

# ActiveImage Protector 2022 Server Setup Guide

6th Edition February, 2024



## Contents

---

1. Overview.....	3
System Requirements.....	3
2. Installation.....	4
3. Product Activation.....	6
4. Configure backup settings and run backup tasks.....	7
4-1. Volume Backup: One Time Only.....	7
4-2. Volume Backup: Scheduled Backups.....	13
4-3. File Backup : Schedule File Backup.....	25
4-4. Agentless Backup (HyperBack).....	33
5. Boot Environment Builder .....	47
Build Windows-PE based Boot Environment .....	47
6. Restore .....	52
6-1. File / Folder Recovery.....	52
6-2. System Recovery : Standard Linux-based boot environment.....	57
6-3. System Recovery : Windows RE-based boot environment.....	64
6-4. Create a new virtual machine from backup image file (HyperRecovery).....	70
6-5. Zero Time Recovery (HyperRecovery LIVE!).....	75
6-6. Cloud Recovery (In-Cloud Recovery) .....	80
7. Image Management – Image Manager .....	88
7-1. Image Manager .....	88
7-2. Check for bootability of backups (BootCheck) .....	89
7-3. Quick Verify .....	91
7-4. Consolidation .....	93
7-5. Archive Backups .....	95
7-6. MD5 Checksum.....	97
7-7. Delete Backup Files.....	99
8. Image Manager: Mount Image .....	100
9. Image Manager: Image Target Server .....	102
10. Remote Management Console.....	110
11. Creates and maintains dormant virtual replicas.....	113
11-1. vStandby .....	113
11-2. HyperStandby .....	120
11-3. HyperBoot .....	129
12. Reference.....	138

## 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 Server (February 2024 Update: Version. 7.0.3.8919). We recommend you read this manual before using ActiveImage Protector 2022 to configure backups. Please visit our online help for more detailed information ( [https://webhelp.actiphy.com/AIP/2022/en\\_US/](https://webhelp.actiphy.com/AIP/2022/en_US/)).

### System Requirements

Please ensure your computer meets these minimum system requirements before using ActiveImage Protector 2022 Server (Version. 7.0.3.8919):

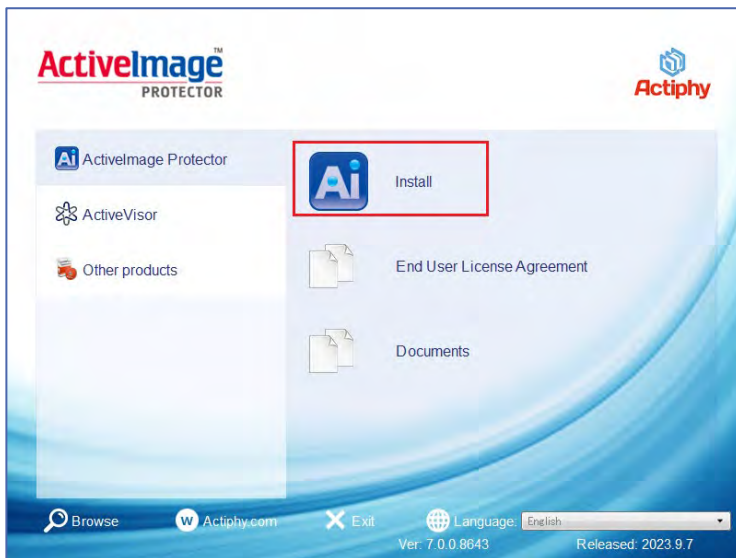
<b>CPU</b>	Pentium 4 or newer.
<b>Main Memory (RAM)</b>	4GB of RAM or greater. (8GB or more is recommended.)
<b>Hard Disk</b>	1.5GB of available disk space or greater.
<b>Supported Operating Systems</b>	<p>Windows:</p> <ul style="list-style-type: none"> <li>• Windows Server 2022</li> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server IoT 2019 / 2022 for Storage</li> <li>• Windows Storage Server 2016</li> <li>• Windows Storage Server 2012 R2</li> </ul> <p>Hypervisor:</p> <ul style="list-style-type: none"> <li>• Windows Server 2022 Hyper-V</li> <li>• Windows Server 2019 Hyper-V</li> <li>• Windows Server 2016 Hyper-V</li> <li>• Windows Server 2012 R2 Hyper-V</li> <li>• VMware vSphere ESX[i] 6.0 / 6.5 / 6.7 / 7.0 / 8.0</li> <li>• Citrix Hypervisor 8.2</li> <li>• Proxmox VE 7.2-1</li> <li>• Nutanix Acropolis Hypervisor (AHV) 20190916.276</li> </ul> <p>* ActiveImageProtector 2022 Server also supports these operating systems as the guest OS on supported hypervisors.</p> <p>* Please refer to our <a href="#">knowledge Base</a> for information on the backup source OS for HyperAgent.</p>

**\*For the latest system requirements for this product, please visit Actiphy's Web site.**  
 (<https://www.actiphy.com/en-us/support/system-requirements/>)

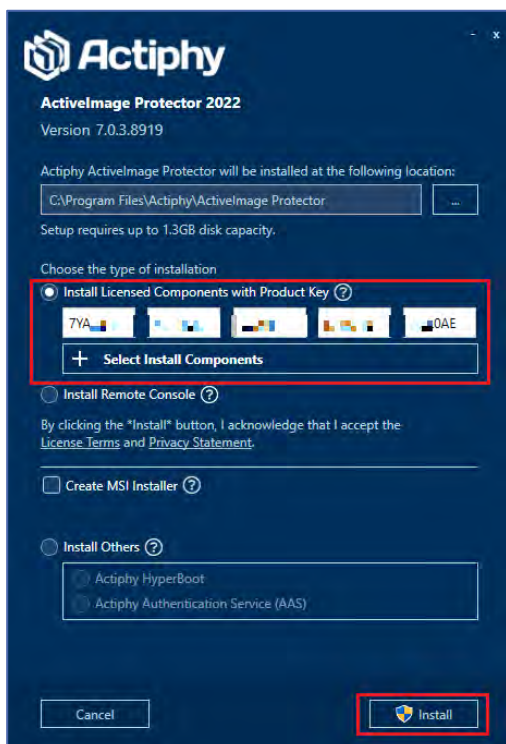
## 2. Installation

The following steps will show you how to install ActiveImage Protector on the computer you wish to keep backed up:

1. Insert the installation disc into your computer. Windows should automatically launch the ActiveImage Protector install screen. If Windows doesn't automatically start the installer, double-click on the *launch.exe*. Or run *setup.exe* files in Setup folder on the installer disc. Once you have the ActiveImage Protector install screen running, click on **[ActiveImage Protector]** → **[Install]**.



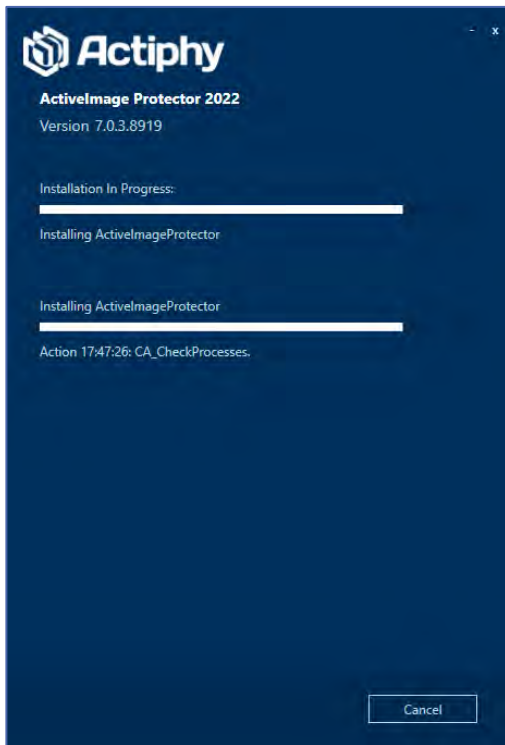
2. Next, insert your product key in the "Install Licensed Components with Product Key" field and click the **[Install]** button to start the installation process.



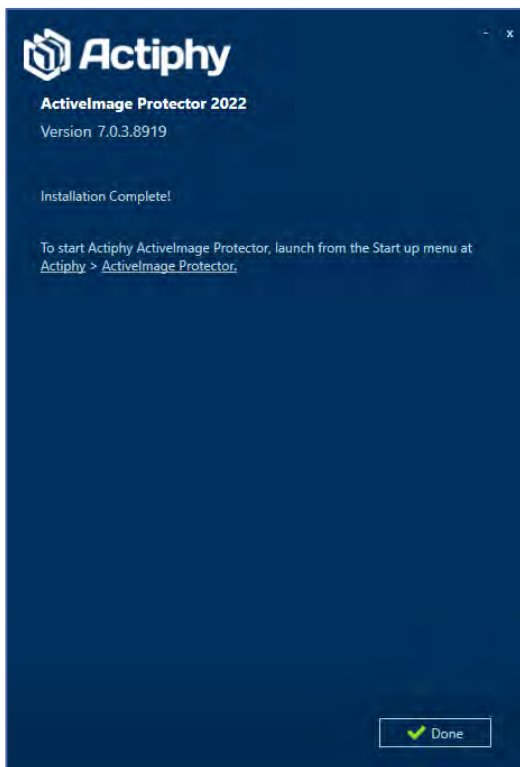


## Installation

3. The program will begin installing ActiImage Protector on your computer and show you its progress.



4. Click on the **[Done]** button when the installer has finished. You **do not need to reboot your system** after installation.



### 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:

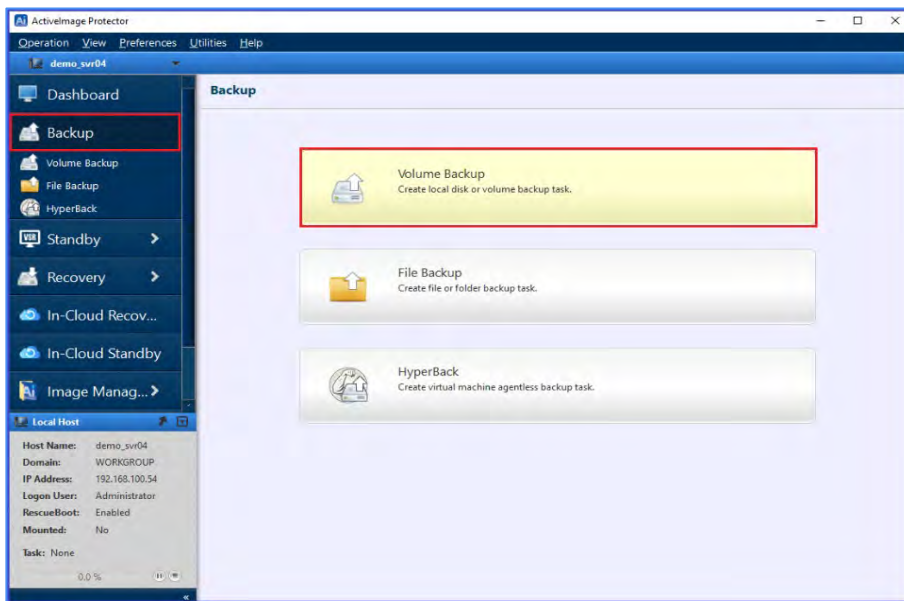
- ActiveImage Protector 2022 Server:  
[https://www.actiphy.com/global/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_server](https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_server)
- ActiveImage Protector 2022 Desktop:  
[https://www.actiphy.com/global/activation\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_desktop](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](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](https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_virtual)
- AAS Docker:  
[https://www.actiphy.com/global/activation\\_guide/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](https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_license_recovery_guide)

## 4. Configure backup settings and run backup tasks

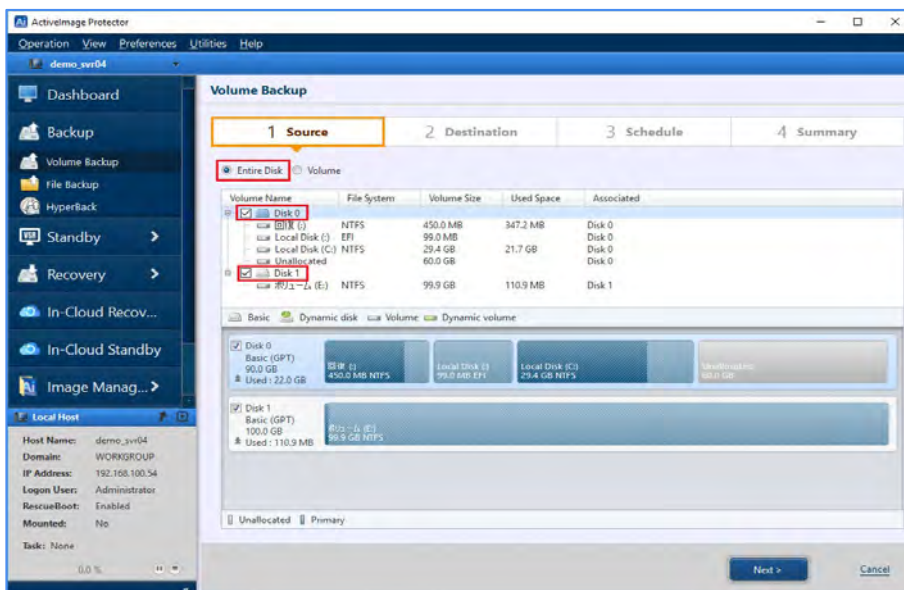
### 4-1. Volume Backup: One Time Only

Use the following steps to run ad hoc backup tasks:

1. Launch ActiImage Protector by clicking on the Windows Start menu and then navigating to **[Actiphy]** → **[ActiImage Protector]**.
2. Once inside ActiImage Protector, click on **[Backup]** → **[Volume Backup]**.

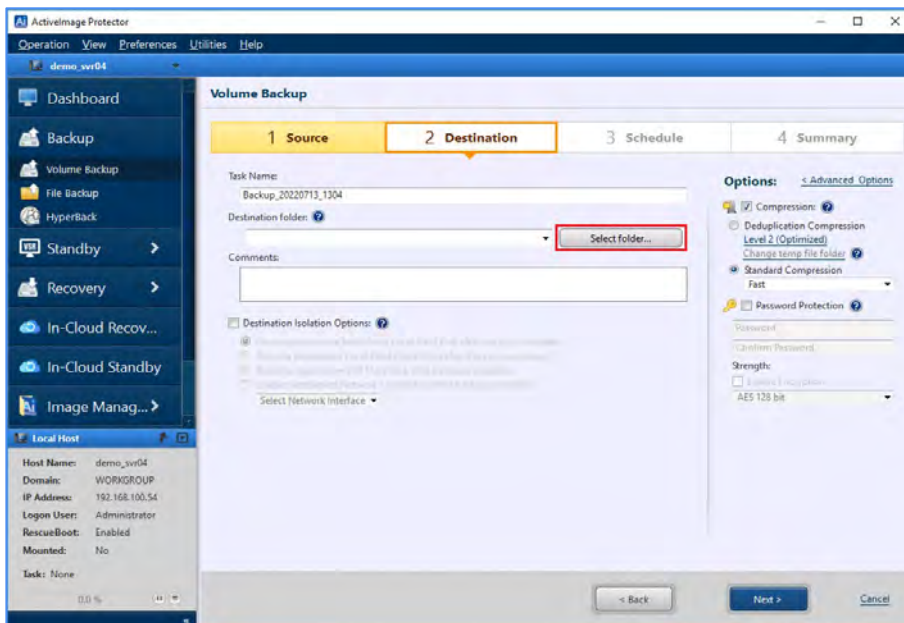


3. Select a backup source. The following example shows the entire disk selected for the backup source. Click **[Entire Disk]** and check the checkbox for **[Disk 0]** and **[Disk 1]**. When the backup source is selected, click **[Next]**.

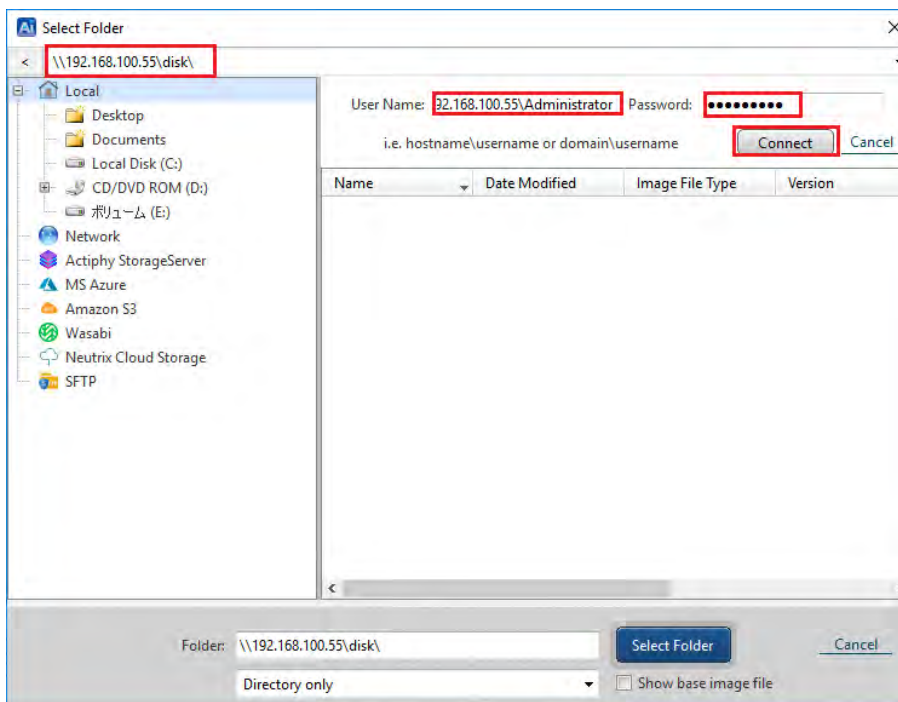


## Configure backup settings and run backup tasks

4. Select a destination folder for the backup image. The following example shows \\192.168.100.55\disk in the network shared folder as the destination. Click the **[Select Folder]** button.

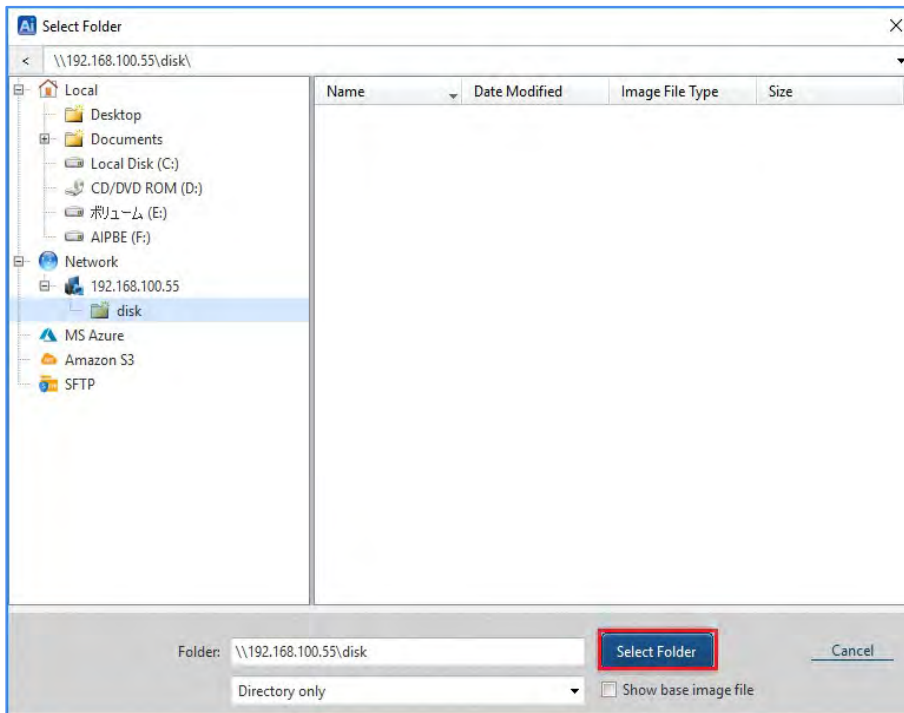


5. Enter \\192.168.100.55\disk as the destination in the shared folder field and press the **[Enter]** key. Next, enter your credentials to log into the destination folder. For example, enter 192.168.100.55\Administrator in the **[User Name]** field and your password in the **[Password]** field. Finally, click on the **[Connect]** button.

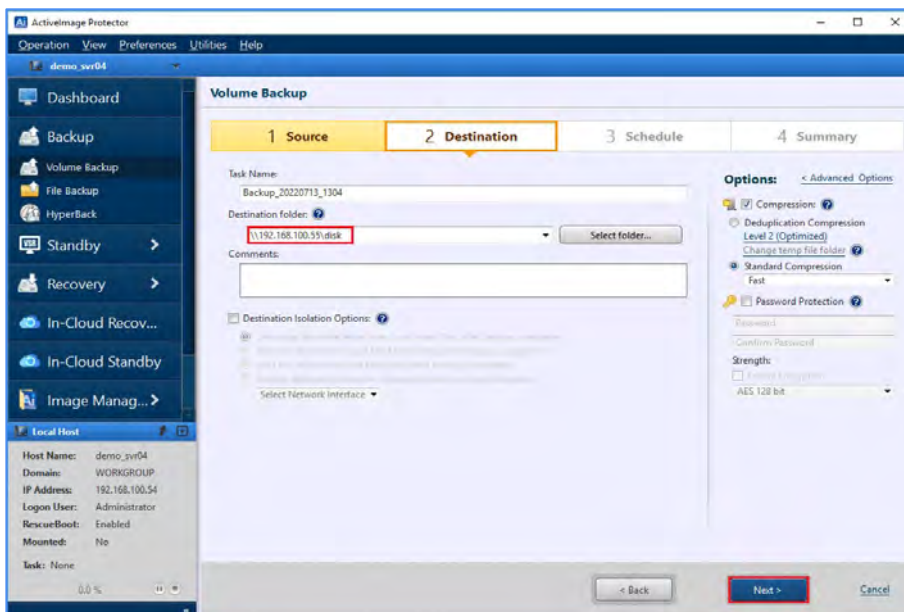


## Configure backup settings and run backup tasks

6. Ensure you have correctly specified the destination shared folder and click the **[Select Folder]** button.



7. Ensure you have selected a shared folder for the destination. Then, click the **[Next]** button. The Destination Isolation feature, and compression & encryption options are available at the bottom and the right side of the screen. Please refer to section **4-2 Volume Backup: Scheduled Backups** of this document for more information.



## Configure backup settings and run backup tasks

8. Select **[Backup Once]** for the Task Type and click **[OK]**.

**Schedule Settings**

Backup\_20220713\_1304      Effective Date/Time: 2022/07/13 13:22 ~ 2023/07/13 13:22    ☒ Not Specified

Task Type: ☒ **Backup Once**    ☐ Schedule Backup

**Base** ?  
☒ Monthly    ☐ Weekly    ☐ Daily    ☐ Monthly    ☐ Quarterly    ☐ Annually

**Incremental** ?  
☒ Weekly    ☐ Monthly    ☐ Quarterly    ☐ Annually

☒ Multi-times  
Start Time: 07:00    End Time: 21:00    Interval: 60 Minutes

☐ One-time only    13:22

Execute Time: 13:22

[Add New Base](#)    [Add New Incremental](#)

**Event Backup:**  
☐ Shutdown/Reboot    ☒ Base and Incremental

**Option:**  
☐ Auto run if a scheduled task is missed.  
☐ Run base backup if scheduled base backup task has been missed.

**OK**    **Cancel**

Click **[Next]** in this example.

**ActiveImage Protector**

Operation View Preferences Utilities Help

demo\_srv04

**Volume Backup**

1 Source    2 Destination    **3 Schedule**    4 Summary

Task type: Backup Once  
Effective From: 7/13/2022 1:22 PM  
Base (Full): Incremental  
[Edit Schedule](#)

**Post-backup Process:**  
☒ BootCheck: Unconfigured    ☒ ImageVerify: Unconfigured    ☒ Consolidation: Unconfigured  
☒ Replication: Unconfigured

**Options:**  
☐ Preserve Replication/Image    ☒ Delete both full and incrementals  
Number of image sets to retain: 3  
☐ Delete the older image before every task backup.  
☐ Reschedule: Task failed

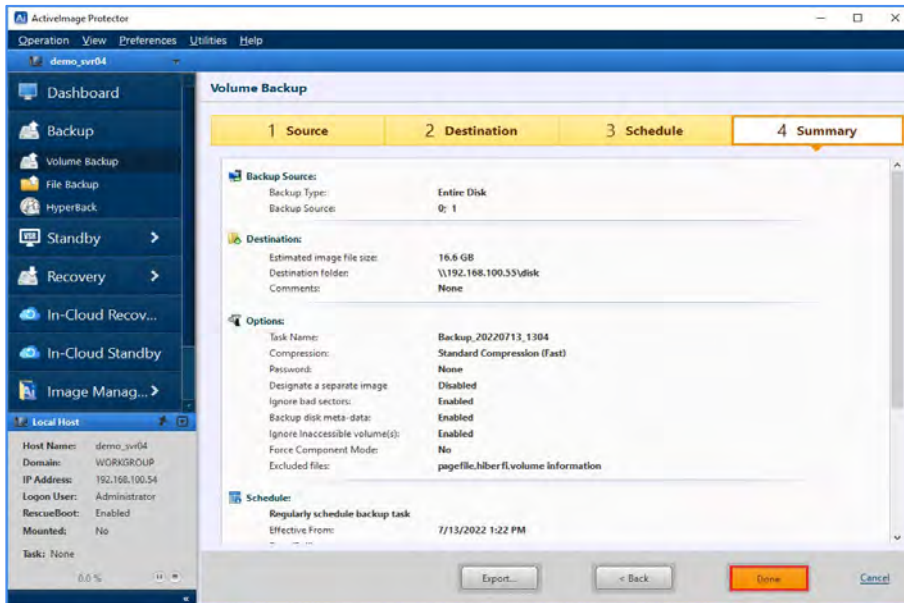
**Execution Priority:**  
Full (Base): Lowest Low Medium High  
Incremental: Lowest Low Medium High

**Next >**    **Back**    **Cancel**

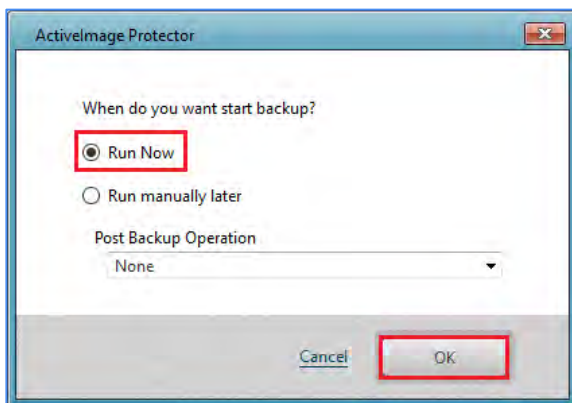


## Configure backup settings and run backup tasks

- Review the summary for the configured settings and click **[Done]** to start the backup task.

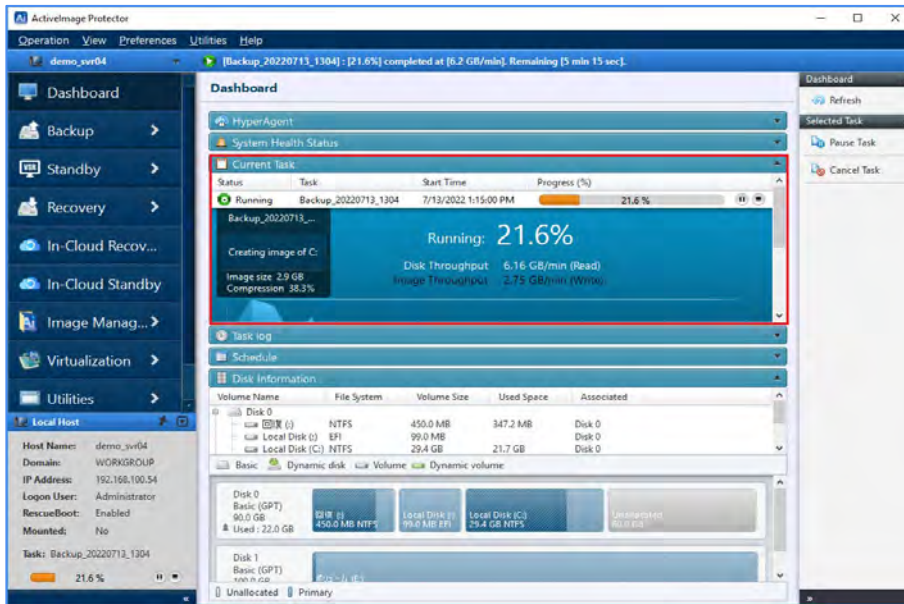


- Select **[Run Now]** and click **[OK]** to start backup task. **[Post Backup Operation]** may be selected to shut down or restart the system upon the completion of backup.

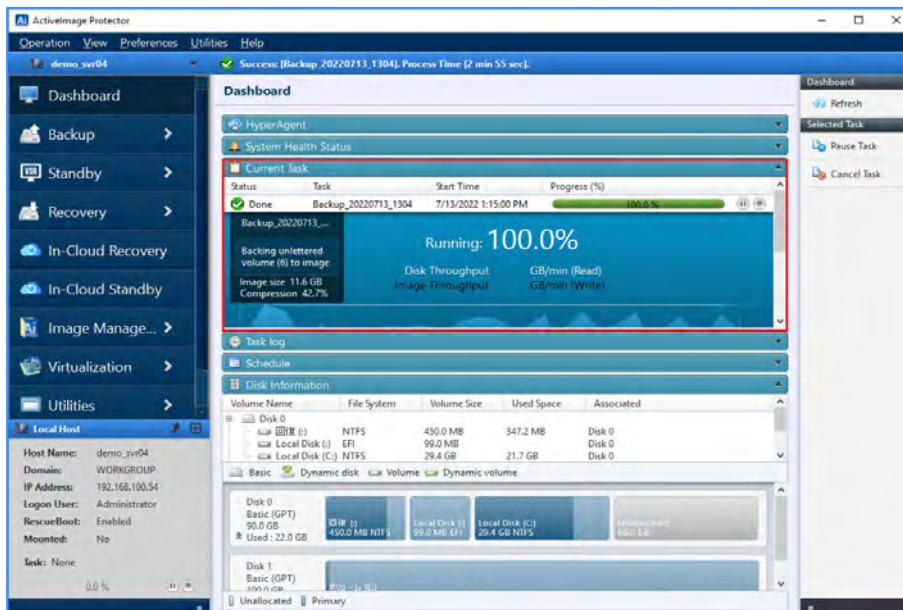


## Configure backup settings and run backup tasks

11. When a backup task starts, you can monitor the progress in the Dashboard window.



12. ActiveImage Protector has finished the backup when the progress bar reaches 100%.

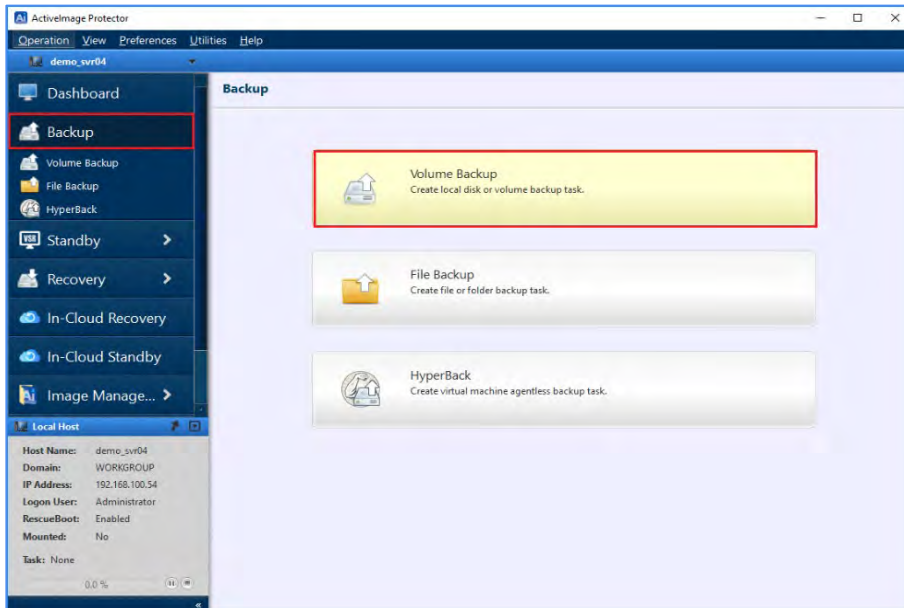




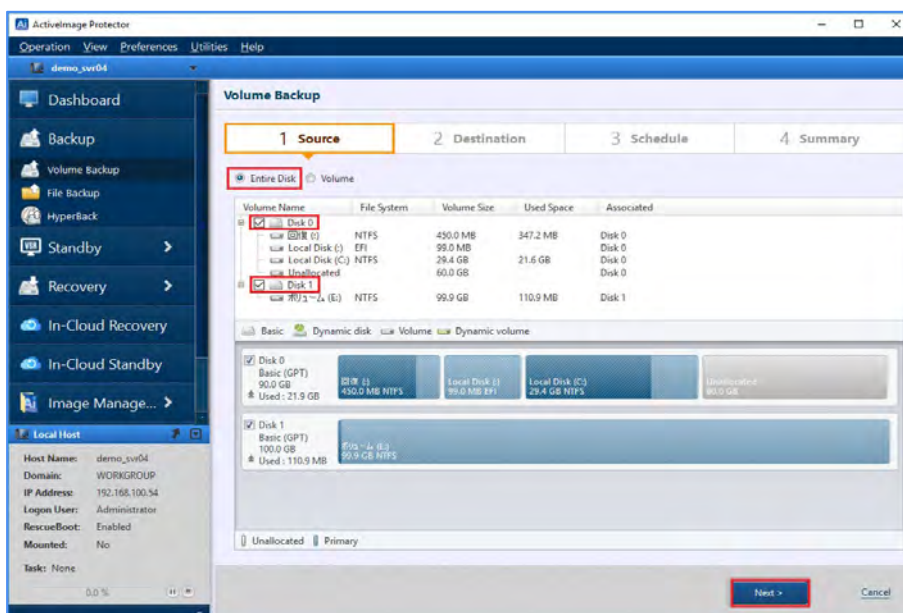
## 4-2. Volume Backup: Scheduled Backups

Please use the following steps to configure regularly scheduled backups (**NOTE:** These steps describe the process of creating the backup schedules depicted in the screenshots. You may want to create different backup settings than depicted here):

1. Start ActiImage Protector by clicking on the Windows Start menu and selecting **[Actiphys] → [ActiveImage Protector]**.
2. Once in ActiveImage Protector, click on **[Backup] → [Volume Backup]**.

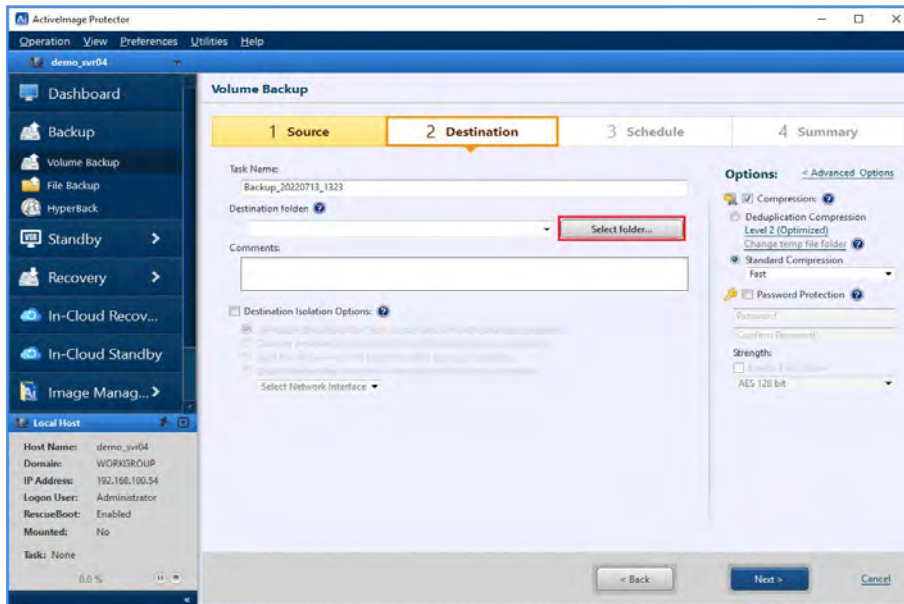


3. Select the backup source from the list of volumes. We will select the entire disk as the backup source in this example. Click **[Entire Disk]** and then click the checkboxes for **[Disk 0]** and **[Disk 1]**. Once you have selected the backup source(s), click the **[Next]** button.

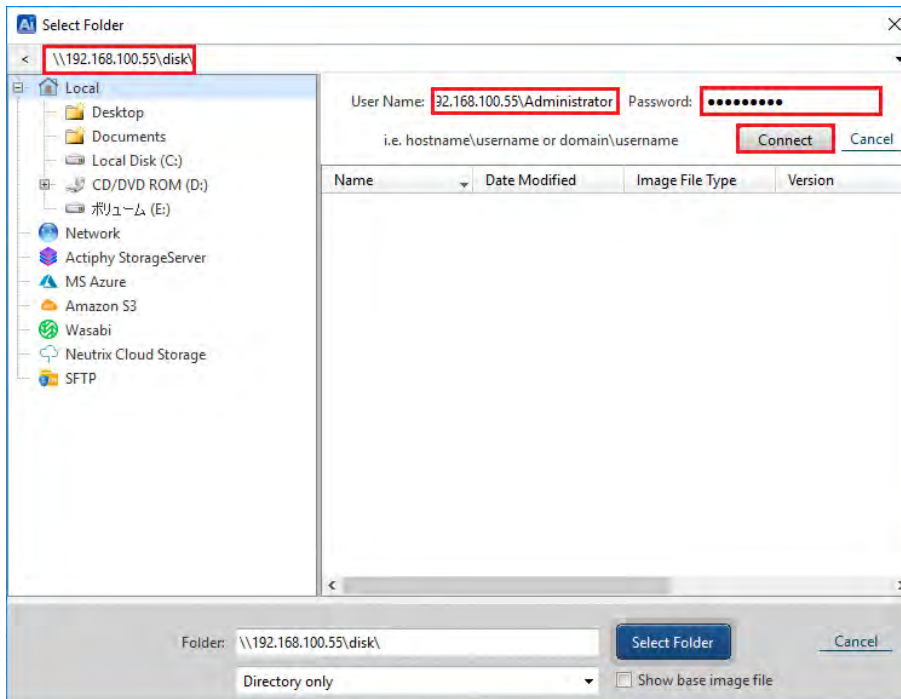


## Configure backup settings and run backup tasks

4. Select a destination folder to save the backup image files to. In this example, we have selected the network shared folder `\\192.168.100.55\disk` as the destination. Click **[Select 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.

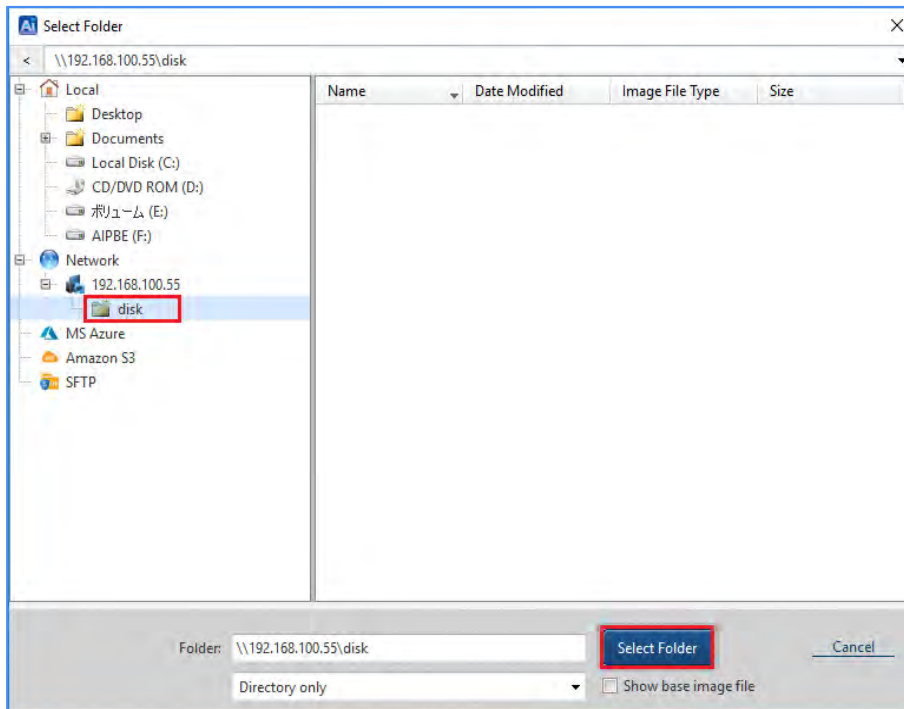


5. Specify a shared folder for the destination storage and press the **[Enter]** key. Also, enter the destination folder's login credentials and click the **[Connect]** button. (In this screenshot, we're using `\\192.168.100.55\disk` as the destination folder and `192.168.100.55\Administrator` as the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

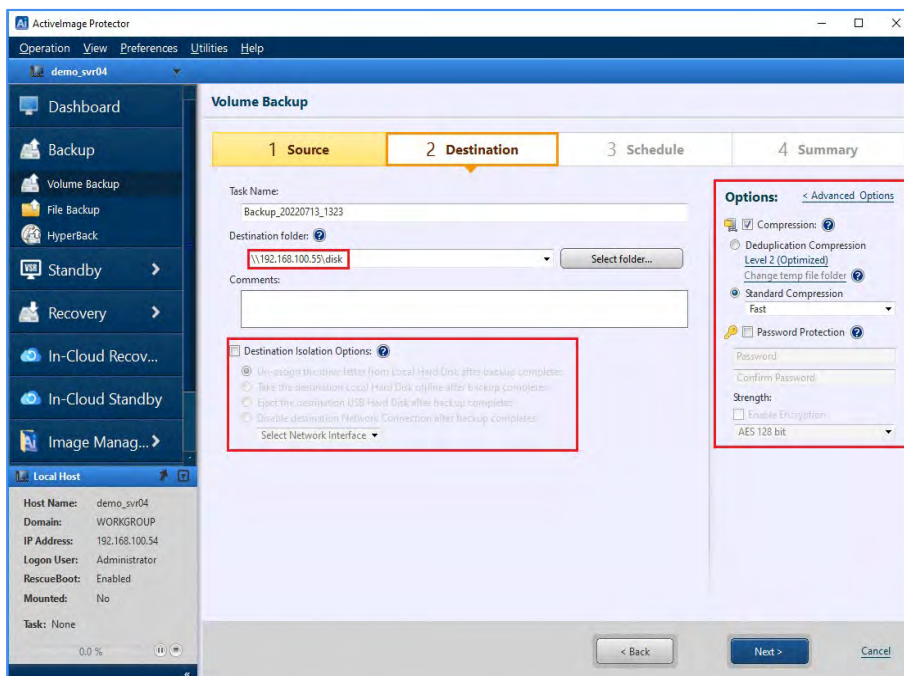


## Configure backup settings and run backup tasks

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



- On the Volume Backup screen, ensure you have filled in the Destination Folder field correctly and click **[Next]**. We will review the **[Destination Isolation Options]** and **[Options]** sections later in this document.



## Configure backup settings and run backup tasks

8. Configure the backup schedule. The steps below shows 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.

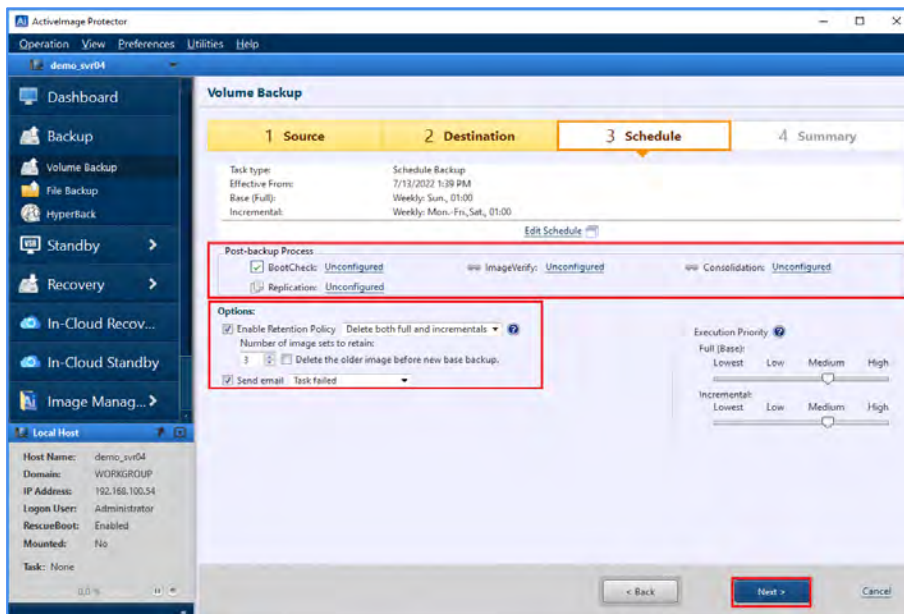
The screenshot shows the 'Schedule Settings' dialog box. At the top, it displays 'Backup\_20220713\_1323' and 'Effective Date/Time: 2022/07/13 13:37 ~ 2023/07/13 13:37' with a 'Not Specified' checkbox. The 'Task Type' is set to 'Schedule Backup'. Below this, there are two main sections: 'Base' and 'Incremental'. The 'Base' section is highlighted with a red box and shows 'Weekly' as the schedule, with 'Sun' selected in the day-of-week buttons and 'Execute Time: 01:00'. The 'Incremental' section is also highlighted with a red box and shows 'Weekly' as the schedule, with 'Mon' through 'Sat' selected in the day-of-week buttons and 'One time only: 01:00' selected under 'Multi-times'. At the bottom, there are links for 'Add New Base' and 'Add New Incremental', an 'Event Backup' section with 'Shutdown/Reboot' and 'Base and Incremental' options, and an 'Option' section with 'Auto run if a scheduled task is missed' and 'Run basebackup if scheduled basebackup task has been missed' checkboxes. 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 'Designate Specific Days' dialog box. It features a 'Month' selector with buttons for days 1 through 12. Below this is a calendar grid with columns for 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. The grid shows 'Week 1' through 'Week 5' and a 'Final Week'. The 'Execute Time' is set to '01:00'. At the bottom, the 'Add New Base' button is highlighted with a red box.

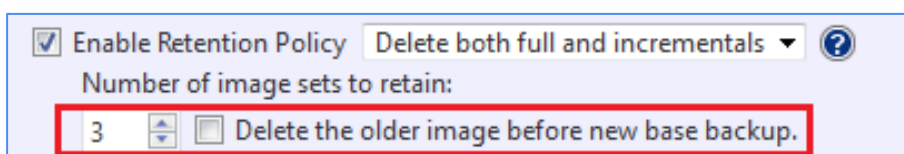
- You can configure your **[Enable Retention Policy]** and **[Send Email]** settings on the **[Schedule]** tab. Then, click the **[Next]** button for the settings to take effect. We will cover details about Post-backup Process in the next chapter.



### (1) 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 ActiveImage Protector backup files consists of one base backup image and any associated incremental backup files.

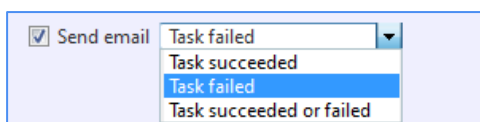


### (2) Send Email

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.

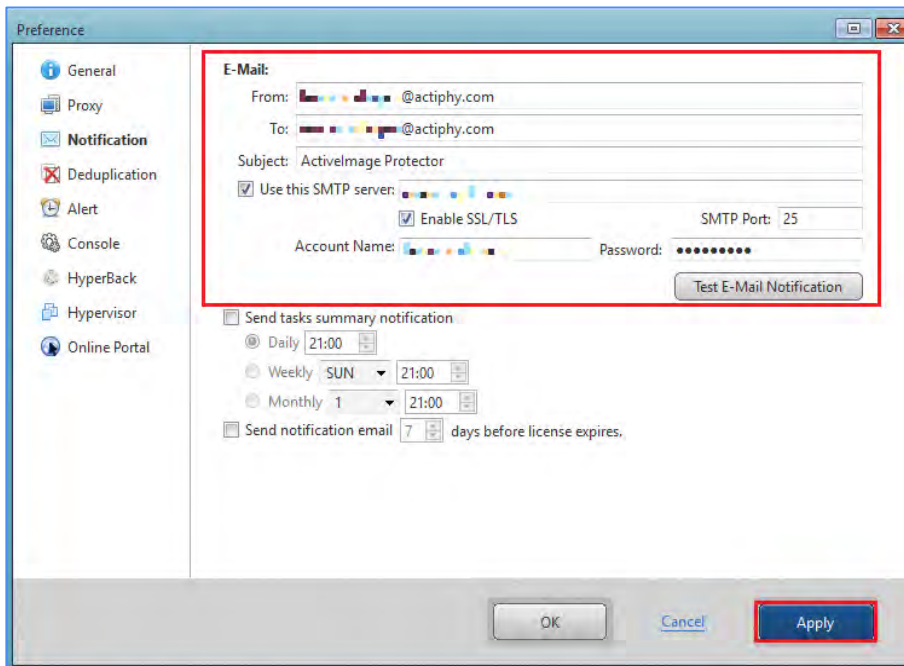




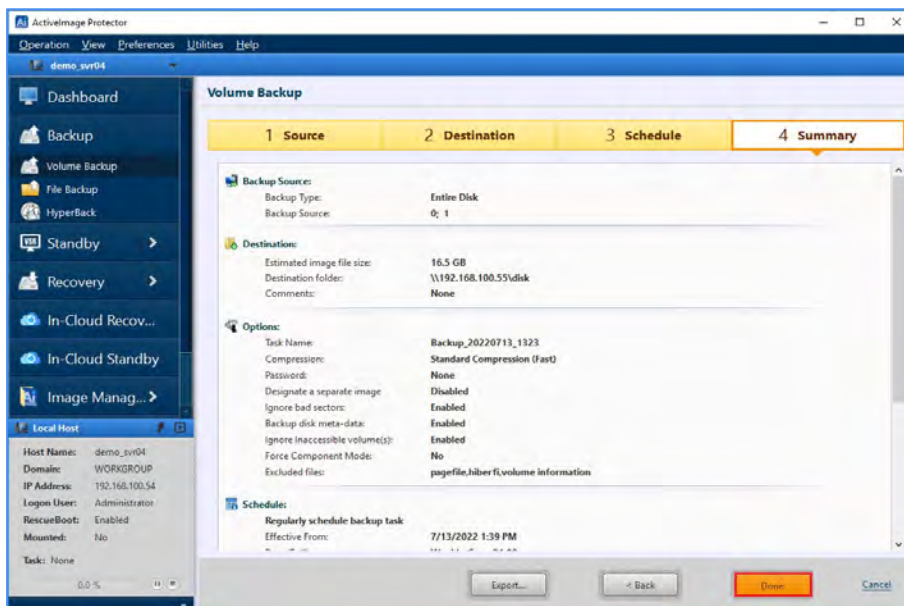
### (3) E-Mail Setting

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.

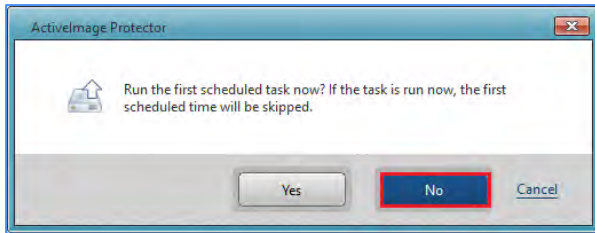


- After setting up your backup schedule, you should see a summary of your configuration. Please review your backup configuration. If everything looks correct, click the **[Done]** button.

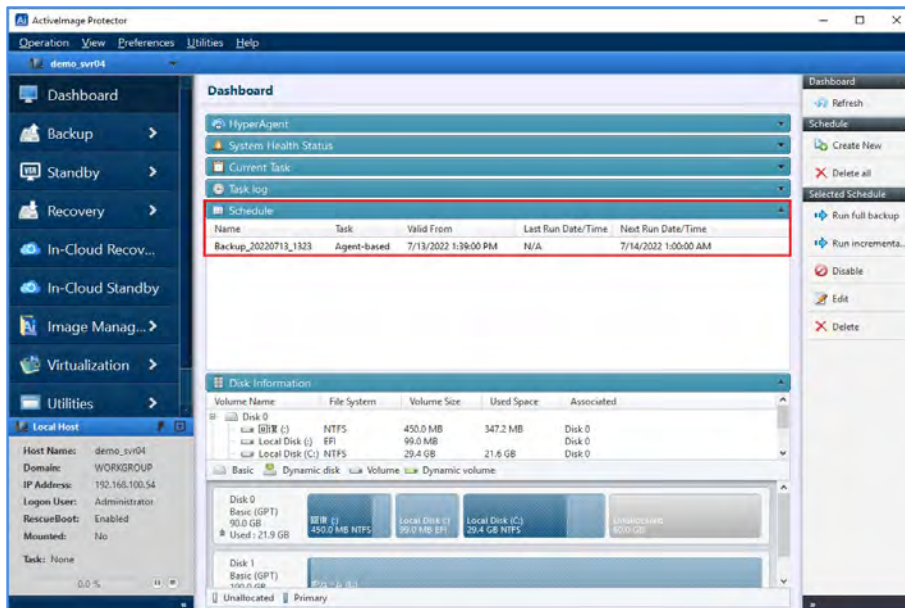


## Configure backup settings and run backup tasks

11. 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.

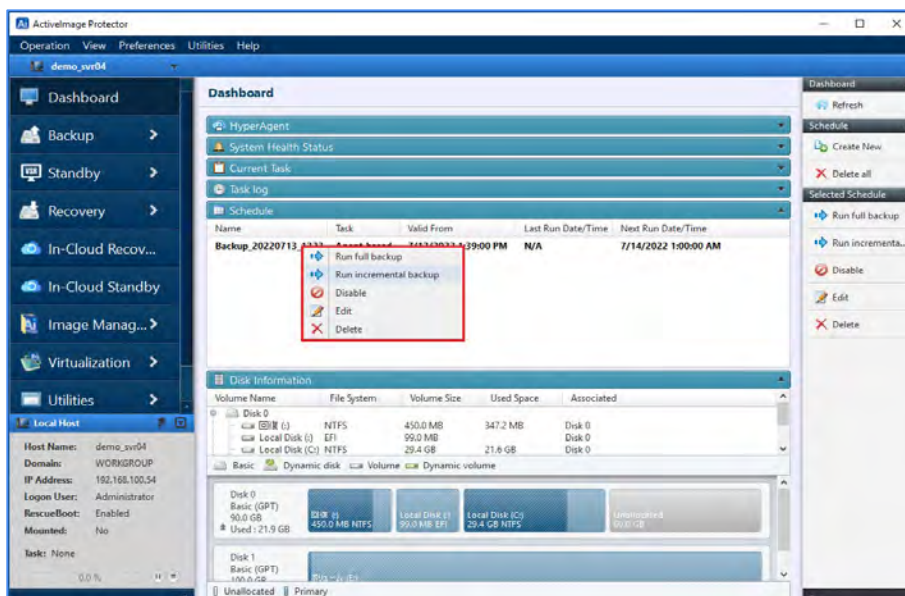


12. Go to **[Dashboard]** → **[Schedule]** to modify or monitor your scheduled tasks.



13. 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.

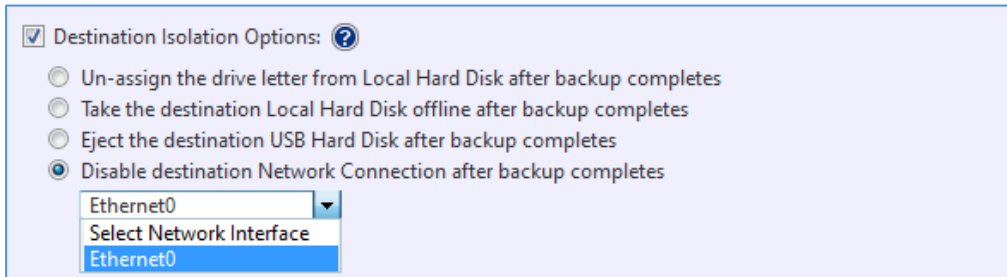


14. When necessary, you can enable the **[Destination Isolation Option]** and configure the **[Option]**, **[Advanced Settings]**, and **[Post-backup Process]** settings. Here are some examples:

(1) **Destination Isolation Options:**

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.

Turning **[Destination Isolation Options]** on gives you access to the following options:



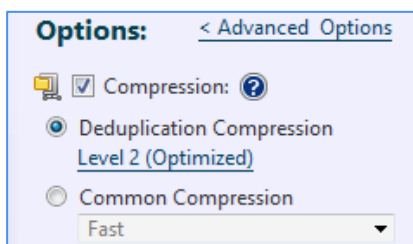
- **Un-assign the drive letter from the local hard disk after completing the backup:** When this option is enabled, ActivelImage Protector will unassign the local hard disk's drive letter once the backup process is complete.
- **Take the destination local hard disk offline after completing the backup:** When you enable this option, ActivelImage Protector will set the destination disk to *offline* once the backup is complete.
- **Eject the destination USB hard disk after completing the backup:** Enabling this option causes ActivelImage Protector to eject the destination drive once the backup is complete if you save your backups to removable media, such as a USB drive.
- **Disable the destination network connection after completing the backup:** This option will disconnect the network connection to your backup destination once the backup is complete if you save backups to a network drive.

(2) **Options:**

• **Compression:**

ActivelImage 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.

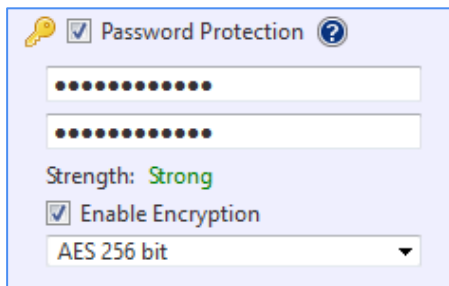


- **Password Protection:** Enabling this option protects the backup image file by assigning a unique password. This additional security prevents anyone from mounting, exploring, or restoring the image file without a password.



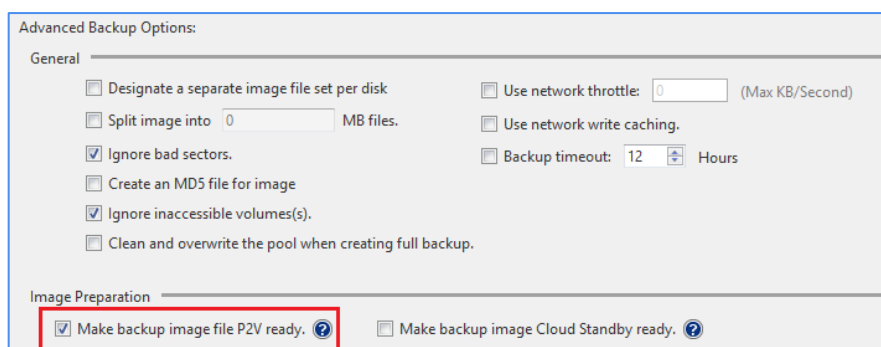
## Configure backup settings and run backup tasks

- **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.



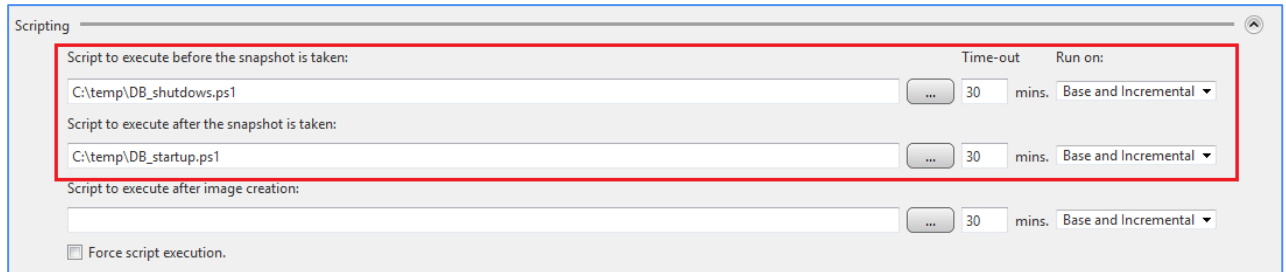
(3) **Advanced Backup Options:** The Advanced Backup Options section contains the following settings:

- **[Designate a separate image file set per disk]:** This option tells Activelmage Protector to create a separate backup file for each disk in your backup plan.
- **[Split image into xx MB files]:** This option lets you split your backup images into multiple smaller files.
- **[Ignore bad sectors]:** This option will cause the backup to skip over bad sectors on the source disk.
- **[Create an MD5 file for the image]:** This option tells Activelmage Protector to create an MD5 hash for each backup image. Activelmage Protector will store MD5 hashes in a separate file in the same directory where it saves your backup images.
- **[Ignore inaccessible volumes]:** Activelmage Protector will skip any inaccessible volumes during the backup process if you enable this option. If this option is disabled, Activelmage Protector will produce an error if it can't access a volume and halt the backup process.
- **[Use network throttle xx (Max KB/Second)]:** This option lets you throttle the amount of network bandwidth Activelmage Protector can use during the backup process.
- **[Use network write caching]:** This option can make the backup process more stable when copying files across a network; however, it can also cause Activelmage Protector to process large files more slowly.
- **[Make backup image file P2V ready]:** This option tells Activelmage Protector to prepare an image file for virtualization later. Please note that this option does not virtualize the file. It only prepares the image so you can virtualize it at a later time.
- **[Make backup images Cloud Standby ready]:** This option prepares virtual copies of your backup images that you can use to launch virtual machines in either AWS or Azure.



## Configure backup settings and run backup tasks

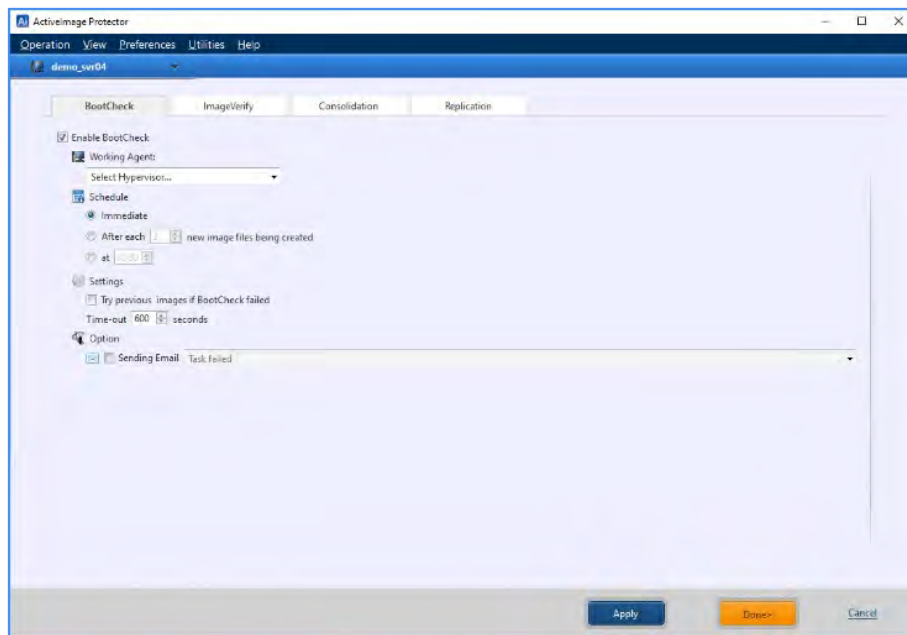
- **[Scripting]:** You can write scripts to run before and after ActiveImage Protector creates snapshots or backups. For example, when backing up non-VSS-savvy databases, you need to stop the service before starting the backup task to maintain the integrity of the data. You can specify a script or batch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



### (4) 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]**.

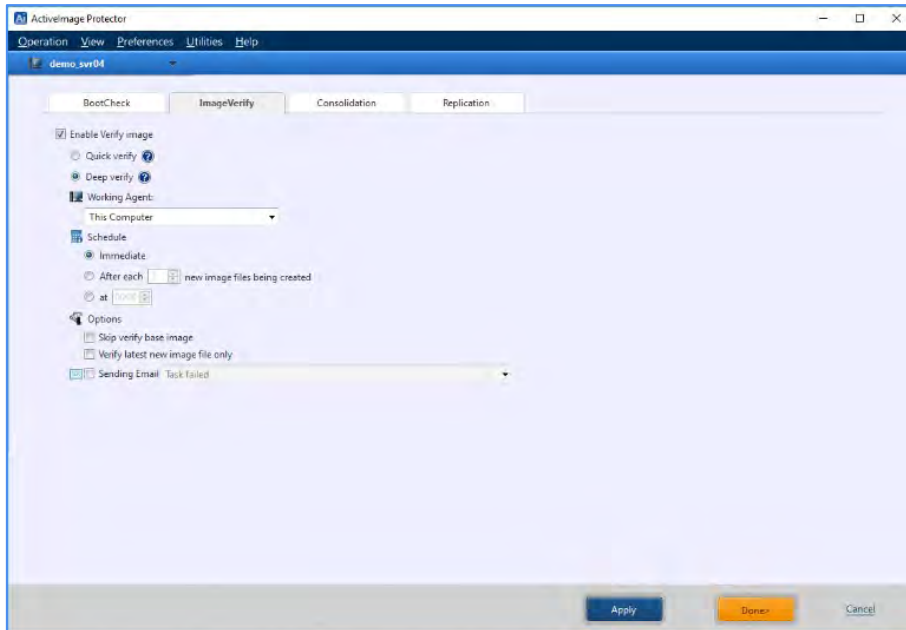
- **BootCheck:**  
BootCheck quickly tests if a created backup of the system volumes can successfully boot on the selected hypervisor. Click in the box to enable the **[Enable BootCheck]** option. Configure the Schedule settings, Sending Email options, etc.



## Configure backup settings and run backup tasks

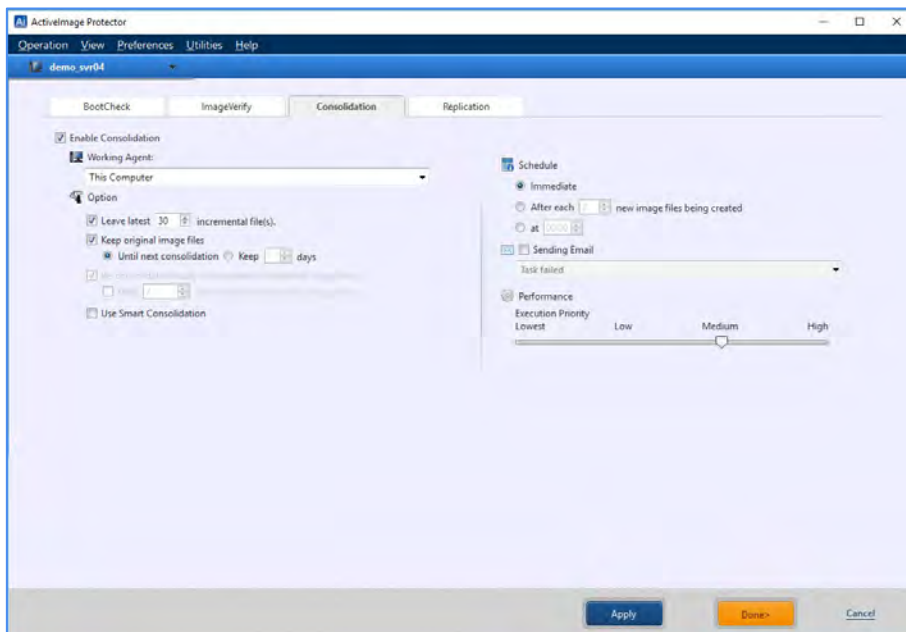
- **Image Verify:**

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



- **Consolidation :**

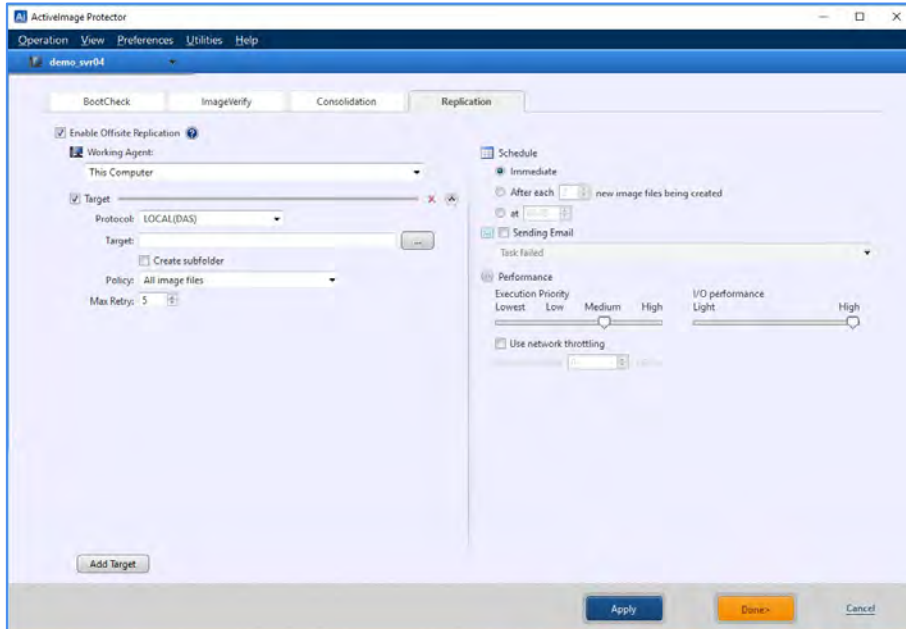
Consolidation can be scheduled to consolidate the incremental backups into a single backup image set reducing storage demands. Click in the box to enable the **[Enable Consolidation]** option. Configure the settings for **[Schedule]**, **[Sending Email]**, **[Performance]**, etc.



## Configure backup settings and run backup tasks

- **Offsite Replication**

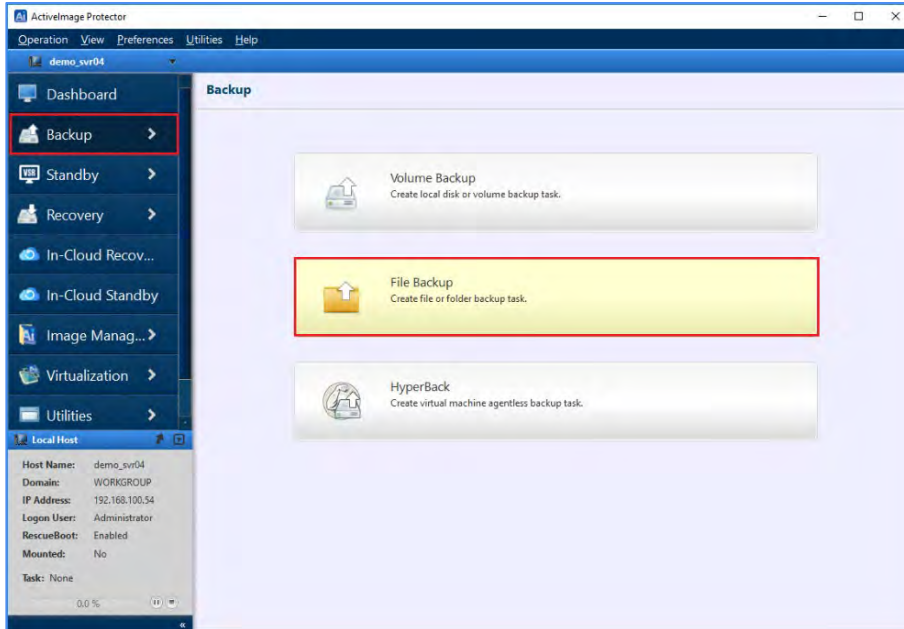
The Replication feature enables you to replicate backup image files to an offsite storage share including cloud storage. ActiveImage Protector Replication feature supports local storage, shared folder, WebDAV, FTP, Amazon S3, Azure Storage, OneDrive, Google Drive, and Dropbox, Wasabi, Neutrix Cloud.



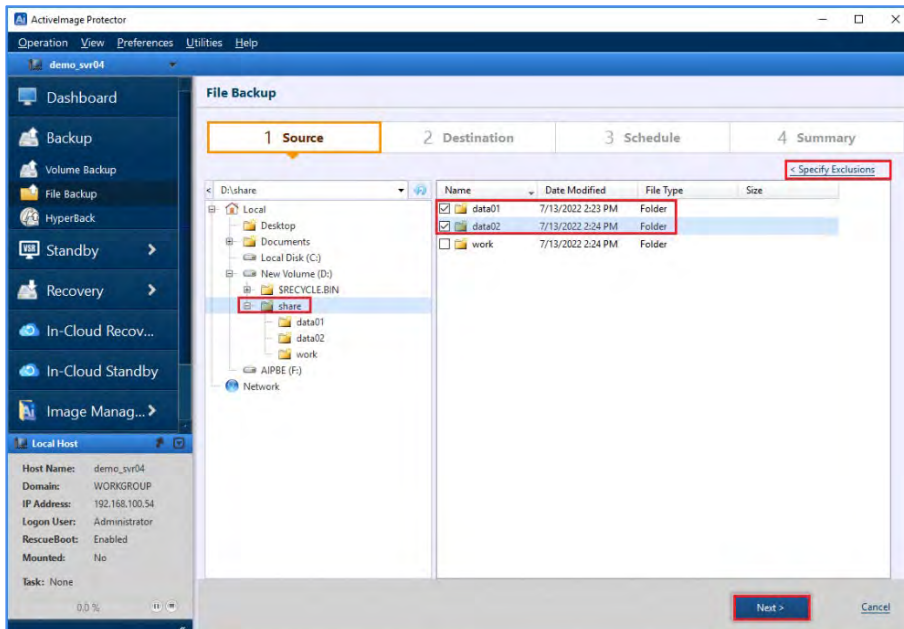
### 4-3. File Backup : Schedule File Backup

Configure the file / folder backup schedule settings.

1. Start ActiImage Protector. Go to Windows Start menu - **[Actiphy]** → **[ActiImage Protector]**.
2. Click **[Backup]** → **[File Backup]**.



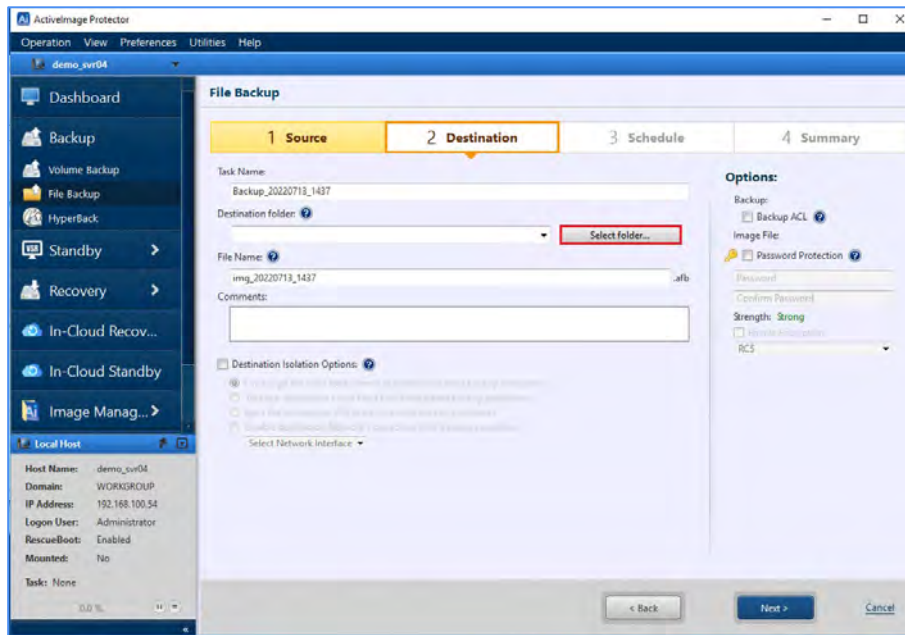
3. Select backup source.  
The following example shows that folders "data01" and "data02" in the "share" folder of "D:" drive are selected for backup. To exclude files from the selected folder you can click on [**< Specify Exclusions**]. You can specify a path to the file (ex: C:\test\EULA.txt), the file extension (ex: EULA.txt), or a wild card "\*" (Ex: \*.txt, EULA.\*). After configuring the settings, click **[Next]**.



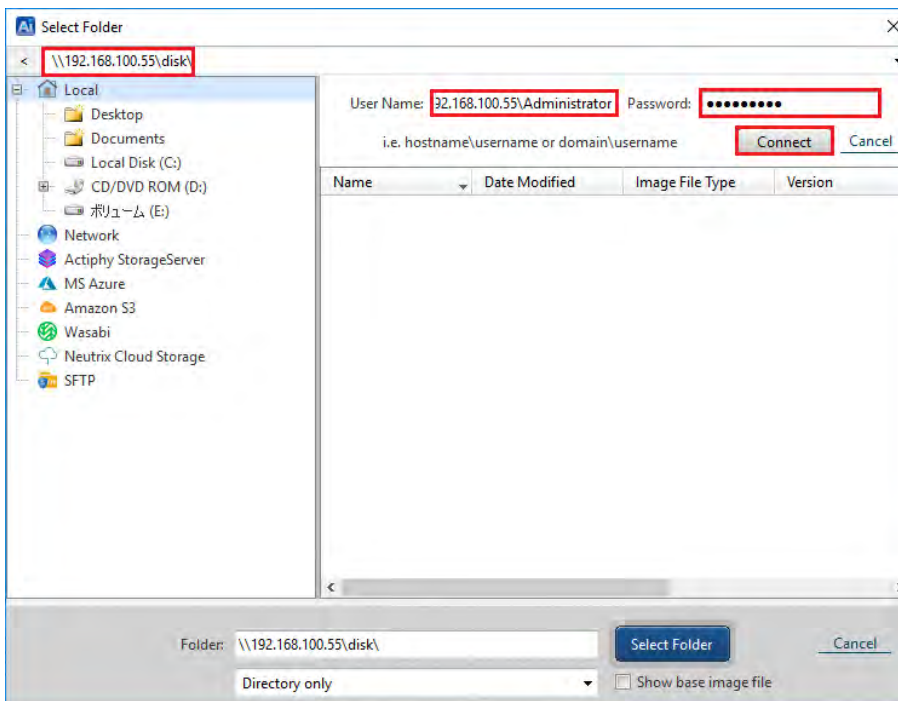
## Configure backup settings and run backup tasks

### 4. Select a destination folder for the backup image.

The following example shows that a network shared folder, “\\192.168.100.55\disk1”, is specified as the destination folder. Click **[Select Folder]** 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.



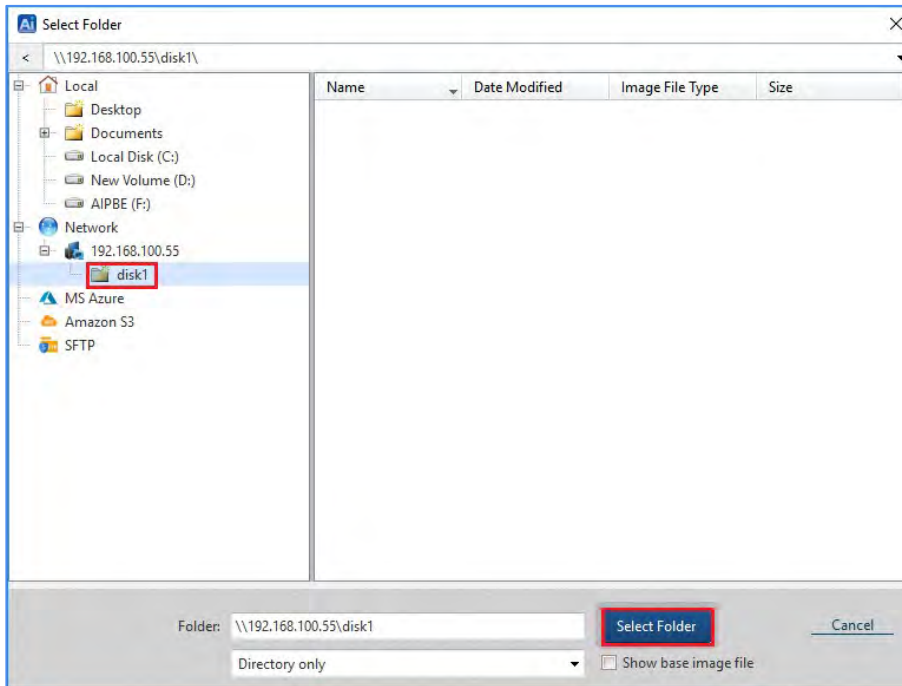
### 5. Specify a shared folder as the destination storage. Enter a network location “\\192.168.100.55\disk1” as the destination folder and press the **[Enter]** key. At the top of screen enter the credentials to log into the target destination. The following example shows “192.168.100.55\Administrator” is entered as **[User Name]** and the password for **[Password]**. Click **[Connect]**.



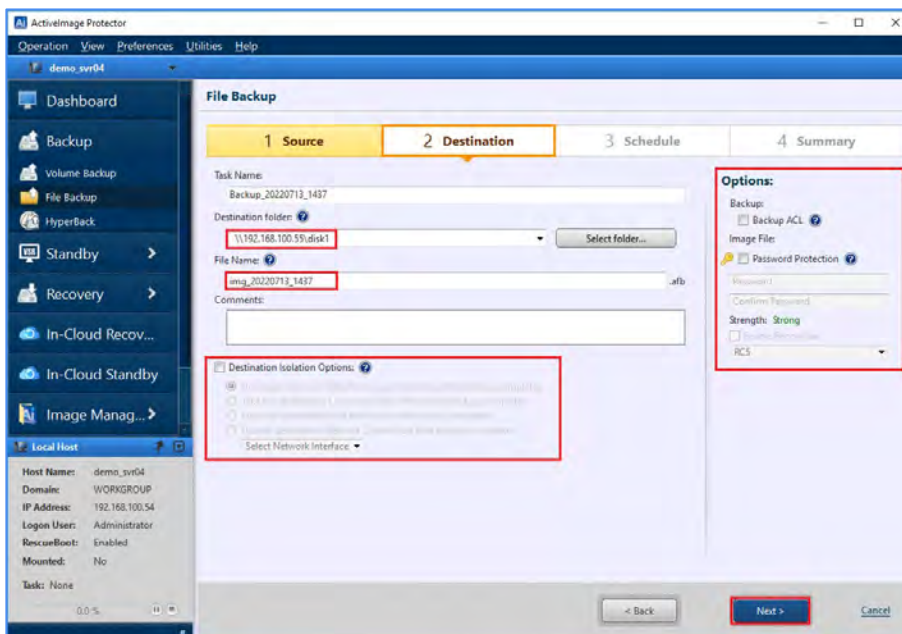


## Configure backup settings and run backup tasks

- Specify a shared folder as the destination storage. The network location is now accessible in the folder tree to the left. Select the destination and click **[Select Folder]**.

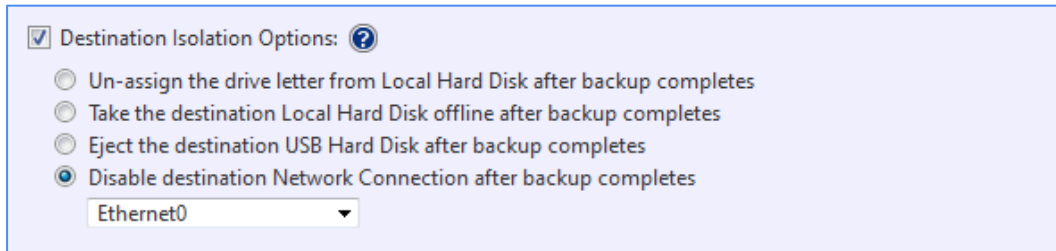


- You can specify a name. If necessary, select any options for the **[Destination Isolation Option]** and **[Options]**.



## (1) Destination Isolation Options

Enabling Destination Isolation Option disconnects network access to backup image storage drives after backups complete rendering the specified destination storage inaccessible. The Destination Isolation feature protects the backup storage and backups from potential malware or ransomware attacks. Destination Isolation Options provide the following four options.



☒ Destination Isolation Options: ?

☐ Un-assign the drive letter from Local Hard Disk after backup completes

☐ Take the destination Local Hard Disk offline after backup completes

☐ Eject the destination USB Hard Disk after backup completes

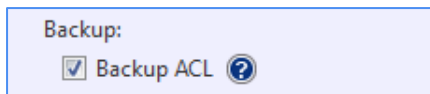
☒ Disable destination Network Connection after backup completes

Ethernet0

- **Un-assign drive letters from Local Hard Disks post backup :**  
The drive letter assigned to the local hard disk is de-assigned upon completion of the backup process.
- **Take destination Local Hard disks offline post backup :**  
Sets destination disks to go offline once the backup process has finished.
- **Eject destination Removable USB Hard disk post backup :**  
After the backup process has finished, the system will eject removable hard disks, such as USB hard disks.
- **Disable destination Network Connections post backup :**  
The system will disconnect network connections to backup destinations once the backup process has finished.

## (2) Option:

- **Backup ACL :**  
Enabling **[Backup ACL]** backs up the Access Control List for the backup source files. The system will restore Access Control Lists when restoring files.



Backup:

☒ Backup ACL ?

- **Password Protection :**  
This option allows you to secure a backup image file by assigning it a password. This option will require users to enter a password before mounting, exploring, or restoring any of the image file's contents.
- **Enable Encryption:**  
You can choose from three levels of encryption to secure your backup images:
  - RCS.
  - AES128 bit.
  - AES256 bit.

By using encryption, you can protect backup image files that you save in remote locations from cyber attacks.



## Configure backup settings and run backup tasks




Image File:

☒ Password Protection

.....

.....

Strength:

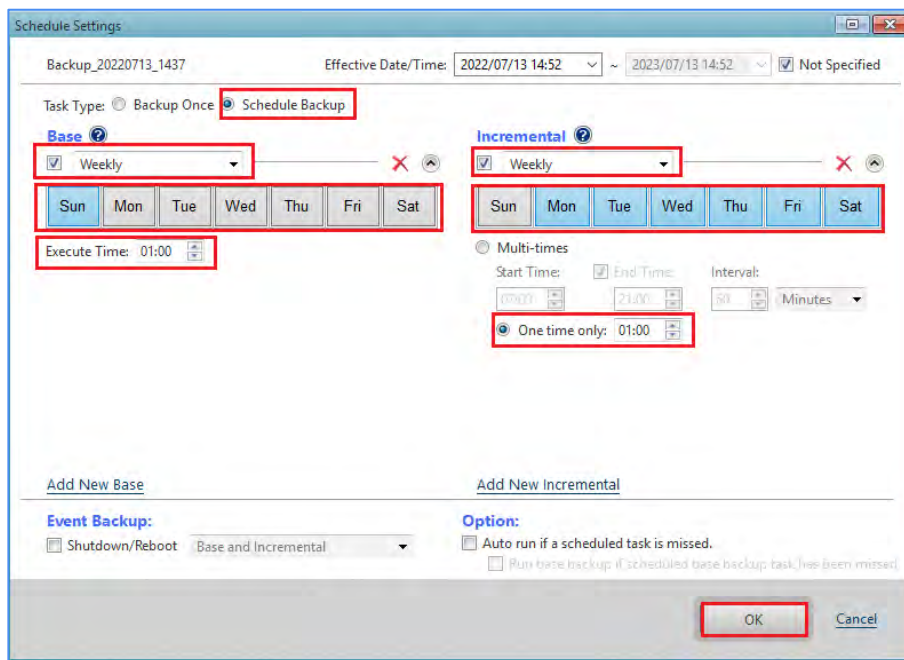
☒ Enable Encryption

AES 256 bit

8. You can configure the times and frequency of your backups on the **[Schedule Settings]** screen. In this example:

- We are configuring our base backup to run every Sunday at 1:00 a.m. in this window's **[Base]** section.
- We are configuring our incremental backups to run weekly, Monday through Saturday, at 1:00 a.m. in this window's **[Incremental]** section.
- You may also run your incremental backups multiple times daily, if you'd like, by selecting a **[Start Time]**, **[End Time]**, and the **[Interval]** to run the incremental backup tasks between those two times.

After configuring your schedule, click the **[OK]** button.



Schedule Settings

Backup\_20220713\_1437 Effective Date/Time: 2022/07/13 14:52 ~ 2023/07/13 14:52 ☒ Not Specified

Task Type: ☐ Backup Once ☒ Schedule Backup

**Base**

☒ Weekly

Sun Mon Tue Wed Thu Fri Sat

Execute Time: 01:00

**Incremental**

☒ Weekly

Sun Mon Tue Wed Thu Fri Sat

☐ Multi-times

Start Time: 01:00 End Time: 21:00 Interval: 60 Minutes

☒ One time only: 01:00

Add New Base Add New Incremental

**Event Backup:**

☐ Shutdown/Reboot Base and Incremental

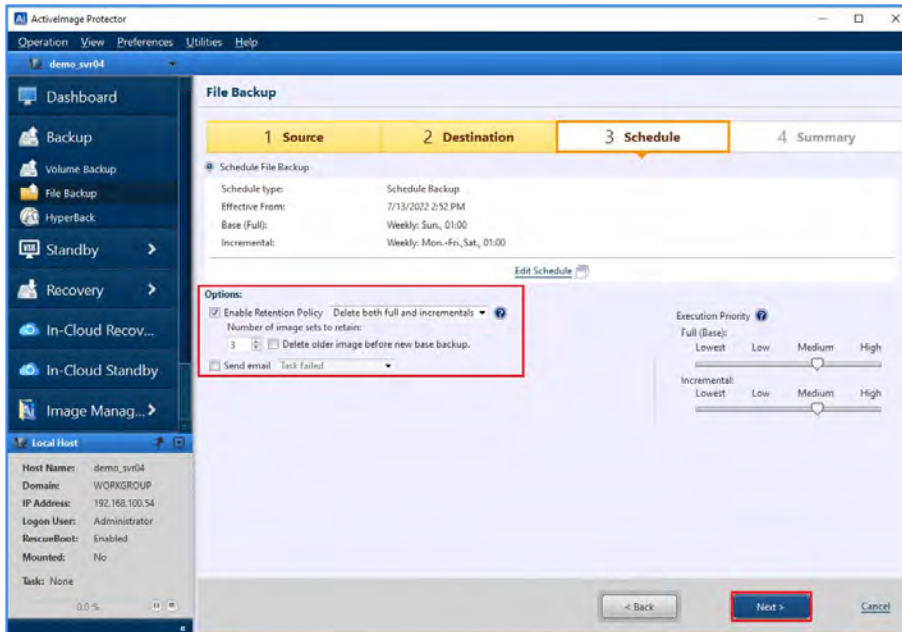
**Option:**

☐ Auto run if a scheduled task is missed.

☐ Run base backup if scheduled base backup task has been missed.

OK Cancel

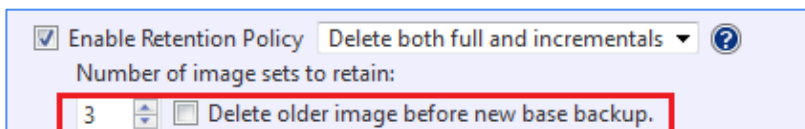
9. You can use the **[Enable Retention Policy]** and **[Send email]** settings to customize your retention policy and email notifications from the **[Schedule]** tab. Once you have configured these options to your liking (see below for more details), click the **[Next]** button to continue.



### (1) Enable Retention Policy

The **[Enable Retention Policy]** option specifies how many sets of backup files ActiveImage Protector will retain before deletion. Click on the **[Enabling Retention Policy]** checkbox to enable the retention policy. By default, ActiveImage Protector will save the three most recent backup sets before it starts deleting them. You can change this default by increasing or decreasing the number of image sets to retain using the **[Number of image sets to retain]** setting.

**Note:** One generation of ActiveImage Protector backup image files represents one base backup image file and all associated incremental backup files.

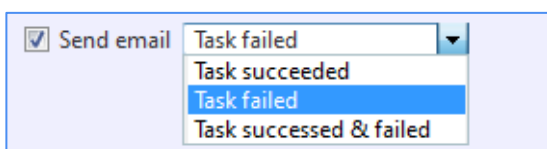


### (2) Send email

You can enable the **[Send email]** option if you want the system to notify you of a scheduled task's completion status by email. You can select from one of three options:

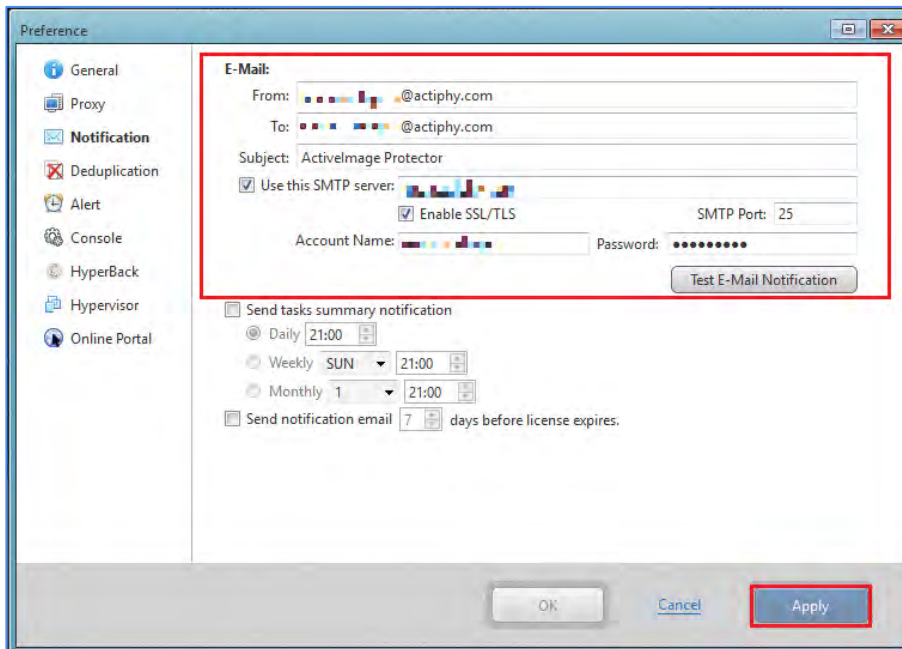
- **[Task succeeded]**
- **[Task failed]**
- **[Task succeeded or failed].**

If you select **[Task succeeded]**, the system will only notify you if a backup task succeeds. If you select **[Task failed]**, the system will only notify you if a backup task fails. If you select **[Task succeeded or failed]**, the system will send you a notification whenever it completes backup tasks, regardless of their status. Before enabling the **[Send email]** option, you will need to go to **[Preferences]** → **[Notifications]** and configure your email settings.

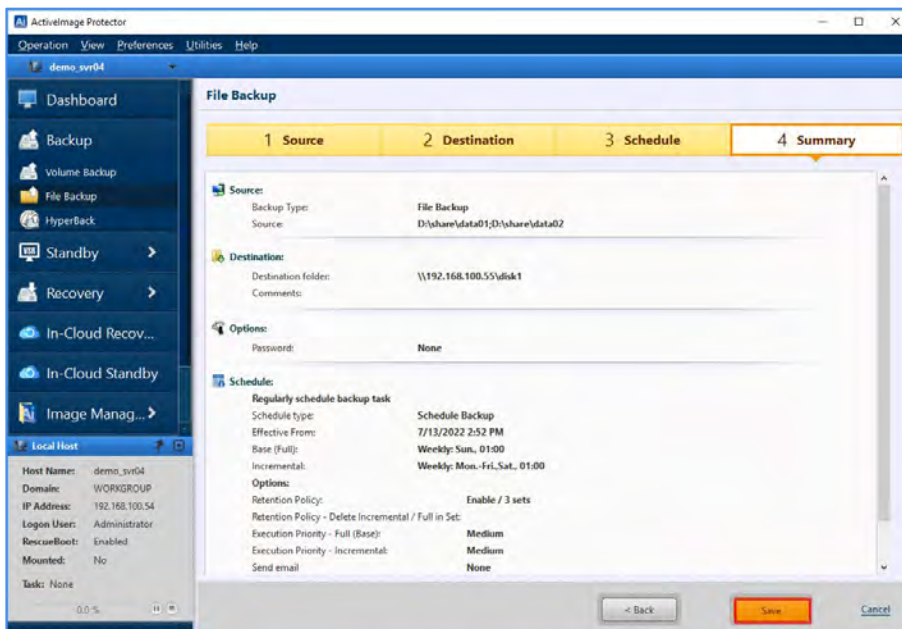


### (3) Email Settings

Go to **[Preferences]** → **[Notifications]** and configure the email settings. After configuring the email settings, click the **[Test E-Mail Notification]** button to ensure that the settings configured for email notifications are accurate. Please use this option to check if the email is received by the specified recipient and click the **[Apply]** button.

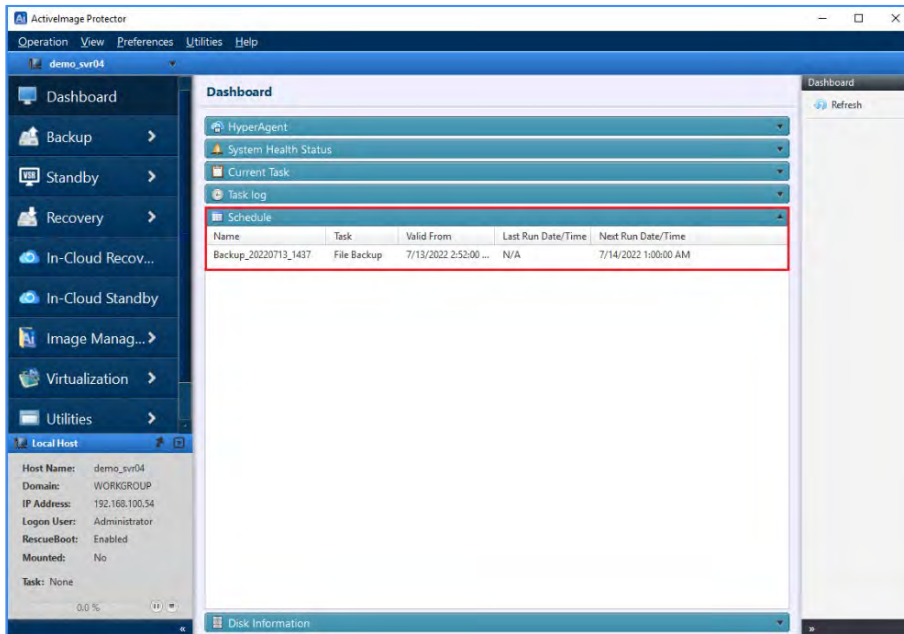


10. A summary of the configured schedule settings are displayed.  
Review the backup configuration and options. Click **[Save]**. The **[Dashboard]** window is displayed.

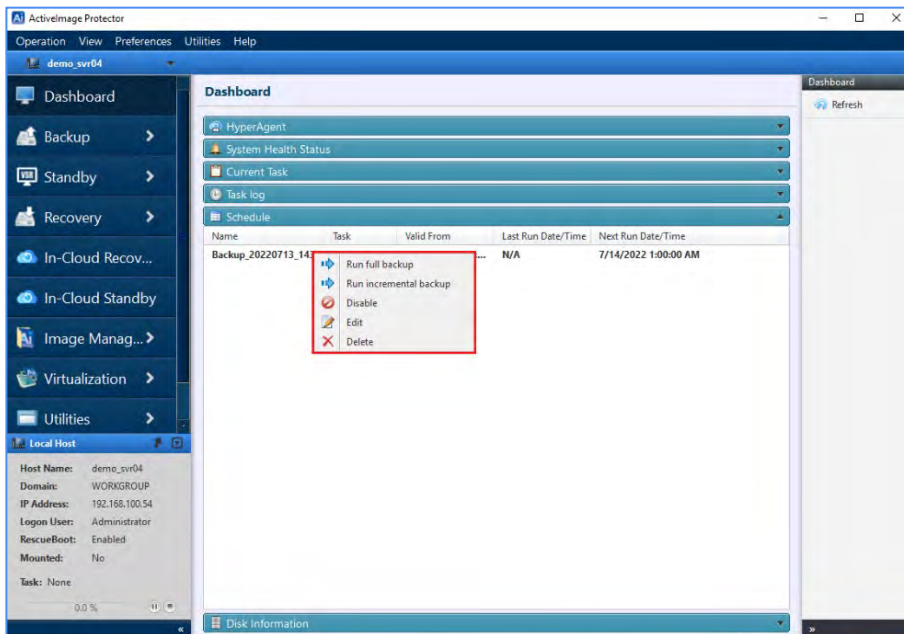


## Configure backup settings and run backup tasks

11. You can monitor the created schedules from the **[Dashboard]** → **[Schedule]**. The scheduled backup task will run according to the schedule you specified.



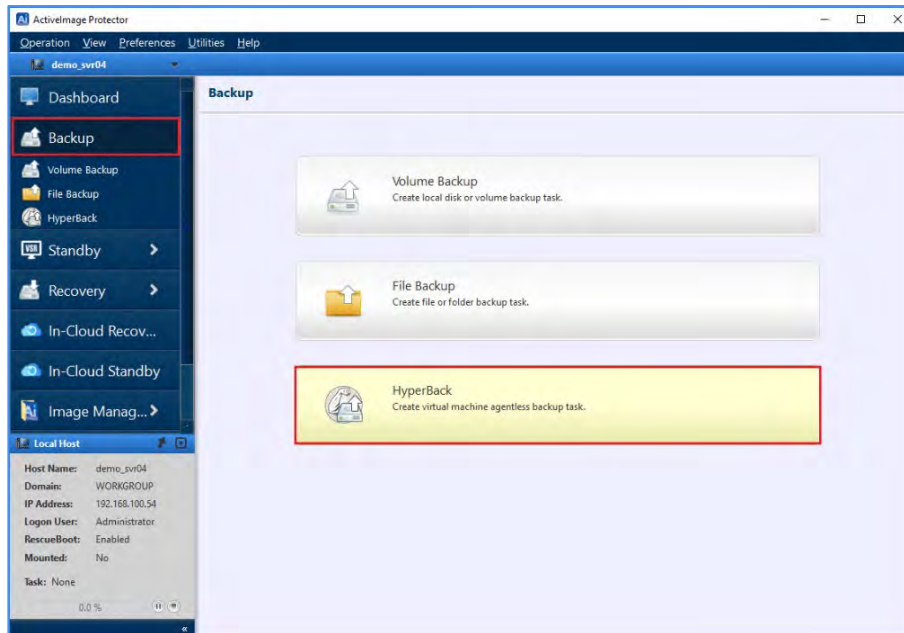
12. Right-click on **[Schedule Name]** to run an immediate full or incremental backup task or edit the schedule settings.



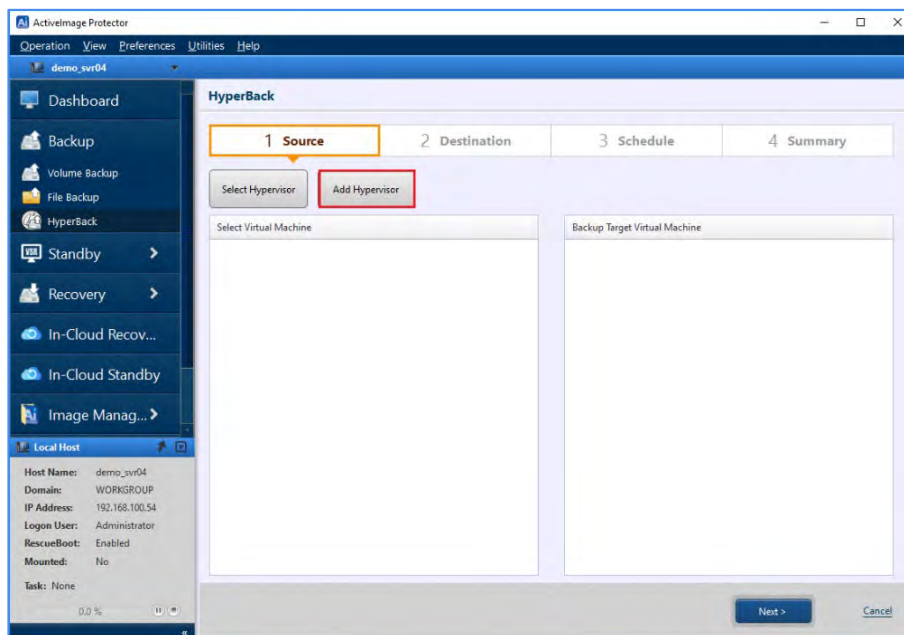
#### 4-4. Agentless Backup (HyperBack)

HyperBack enables you to back up virtual machines on specific hypervisors (Microsoft Hyper-V or VMware vSphere ESXi) without installing an agent on your source hypervisor or virtual machine, which minimizes CPU and memory usage on hypervisor machines. To use HyperBack:

1. Start ActiImage Protector by clicking on the Windows Start menu and selecting **[Actiphy]** → **[ActiImage Protector]**.
2. Once ActiImage Protector is running, click on **[Backup]** → **[HyperBack]**.

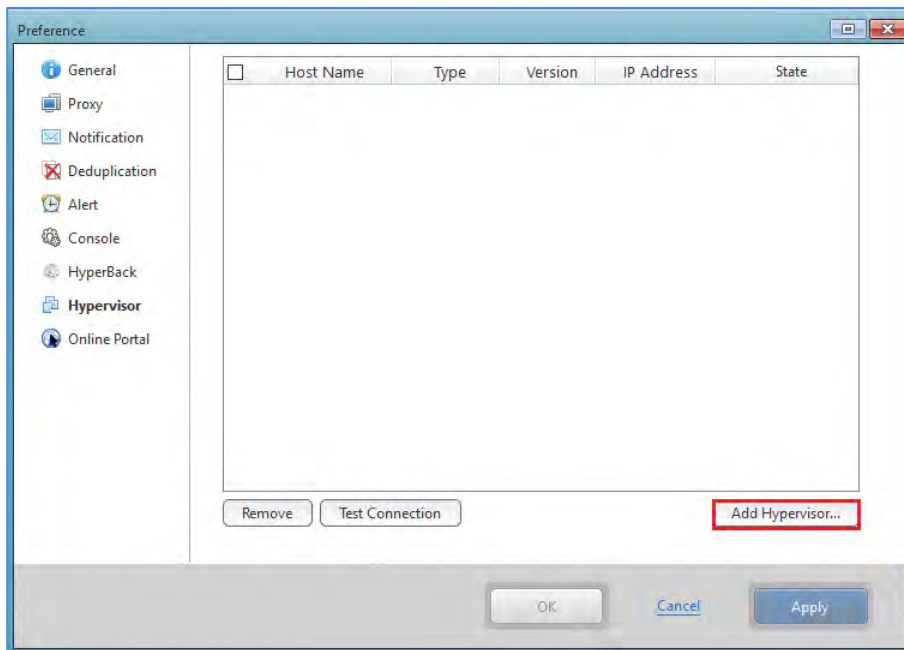


3. Click **[Add Hypervisor]** to configure the virtual machine you want to backup.

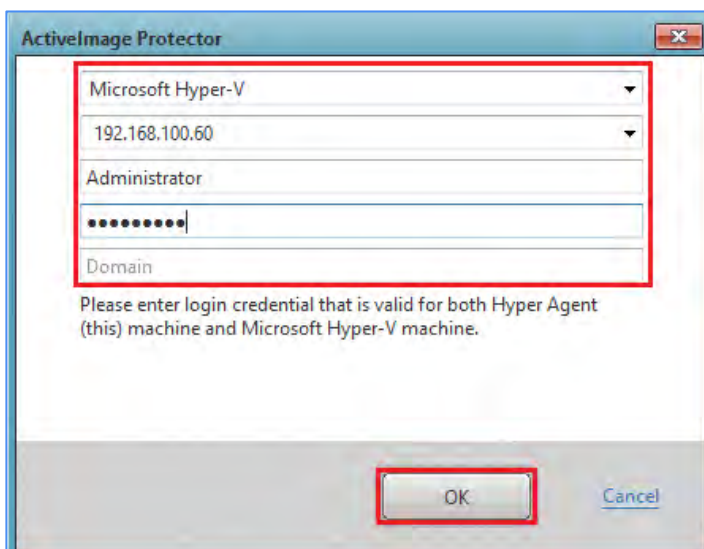




4. Click the **[Add Hypervisor]** button.



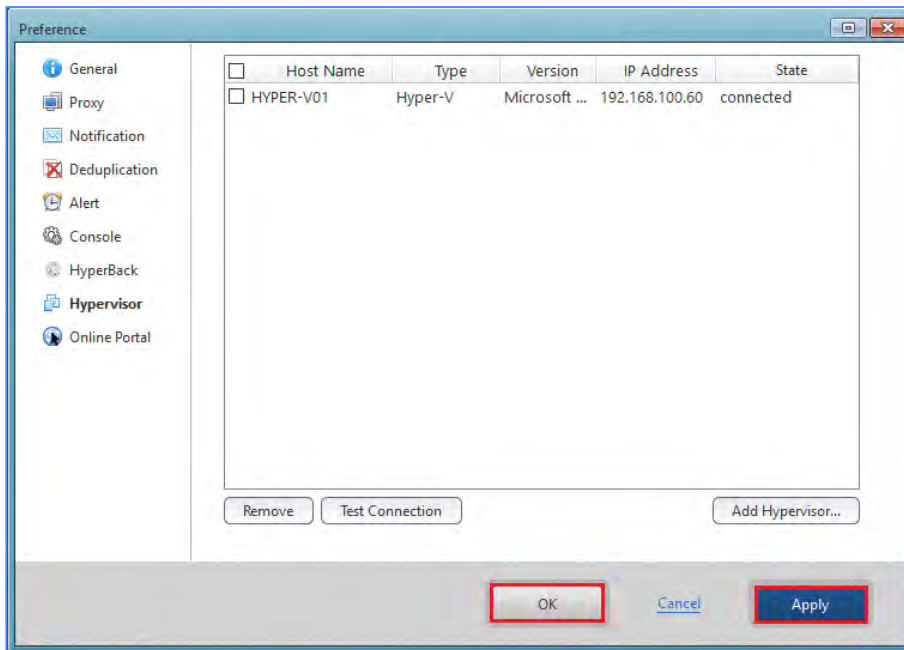
5. Select the hypervisor type and enter your credentials. We have selected "**Microsoft Hyper-V**" as the hypervisor type in this example.
- Enter the IP address or hostname of your Hyper-V host. We have entered "192.168.100.60" in this example.
  - Enter the username for the hypervisor. For example, "Administrator."
  - Enter the password for your hypervisor.
  - You can optionally enter the domain. We are not including domain information in this example.
  - When you have finished configuring your hypervisor, click the **[OK]** button.



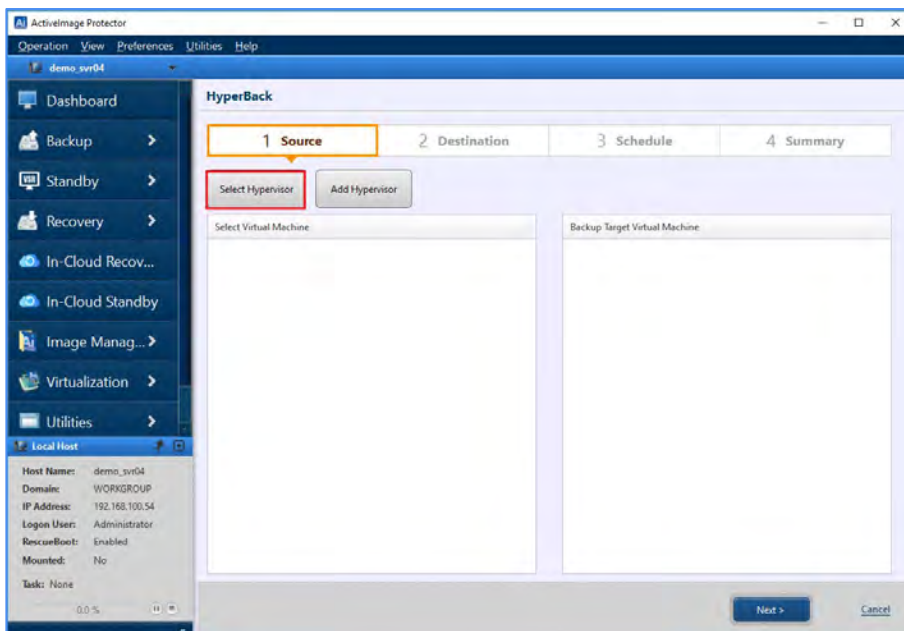


## Configure backup settings and run backup tasks

- Review the information for your hypervisor and click the **[Apply]** button. Click the **[OK]** button to complete the configuration and return to the **[HyperBack]** settings screen.

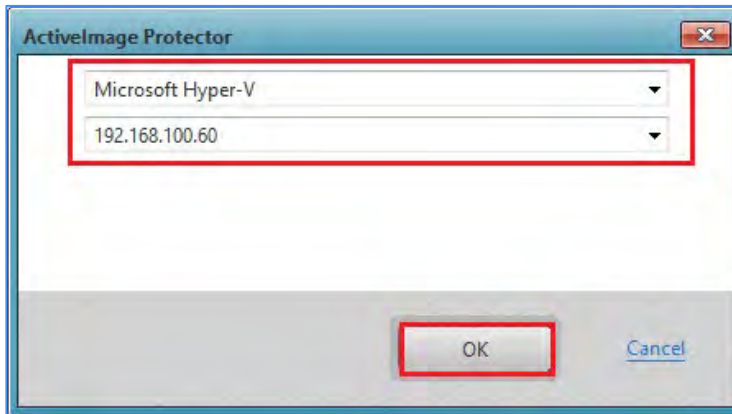


- Now that you have configured the source hypervisor that you want to backup, you need to configure the destination by following these steps:
  - Click **[Source]**.
  - Click **[Select Hypervisor]**.

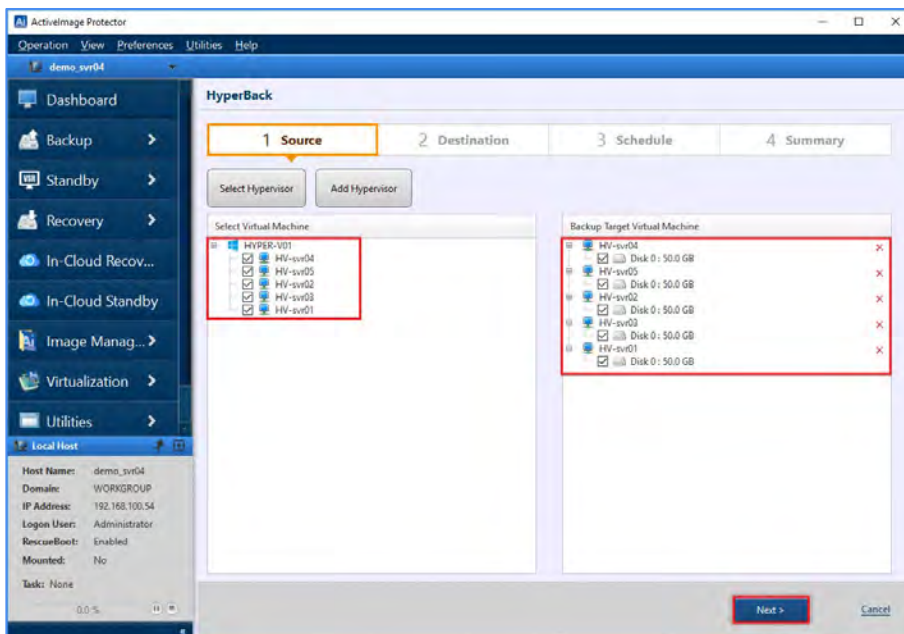


## Configure backup settings and run backup tasks

8. Select the source hypervisor you just configured. Click the **[OK]** button.



9. Enable the checkbox next to the virtual machine(s) where you want to save your backup in the **[Backup Target Virtual Machine]** list. Click the **[Next]** button. By default, you may execute five backup tasks in parallel when backing up multiple virtual machines.



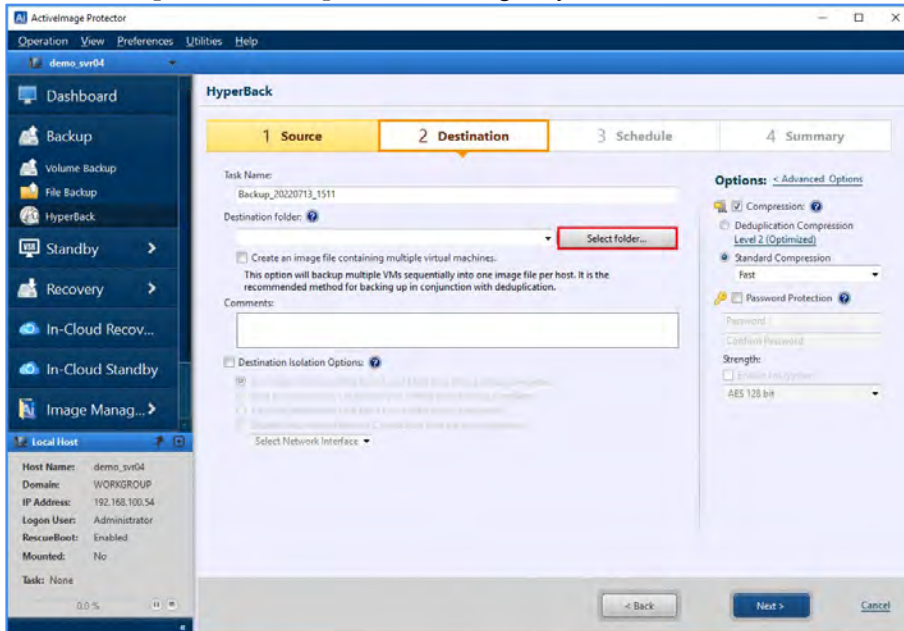
## Configure backup settings and run backup tasks

10. Now, you should be on the **[2 Destination]** screen. From here, you can:

- Set a name for your backup task.
- Select a destination folder to store your backup image.
- Create an image file that contains multiple virtual machines.
- Add a comment to your backup task.
- Configure the isolation options for your backup.

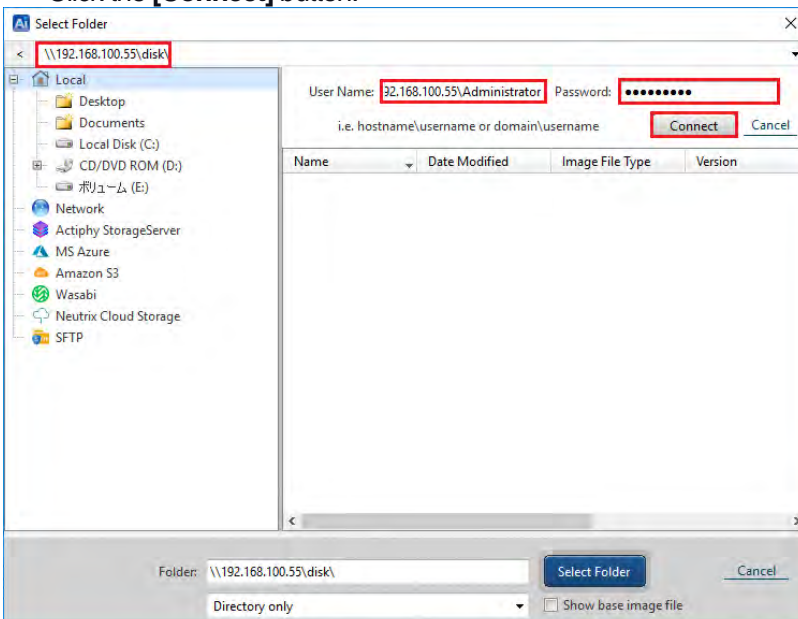
Let's configure a destination for your backup task by following these steps:

- Enter the name of your backup task in the **[Task Name]** field. We've named our task "Backup\_20220713\_1511" in this example.
- Click the **[Select Folder]** button to configure your destination folder.

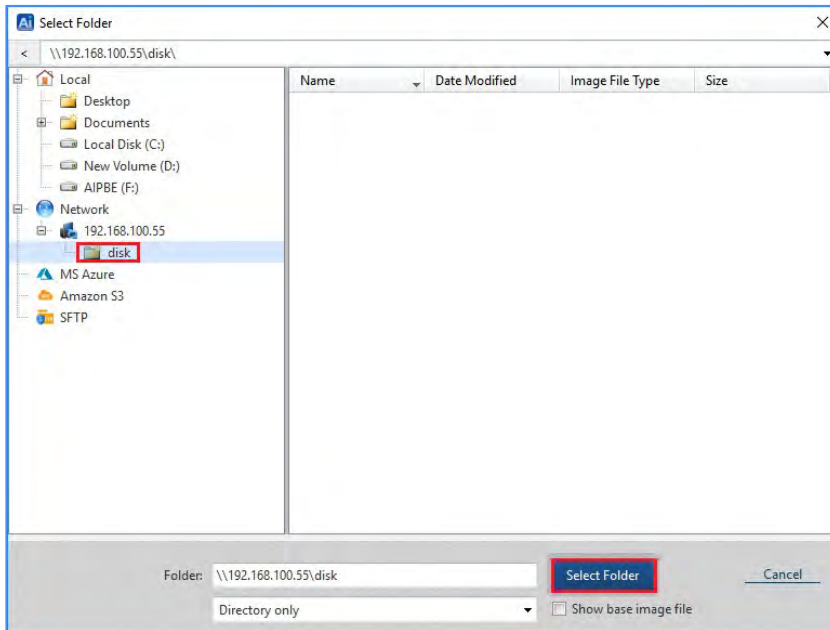


11. Specify the destination folder and press the [Enter] key to set the destination folder. For example, we've entered "\\192.168.100.55\disk" as the destination folder.

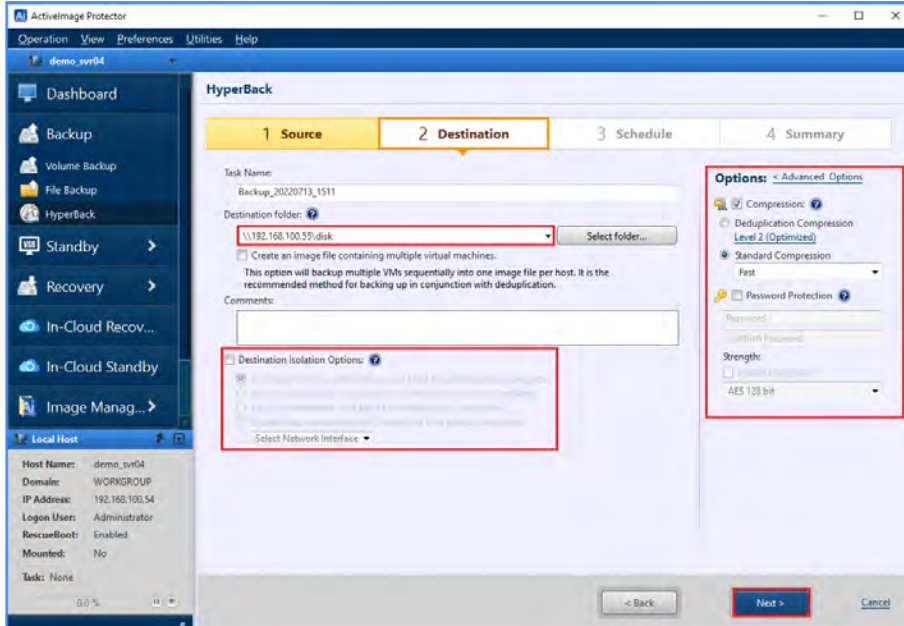
- Enter your username in the **[User Name]** field (e.g., "192.168.100.55\Administrator").
- Enter your password in the **[Password]** field.
- Click the **[Connect]** button.



12. Ensure the destination folder is correct and click the **[Select Folder]** button.



13. We will discuss the [Destination Isolation Options] and [Options] portions of this screen later in the section "4-2. Volume Backup: Scheduled Backup." For now, skip those sections, ensure your destination folder is correct, and click the **[Next]** button.

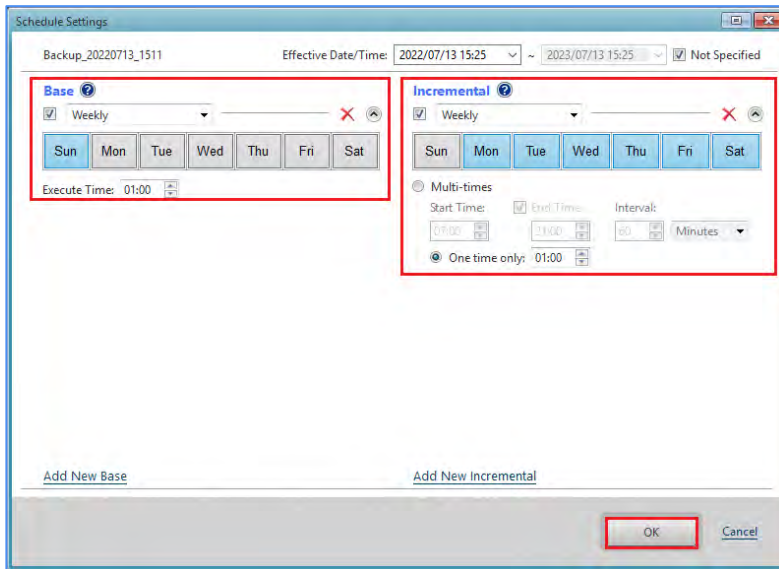


## Configure backup settings and run backup tasks

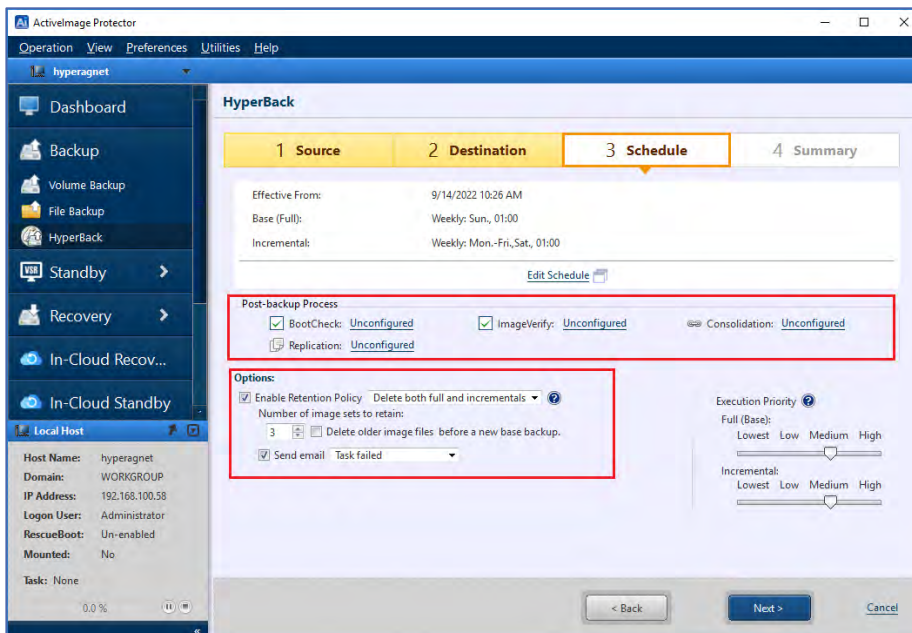
14. You should now see the **[Schedule Settings]** window. This window is where you will configure the times and frequency of your backups. In this example:

- We are configuring our base backup to run every Sunday at 1:00 a.m. in this window's **[Base]** section.
- We are configuring our incremental backups to run weekly, Monday through Saturday, at 1:00 a.m. in this window's **[Incremental]** section.
- You may also run your incremental backups multiple times daily, if you'd like, by selecting a **[Start Time]**, **[End Time]**, and the **[Interval]** to run the incremental backup tasks between those two times.

After configuring your schedule, click the **[OK]** button.



15. You can use the **[Enable Retention Policy]** and **[Send email]** settings to customize your retention policy and email notifications from the **[Schedule]** tab. Once you have configured these options to your liking (see below for more details), click the **[Next]** button to continue.

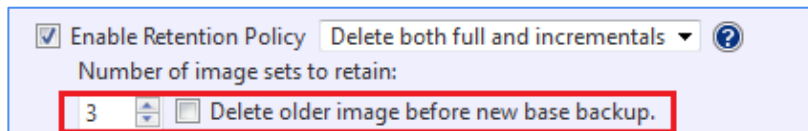




## (1) Enable Retention Policy

The **[Enable Retention Policy]** option specifies how many sets of backup files ActiveImage Protector will retain before deletion. Click on the **[Enabling Retention Policy]** checkbox to enable the retention policy. By default, ActiveImage Protector will save the three most recent backup sets before it starts deleting them. You can change this default by increasing or decreasing the number of image sets to retain using the **[Number of image sets to retain]** setting.

**Note:** One generation of ActiveImage Protector backup image files represents one base backup image file and all associated incremental backup files.

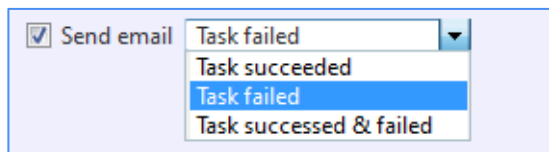


## (2) Send email

You can enable the **[Send email]** option if you want the system to notify you of a scheduled task's completion status by email. You can select from one of three options:

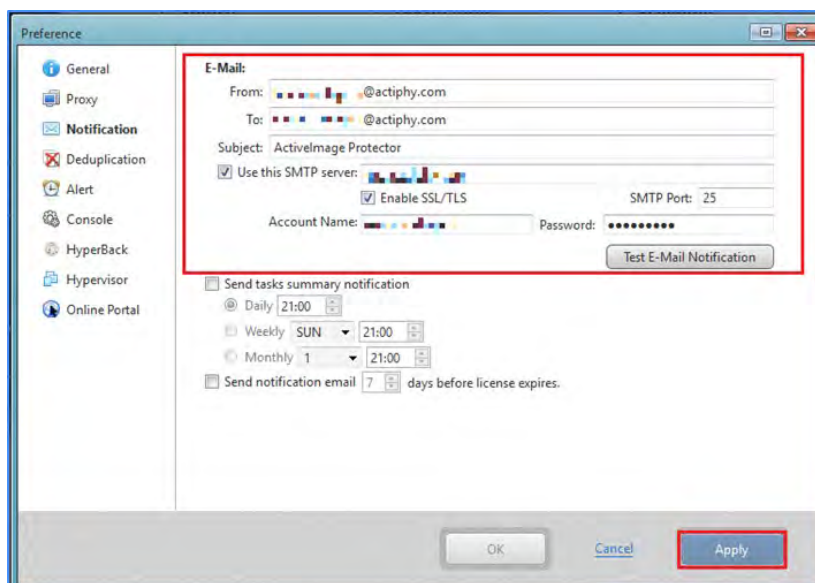
- **[Task succeeded]**
- **[Task failed]**
- **[Task succeeded or failed]**.

If you select **[Task succeeded]**, the system will only notify you if a backup task succeeds. If you select **[Task failed]**, the system will only notify you if a backup task fails. If you select **[Task succeeded or failed]**, the system will send you a notification whenever it completes backup tasks, regardless of their status. Before enabling the **[Send email]** option, you will need to go to **[Preferences]** → **[Notifications]** and configure your email settings.



## (3) Email Settings

Go to **[Preferences]** → **[Notifications]** and configure the email settings. After configuring the email settings, click the **[Test E-Mail Notification]** button to ensure that the settings configured for email notifications are accurate. Please use this option to check if the email is received by the specified recipient and click the **[Apply]** button.

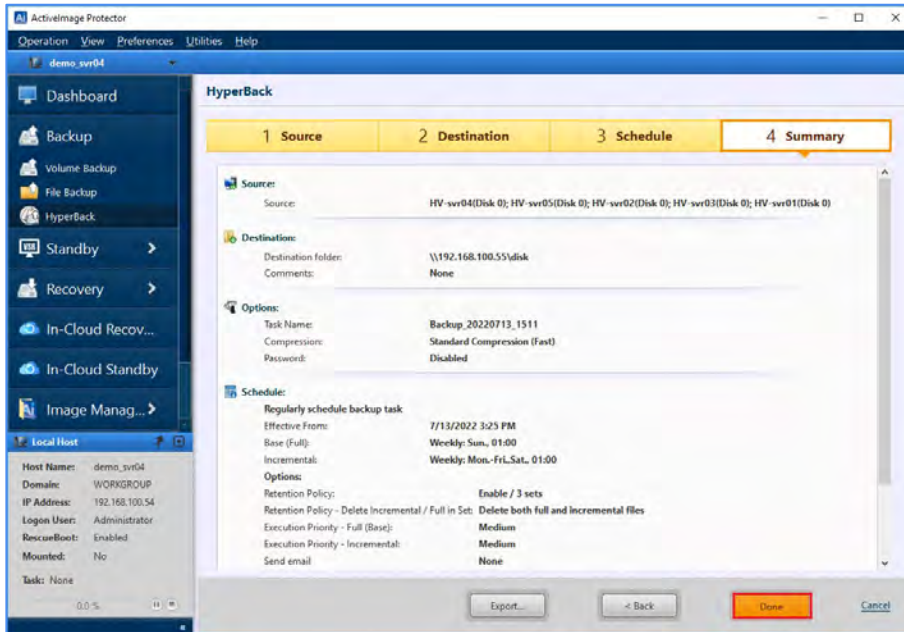




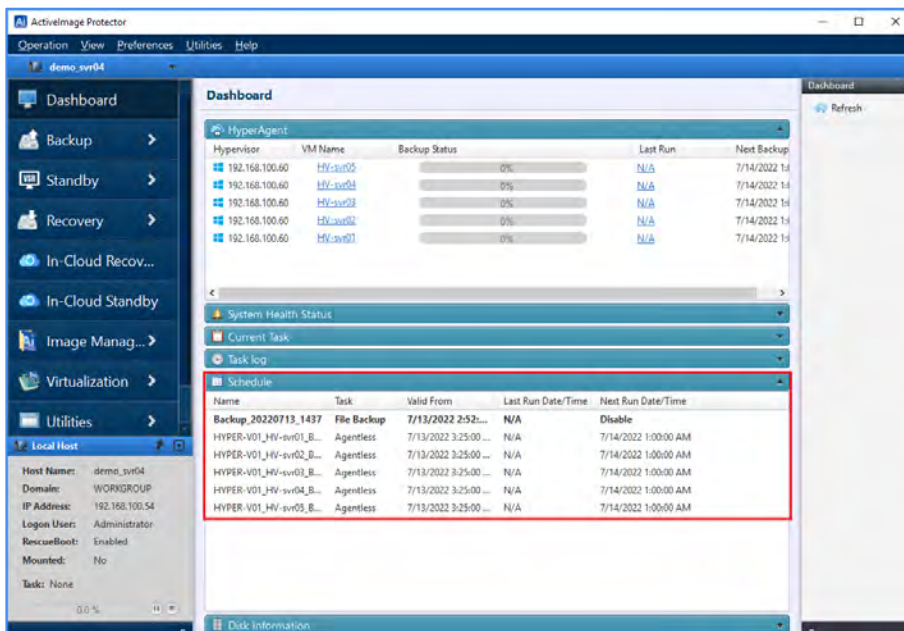
## Configure backup settings and run backup tasks

16. You should now be on the [4 Summary] screen. You should see a summary of your backup configurations and schedule settings.

Review the information on this screen and click the **[Done]** button if everything looks OK. ActiImage Protector should return you to the **[Dashboard]** screen.

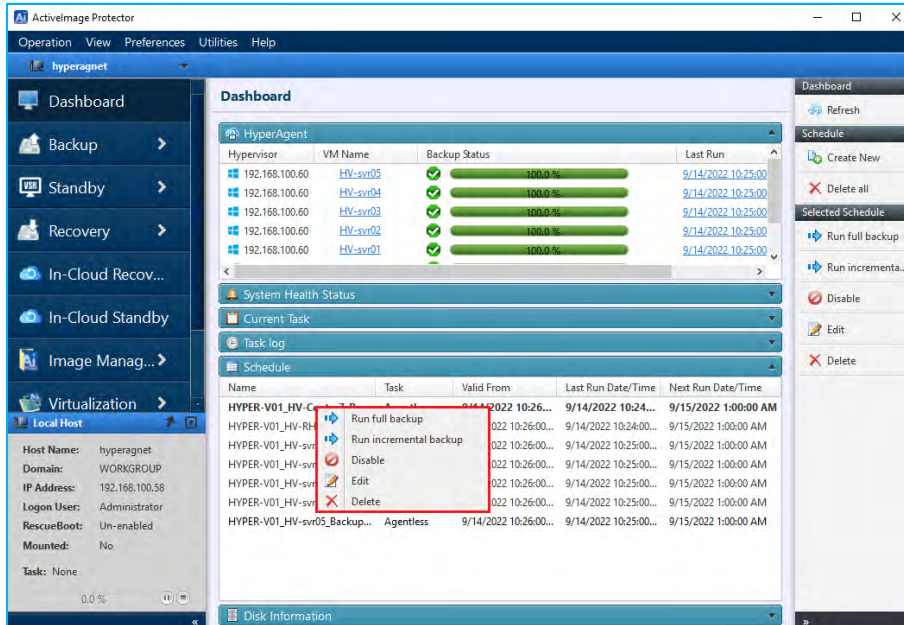


17. You can see a list of all your configured backup tasks and their status in the **[Schedule]** section of the **[Dashboard]**.



18. 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.



19. Option settings for HyperBack

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



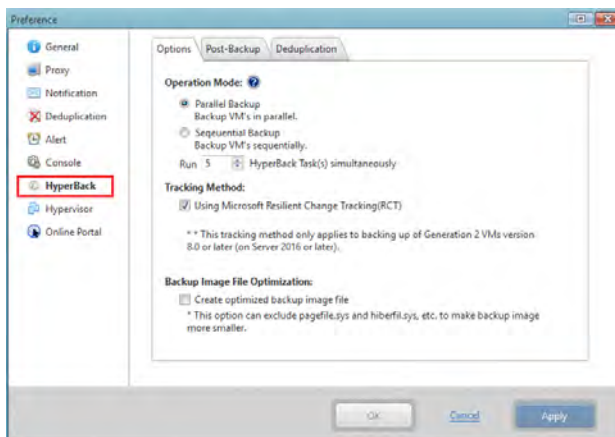
### • Operation Mode

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

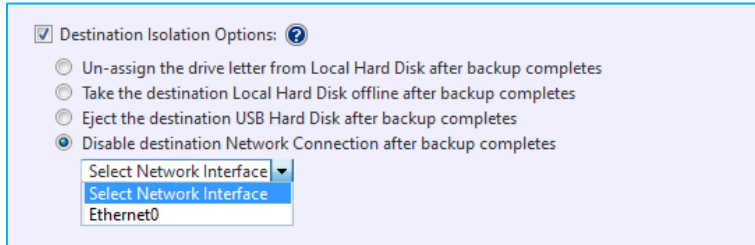
When **[Parallel Backup]** is enabled, specify the concurrently executable number of HyperBack tasks. If the system resources of your HyperAgent computer or your network resources are insufficient, we recommend you select **[Sequential Backup]**.

### • 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.



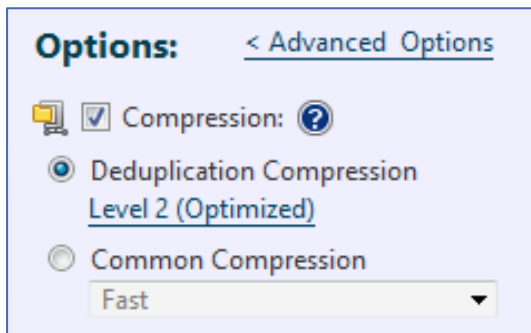
20. Configure Destination Isolation Options settings. Enabling the **[Destination Isolation Options]** causes the system to disconnect network access to the backup image's storage drives or sets the destination disk offline once the backup task is complete. The **[Destination Isolation Options]** feature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



21. 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.

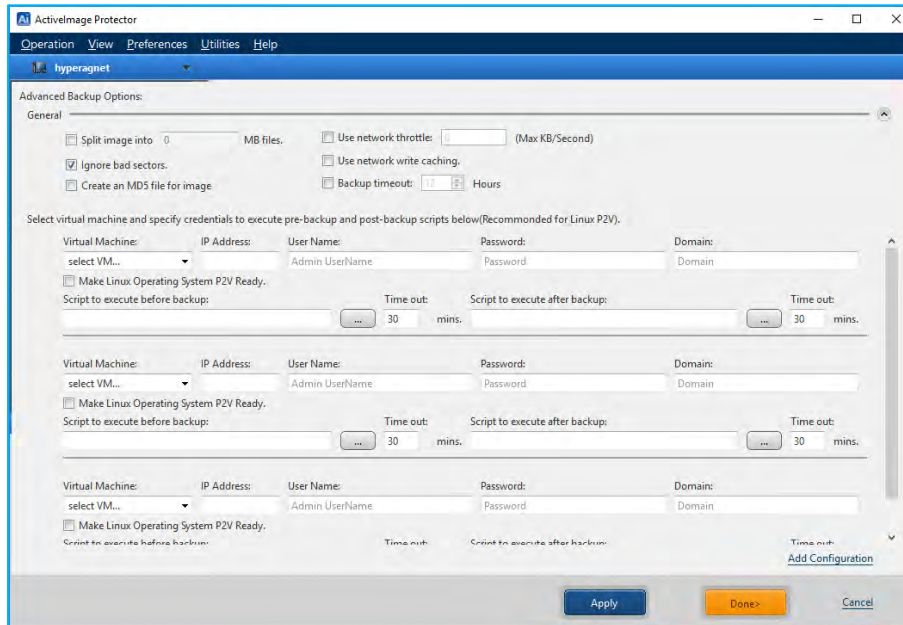
- **Enable Encryption**

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.



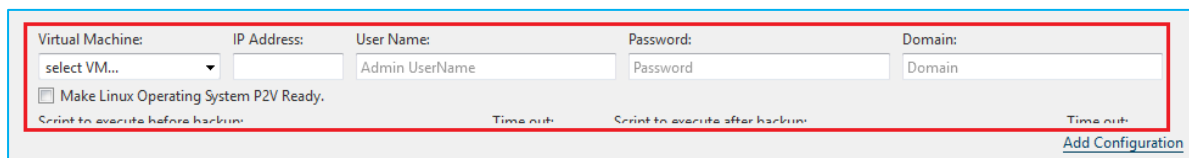
## Configure backup settings and run backup tasks

22. 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 ActiveImage 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 ActiveImage Protector takes a snapshot and then start it again once the backup is complete.

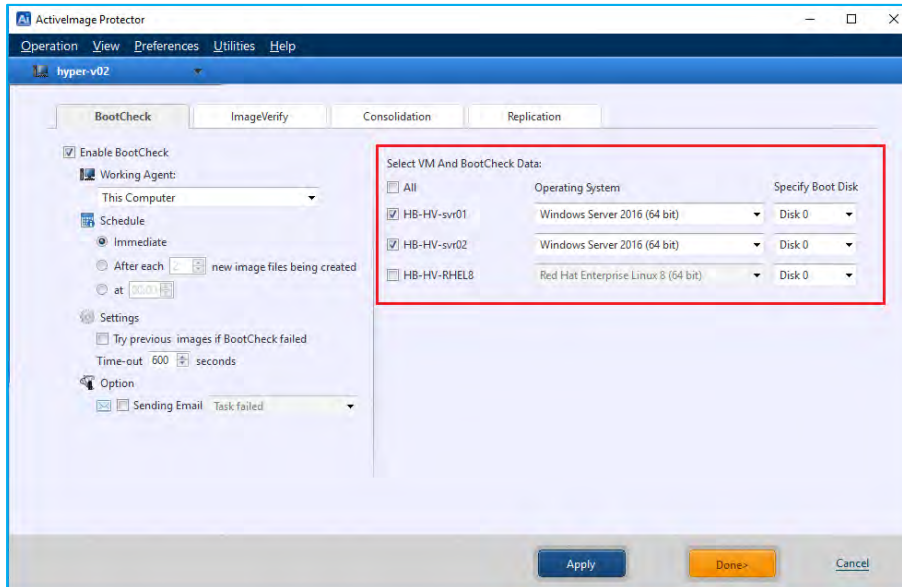


23. Post-backup Process. The Post-backup process is executed upon completion of a backup task or at a specified time. You can select an option for Post-backup Process, i.e., **[BootCheck]**, **[Image Verify]**, **[Consolidation]**, or **[Replication]**.

- **BootCheck**

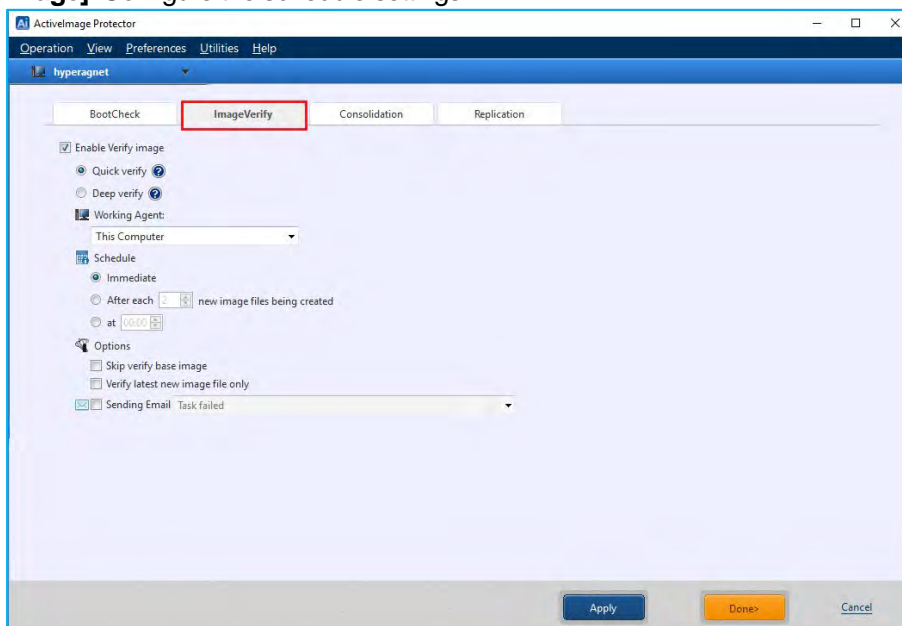
BootCheck quickly tests if a created backup of the system volumes can successfully boot on the selected hypervisor. First, click in the box to enable the **[Enable BootCheck]** option. Next, configure the Schedule settings, Sending Email options, etc.

**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.

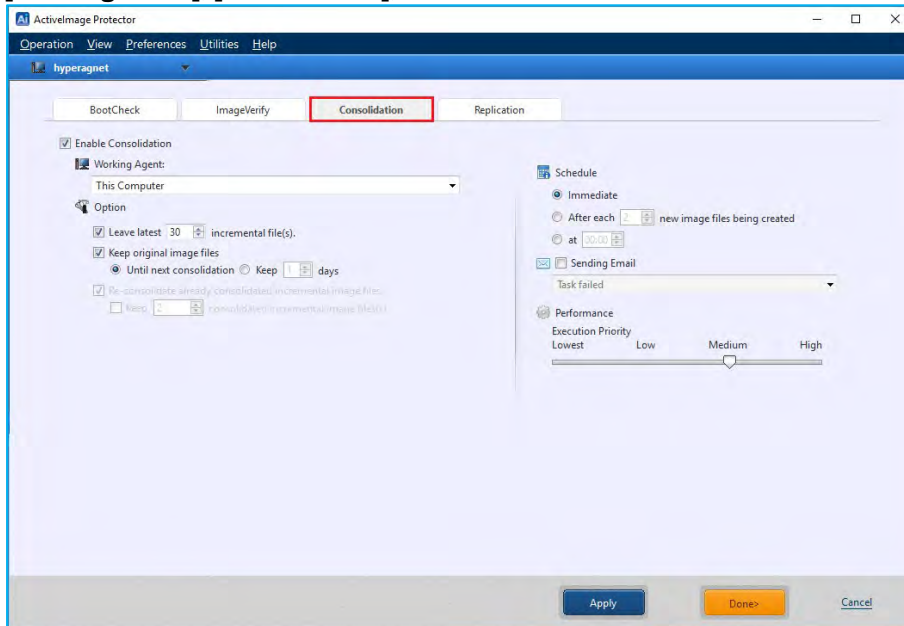




## Configure backup settings and run backup tasks

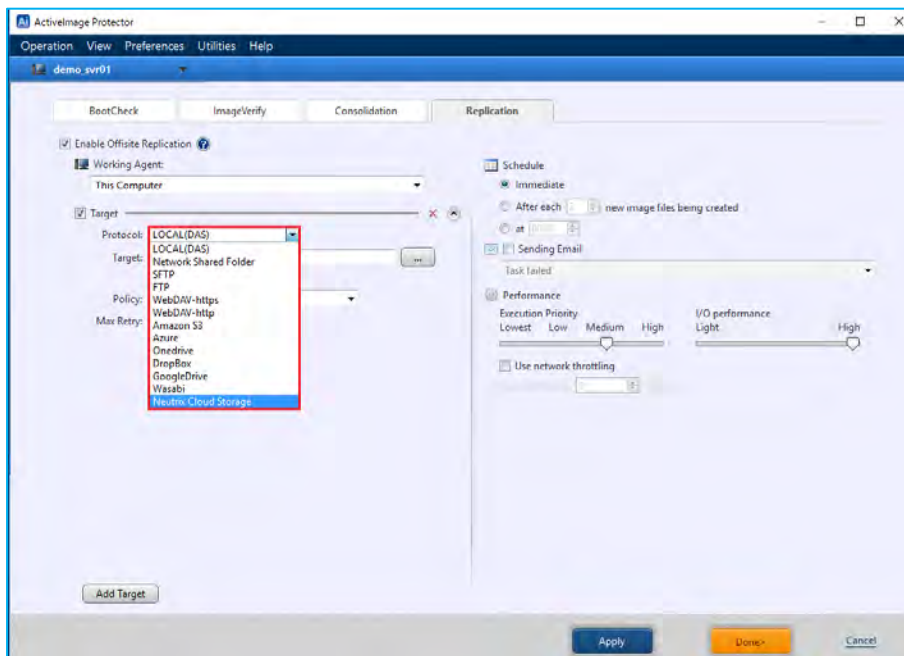
- **Consolidation**

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. Boot Environment Builder

### Build Windows-PE based Boot Environment

The ActiImage Protector media includes a Linux-based boot environment. We recommend you use this boot environment. However, if the Linux-based boot loader doesn't recognize your disks, network devices, or other hardware, you can create a Windows-based (Windows RE or Windows PE) boot environment.

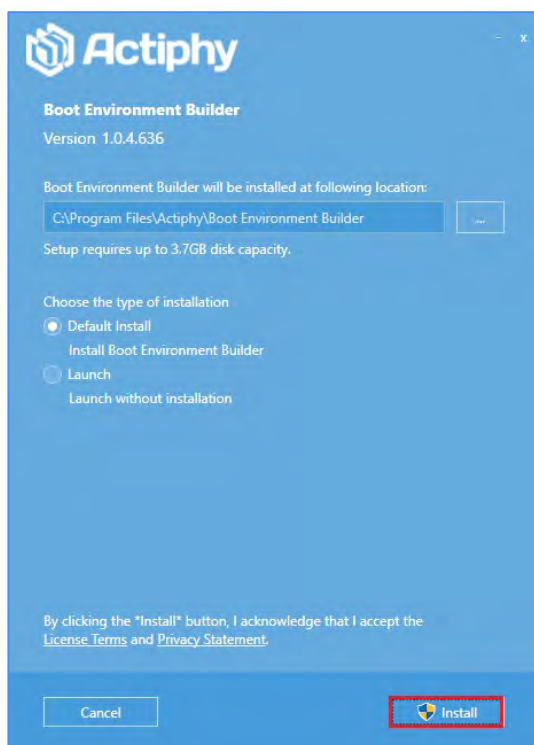
This section shows you how to build Windows RE-based (Windows Recovery Environment), should that be necessary.

Before building a Windows RE-based boot environment, please install the "Actiphy Boot Environment Builder" on a machine running Windows 10, Windows 11, Windows Server 2016, or later by following these steps:

1. Install Actiphy Boot Environment Builder.

- Run BEBuilder.exe in Setup folder in the product media.
- Start the installer.
- Click [Install] to start the installation process.

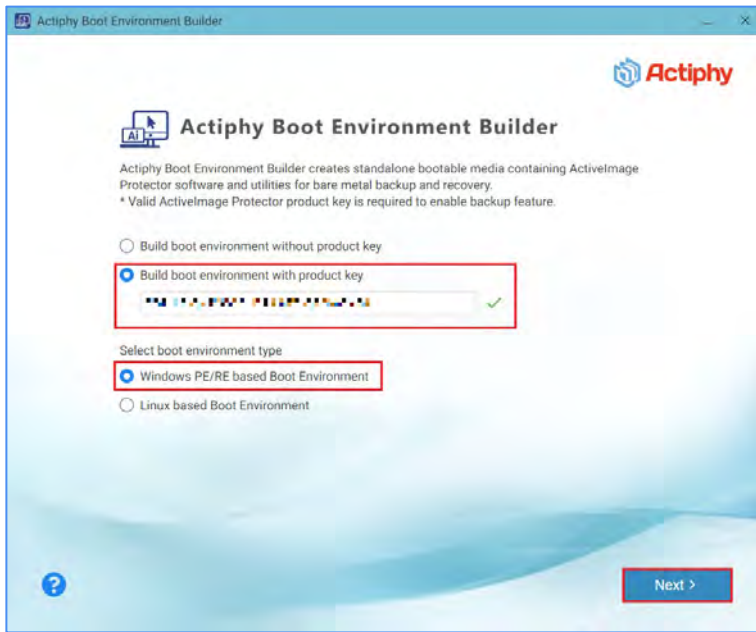
Once you have completed the installation process, you should see the **Actiphy Boot Environment Builder** on your Desktop.



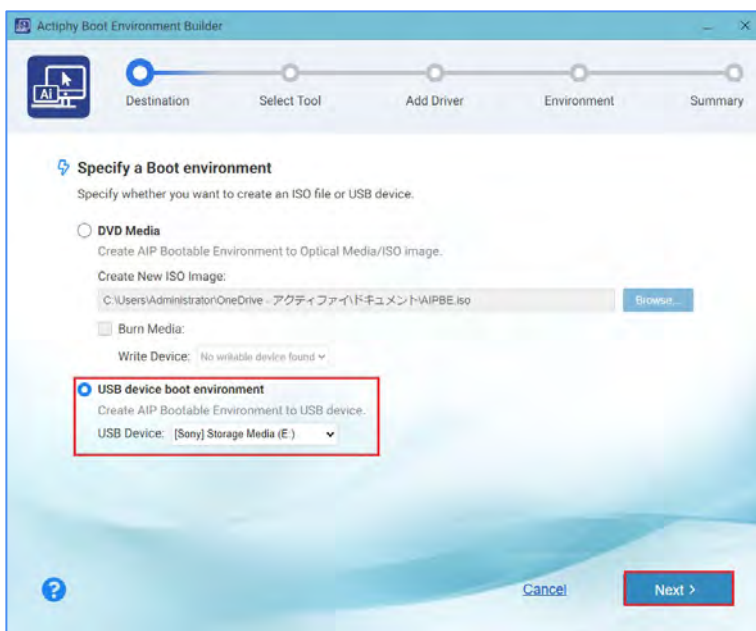
## Boot Environment Builder

2. Once you have the Actiphy Boot Environment Builder installed on your machine, you can follow these steps to create a Windows RE/PE boot environment:

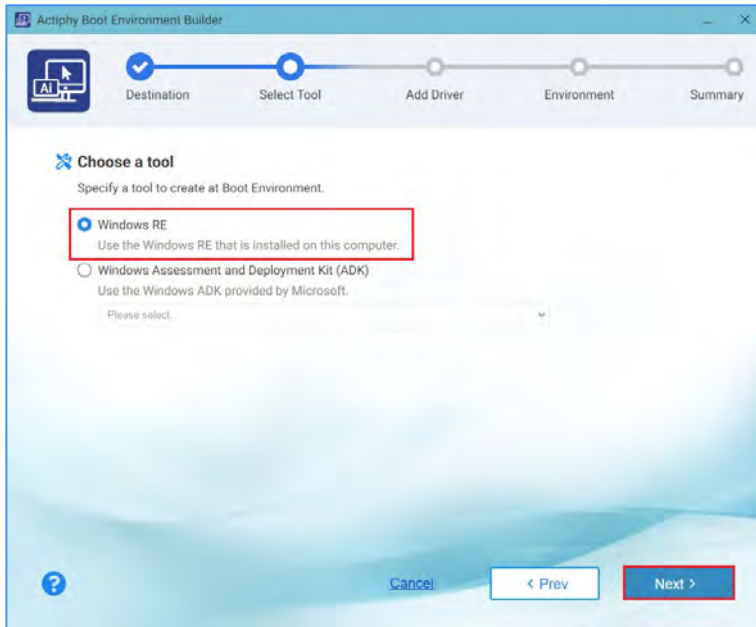
- Click on the **[Actiphy Boot Environment Builder]** icon on your Desktop.
- Once the Actiphy Boot Environment Builder starts up, select the **[Build boot environment with product key]** option and enter your Windows product key.
- Next, select the **[Windows RE/PE]** option beneath **[Select boot environment type]**.
- Click the **[Next]** button.



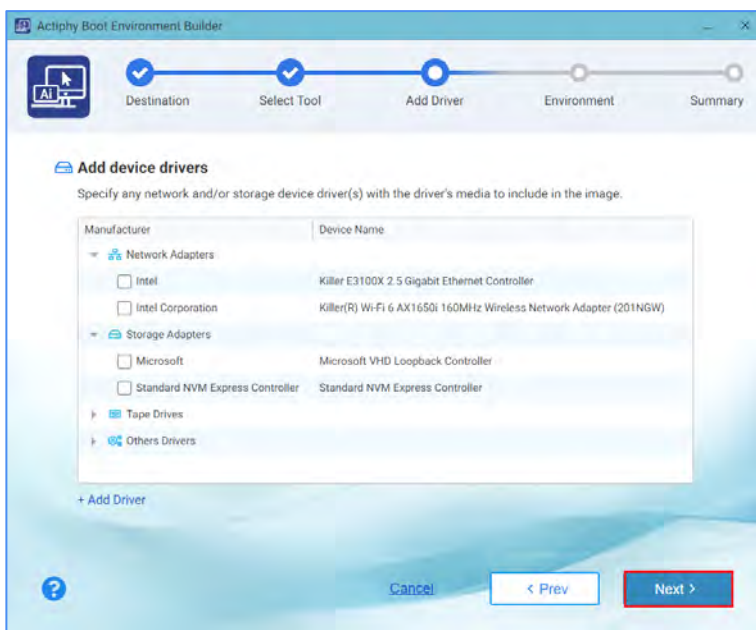
3. On the **[Destination]** screen, you can choose to create a bootable DVD or a bootable USB image. Select the image type you want to make and click the **[Next]** button.



- You should now be on the [Select Tool] screen. Here, you can specify the tool for building your boot environment.  
Please select **[Windows RE]** and click the **[Next]** button for this example.



- Next, on the **[Add Driver]** screen, select the device driver(s) you want to include in your boot environment. The Actiphy Boot Environment Builder will automatically detect the network and storage devices for the current system and include them in the device list. Click on the checkbox next to the device drivers you want to include in the boot environment. If any driver is missing from the device list, you can manually add it by clicking on the **[+ Add Driver]** link and providing the INF file for your device. Once you have selected all the necessary drivers for your computer, click the **[Next]** button to continue.



6. Next, you need to configure the following on the **[Environment]** screen:

- The language you want to use in your bootloader.
- The type of keyboard you are using.
- The keyboard layout.
- The time zone your bootloader should use.
- The display resolution for your bootloader.

Please configure the settings for **[Language]**, **[Keyboard type]**, **[Keyboard layout]**, **[Time Zone]**, and **[Display Resolution]** for your bootloader and click the **[Next]** button.

Actiphy Boot Environment Builder

Destination Select Tool Add Driver Environment Summary

**Specify environment**

Specify language, keyboard type, timezone and resolution for then Boot Environment.

Language: English

Keyboard type: 106 Key Japanese

Keyboard layout: United States

Time zone: (UTC+09:00) Seoul

Display resolution: 1024\*768 : XGA (Recommended)

Cancel < Prev Next >

7. Finally, review your settings on the **[Summary]** screen and ensure you have configured your bootloader the way you want it to be.

If you need to make any changes, you can click on the **[< Prev]** button to go back to previous pages and make any necessary changes to the configuration. You can also click on one of the blue nodes at the top of the screen to jump to a specific page.

Once you have verified your configuration, click the **[Done]** button. You will see a confirmation message. If you are ready to build your bootloader, click the **[OK]** button to build your boot environment.

Actiphy Boot Environment Builder

Destination Select Tool Add Driver Environment Summary

**Summary**

To create USB device or ISO file when you click a [Done] button.

Tool:	Windows RE
Destination:	E
Timezone:	(UTC+09:00) Seoul
Language:	English
Keyboard Type:	106 Key Japanese
Keyboard Layout:	United States
Display resolution:	1024*768 : XGA (Recommended)
Estimated size:	718.84 MB

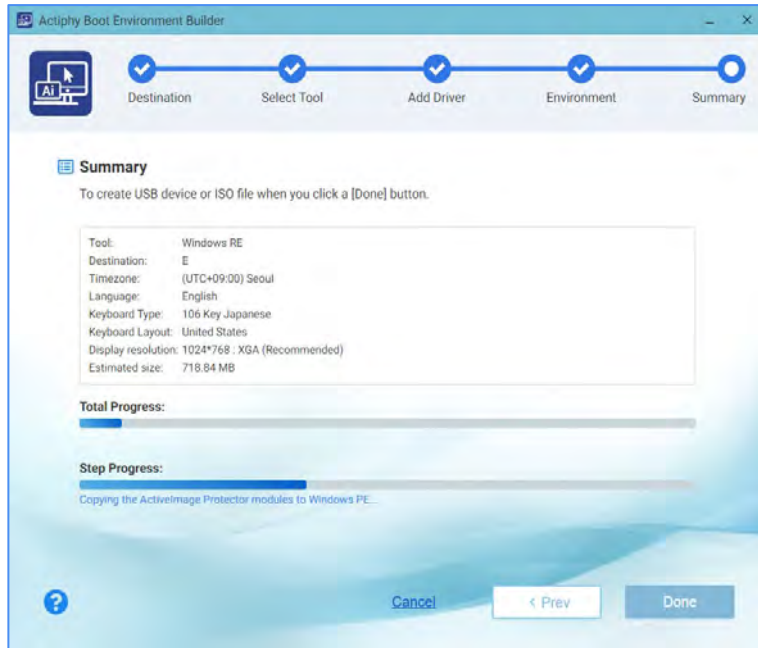
Total Progress:

Step Progress:

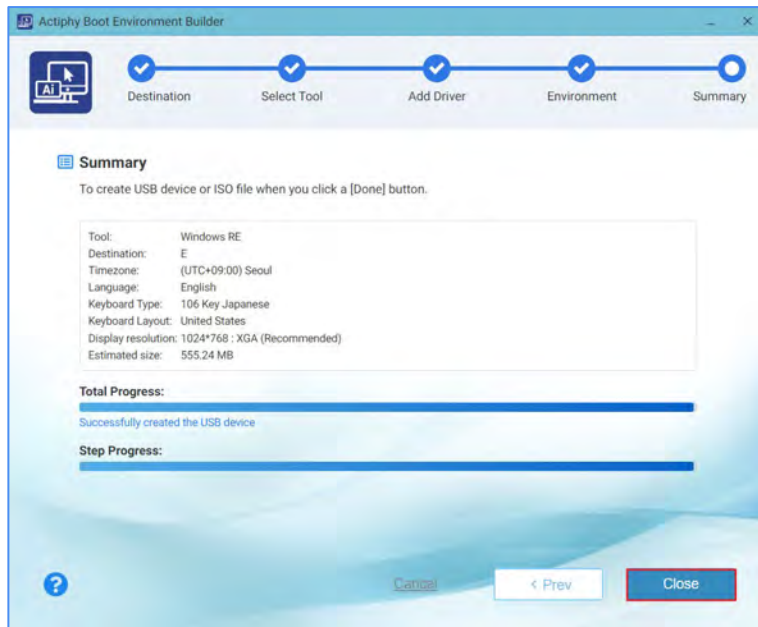
Cancel < Prev Done

## Boot Environment Builder

- The Actiphy Boot Environment Builder will start building your boot environment. Progress bars allow you to monitor the total progress and the progress of each step as the system builds your boot environment.



- Once the Actiphy Boot Environment Builder has completed the creation process, you will see the message "Successfully created the [USB or DVD] device." Click the **[Close]** button to complete the process.



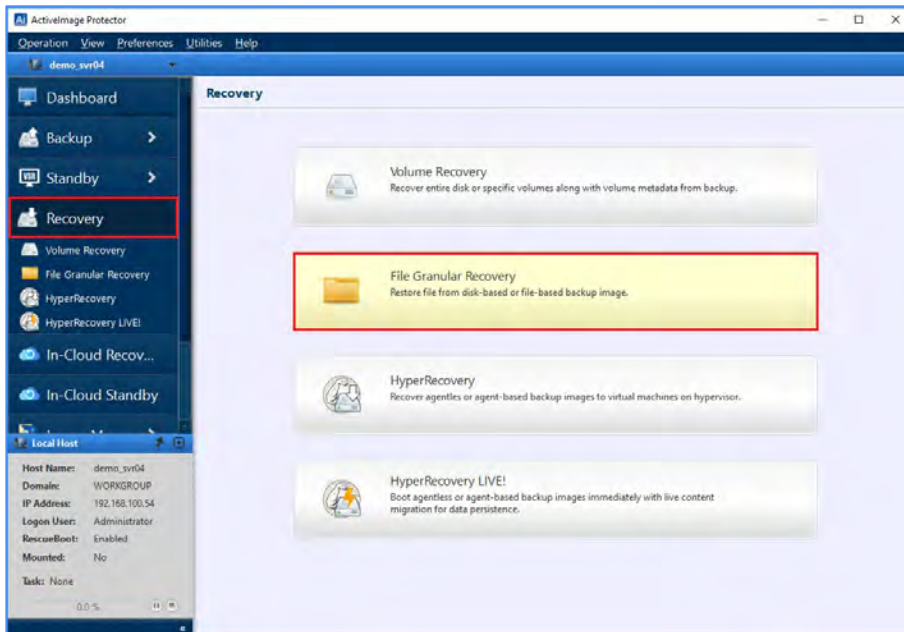


## 6. Restore

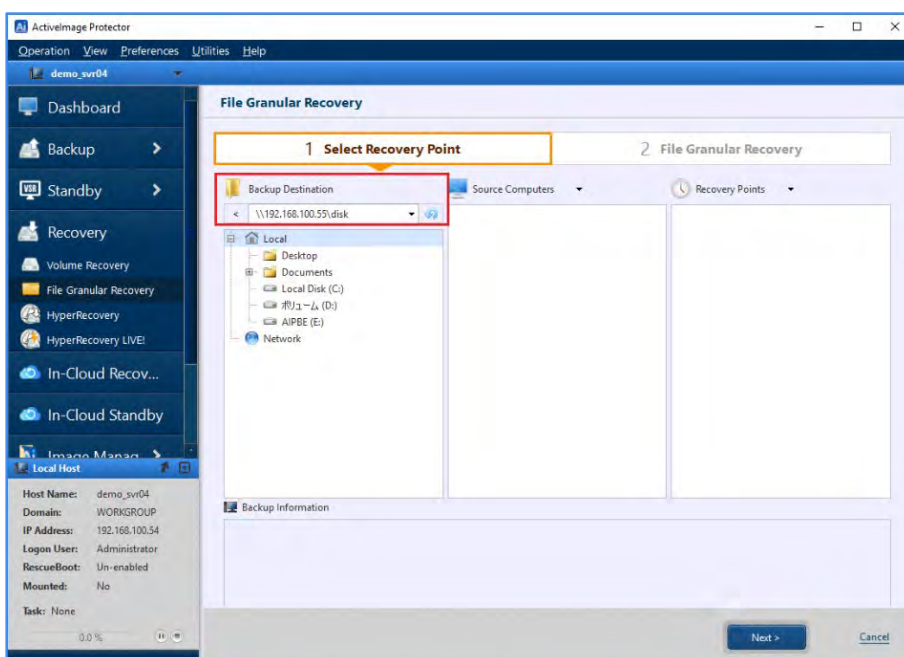
### 6-1. File / Folder Recovery

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

1. Start ActiImage Protector by clicking on the Windows Start menu and navigating to **[Actiphy]** → **[ActiImage Protector]**.
2. Select the **[Recovery]** menu. Click on the **[File Granular Recovery]** button.



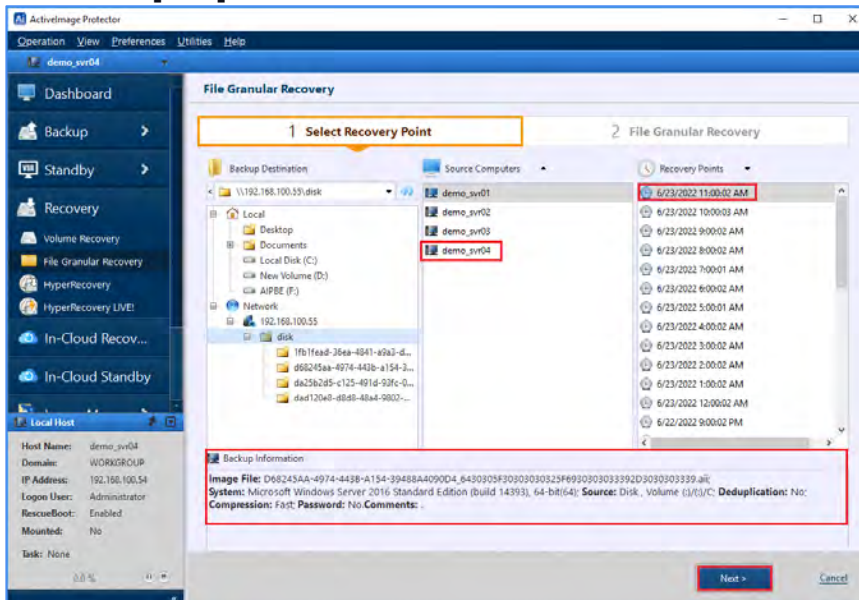
3. Next, on the **[File Granular Recovery]** screen: Click on the [▼] icon under **[Backup Destination]**.
  - Select the folder containing the backup image file from which you want to restore a file or folder.
  - You can also specify the path to the backup image. In this example, we're using "\\192.168.100.55\disk"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





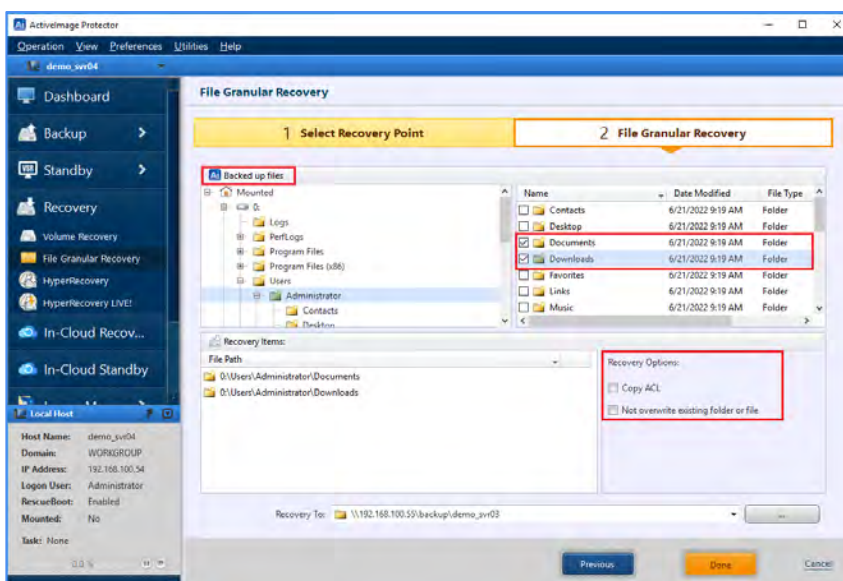
## Restore

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



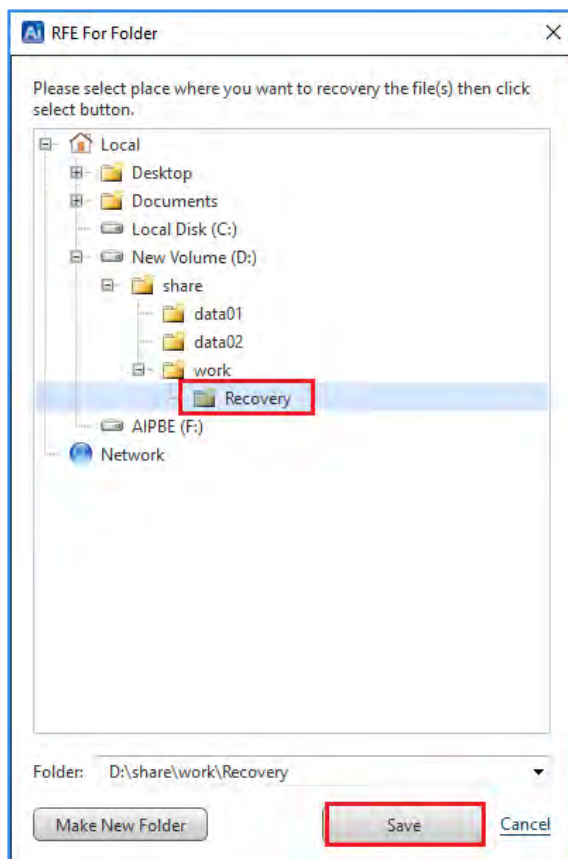
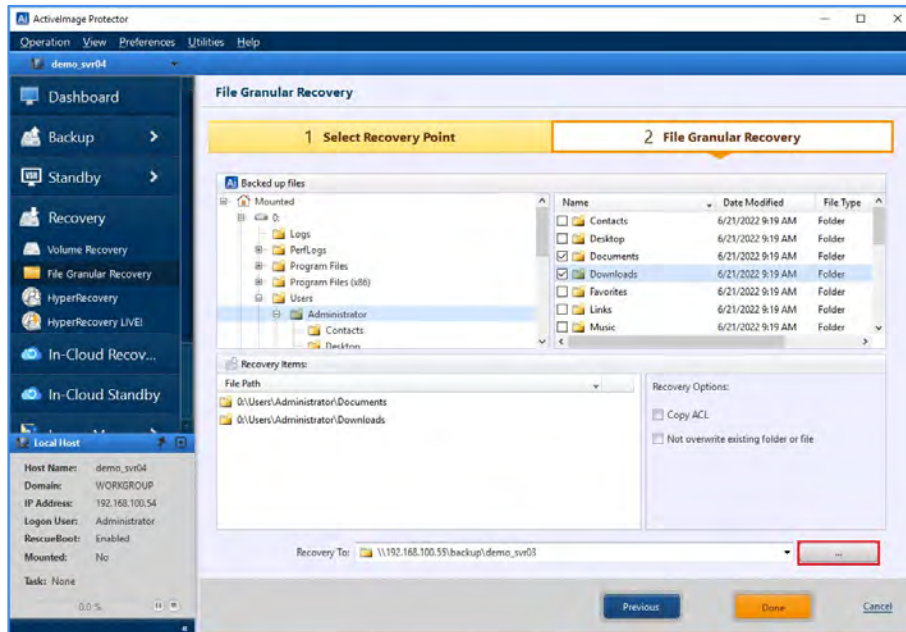
5. Now, click the checkbox next to each file or folder you want to restore in the **[Backed up files]** list. Activelmage Protector will list each item you've selected in the **[Recovery Items]** section of the page. Once you have selected all the files and folders you want to restore from the **[Backup 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.



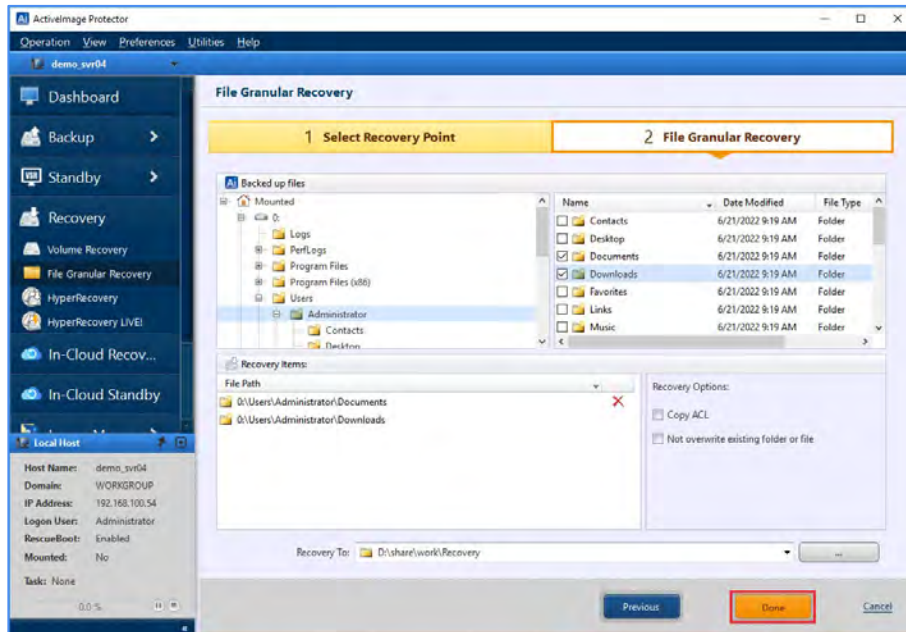
## Restore

- Click the [...] button to specify a destination folder to save your restored items. When finished, click the **[Save]** button.

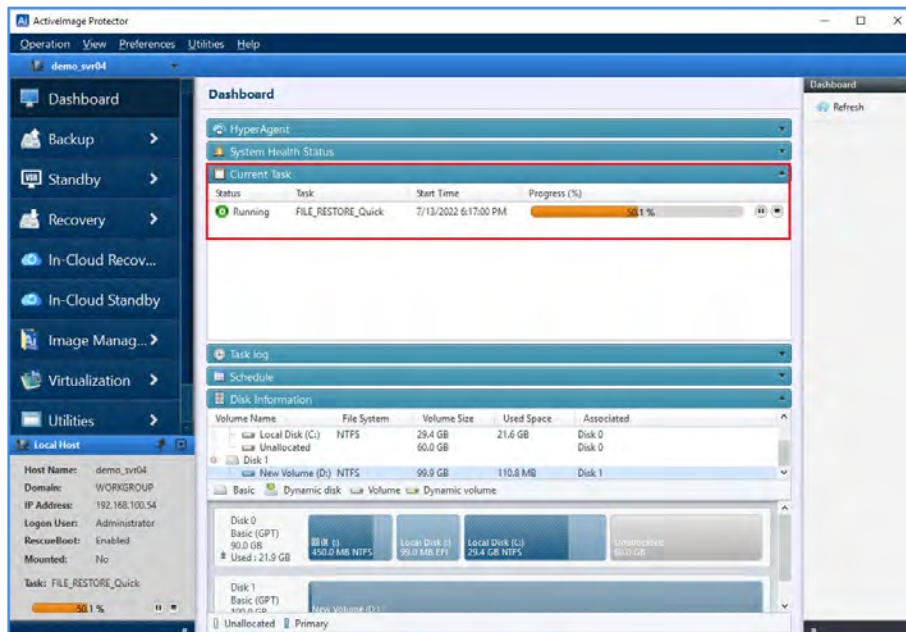


## Restore

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

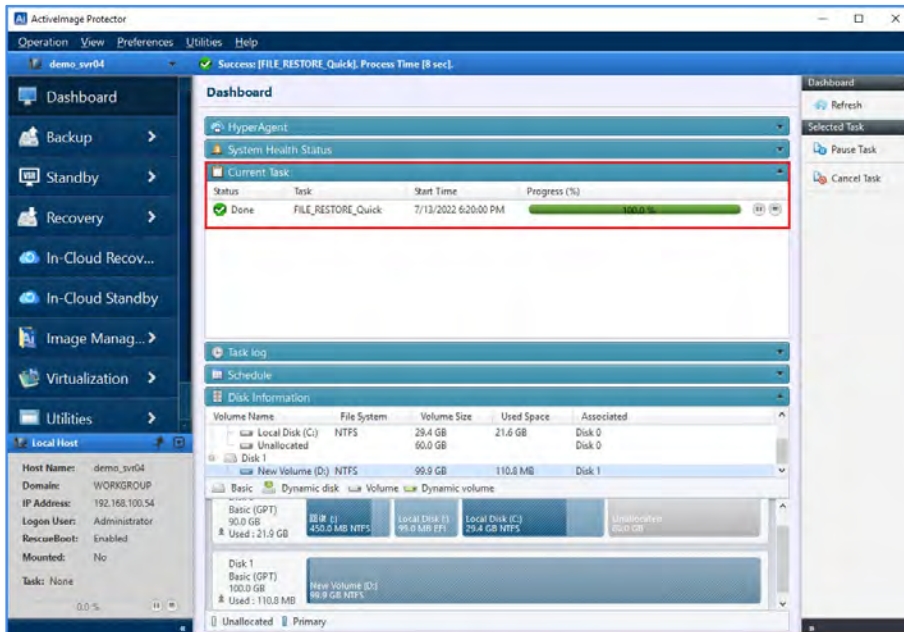


- ActiveImage Protector will display the restoration progress in the **[Current Task]** section.



## Restore

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



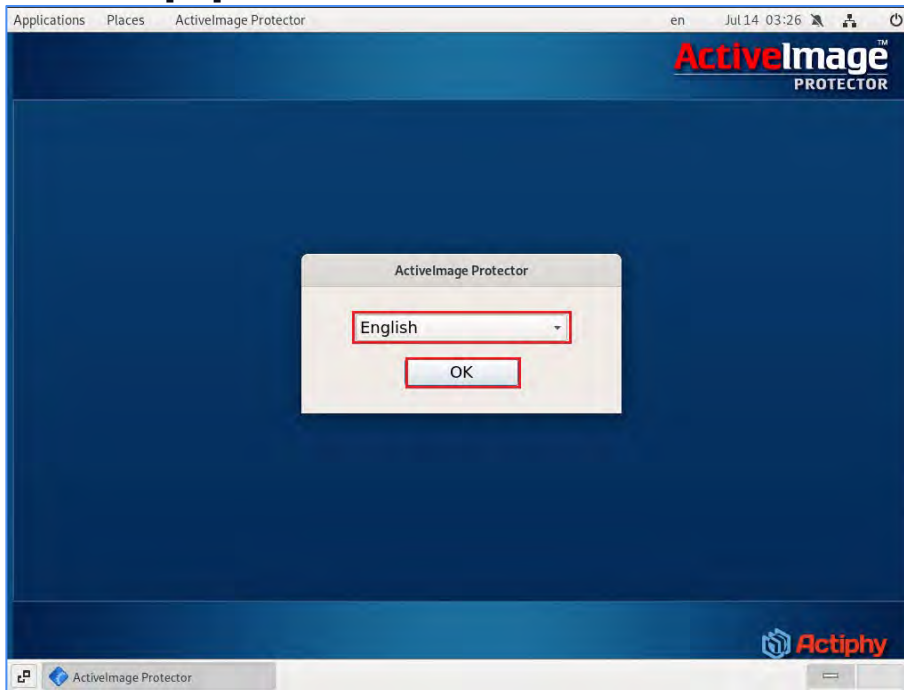


## 6-2. System Recovery : Standard Linux-based boot environment

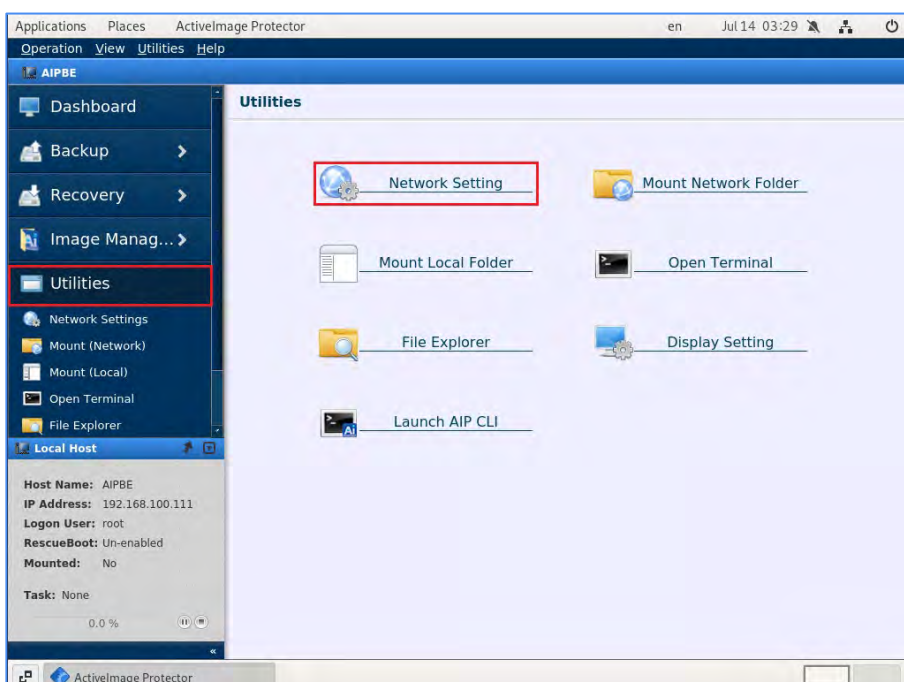
Use the following steps to recover a system using ActiveImage Protector's product media.

**Note:** ActiveImage Protector will purge all the data on the local disk when recovering an entire system. Please ensure you have backed up any necessary files before performing a full system restore.

1. Insert the ActiveImage Protector media into your computer.
  - Reboot the computer to boot into ActiveImage Protector.
  - Select **[English]** (or whichever language you prefer).
  - Click the **[OK]** button.



2. Go to **[Utilities]** → **[Network Setting]** to configure your network settings. You will need to configure your network to access shared network folders to save your backup images.



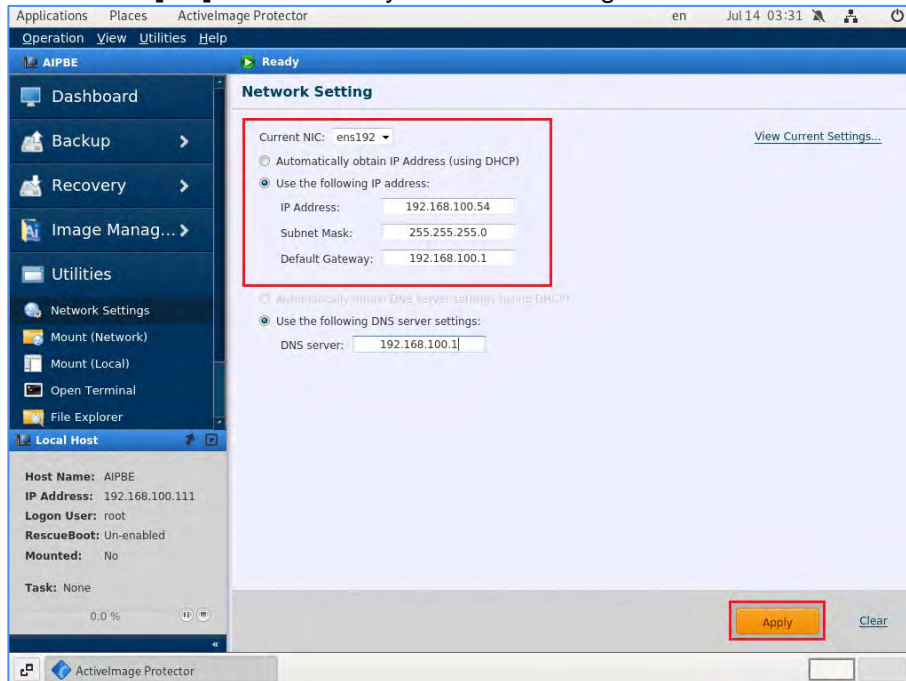
## Restore

3. Select the **[Use the following IP address]** radio button and enter your network information. We are going to use the following network information in our example:

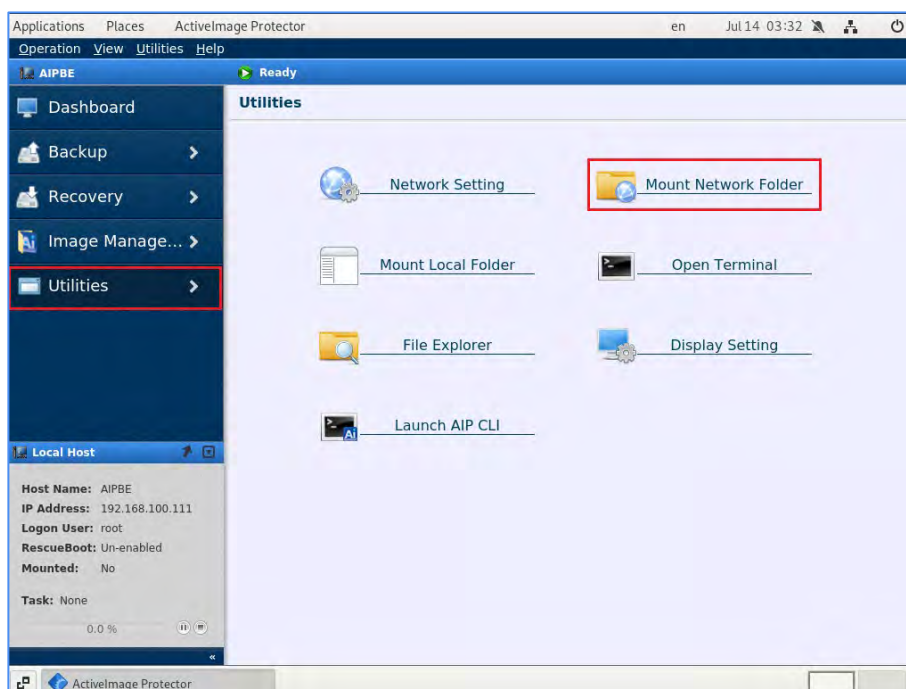
- **[IP Address]:** 192.168.100.54
- **[Subnet Mask]:** 255.255.255.0
- **[Default Gateway]:** 192.168.100.1

Please replace these IP addresses with the appropriate information for your network. Click on the **[Use the following DNS server settings]** radio button and enter your **[DNS server]** information (e.g., 192.168.100.1).

- Click the **[Apply]** button.
- Click the **[OK]** button to save your network settings.



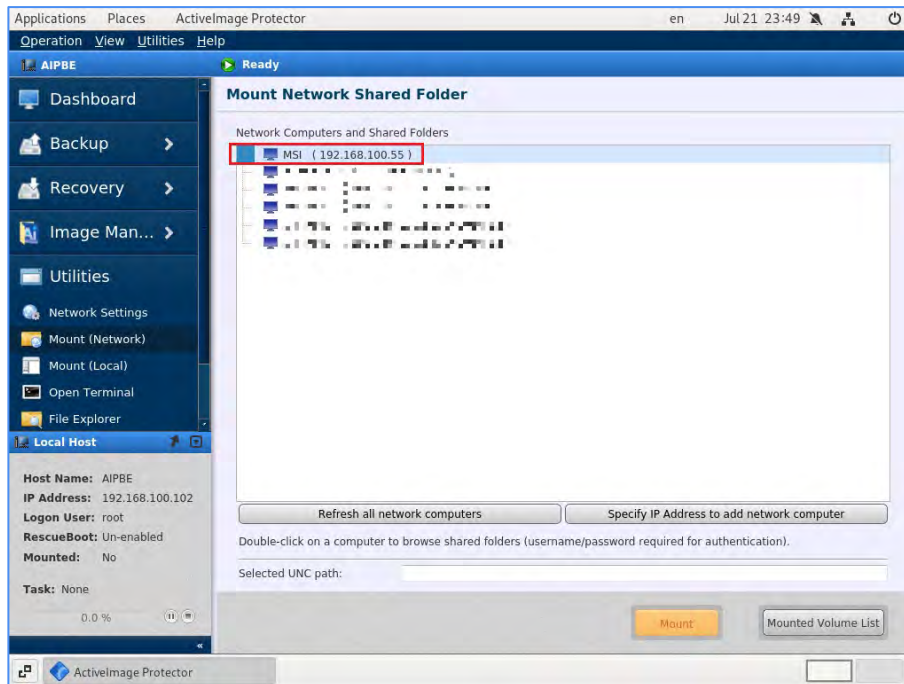
4. Click on **[Utilities]** → **[Mount Network Folder]** to mount the shared network folder you want to use as a destination for your backup images.



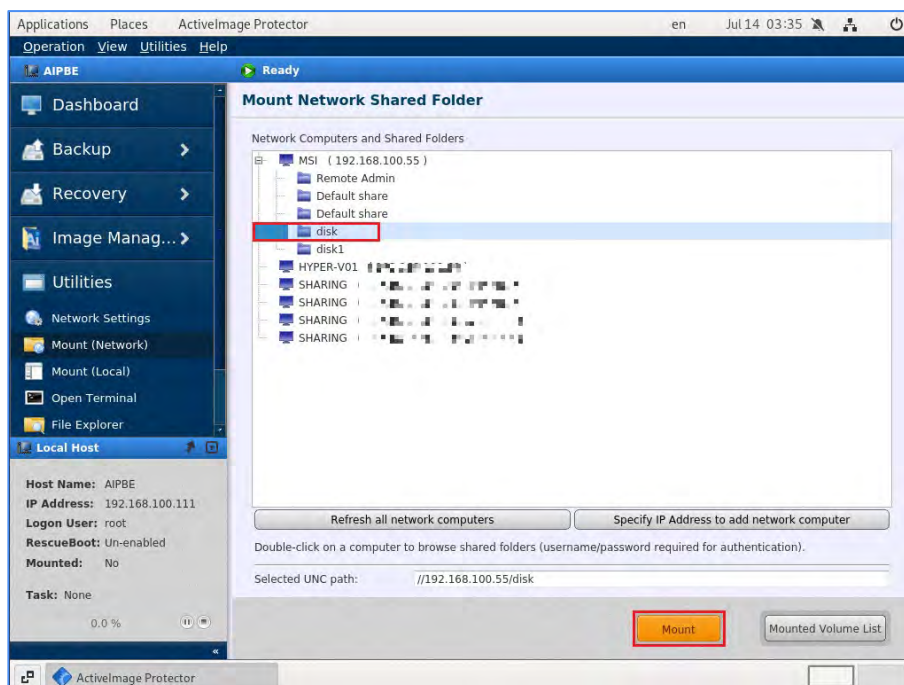


## Restore

5. Browse the shared folder. Double-click on the remote computer containing the destination shared folder. Enter your **[User Name]** and **[Password]** information to authenticate to the remote computer.

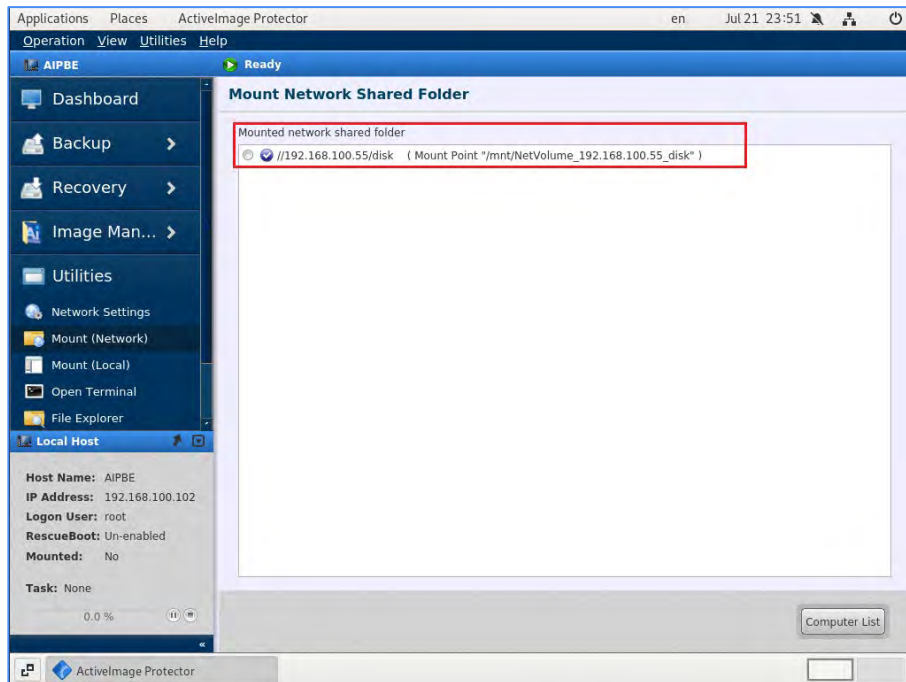


6. Mount the destination shared folder. In this example, we use the remote computer at "192.168.100.55" and the shared folder called "disk" as our backup destination. Click the **[Mount]** button.

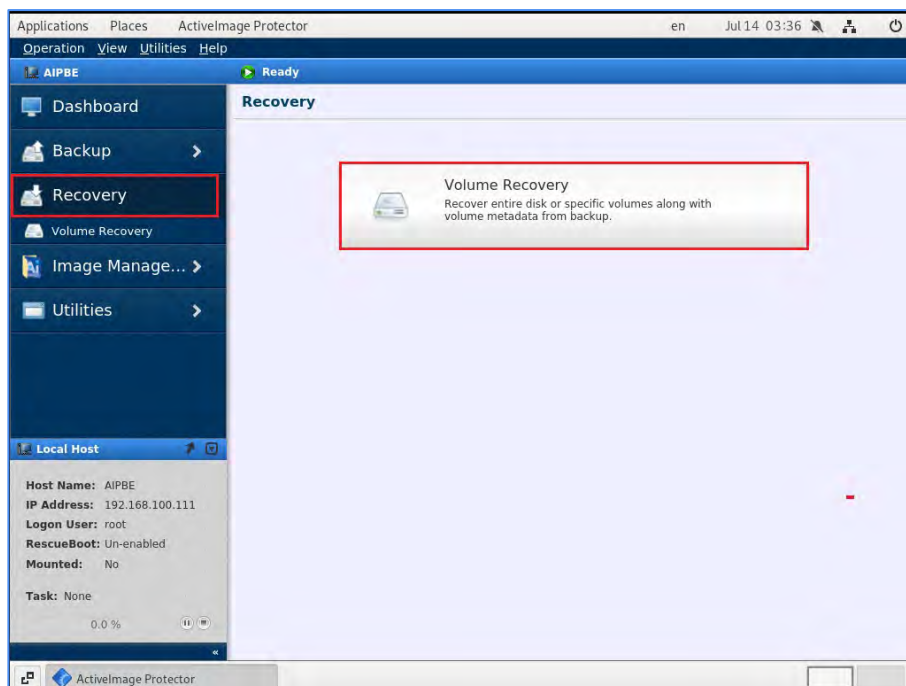


## Restore

- Once you have mounted the shared network folder, you'll see the mount point in the **[Mounted network shared folder]** list.



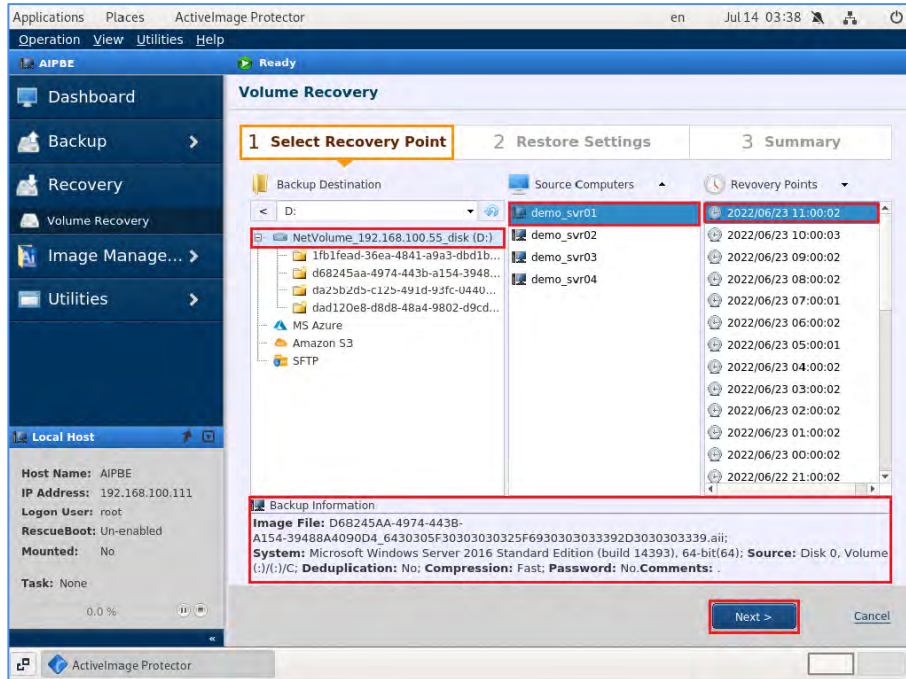
- Click on **[Recovery]** → **[Volume Recovery]** to recover your entire disk or specific volumes, including volume metadata, from a backup image.



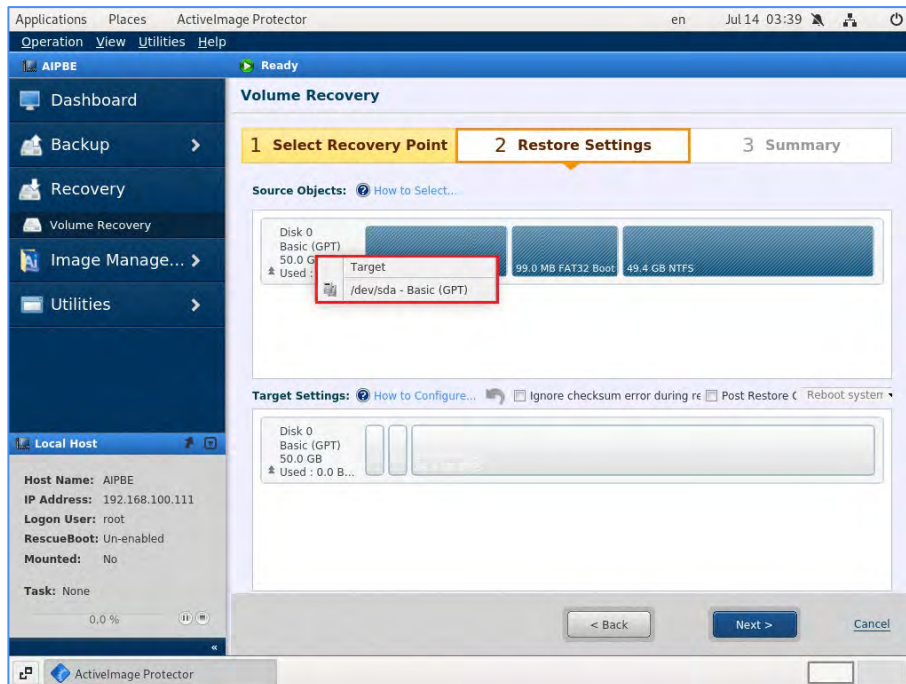
## Restore

### 9. Select the mounted shared network folder.

- Select the **[Host]** backup source.
- Select the **[Recovery Point]**.
- Click the **[Next]** button.

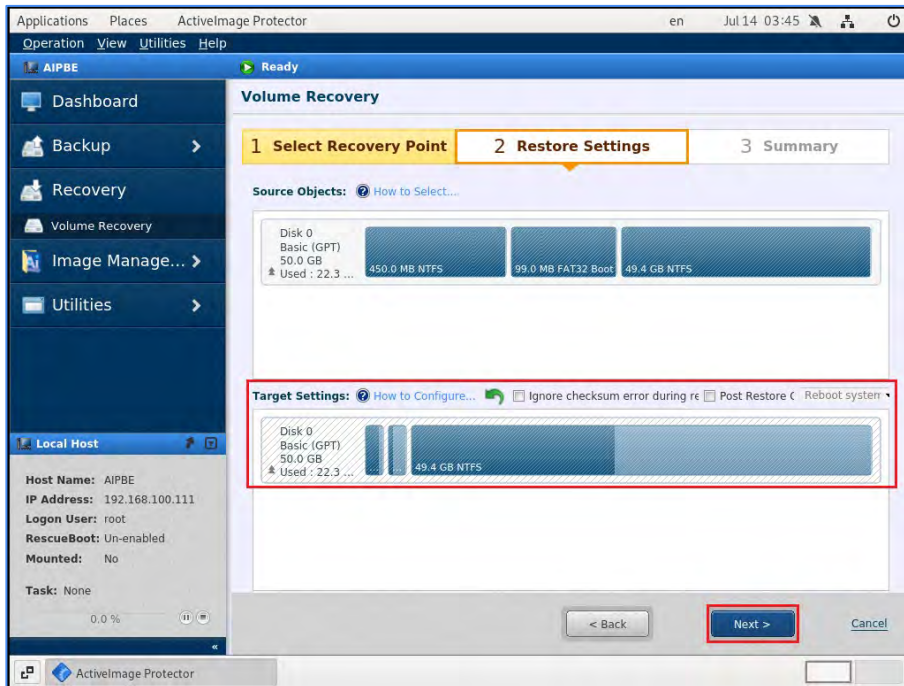


### 10. Right-click on the left part of the disk map in the **[Source Objects]** section. Select "/dev/sda – Basic (GPT)" for your **[Target]**, or drag and drop "/dev/sda – Basic (GPT)" to the restore target disk.

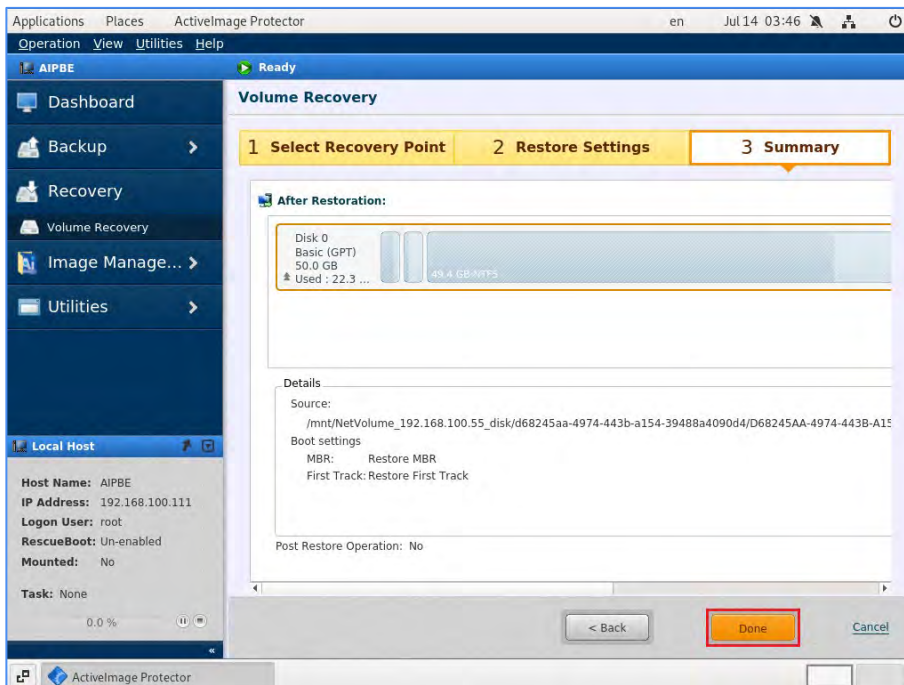


## Restore

11. Ensure the **[Target Settings]** information under the **[Restore Settings]** screen is correct. Click the **[Next]** button.



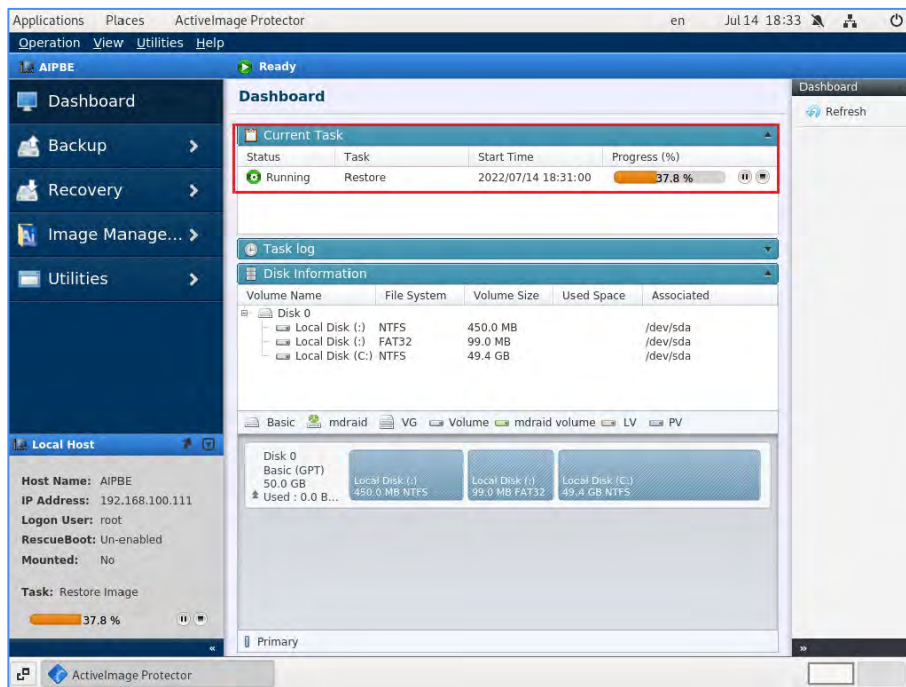
12. Verify the information on the **[Summary]** screen is accurate. Click the **[Done]** button to begin the restore process.





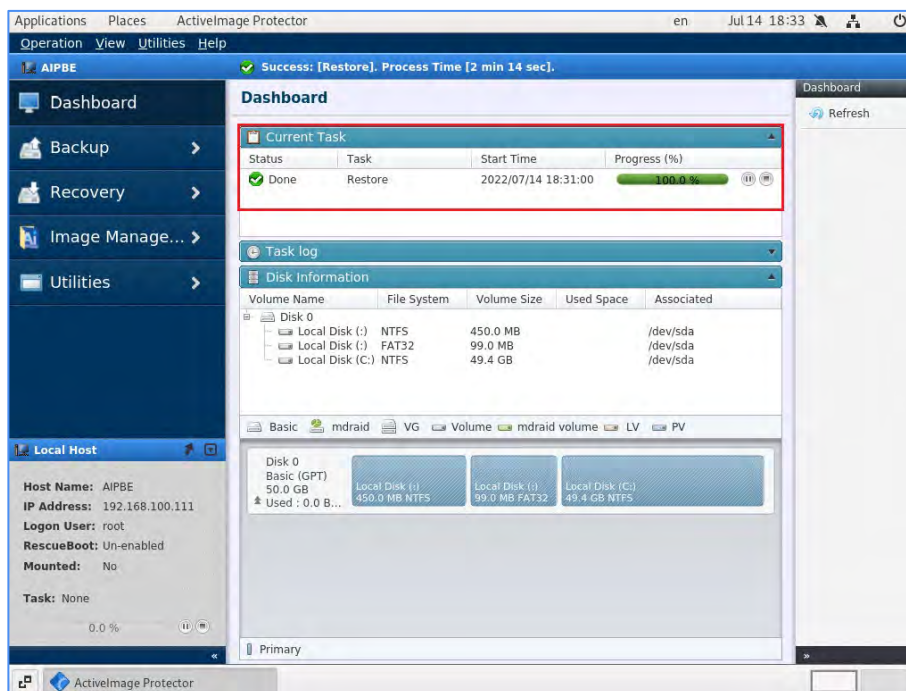
## Restore

13. ActiImage Protector will display a progress bar once you start the recovery process.



14. Once the progress bar reaches "100%," your recovery task is complete. You may now:

- Remove the boot media.
- Go to **[Operation]** → **[End]** to shut down or reboot the machine.
- Restart the computer and verify the restore task is completed successfully.



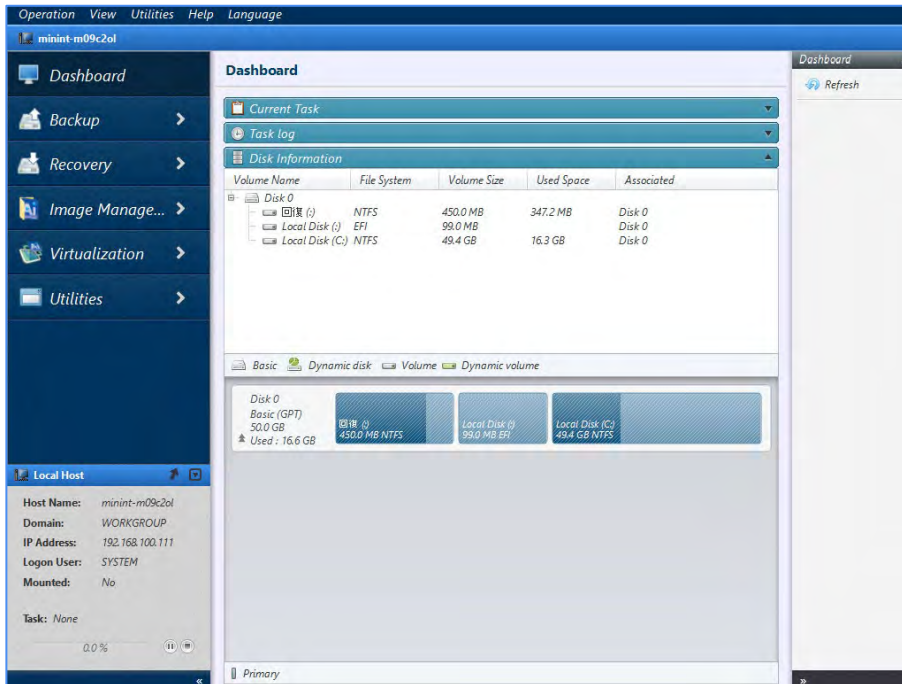


## Restore

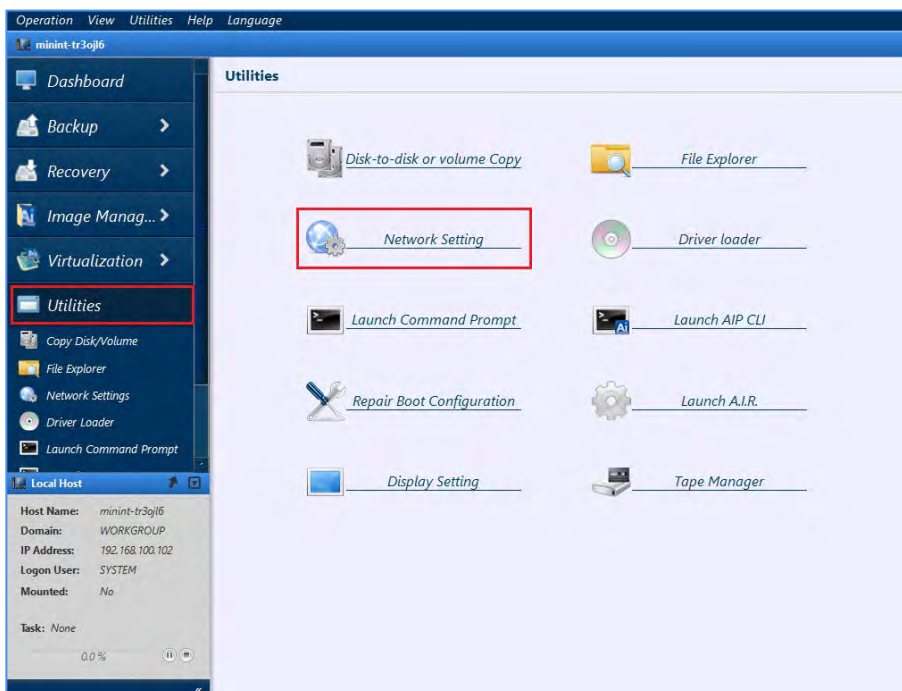
### 6-3. System Recovery : Windows RE-based boot environment

ActiveImage Protector BE builder can create recovery boot environment based on Windows-RE to be used in the case of system recover. The following is an explanation of performing a restore operation while booted into the recovery environment.

1. Insert the boot media into your machine and boot into the recovery environment. Please wait until recovery environment completely boots up.

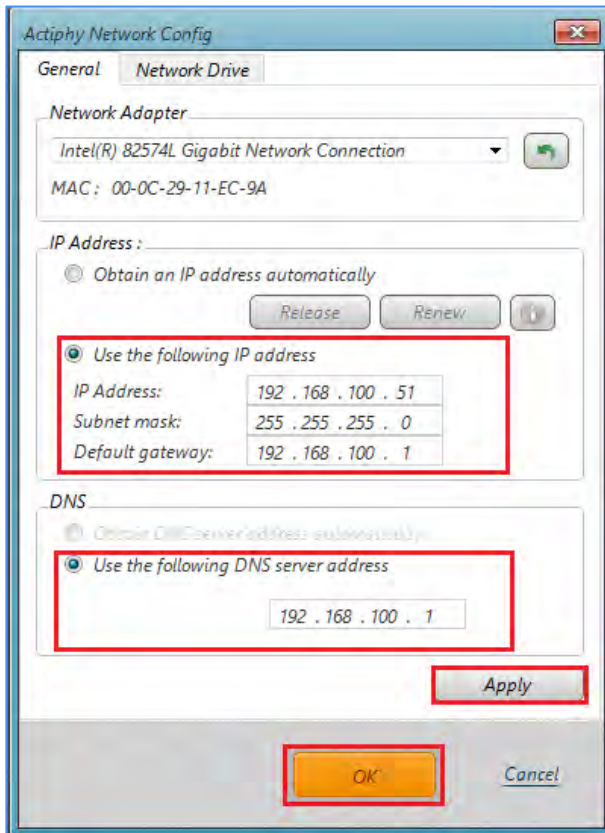


2. Configure network settings in order to access the network shared folder that contains backup image files. Click [Utilities] → [Network Setting].

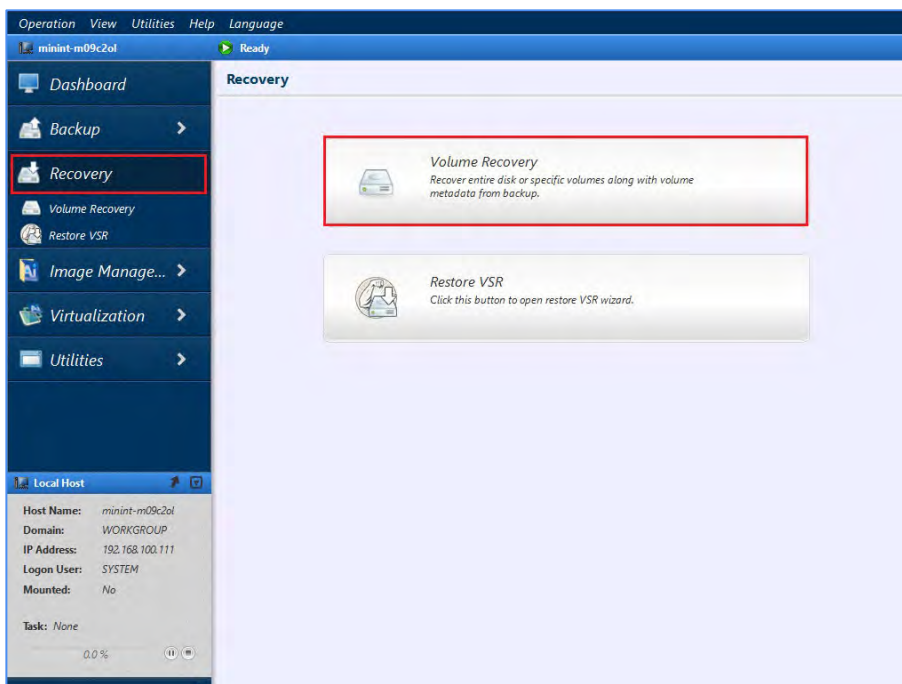


## Restore

- The **[Actiphy Network Config]** dialog is displayed. This example shows that **[Use the Following IP address]** is selected. It has The IP “192.168.100. 51” address is specified as the **[IP Address:]**, “255.255.255.0” for **[Subnet mask]**, and “192.168.100.1” for **[Default gateway]**. **[Use the following DNS server address]** is entered as “192.168.100.1”. After configuring the settings for your network environment, click **[OK]** to apply and exit the dialog.

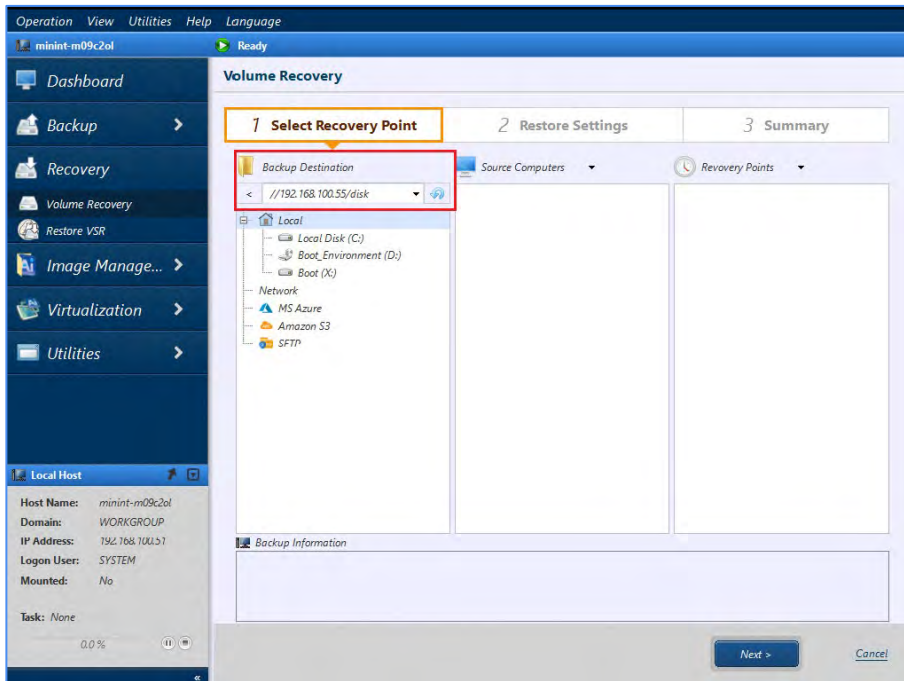


- Select **[Recovery]** → **[Volume Recovery]**.

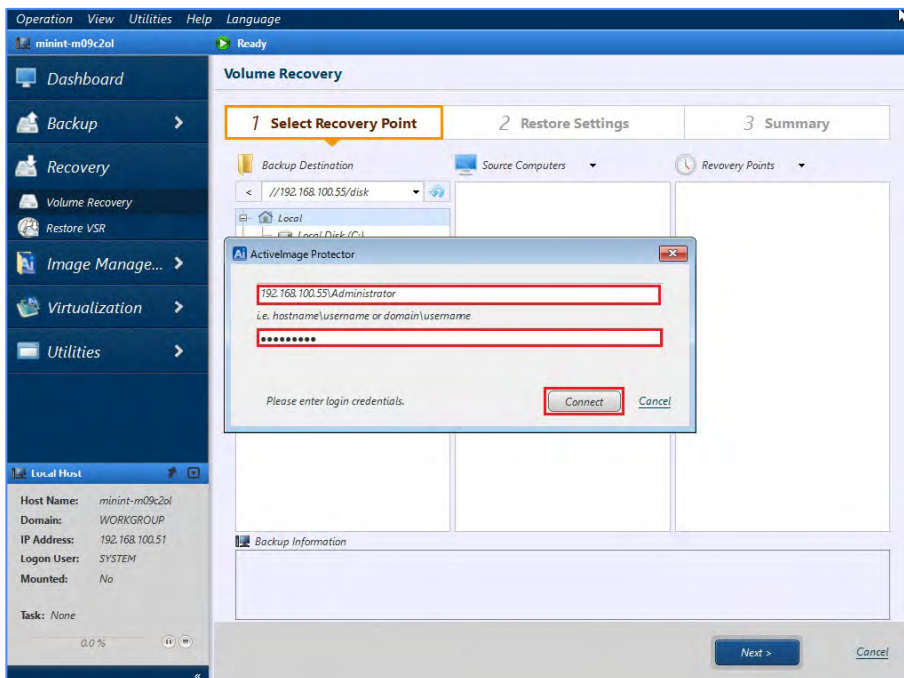


## Restore

5. In this example “\\192.168.100.55\disk” is specified for **[Backup Destination]**. Press Enter key.

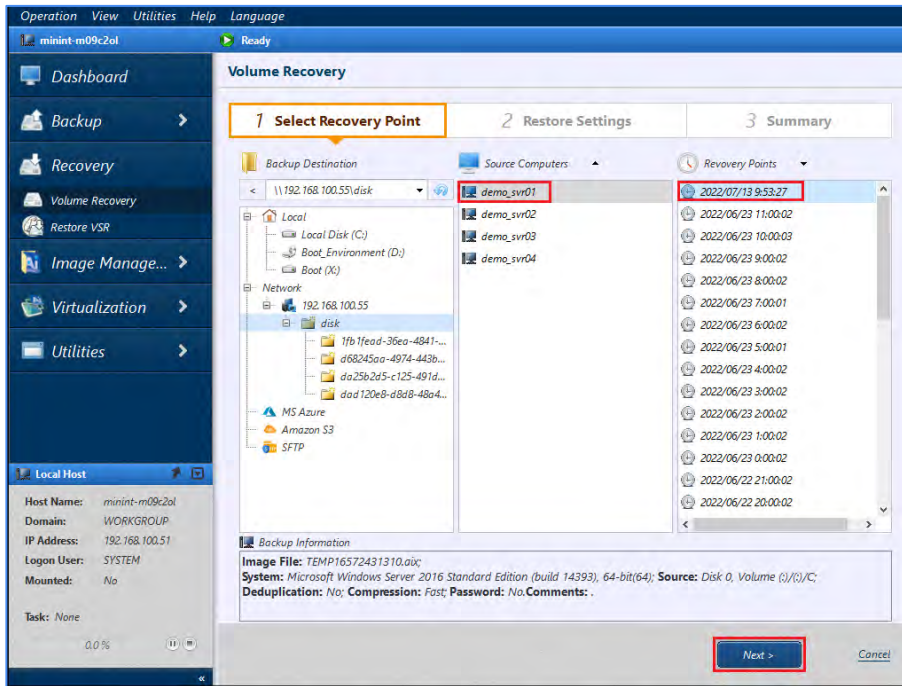


6. Enter the required credentials to access the storage location. In this example we have entered “192.168.100.55\Administrator” for the **[User Name]** and the password. Click **[Connect]**.

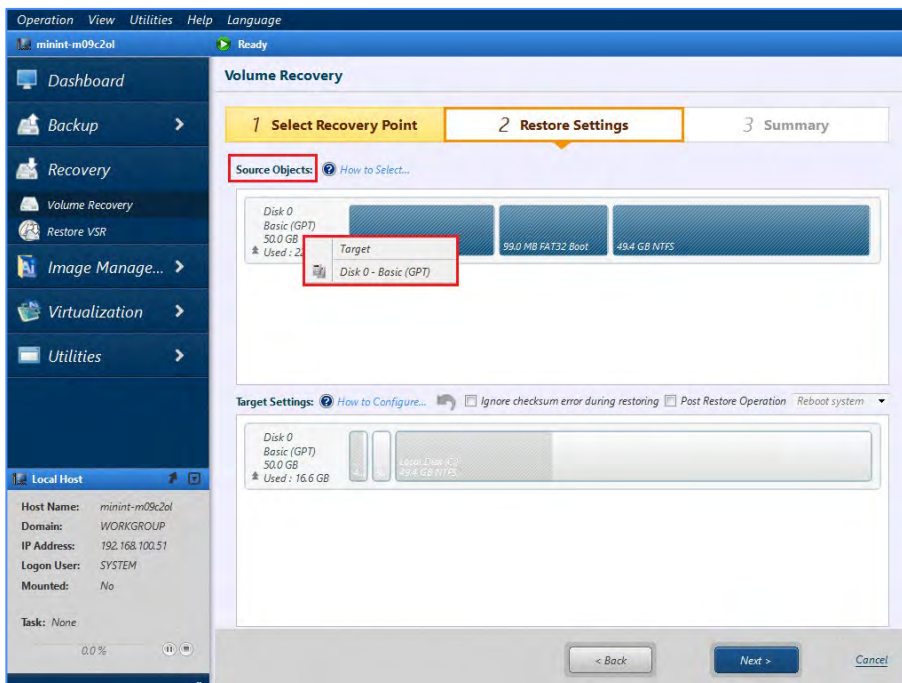


## Restore

7. Select the **[Source Computer]** and **[Recovery Point]**. Click **[Next]**.



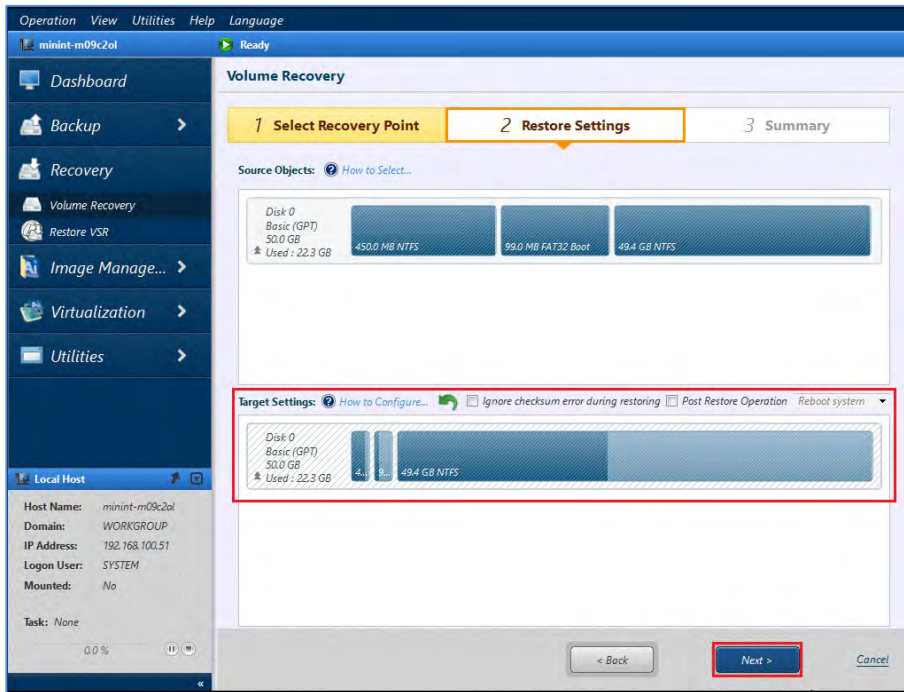
8. Right-click on the left part of disk map (around "Basic (GPT)") in **[Source Objects]**. From the context menu select "Disk 0 - Basic (GPT)" for **[Target]**.



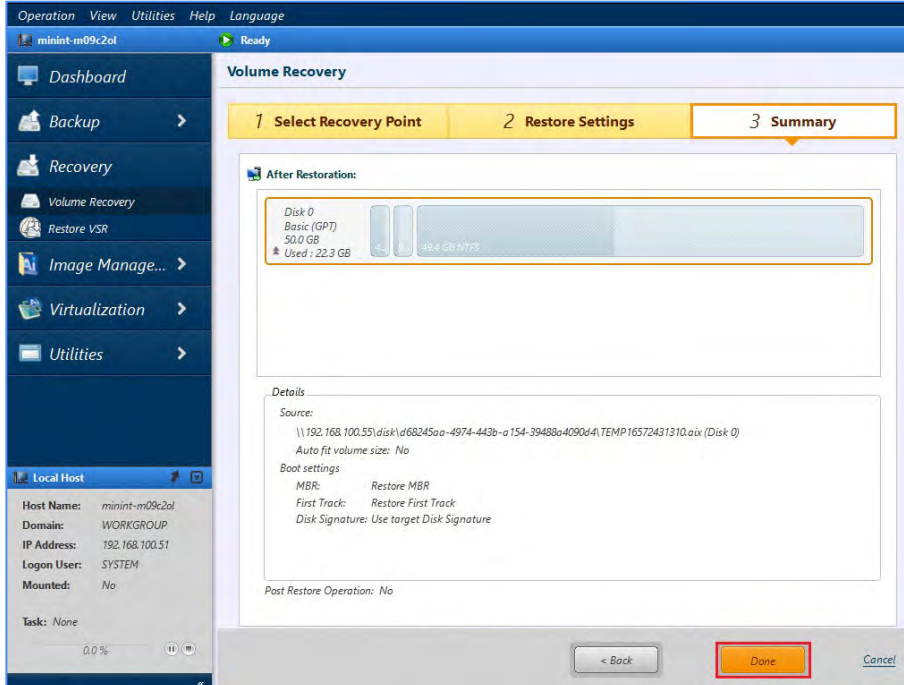


## Restore

- Review the restore target information displayed in **[Target Settings]** window and click **[Next]**.



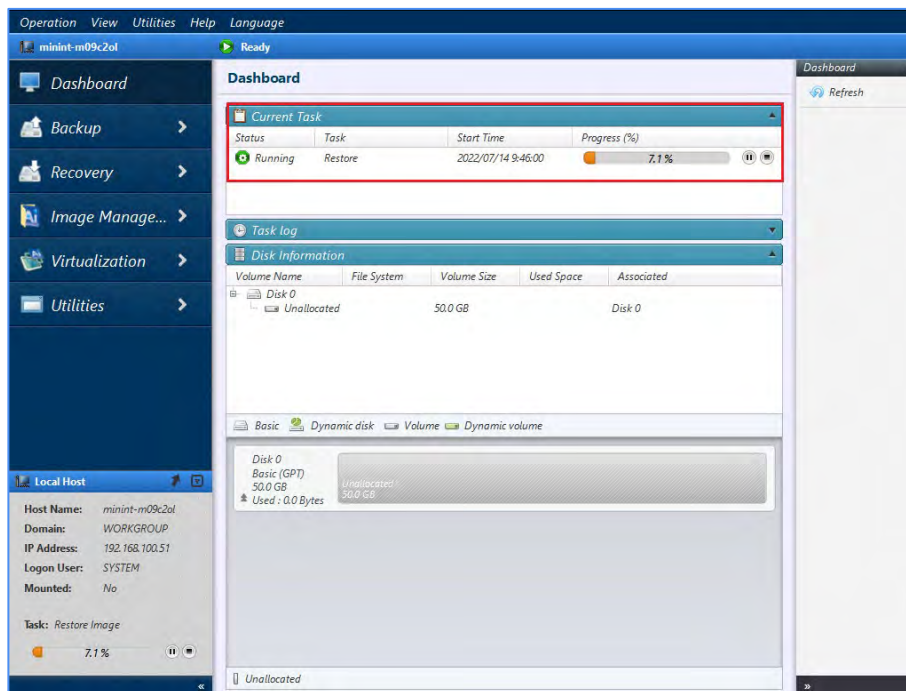
- A summary window is displayed. Click **[Done]**.



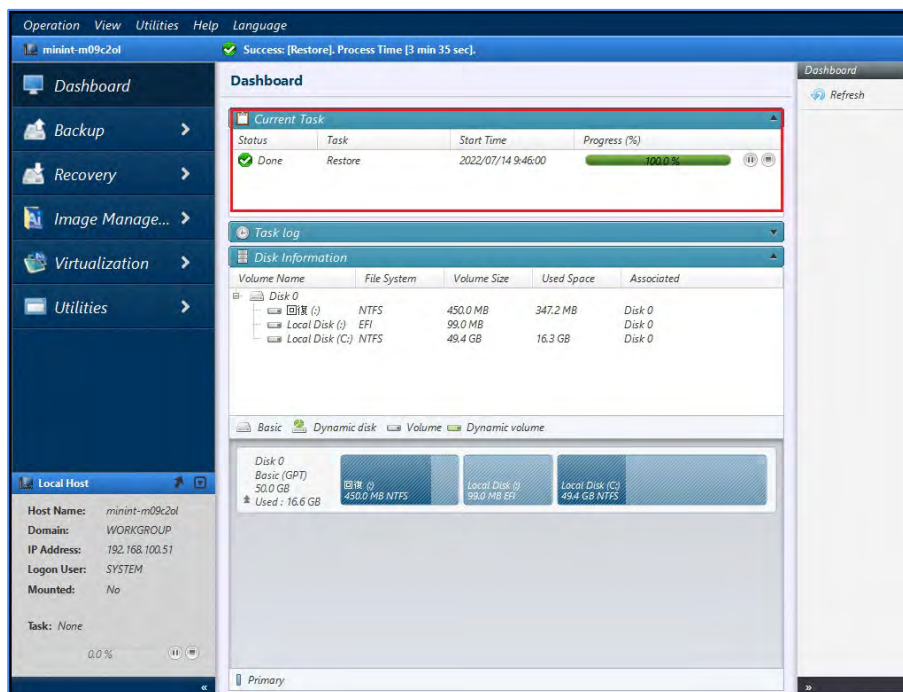


## Restore

11. When the recovery task starts, the progress is displayed.



12. When the Progress reaches “100%”, the recovery task has completed. Remove the boot media and click on **[Operation]** → **[End]** to shut down or reboot the machine.



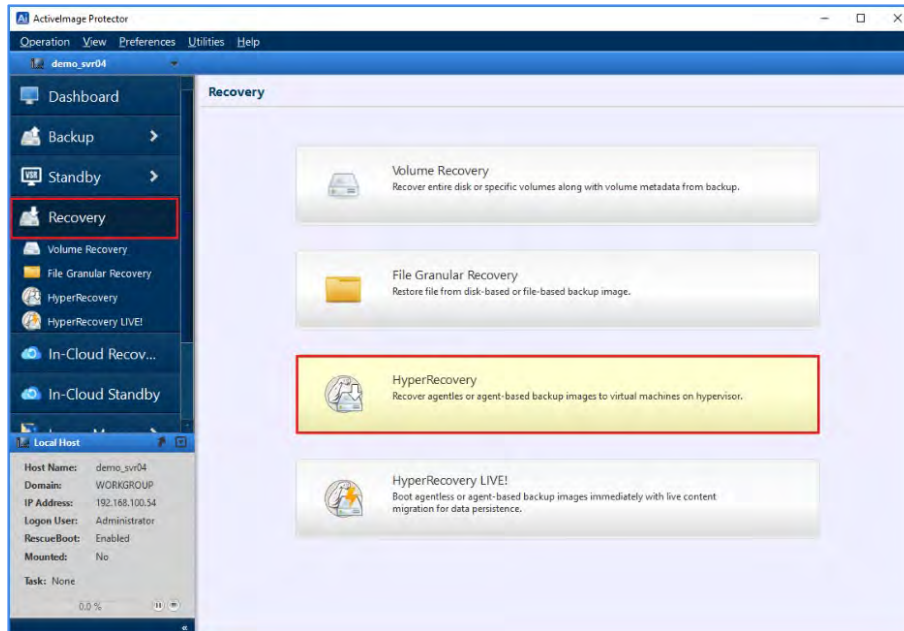
## Restore

### 6-4. Create a new virtual machine from backup image file (HyperRecovery)

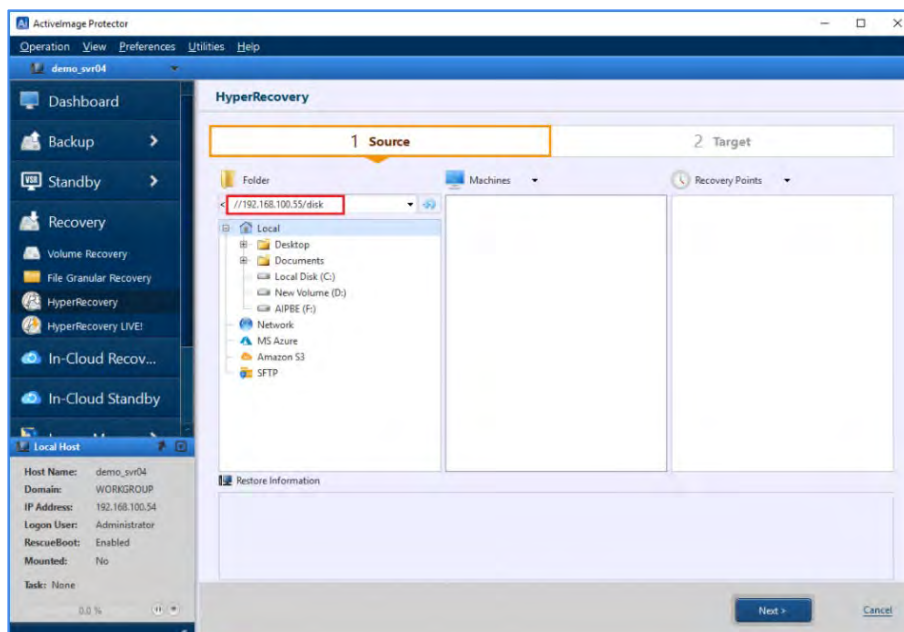
Using HyperRecovery you can restore a backup image file as a virtual machine or virtual disk.

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

1. Start ActiImage Protector. Go to Windows Start menu - **[Actiphy]** → **[ActiImage Protector]**.
2. Select **[Recovery]** - click **[HyperRecovery]**.

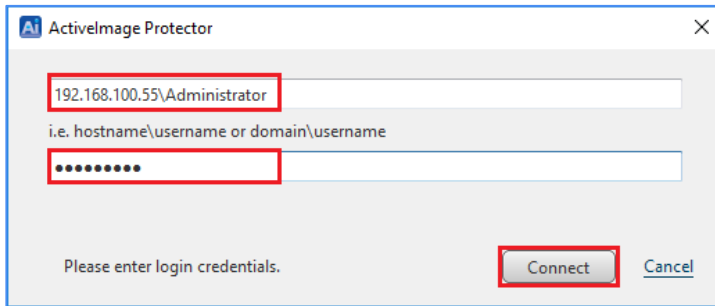


3. Select a folder contain backed image files. The following example show that the network shared folder "\\192.168.100.55\disk" is specified for the destination folder. Press Enter key.

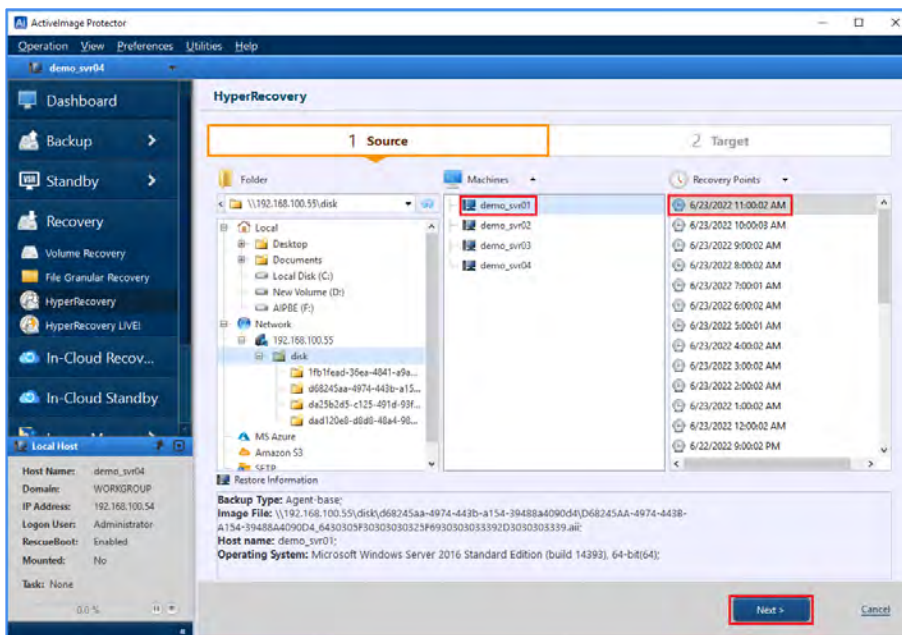


## Restore

4. Enter the required credentials to access the storage location. In this example we have entered "192.168.100.55\Administrator" for the **[User Name]** and the password. Click **[Connect]**.

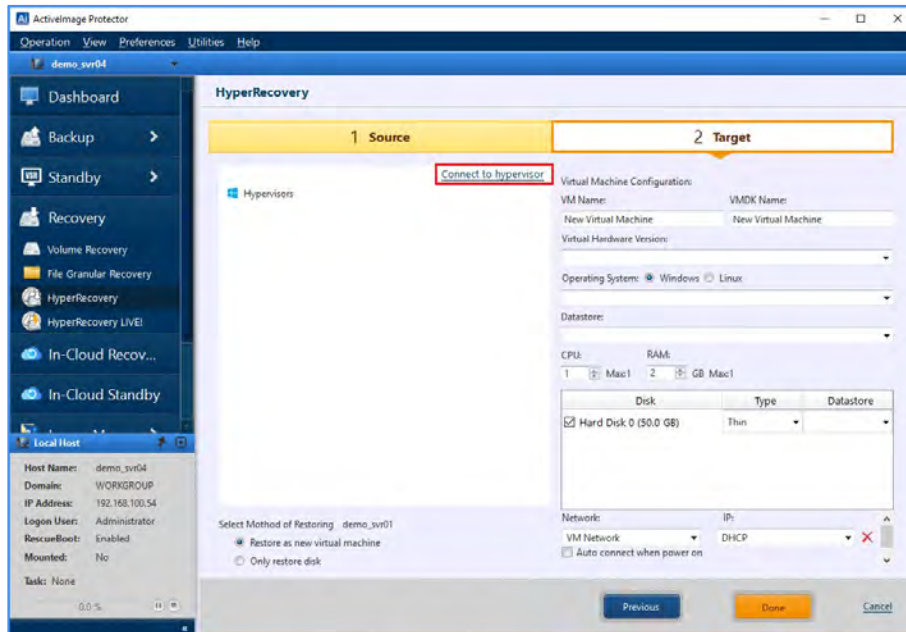


5. Select backup source **[Machine]** and **[Recovery Point]**. Click **[Next]**.

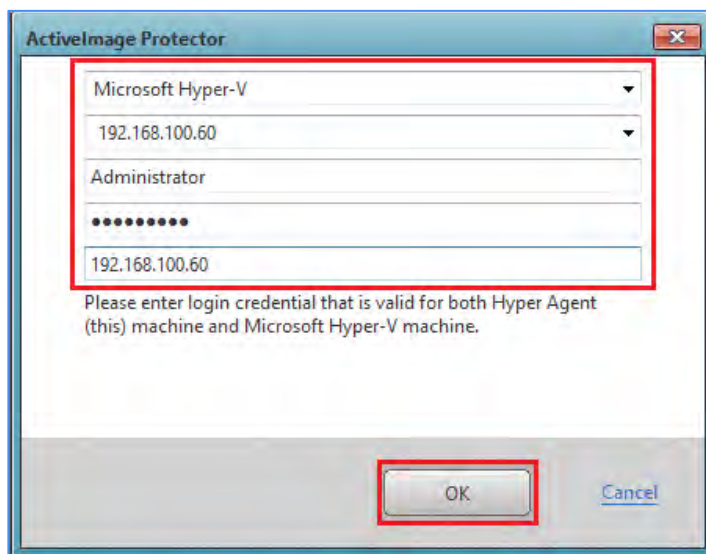


## Restore

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

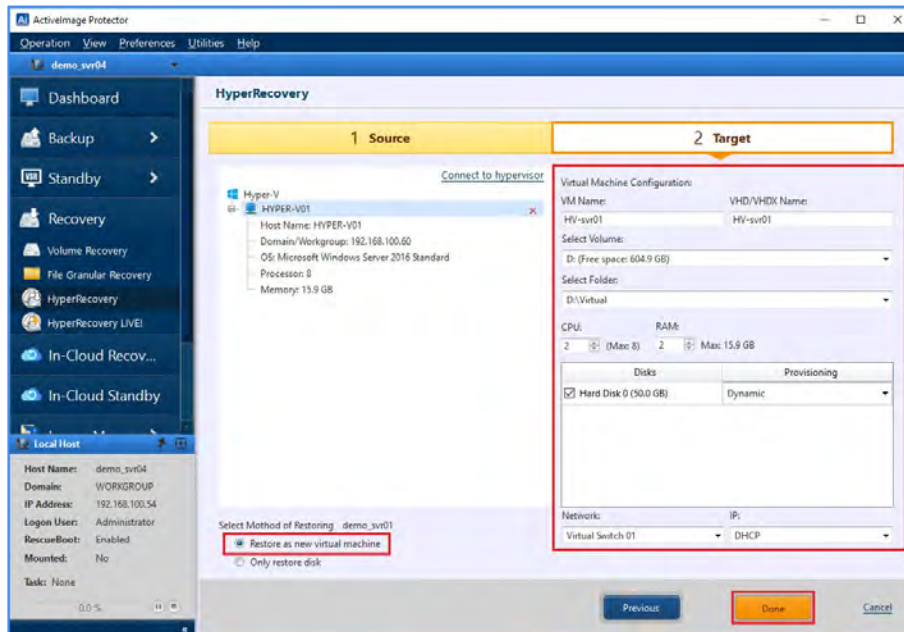


7. Supported hypervisors are Microsoft Hyper-V or VMware vSphere vCenter. In the following example we have selected **[Microsoft Hyper-V]** running on the local computer. Click **[OK]**

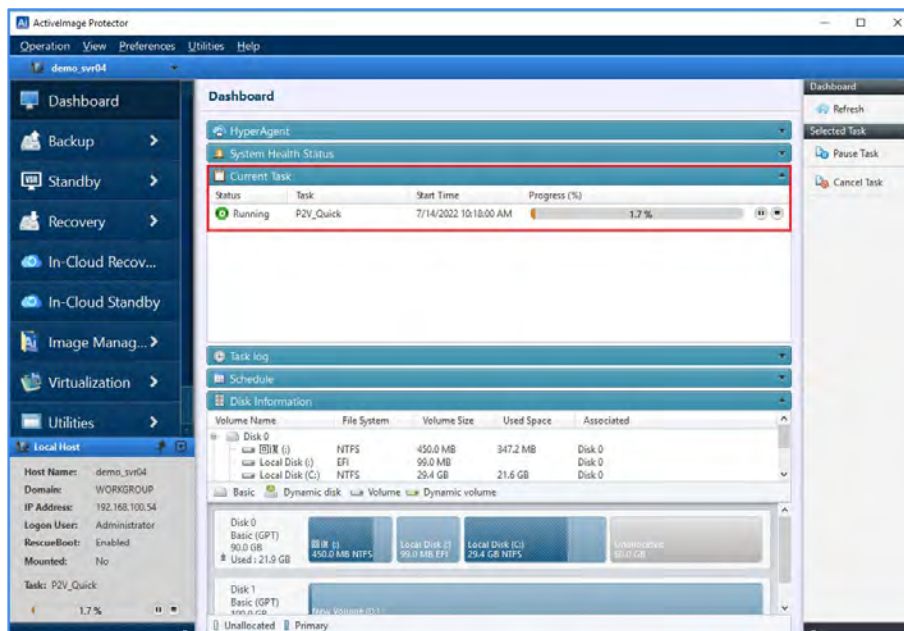


## Restore

- Configure the setting for the virtual machine. The following example shows settings configured for the new virtual machine. "hv-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]**. After configuring the settings, click **[Done]** to create the virtual machine.



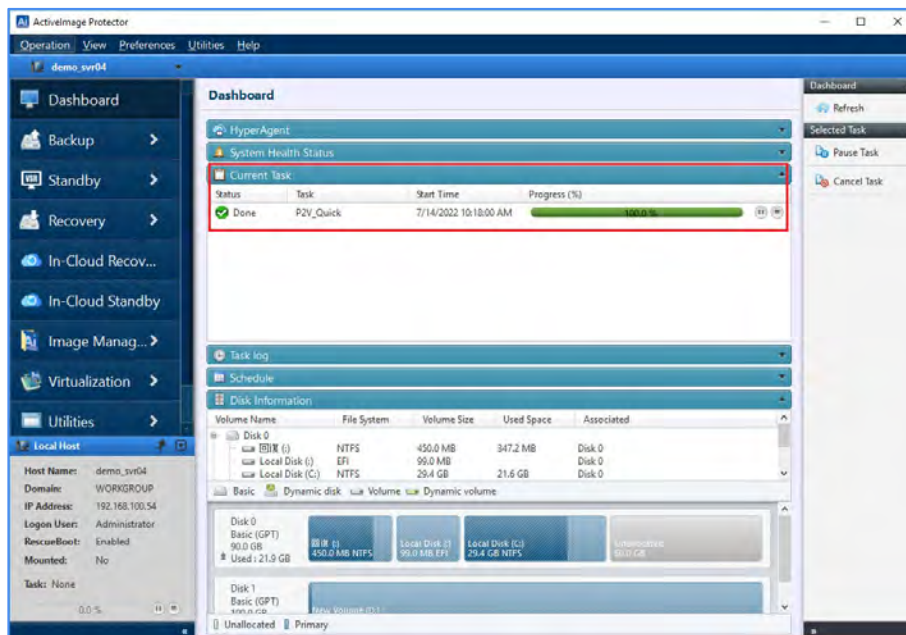
- The task for creating the virtual machine and the progress are displayed.





## Restore

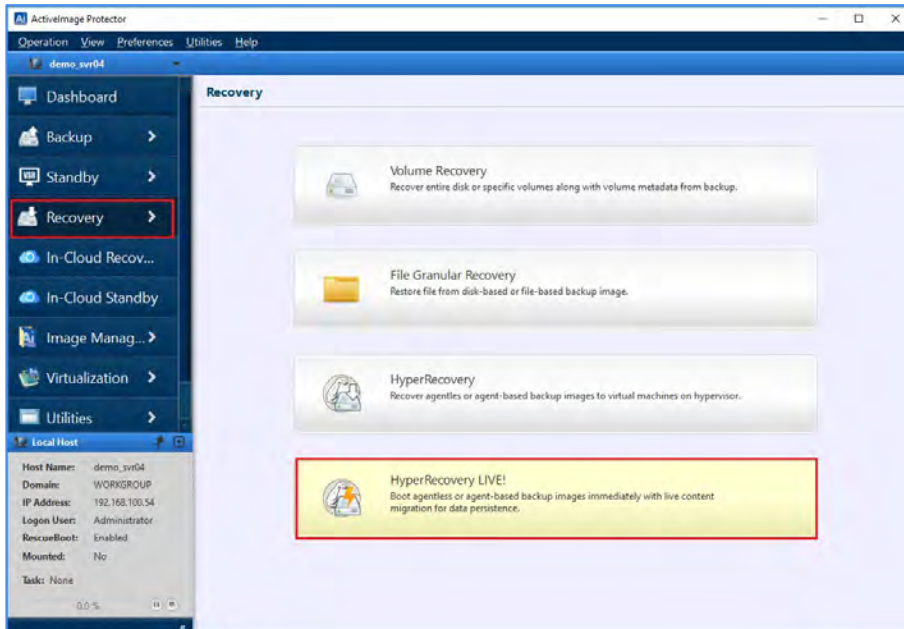
10. When the progress reaches 100%, the process is complete.



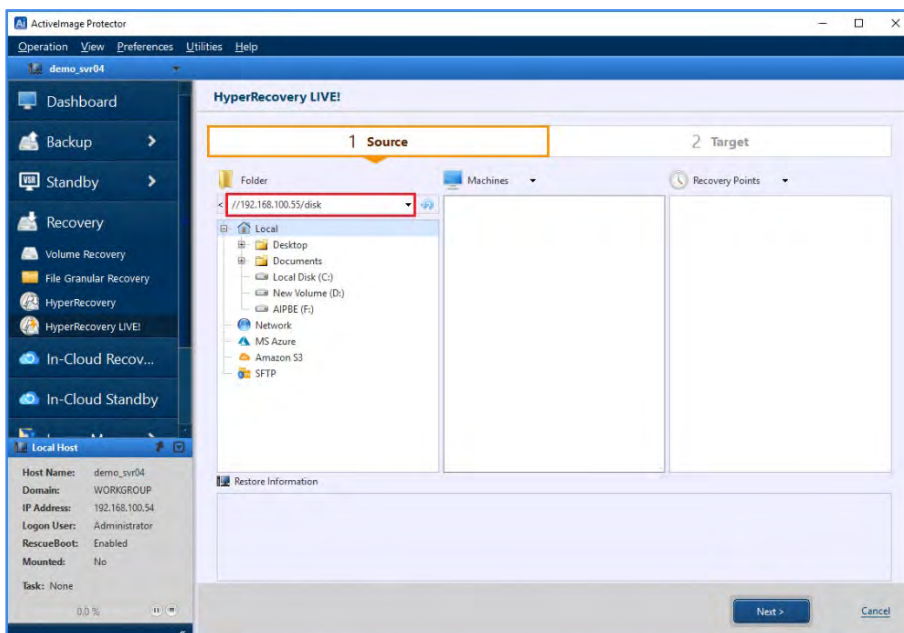
## 6-5. Zero Time Recovery (HyperRecovery LIVE!)

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

1. Go to **[Recovery]** → **[HyperRecovery LIVE!]**.

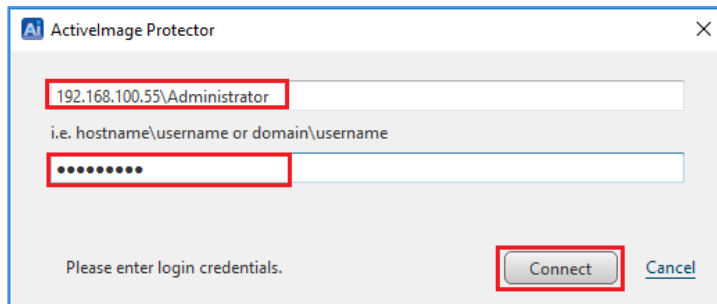


2. Select a storage location contain backup images. This example shows that “\\192.168.100.55\disk” is entered for a shared folder continuing backup images.. Press Enter key.

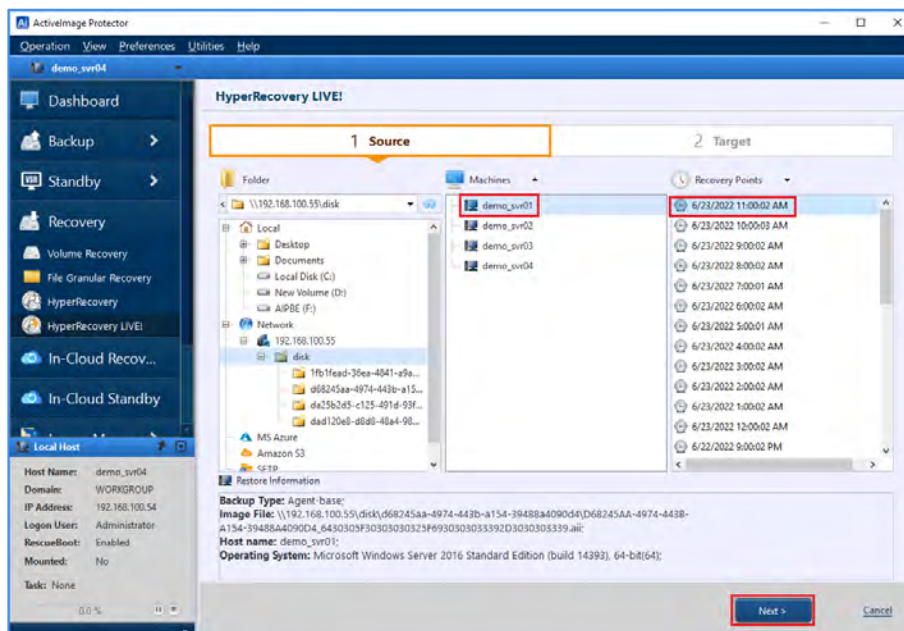


## Restore

3. Enter the required credentials to access the storage location. In this example we have entered "192.168.100.55\Administrator" for the **[User Name]** and the password. Click **[Connect]**.

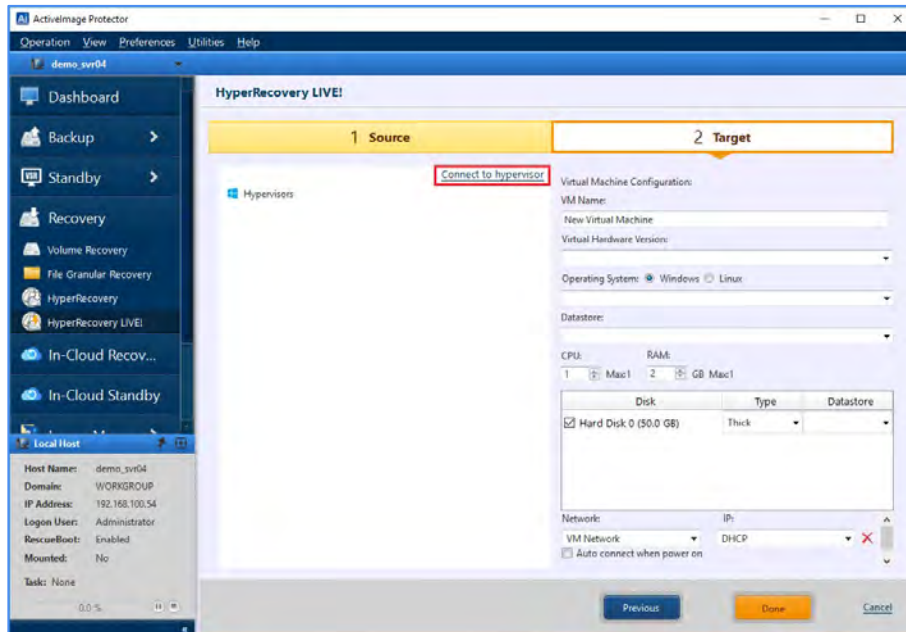


4. Select the source computer from **[Machine]** and the **[Recovery Point]**. Click **[Next]**.

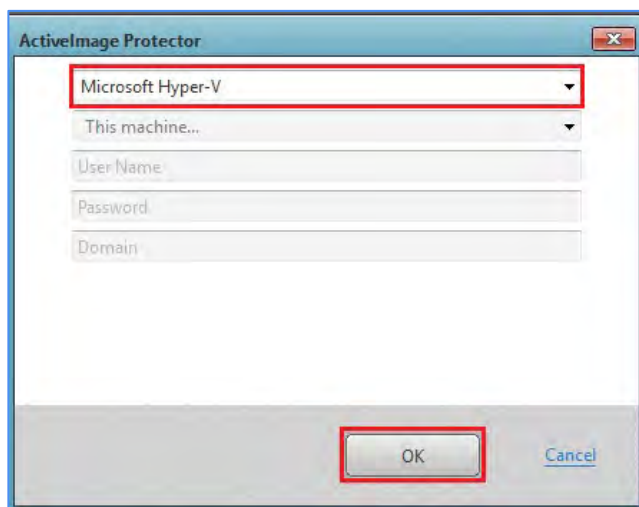


## Restore

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

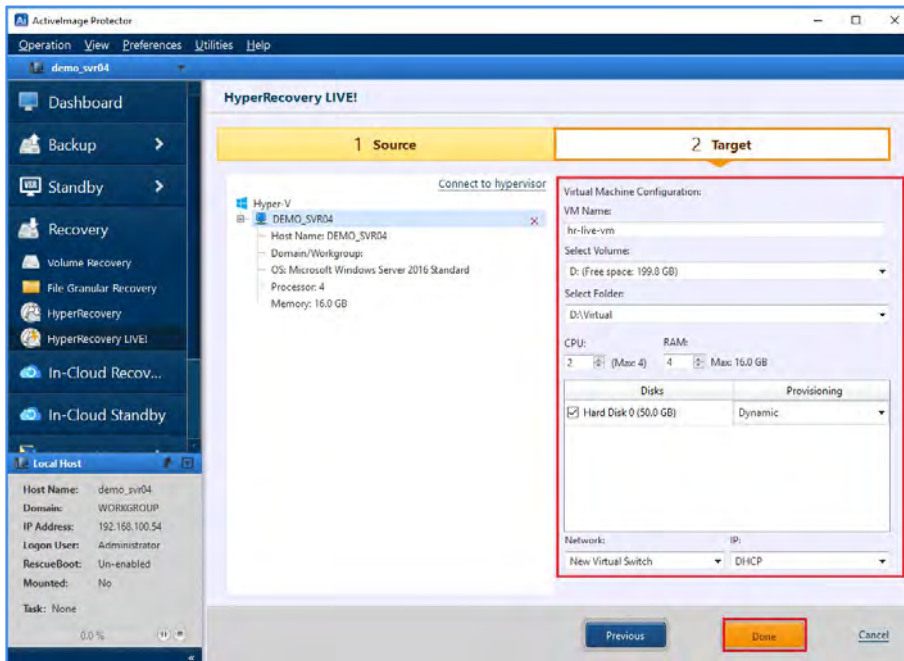


6. Select the type of the hypervisor. The supported hypervisors are Microsoft Hyper-V or VMware vSphere vCenter. In the following example we have selected **[Microsoft Hyper-V]** running on the local computer.

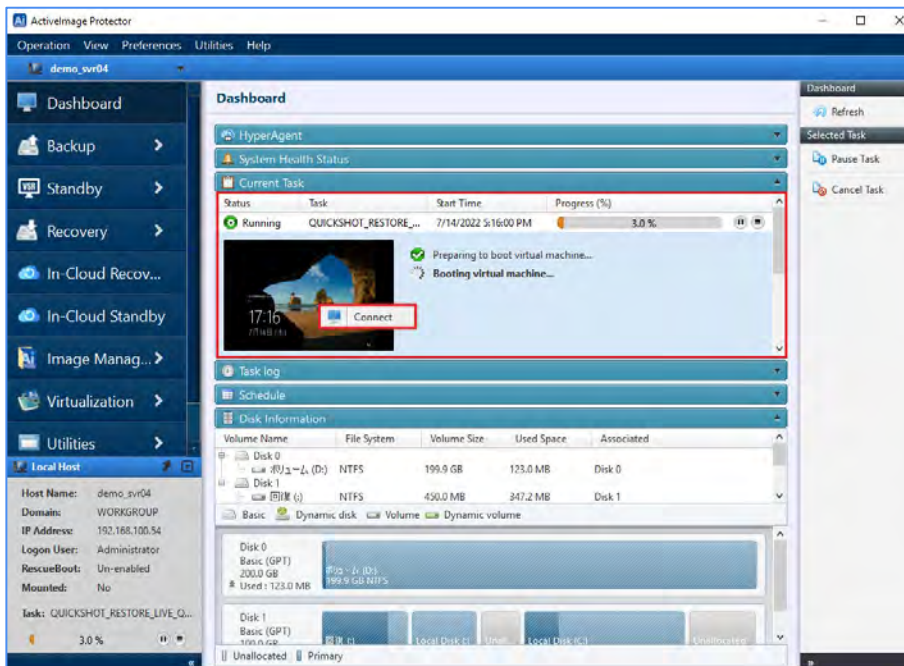


## Restore

- Configure the setting for the virtual machine. The following example shows settings configured for the new virtual machine. “hr-live-vm” is specified for **[VM name]**, “D:” drive for **[Volume:]** of datastore, “Virtual” for **[Folder]**, “2” for **[CPU:]**, “4GB” for **[RAM]** and “Dynamic” for **[Provisioning]**. After configuring the settings, click **[Done]** to create the virtual machine.



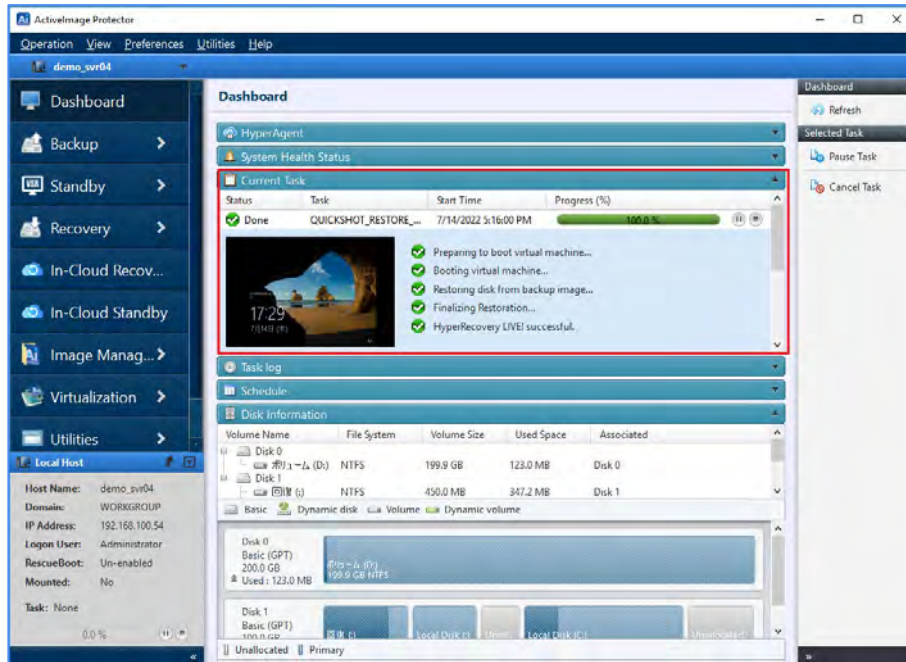
- When the task starts, the virtual machine will boot. Right-click on the thumbnail and select **[Connect]**. You can operate the virtual machine by using remote console. In background, the backup is restored to the virtual machine.



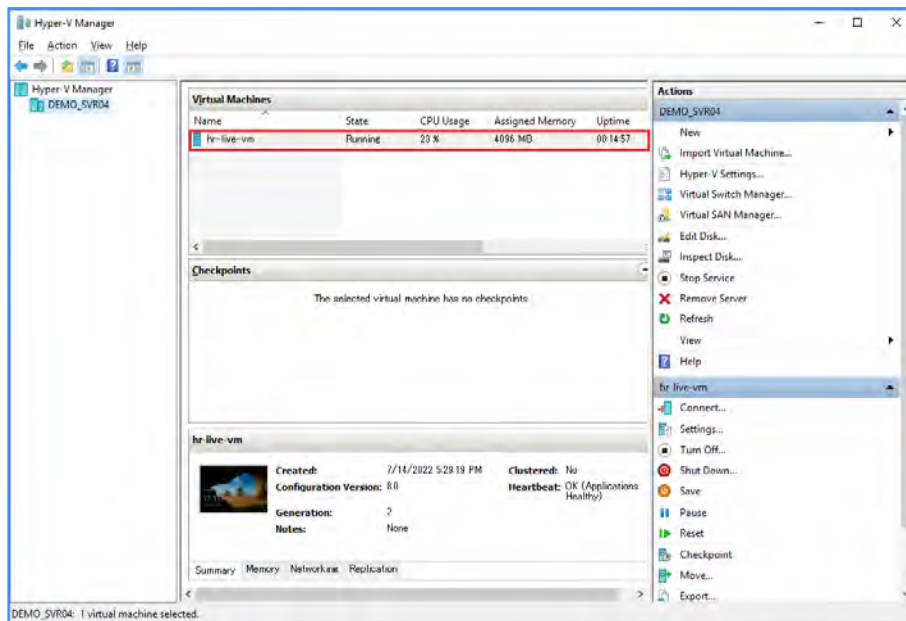


## Restore

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



10. You can monitor the virtual machine using the Hyper-v Manager consol. In the dialogue below we can the virtual machine “hr-live-vm“ was created and is running.

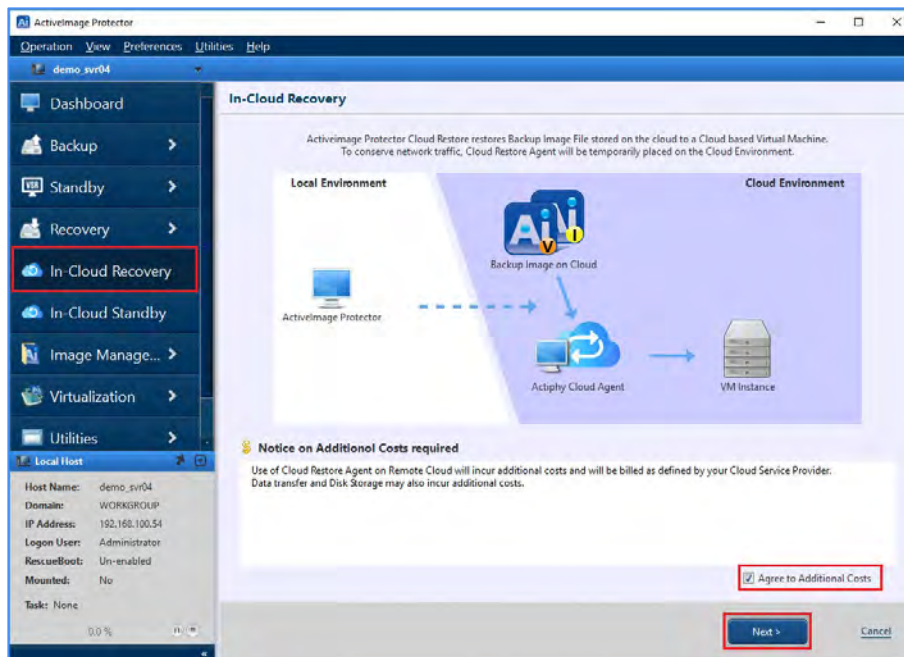


## 6-6. Cloud Recovery (In-Cloud Recovery)

In-Cloud Recovery restores the entire system to virtual machine on Amazon Web Service (AWS) or Microsoft Azure cloud environment. The recovery operation is executed by running “Actiphy Cloud agent (boot environment)” deployed on the respective cloud regions, therefore, no complicated operation of cloud management console or command line is required.

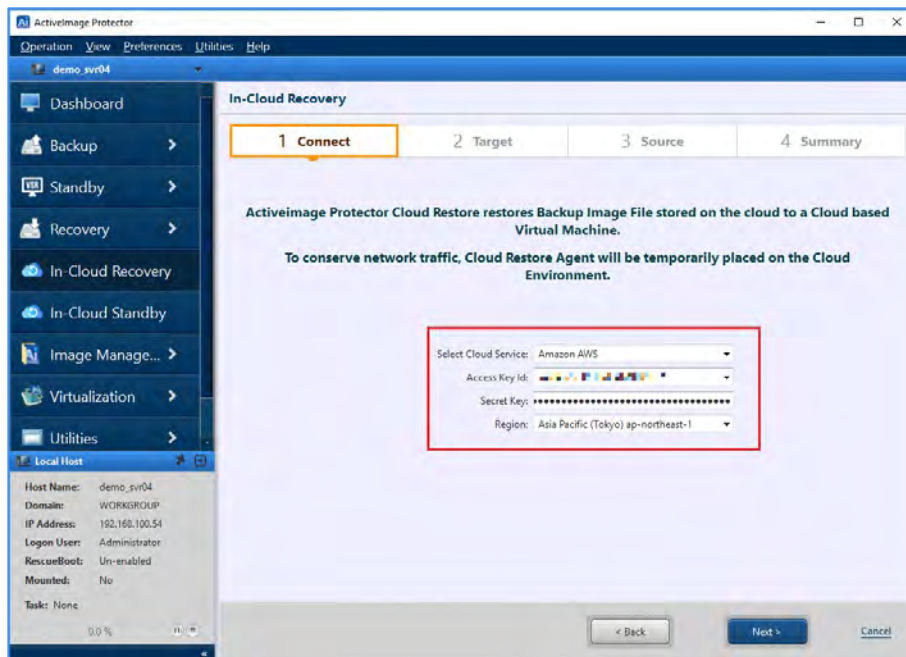
The following are the operating procedures how to restore the system from a backup file to “AWS EC2”.

1. Click **[In-Cloud Recovery]** in the left menu. Additional costs for the use of the cloud services during the execution of this process and operation of the restored virtual machine may be incurred by cloud service provider. To proceed with further operation, please check the checkbox for **[Agree to Additional Cost]** and click **[Next]**.

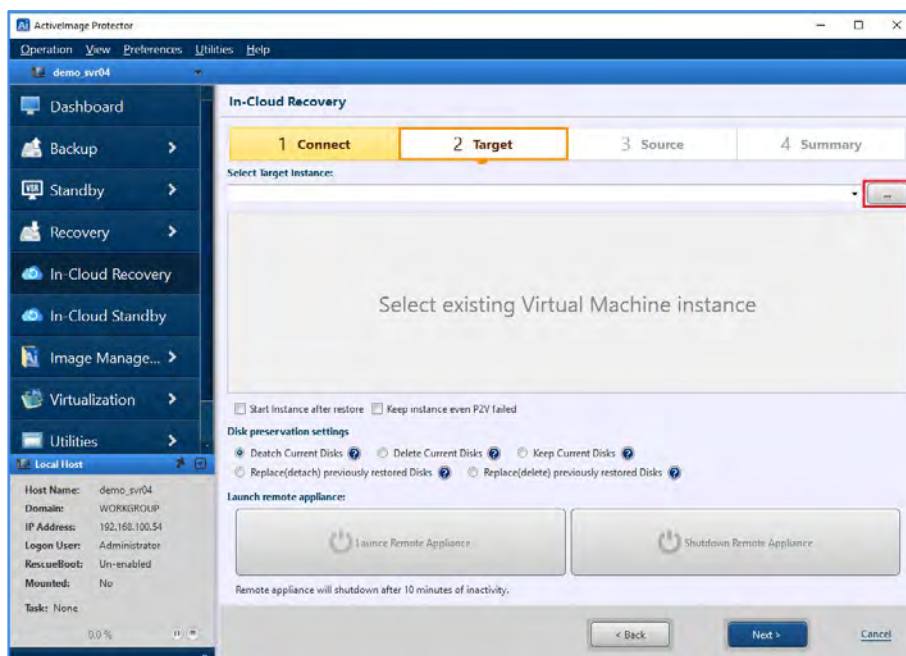


## Restore

2. Select the cloud service you want to use and enter the credential information. This example shows that **[Amazon AWS]** is selected for the cloud service, the required **[Access Key ID]** and **[Secret Key]** are entered for AWS. Select **[Region]** and click **[Next]**.

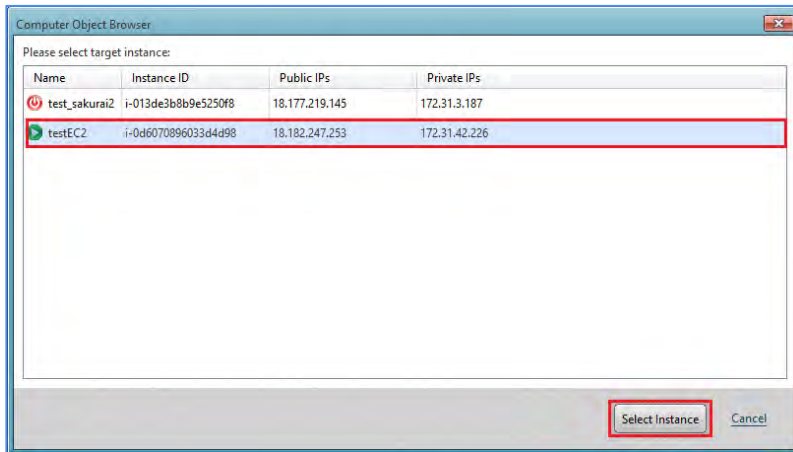


3. Click **[...]** and select the instance for a restore target.

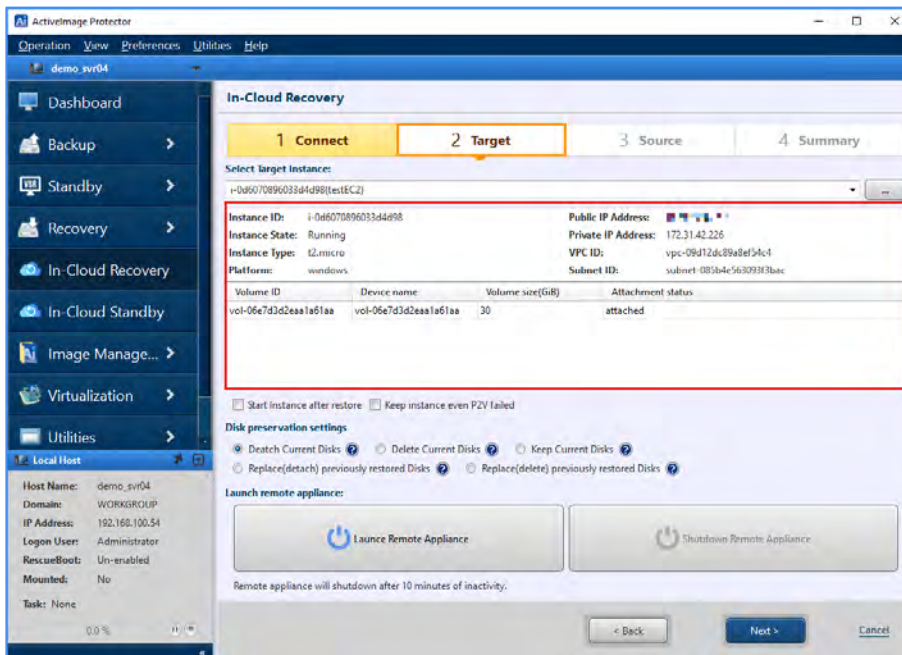


## Restore

4. Select an instance and click **[Select Instance]**. This example shows that “testEC2” is selected.

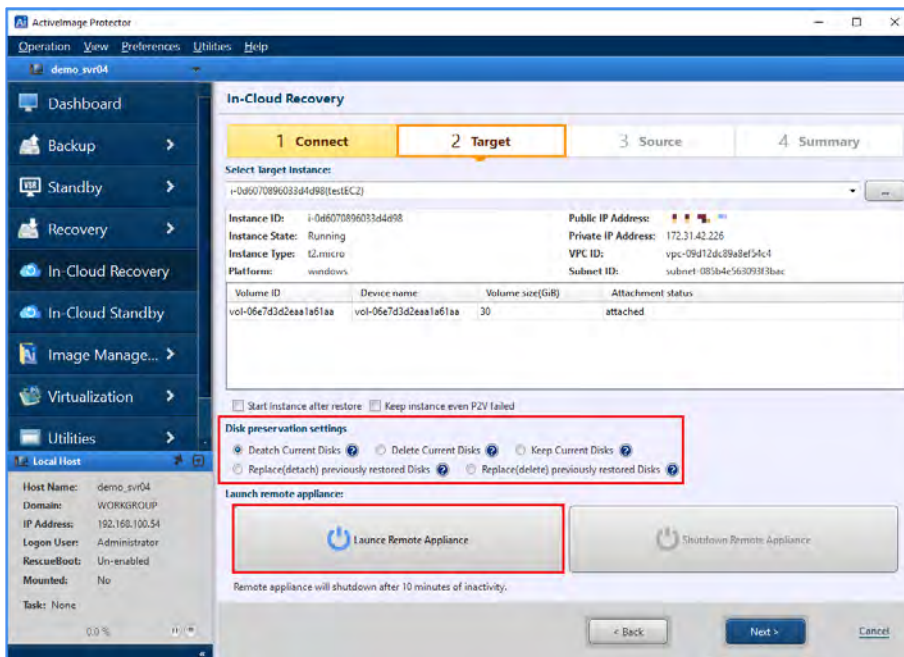


5. The information of the selected instance for the restore target is displayed.



## Restore

6. Select an option for **[Disk Preservation Settings]** for the restored virtual disk. This example shows that **[Detach Current Disks]** is selected. Click **[Launch Remote Appliance]** and ActiPhy Cloud Agent (boot environment) will launch.



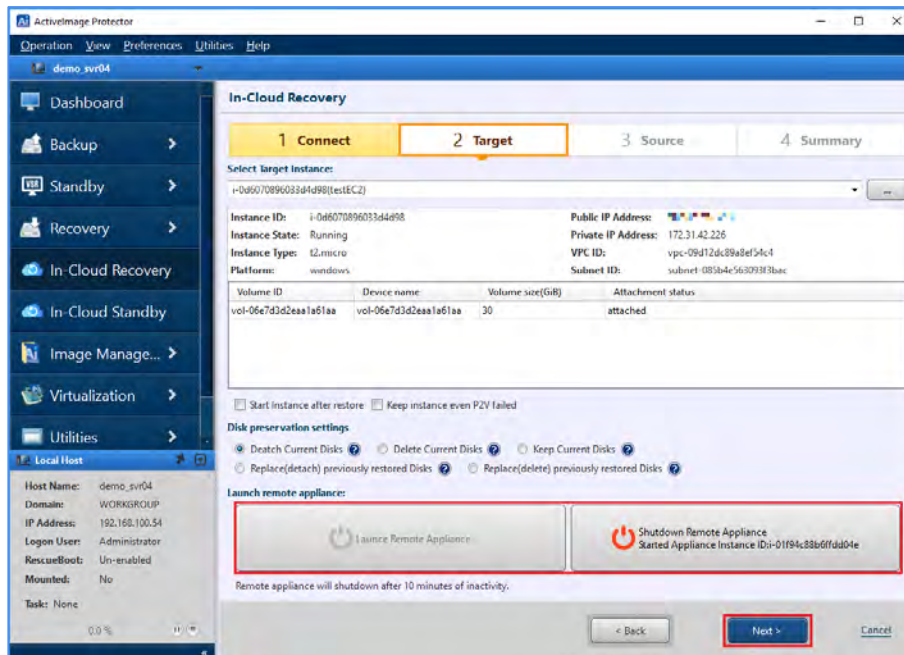
### Disk preservation settings:

- **Detach Current disks:** Detach the disk connected to the instance and connect the restored disk to the instance. The detached disk remains instead of being deleted.
- **Delete Current disks:** Detach and delete the disk connected to the instance and connect the restored disk to the instance.
- **Keep Current disks:** The disk connected to the instance is not detached, the restored disk is attached as another disk to the instance.
- **Replace (Detach) previously restored disks:** Detach the restored disk connected to the instance and connect the newly restored disk to the instance. The detached disk remains and is not deleted. Disks that have not been restored using this product are not detached from the instance.
- **Replace (Delete) previously restored disks:** Detach and delete the restored disk connected to the instance and connect the newly restored disk to the instance. Disks that have not been restored using this product are not detached from the instance.

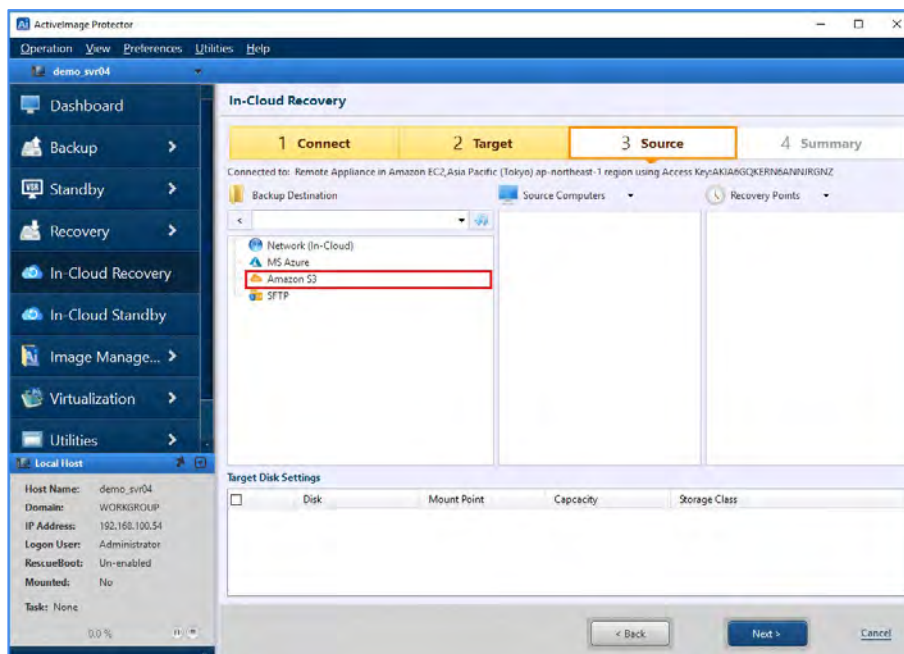


## Restore

- When the **[Launch Remote Appliance]** becomes disabled and the **[Shut-down Remote Appliance]** button becomes active, the Actiphy Cloud Agent (boot environment) starting process has completed. Click **[Next]**.

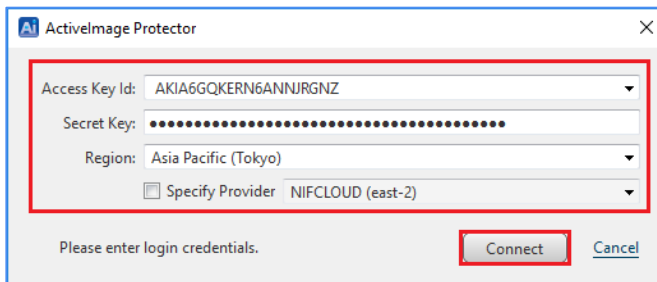


- Please specify a Backup Destination where backup files are located. This example shows that "Amazon S3" is selected.

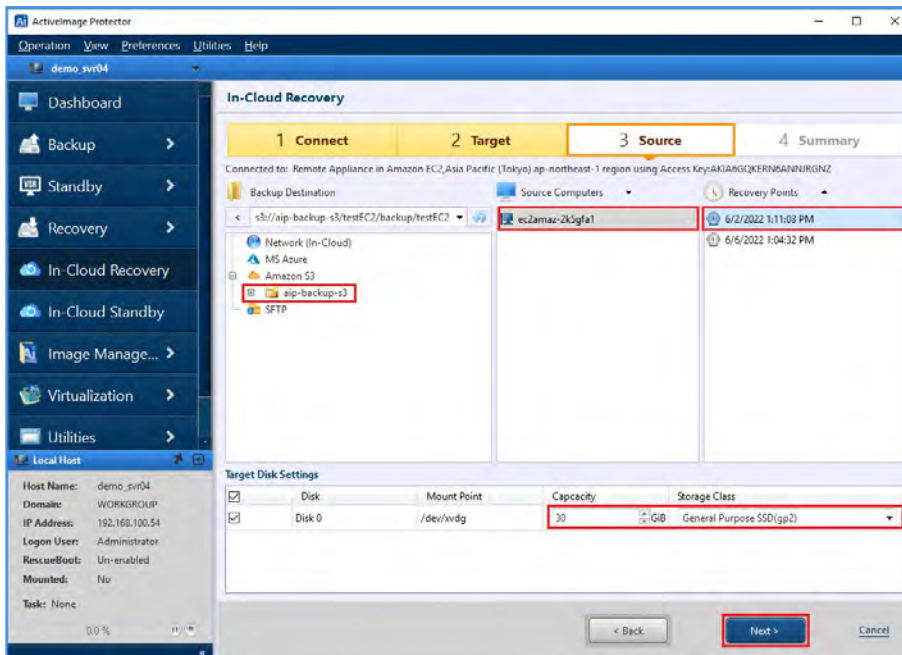


## Restore

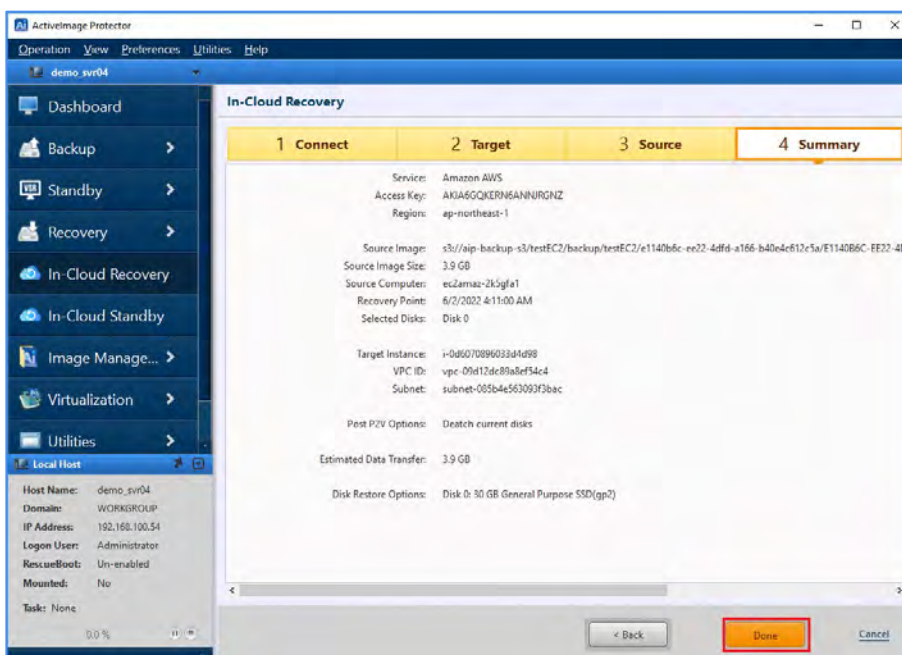
- Enter the **[Access Key]**, **[Secret Key]** for AWS account and select **[Region]**. Click **[Connect]**.



- Select **[Backup Destination]** folder, **[Source Computer]** and **[Recovery Point]**. Click **[Next]**. You can also configure the settings for **[Target Disk Settings]**.

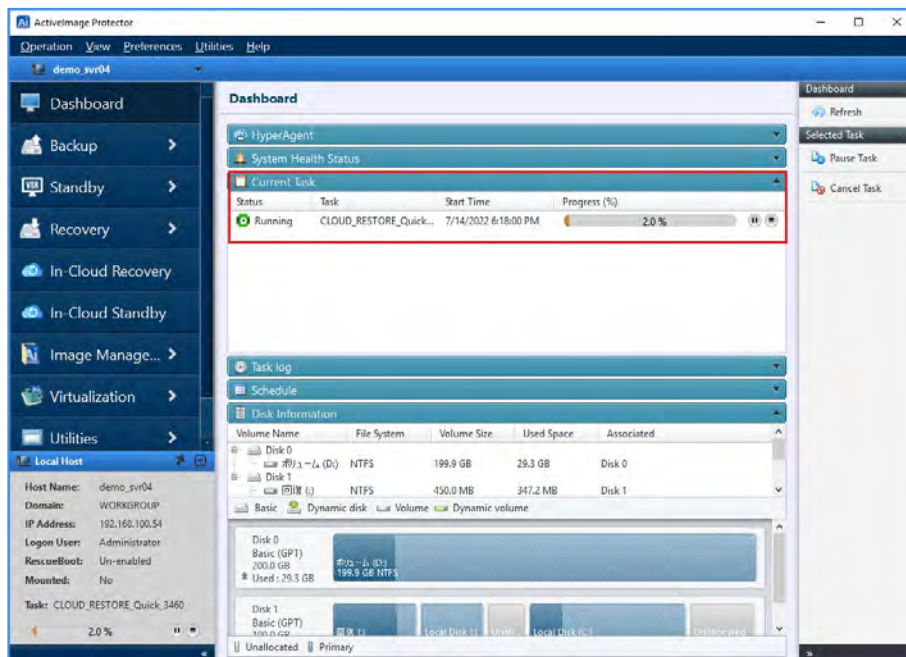


- Review the configured settings and click **[Next]**. The In-Cloud Recovery task is started.

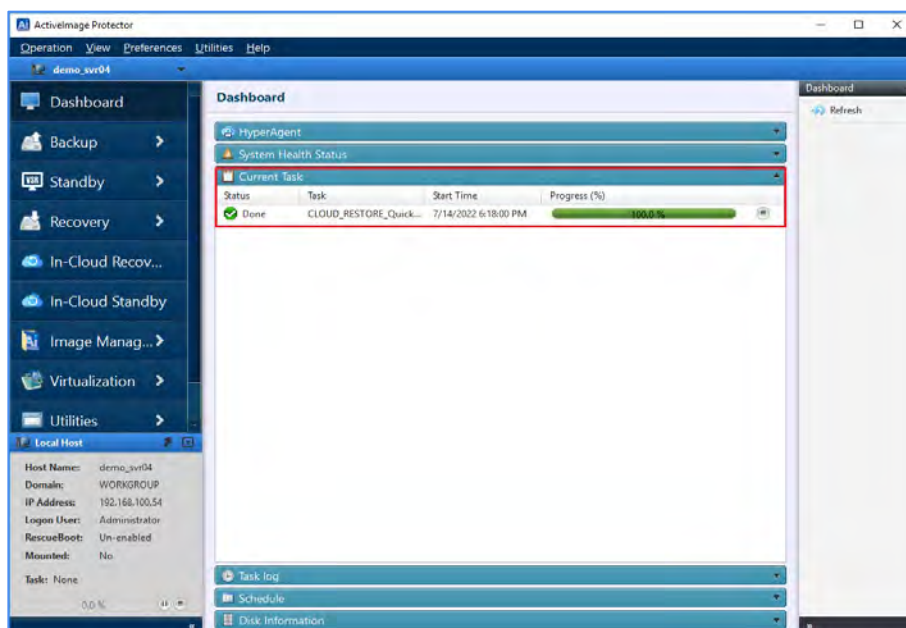


## Restore

12. The progress of the recovery process is displayed.

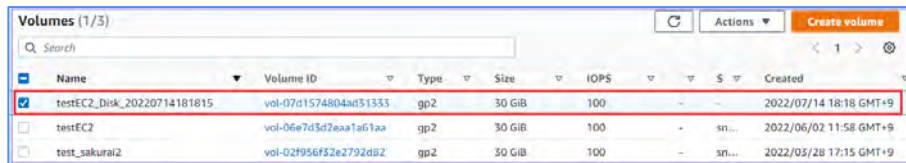


13. When the progress reaches 100%, process is complete.



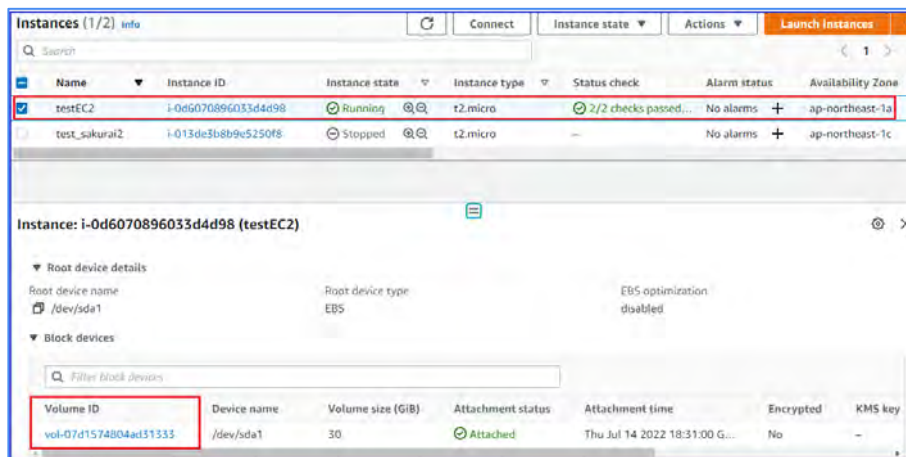
## Restore

14. In the AWS Management Console you can confirm the disk that was connected to the instance is detached and the restored disk is connected.



Name	Volume ID	Type	Size	IOPS	\$	Created
<input checked="" type="checkbox"/> testEC2_Disk_20220714181815	vol-07d1574804ad31333	gp2	30 GiB	100	-	2022/07/14 18:18 GMT+9
<input type="checkbox"/> testEC2	vol-06e7d3d2eaa1a61aa	gp2	30 GiB	100	sn...	2022/06/02 11:58 GMT+9
<input type="checkbox"/> test_sakurai2	vol-02f956f52e2792d82	gp2	30 GiB	100	sn...	2022/03/28 17:15 GMT+9

The created volume is connected as a root device of the instance.



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/> testEC2	i-0d6070896033d4d98	Running	t2.micro	2/2 checks passed...	No alarms	ap-northeast-1a
<input type="checkbox"/> test_sakurai2	i-013de3b8b9e5250f8	Stopped	t2.micro	-	No alarms	ap-northeast-1c

Root device details	
Root device name /dev/sda1	Root device type EBS

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key
vol-07d1574804ad31333	/dev/sda1	30	Attached	Thu Jul 14 2022 18:31:00 G...	No	-

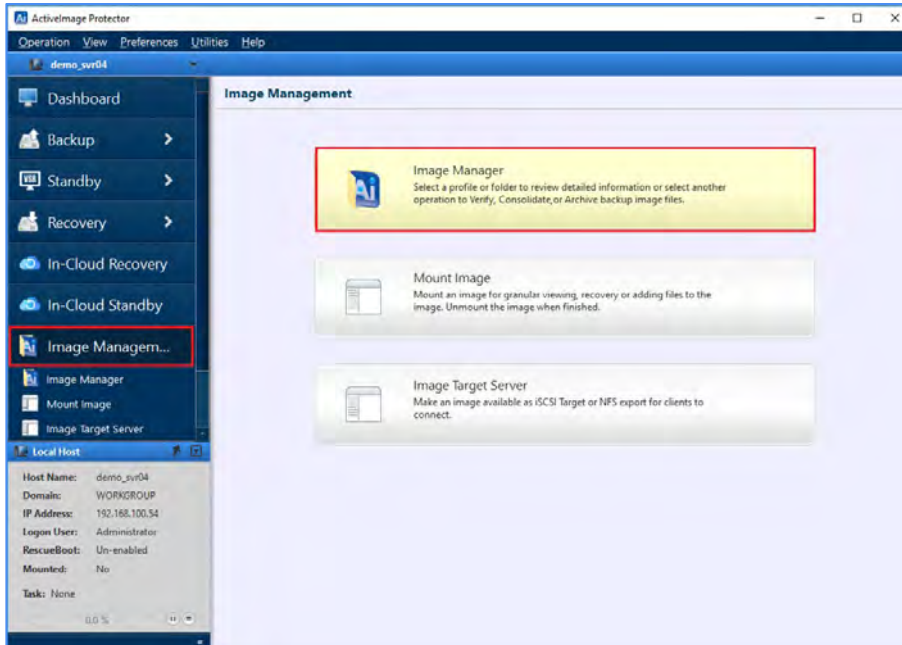


## 7. Image Management – Image Manager

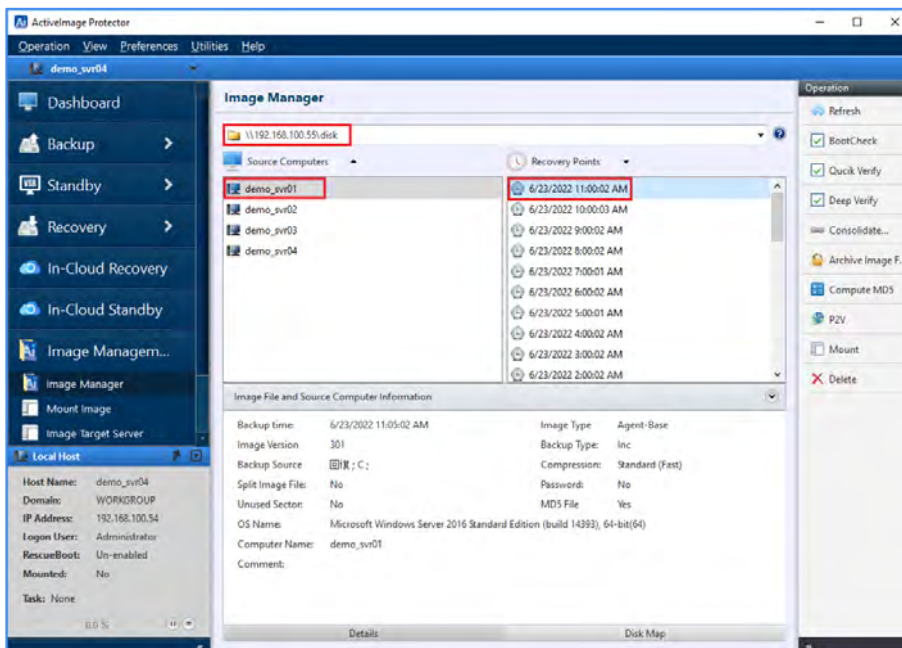
These tools are provided to enable you to manage various operations relating to image files.

### 7-1. 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..

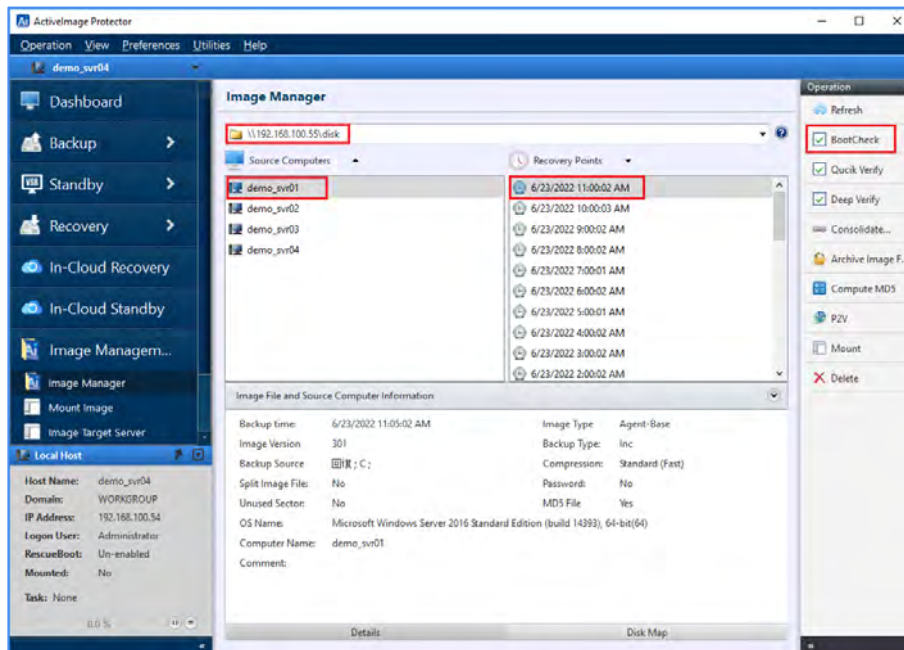




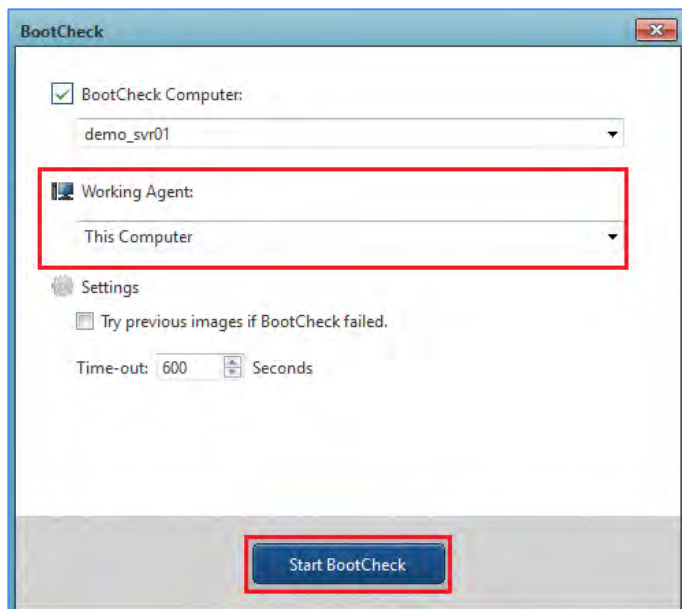
## 7-2. Check for bootability of backups (BootCheck)

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

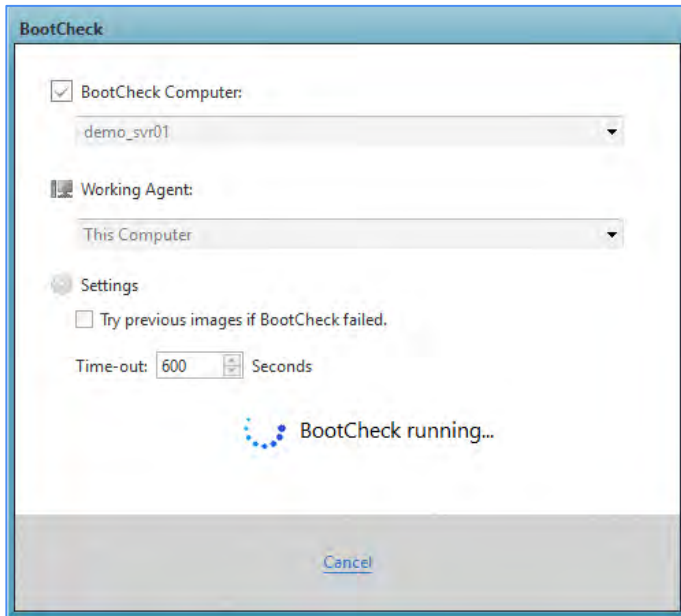
1. Select **[Source Computer]** and **[Recovery Point]** and click **[BootCheck]** in the right pane.



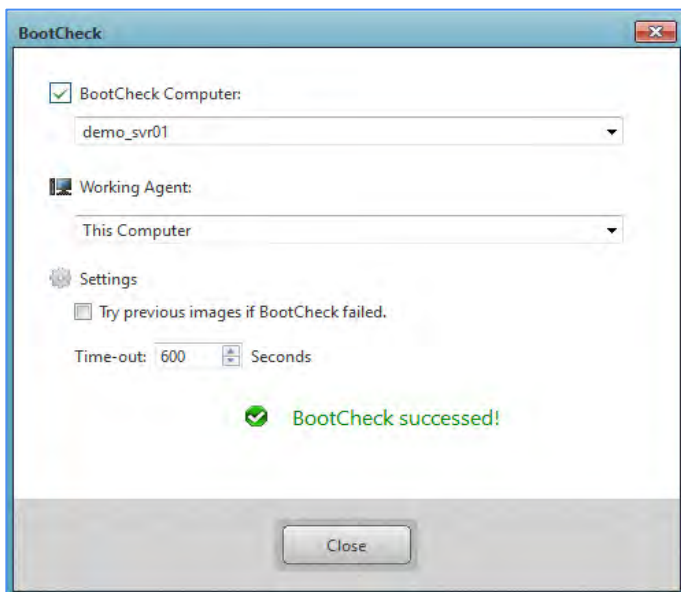
2. In this example, “this computer” (local Hyper-V) is selected as the **[Working Agent:]** (hypervisor for running BootCheck). Click **[Start BootCheck]**.



3. BootCheck is executed for the specified backup.



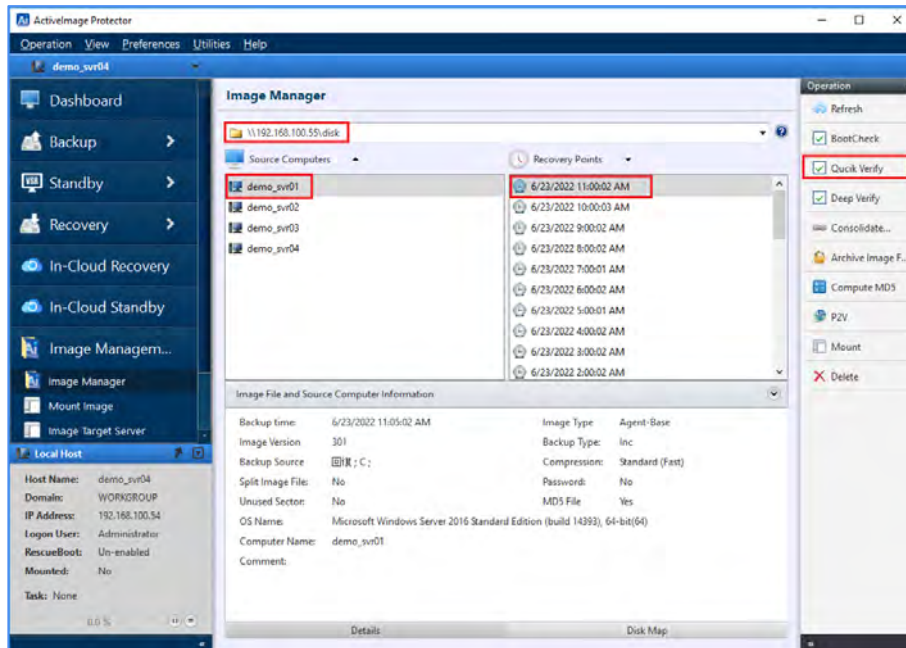
4. Upon completion of BootCheck process, the following window is displayed. BootCheck can be executed at anytime, for example, right before running a backup task.



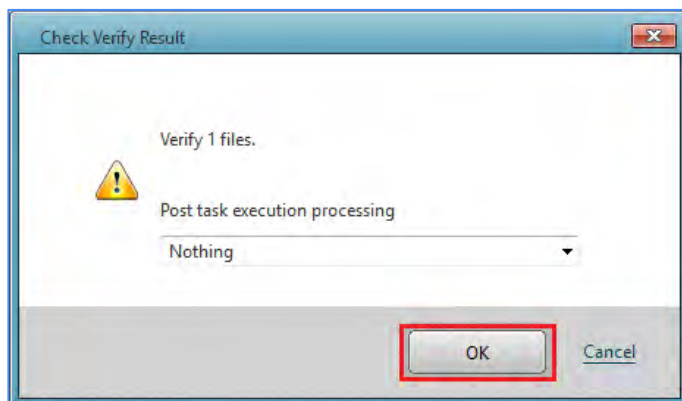
### 7-3. Quick Verify

Quick Verify ensures that the backup file has no been corrupted since the backup was created.

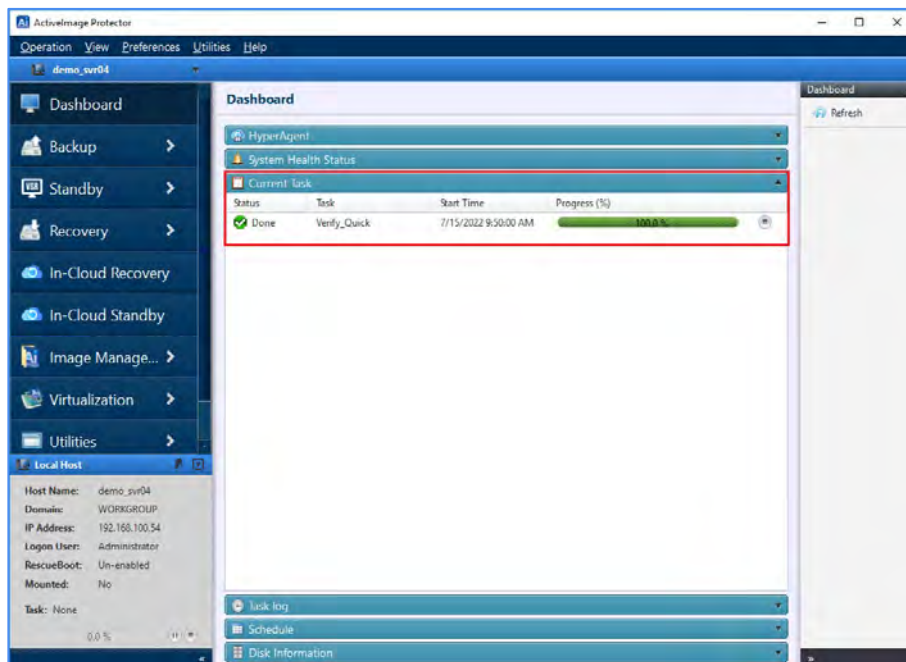
1. Select **[Source Computer]** and **[Recovery Point]** and click **[Quick Verify]** in the right pane.



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



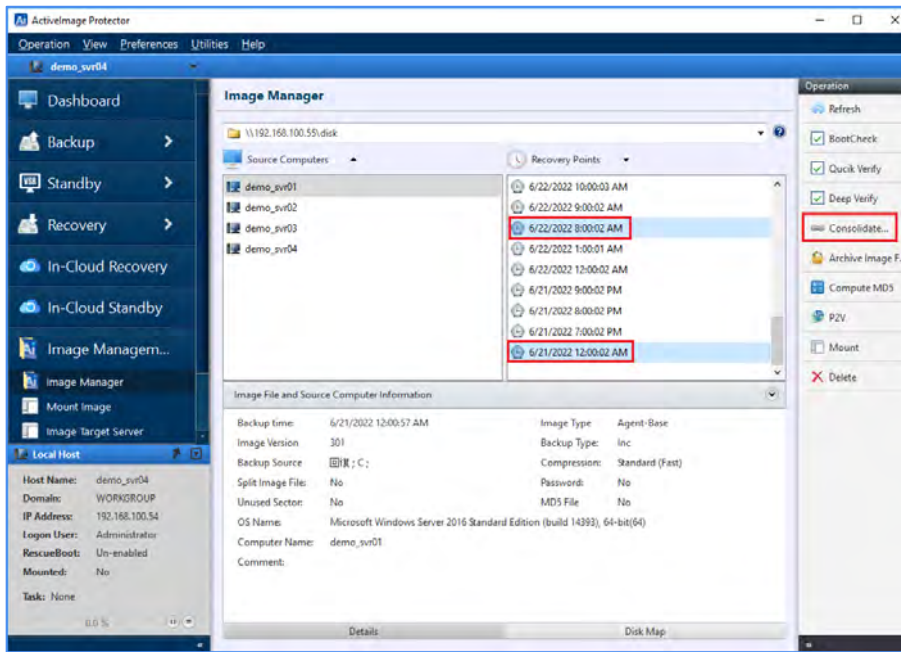
- After the Verify completes the following window is displayed.



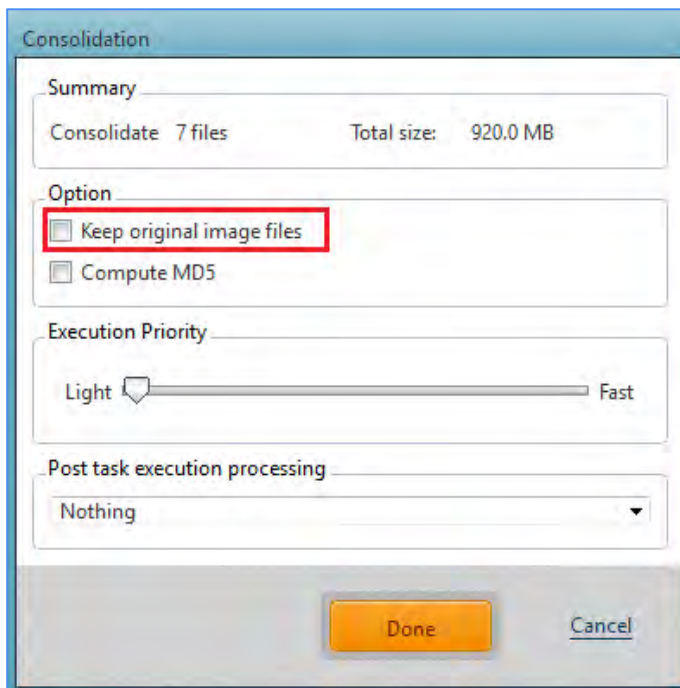
## 7-4. Consolidation

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.

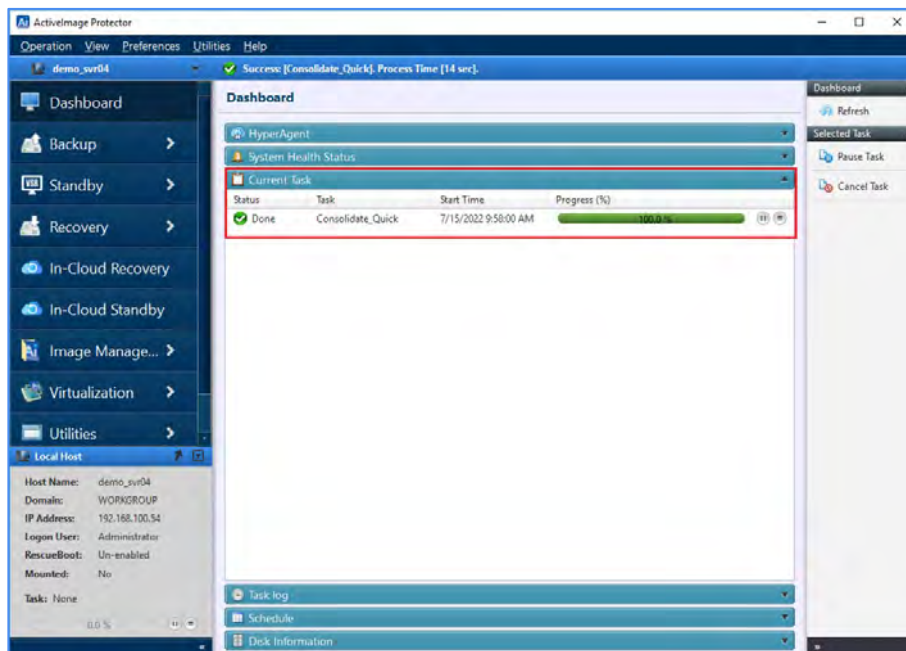


2. Configure the Option settings. To preserve the original files, tick the checkbox for **[Keep original image files]**.





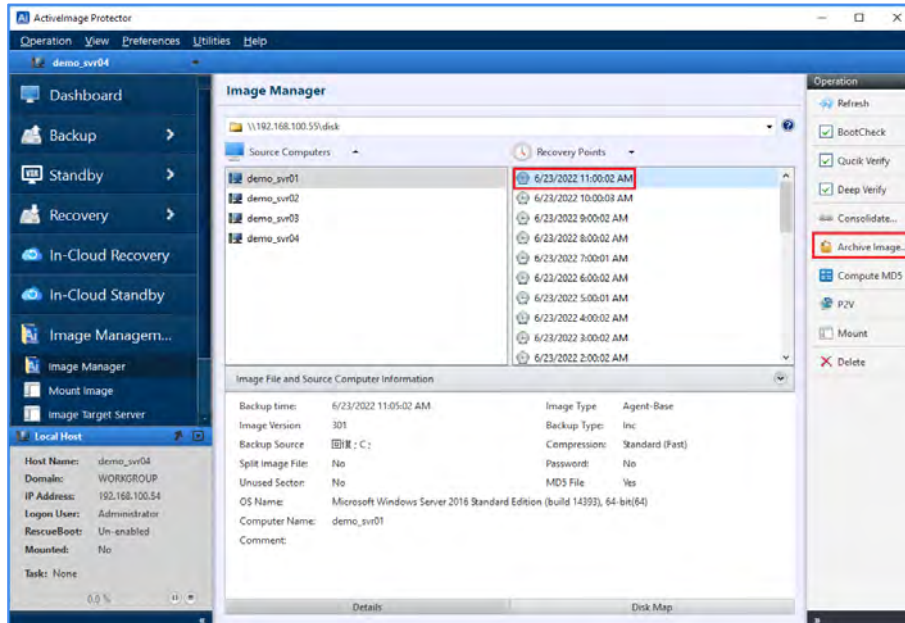
3. After the consolidation process completes, the following window is displayed.



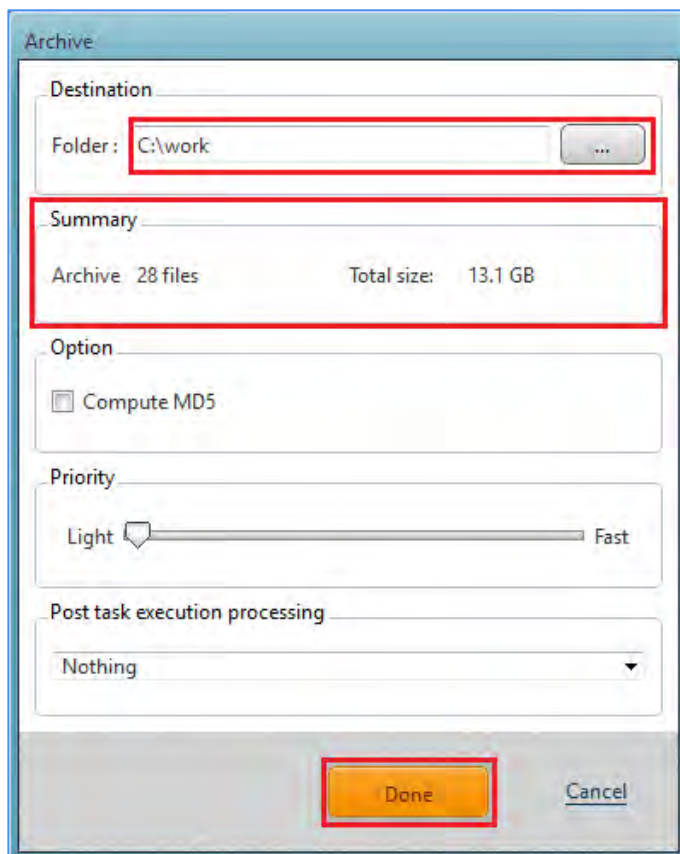
## 7-5. Archive Backups

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

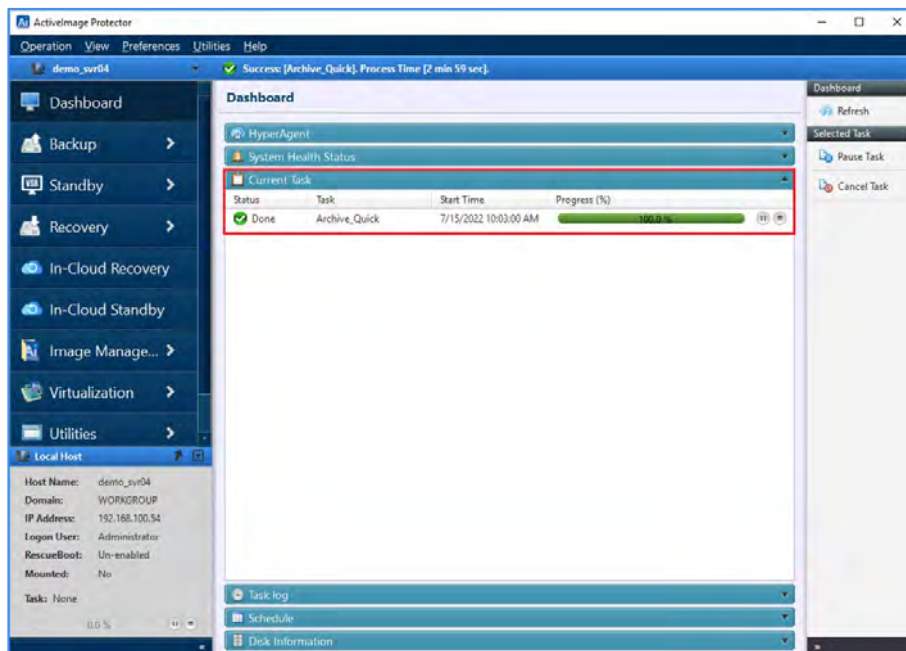
1. Select **[Source Computer]**, select the latest **[Recovery Point]** and click **[Archive Image]** in the right pane. The base backup and the associated incremental backups will be combined into one archived backup file.



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.



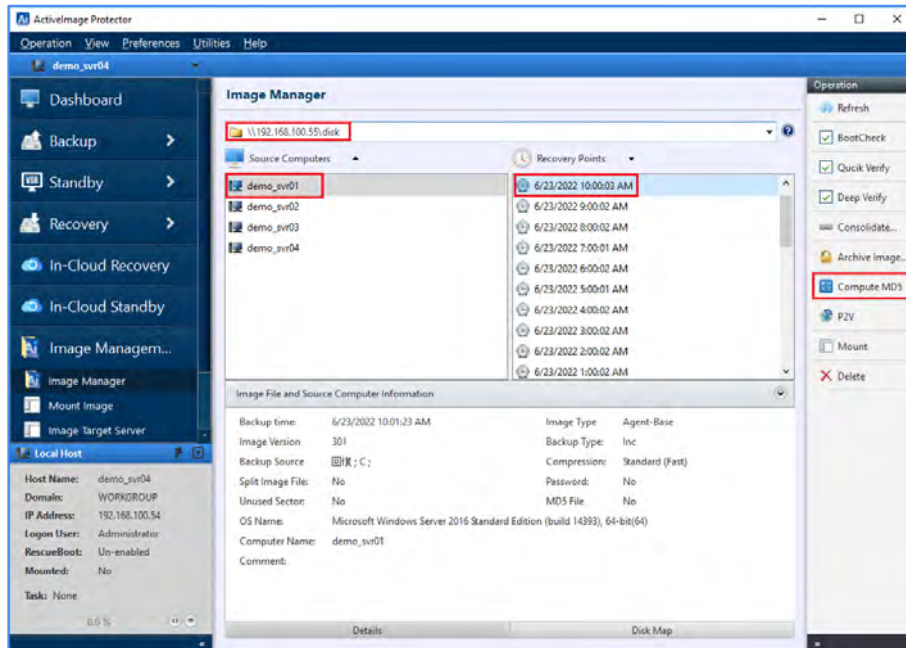
3. After archived backup has completed, the following window is displayed.



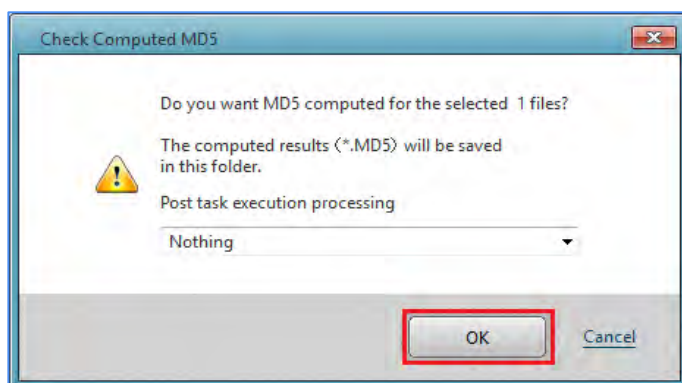
## 7-6. MD5 Checksum

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.

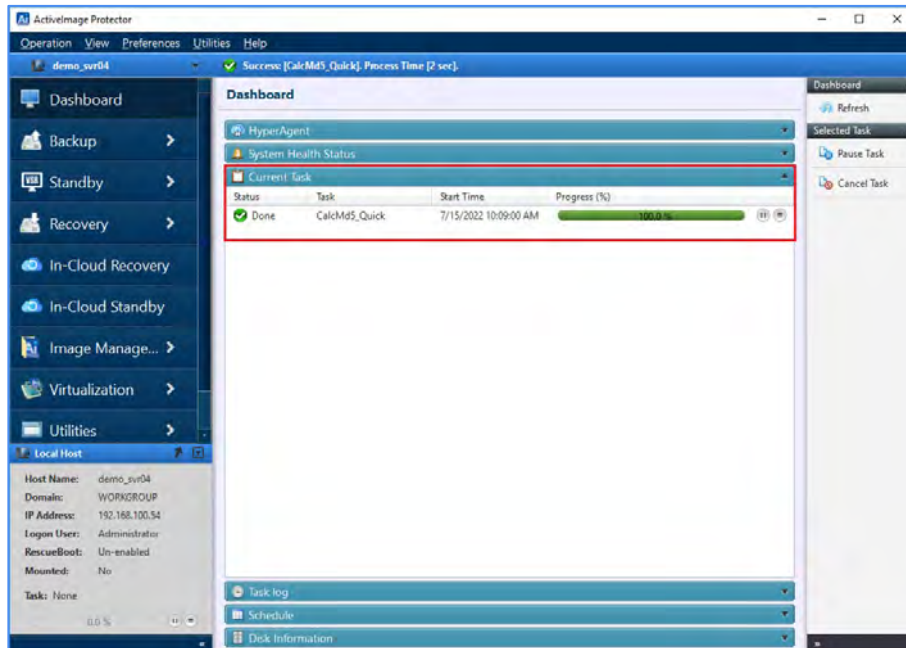
1. Select **[Source Computer]** and **[Recovery Point]** and click **[Compute MD5...]** in the right pane. To select multiple files, hold down the SHIFT/CTRL key and click on the starting and ending backup points.



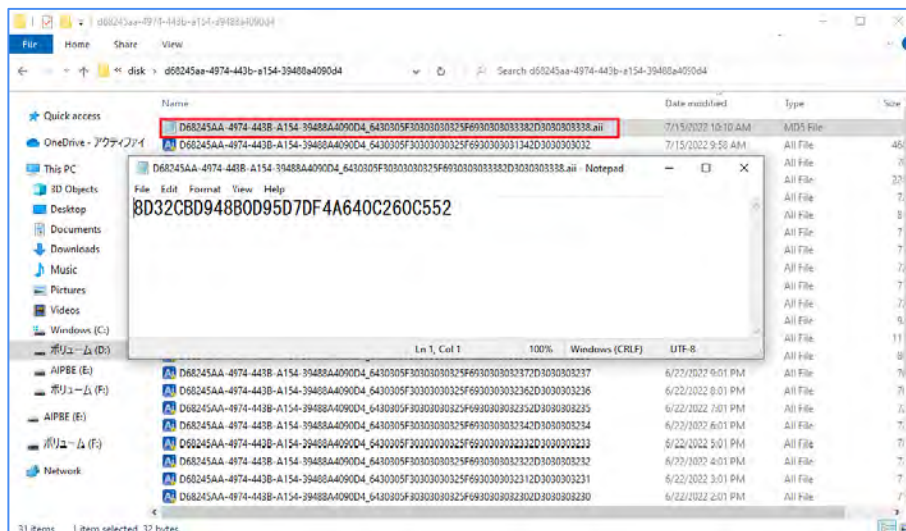
2. Click **[OK]**.



3. After MD5 Checksum process starts, the progress of the process is displayed in the **[Dashboard]**.



4. MD5 files will be saved in the same location as the image file. You can check the MD5 files from Windows explorer.



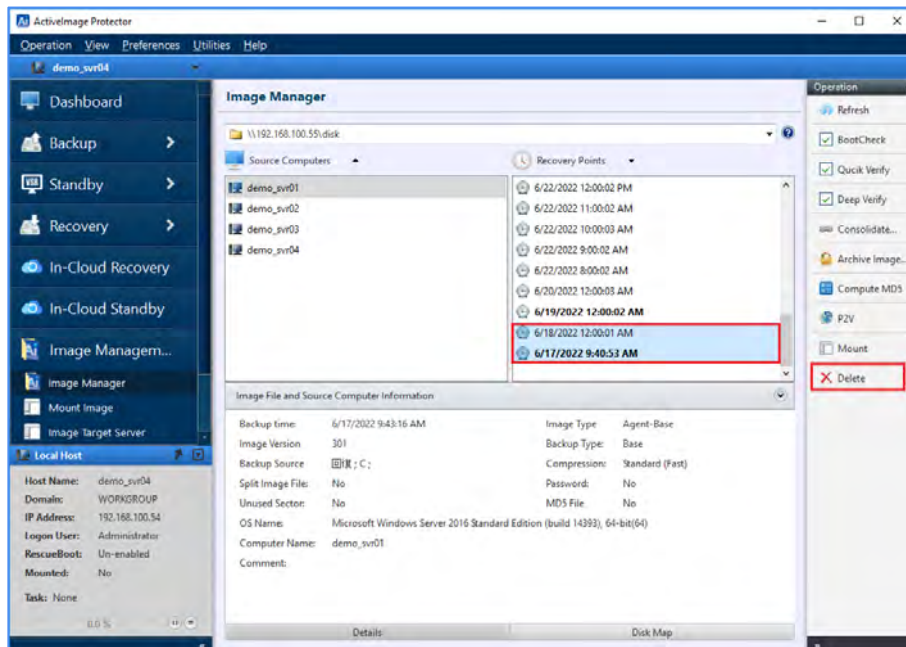


## 7-7. Delete Backup Files

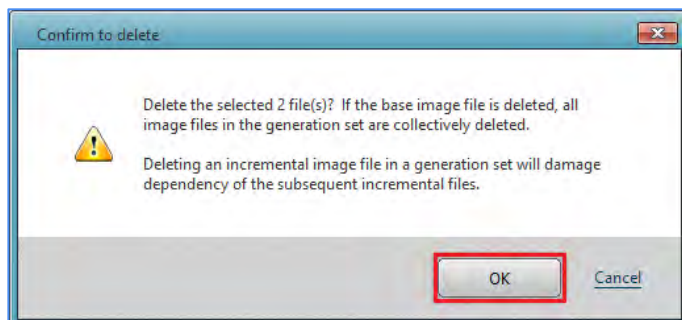
Specified backup files can be deleted.

**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.



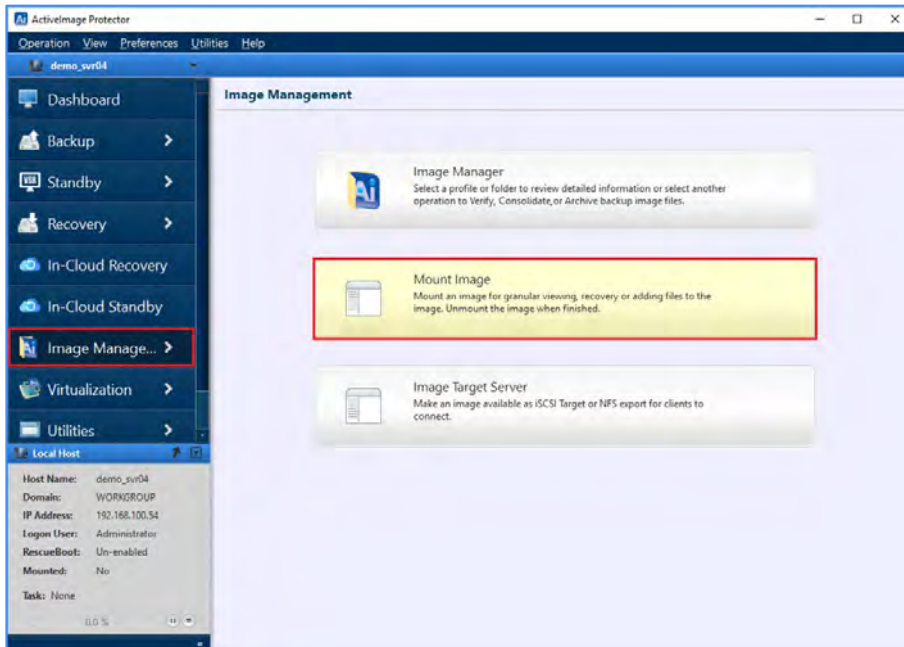
2. Click **[OK]** to deleted the selected backup files.



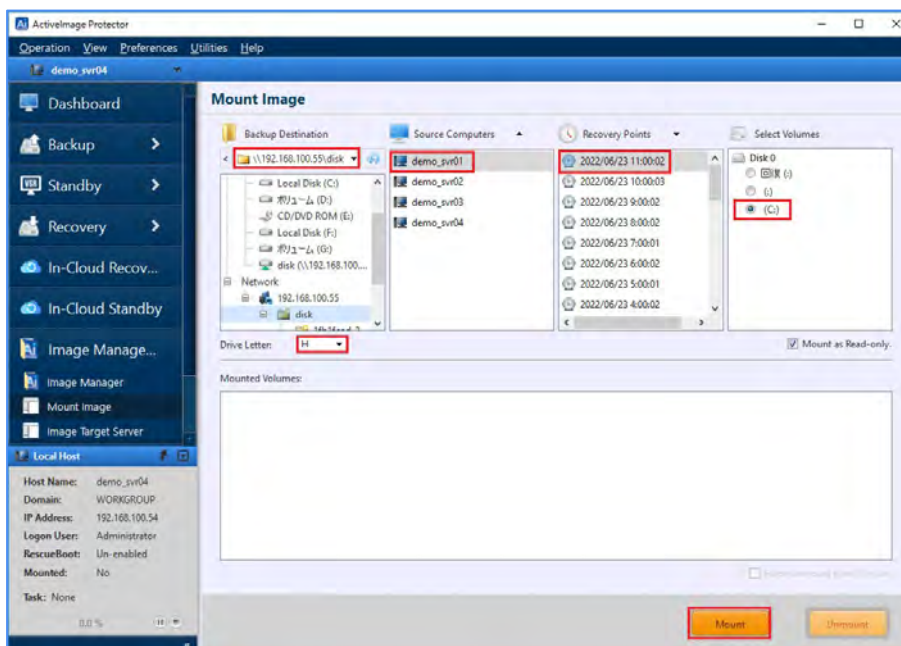
## 8. Image Manager: Mount Image

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]**.

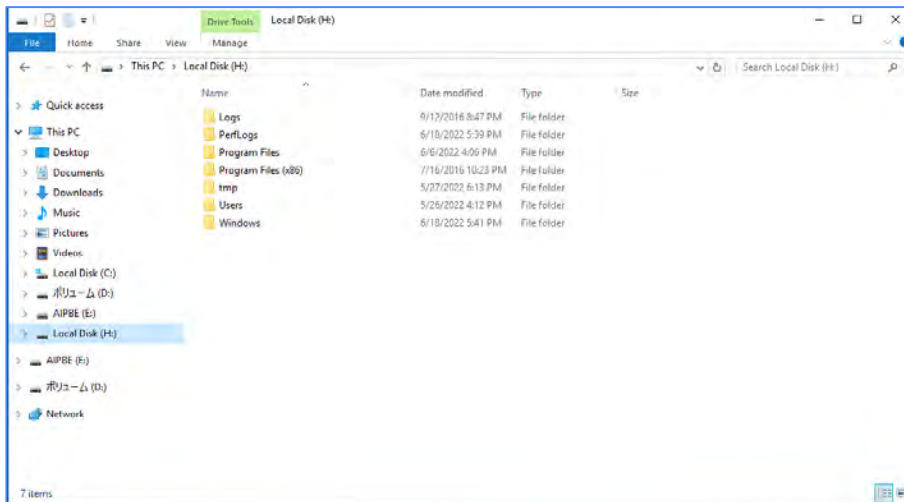


2. Select **[Source Computer]** and **[Recovery Point]** of a backup. When the backup includes multiple disks, select a volume to mount. Specify the drive letter to assign to the volume and click **[Mount]**. The backup can be mounted as read-only by selecting the **[Mount as Read-only]** option.

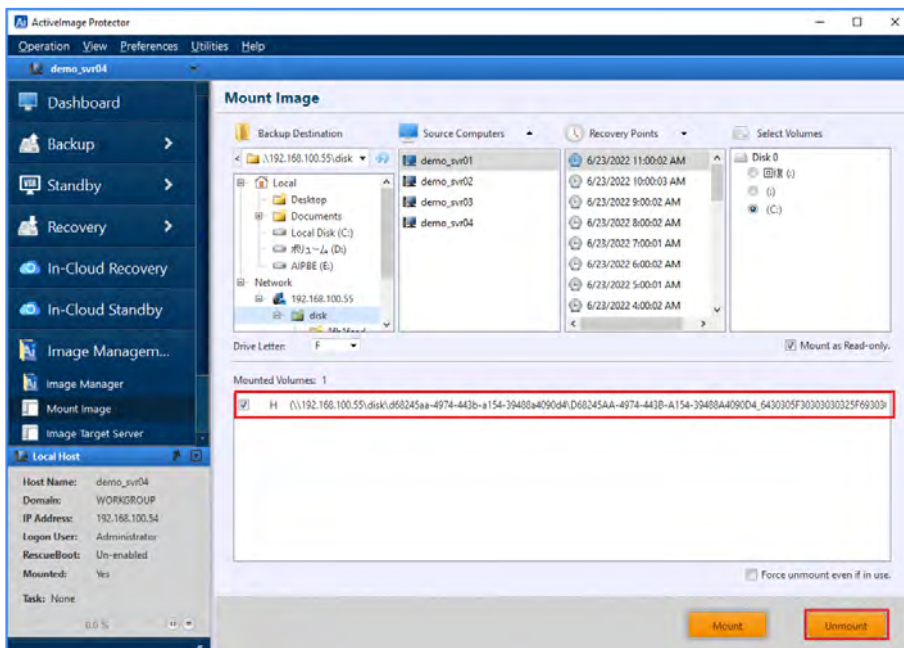


## Image Manager: Mount Image

- 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]**.



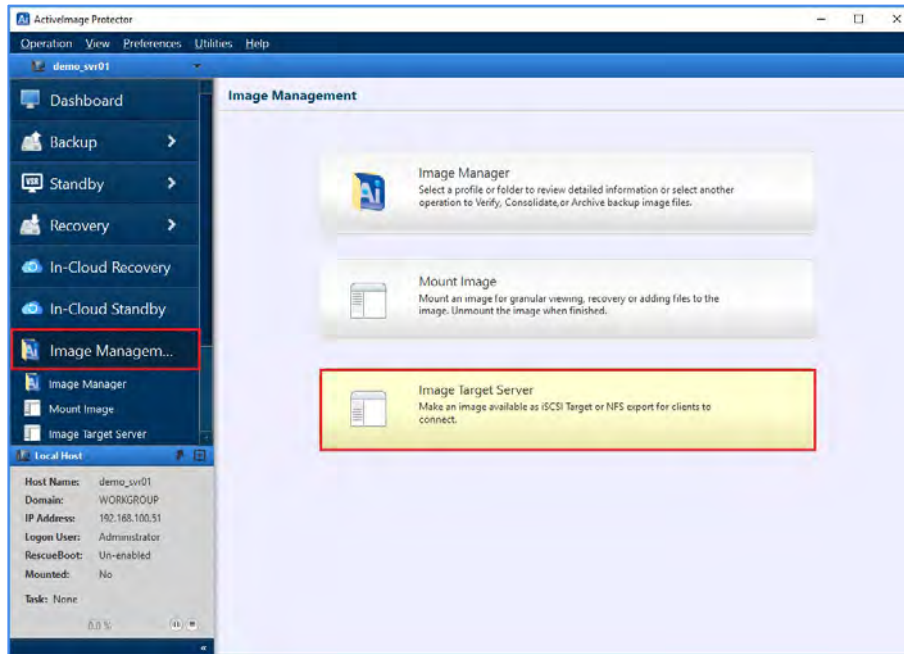
\*The backup can also be mounted as writable. The changes made to the backup are saved in a differential backup (.aix) after the volume is unmounted.

## 9. Image Manager: Image Target Server

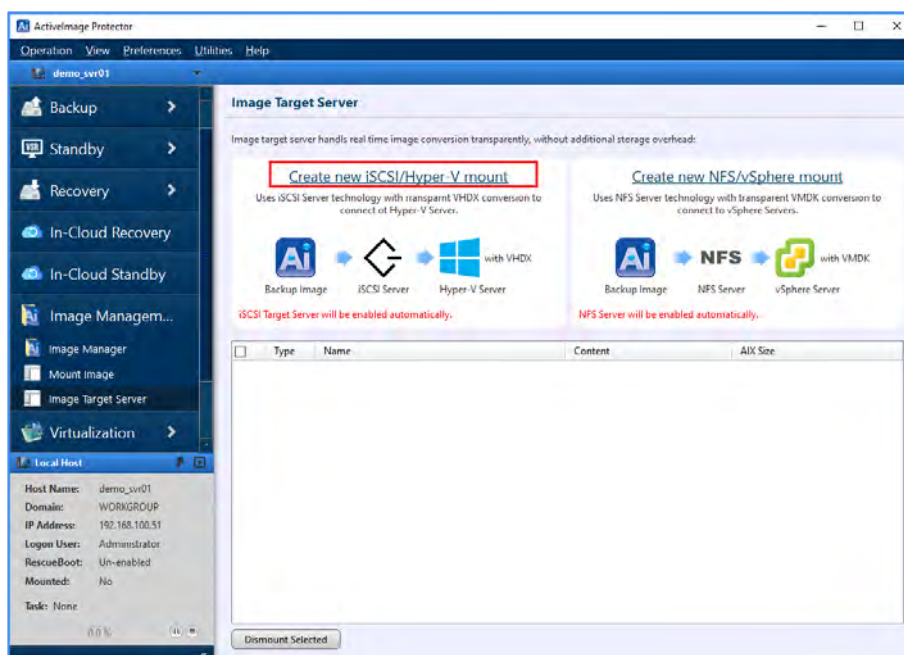
ActiveImage Protector backups can be configured as iSCSI or NFS target.

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]**.



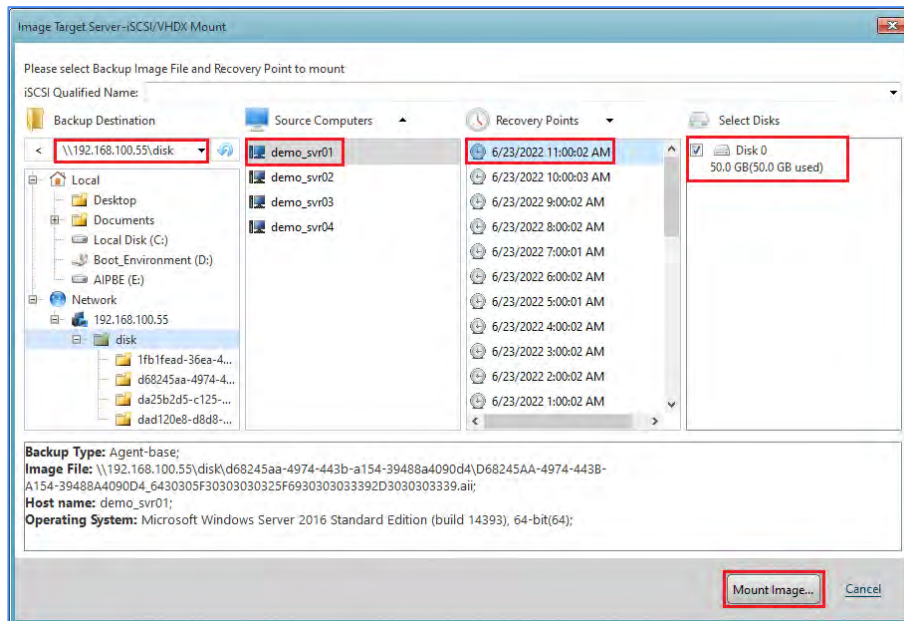
2. Depicted below is **[Image Target Server]** window. Select **[Create new iSCSI/Hyper-V mount]**.



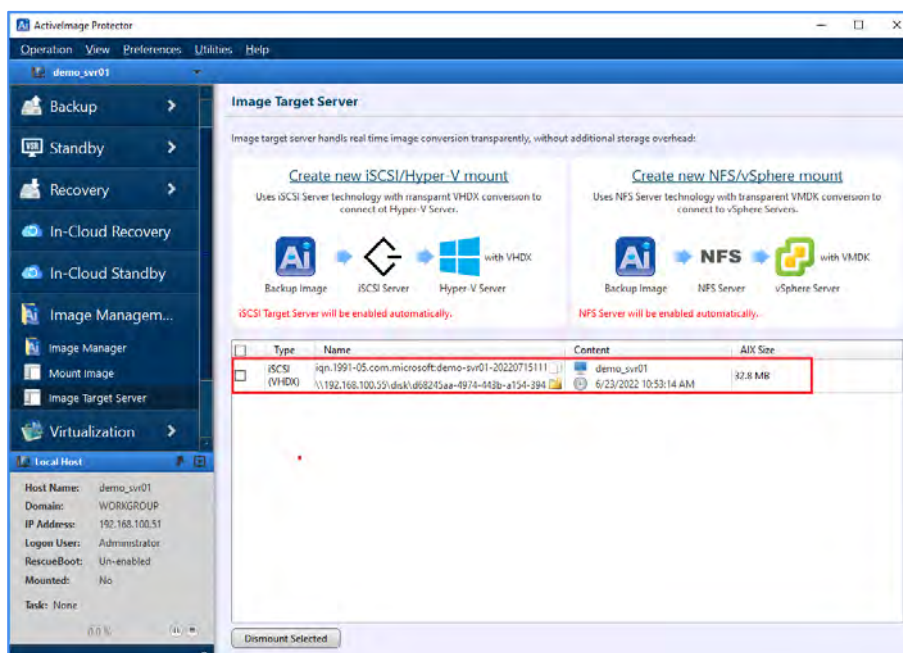


## Image Manager: Image Target Server

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]**.

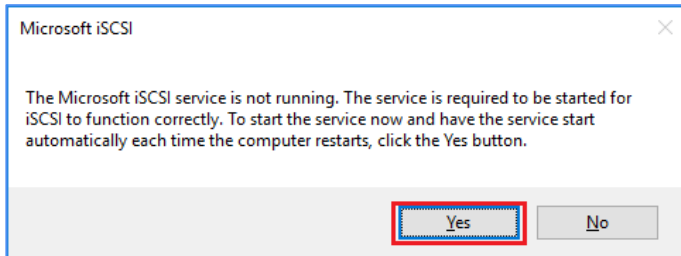


4. The backup will be served as an iSCSI target that can be connected via remote iSCSI initiator.

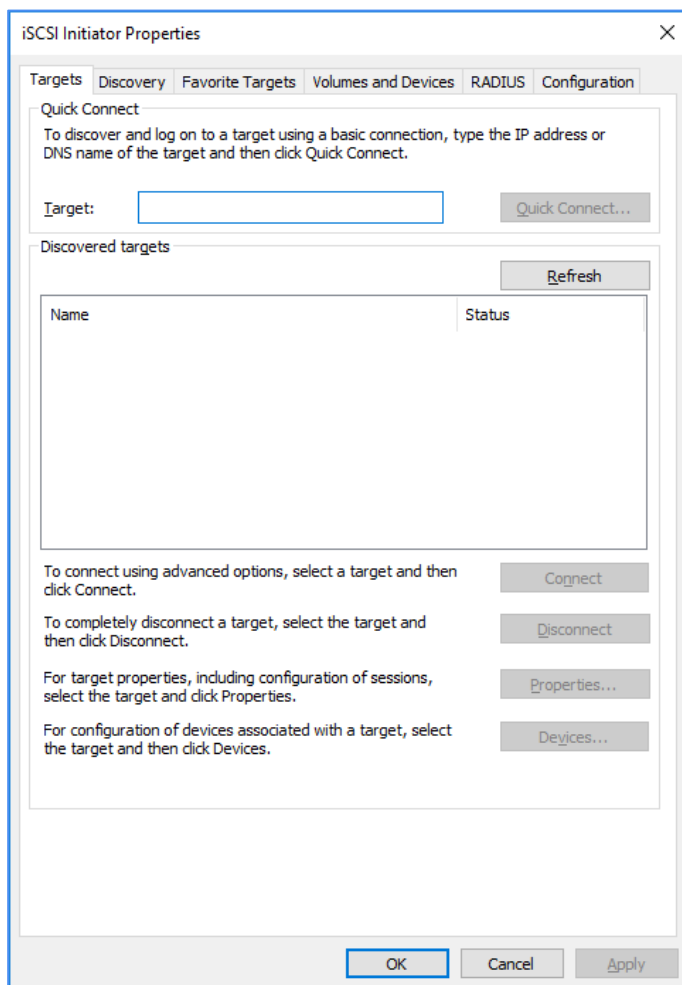




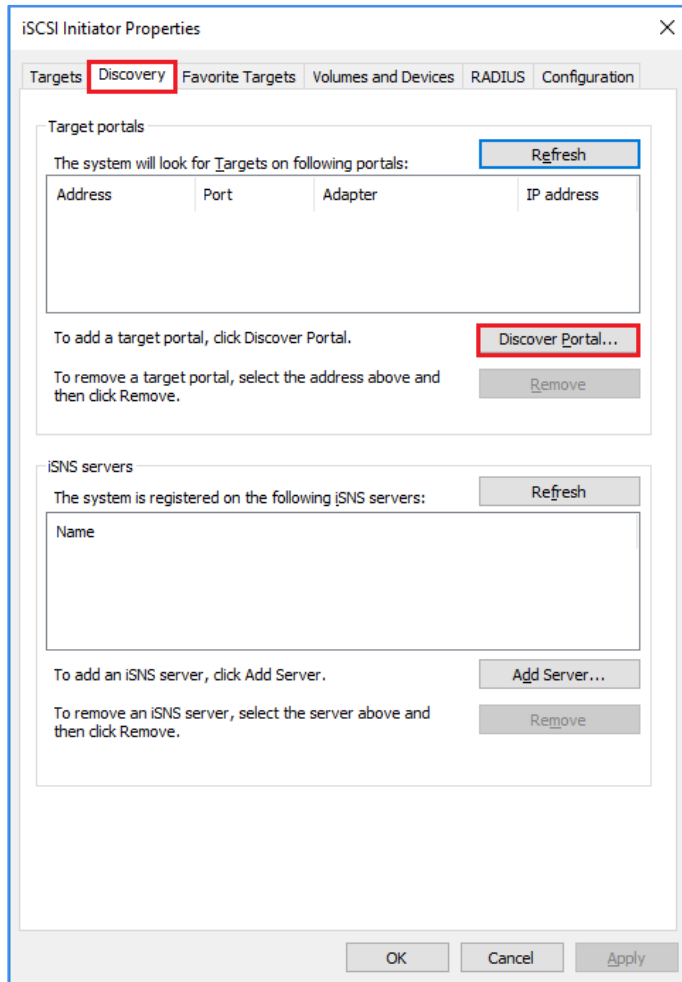
5. On the machine you wish to mount the image, go to Windows Start menu - **[iSCSI Initiator]**.
6. When the **[iSCSI Initiator]** is launched for the first time, please select **[Yes]** in the following dialog.



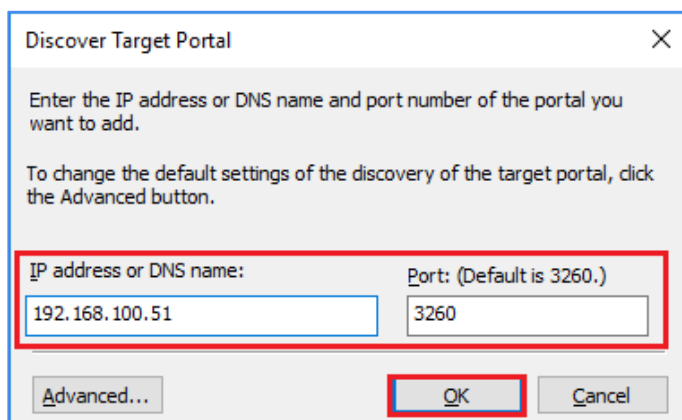
7. The dialog displayed after iSCSI Initiator has started.



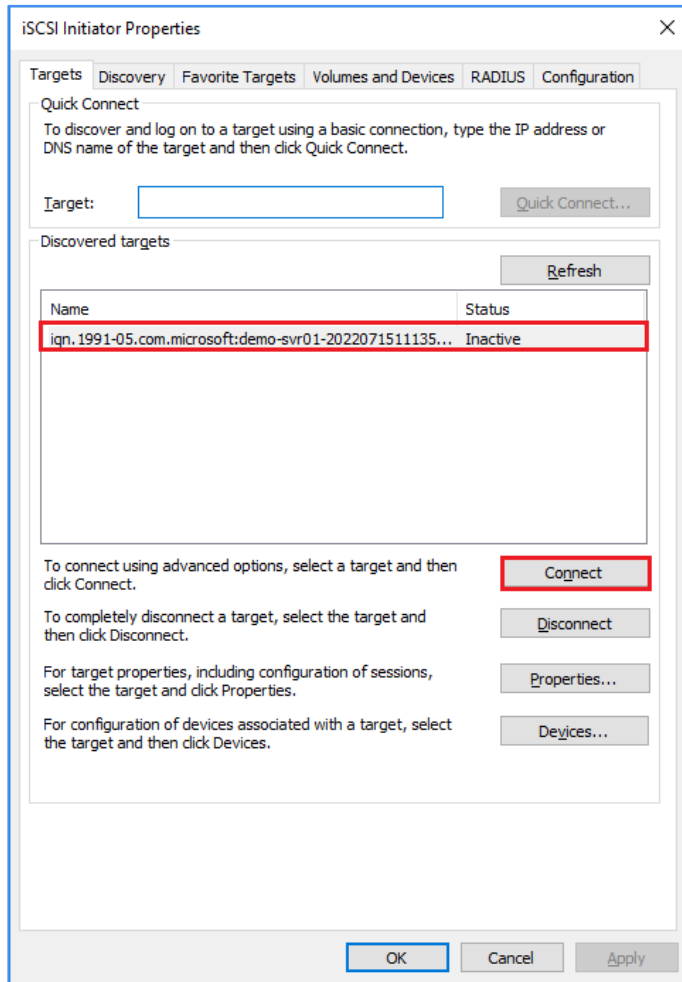
8. Select **[Discovery]** tab and click **[Discover Portal]**.



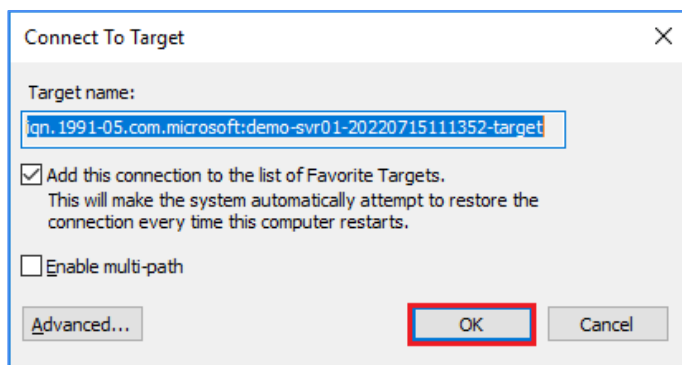
9. In this example, for the iSCSI server the IP address “192.168.100.51” is entered in the **[IP address or DNS name]** field. For the **[Port]** the default value “3260” is being used. Click **[OK]**.



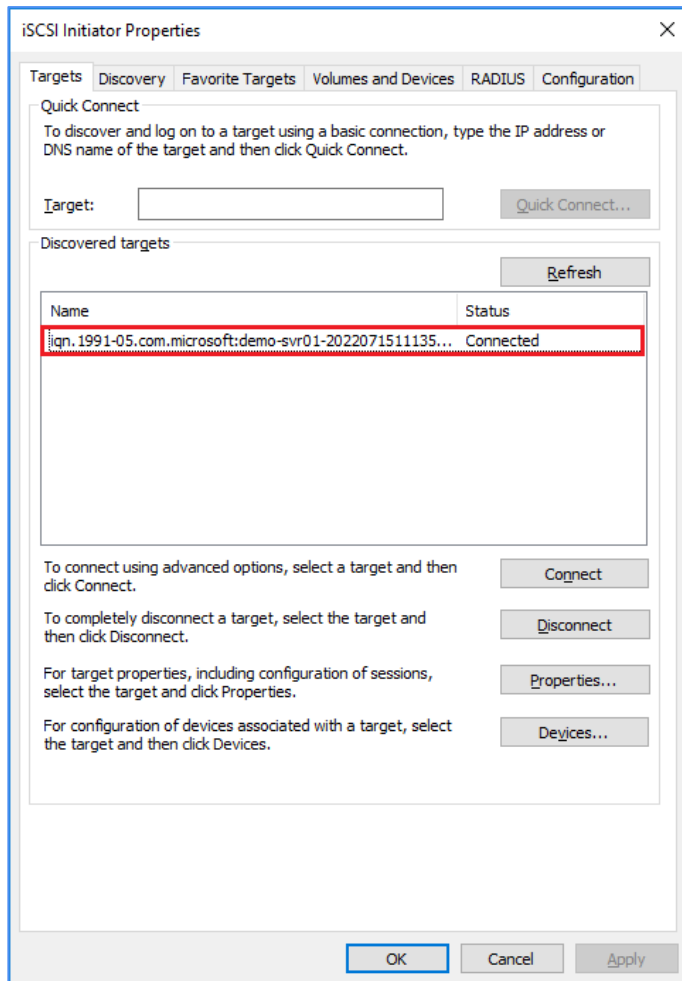
10. Go back to **[Target]** tab. iSCSI target is indicated for **[Discovered targets]**. Click **[Connect]**.



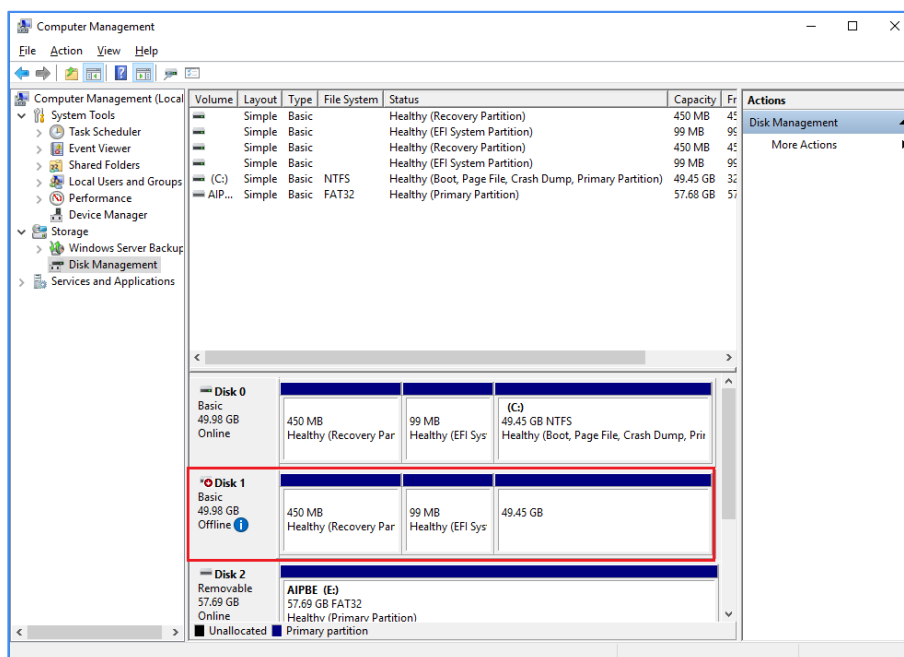
11. When establishing a connection to the target, [Add the connection to the list of Favorite Targets] is enabled by default. As the stated in description below, enabling this option will make the system automatically attempt to restore the connection every time this computer restarts]. Click **[OK]**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



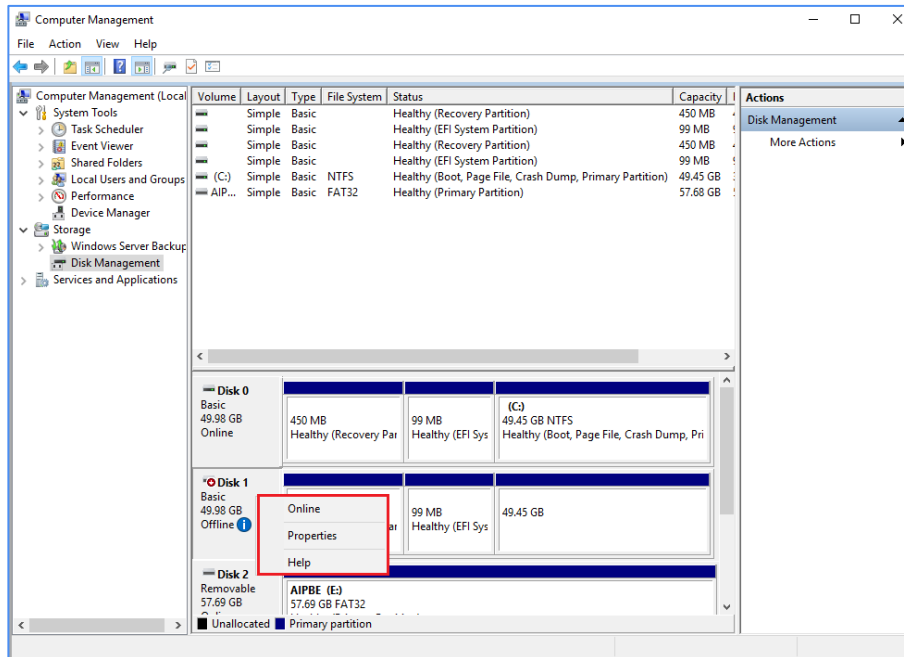
12. Please make sure that **[Status]** of the **[Discovered targets]** item has changed to **[Connected]** in **[Target]** tab.



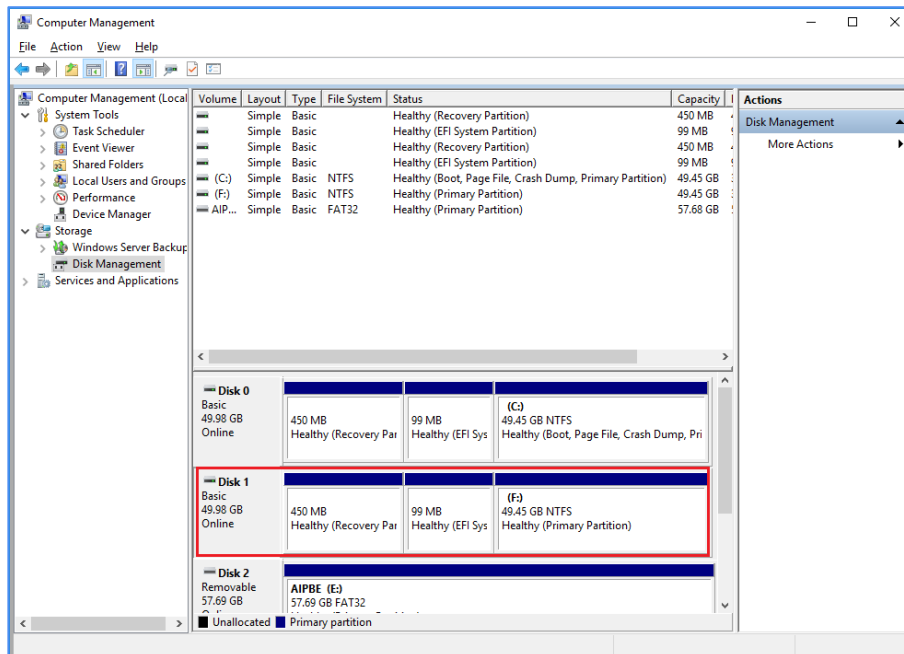
13. Next, go to **[Control Panel] - [Computer Management]** and select **[Disk Management]** in the left menu. A new disk, in the case "Disk 1", is added and the status indicates "Offline".



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

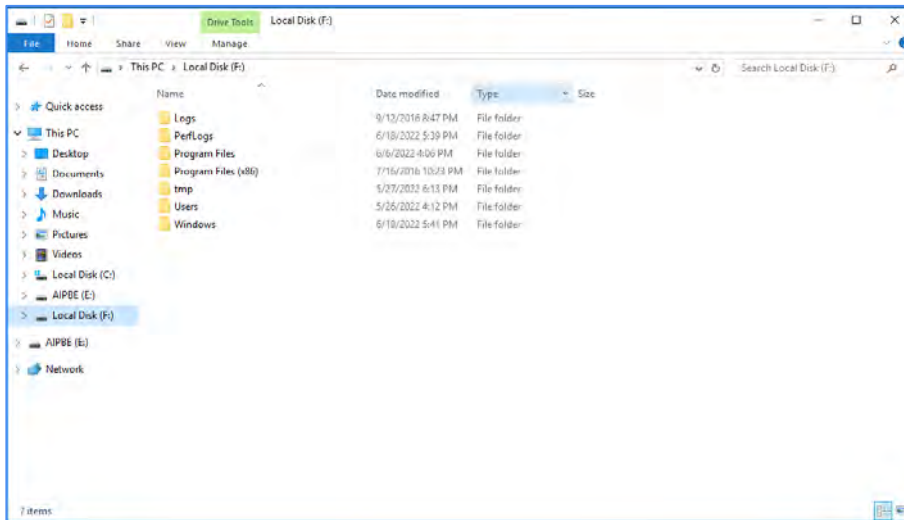


15. Because “Disk 1” is recognized as local disk, and a drive letter is assigned to the partition.

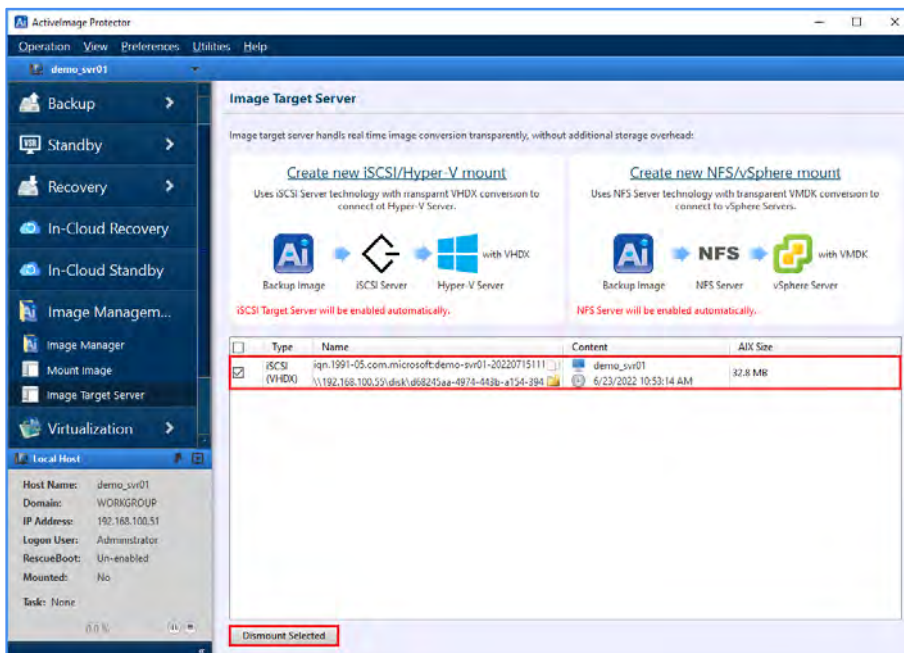




16. You can browse the contents using Windows file explorer.



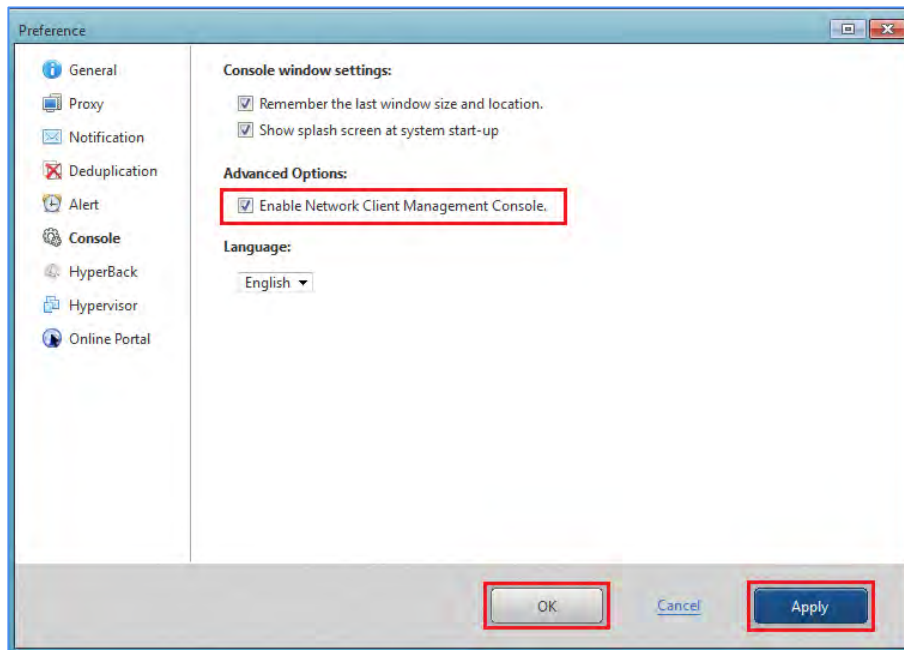
17. When you are finished using the iSCSI disk, please disconnect the iSCSI initiator. Tick the checkbox for the iSCSI target and click **[Dismount Selected]**. If you get 'The session cannot be logged out since a device on that session is currently in use' message, go to **[Disk Management]**, set the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



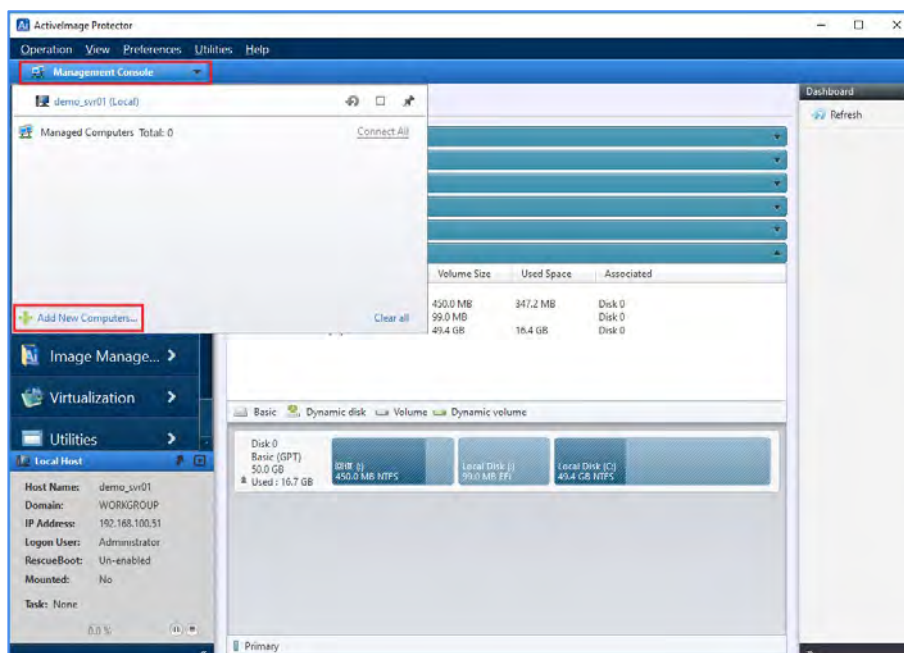
## 10. Remote Management Console

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

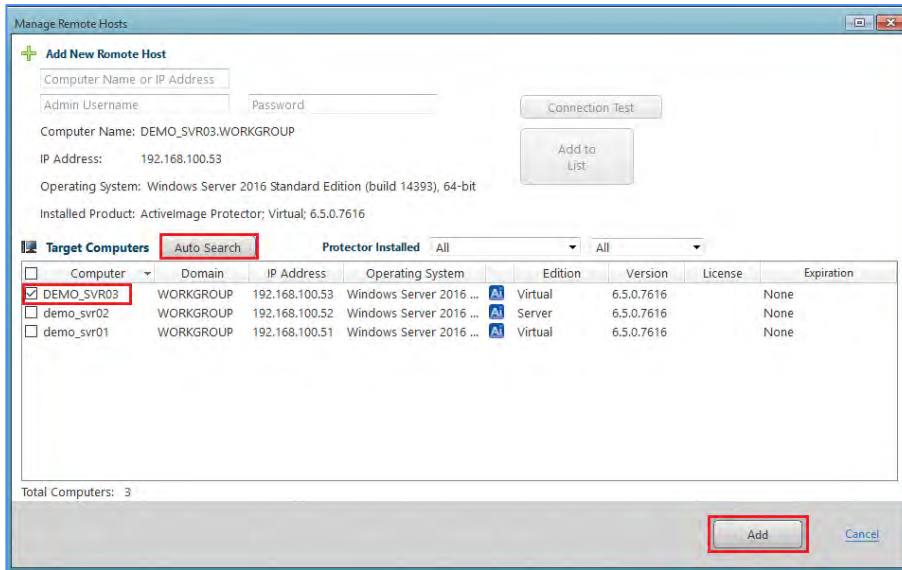
1. Go to Windows Start menu - **[Actiphy]** → **[ActiveImage Protector]**.
2. Go to **[Preference]** → **[Console]** and check in the checkbox for **[Enable Network Client Management Console]** and click **[Apply]**. Click **[OK]** and go back to Dashboard.



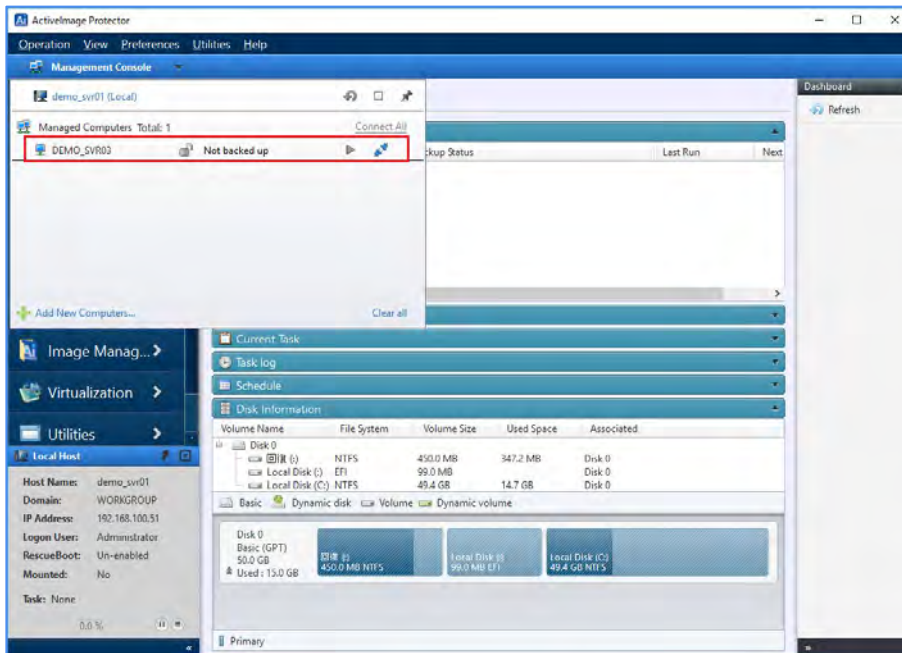
3. Click **[Management Console]** located in the upper left of the window. Before using the Remote Control feature, you need to add any clients you wish to control to the list of Managed Computers. Click **[Add New Computer]**.



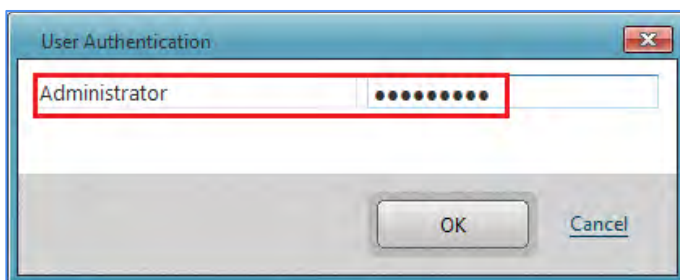
- You are presented with two options to add clients **[Auto Search]** and **[Manual Setting]**. In this example, **[Auto Search]** and **[All]** versions are selected. After the search has completed we tick the checkbox for the computer "DEMO\_SVR03", which has ActiveImage Protector installed, and click **[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.

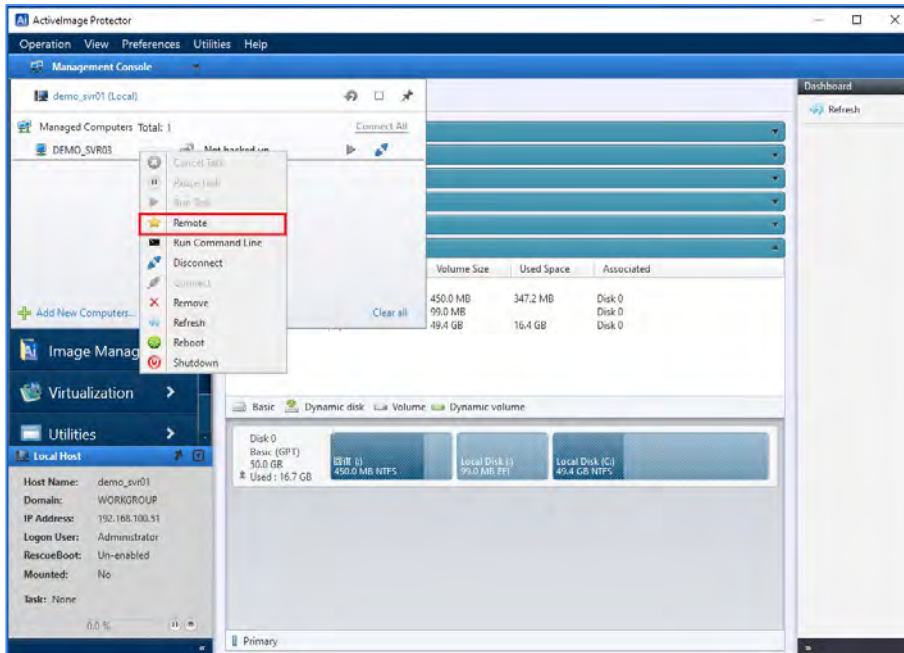


- Enter the credential information to access the client.

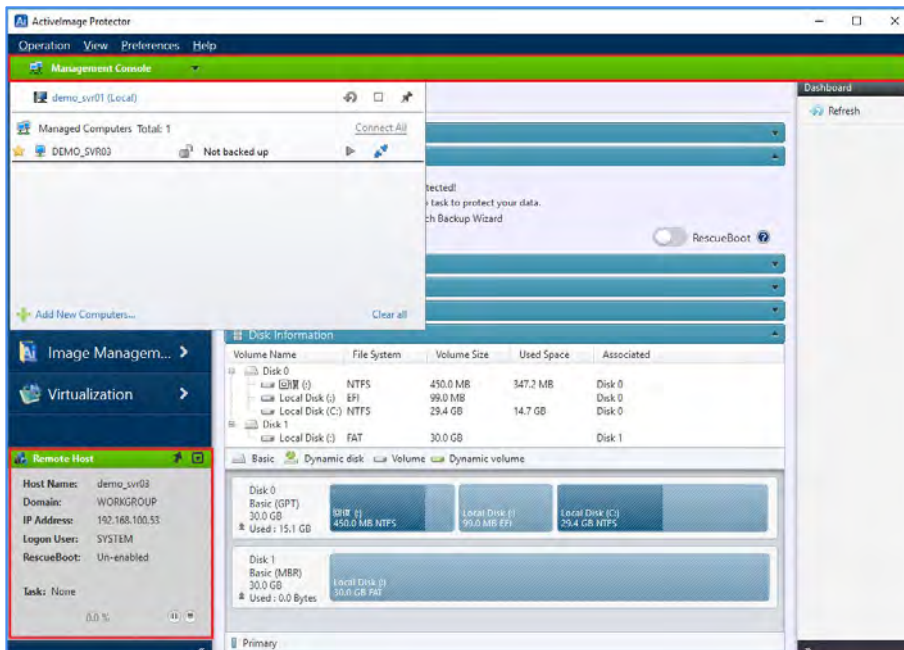


## Remote Management Console

- 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.



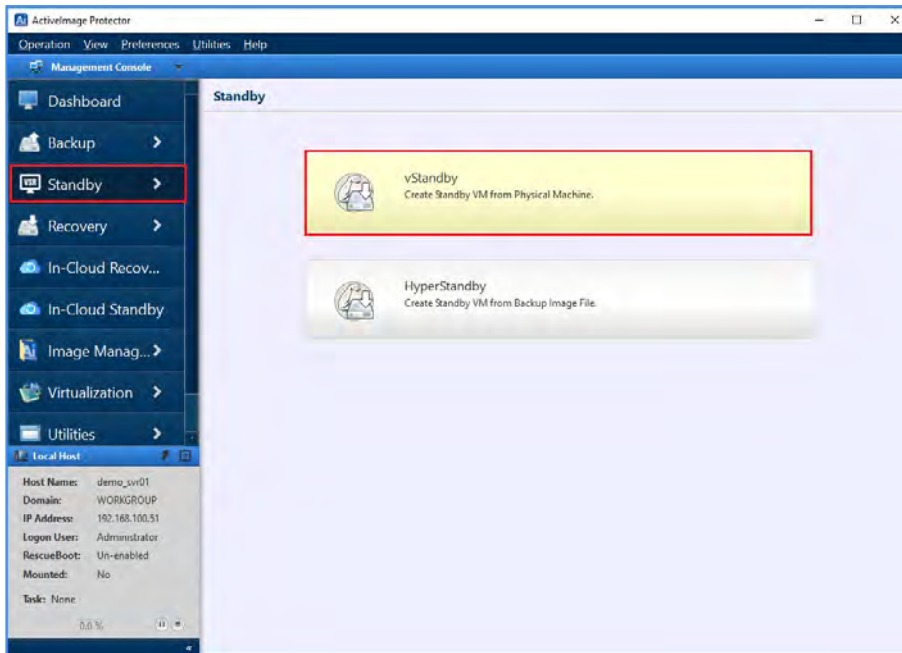


## 11. Creates and maintains dormant virtual replicas

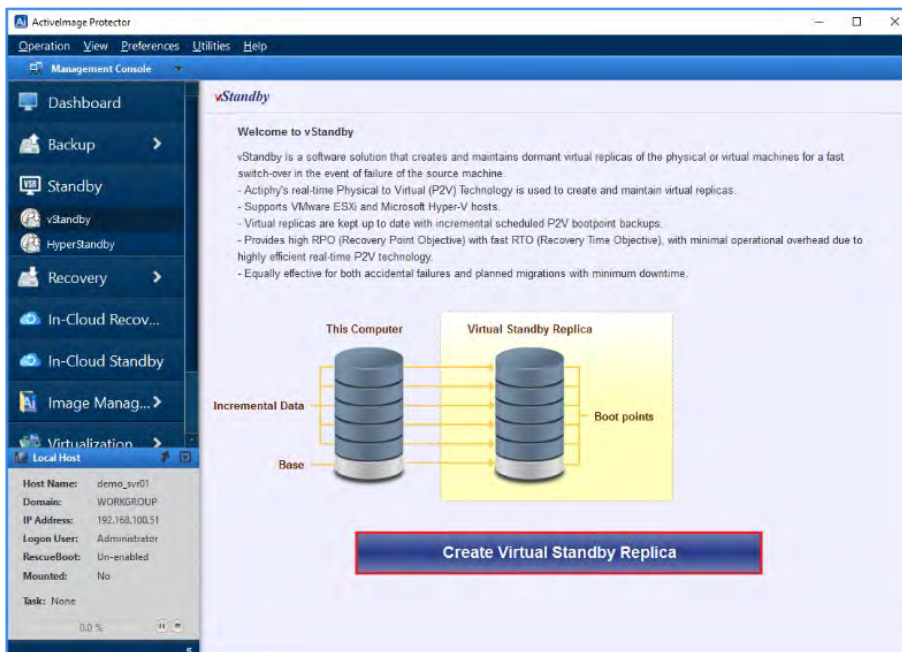
### 11-1.vStandby

vStandby is a software solution that creates and maintains dormant virtual replicas of physical or virtual machines to provide a switch-over option in the event of failure of the source machine. This virtual standby replica is kept current by taking scheduled incremental P2V boot points of the source machine. This ensures a successful startup of the standby virtual machine at the time of the switch-over. The following is an example of how to configure backup settings for vStandby.

1. Select **[Standby]** in the left menu and click **[vStandby]**.



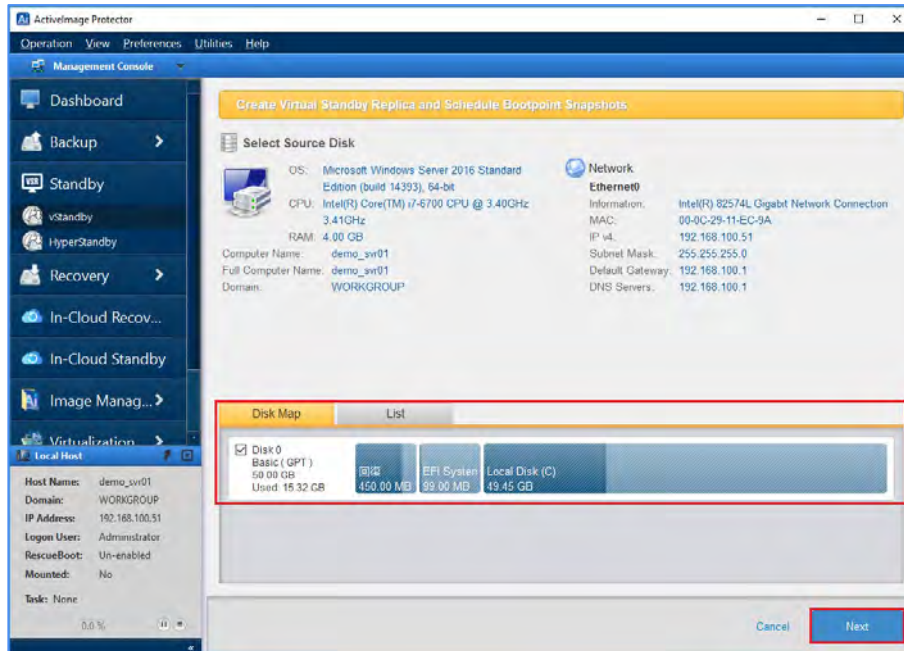
2. The **[Welcome to vStandby]** window is displayed. Click **[Create Virtual Standby Replica]**.



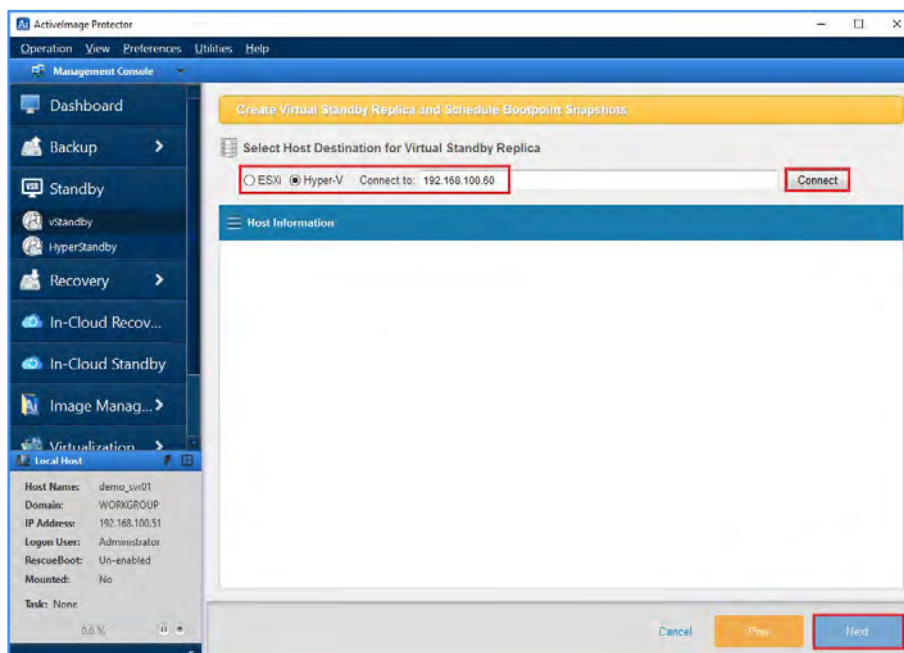


Creates and maintains dormant virtual replicas

3. The **[Select Source Disk]** window is displayed. Select the checkbox of the source disk in the disk map or the list to create the standby virtual replica. Click **[Next]**.

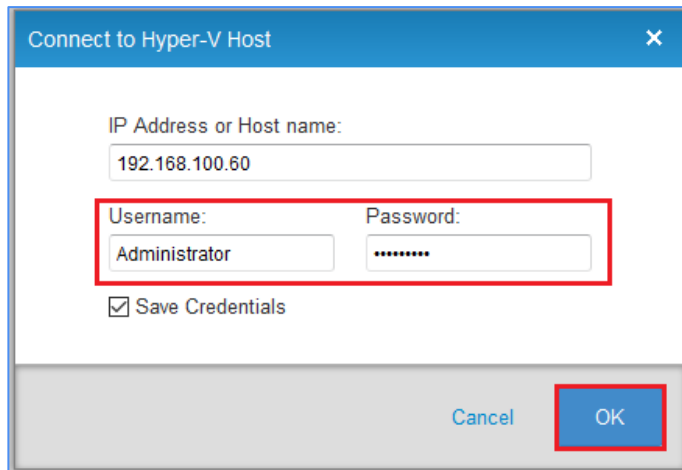


4. Select ESXi or Hyper-V as a host destination to create the standby virtual replica on. This example shows that [Hyper-V] is selected and "192.168.100.60" is specified as the target Hyper-V Host. Click **[Connect]**.



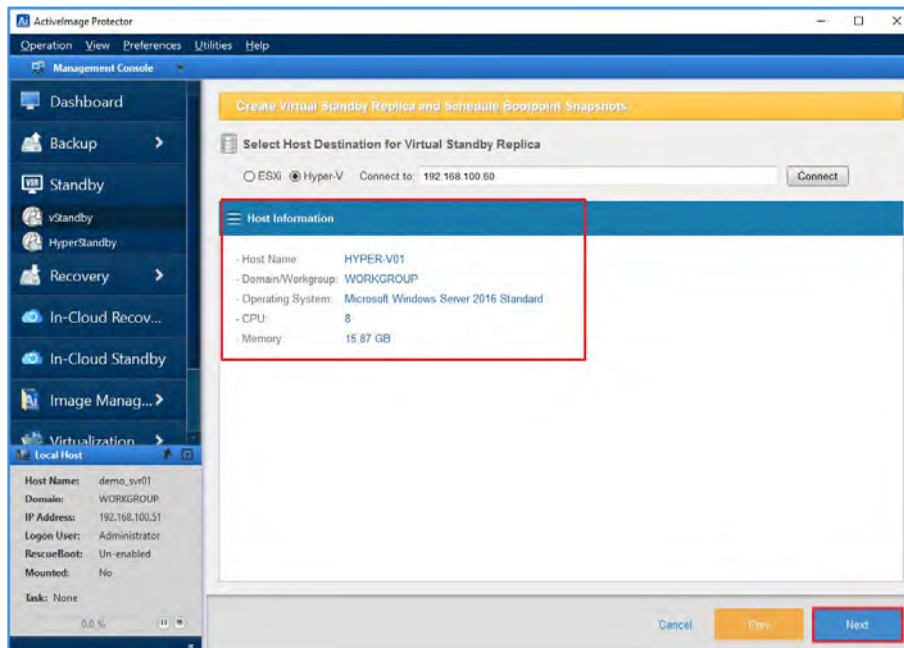
Creates and maintains dormant virtual replicas

- Please enter the credential information in the popup window to logon to the Hyper-V host. Here we have entered "Administrator" for the **[User Name:]** and a password for the **[Password]**.



The image shows a 'Connect to Hyper-V Host' dialog box. It has a title bar with a close button. The main area contains a label 'IP Address or Host name:' followed by a text box containing '192.168.100.60'. Below this, there are two text boxes: 'Username:' containing 'Administrator' and 'Password:' containing a masked password '\*\*\*\*\*'. A checkbox labeled 'Save Credentials' is checked. At the bottom right, there are 'Cancel' and 'OK' buttons. A red rectangle highlights the 'Username' and 'Password' fields.

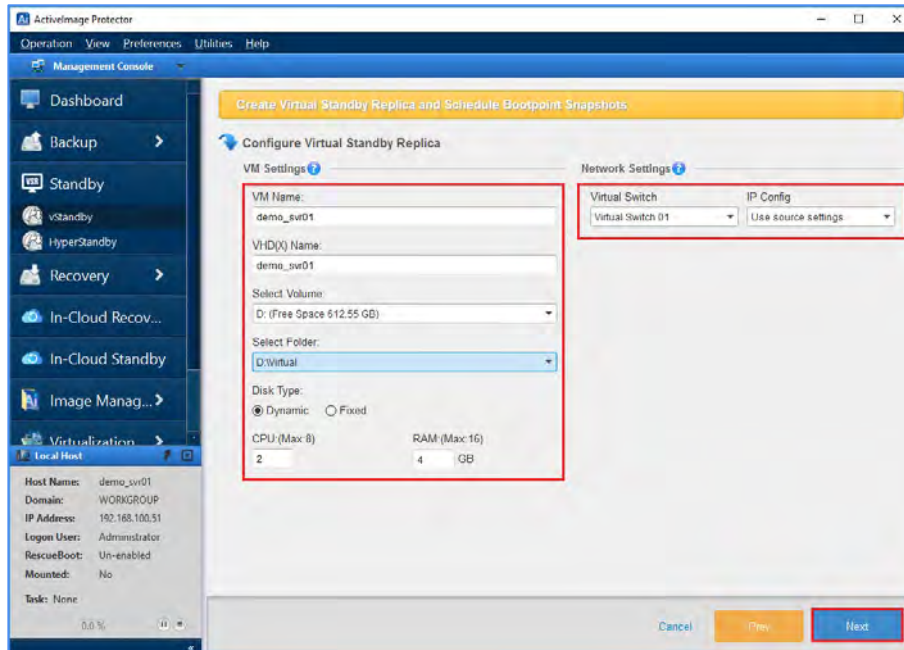
- The **[Host Information]** of the Hyper-V host is displayed as follows. Click **[Next]**.



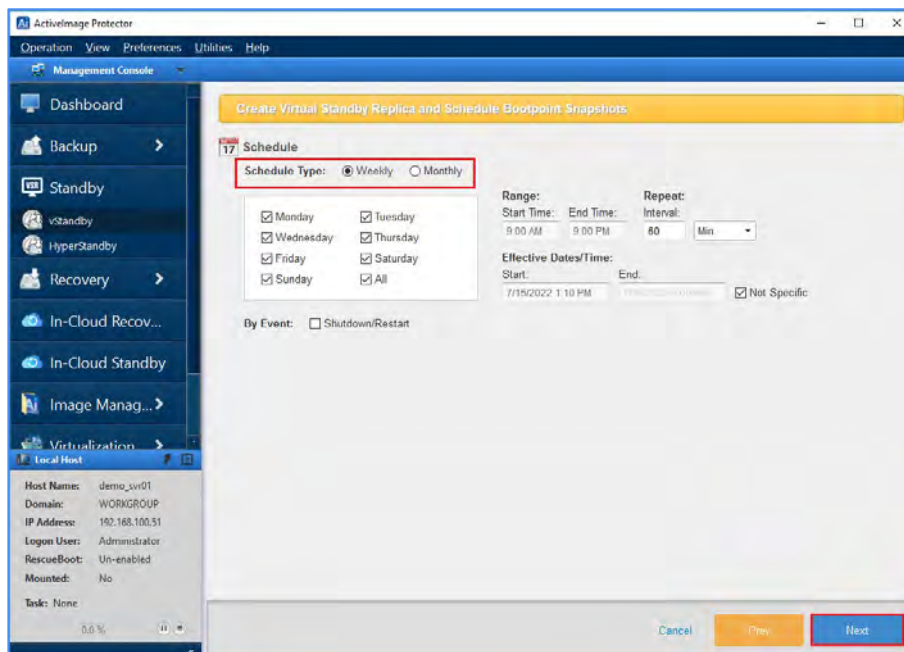
The image shows the 'ActivImage Protector' application window. The title bar says 'ActivImage Protector'. The menu bar includes 'Operation', 'View', 'Preferences', 'Utilities', and 'Help'. The left sidebar has a 'Management Console' section with icons for 'Dashboard', 'Backup', 'Standby', 'vStandby', 'HyperStandby', 'Recovery', 'In-Cloud Recov...', 'In-Cloud Standby', 'Image Manag...', and 'Virtualization'. The main area has a yellow header 'Create Virtual Standby Replica and Schedule Bootpoint Snapshots'. Below it, a section 'Select Host Destination for Virtual Standby Replica' has radio buttons for 'ESXi' and 'Hyper-V' (selected), and a 'Connect to:' field with '192.168.100.60' and a 'Connect' button. A 'Host Information' section is highlighted with a red rectangle, showing: 'Host Name: HYPER-V01', 'Domain/Workgroup: WORKGROUP', 'Operating System: Microsoft Windows Server 2016 Standard', 'CPU: 8', and 'Memory: 15.87 GB'. At the bottom, there are 'Cancel', 'Prev', and 'Next' buttons. A red rectangle highlights the 'Next' button.

Creates and maintains dormant virtual replicas

- Configure the hardware settings for the standby replica VM in the **[VM Settings]**. For **[Network Settings]**, select the values for **[Virtual Switch]** and **[IP Config]**. To use the same values as the source machine, select the **[Virtual Switch]** and for **[IP Config]** select **[Use source settings]**. Click **[Next]**.

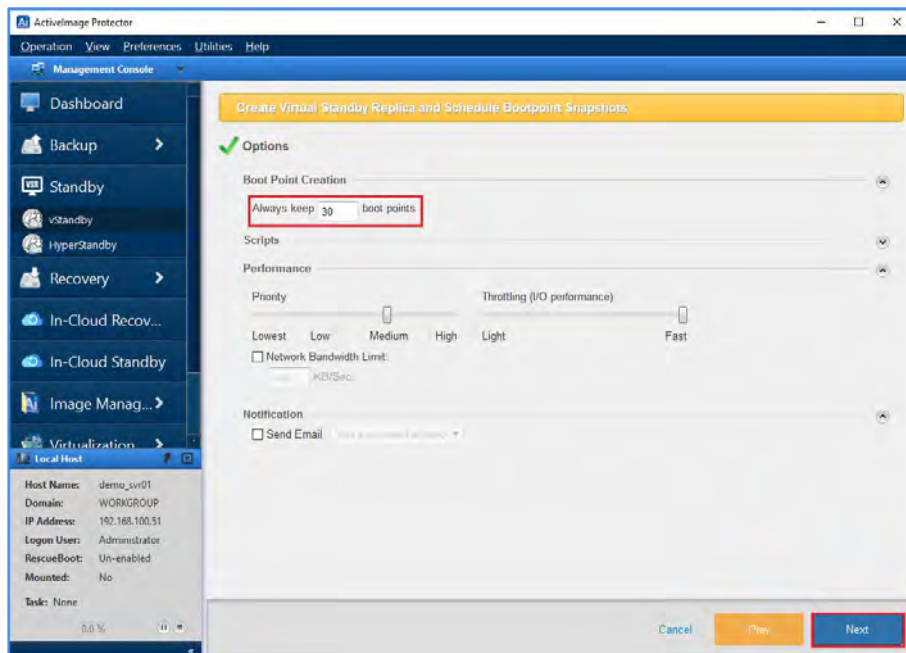


- Configure the weekly or monthly schedule for creating incremental boot points on the standby virtual replica. In the following example, vStandby is scheduled to executed daily from 9:00 to 21:00 in 60-minute intervals. Click **[Next]**.

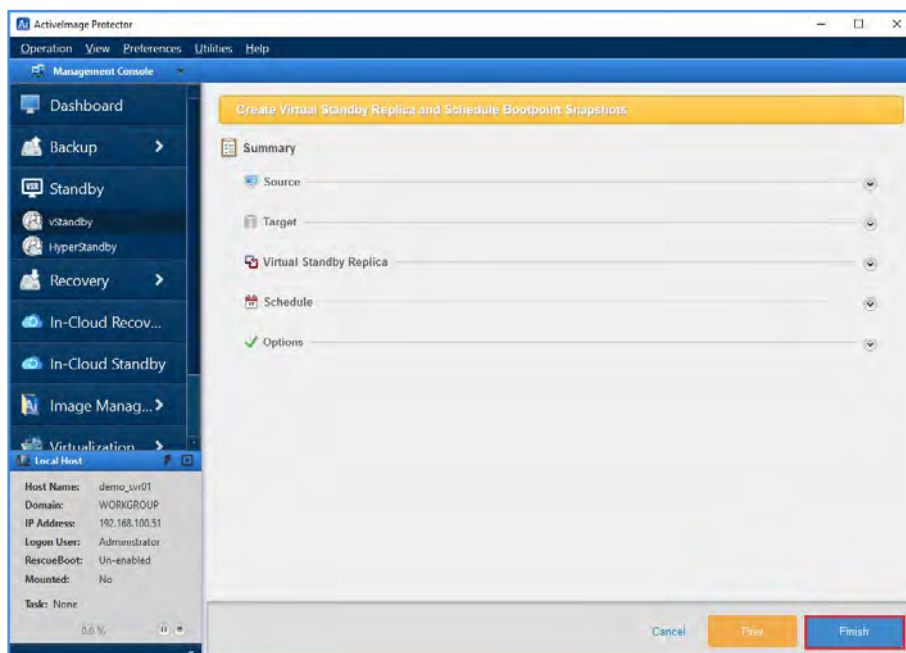


Creates and maintains dormant virtual replicas

9. Configure Option settings. Specify the maximum number of boot points to create on the virtual standby replica (maximum of 30). When the number of the boot points reaches the predefined limit, the oldest 2 boot points will be merged. Click **[Next]**.

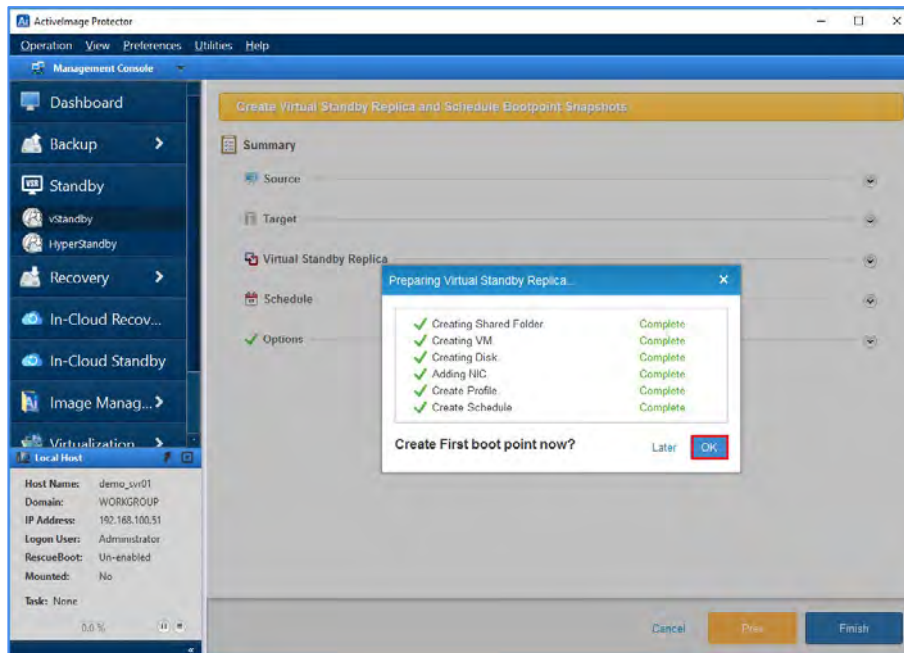


10. Review your configuration the Summary window. Click **[Finish]** to proceed.

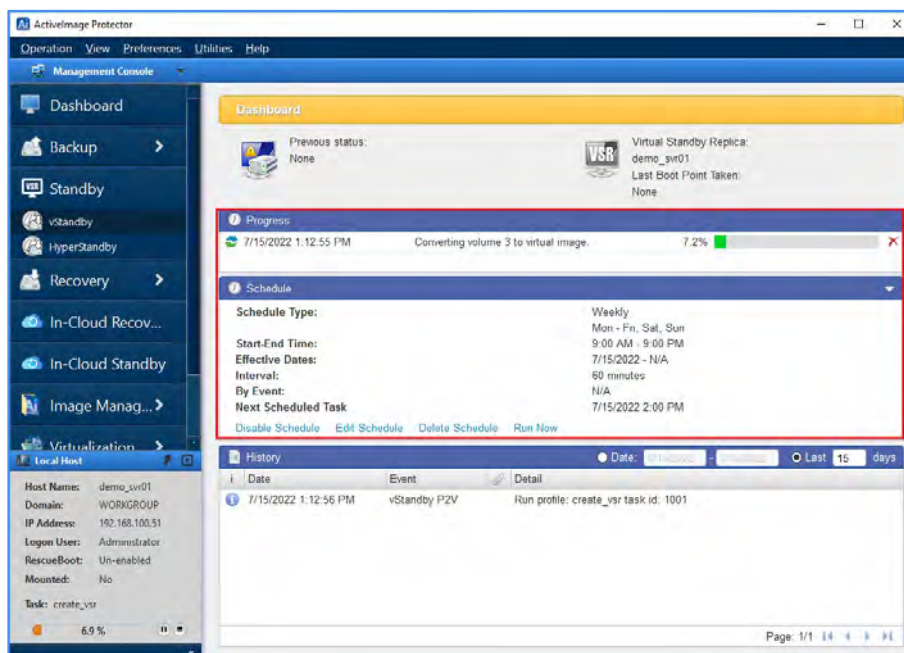


Creates and maintains dormant virtual replicas

11. The task will start and create the virtual standby replica on the host. When the virtual standby replica creation is complete, click **[OK]** to create the first boot point now, or later to have it run at the first scheduled run time.



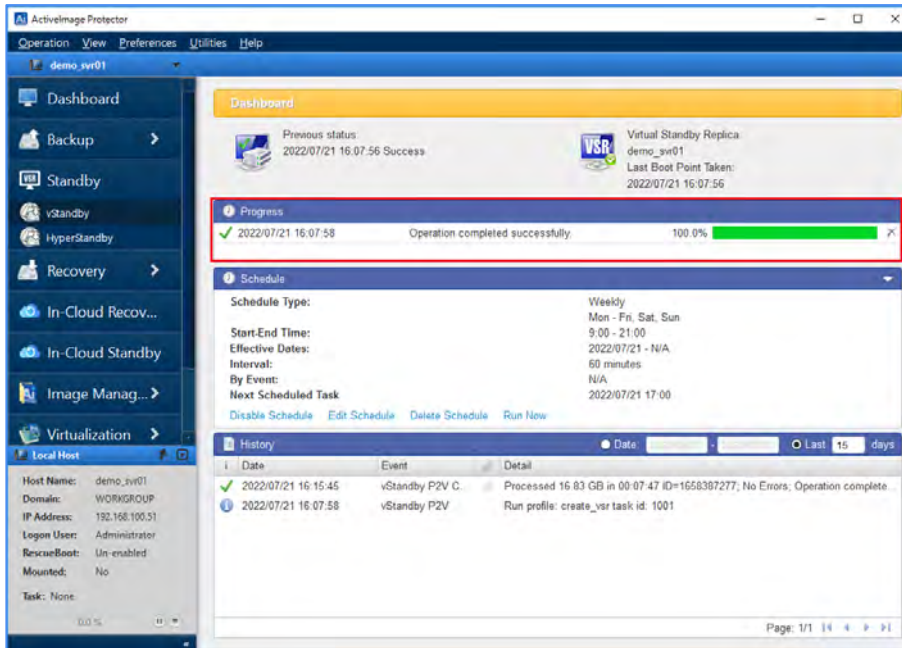
12. When the task schedule is configuration is complete the console defaults to Dashboard view indicating the progress of tasks.



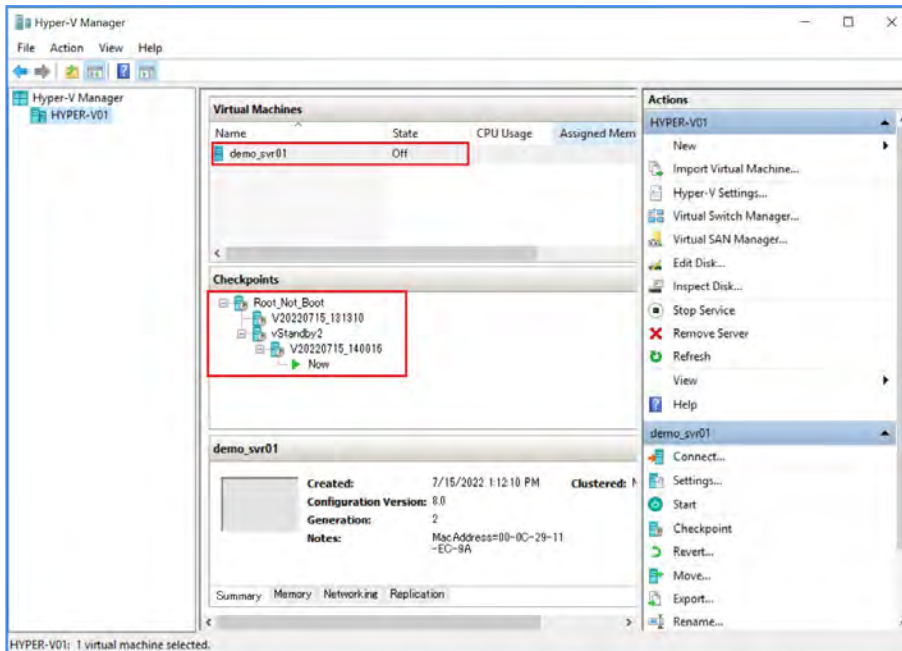


Creates and maintains dormant virtual replicas

13. The Dashboard shows regularly scheduled incremental boot points task results. These boot points can be used to boot the VM should a switchover to the standby virtual machine become necessary.



14. You can monitor the virtual standby replica / standby VM from Hyper-V Manager. In this example, the incremental disk changes of the source machine are taken on a 60-minute interval and added as checkpoints to the virtual standby machine.



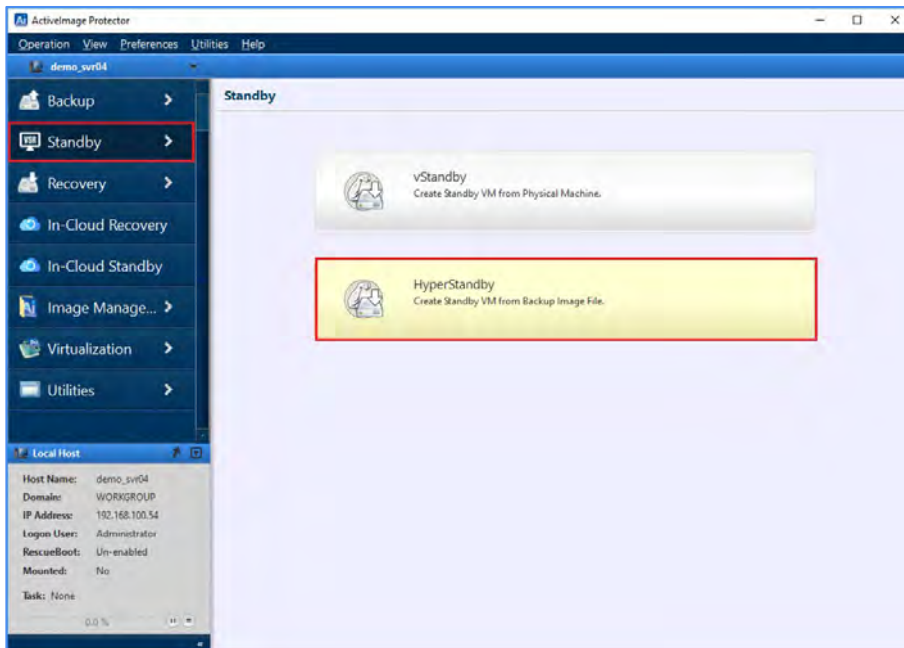
Creates and maintains dormant virtual replicas

## 11-2.HyperStandby

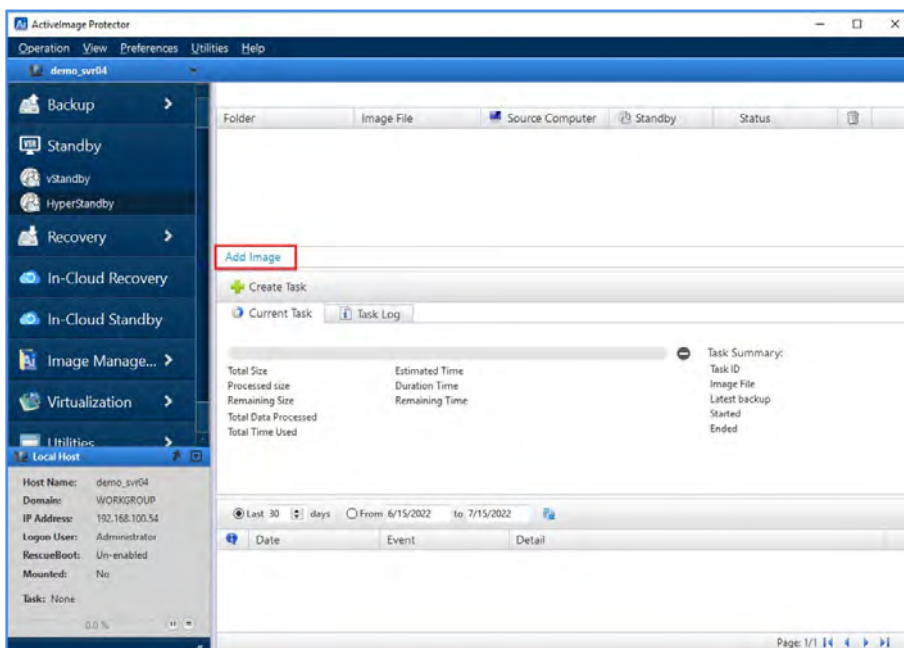
HyperStandby creates and maintains dormant virtual replicas of physical or virtual machines from ActiveImage Protector backups on a predefined schedule. HyperStandby can be used as a switch-over solution in the event of a failure of the source machine.

Below is an explanation of the operating procedures to use HyperStandby.

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

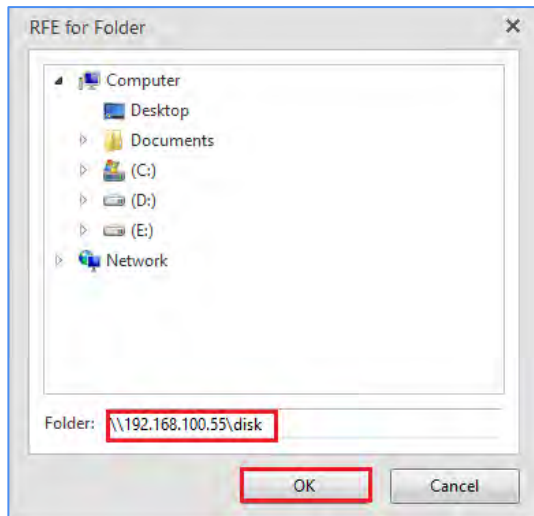


2. Click **[Add Image]** in the list dialog and check a box to select a backup.

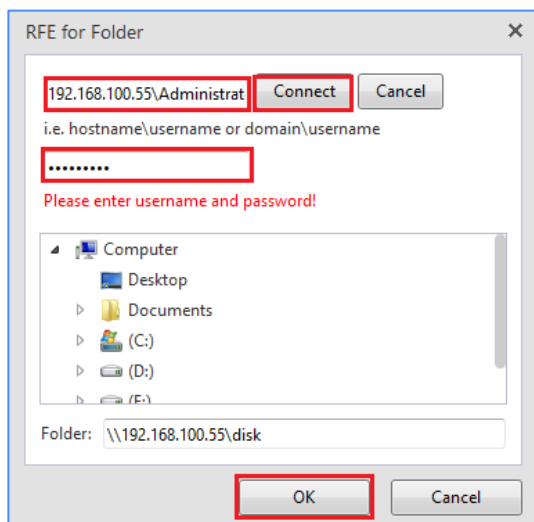


Creates and maintains dormant virtual replicas

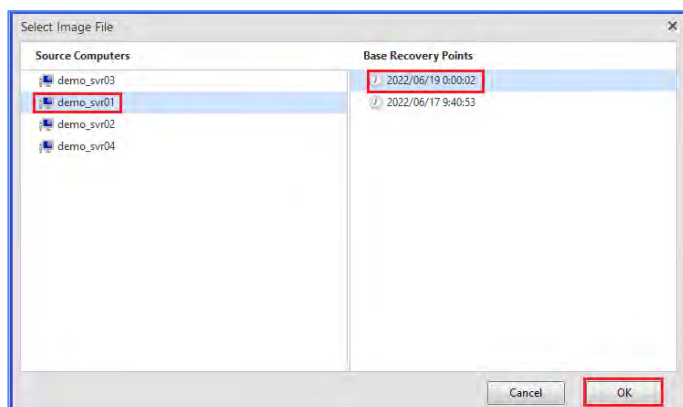
- Specify a folder that contains backup image files. This example shows entering a path to a shared folder “\\192.168.100.55\disk”. Click **[OK]**.



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

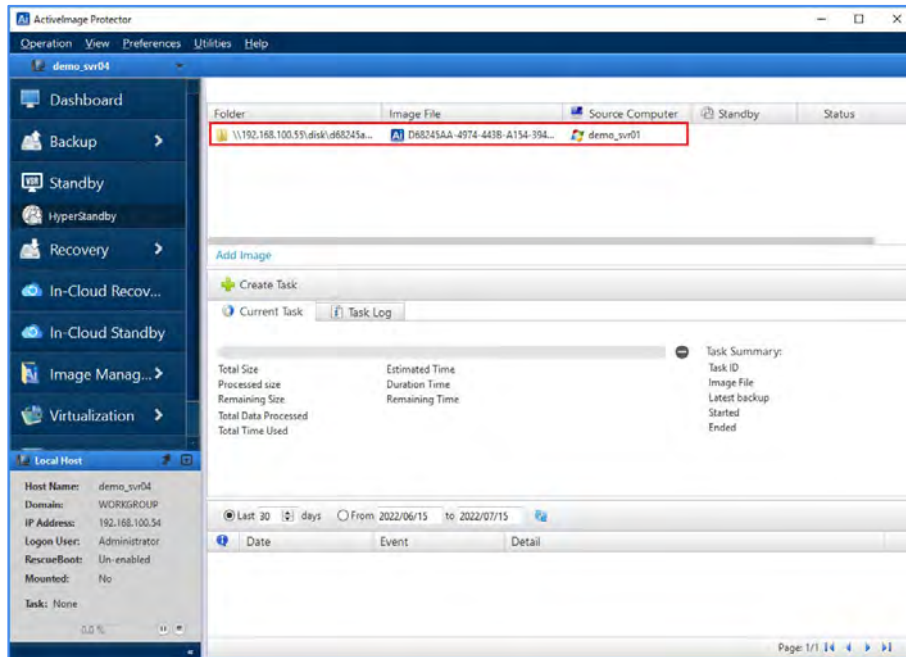


- Select the source computer and recovery point of the base (full) backup. Click **[OK]**.

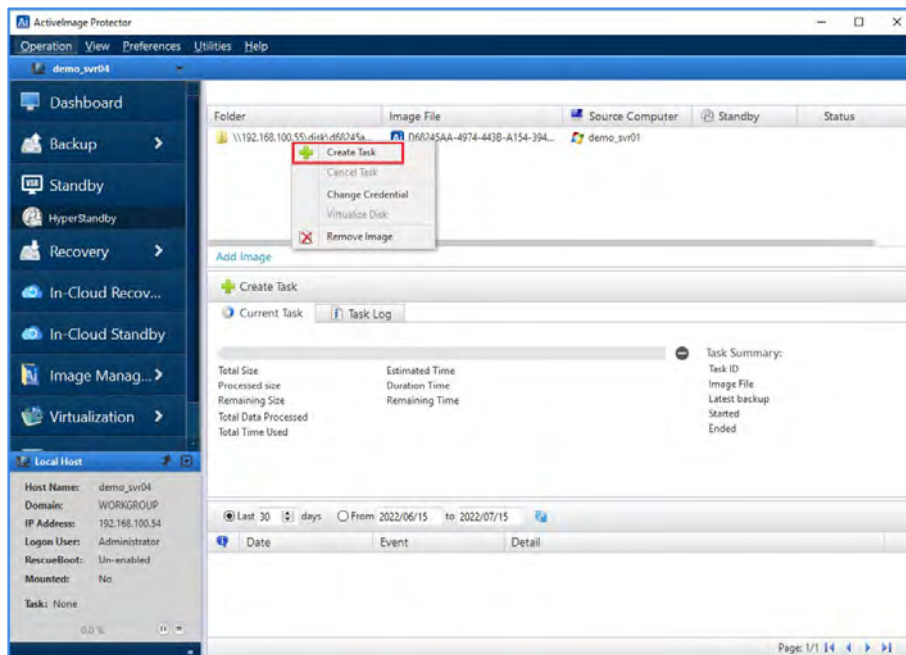


Creates and maintains dormant virtual replicas

- The backup is added to the image list.



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



Creates and maintains dormant virtual replicas

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

Source: \\192.168.100.55\disk\7bab6c18-b299-499b-a893-5adb32f7c Browse...

Profile Name: demo\_svr01220721184447

Image Info | Disk Map | Disk List

Folder name: //192.168.100.55/disk/7bab6c18-b299-499b-a893-5adb32f7dc2b  
Base image: 7BAB6C18-B299-499B-A893-5ADB32F7DC2B\_6430305F30303030315F693030...  
Image version: 6.5.0.7616 (301)  
Source computer: demo\_svr01  
Operating system: Microsoft Windows Server 2016 Standard Edition (build 14393), 64-bit  
CPU: 2  
Memory: 4.00 GB

Cancel Next

9. 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]**. In this case “Administrator” is entered for **[User Name]** and a password for **[Password]**. Click **[Connect]**.

Select Target

☒ Hyper-V ☐ ESXi ☐ Storage Server

Hyper-V Host

192.168.100.60 Connect

Administrator Password

i.e.hostname\username or domain\username

Please enter username!

Host Information

Host Name:  
Domain/Workgroup:  
Operating System:  
CPU:  
Memory:

Cancel Back Next



10. Please review the host information and click **[Next]**.

Create Profile

Source Target Standby Settings Schedule Option Summary

Select Target

☒ Hyper-V ☐ ESXi ☐ Storage Server

Hyper-V Host

192.168.100.60 Connect

Host Information

Host Name:	HYPER-V01
Domain/Workgroup:	WORKGROUP
Operating System:	Microsoft Windows Server 2016 Standard
CPU:	8
Memory:	15.87GB

Cancel Back 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 backup source and firmware are automatically selected to be the same as the source. Please note, when selecting firmware that differs from the backup source, the virtual machine may fail to boot. For **[Virtual Switch:]** and **[IP Address:]** the same values as the source have been selected. After configuring the settings, click **[Next]**.

Create Profile

Source Target Standby Settings Schedule Option Summary

Configure Standby Virtual Machine

VM Setting:

VM Name: demo\_svr01220721185034

VHD(X) Name: demo\_svr01220721185034

Select Volume: D: (free space 567.36GB)

Select Folder: D:\Virtual

Disk type: ☒ Dynamic ☐ Fixed

CPU (max:8): 2 RAM (max:15): 4 GB

System Settings:

Operating System: Windows Server 2016 (64 bit) Firmware: UEFI

Network Settings:

Virtual Switch: Virtual Switch 01 IP Config: DHCP

Add NIC

Cancel Back Next

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

The screenshot shows the 'Create Profile' dialog box with the 'Schedule' tab selected. The progress bar at the top indicates the current step is 'Schedule'. The 'Schedule' section has the following options:

- ☒ **Immediate** (highlighted with a red box)
- ☐ After each 2 new incremental file
- ☐ At 21:00

Schedule Type: ☒ Weekly ☐ Monthly

Days: ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Buttons: Cancel, Back, **Next** (highlighted with a red box)

13. Configure the options settings. Specify the maximum limit for the number of boot points to create virtual standby replicas (up to 30). When the specified number of the boot points reaches the predefined limit, the oldest boot points are merged. 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.

The screenshot shows the 'Create Profile' dialog box with the 'Option' tab selected. The progress bar at the top indicates the current step is 'Option'. The 'Option' section has the following settings:

- ☒ **Only create most recent incremental image boot point** (highlighted with a red box)
- Always keep 30 boot points per each image set (highlighted with a red box)

Option: ☐ Sending Email Task Success and Failure

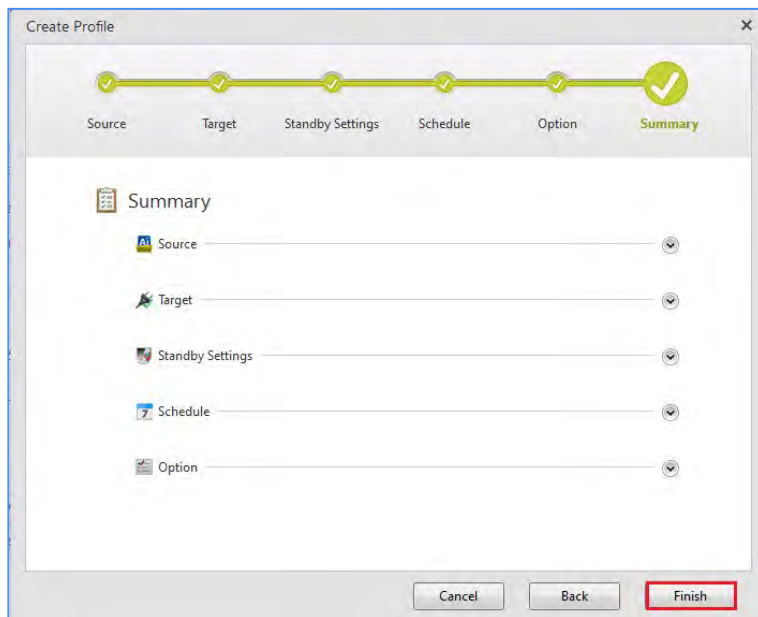
Performance:

- Execution Priority: Lowest Low Medium High
- I/O Performance: Light Fast
- ☐ Use network throttling
- Bandwidth Limit: 200 KB/Sec.

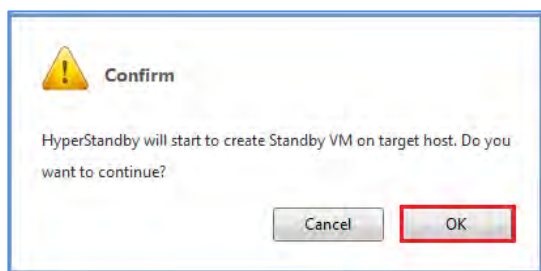
Buttons: Cancel, Back, **Next** (highlighted with a red box)

Creates and maintains dormant virtual replicas

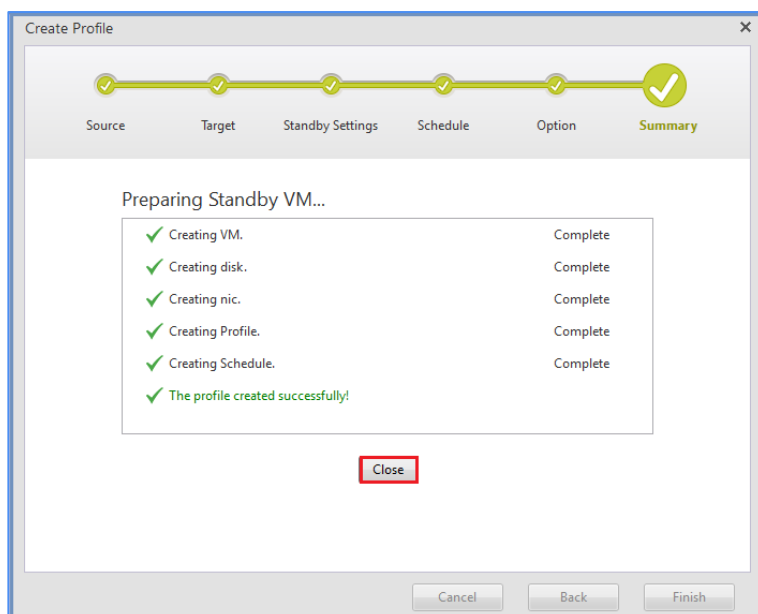
14. When option settings are configured, click **[Finish]**. The following **[Summary]** dialog is displayed.



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

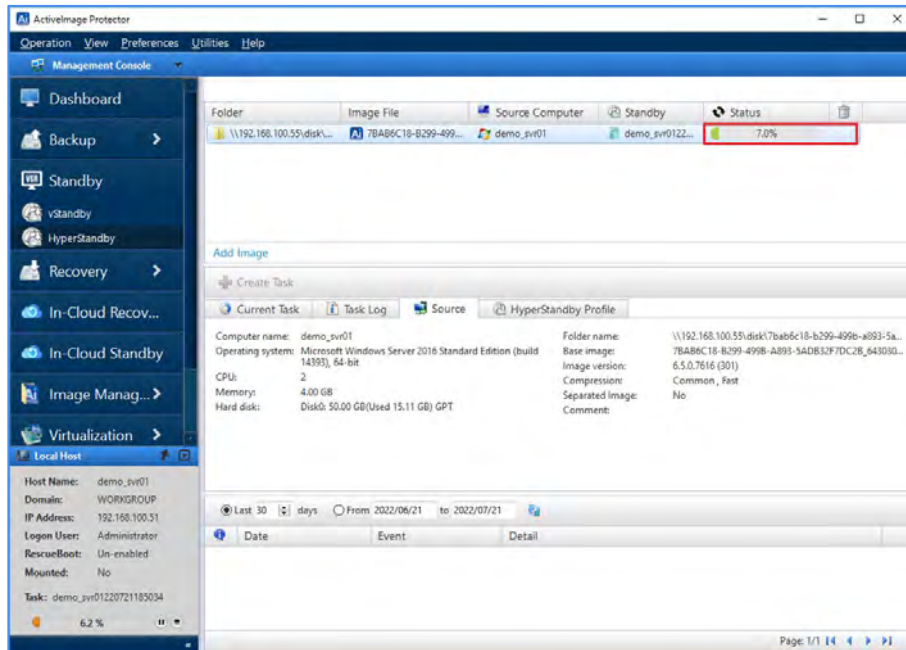


16. When virtual standby machine and profile creation process completes, the following dialog is displayed. Click the **[Close]** button and the **[Dashboard]** window will be displayed.

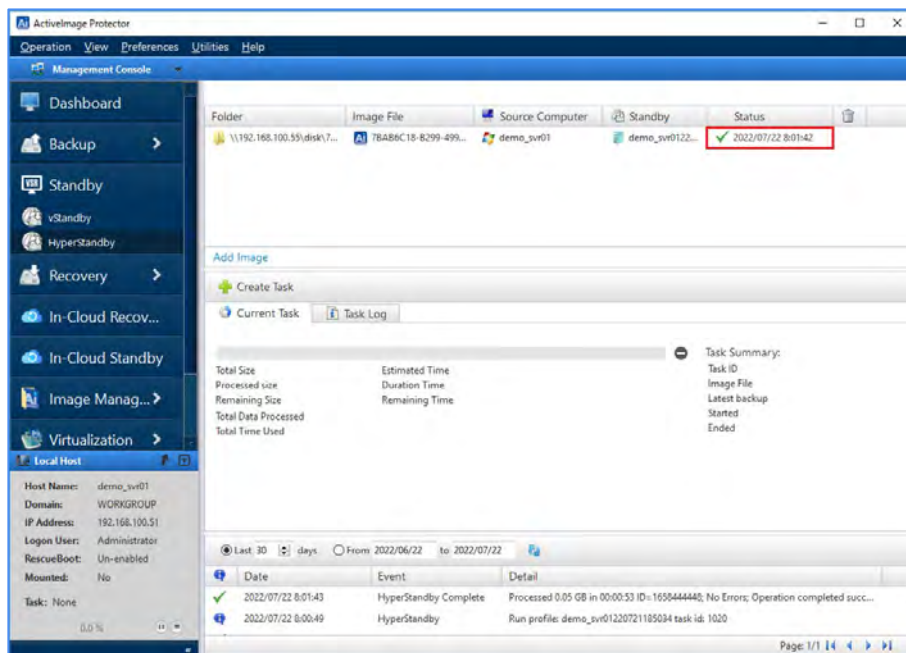


Creates and maintains dormant virtual replicas

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

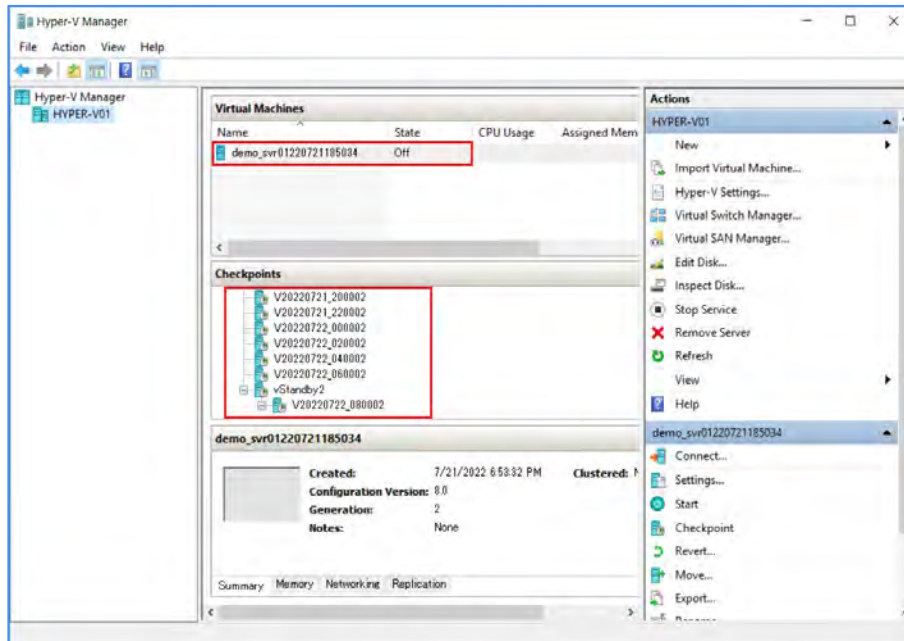


18. Upon completion of a task, the information window is displayed in the dashboard.



Creates and maintains dormant virtual replicas

19. You can also monitor virtual standby machines from Hyper-V Manager. Checkpoints are added for the virtual standby machine as backups complete.

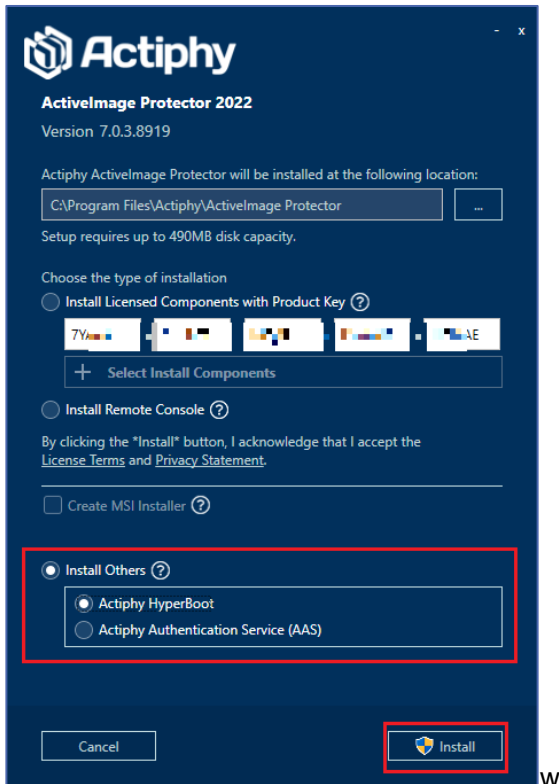




### 11-3.HyperBoot

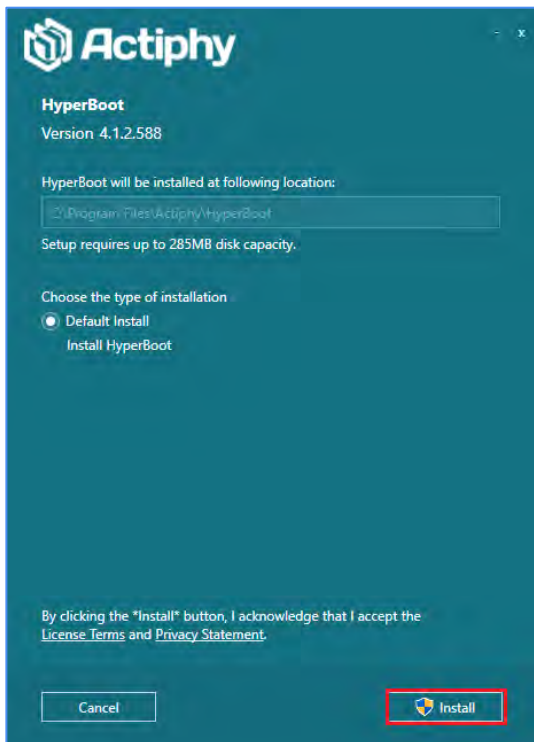
HyperBoot is a free standalone add-on that can boot any ActiImage Protector backup image as a virtual machine in minutes, bypassing lengthy physical to virtual conversion and recovery process. You can install HyperBoot from the ActiImage Protector installer in the product media. The following is a description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

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

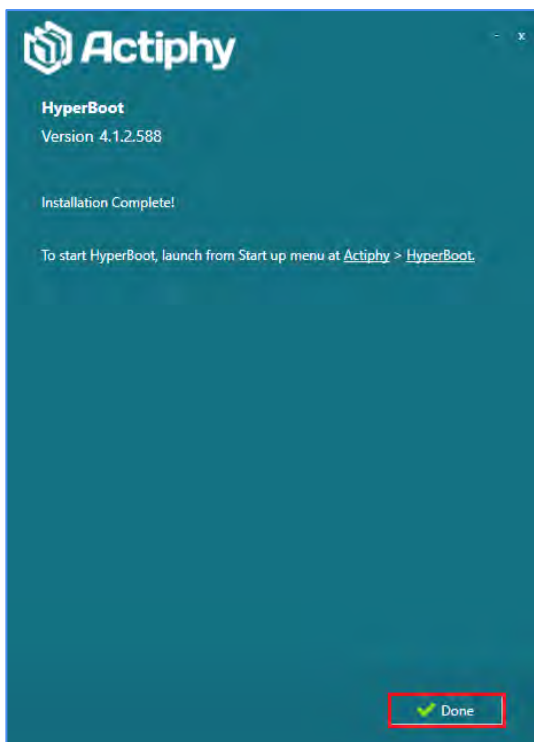


Creates and maintains dormant virtual replicas

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

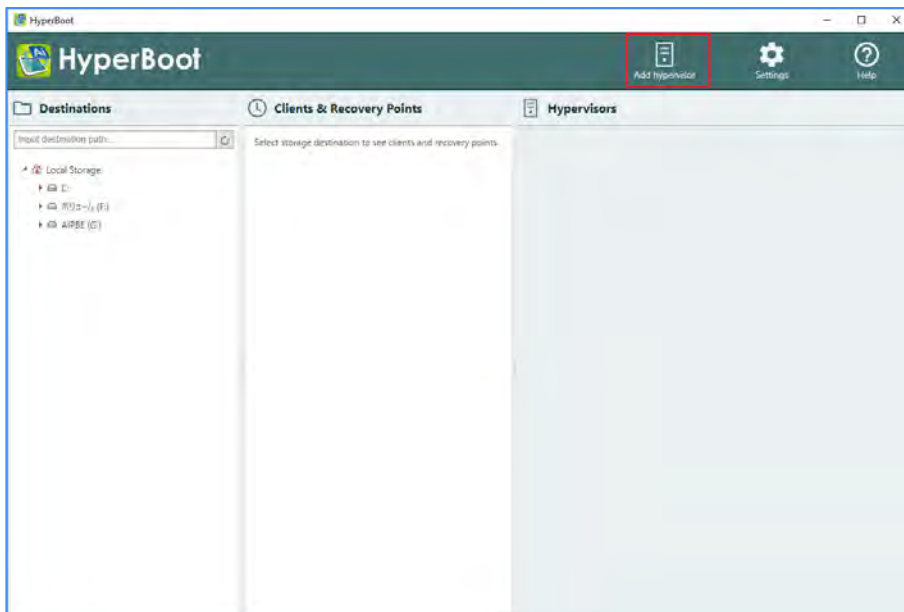


3. When the following window is displayed, installation process completed. Click **[Done]** to end the setup wizard.

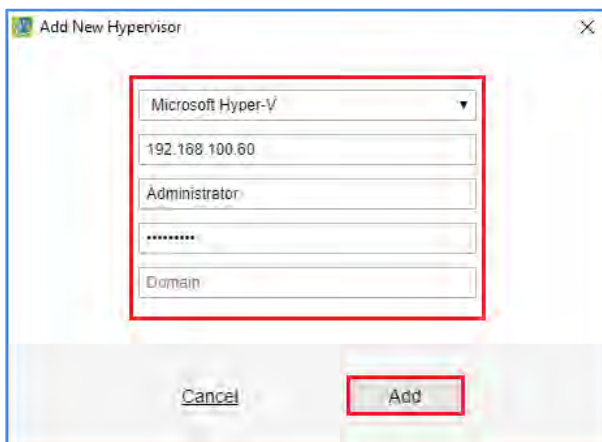


Creates and maintains dormant virtual replicas

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

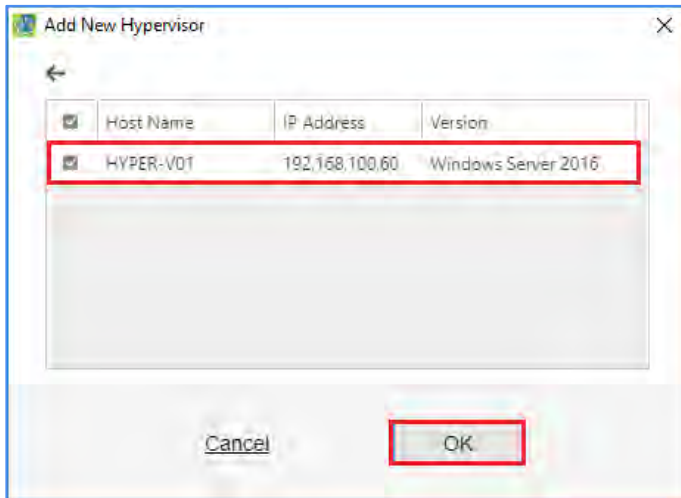


6. This example shows that "Hyper-V" is selected for **[Add Target:]**, IP address of Hyper-V host "192.168.100.60" for **[Host Name or IP address:]**, "Administrator" for **[User Name:]** and Password. Click **[Add]**.

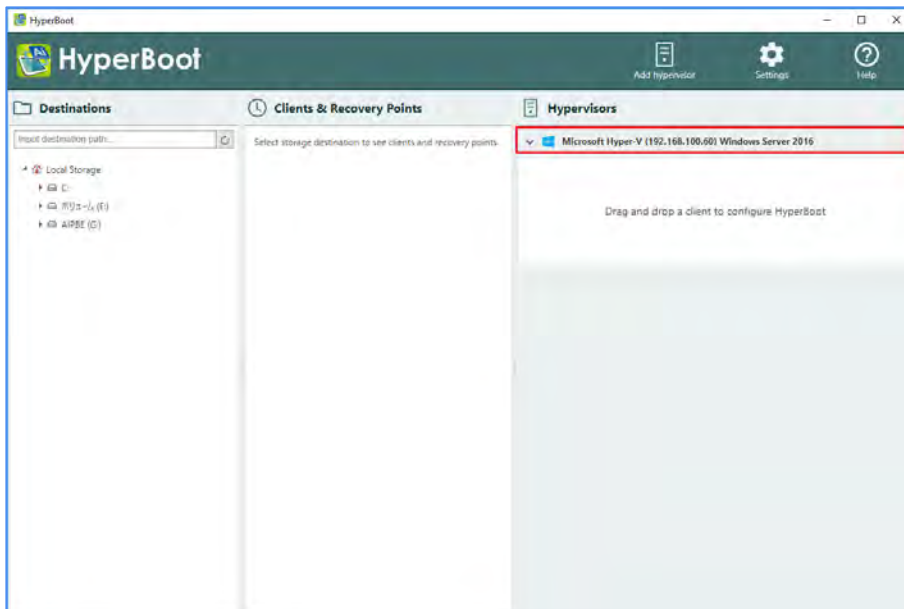


Creates and maintains dormant virtual replicas

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

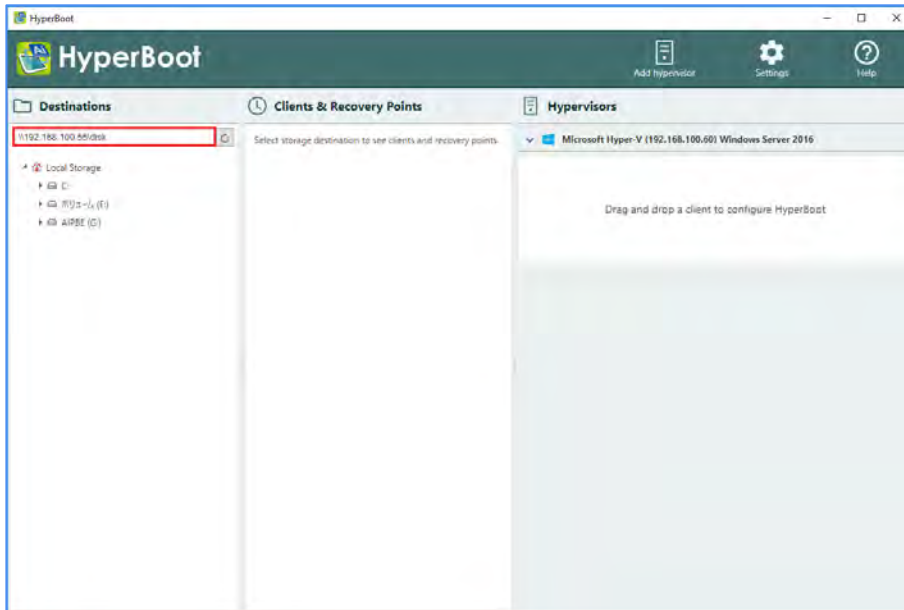


8. In the console you can confirm that Hyper-V has been added to **[Hypervisors]**.

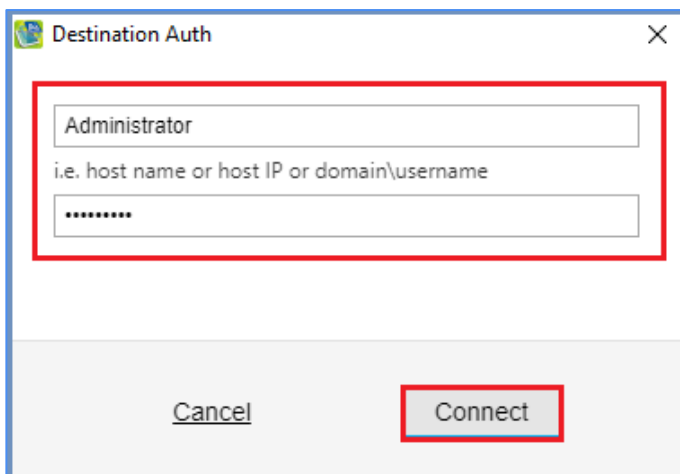


Creates and maintains dormant virtual replicas

9. Select the recovery point of Axiemage 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.



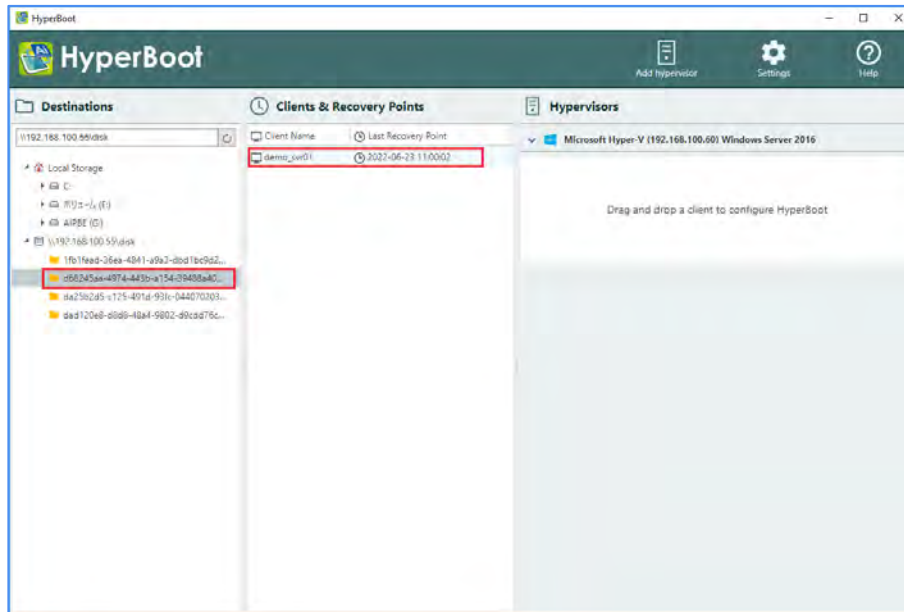
10. In **[Destination Auth]** dialog, please enter your credentials for the shared folder, [User Name:] and [Password]. Click **[Connect]**.



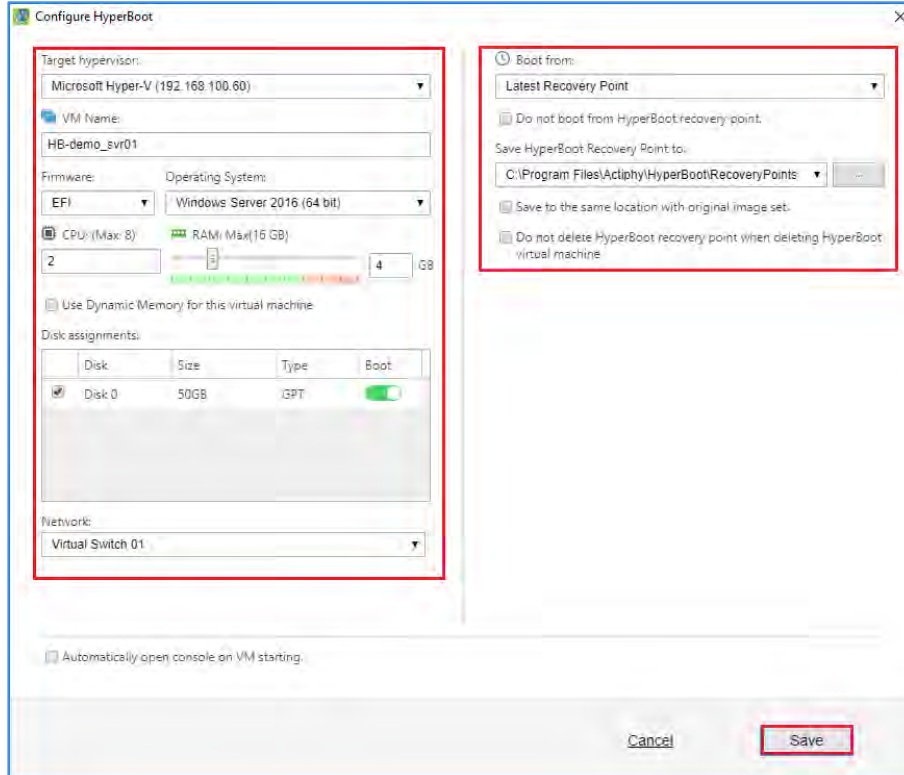


Creates and maintains dormant virtual replicas

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

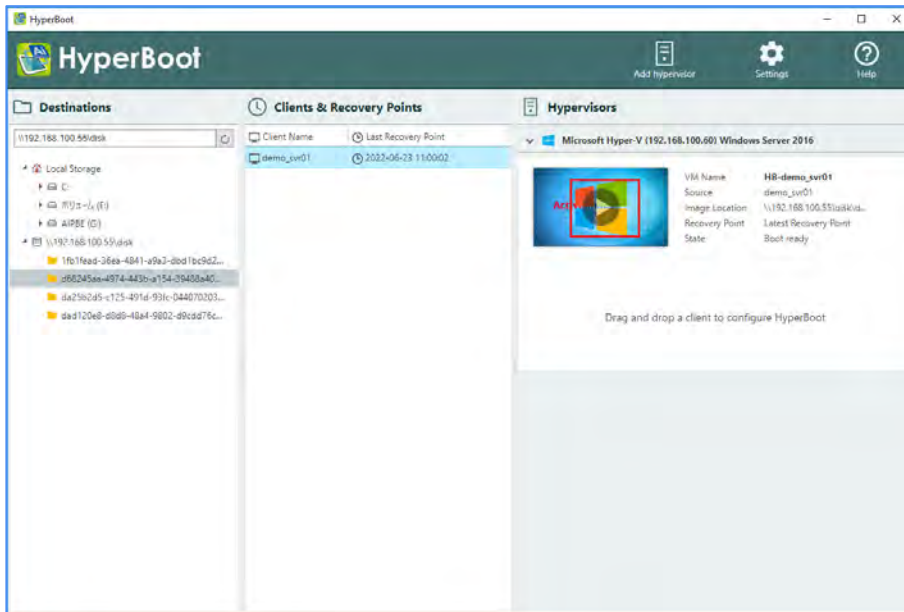


12. In this example, "Microsoft Hyper-V" is selected for **[Target hypervisor]**. Please configure the settings for **[CPU]**, **[RAM]**, **[Network]**, etc. If necessary, please change **[VM Name:]**. A default path is configured for the setting **[Save HyperBoot Recovery Point to:]**. However, enabling **[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]**.

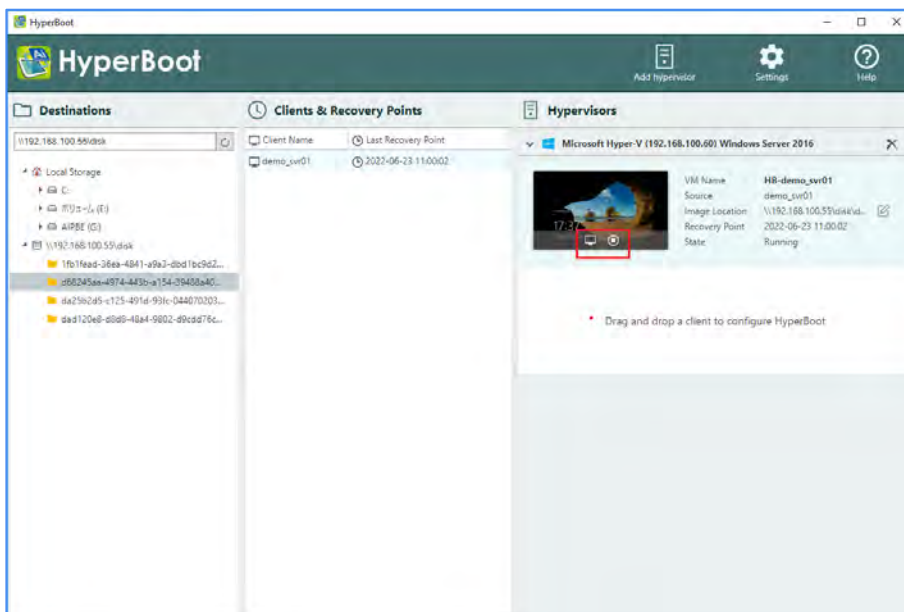


Creates and maintains dormant virtual replicas

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

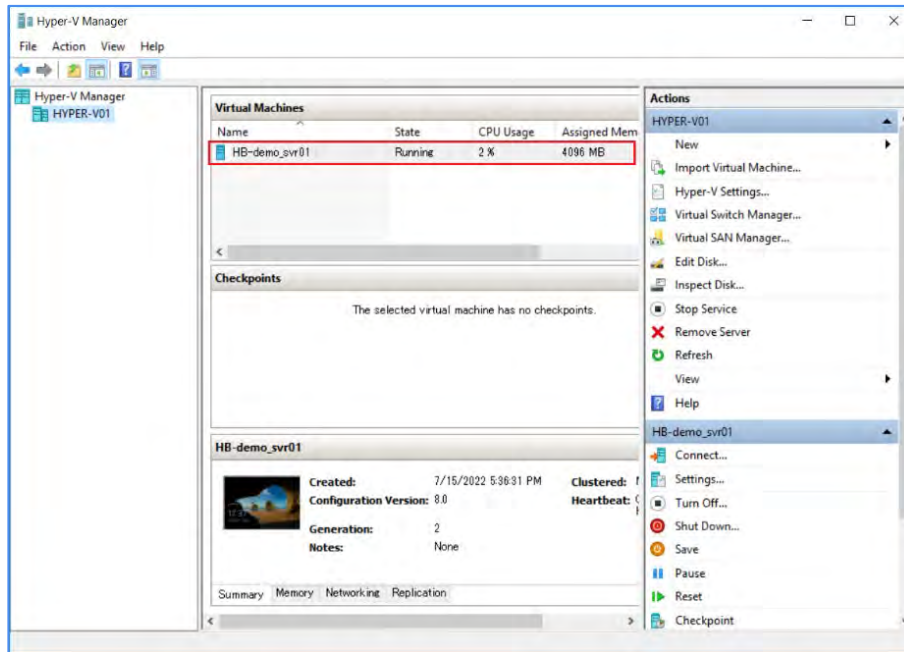


14. Click on the left icon to launch the VM connection console.

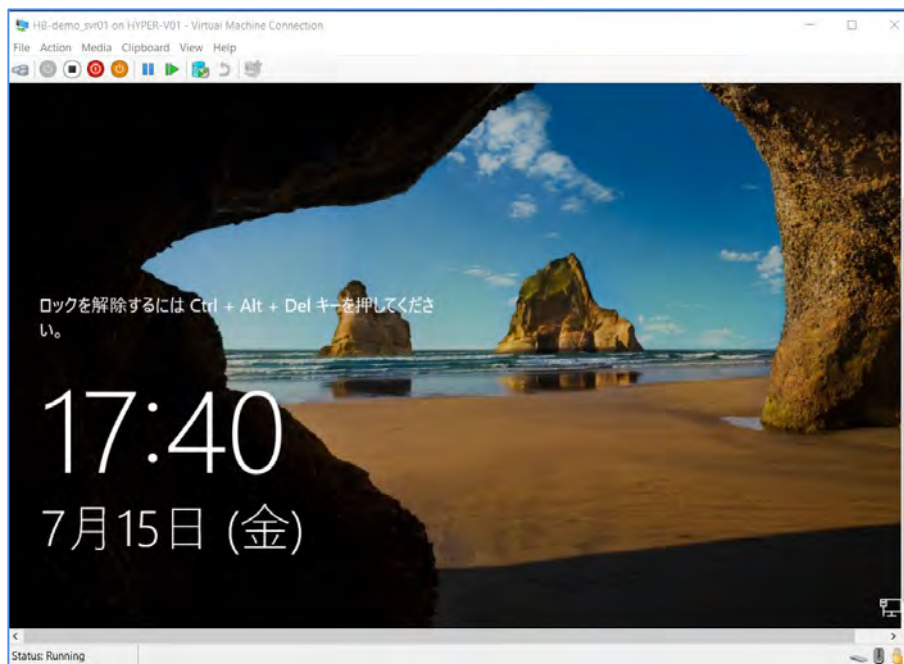


Creates and maintains dormant virtual replicas

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

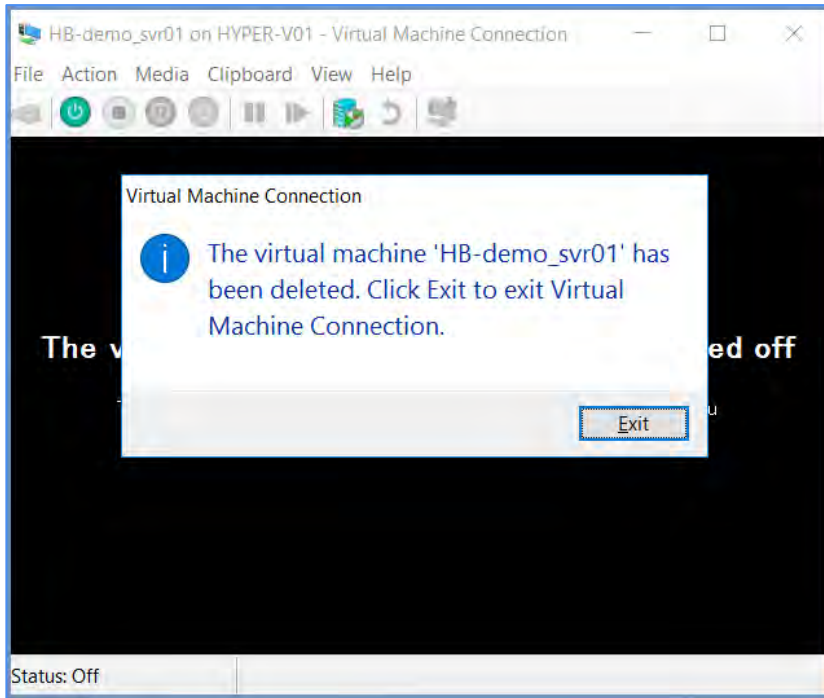


16. You can access the virtual machine through the Hyper-v console.



Creates and maintains dormant virtual replicas

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



## 12. 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/>
- **ActiveImage Protector Help Center**  
Support information is accessible at the following web site.  
<https://actiphyhelp.zendesk.com/hc/en-us>
- **For any inquiries about ActiveImage Protector, please contact:**  
Global Sales Dept., Actiphy Inc.  
E-mail: [global-sales@actiphy.com](mailto:global-sales@actiphy.com)

© 2024 Actiphy, Inc. Actiphy, Inc. All rights reserved.

ActiveImage 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.