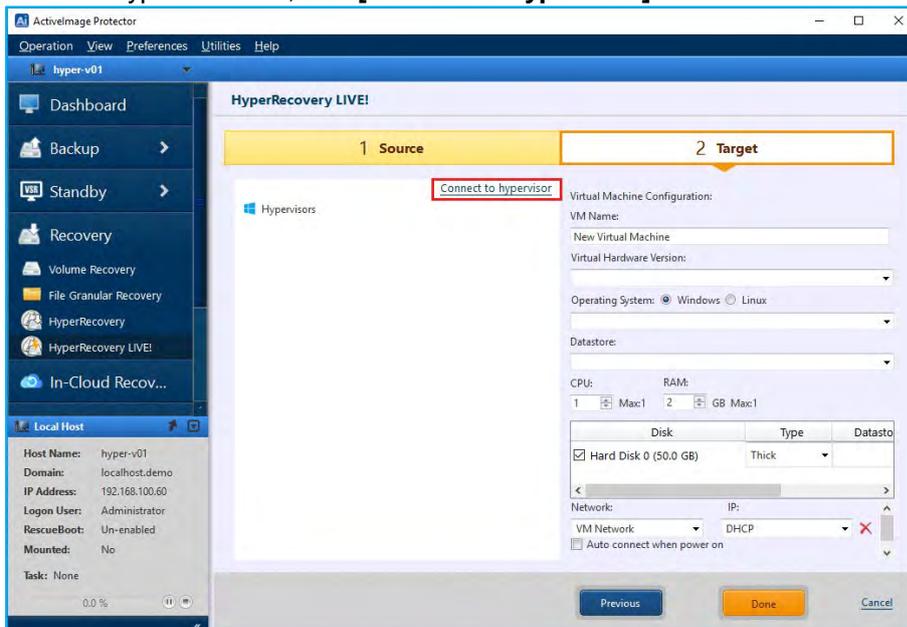


Restore

3. Select a backup source **[Machine]** and **[Recovery Points]**. Click **[Next]**.

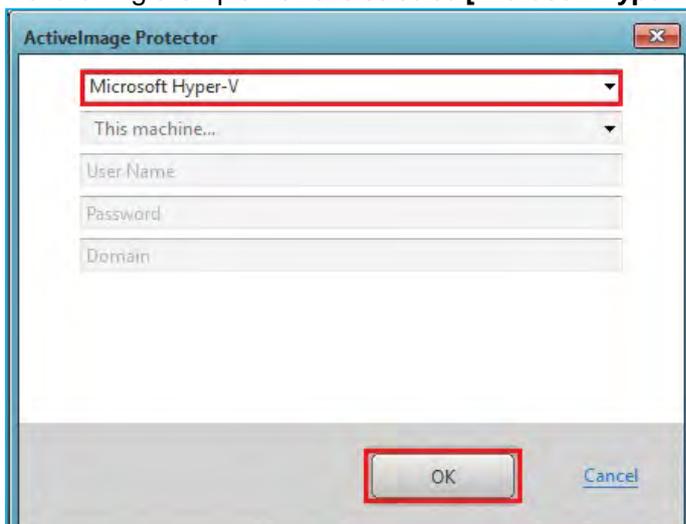


4. To add a hypervisor host, click **[Connect to hypervisor]**.

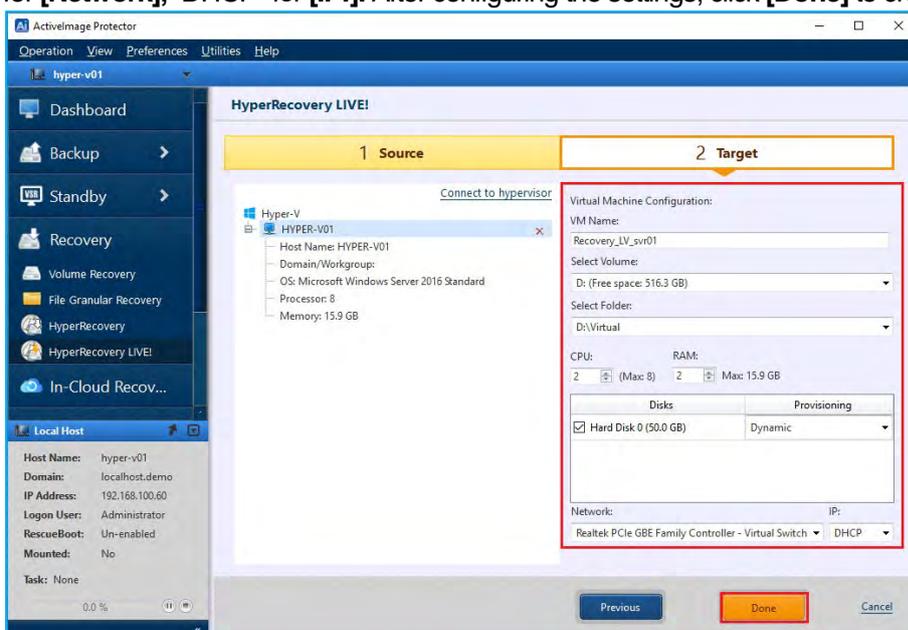


Restore

- Supported hypervisors are Microsoft Hyper-V configured on local computer or VMware vSphere vCenter. In the following example we have selected **[Microsoft Hyper-V]** running on the local computer. Click **[OK]**.

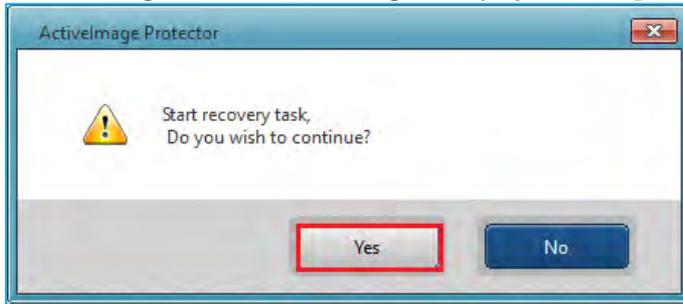


- Configure the setting for the virtual machine. The following example shows settings configured for the new virtual machine. "Recovery_LV_svr01" is specified for **[VM name]**, "D:" drive for **[Volume:]** of datastore, "Virtual" for **[Folder]**, "2" for **[CPU:]**, "2GB" for **[RAM]** and "Dynamic" for [Provisioning], Virtual Switch on the target host for **[Network]**, "DHCP" for **[IP:]**. After configuring the settings, click **[Done]** to create the virtual machine.

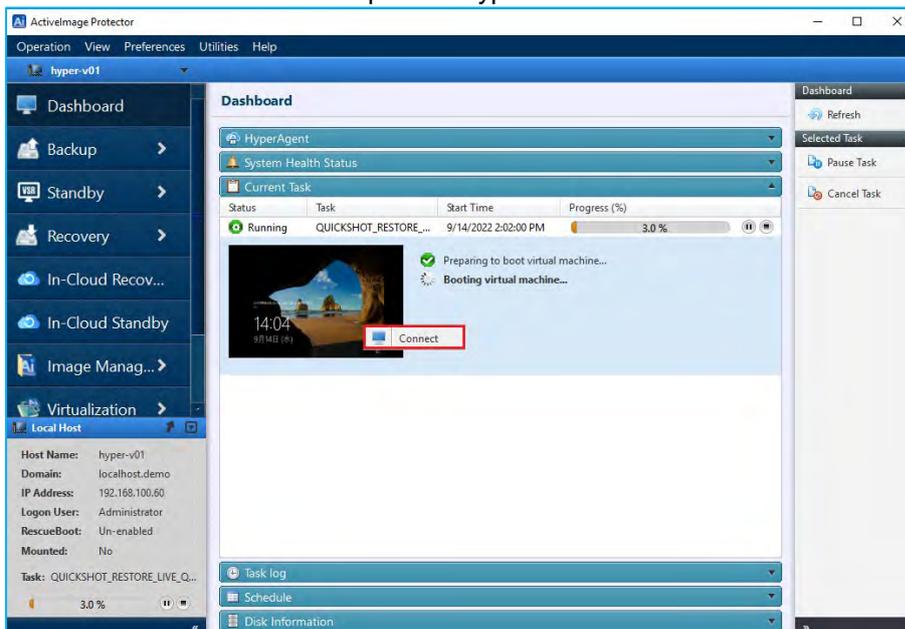


Restore

7. The following confirmation message is displayed. Click **[Yes]**.

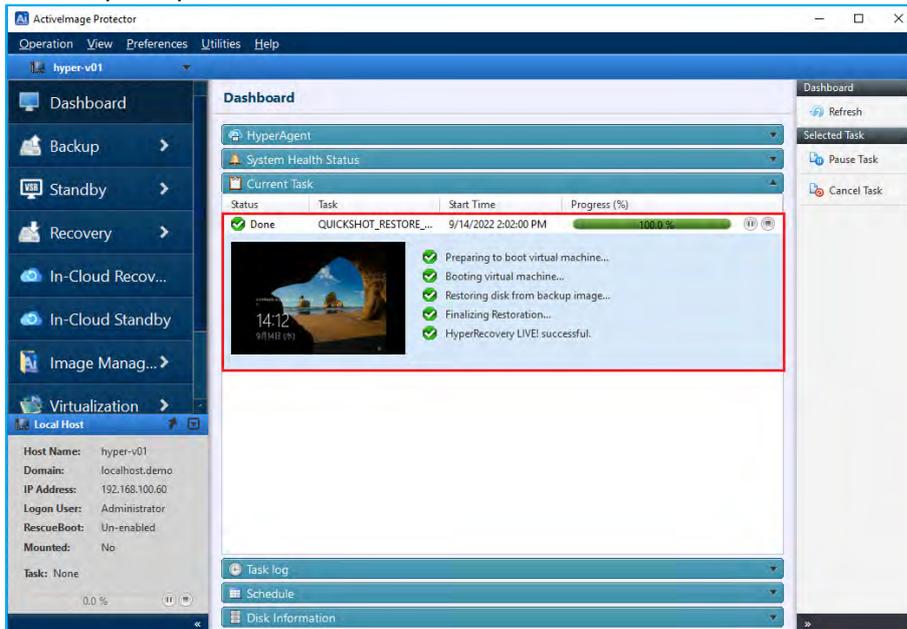


8. When the task starts, the virtual machine will boot. Right-click on the thumbnail and select **[Connect]**. This will connect to the virtual machine via remote desktop console. In background, the backup is restored to the newly created virtual machine on the specified hypervisor.

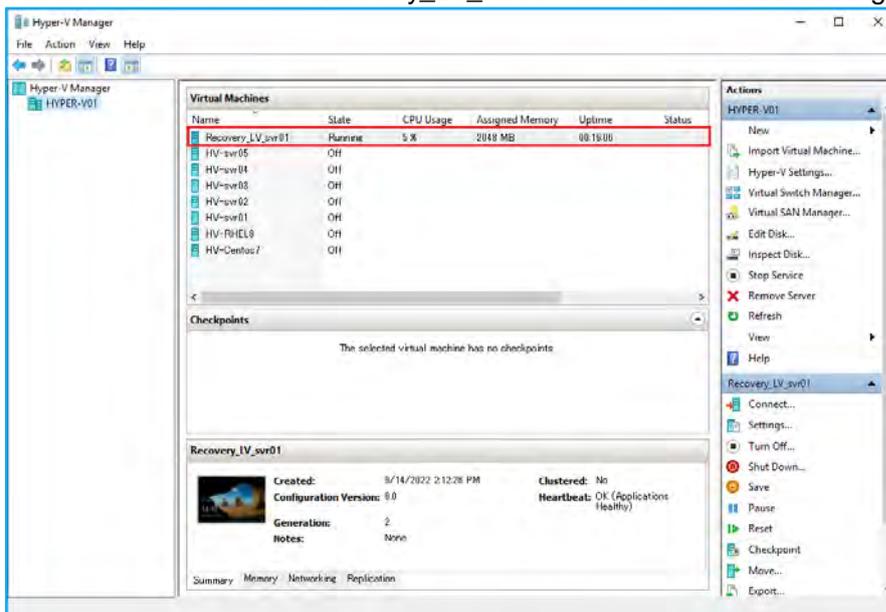


Restore

9. The virtual machine can be used while the machine is being migrated in the background. This allows for uninterrupted operations on the virtual machine.



10. You can manage the virtual machine using the Hyper-V Manager console. In our example, in the dialogue below the virtual machine "Recovery_LV_svr01" was created and is running.

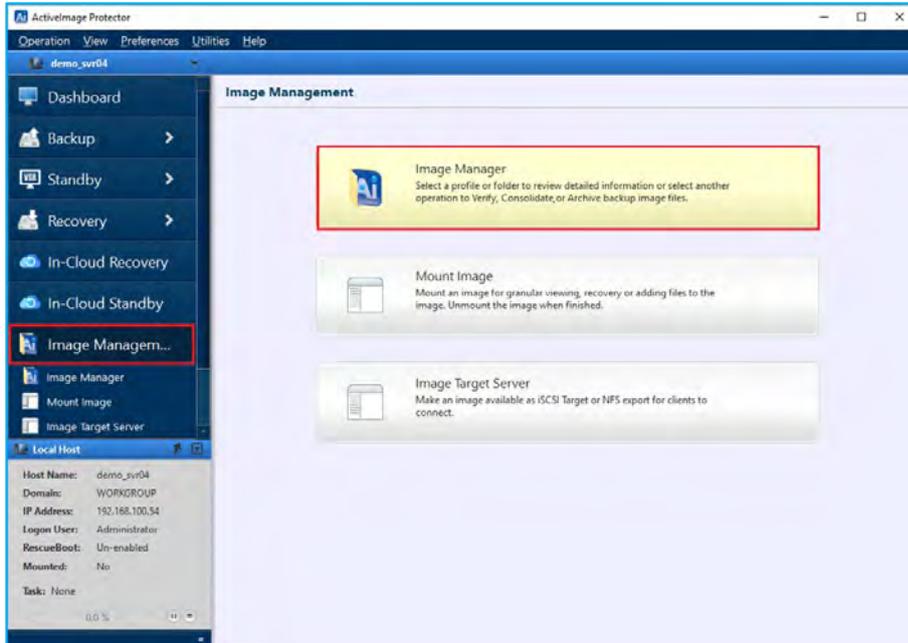


6. Image Management – Image Manager

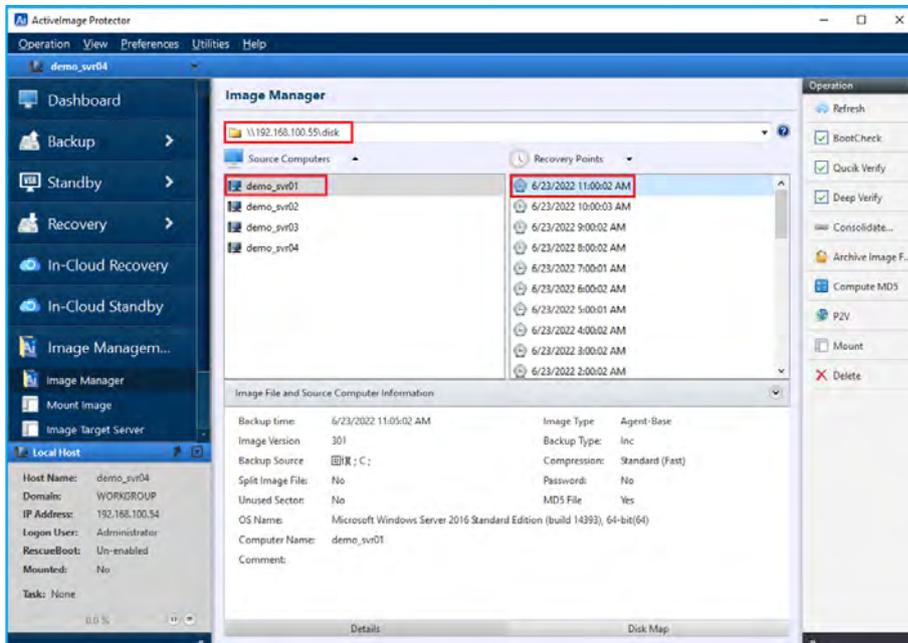
These tools are provided to enable you to manage various operations relating to image files.

6-1. Image Manager

1. Go to **[Image Management]** in the left pane and **[Image Manager]**.



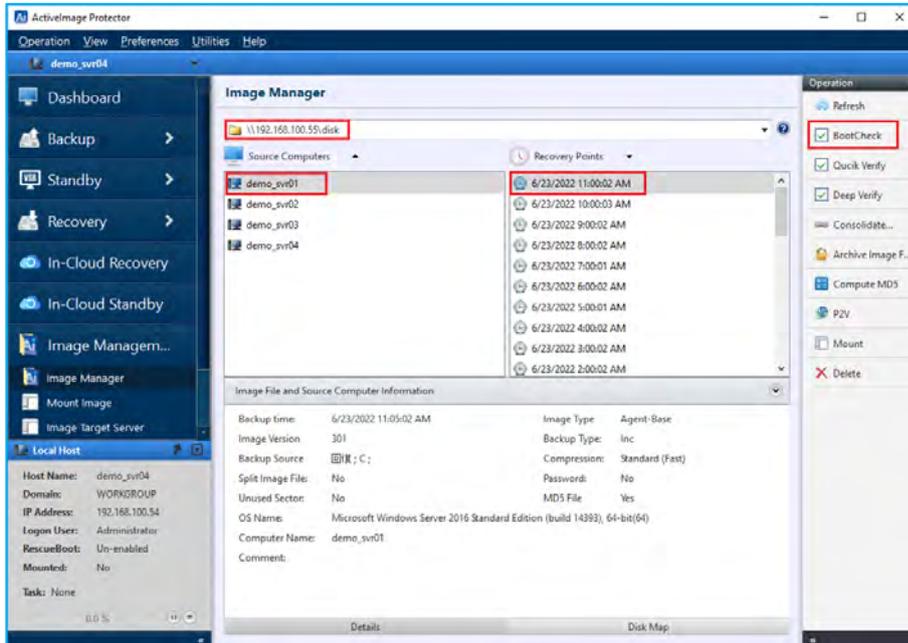
2. Please select a folder where backups are saved. Select **[Source Computer]** and **[Recovery Point]** for the backup to run an image management operation.



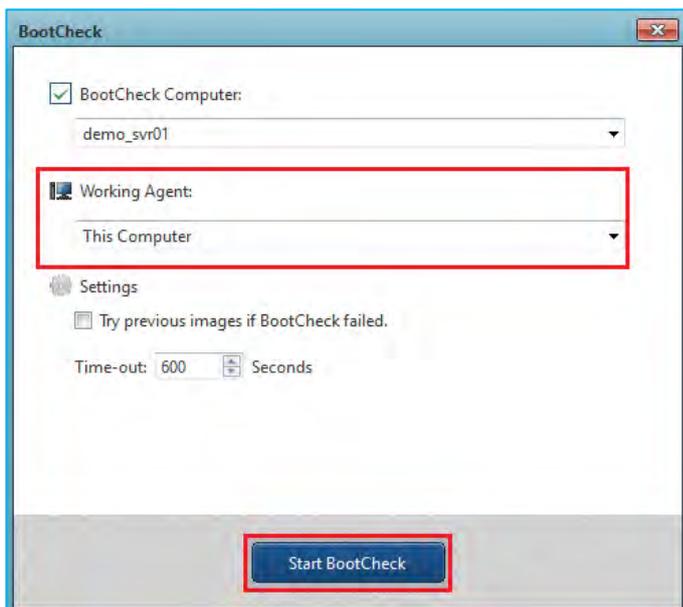
6-2. Check for bootability of backups (BootCheck)

BootCheck tests if the specified backup can successfully boot as virtual machines on a hypervisor.

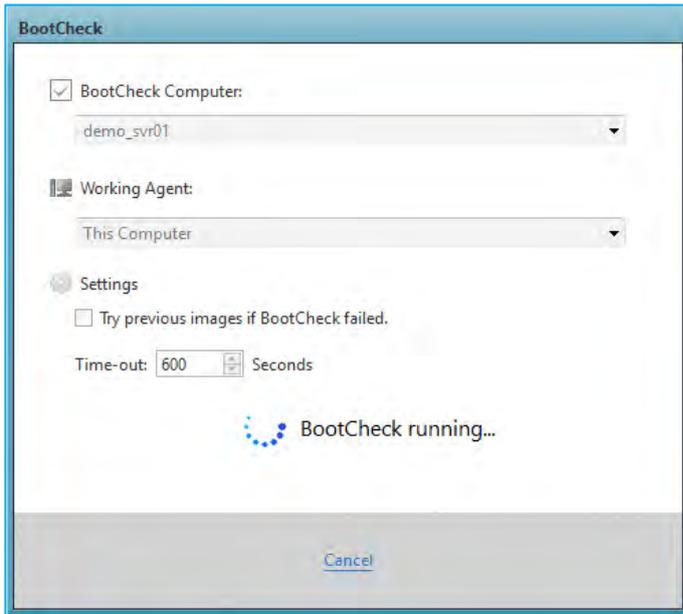
1. Select **[Source Computer]** and **[Recovery Point]** and click **[BootCheck]** in the right pane.



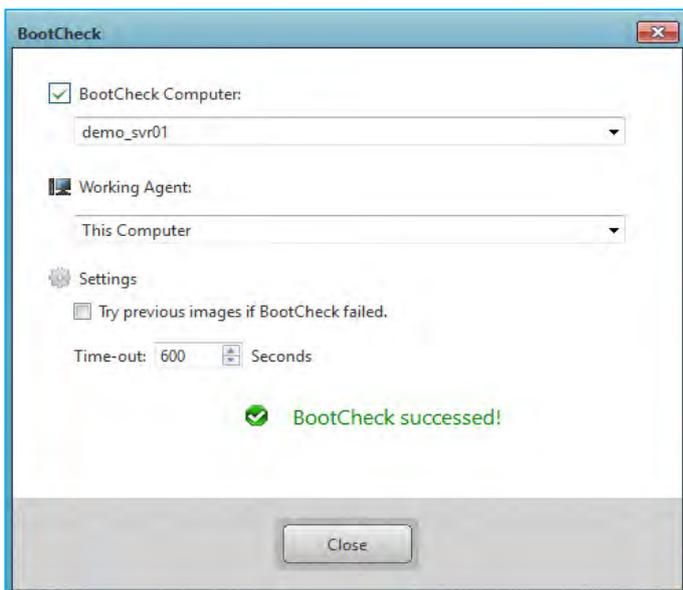
2. In this example, “this computer” (local Hyper-V) is selected as the **[Working Agent:]** (hypervisor for running BootCheck). Click **[Start BootCheck]**.



3. BootCheck is executed for the specified backup.



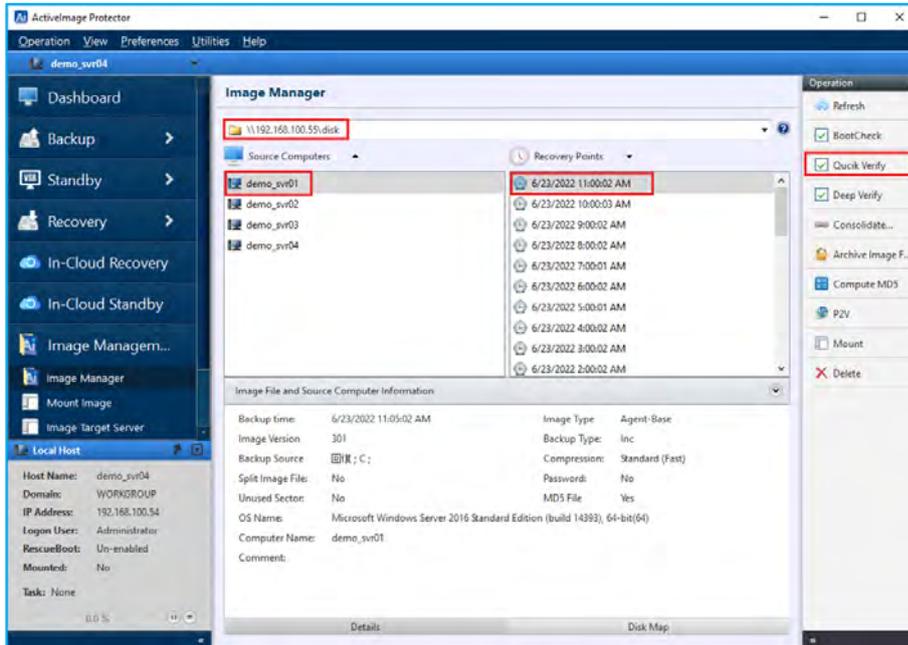
4. Upon completion of BootCheck process, the following window is displayed. BootCheck can be executed at anytime, for example, right before running a backup task.



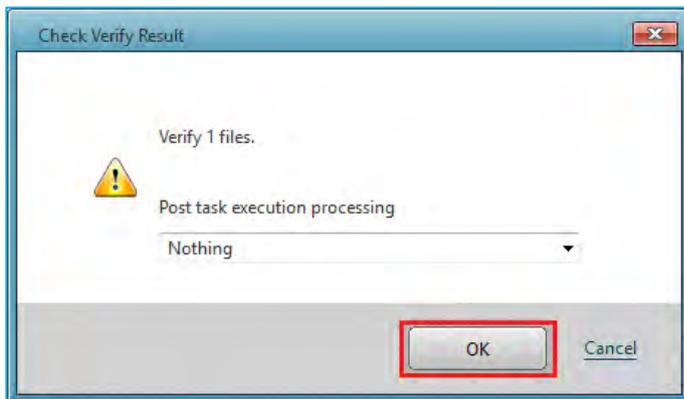
6-3. Quick Verify

Quick Verify ensures that the backup file has not been corrupted since the backup was created.

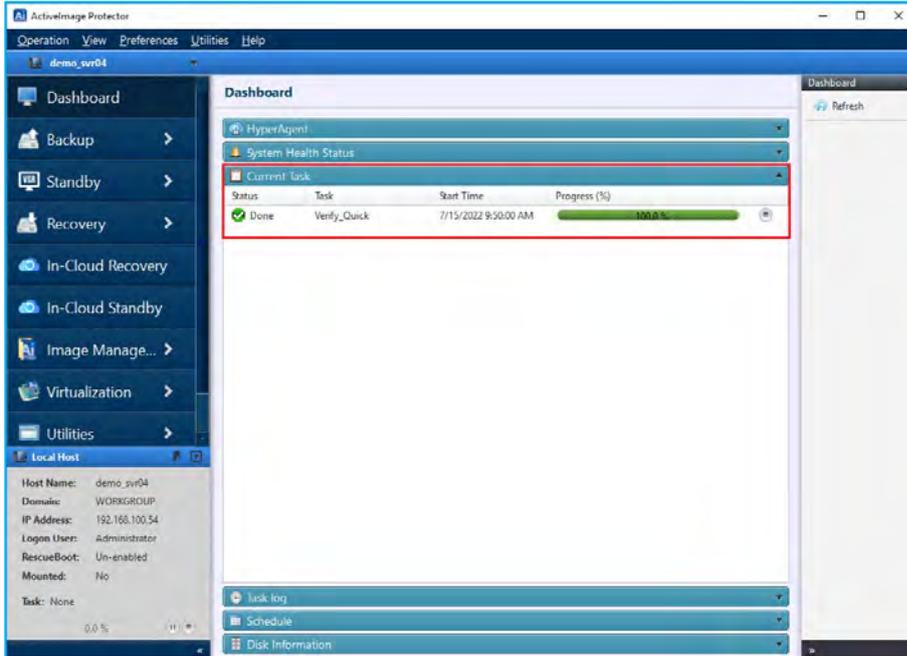
1. Select **[Source Computer]** and **[Recovery Point]** and click **[Quick Verify]** in the right pane.



2. Click **[OK]** and Quick Verify task starts running.



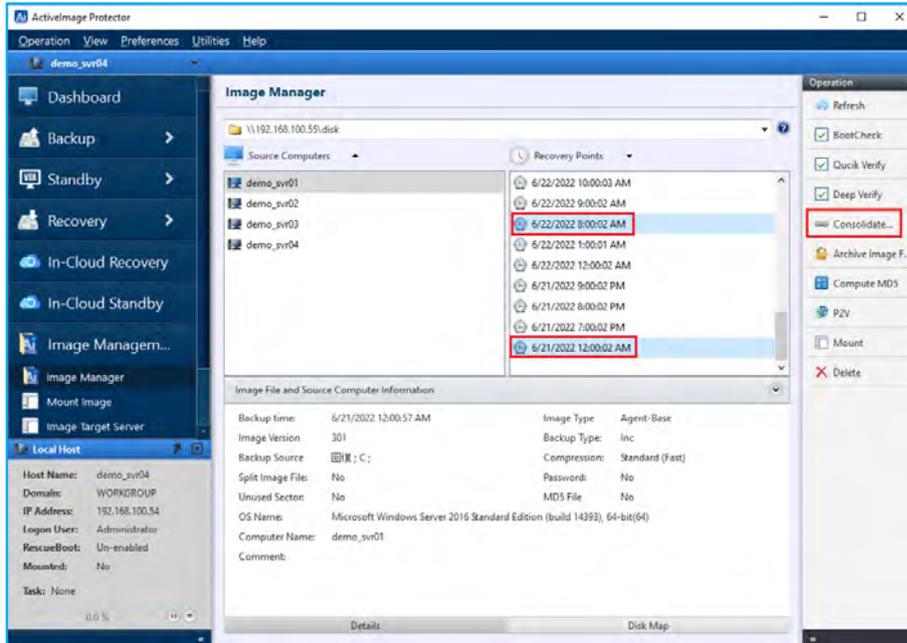
3. After the Verify completes the following window is displayed.



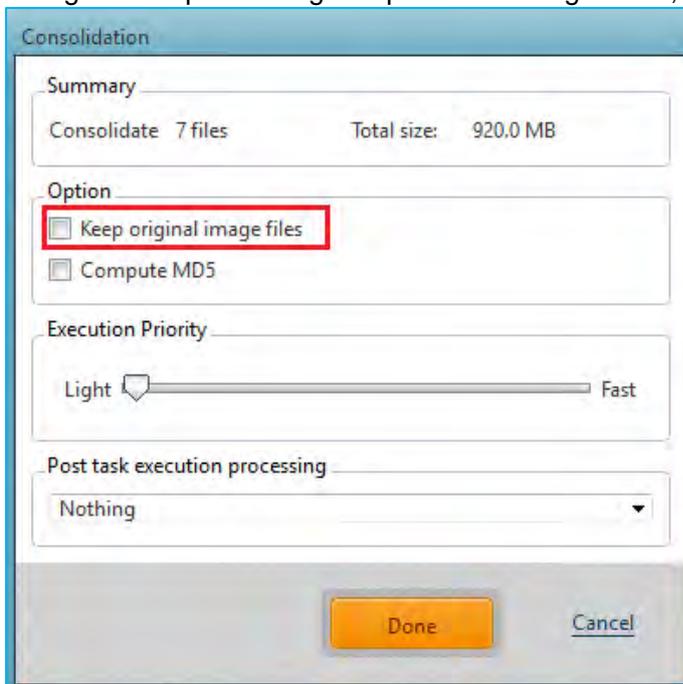
6-4. Consolidation

Reduce the number of files and save space using consolidation to consolidate your incremental backups.

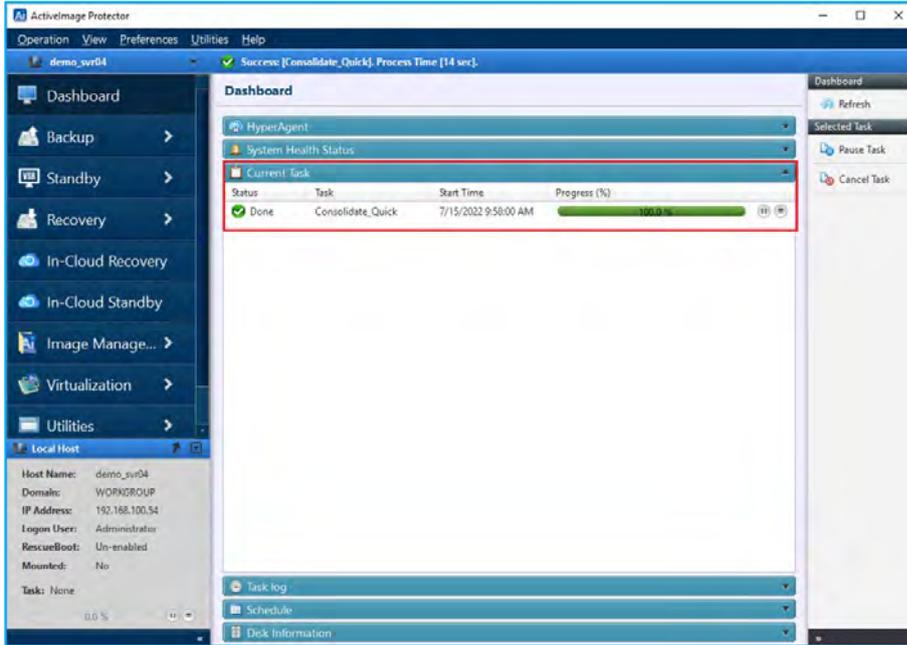
1. Select **[Source Computer]** and **[Recovery Point]**, hold down the SHIFT/CTRL key and click on the start and end point of the incremental backups you want to consolidate and then click **[Consolidate...]**. This example shows that recovery point “06/21/2022 12:00” is selected as the beginning and “06/22/2022 8:00” for the ending of incremental backups to consolidate.



2. Configure the Option settings. To preserve the original files, tick the checkbox for **[Keep original image files]**.



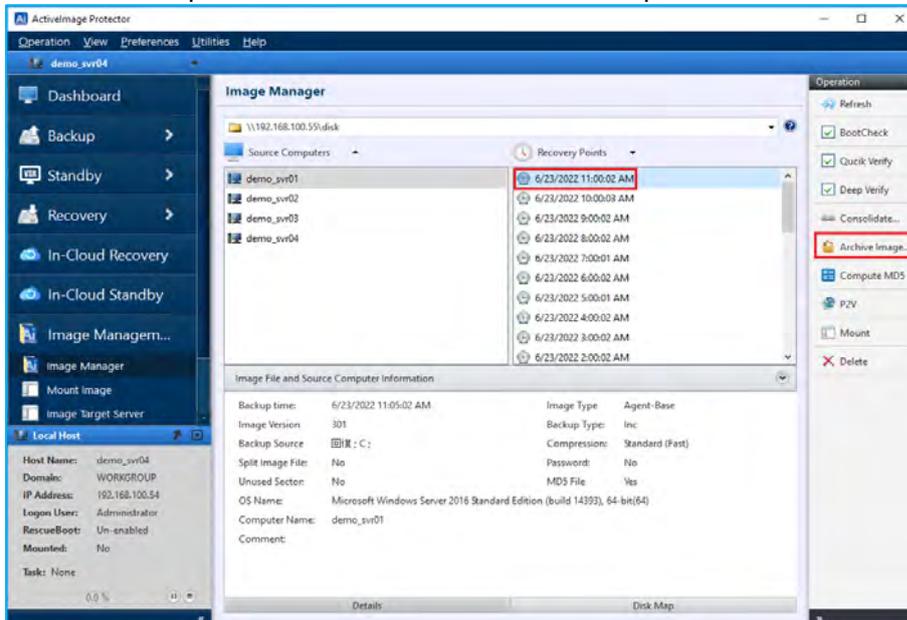
3. After the consolidation process completes, the following window is displayed.



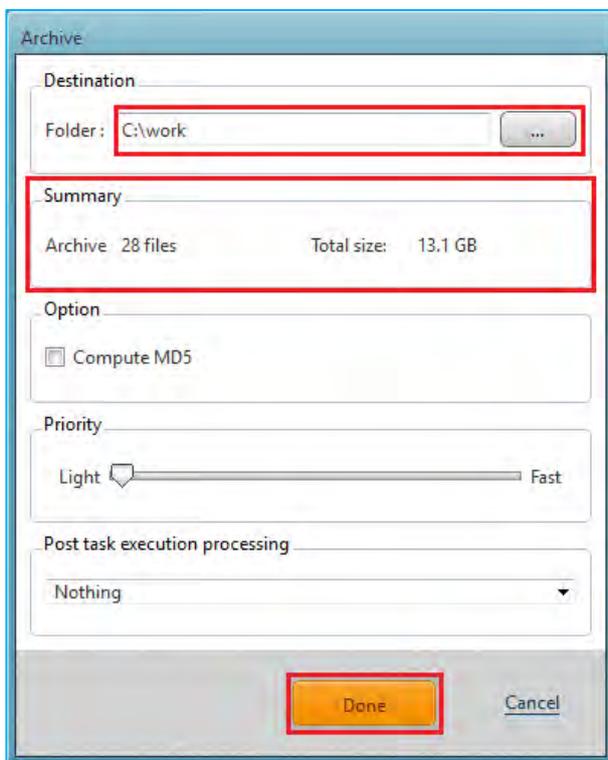
6-5. Archive Backups

Reduce file clutter by combining same-generation base and incremental backups and save an archived backup to a specified location.

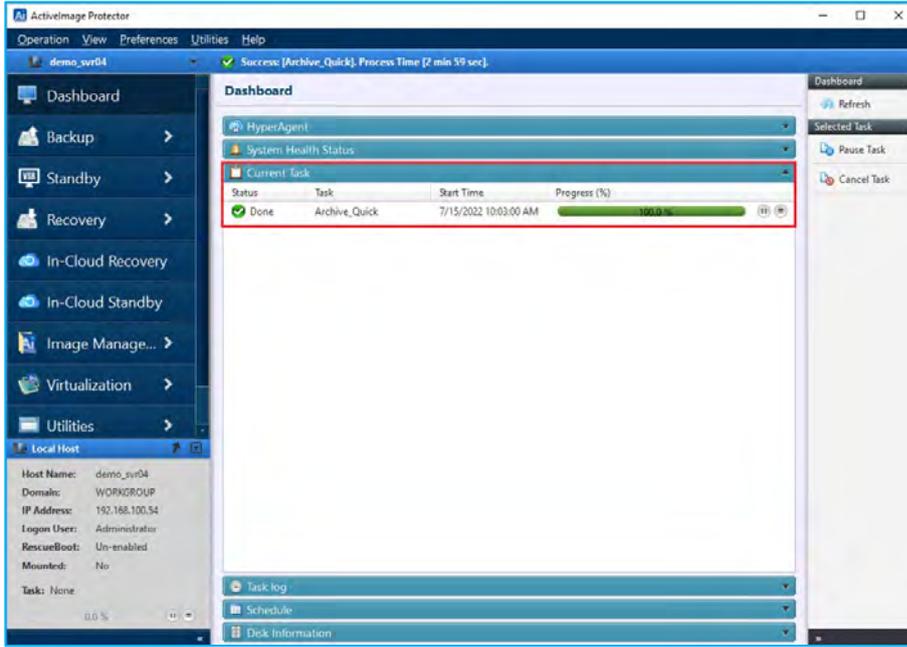
1. Select **[Source Computer]**, select the latest **[Recovery Point]** and click **[Archive Image]** in the right pane. The base backup and the associated incremental backups will be combined into one archived backup file.



2. A popup dialog showing the number of selected backups and the total output size of the archive will be displayed. Please specify a destination that has enough space to save the archive file. Click **[Done]** to start the archival process.



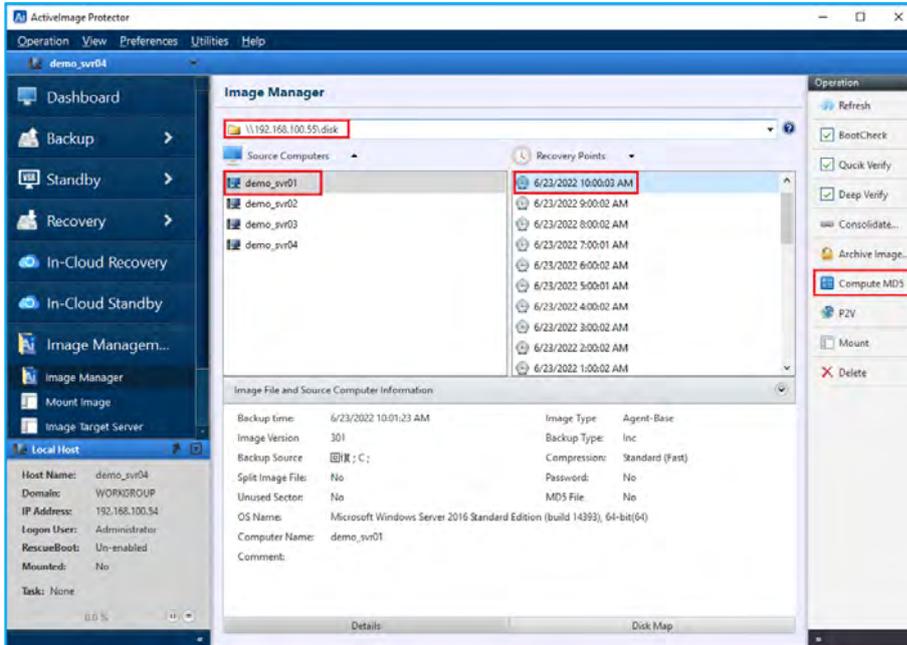
3. After archived backup has completed, the following window is displayed.



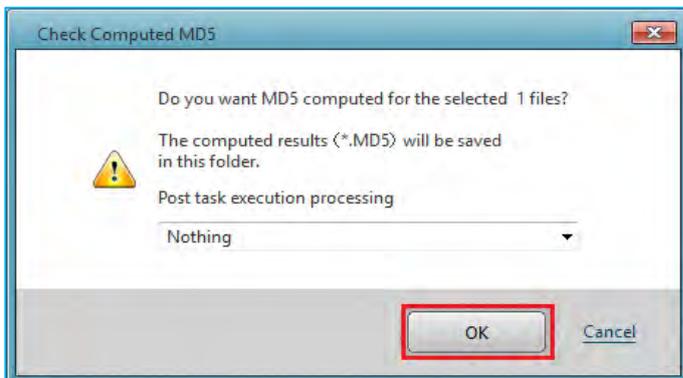
6-6. MD5 Checksum

Create a MD5 checksum for the selected backup. This can be used as a security measure to check if internal tampering of the backup has occurred.

1. Select **[Source Computer]** and **[Recovery Point]** and click **[Compute MD5...]** in the right pane. To select multiple files, hold down the SHIFT/CTRL key and click on the starting and ending backup points.



2. Click **[OK]**.

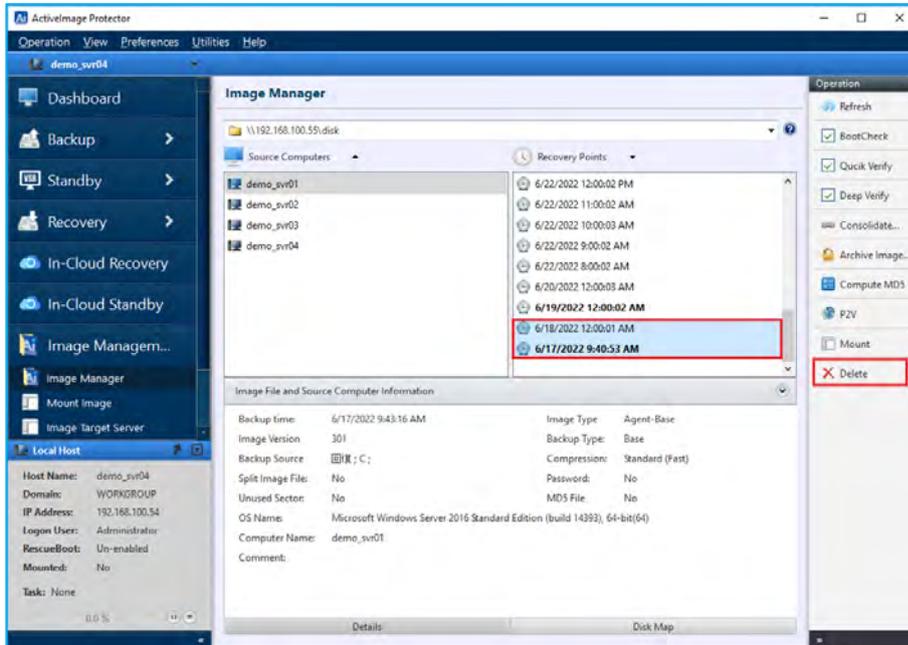


6-7. Delete Backup Files

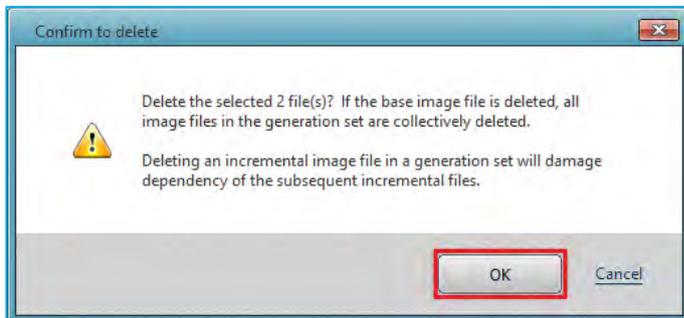
Specified backup files can be deleted.

Note: Please keep in mind that this deletion operation is permanent and cannot be undone.

1. Select **[Source Computer]** and **[Recovery Point]** of a backups to delete. Click **[Delete]** in the right pane. To select multiple files, hold down the SHIFT/CTRL key and click on the starting and ending backup points.



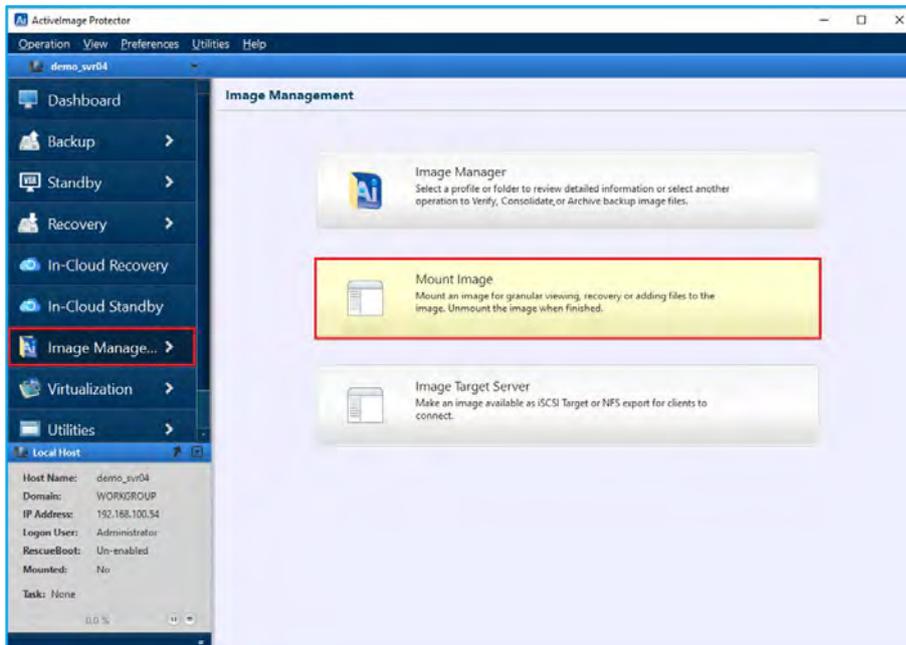
2. Click **[OK]** to delete the selected backup files.



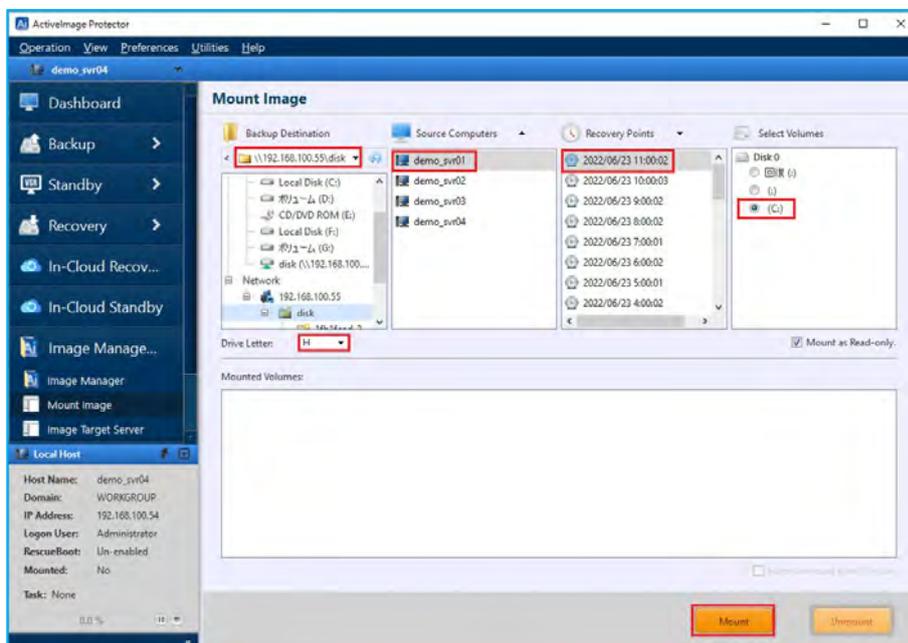
6-8. Image Manager: Mount Image

The Mount Image feature allows you to mount a backup on the OS file system and assign a drive letter. A mounted image can be browsed from Windows explorer and files and folders can be copied from ActiveImage Protector backups.

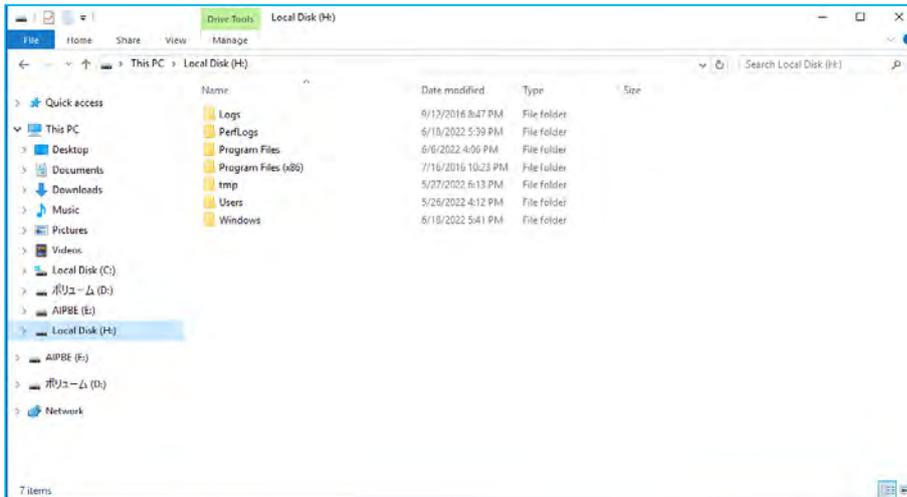
1. Select **[Image Manager]** in the left pane and **[Mount Image]**.



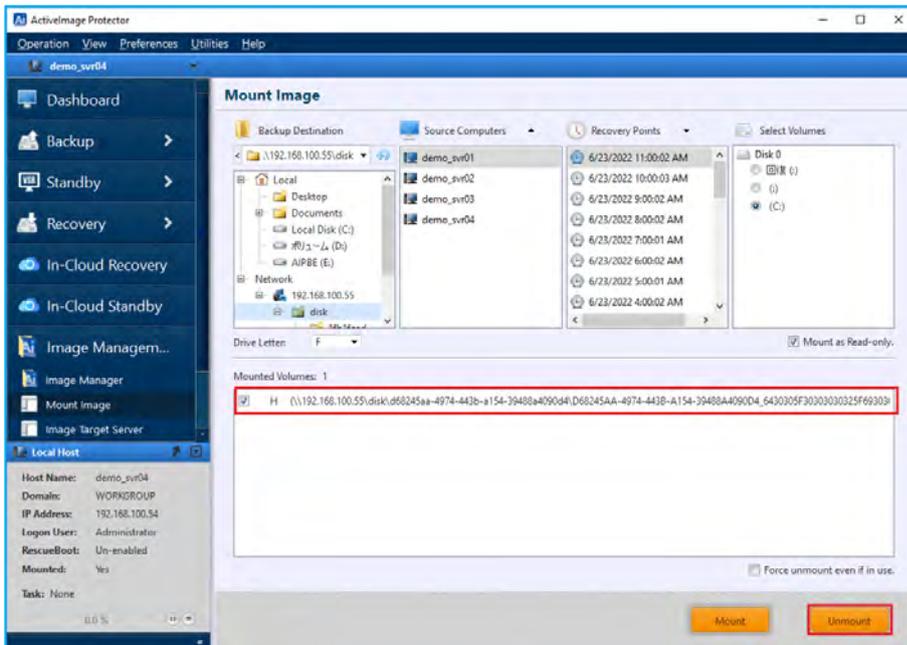
2. Select **[Source Computer]** and **[Recovery Point]** of a backup. When the backup includes multiple disks, select a volume to mount. Specify the drive letter to assign to the volume and click **[Mount]**. The backup can be mounted as read-only by selecting the **[Mount as Read-only]** option.



- When mounted, you can browse the contents from Windows explorer as shown below, enabling you to open or copy a files.



- When unmounting, select a mount point from the **[Mounted Volumes]** and click **[Unmount]**.



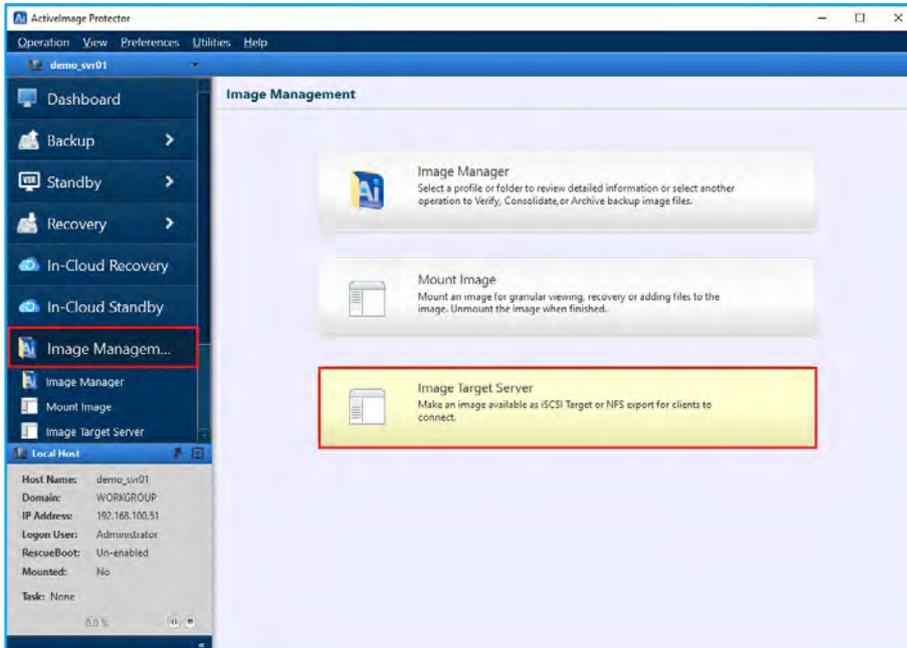
Note: The backup can also be mounted as writable. The changes made to the backup are saved in a differential backup (.aix) after the volume is unmounted.

6-9. Image Manager: Image Target Server

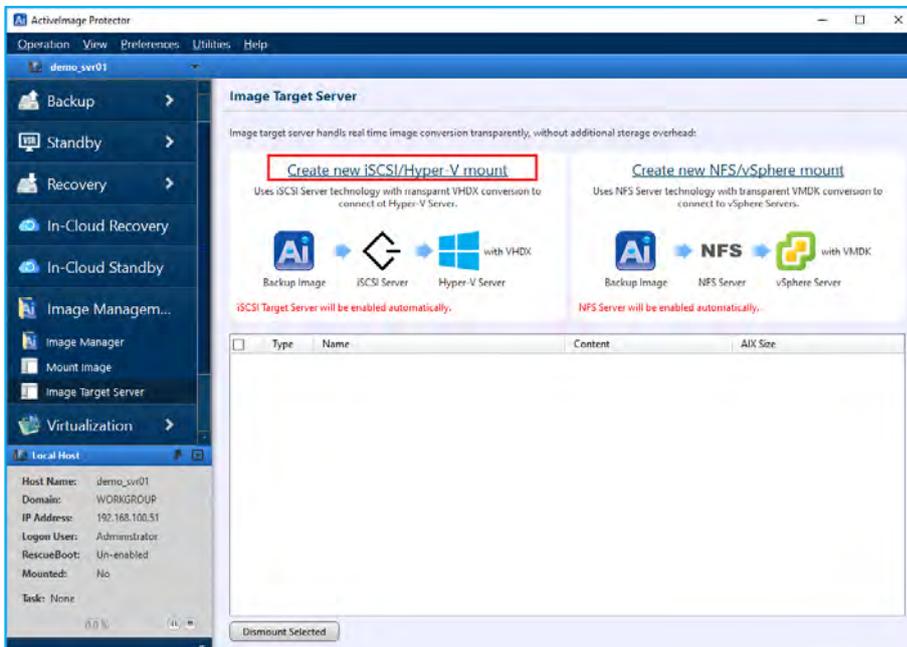
ActiveImage Protector backups can be configured as iSCSI or NFS target.

This example show how a backup can be configured as an iSCSI target. Connecting to this iSCSI target will enable you to mount the backup as a local disk on the iSCSI initiator OS.

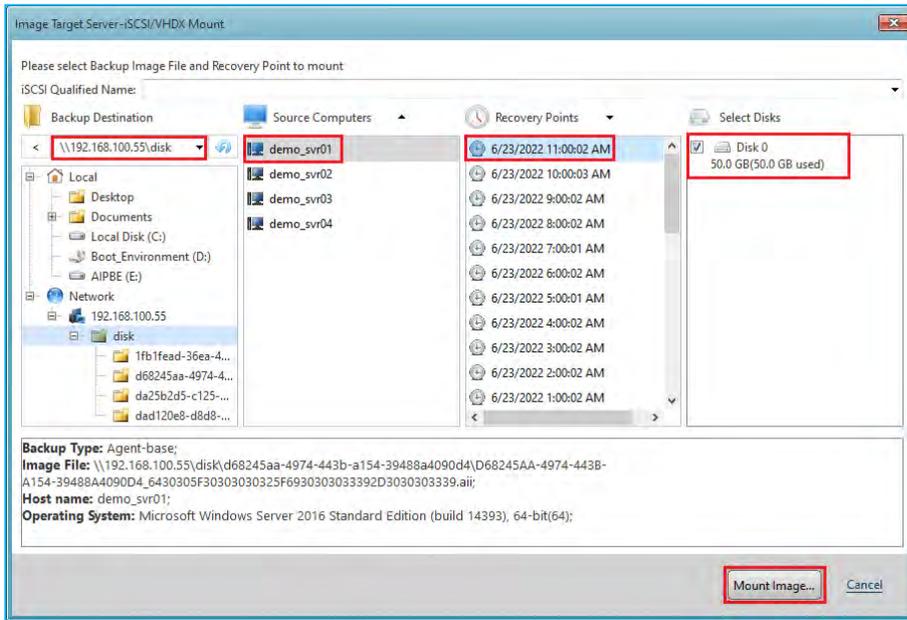
1. Select **[Image Management]** in the left pane and **[Image Target Server]**.



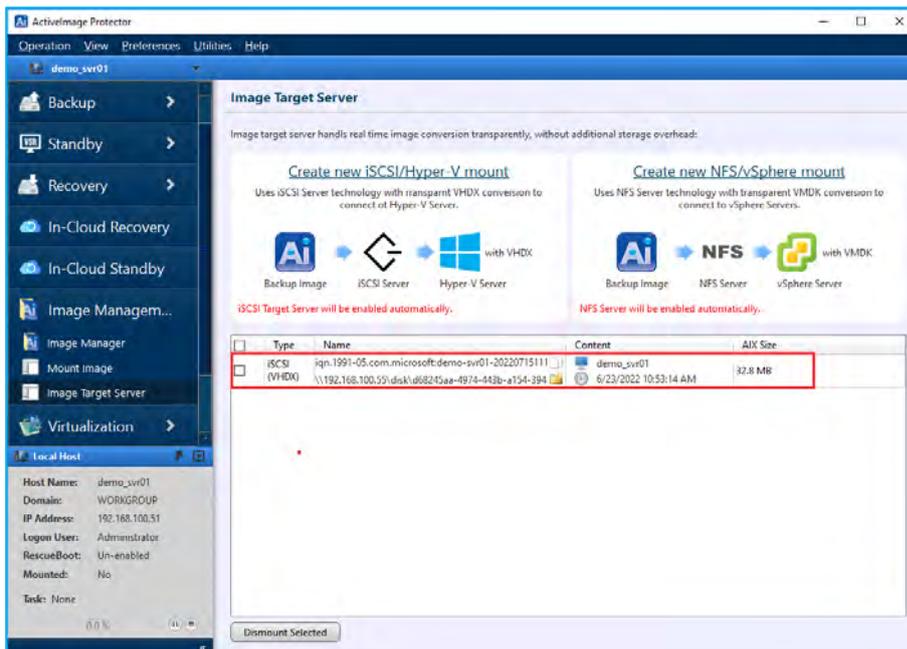
2. Depicted below is **[Image Target Server]** window. Select **[Create new iSCSI/Hyper-V mount]**.



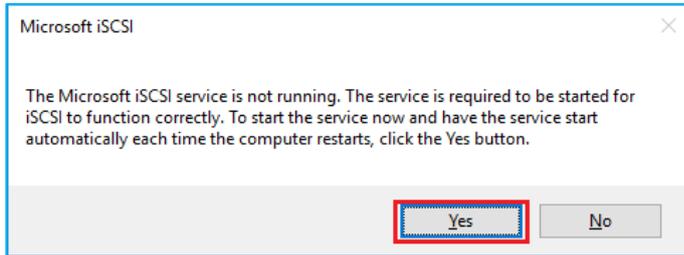
3. Select **[Source Computers]**, **[Recovery Points]** and a disk. Click **[Mount]**. When multiple disks are included, select the disks you want to target under **[Select Disks]**.



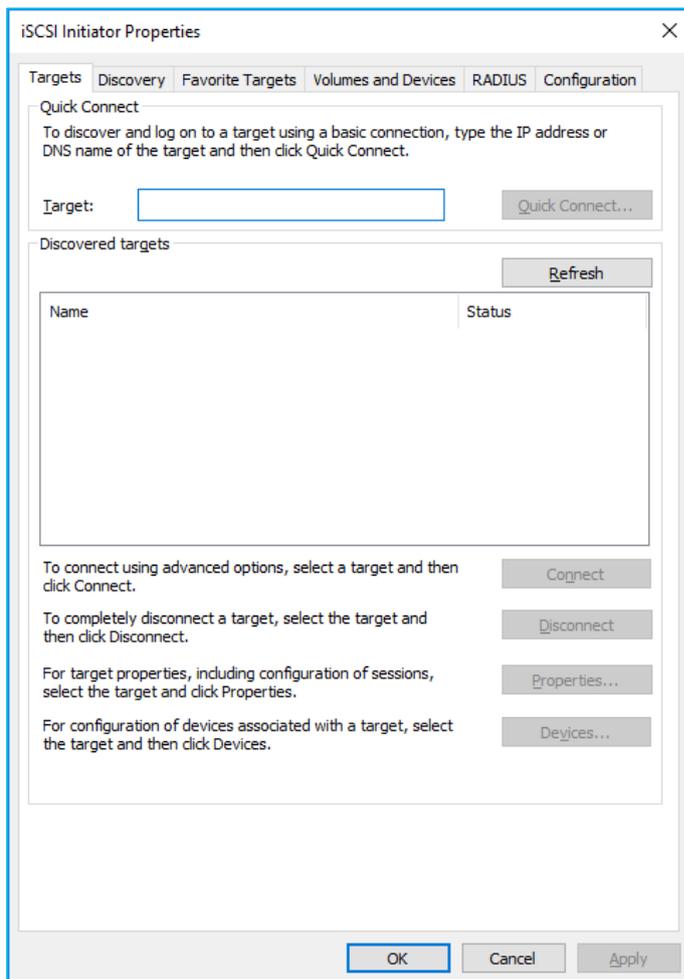
4. The backup will be served as an iSCSI target that can be connected via remote iSCSI initiator.



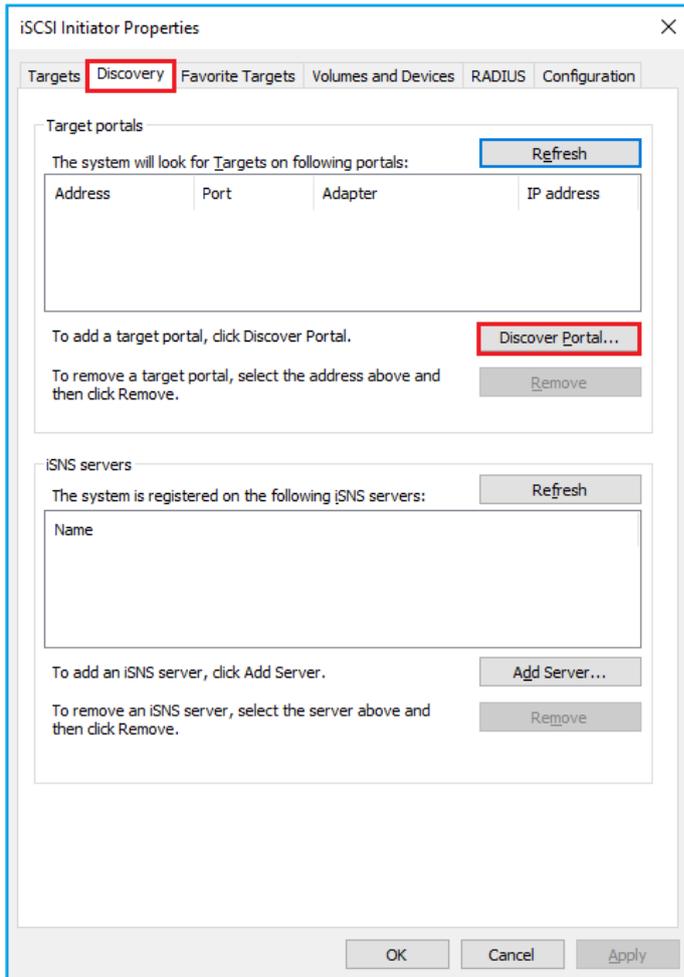
5. On the machine you wish to mount the image, go to Windows Start menu - **[iSCSI Initiator]**.
6. When the **[iSCSI Initiator]** is launched for the first time, please select **[Yes]** in the following dialog.



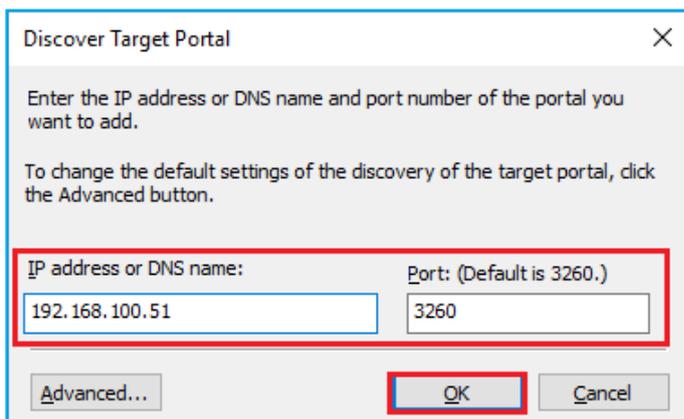
7. The dialog displayed after iSCSI Initiator has started.



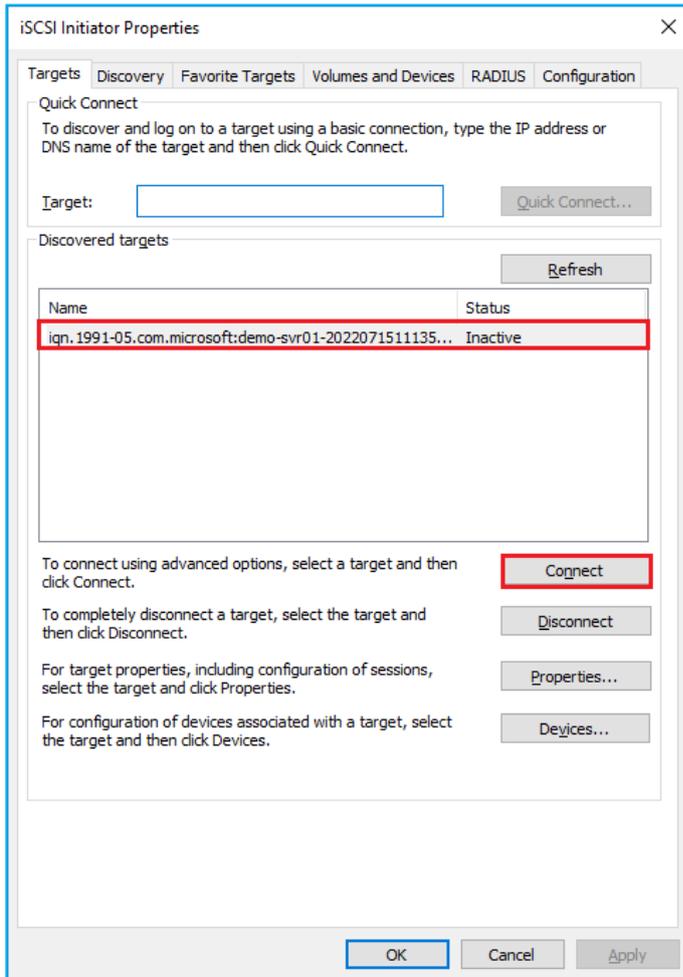
8. Select **[Discovery]** tab and click **[Discover Portal]**.



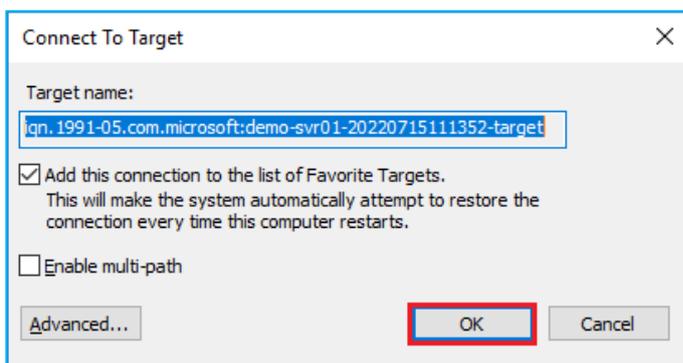
9. In this example, for the iSCSI server the IP address "192.168.100.51" is entered in the **[IP address or DNS name]** field. For the **[Port]** the default value "3260" is being used. Click **[OK]**.



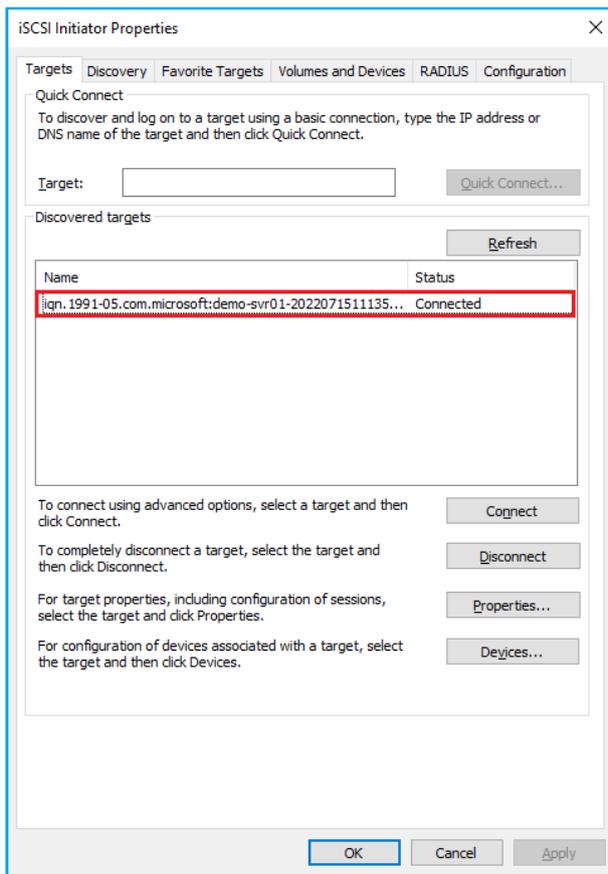
10. Go back to **[Target]** tab. iSCSI target is indicated for **[Discovered targets]**. Click **[Connect]**.



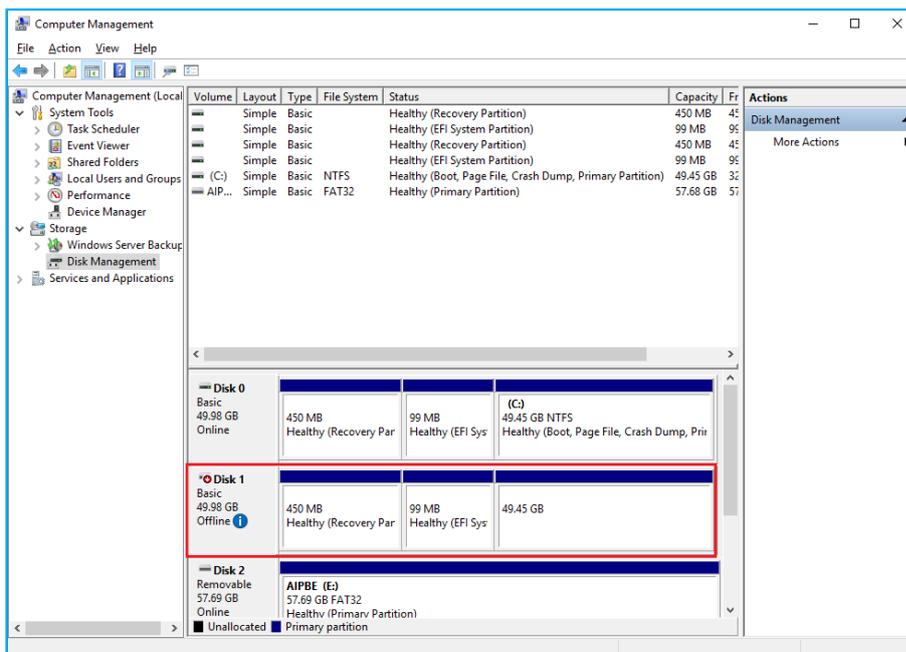
11. When establishing a connection to the target, **[Add the connection to the list of Favorite Targets]** is enabled by default. As the stated in description below, enabling this option will make the system automatically attempt to restore the connection every time this computer restart. Click **[OK]** to establish the connection.



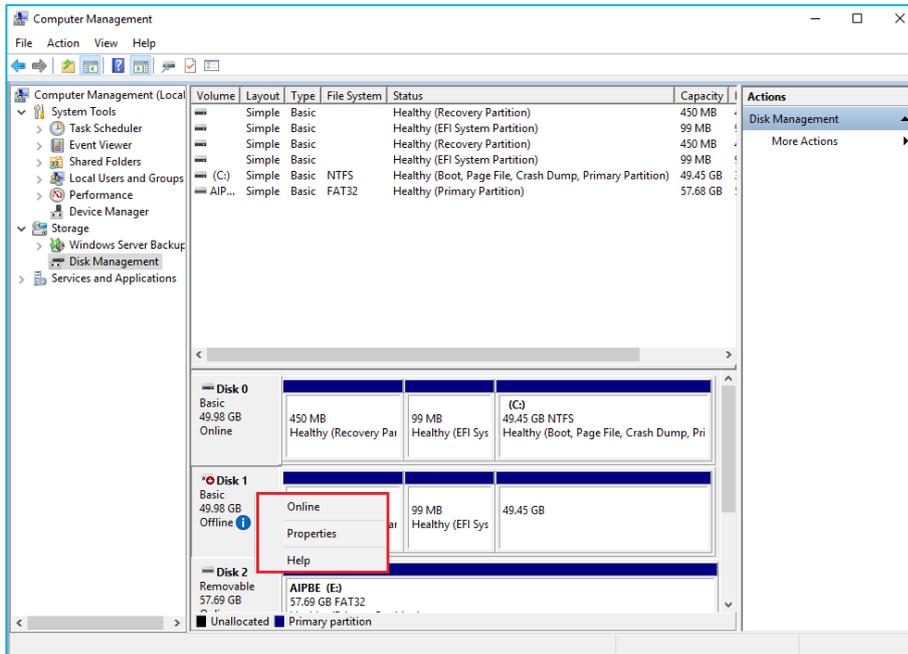
- Please make sure that **[Status]** of the **[Discovered targets]** item has changed to **[Connected]** in **[Target]** tab.



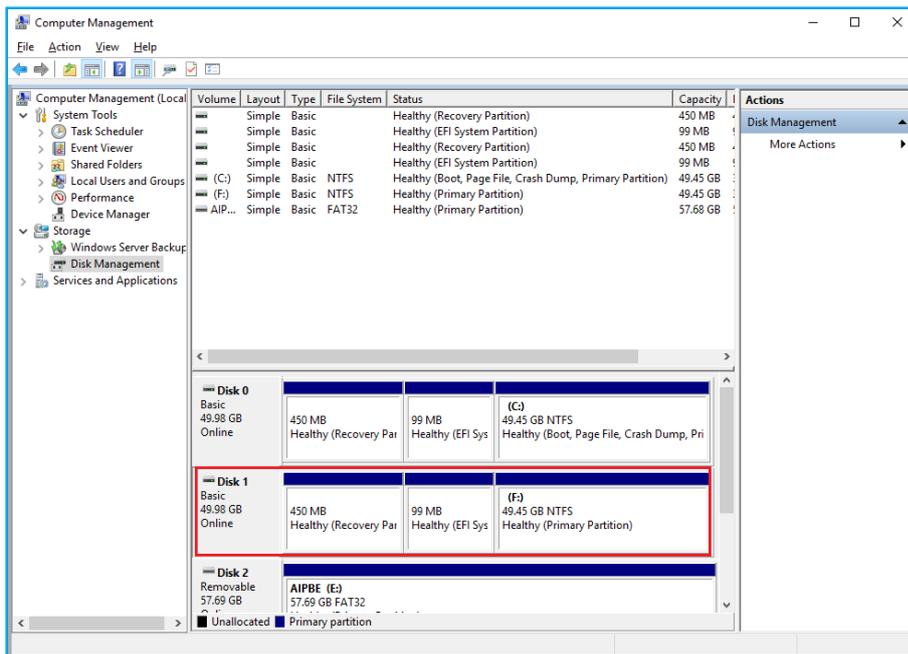
- Next, go to **[Control Panel] - [Computer Management]** and select **[Disk Management]** in the left menu. A new disk, in the case "Disk 1", is added and the status indicates "Offline".



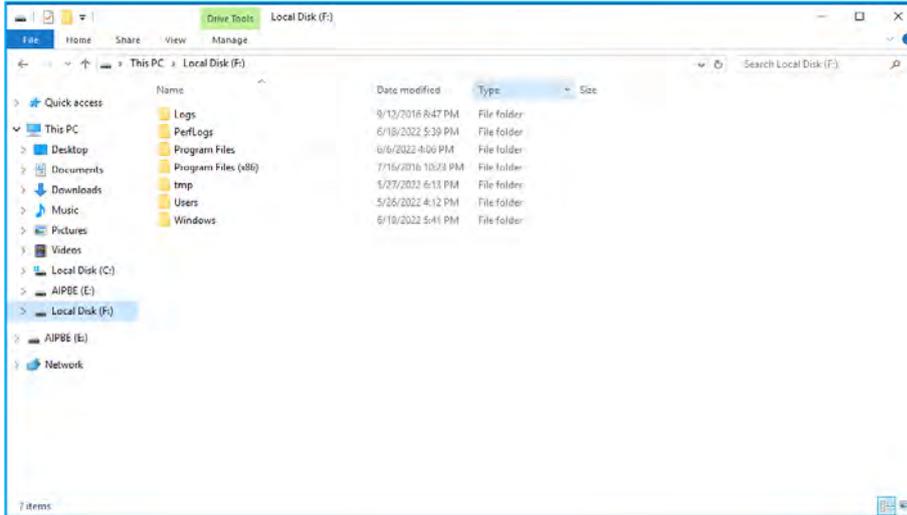
14. Right-click on “Disk 1” and the following context menu is displayed. Select **[Online]** and “Disk 1” is recognized as local disk.



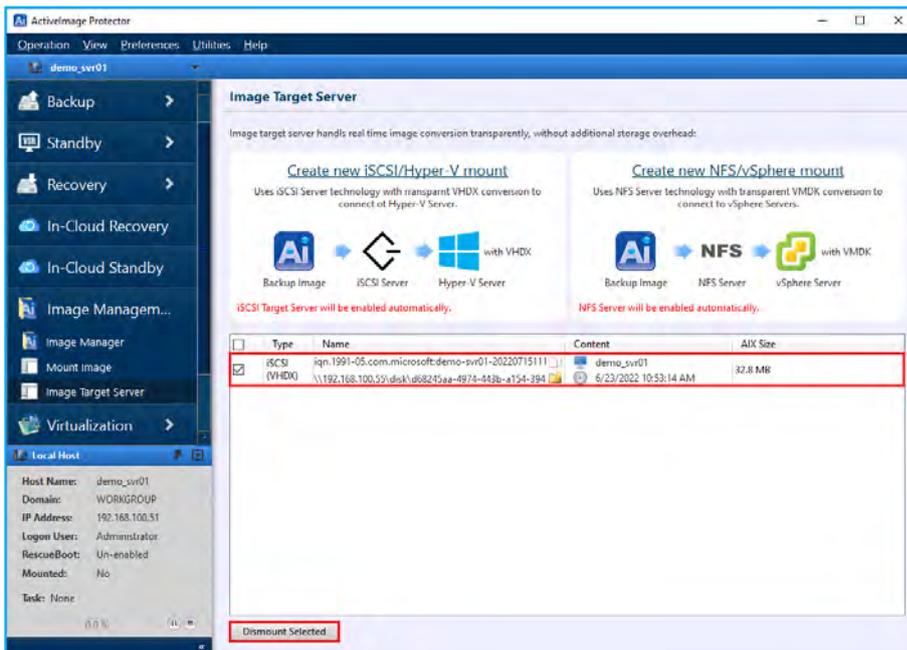
15. Because “Disk 1” is recognized as local disk, and a drive letter is assigned to the partition.



16. You can browse the contents using Windows file explorer.



17. When you are finished using the iSCSI disk, please disconnect the iSCSI initiator. Tick the checkbox for the iSCSI target and click **[Dismount Selected]**. If you get 'The session cannot be logged out since a device on that session is currently in use' message, go to **[Disk Management]**, set the iSCSI disk to offline and try again.



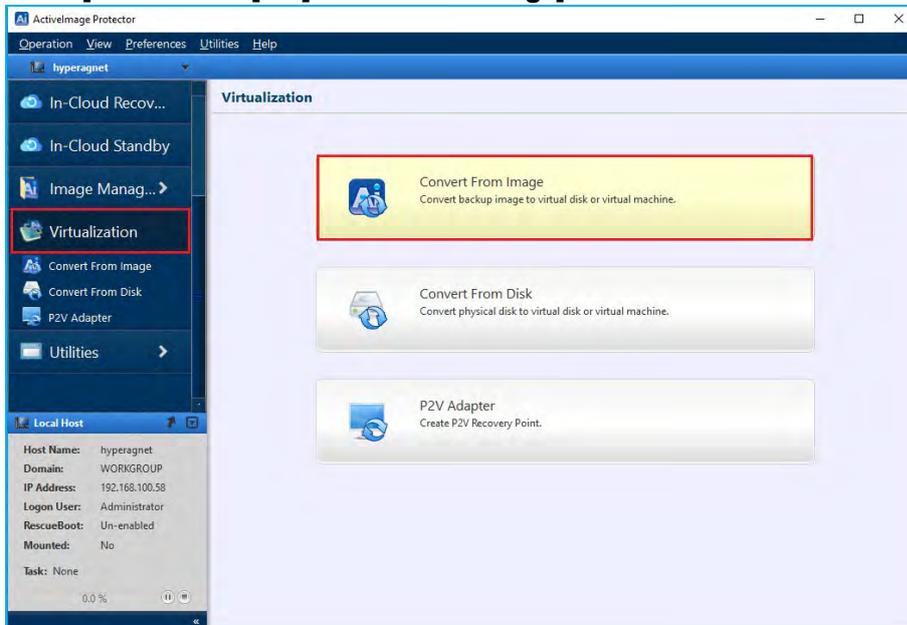
7. Virtualization

Virtualization converts backup image files to virtual disks or virtual machines. You can specify VMware vSphere or Microsoft Hyper-V hosts as targets, or you can convert to a virtual disk on a local file system to migrate to a virtual system.

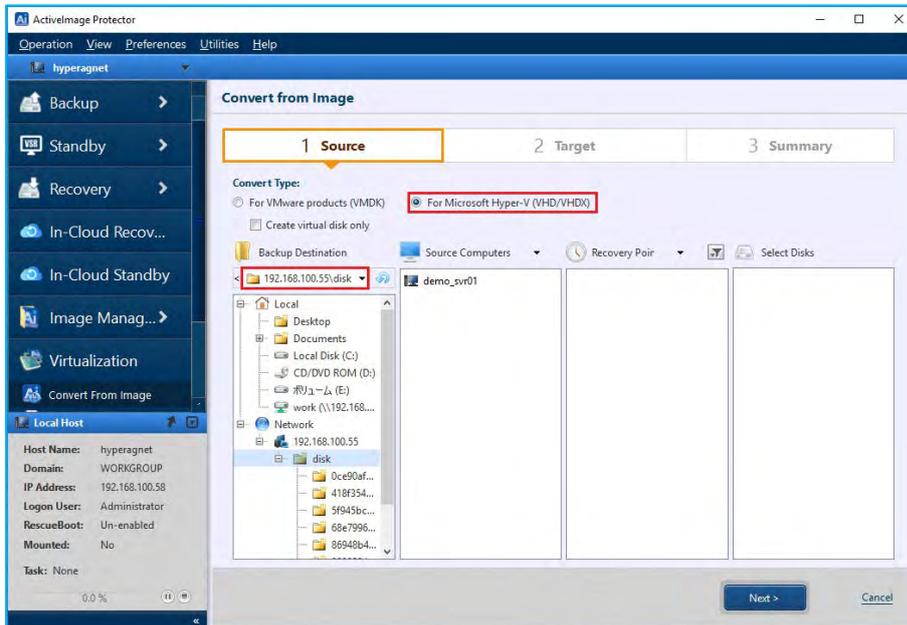
7-1. Migration from backup source to virtual environment

The following explains how to convert an image file to a virtual machine on hypervisor (Hyper-V).

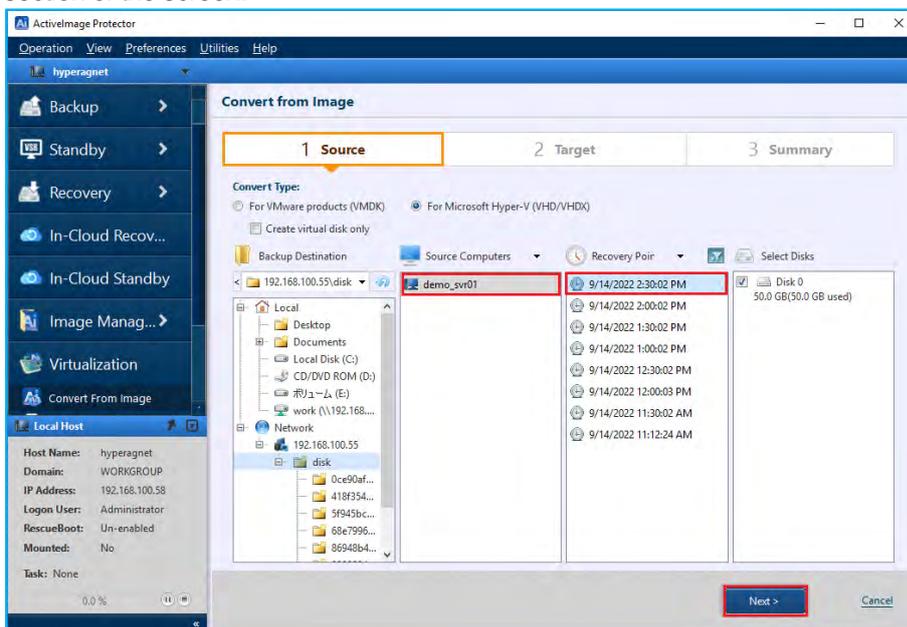
1. Select **[Virtualization]** → **[Convert from Image]** from the menu.



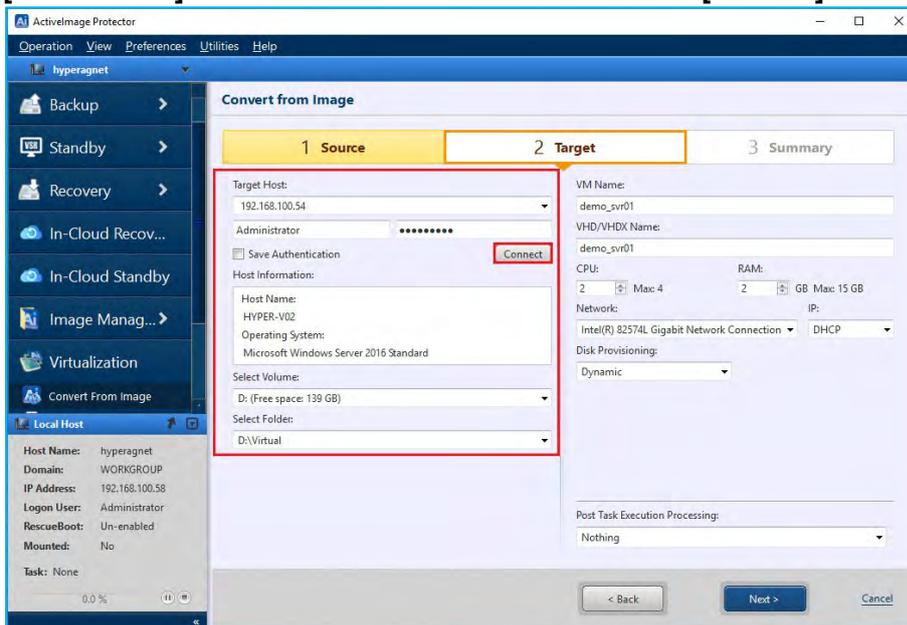
- In this example, we have selected “Microsoft Hyper-V” for **[Convert Type]** and a network shared folder, “\\192.168.100.55\disk1”, is specified as the destination folder. Click **[Backup Destination]** to browse to a location. Or click “▼” on the right hand of the text box to select a location previously used as a destination in other backup tasks. You can also enter in a the destination location and press the **[Enter]** key to set the destination folder.



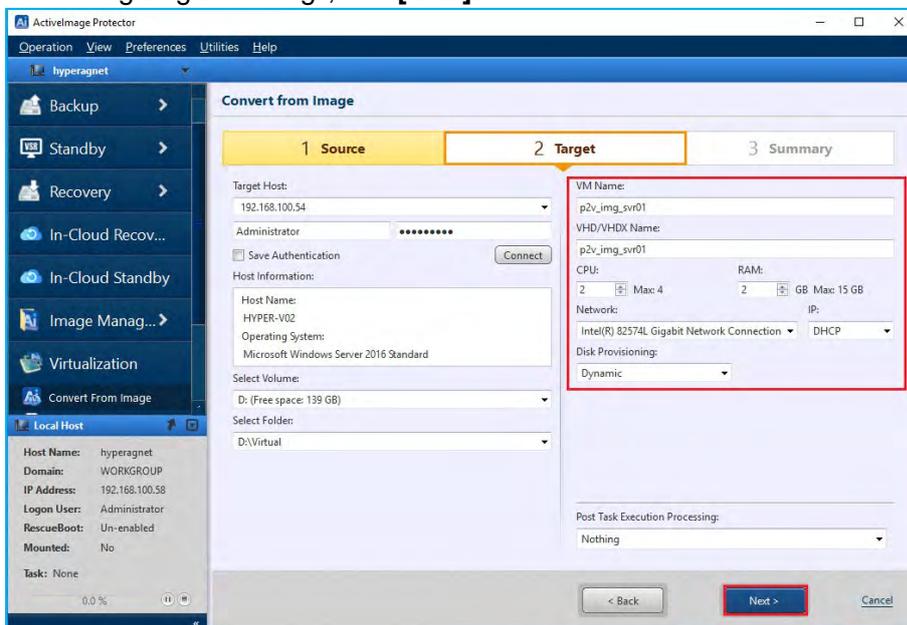
- Select the **[Source Computer]** and **[Recovery Point]**. Click **[Next]**. ActiImage Protector will display information about your selected backup image in the **[Backup Information]** section of the screen.



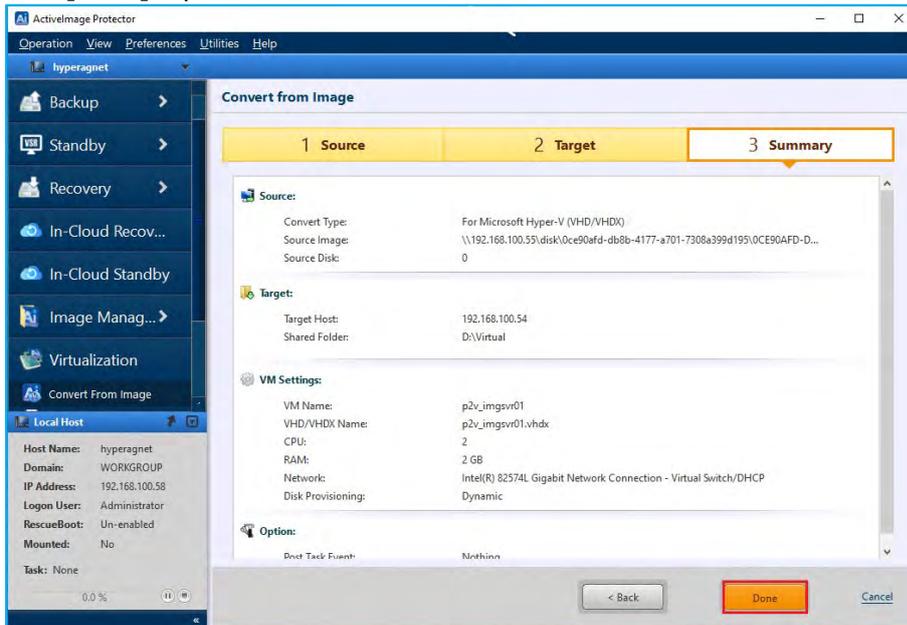
4. Configure the settings for the target host. In this example, “Microsoft Hyper-V” is selected for the **[Target Host]**, and “192.168.100.54” is the IP address of the target host, “Administrator” is used for the **[User Name]** and the password is entered. “D drive” selected for **[Select Volume]** and this is where the virtual machine files will be saved. The folder “Virtual” is specified for **[Select Folder]** this sub folder for virtual files in D drive. Click **[Connect]**.



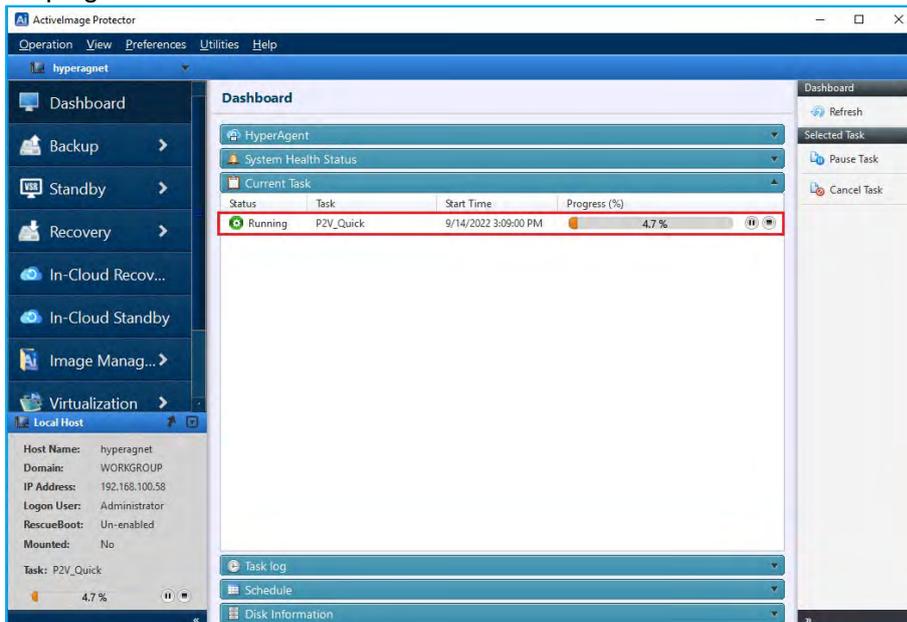
5. Configure the setting for the virtual machine. The following example shows settings configured for the virtual machine to be created in the process. “p2v_img_svr01” is specified for **[VM name]**, “2” for **[CPU:]**, “2GB” for **[RAM]** and “Dynamic” for **[Disk Provisioning]**. For **[Network]**, select the values for **[Virtual Switch]** on the target host, and “DHCP” for **[IP]**. After configuring the settings, click **[Next]**.



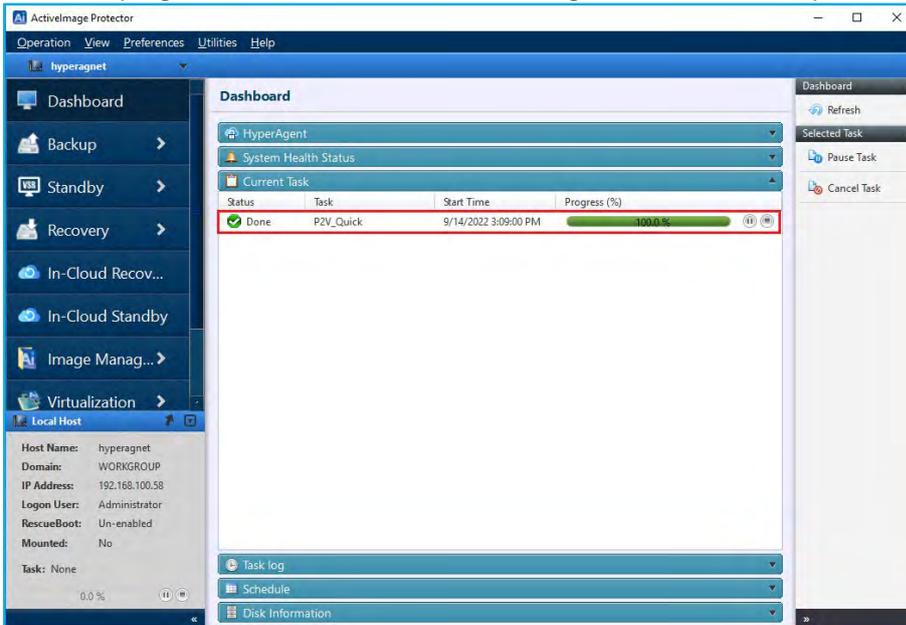
- Review your configuration the Summary window.
Click **[Done]** to proceed.



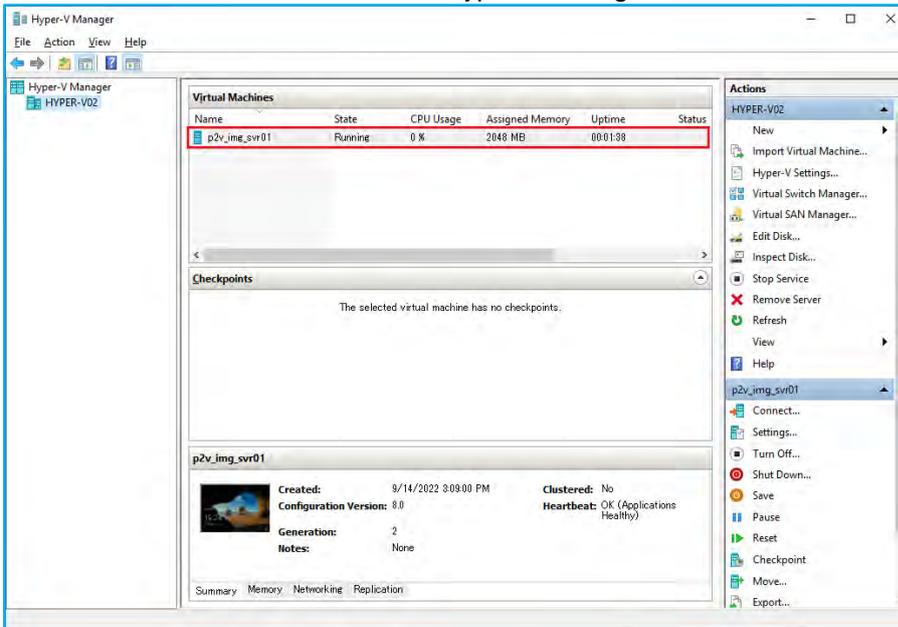
- The task will start and create the virtual machine on the host. The console returns to Dashboard view indicating the progress of task.



8. When the progress bar reaches 100%, ActiveImage Protector has completed the virtualization.



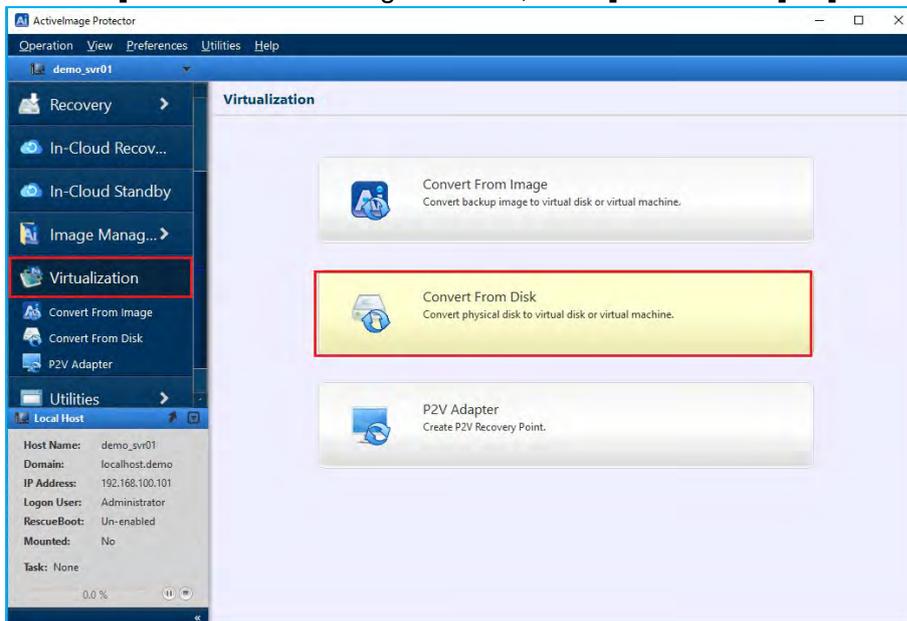
9. You can use the virtual machine in the Hyper-V Manager console.



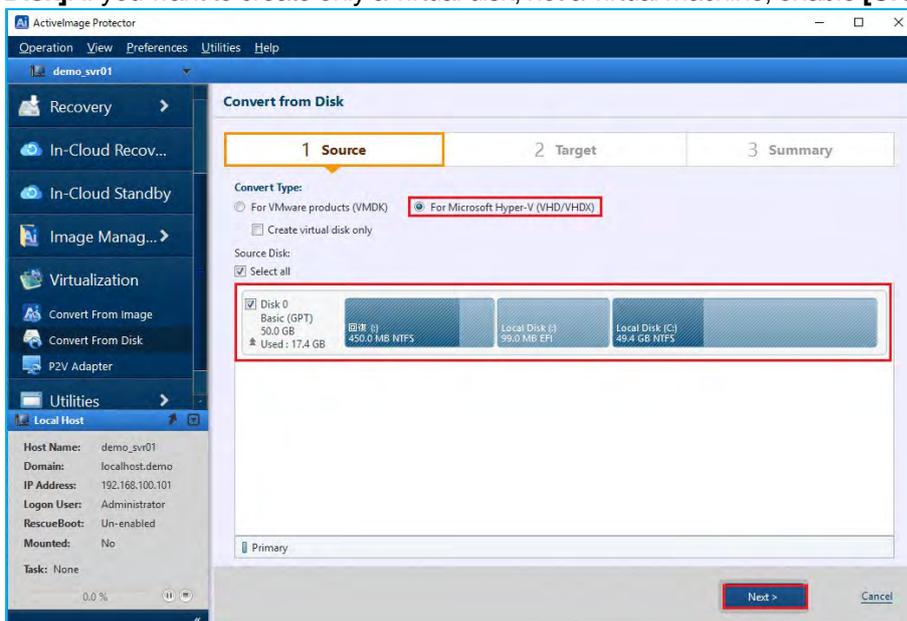
7-2. Migration from physical disk to virtual environment

The following explains how to virtualize a physical disk to a virtual machine on Hyper-V or VMware vSphere.

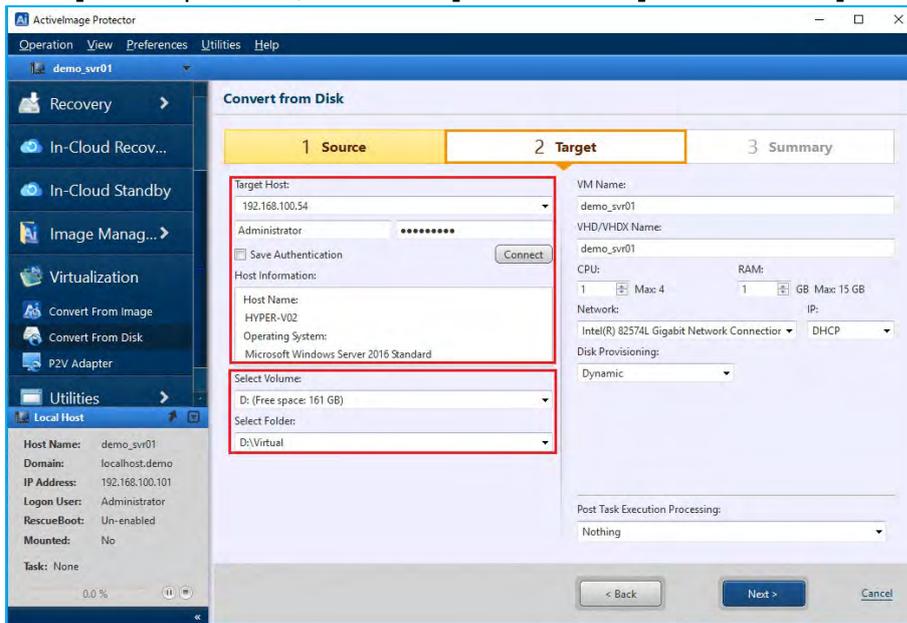
1. Start ActiImage Protector by clicking on the Windows Start menu and selecting **[ActiPhy]** → **[ActiImage Protector]**. Once in ActiImage Protector, select **[Virtualization]** → **[Convert from Disk]** in the menu.



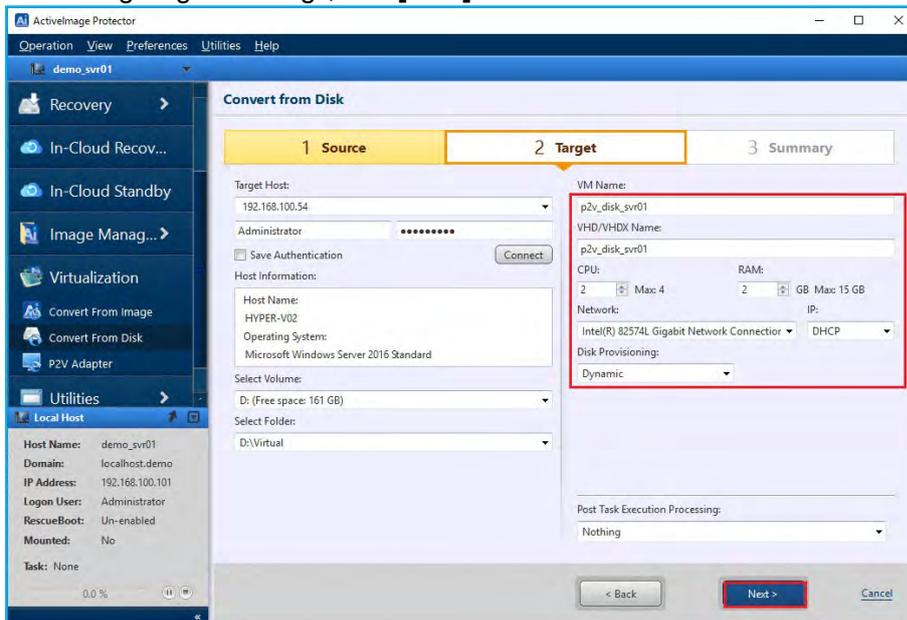
2. In this example, we have selected "Microsoft Hyper-V" for **[Convert Type]** and enabled **[Select all]** for **[Source Disk]**. If you want to create only a virtual disk, not a virtual machine, enable **[Create virtual disk only]** option.



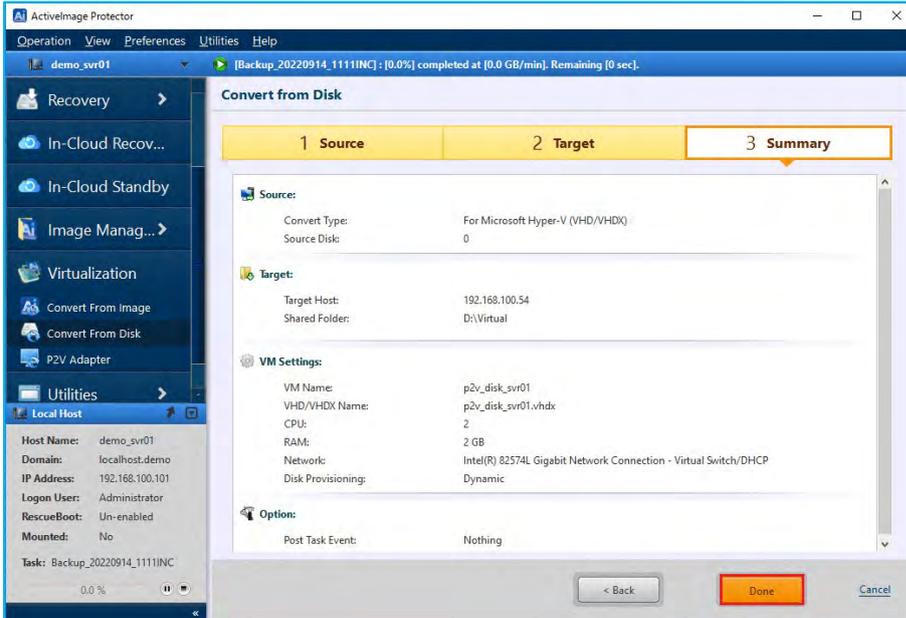
- Configure the settings for the target host.
In this example, we will enter “192.168.100.54” for IP address of the Hyper-V host, “Administrator” for the [User Name] and the password, “D drive” for [Select Volume] and “Virtual” for [Select Folder]. Click [Connect].



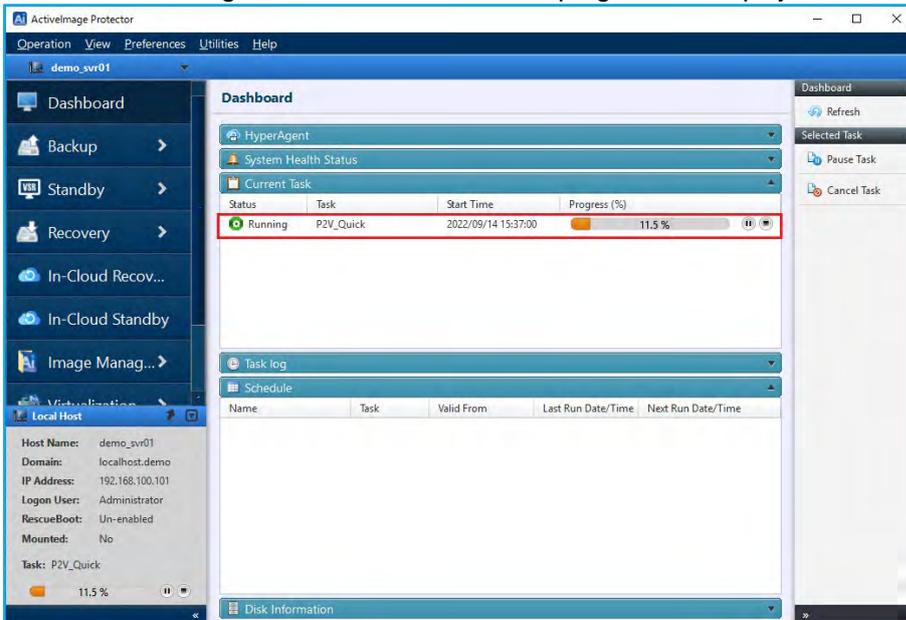
- The following example shows settings configured for the new virtual machine. “p2v_img_svr01” is specified for [VM name], “2” for [CPU:], “2GB” for [RAM] and “Dynamic” for [Disk Provisioning]. For [Network], select the values for [Virtual Switch] on the target host, and “DHCP” for [IP]. After configuring the settings, click [Next].



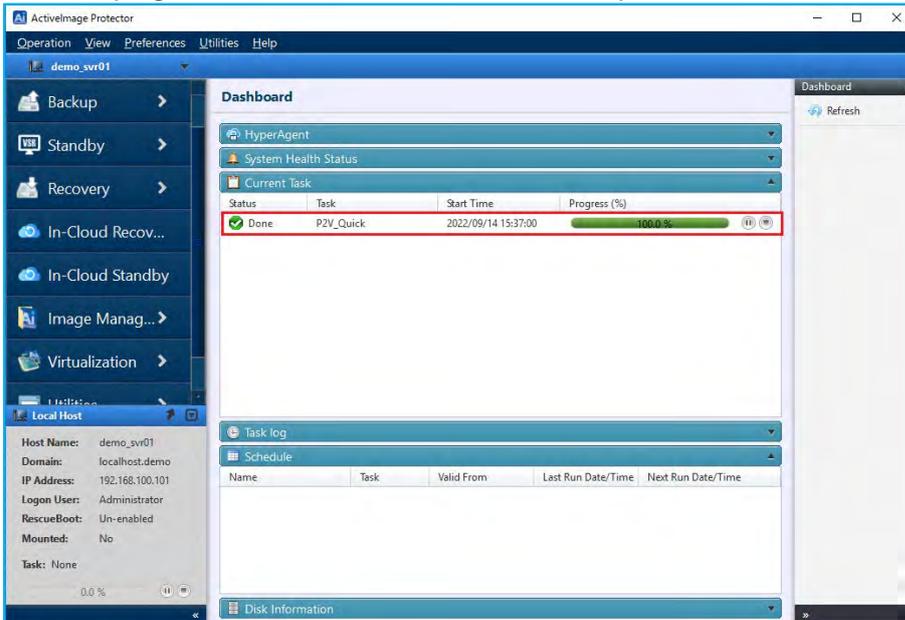
- Please review the virtual conversion configuration. If everything looks correct, click the **[Done]** button.



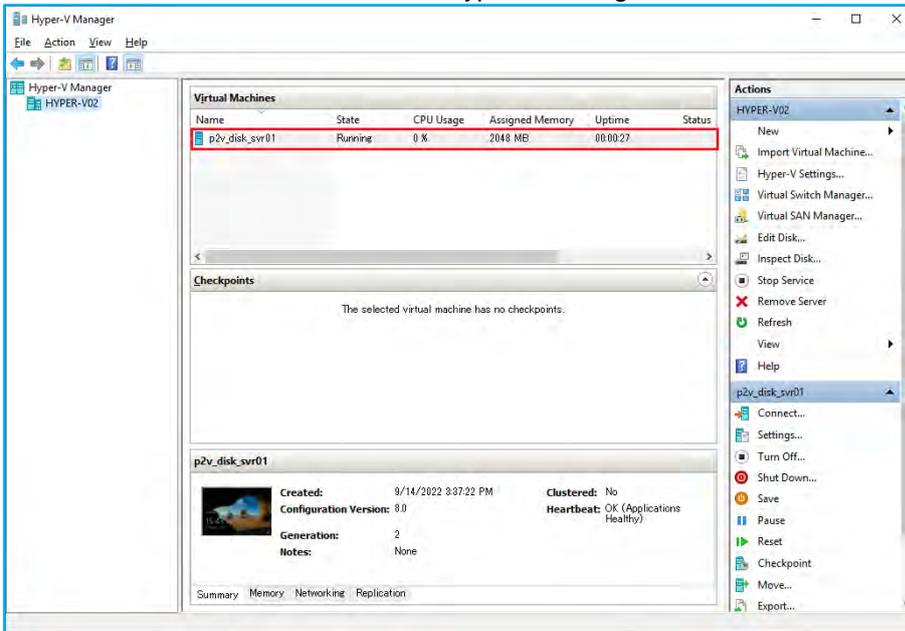
- The task for creating the virtual machine and the progress are displayed.



- Once the progress bar reaches 100%, the task is complete.



- You can use the virtual machine in the Hyper-V Manager console.



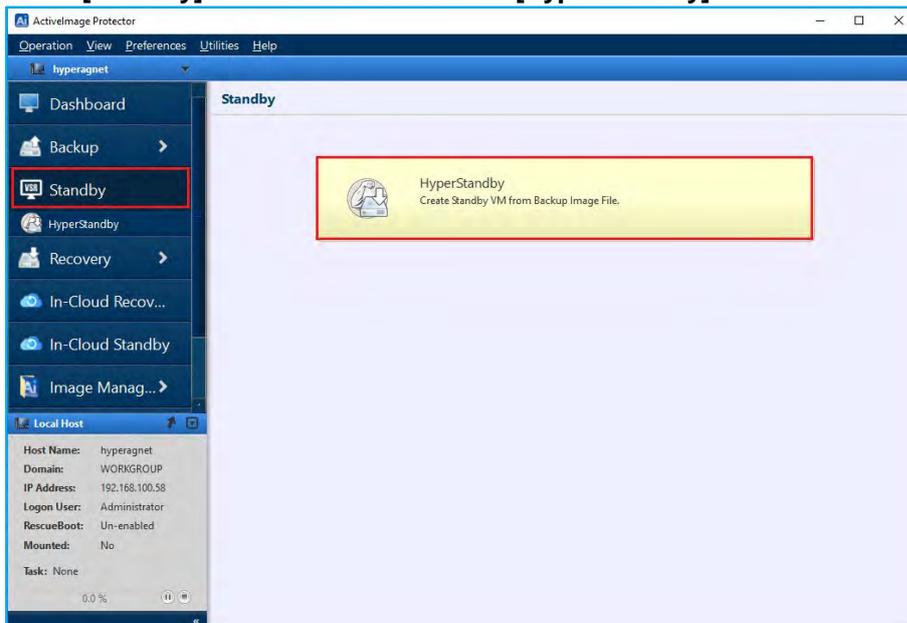
8. Creates and maintains dormant virtual replicas

8-1. HyperStandby

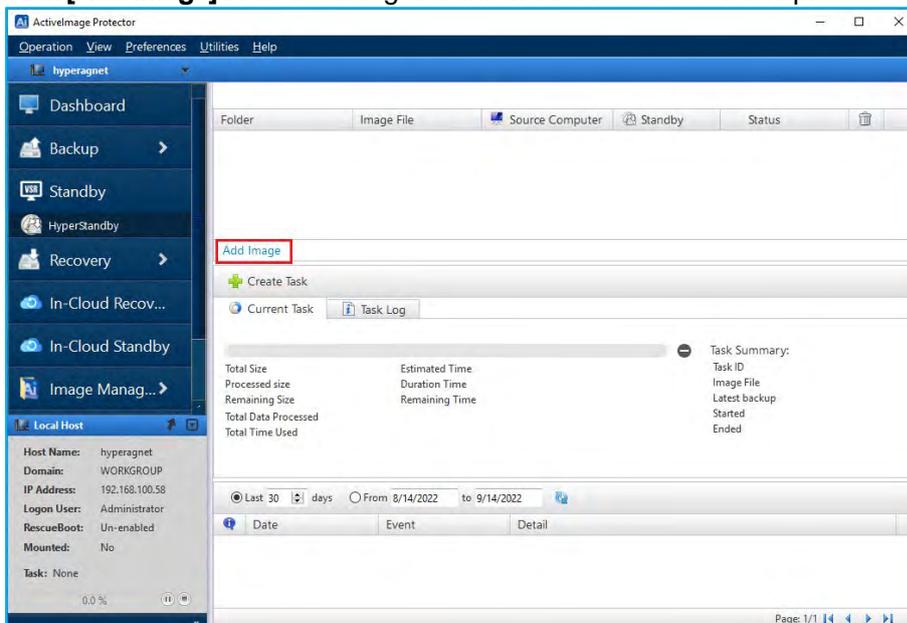
HyperStandby creates and maintains dormant virtual replicas from ActiveImage Protector (AIP) backups to provide a switch-over option in the event of a failure of the source machine. This virtual standby replica is added into a specific hypervisor host and kept current by taking scheduled incremental P2V boot points of the source machine. This ensures a successful startup of the standby virtual machine. Minimal downtime can be expected, bypassing a lengthy restore process or virtual conversion.

Below is an explanation of how to use HyperStandby to create standby virtual machines.

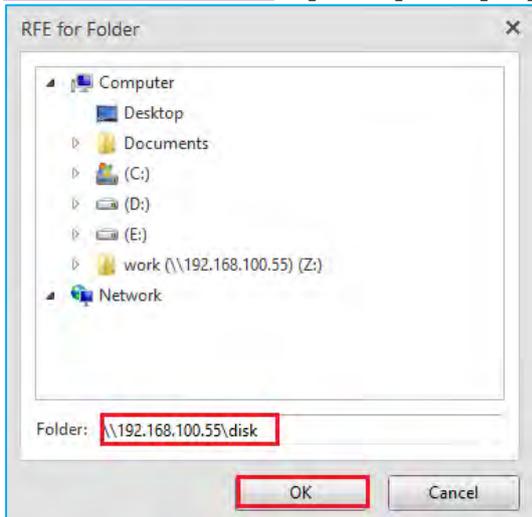
1. Select **[Standby]** in the left menu and select **[HyperStandby]**.



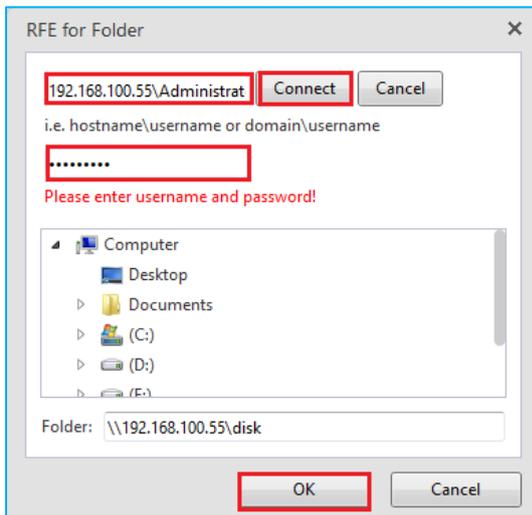
2. Click **[Add Image]** in the list dialog and check a box to select a backup.



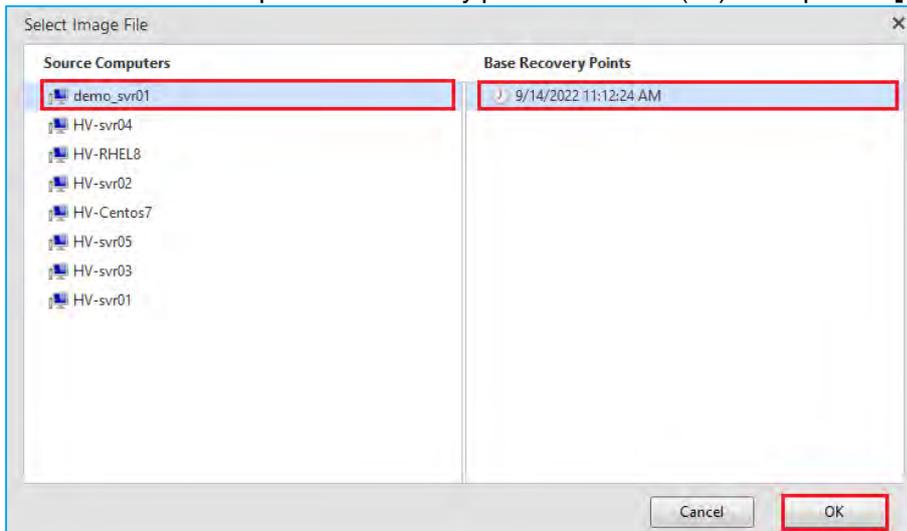
- Specify a folder that contains backup image files. This example shows entering a path to a shared folder `\\192.168.100.55\disk` in **[Folder]**. Click **[OK]**.



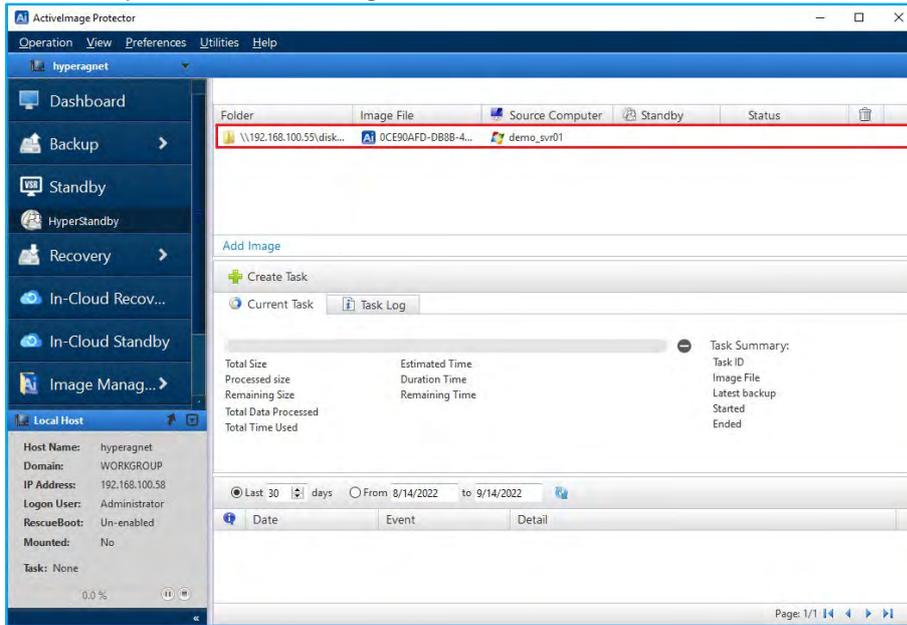
- Enter credential information to the shared folder. Click **[OK]**.



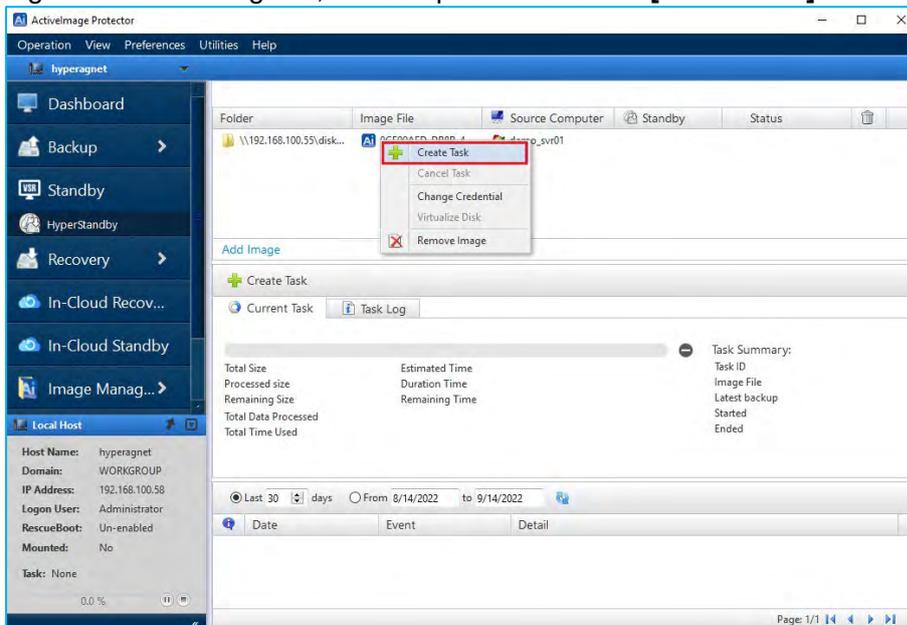
- Select the source computer and recovery point of the base (full) backup. Click **[OK]**.



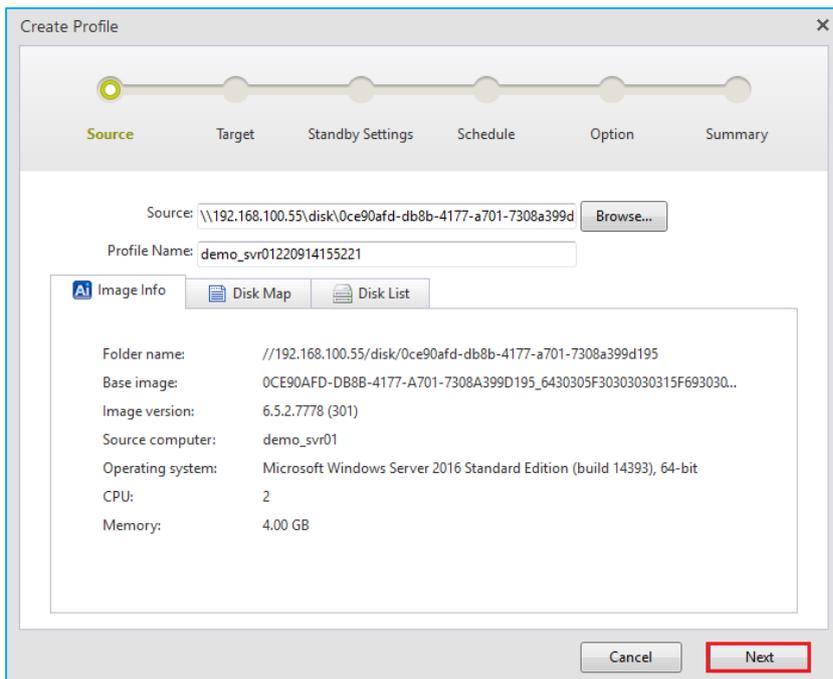
6. The backup is added to the image list.



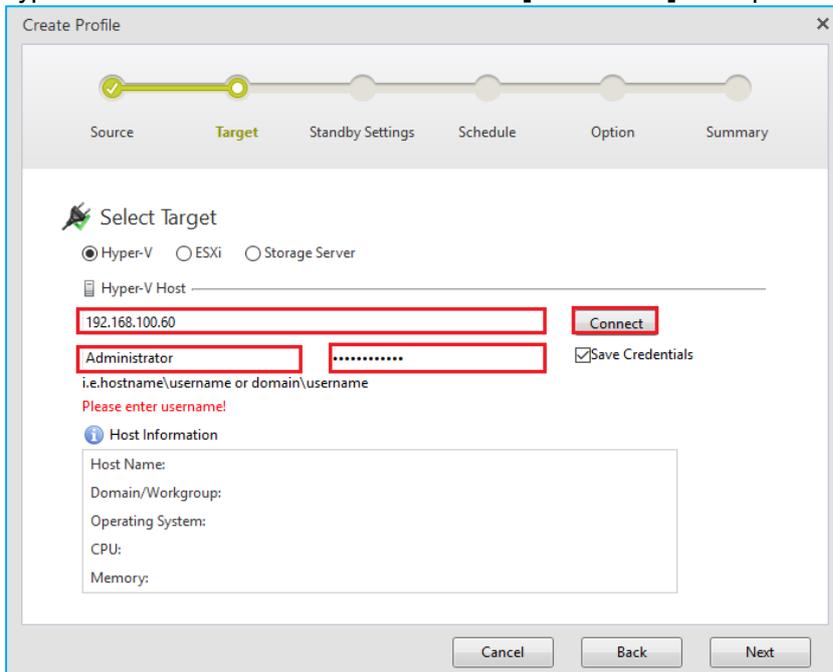
7. Right-click on the image file, in the dropdown menu click **[Create Task]**.



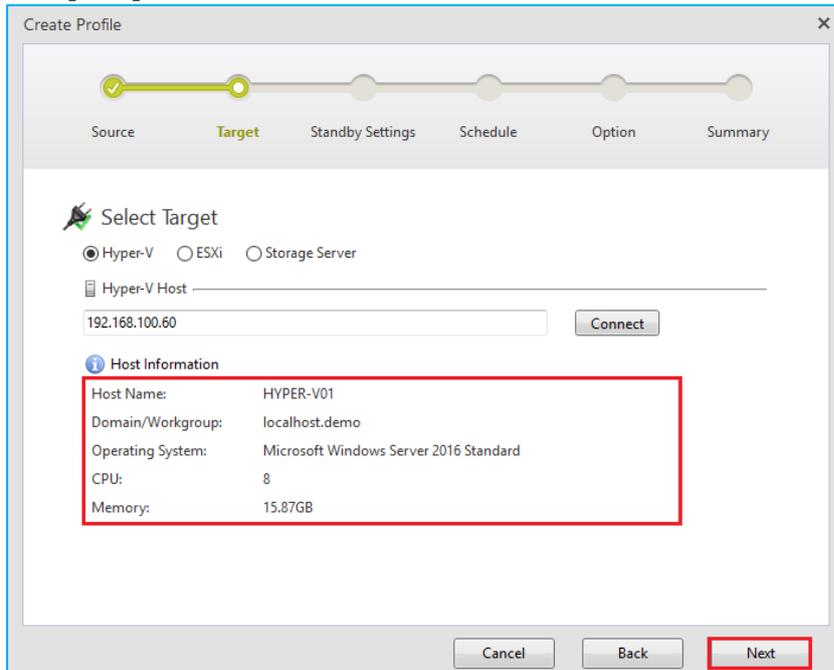
- The **[Create Profile]** window displays the information of the source backup. Please review the information of the backup and click **[Next]**.



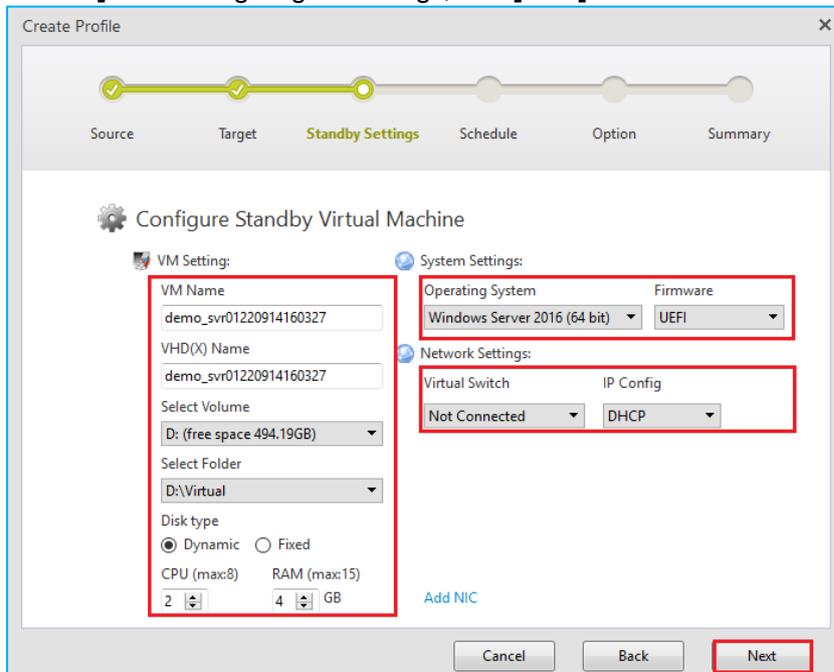
- Select the type of the hypervisor. You can select Microsoft Hyper-V or VMware vSphere (ESXi) as a target. The example screen below shows that "Microsoft Hyper-V" is selected for **[Hypervisor Type]**, and the IP address "192.168.100.60" is specified for **[Host Name or IP address]**. Enter the credentials to access the hypervisor. In this case "Administrator" for the **[User Name]** and a password for **[Password]**. Click **[Connect]**.



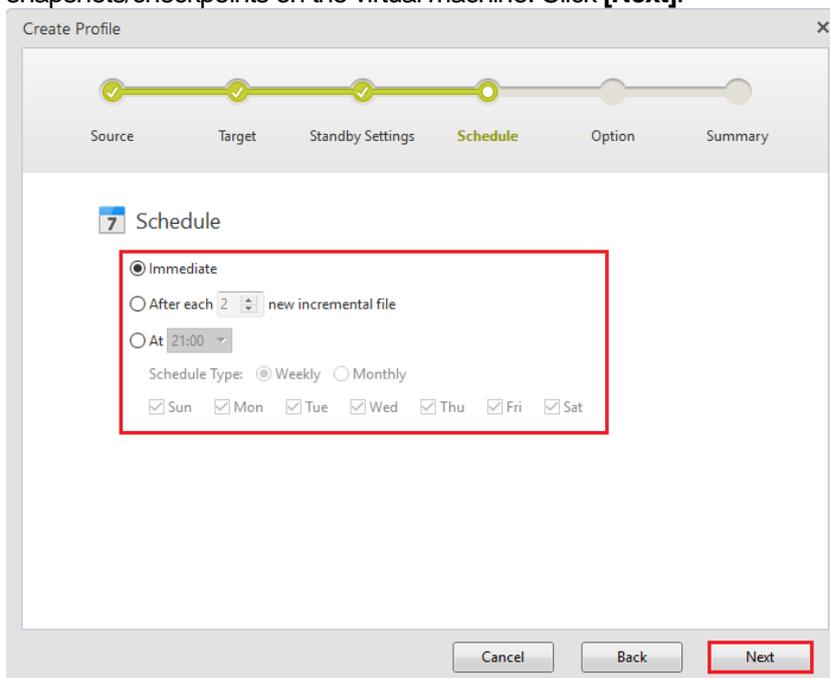
10. After connecting the hypervisor you can review its information in **[Host Information]**. Click **[Next]**.



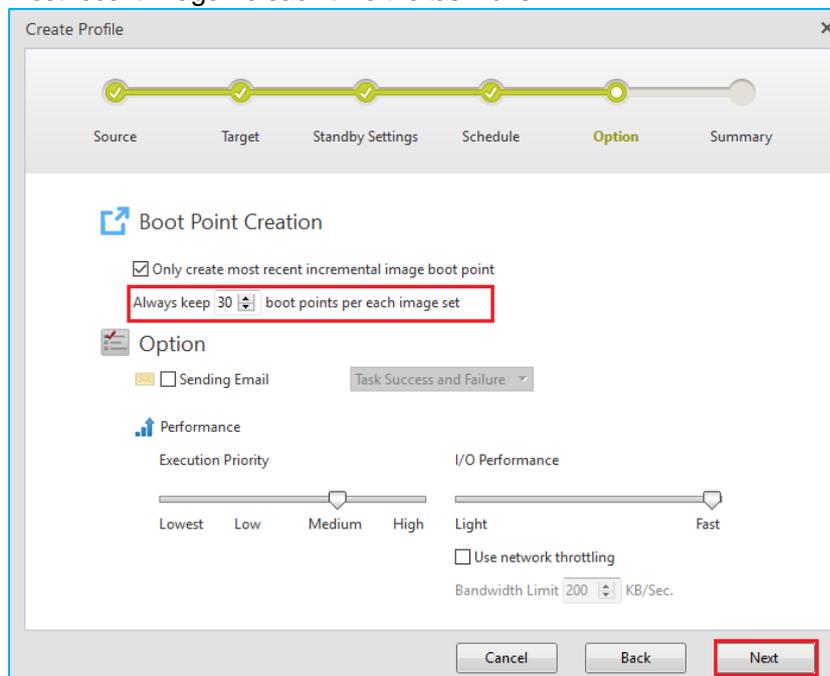
11. On the **[Configure Standby Virtual Machine]** window please configure the settings for the standby replica VM. The example below shows that the folder "Virtual" in "D drive" is selected as the destination for the virtual machine, the **[CPU]** is set to 2 with "4GB" for **[RAM]**, these are same values as backup source. In **[System Settings]** the operating system and firmware are automatically selected to be the same as the backup source. Please note, when selecting firmware that differs from the backup source, the virtual machine may fail to boot. "DHCP" is specified for **[IP address]** and the same values as the source have been selected for **[Virtual Switch:]**. After configuring the settings, click **[Next]**.



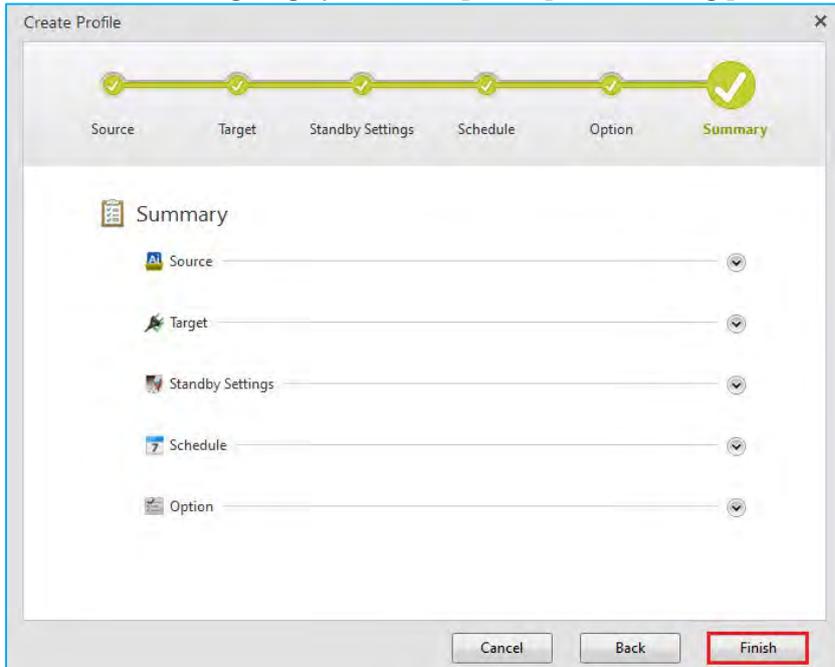
- Configure a weekly or monthly schedule for creating boot points on the virtual standby replica. This example shows that **[Immediate]** is selected. When backups are created, boot points for the backups as snapshots/checkpoints on the virtual machine. Click **[Next]**.



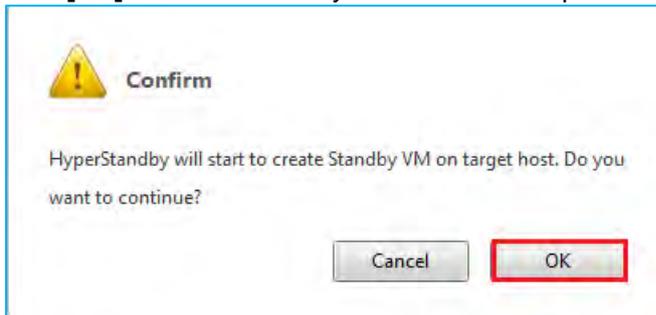
- Configure the option settings. Specify a limit for the number of boot points to create on the virtual standby replica (maximum is 30). When the specified number of the boot points reaches the predefined limit, the oldest boot point is merged into the VM. Enabling **[Only create most recent incremental image boot point]** option will create a boot point for the most recent image file each time the task runs.



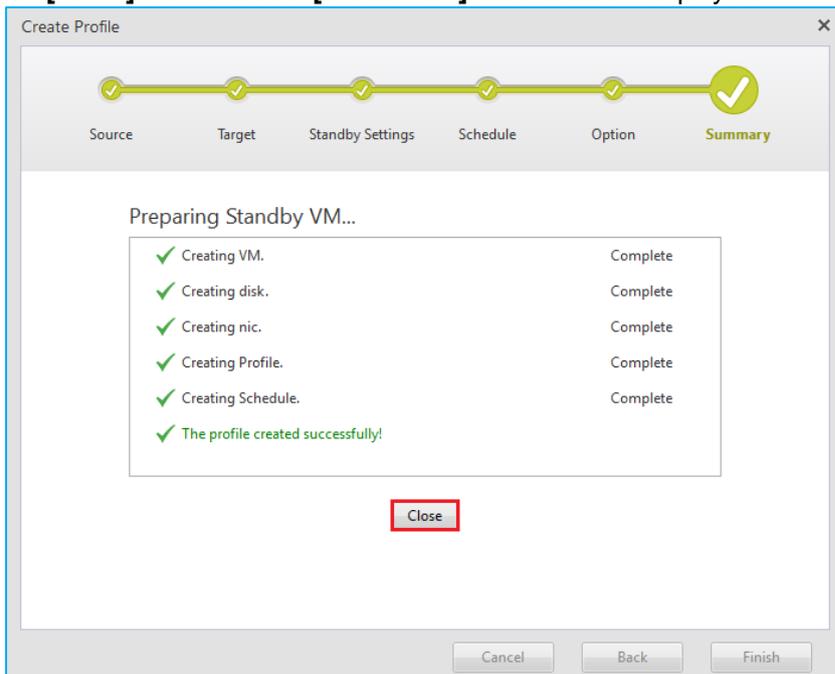
14. When finished configuring options, click **[Finish]**. The following **[Summary]** dialog is displayed.



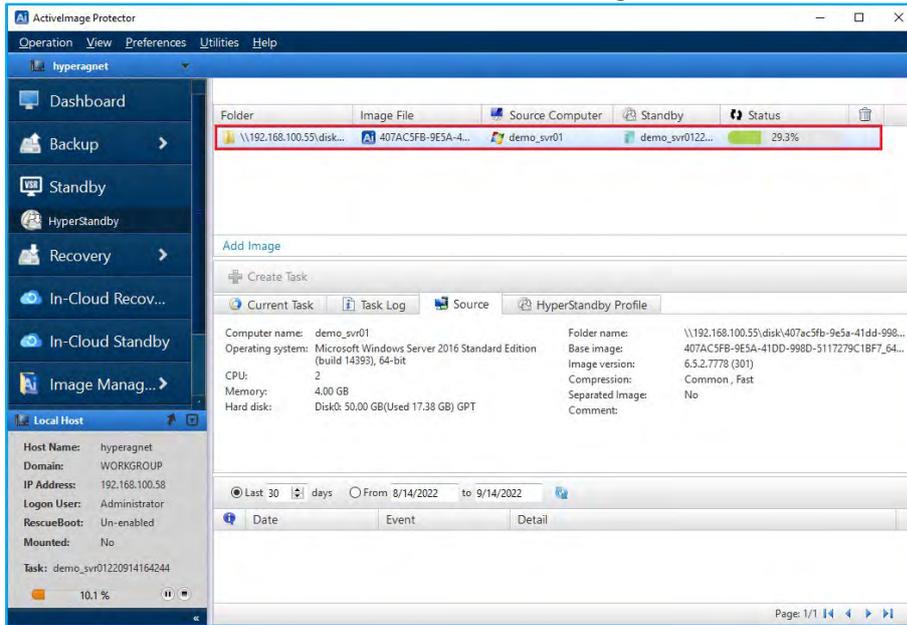
15. Click **[OK]** and virtual standby machine and task profile will be created.



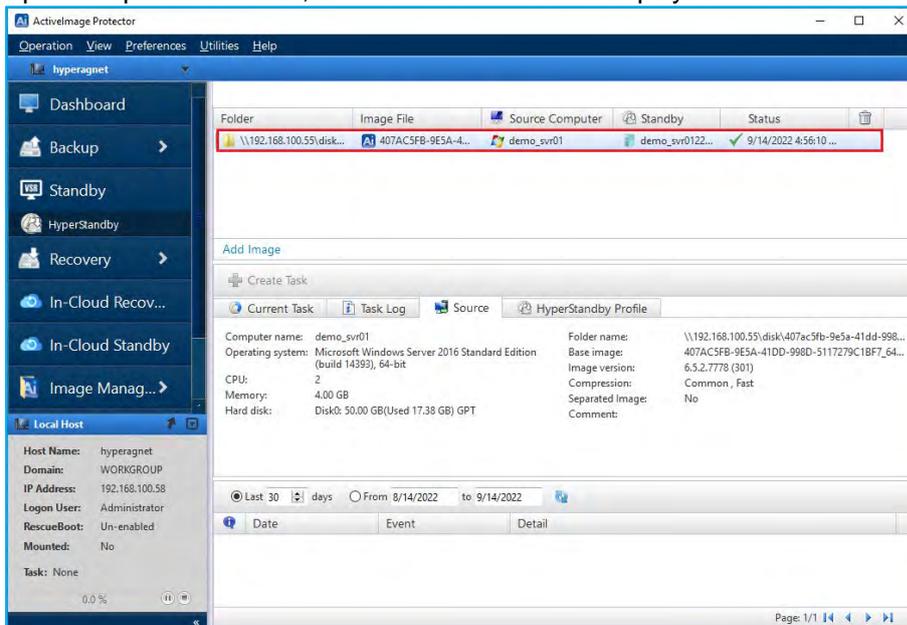
16. When virtual standby machine and profile creation process completes, the following dialog is displayed. Click the **[Close]** button and the **[Dashboard]** window will be displayed.



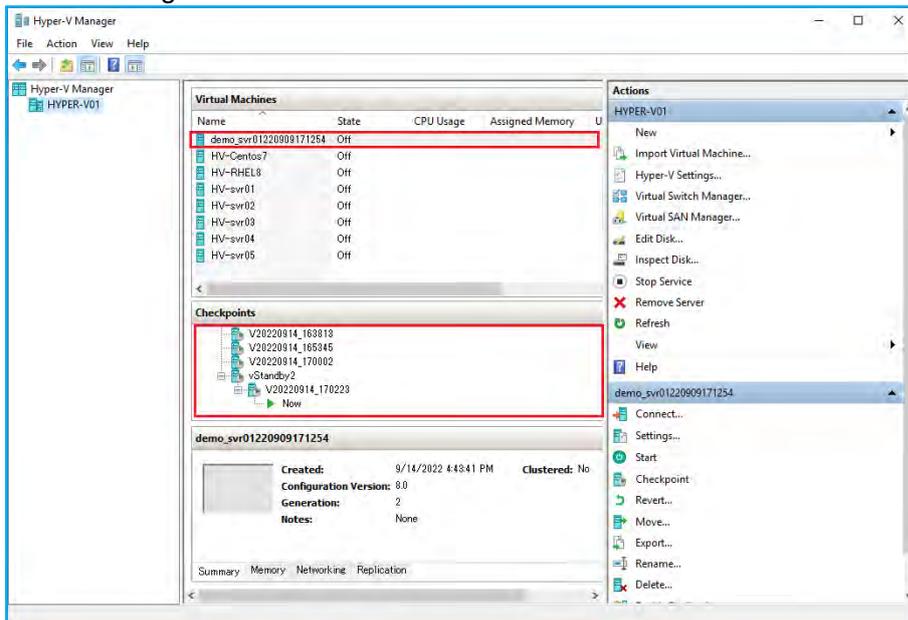
17. The dashboard view indicates the status of the running tasks.



18. Upon completion of a task, an information window is displayed in the dashboard.



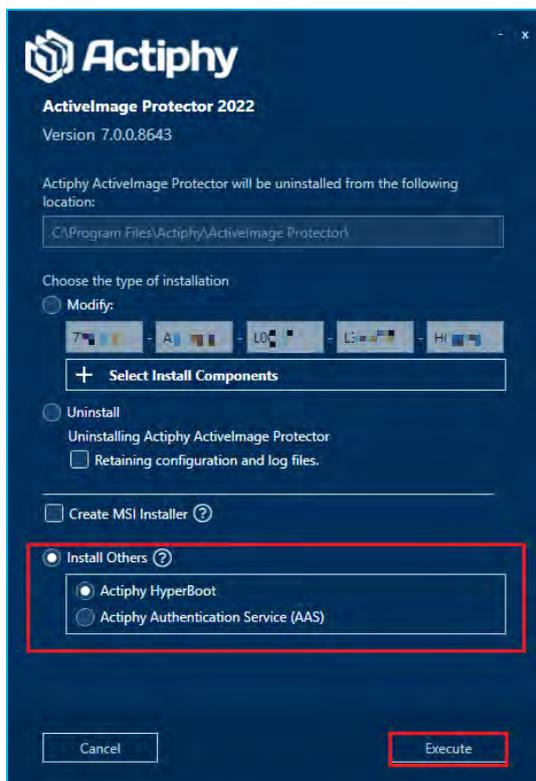
19. You can also monitor virtual standby machines from Hyper-V Manager or VSphere console. Checkpoints are added for the virtual standby machine as backups complete. When an emergency occurs, the virtual standby machine can be booted from a point in time as the interim server or a migrated server.



8-2. HyperBoot

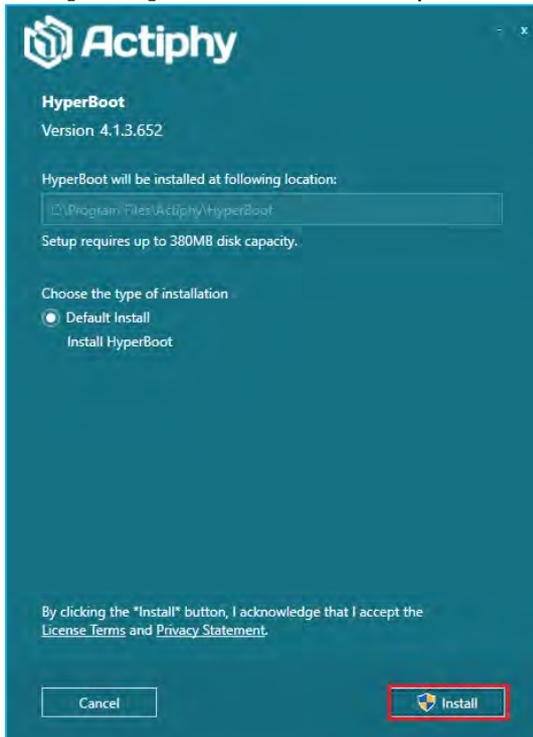
HyperBoot is a free standalone add-on that can boot any ActiImage Protector backup image as a virtual machine in minutes, bypassing lengthy physical to virtual conversion and recovery process. You can install HyperBoot from the ActiImage Protector installer in the product media. The following is a description about the operating procedures of HyperBoot.

1. Run "Setup.exe" directly from the product media and start the installer. Select **[Install Others]** → **[ActiImage HyperBoot]** → **[Execute]** and click **[Execute]**.

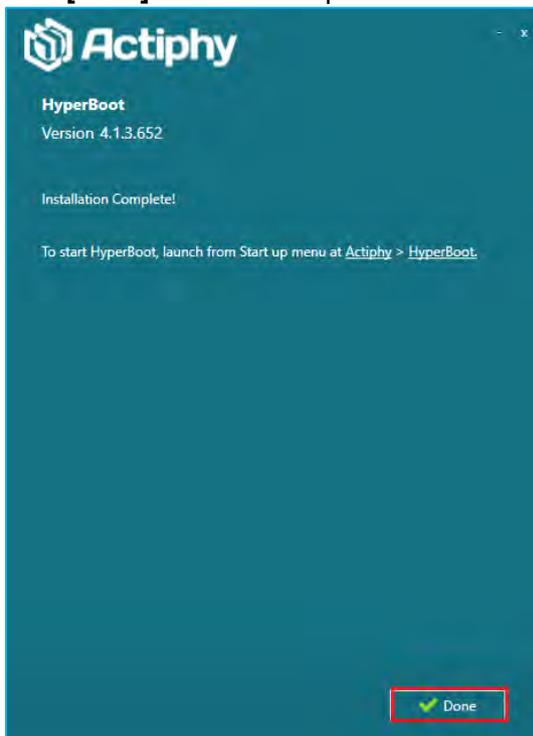


Creates and maintains dormant virtual replicas

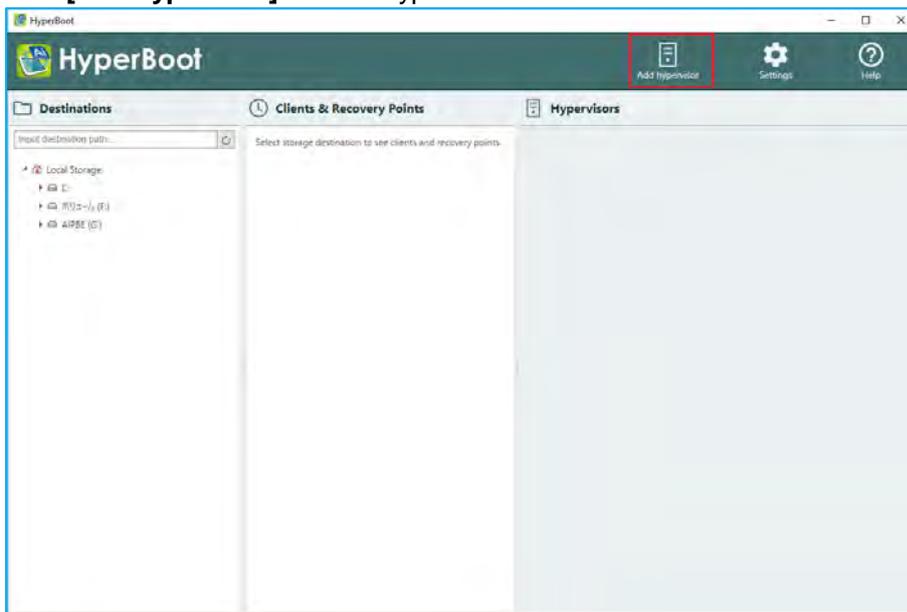
2. When setting up HyperBoot, there are no additional options to set. Click **[Install]** to start the installation process.



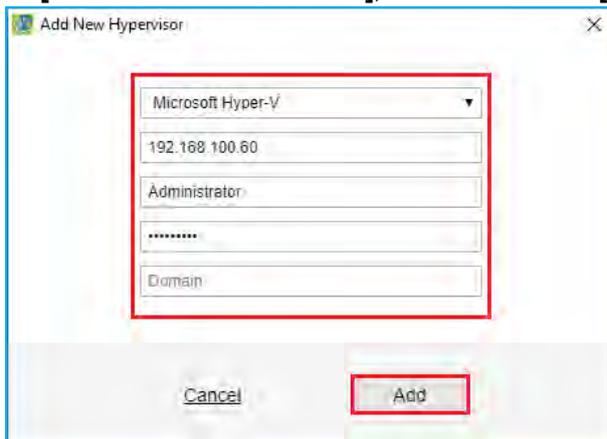
3. When the following window is displayed, installation process completed. Click **[Done]** to end the setup wizard.



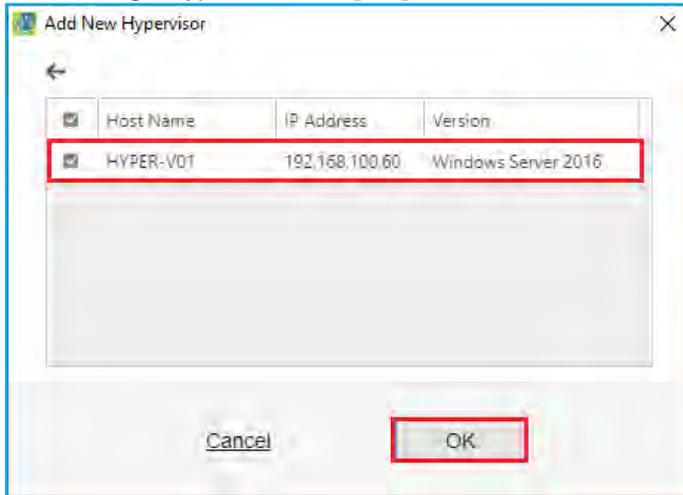
4. Start HyperBoot. Go to Windows Start menu and select **[Actiphy]** → **[HyperBoot]**.
5. Click **[Add Hypervisor]** to add a hypervisor to boot virtual machine.



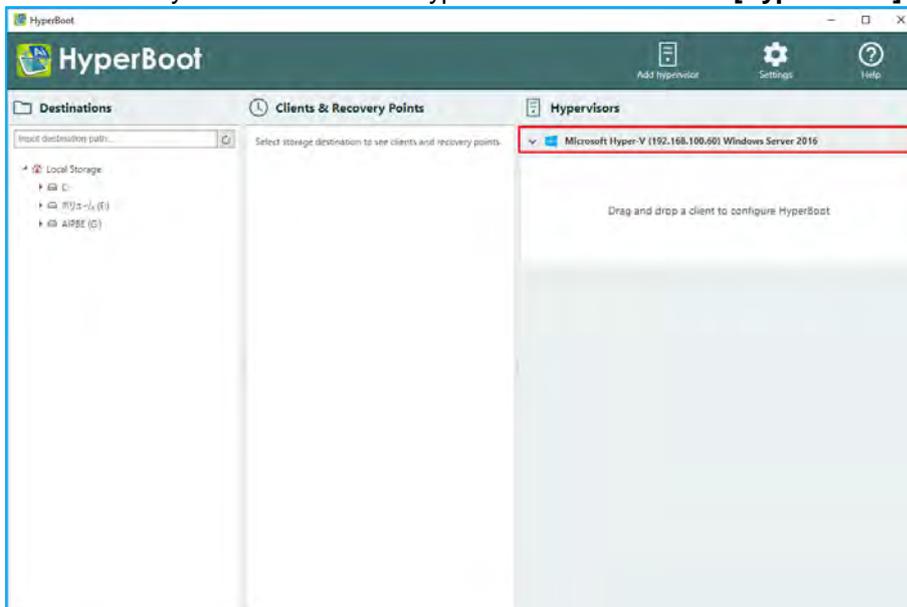
6. This example shows that "Hyper-V" is selected for **[Add Target:]**, IP address of Hyper-V host "192.168.100.60" for **[Host Name or IP address:]**, "Administrator" for **[User Name:]** and Password. Click **[Add]**.



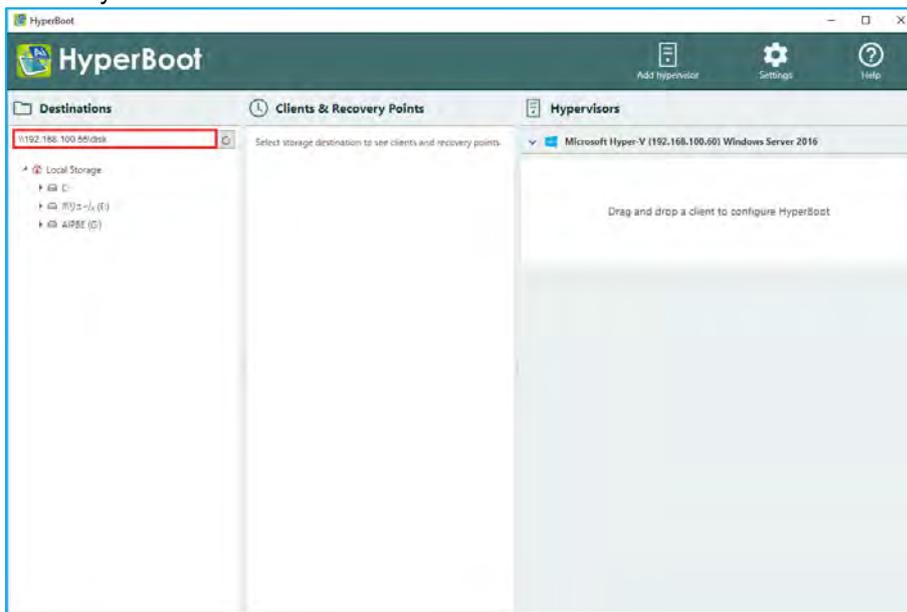
7. After adding a hypervisor click **[OK]**. The software we return to the default console.



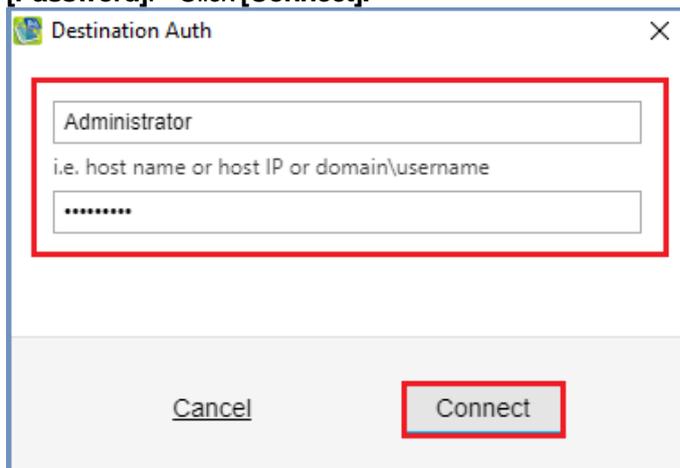
8. In the console you can confirm that Hyper-V has been added to **[Hypervisors]**.



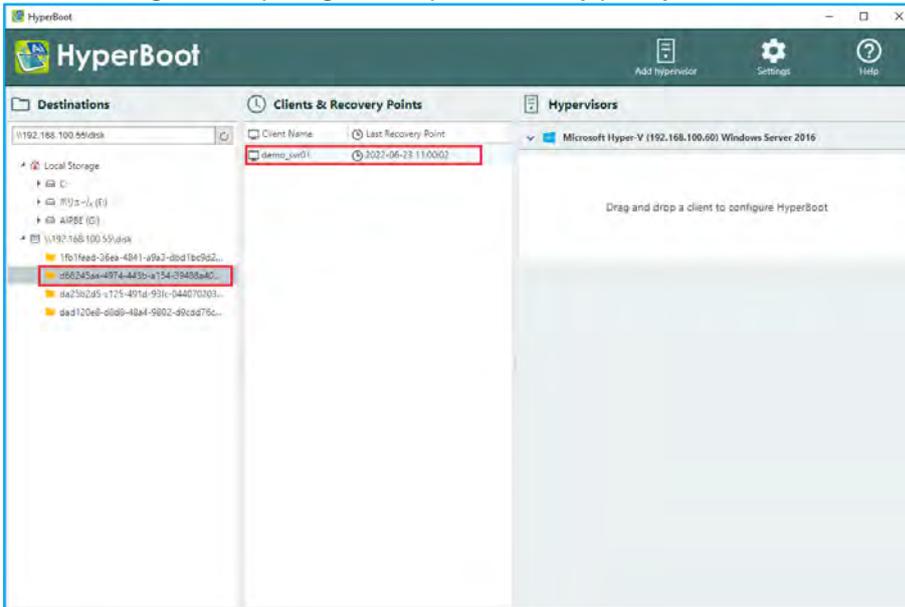
9. Select the recovery point of AclImage Protector backup from **[Destinations]**. This example shows that "192.168.100.55\disk" is entered for the shared folder destination point containing image files. Press the Enter key.



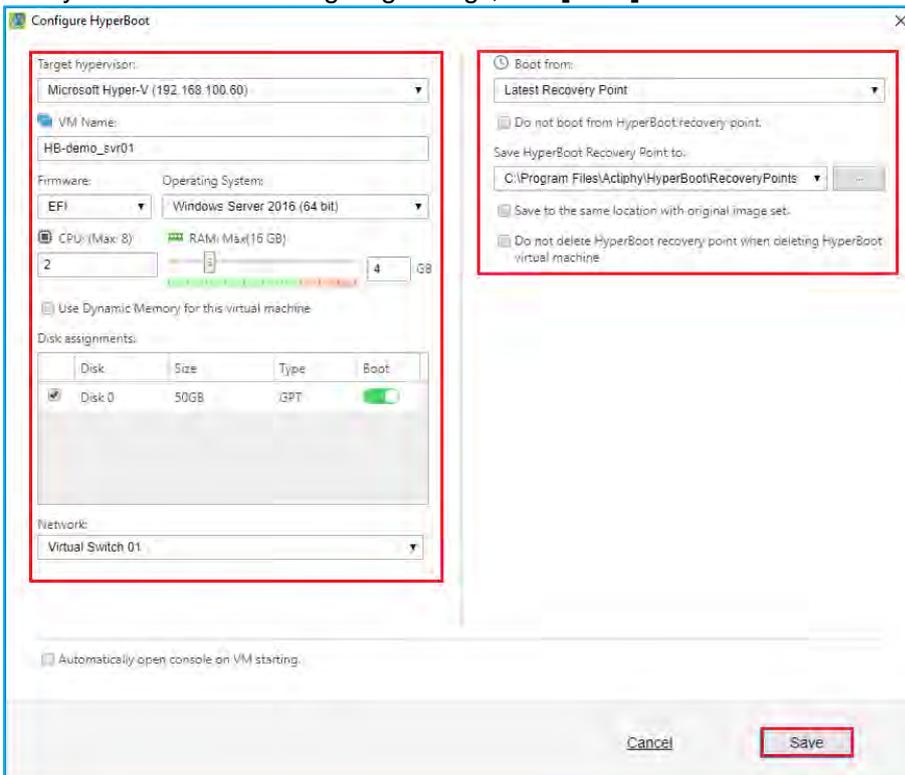
10. In **[Destination Auth]** dialog, please enter your credentials for the shared folder, **[User Name:]** and **[Password]**. Click **[Connect]**.



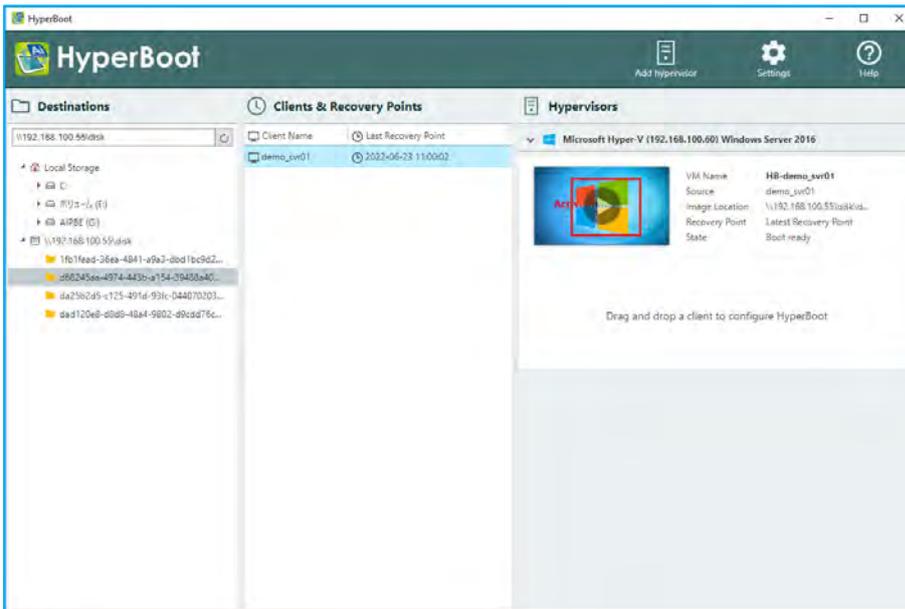
- After selecting a backup drag and drop the recovery point you want to boot to the blank in right pane.



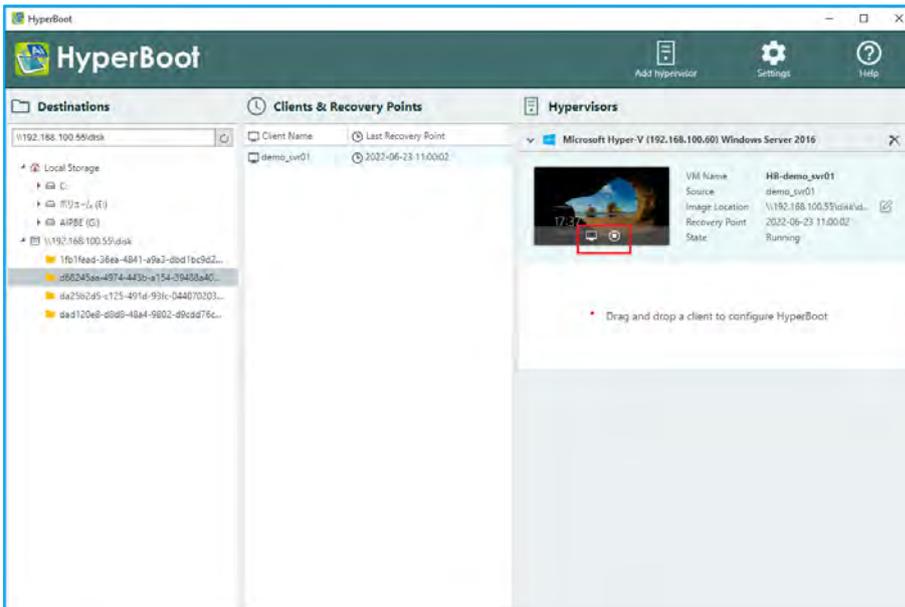
- In this example, “Microsoft Hyper-V” is selected for **[Target hypervisor]**. Please configure the settings for **[CPU]**, **[RAM]**, **[Network]**, etc. If necessary, please change **[VM Name:]**. A default path is configured for the setting **[Save HyperBoot Recovery Point to:]**. However, enabling **[Save to the same location with original image set.]** option will create the config file in the same folder as the backup images. This might be convenient when booting backup images on a different host using HyperBoot. After you have finished configuring settings, click **[Save]**.



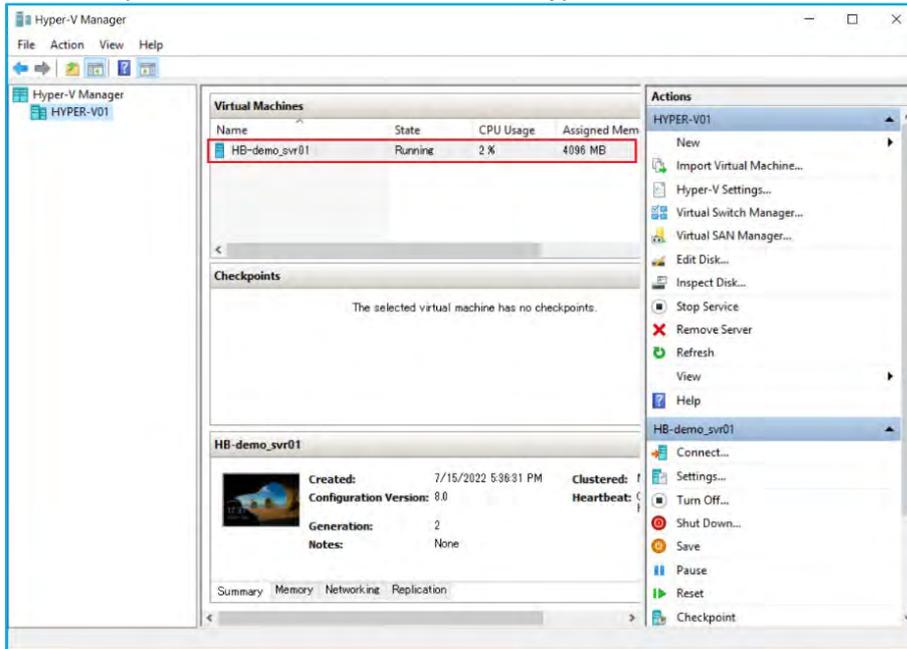
- The information for the virtual machine is displayed in **[Hypervisors:]**. Click on "▶" to start the virtual machine.



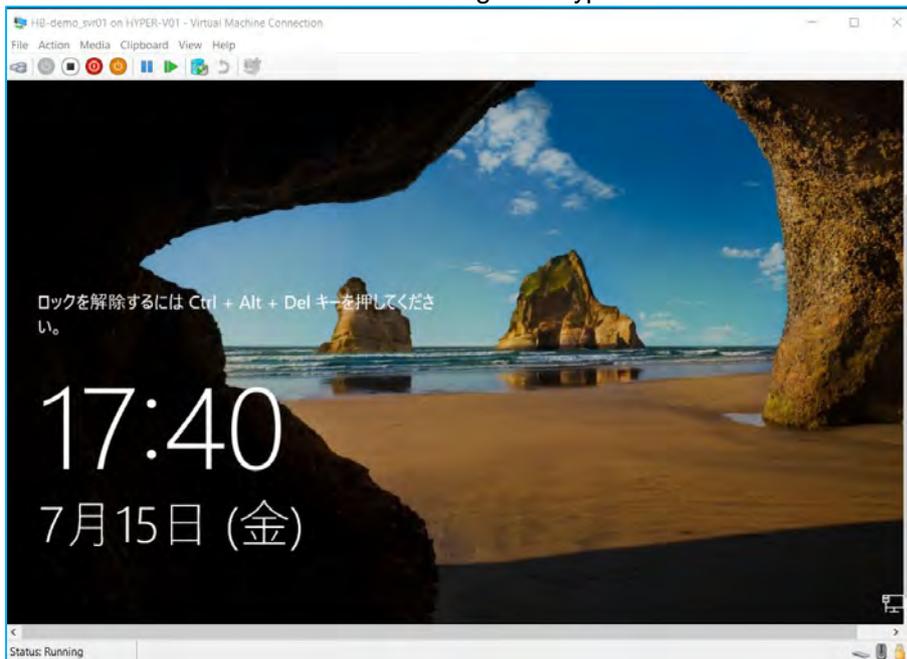
- Click on the left icon to launch the VM connection console.



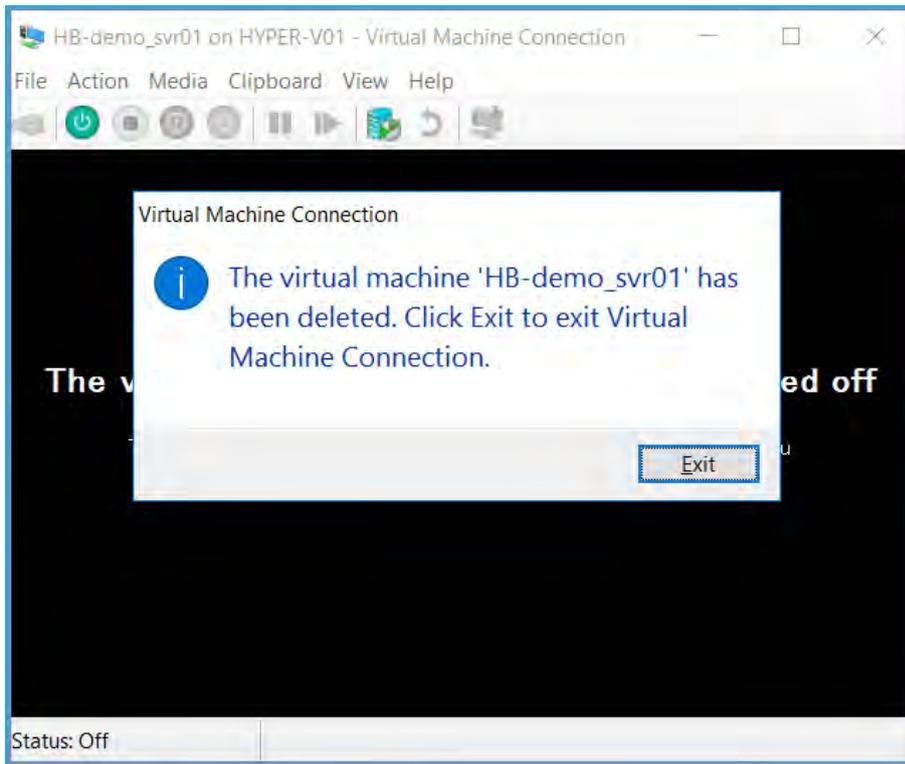
15. The backup is booted as a virtual machine on Hyper-V.



16. You can access the virtual machine through the Hyper-V console.



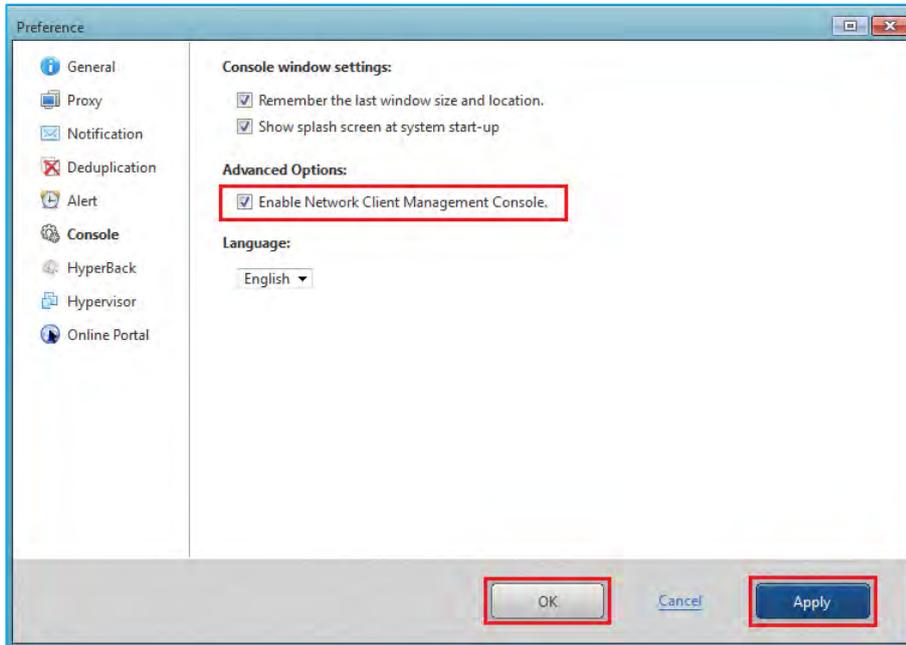
17. When you power down the virtual machine, HyperBoot will delete it. If the console is still open, Hyper-V will display the following message. Click the **[Exit]** button to disconnect from the virtual machine and close the console.



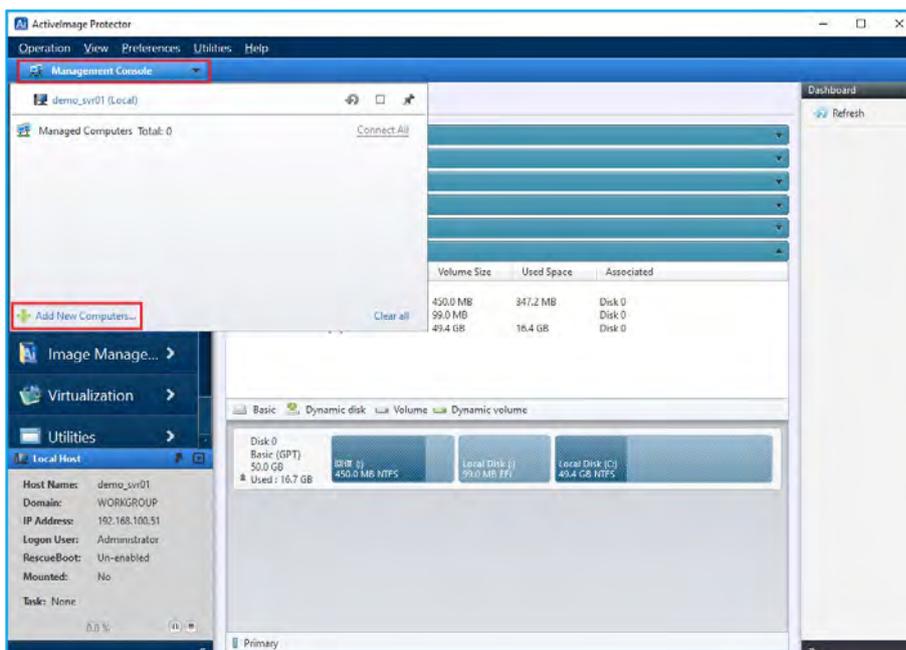
9. Remote Management Console

Monitor the status of ActiveImage Protector agents installed on a networked remote host.

1. Go to Windows Start menu - **[Actiphys]** → **[ActiveImage Protector]**.
2. Go to **[Preference]** → **[Console]** and check in the checkbox for **[Enable Network Client Management Console]** and click **[Apply]**. Click **[OK]** and go back to Dashboard.

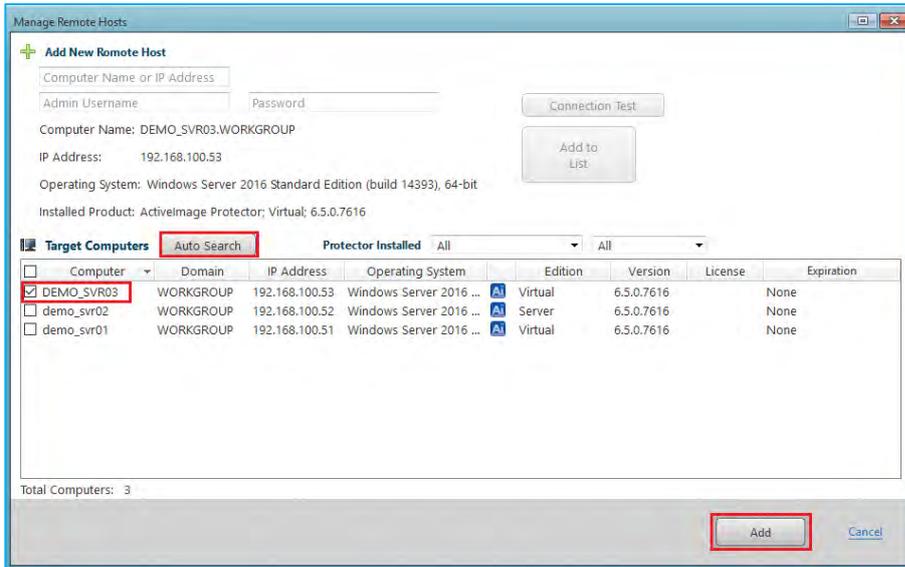


3. Click **[Management Console]** located in the upper left of the window. Before using the Remote Control feature, you need to add any clients you wish to control to the list of Managed Computers. Click **[Add New Computer]**.

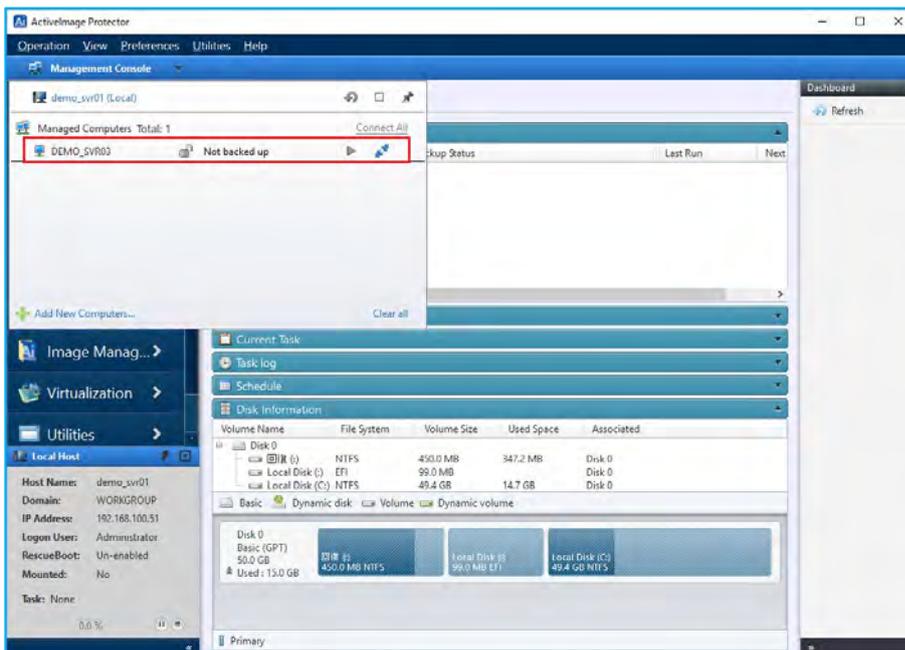


Remote Management Console

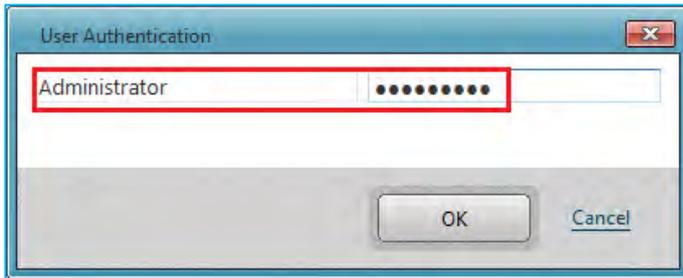
- You are presented with two options to add clients **[Auto Search]** and **[Manual Setting]**. In this example, **[Auto Search]** and **[All]** versions are selected. After the search has completed we tick the checkbox for the computer "DEMO_SVR03", which has ActiveImage Protector installed, and click **[Add]**.



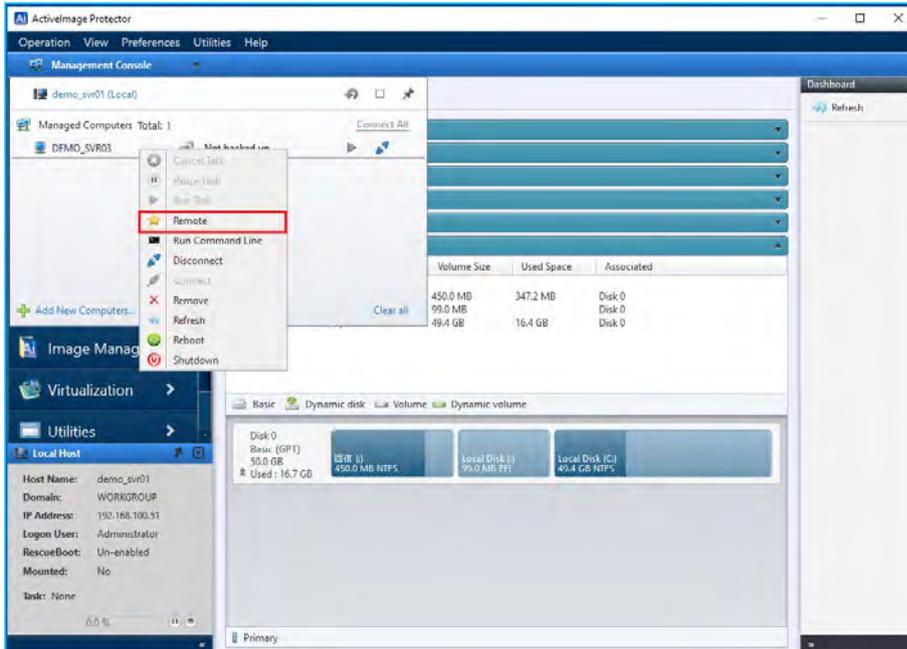
- The client is added to the list of Managed Computers. Select and double-click on any client from the list. A **[User Authentication]** dialog will be displayed.



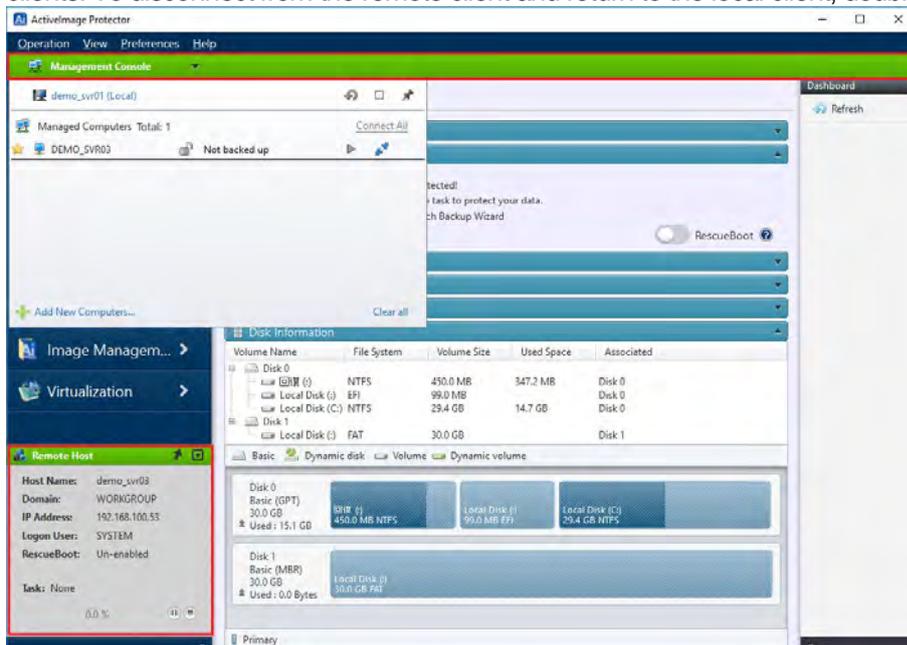
- Enter the credential information to access the client.



- After a client is connected, you are able to perform remote operations on the client. Right clicking a client will display a menu, from that menu click on remote to remote control the console on the client.



- When the remote console is successfully established, the status bar will turn green. After having connected one time, you only need a single click to reconnect in the future. Most operations such as running backup/recovery tasks, image management operations and monitoring log information can be done on remote clients. To disconnect from the remote client and return to the local client, double click on the local host name.



10. Reference

- **Actiphy's Web site:**
Actiphy's Web site provides access to comprehensive information, including product information, related documents, technical support, updates, etc.
<https://www.actiphy.com/global>
- **Knowledge Base**
<https://enkb.actiphy.com/>
- **Activelmage Protector Help Center**
Support information is accessible at the following web site.
<https://actiphylhelp.zendesk.com/hc/en-us>
- **For any inquiries about Activelmage Protector, please contact:**
Global Sales Dept., Actiphy Inc.
E-mail: global-sales@actiphy.com

Copyright © 2023 Actiphy, Inc. Actiphy, Inc. All rights reserved.

Activelmage Protector and related documents are proprietary products copyrighted by Actiphy, Inc.

Other brands and product names mentioned in this guide are trademarks or registered trademarks of their respective holders.