ActiveImage Protector 2022 Linux

Setup Guide

3rd Edition (February, 2024)

Actiphy

CONTENTS

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 Linux (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/linux/2022/en_US/).

1.1. System Requirements

Please ensure your computer meets these minimum system requirements before using ActiveImage Protector 2022 Linux Version 7.0.3.8919:
For the latest system requirements, please access Actiphy's Web site (https://www.actiphy.com/global/support/system-requirements/).

CPU	Pentium 4 or newer.
Main Memory（RAM）	2GB of RAM or greater.
Hard Disk	2GB of available disk space or greater.
DVD-ROM drive	Required to install the product and boot up the ActiveImage Protector Boot Environment.
Internet	An Internet connection is required to activate the product.
Supported OS	・Red Hat Enterprise Linux：9.0 – 9.3 / 8.0 – 8.9 / 7.0 – 7.9 ・CentOS：8.1 – 8.4 / 7.0 – 7.9 ・Oracle Linux：9.0 – 9.3 / 8.1 – 8.9 / 7.0 – 7.9 ・AlmaLinux 9.0 – 9.3 / 8.3 – 8.9 ・MIRACLE LINUX 9.0, 9.2 / 8.4, 8.6, 8.8 ・Rocky Linux 9.0 – 9.3 / 8.3 – 8.9 ・Amazon Linux 2 ・SUSE Linux Enterprise Server 15 / Desktop 15 ・OpenSUSE Leap 15 ・Ubuntu 18.04LTS / 20.04LTS / 22.04LTS ・Debian 9 – 12 * ActiveImage Protector Linux Edition only supports the x86_64 architecture. * SecureBoot is not supported.

2. Installation

2-1. Advance preparation before setting up ActiveImage Protector

Before setting up ActiveImage Protector, you need to install the required Linux packages. You can use the [AIP-packages-tool] found on your ActiveImage Protector installation disc to facilitate the installation of the required packages and drivers. The **[AIP-packages-tool]** automatically detects, downloads, and installs the required packages.

Note: Your computer must have an Internet connection to install ActiveImage Protector and the required packages and drivers. If your system does not have Internet access, please refer to the "Install and start ActiveImage Protector" section in the online help (https://webhelp.actiphy.com/AIP/linux/2022/en_US/).

1. Log in as the root user.
2. Mount the installation disc. In this example, we create a new mount point in the /mnt directory using the mkdir command. Then, we mount the disc using the mount command.

   Note: The device name /dev/cdrom may differ depending on your Linux environment. If you get an error when attempting to mount /dev/cdrom, please search for another likely device name in the /dev directory and replace /dev/cdrom with this alternative device name.

   ```
   # mkdir /mnt/cdrom
   # mount -t iso9660 /dev/cdrom /mnt/cdrom
   ```

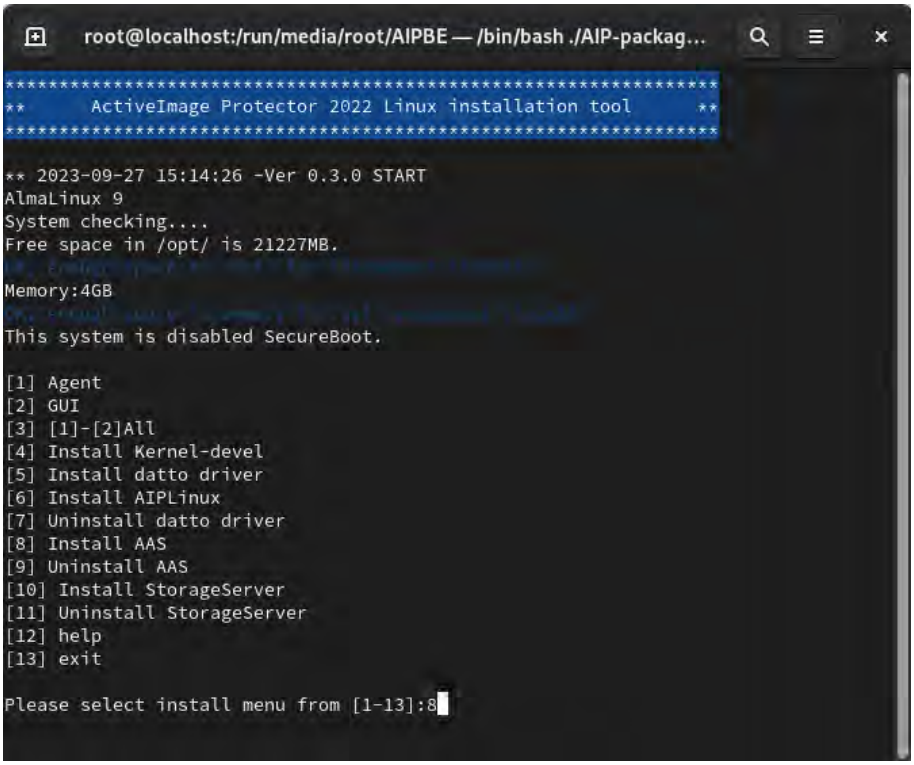
3. Once you successfully mount your installation disc, you'll be able to access its contents in the /mnt/cdrom directory.

   ```
   # cd /mnt/cdrom
   # ls
   AIP-packages-tool.sh  Documents  Lanch.ini        TRANS.TBL  iso       scripts
   AIP.ico               EFI        Launcher         autorun.inf  isolinux
   AIPlinuxInstaller     EULA       Rebuild_by_user  boot       live
   DEBIAN_LIVE           Launch.exe setup            buildNum   packages
   ```

4. Run the [AIP-packages-tool.sh] script from the terminal.

   ```
   # cd /mnt/cdrom
   # ./AIP-packages-tool.sh
   ```

5. You will see the following message when you run the **[AIP-packages-tool]**. In this example, the script runs steps **[3]**, **[4]**, and **[5]** in order and installs the required packages and drivers. You don't have to reboot your system after the installation completes.



[1] **Agent**: Installs the modules necessary for using ActiveImage Protector agents.

[2] **GUI**: Installs the modules necessary for using ActiveImage Protector GUI.

[3] **[1]-[2]All**: Installs both ActiveImage Protector agents and the GUI.

[4] **Kernel-devel**: Installs the kernel-supported version of Kernel-devel.

[5] **Install Datto driver**: Installs the Datto driver (Incremental backups tracking driver).

[6] **Install AIPLinux**: Installs ActiveImage Protector Linux.

[7] **Uninstall Datto driver**: Uninstalls the Datto driver.

[8] **Install AAS**: Installs the Linux AAS (Actiphy Authentication Service).

[9] **Uninstall AAS**: Uninstalls the Linux AAS (Actiphy Authentication Service).

[10] Install StorageServer: Install Actiphy StorageServer.

[11] Uninstall StorageServer: Uninstall Actiphy StorageServer.

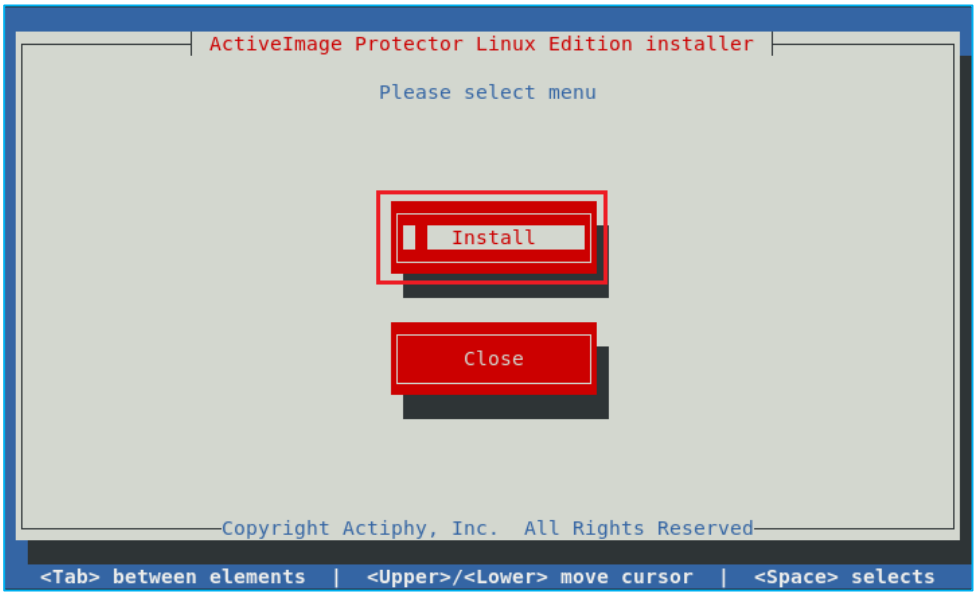
[12] help： Help

[13] exit： Exit.

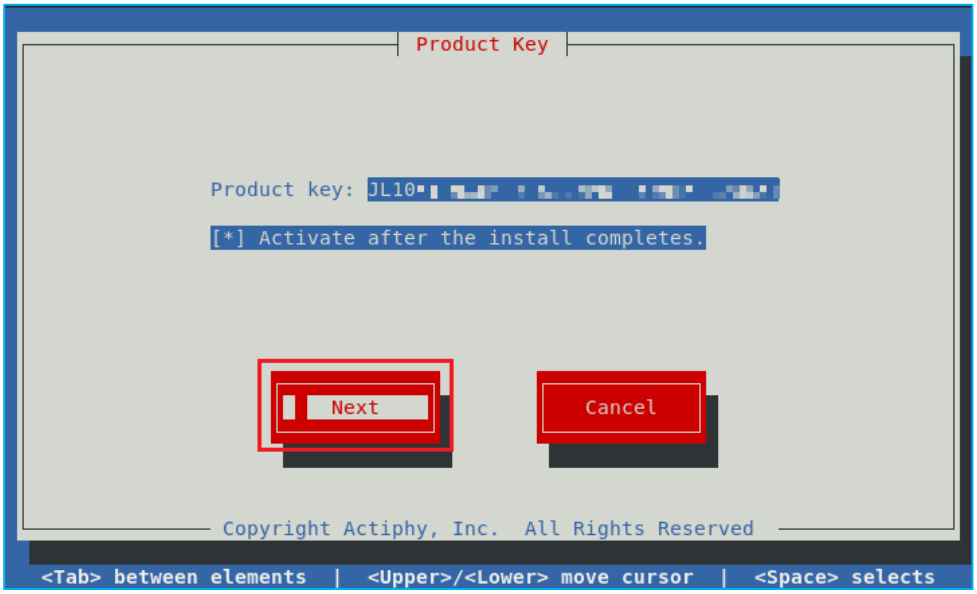
2-2. Installation

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

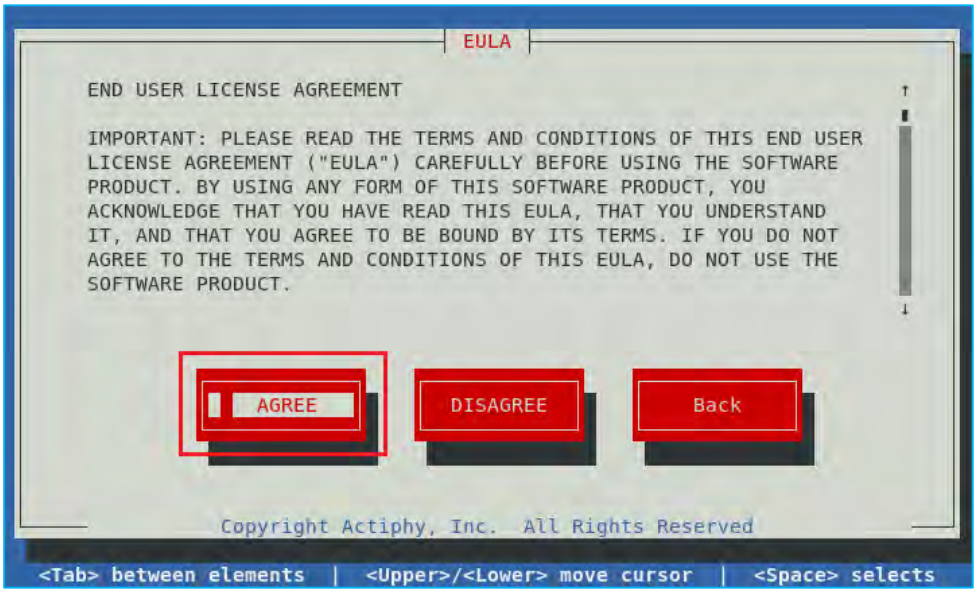
1. Run **[[6] Install AIPLinux]** from the menu of the script "AIP-packages-tool" and start the installer. Or, run the installer "AIPLinuxInstaller" from the product media.
2. When the installer starts, select **[Install]** and press **Enter** key.
   Note: You can only operate the Terminal using a keyboard. Use the **Tab** or arrow keys to move the cursor between fields. Use the **Space** or **Enter** key to select an item.



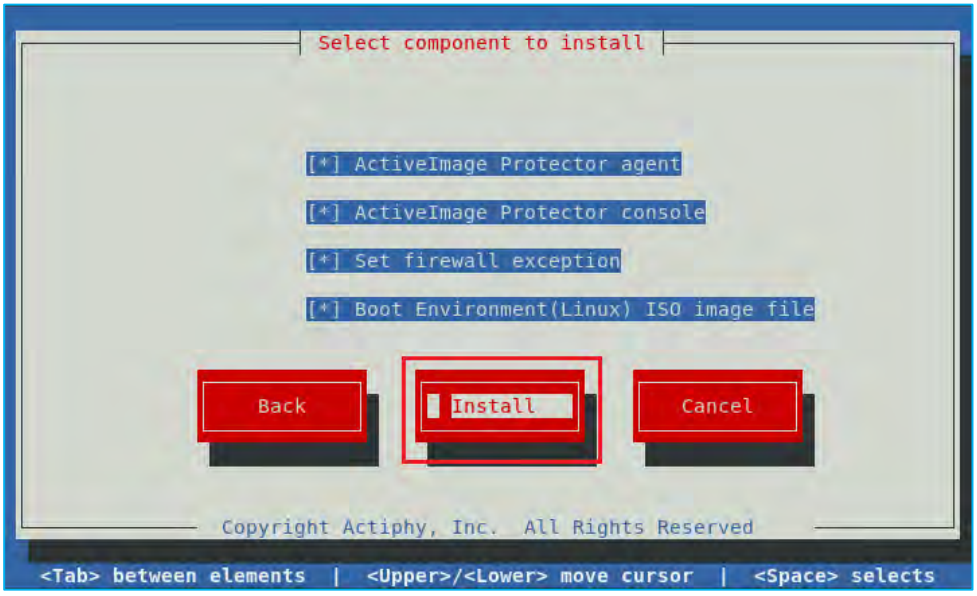
3. Enter the product key and select the **[Activate after the install completes]** option. Select **[Next]**, and press the **Enter** key. The product activation will start automatically once the installation completes.



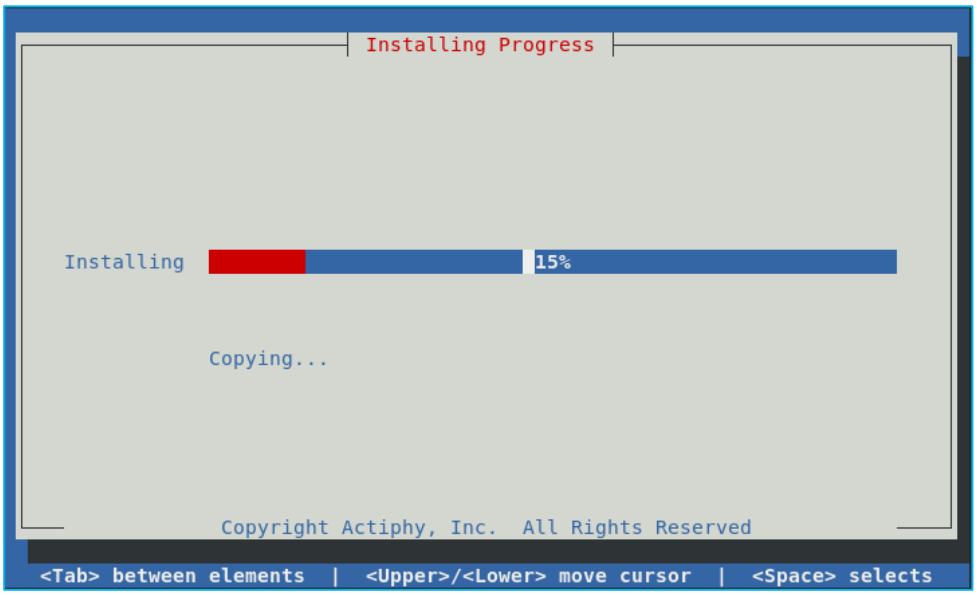
4. Read the End User License Agreement carefully, select **[AGREE]** to proceed with the installation, and then press the **Enter** key.



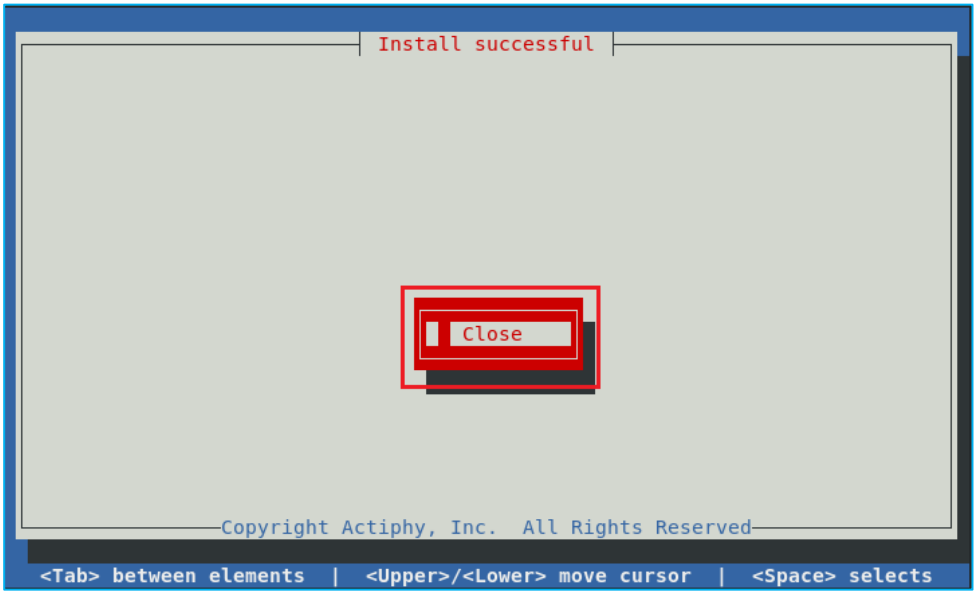
5. Select all components, select the **[Install]** option, then press the **Enter** key.



6. The installer will display a progress bar when you start the installation.



7. Once the installation is complete, you'll see the **[Install successful]** dialog. Select the **[Close]** option and press the **Enter** key to exit the installer. No system reboot is required.

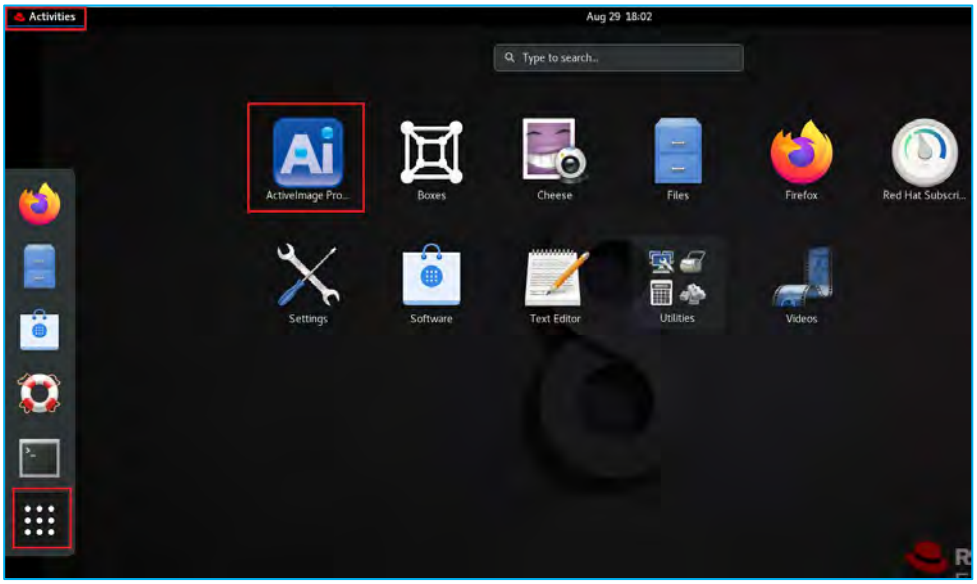


8. Launch ActiveImage Protector GUI.

   When installing the product on Red Hat Enterprise Linux, select **[Activities]** -> **[Display activities]** in the desktop menu and launch ActiveImage Protector's GUI.

   When installing the product on CentOS, select **[Application]** -> **[System Tool]** in the desktop menu and launch ActiveImage Protector's GUI.

   Note: If you're not using a desktop computer, please use ActiveImage Protector's Remote Console to manage the ActiveImage Protector agent. For further information on installing the remote console and connecting to a remote host, please refer to section **8, Remote Management Console,** of this document.



3. Product Activation

ActiveImage Protector supports three types of product activation:

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

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

Note: 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 further information on activating your product, please see the Activation Guide on Actiphy's website.
https://www.actiphy.com/global/support/tech-resource/

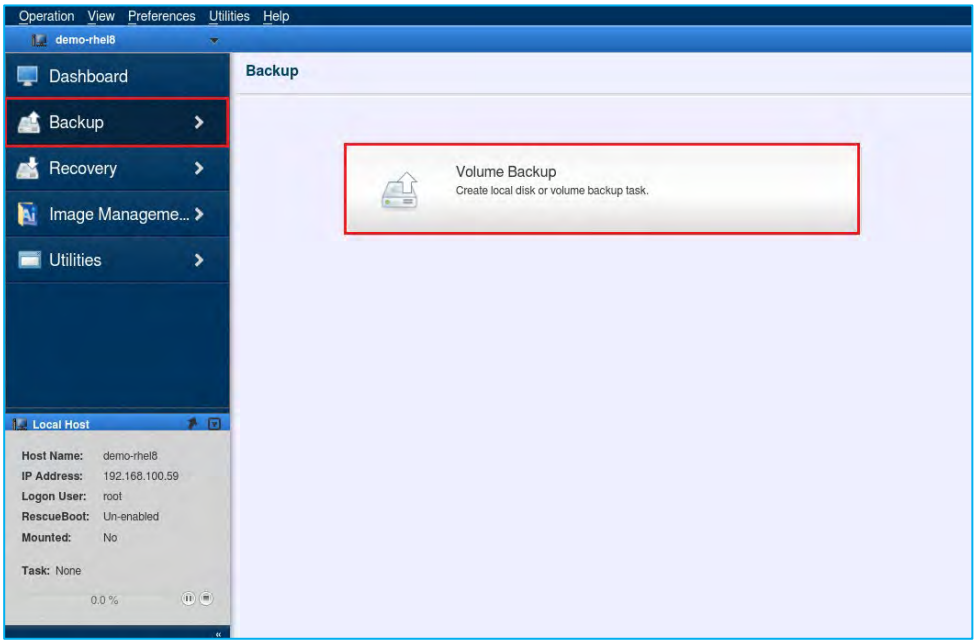
- ActiveImage Protector 2022 Server
  https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_server
- ActiveImage Protector 2022 Desktop
  https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_desktop
- ActiveImage Protector 2022 Linux
  https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_linux
- ActiveImage Protector 2022 Virtual
  https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_virtual
- AAS Docker
  https://www.actiphy.com/global/activation_guide/aas_docker/
- Deactivating License/Bundle File
  https://www.actiphy.com/global/activation_guide/actiphy_activeimage_protector_2022_license_recovery_guide

4. Configure backup settings and run backup tasks

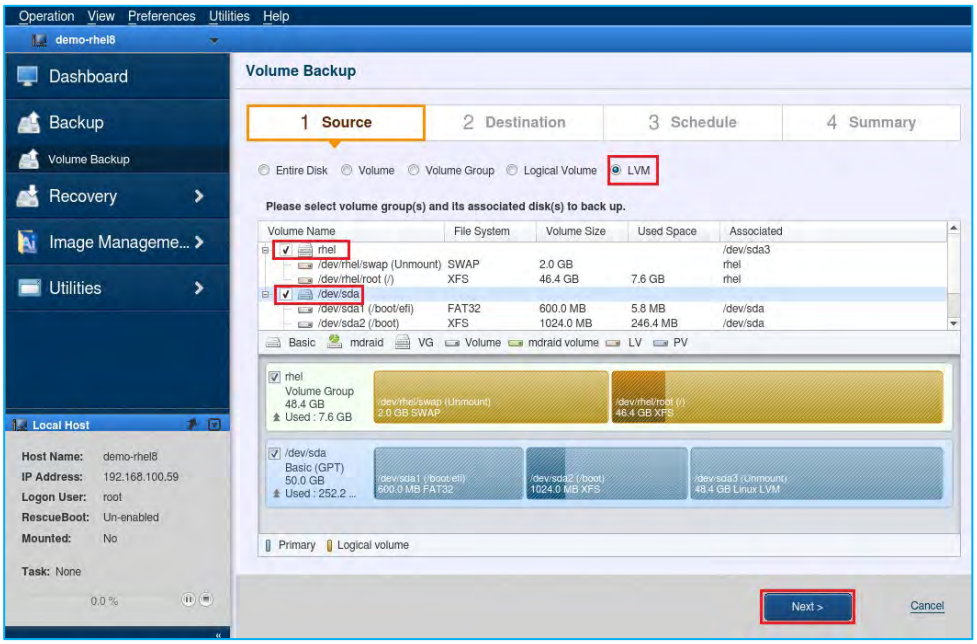
4-1. Volume Backup : One Time Only

Use the following steps to run ad hoc backup tasks:

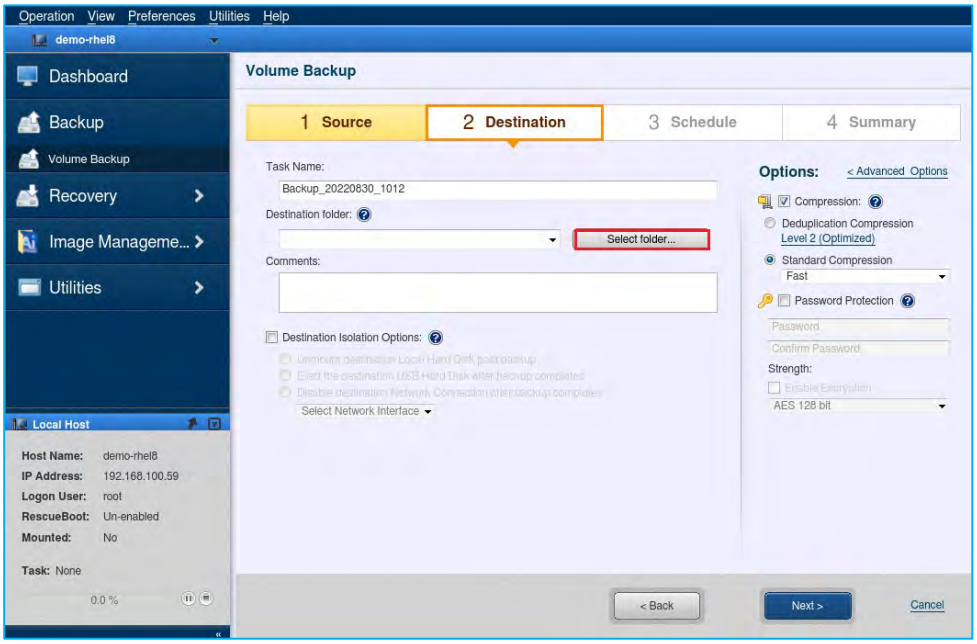
1. Launch ActiveImage Protector's console and select **[Backup]** → **[Volume Backup]** from the left sidebar menu.



2. The following example describes how to back up LVM volumes on Linux computers. In this example, you would:
   - Select **[LVM]** in the **[Source]** window.
   - Select the volume group (VG), "rhel," and its related disks, "/dev/sda," as backup sources.
   - Click the **[Next]** button.



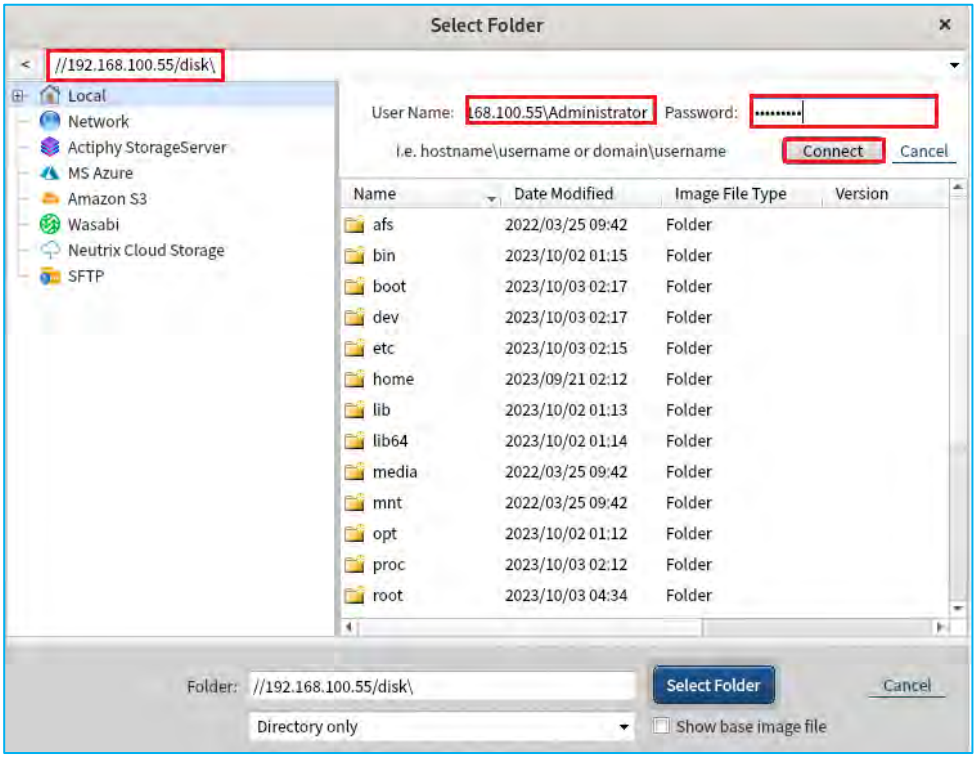
3. Select a destination folder to save the backup image files. In this example, we have selected the network-shared folder “¥¥192.168.100.55¥disk” as the destination. Click the **[Select Folder]** button.



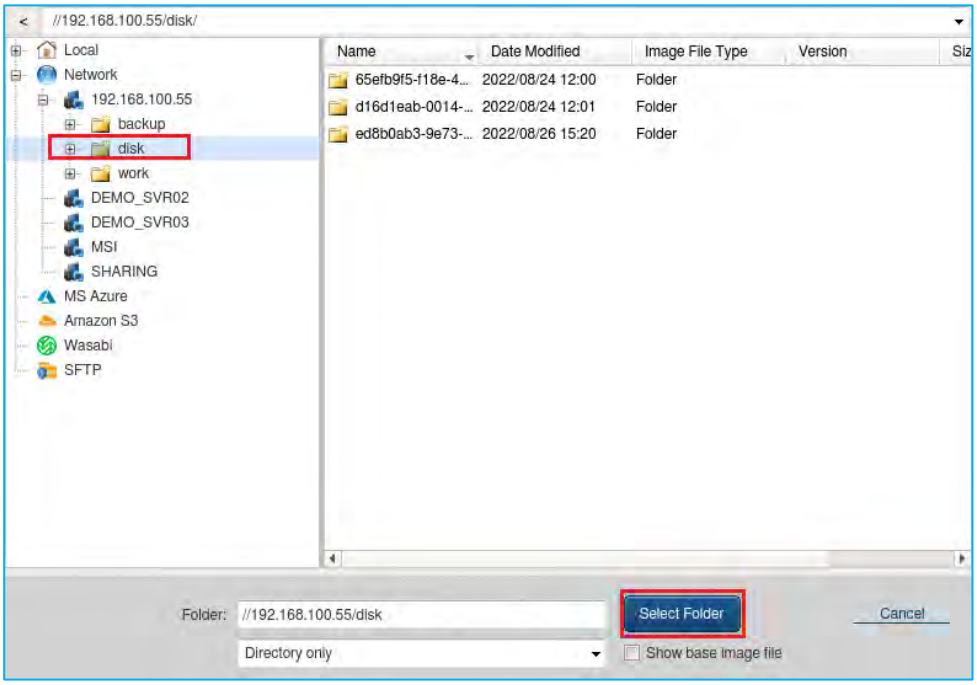
4. Specify a shared folder for the destination storage and press the **[Enter]** key. Then, enter the destination folder's login credentials and click the **[Connect]** button.

   For example, in this screenshot, we're using "¥¥192.168.100.55¥disk" as the destination folder and "192.168.100.55¥Administrator" as the username.

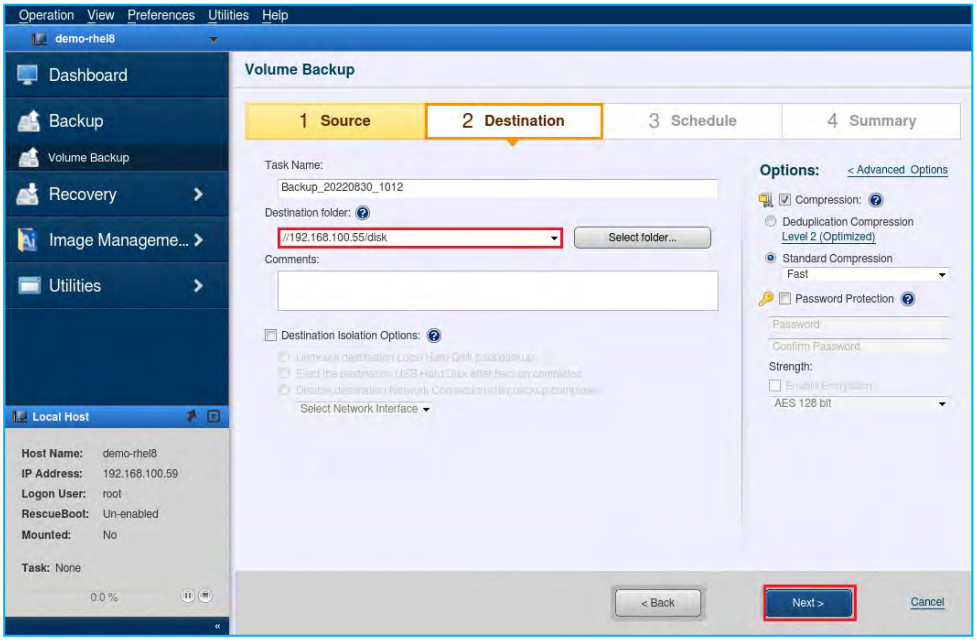
   Enter the password and click the **[Connect]** button.



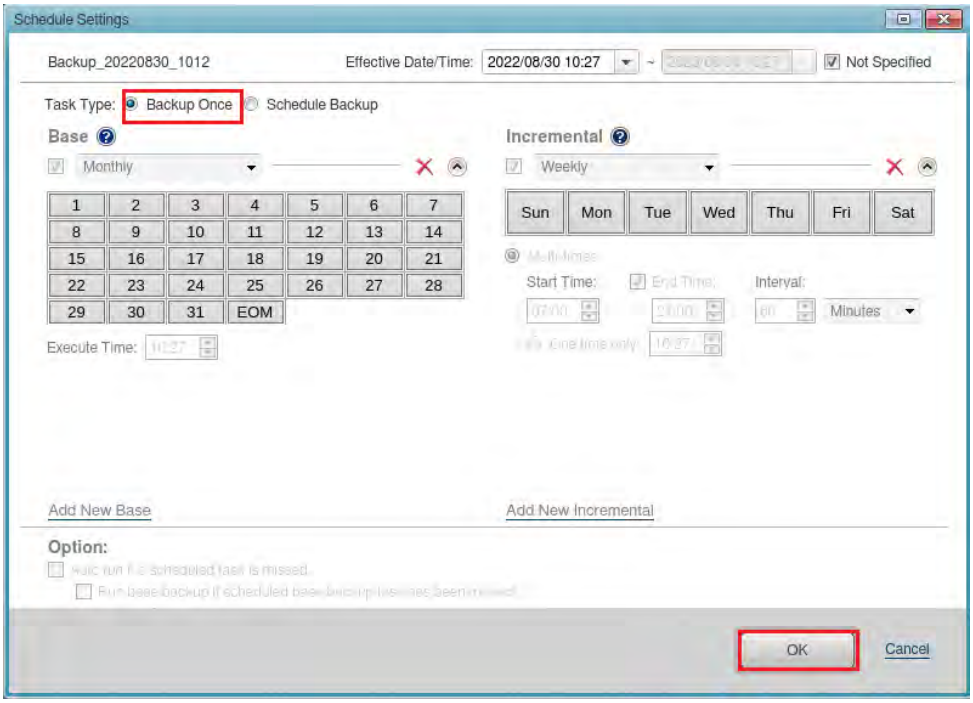
5. Select the shared folder “disk” as the backup destination and click the **[Select Folder]** button.



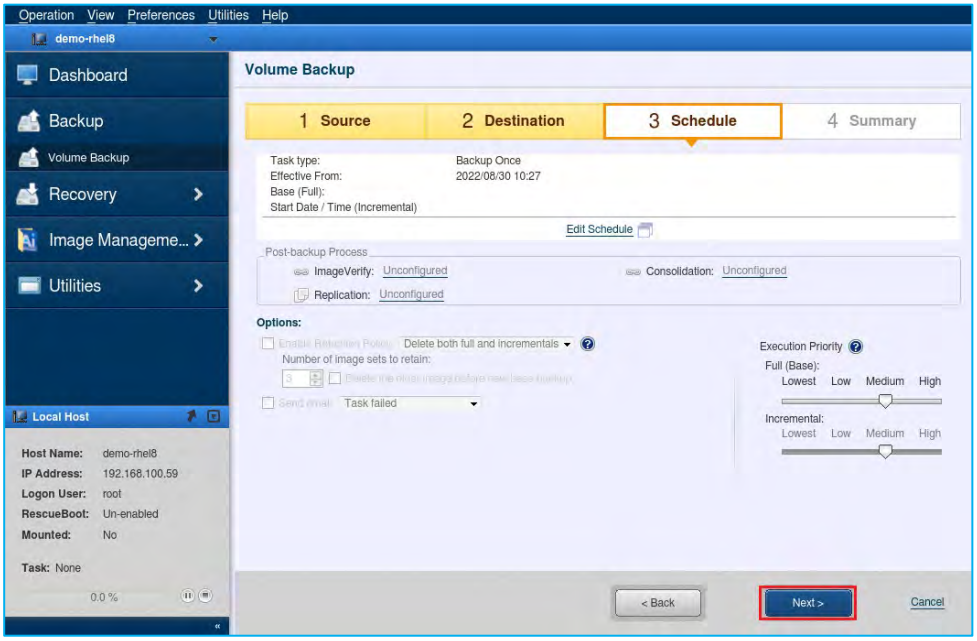
6. On the Destination dialog on the Volume Backup screen, ensure you have filled in the Destination Folder field correctly and click the **[Next]** button. We will review the **[Destination Isolation Options]** and **[Options]** sections later in this document.



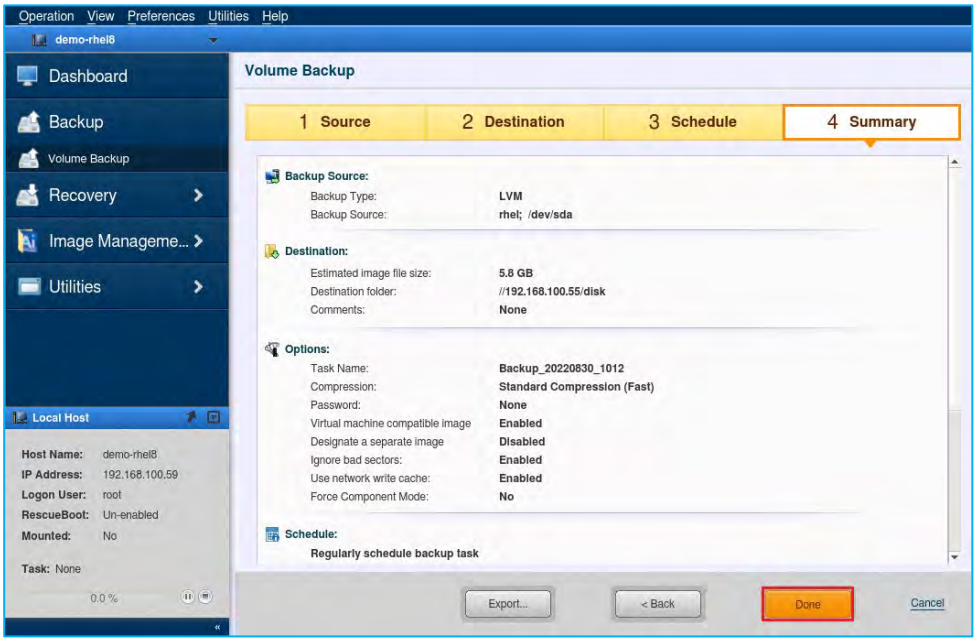
7. On the Destination dialog, select the **[Backup Once]** option for **[Task Type]** and click the [OK] button.



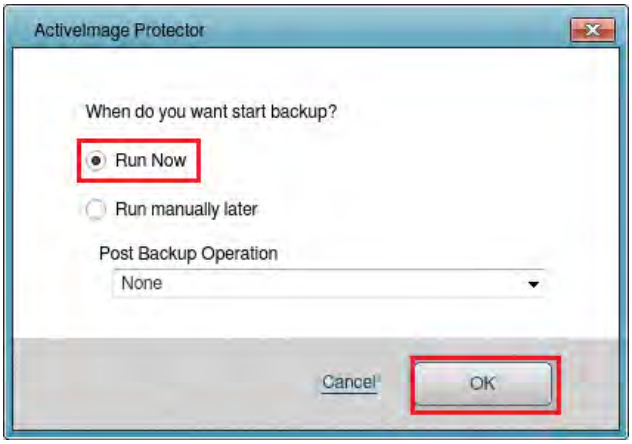
8. Without configuring the schedule settings here, click the **[Next]** button.



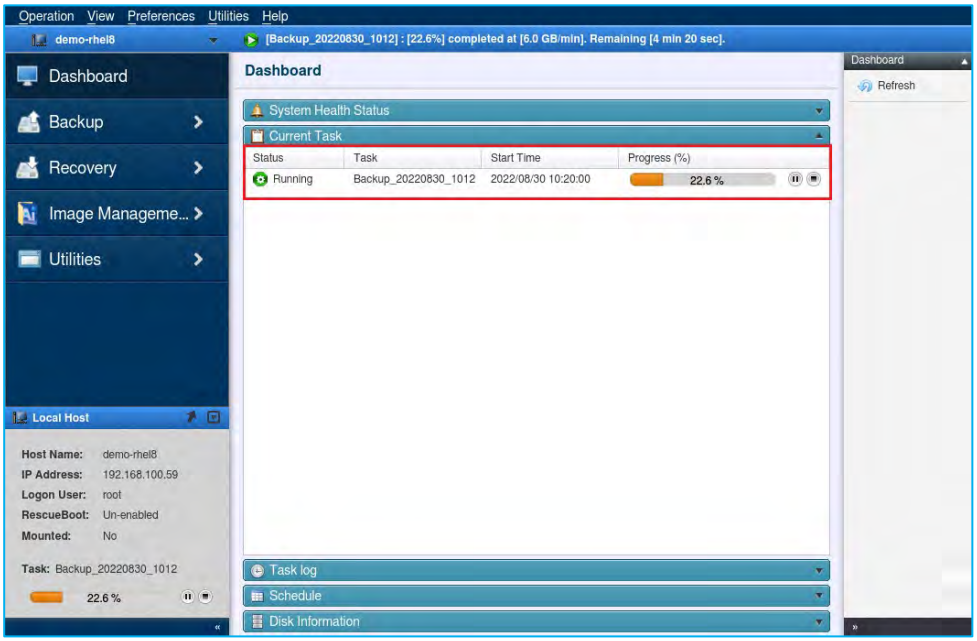
9. After setting up your backup schedule, you should see a summary of your configuration. Please review your backup configuration. If everything looks correct, click the **[Done]** button.



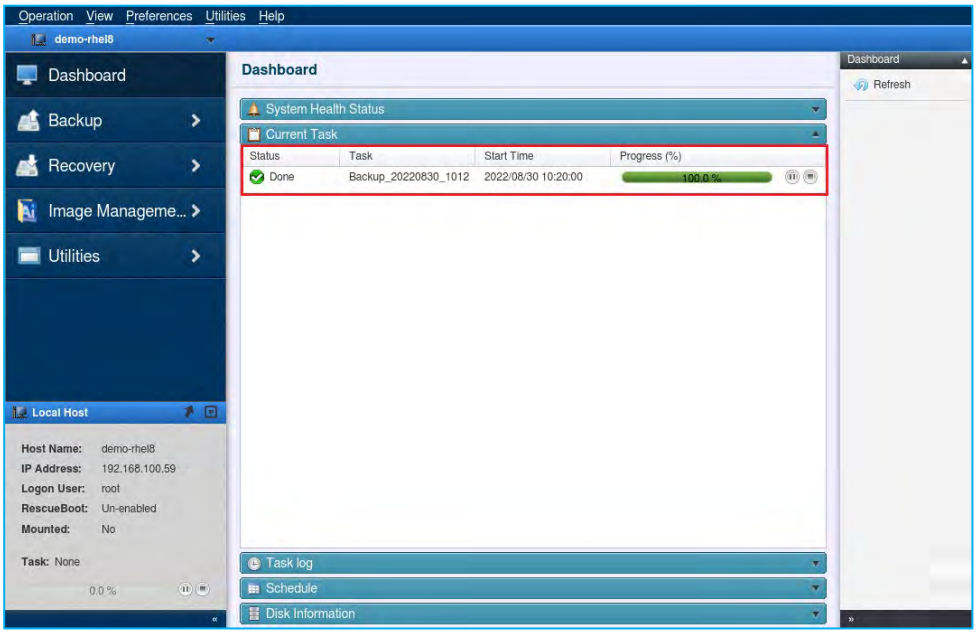
10. Select the **[Run Now]** option and click the **[OK]** button to start the backup task.
    You may select a **[Post Backup Operation]** to shut down or restart the system once the backup is complete.



11. You can monitor the progress of your backup on the Dashboard window after starting your backup.



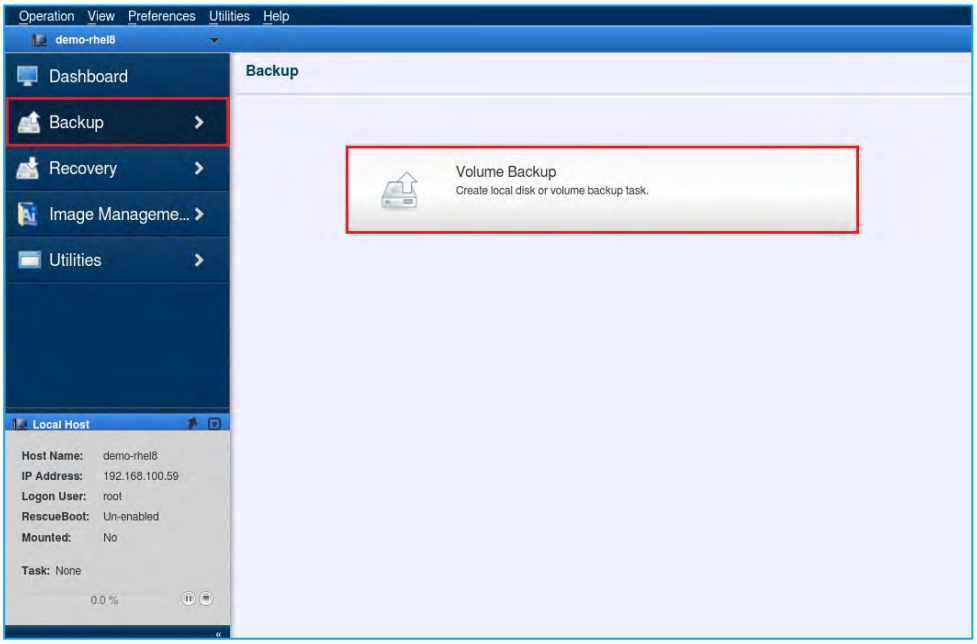
12. When the progress bar reaches 100% the recovery is complete.



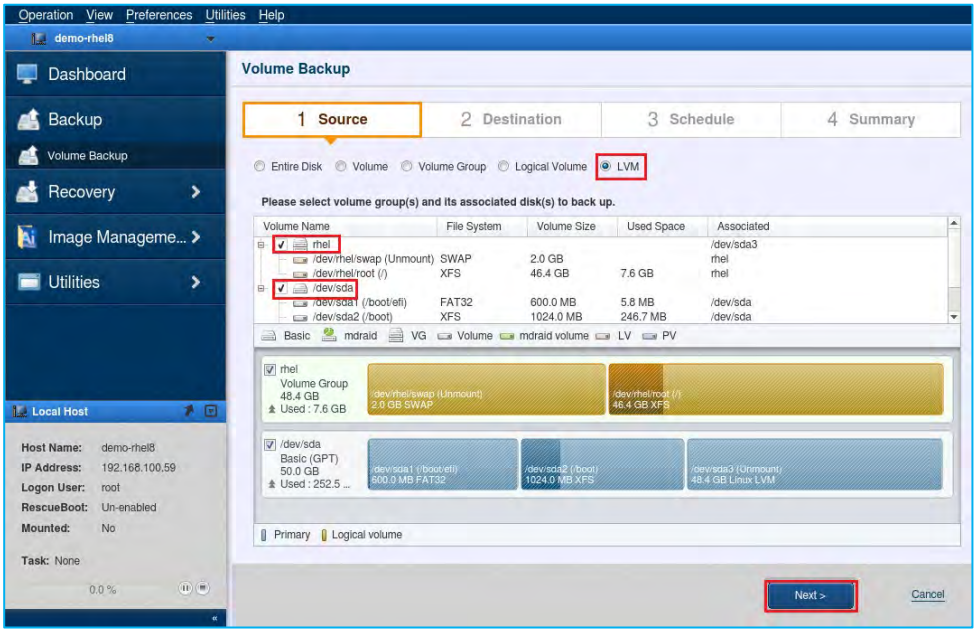
4-2. Volume Backup: Scheduled Backups

Please use the following steps to configure regularly scheduled backups.

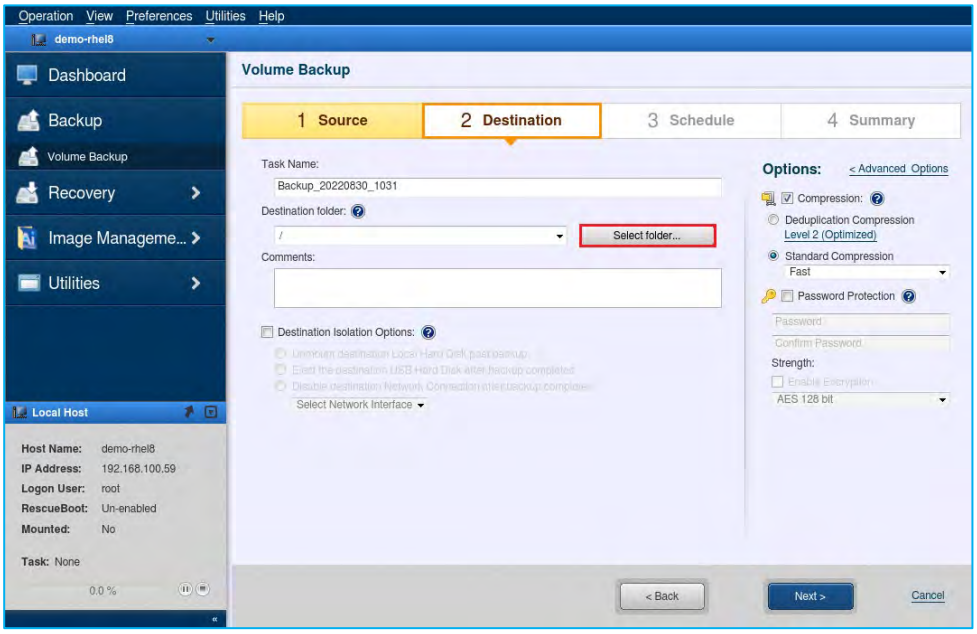
1. Start ActiveImage Protector. Click on **[Backup]** → **[Volume Backup]**.



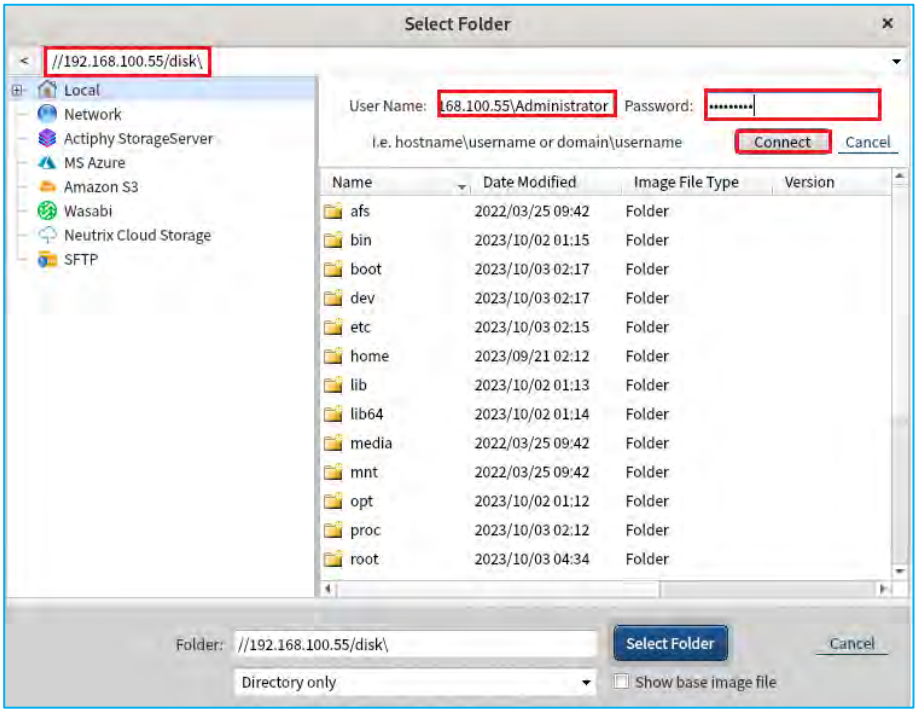
2. Select the backup source from the list of volumes. Next, we will select the volume group (VG) **[rhel]** and the related disks **[/dev/sda]** for the backup source. Once you have selected the backup source(s), click the **[Next]** button.



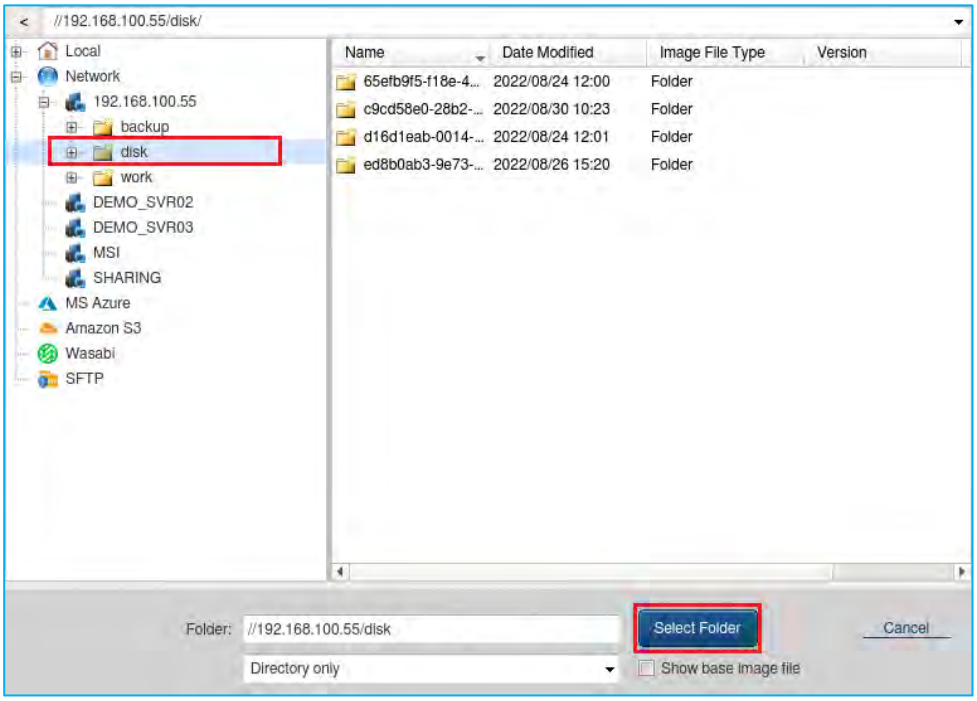
3. Select a destination folder to save the backup image files. In this example, we have selected the network shared folder **¥¥192.168.100.55¥disk** as the destination. Click **[Select Folder]** or click on the "▼" icon on the right-hand side of the **[Destination folder]** text box to select a location to save your backup.



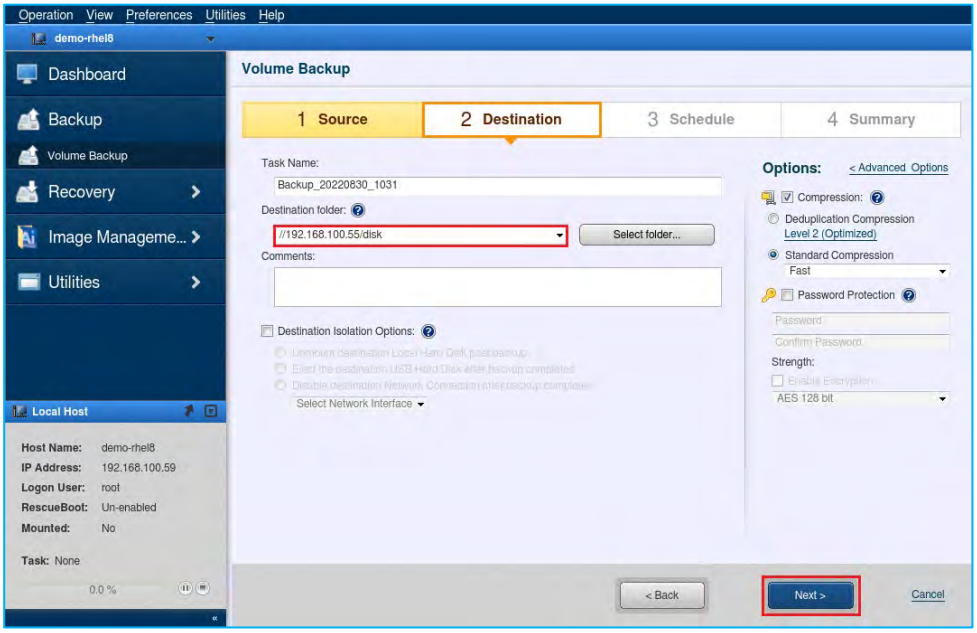
4. Specify a shared folder for the destination storage. Also, enter the destination folder's login credentials and press Enter key. (In this screenshot, we're using **¥¥192.168.100.55¥disk** as the destination folder and **192.168.100.55¥Administrator** as the username). Enter the password and click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



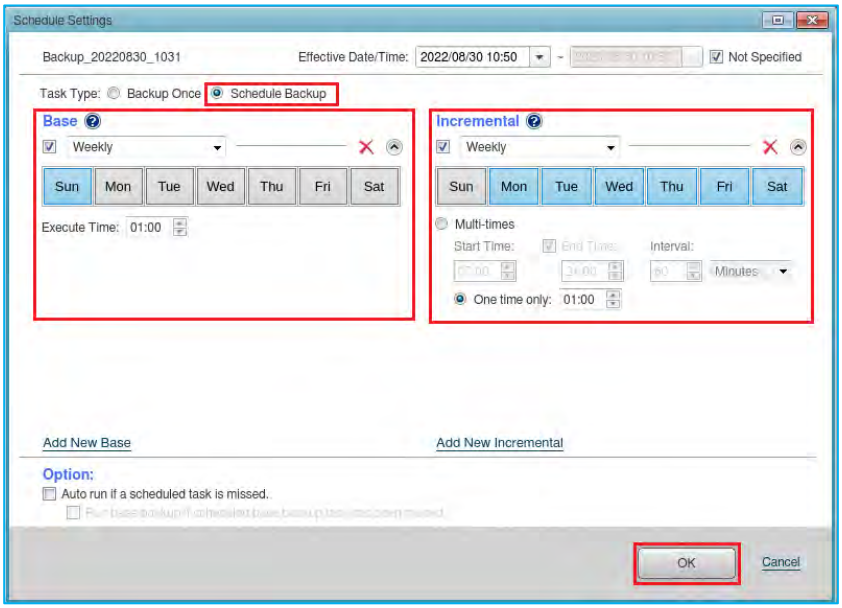
5. Specify the shared folder for the destination and click **[Select Folder]**.



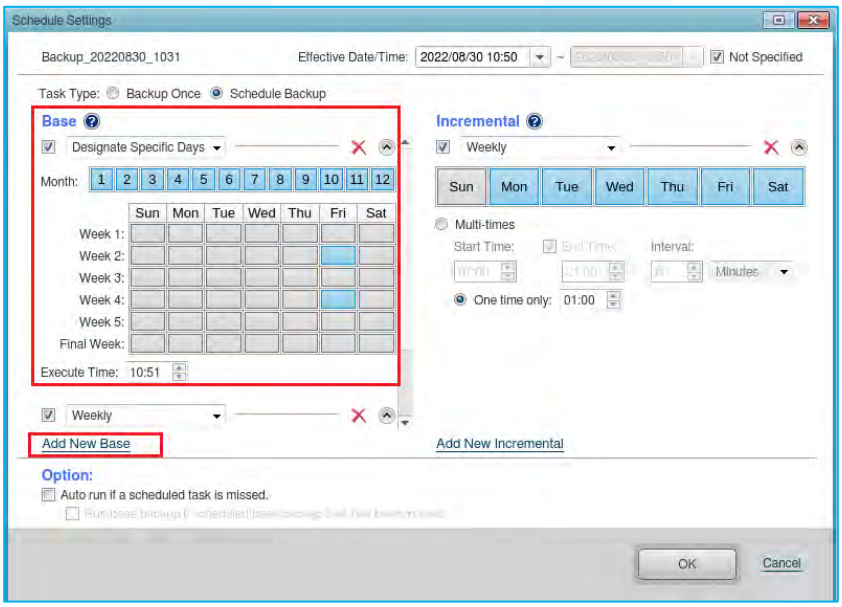
6. On the Volume Backup screen, ensure you have filled in the Destination Folder field correctly and click **[Next]**. We will review the **[Destination Isolation Options]** and **[Options]** sections later in this document.



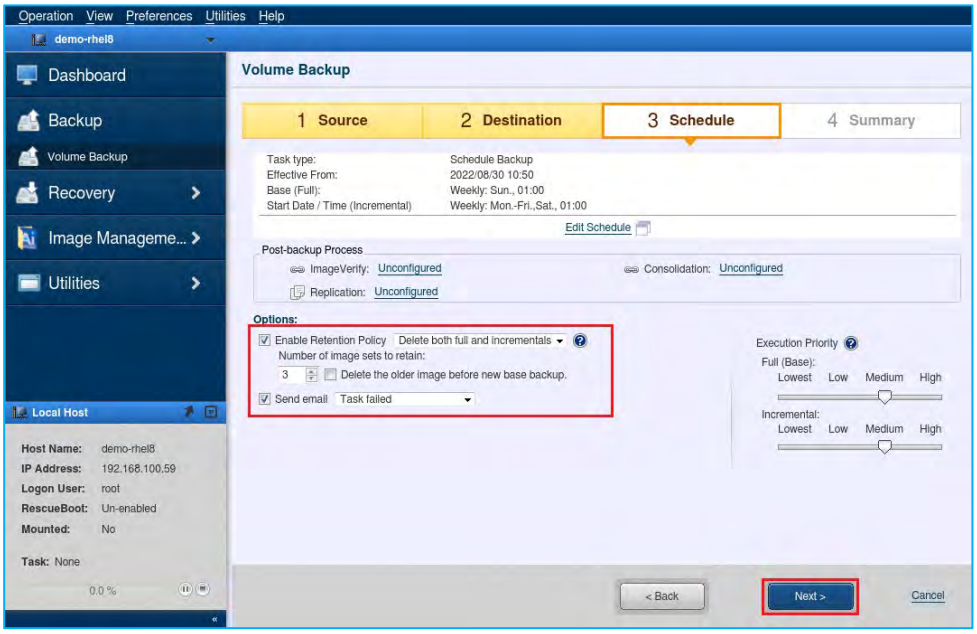
7. You can flexibly configure the backup schedule settings. Options include **[Monthly], [Weekly]**, [**Specified Date/Time]**, **[Designate Specific Days]**. The steps below show an example of configuring a schedule:
   - Select **[Schedule Backup]** for the Task Type and configure the Weekly backup schedule settings.
   - Set the Base backup schedule to **Weekly**.
   - Set the Incremental backup schedule to **Weekly**.
   - Set the Execute Time of the Base backup to **Sundays at 1:00 am**.
   - Set the Incremental Backup schedule to **Monday to Saturday at 1:00 am**.
   - After configuring all options, click the **[OK]** button.



8. 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.



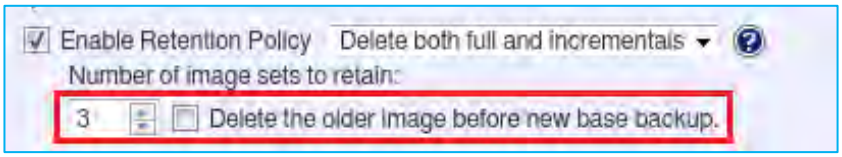
9. You can configure your **[Enable Retention Policy]** and **[Send Email]** settings on the **[Schedule]** tab. Then, click the **[Next]** button for the settings to take effect. We will cover details about the **Post-backup Process** in the next chapter.



① **Enable Retention Policy**

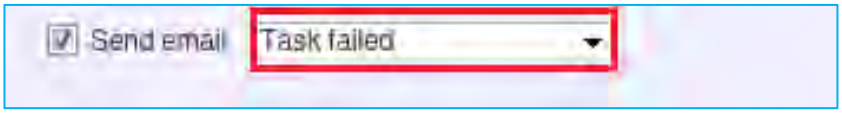
The Retention Policy defines how many sets of backup files to retain before deletion. In this example, we've enabled the retention policy by checking the **[Enabling Retention Policy]** checkbox. We've also configured the program to keep the three most recent backups in the destination folder and delete 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 **Email Setting**

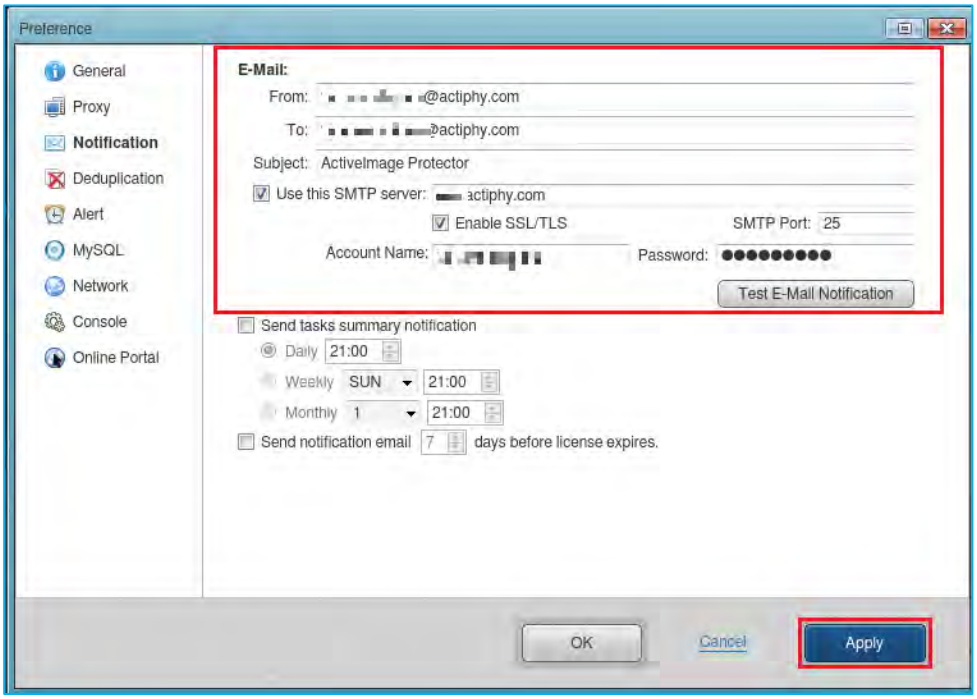
Check this box to send an email notification of a task completed with a specified status.



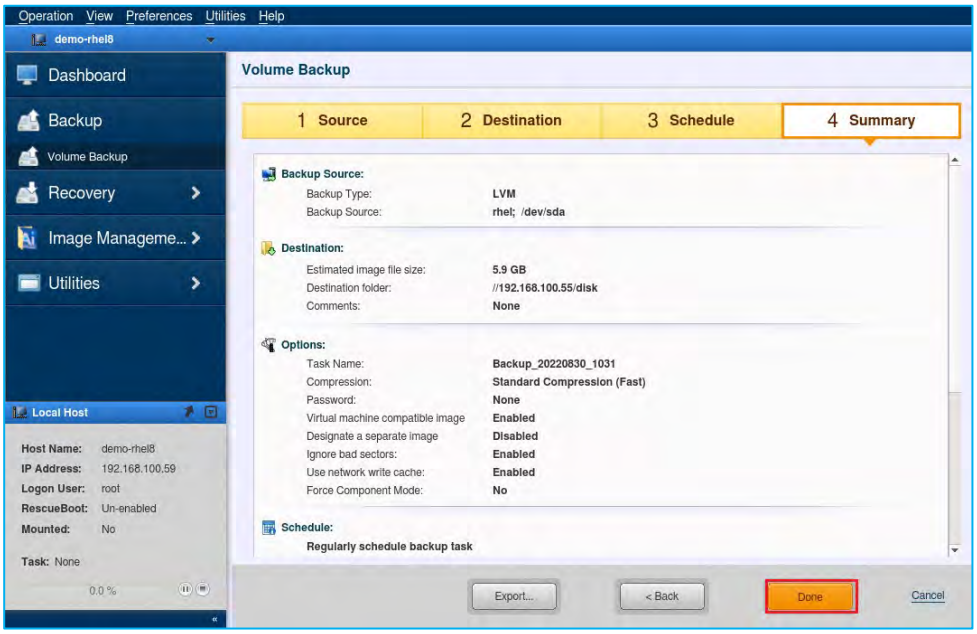
③ **Predefine the email notification settings by selecting [Preferences]**

Predefine the email notification settings by selecting [Preferences] - [Notification] from the menu bar.

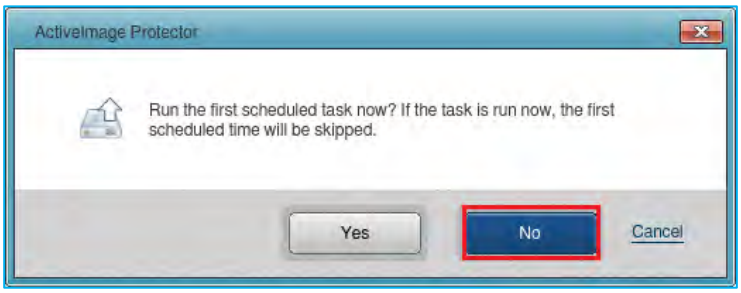
After configuring your email settings, click the **[Test Email Notification]** button to ensure your email notification settings are correct. Once you have received the test email, click the **[Apply]** button to save your configuration.



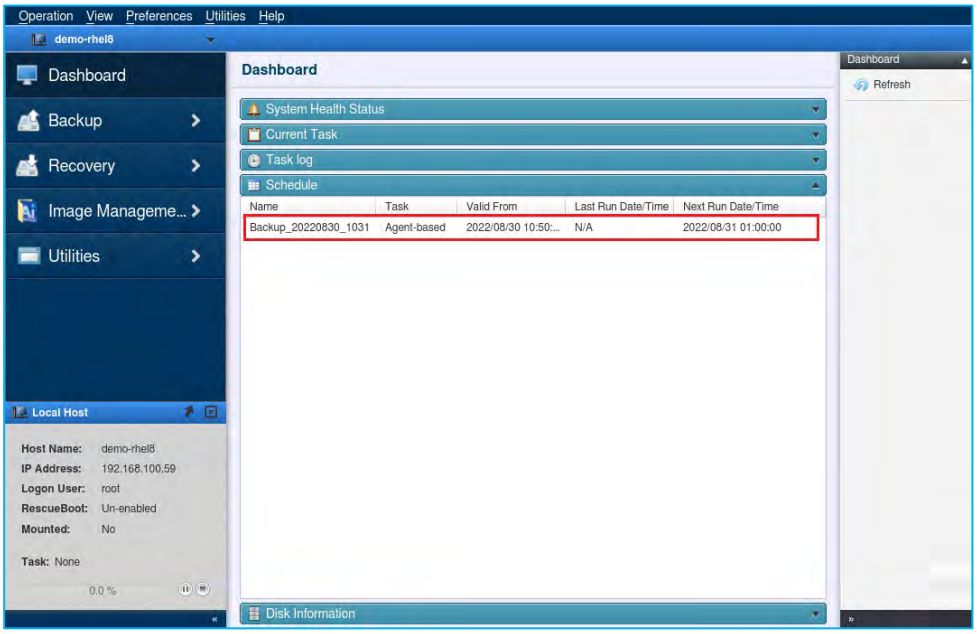
10. After setting up your backup schedule, you should see a summary of your configuration. Please review your backup configuration. If everything looks correct, click the **[Done]** button.



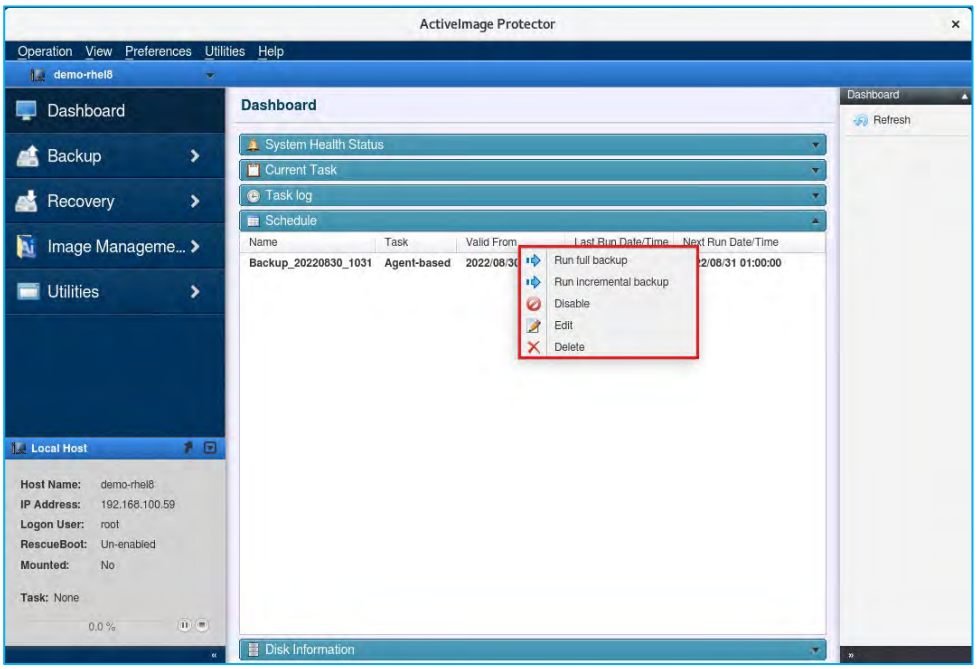
11. Next, you'll see a dialog asking if you want to run the initial backup now. If you click the **[No]** button, the system will take you back to the Dashboard, and your initial backup will run according to your schedule. If you click the **[Yes]** button, the system will immediately run the initial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



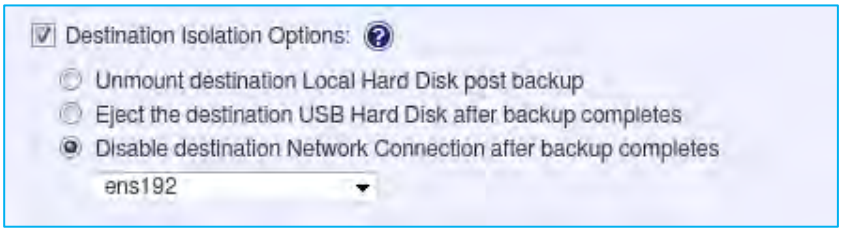
12. Go to **[Dashboard]** → **[Schedule]** to modify or monitor your scheduled tasks.



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. 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:

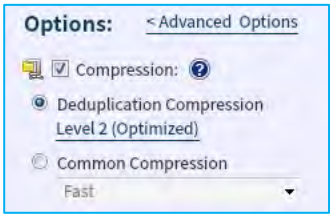


- **Unmount destination Local Hard Disk**:
  When this option is enabled, ActiveImage Protector will unmount the destination Local Hard Disk once the backup process is complete.
- **Eject the destination USB hard disk after the backup completes:**
  Enabling this option causes ActiveImage Protector to 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 the backup completes:**
  This option will disconnect the network connection to your backup destination once the backup is complete if you save backups to a network drive.

15. Options:

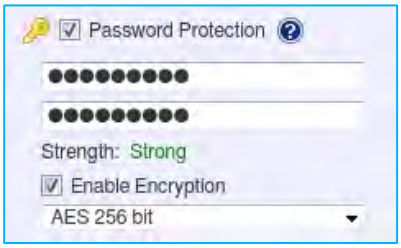
Compression: ActiveImage Protector provides two types of compression: **[Standard Compression]** and **[Deduplication Compression]**. The compression ratio differs depending on the type of compression you choose.

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.



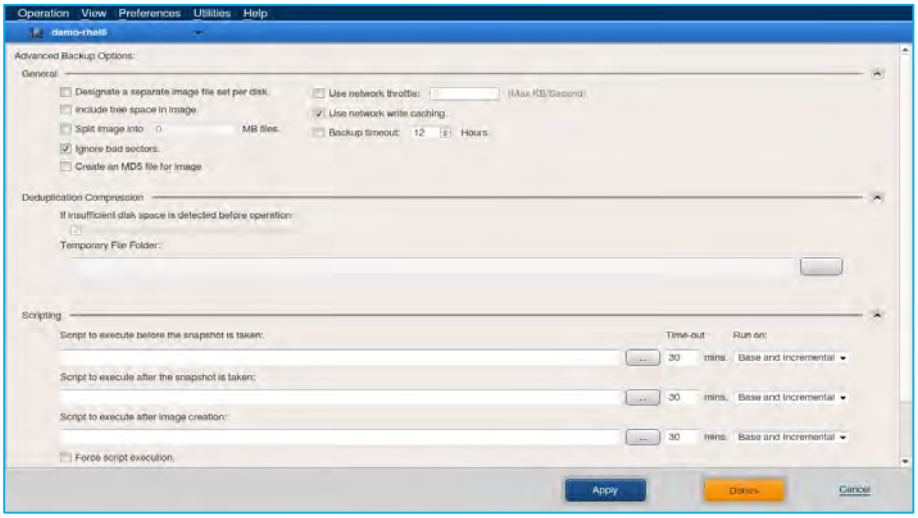
② **Password Protection:** Enabling this option protects the backup image file by assigning a unique password. This additional security prevents anyone from mounting, exploring, or restoring the image file without a password.

③ **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.



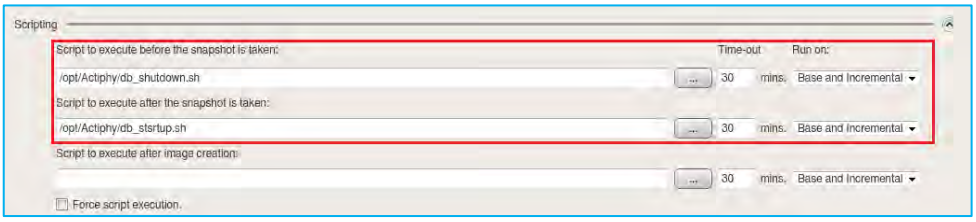
16. Advanced Backup Options: The Advanced Backup Options section contains the following settings:

- **Designate a separate image file set per disk**: This option tells ActiveImage Protector to create a separate backup file for each disk in your backup plan.
- **Include free space in mage**: The system takes a backup of all sectors, including the free space of the selected volume.
- **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 ActiveImage Protector to create an MD5 hash for each backup image. ActiveImage Protector will store MD5 hashes in a separate file in the same directory where it saves your backup images.
- **Use network throttle xx (Max KB/Second)**: This option lets you throttle the amount of network bandwidth ActiveImage 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 ActiveImage Protector to process large files more slowly.
- **Backup timeout xx hours:** Timeout occurs to cancel the backup task if the backup process does not complete within the specified time.



- **Scripting:**

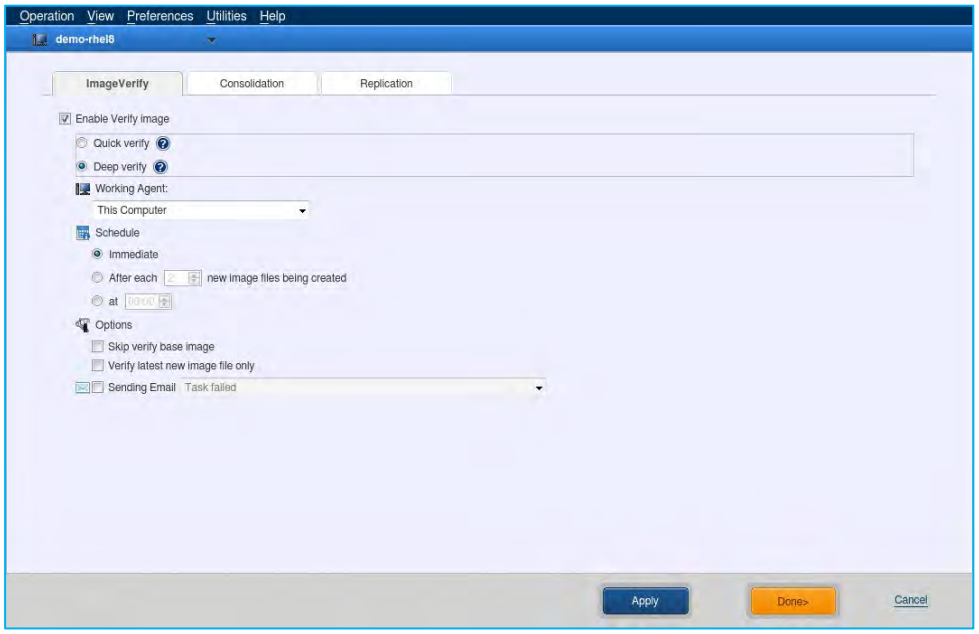
  You can write scripts to run before and after ActiveImage Protector creates snapshots or backups. For example, when backing up non-VSS-savvy databases, you need to stop the service before starting the backup task to maintain the integrity of the data. You can specify a script or batch file to stop the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



17. 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].

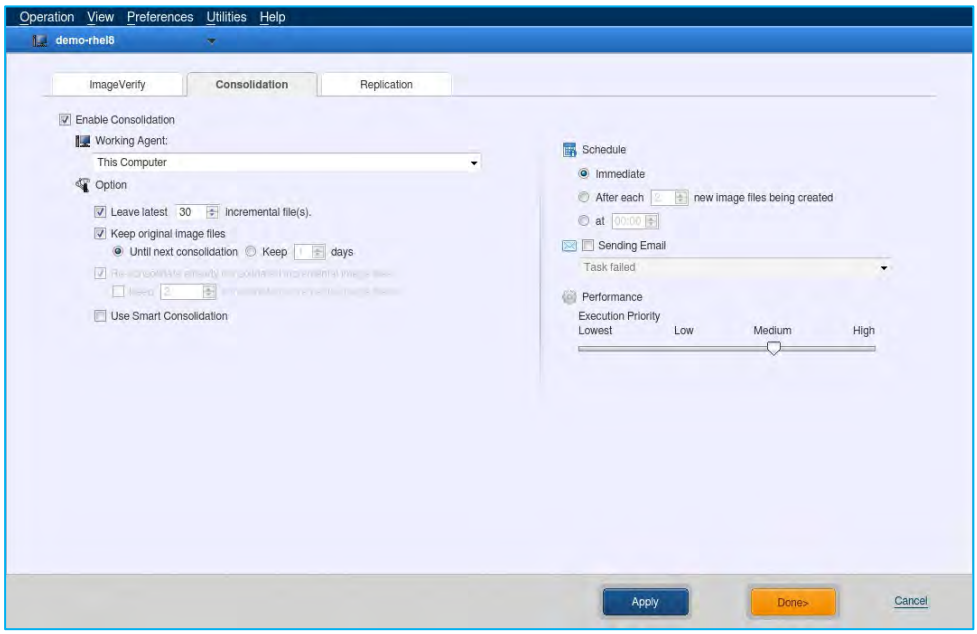
    ① **BootCheck:**

    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. Next, configure the Schedule settings, Sending Email options, etc.



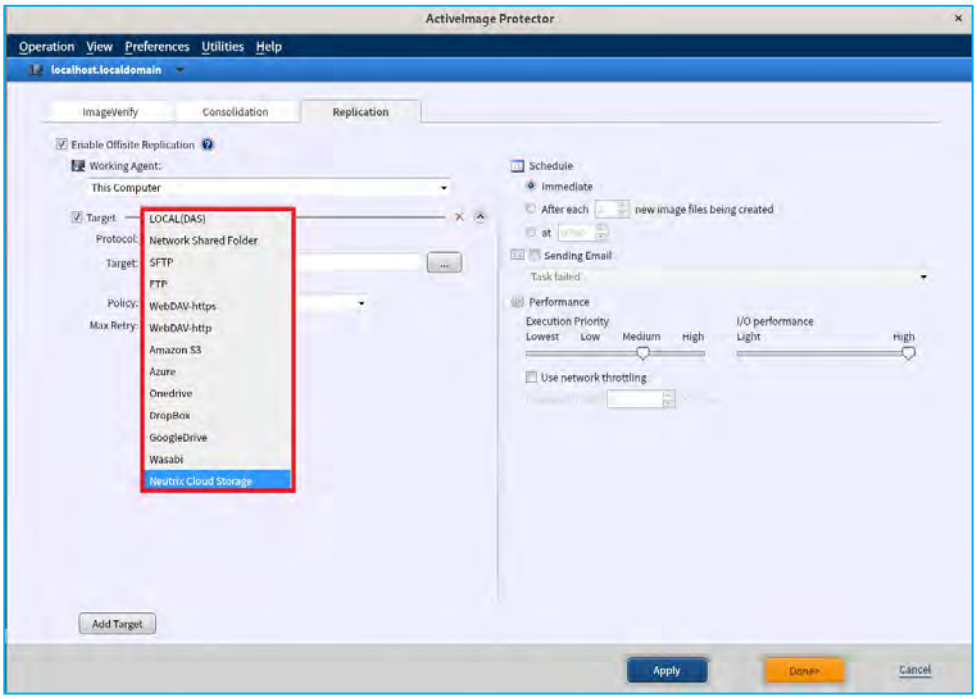
② **Consolidation :**

You can schedule consolidation 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.



③ **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, and cloud storage systems, including Amazon S3, Azure Storage, OneDrive, Dropbox, Google Drive, Wasabi and Neutrix Cloud.



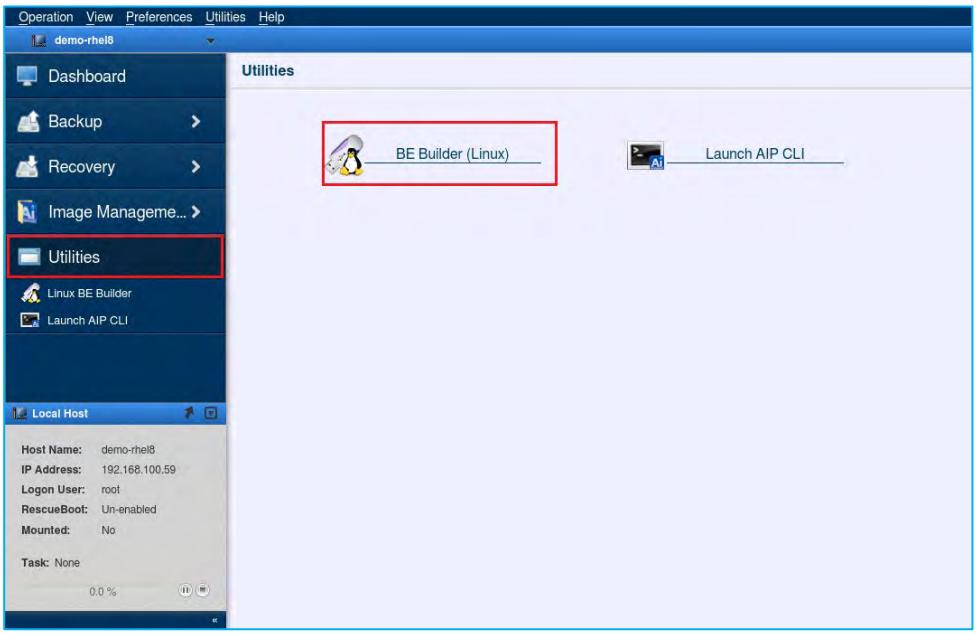
5. Boot Environment Builder

Build Linux-based boot environment

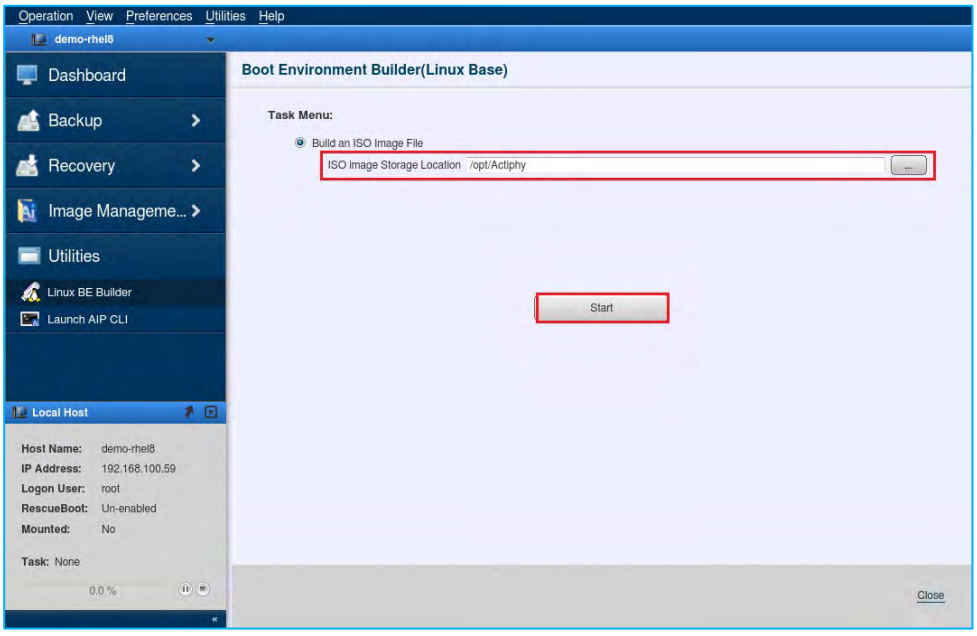
The ActiveImage Protector media includes a Linux-based boot environment. Please ensure you have applied the latest version of ActiveImage Protector patch before building the Linux-based boot environment.

This section shows you how to build a Linux-based Recovery Environment, should that be necessary.

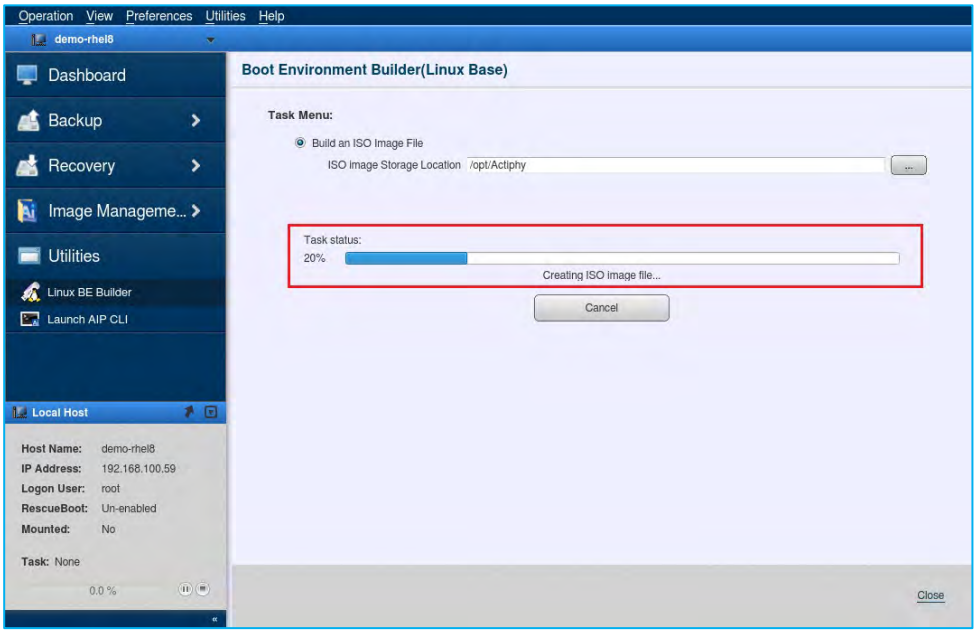
1. Launch ActiveImage Protector, select **[Utilities]** in the menu and **[BE Builder (Linux)]** in the menu.



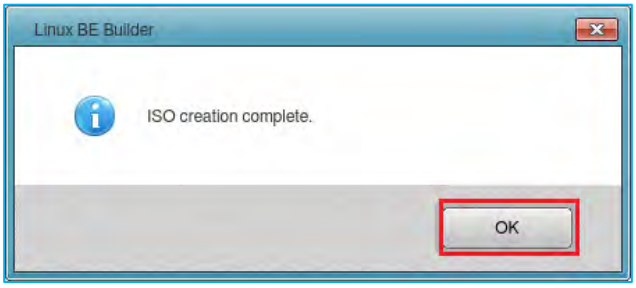
2. Specify the location of the ISO image storage and click **[Start]**.



3. When the ISO creation task starts, the progress bar is displayed.



4. When the process completes, the following “ISO creation complete” dialog is displayed. Burn the ISO image to optical media to use it as a recovery boot environment.



6. Restore

6-1. File / Folder Recovery

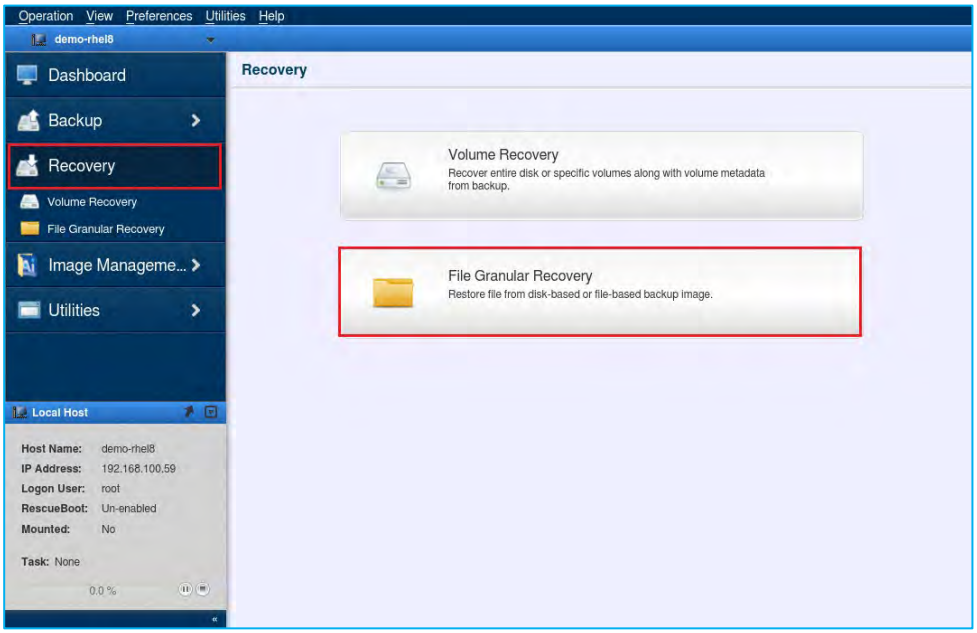
Please use the following steps to restore a specific file or folder from a backup image:

Note: When specifying a network shared folder, you need to mount the folder on the local system first.

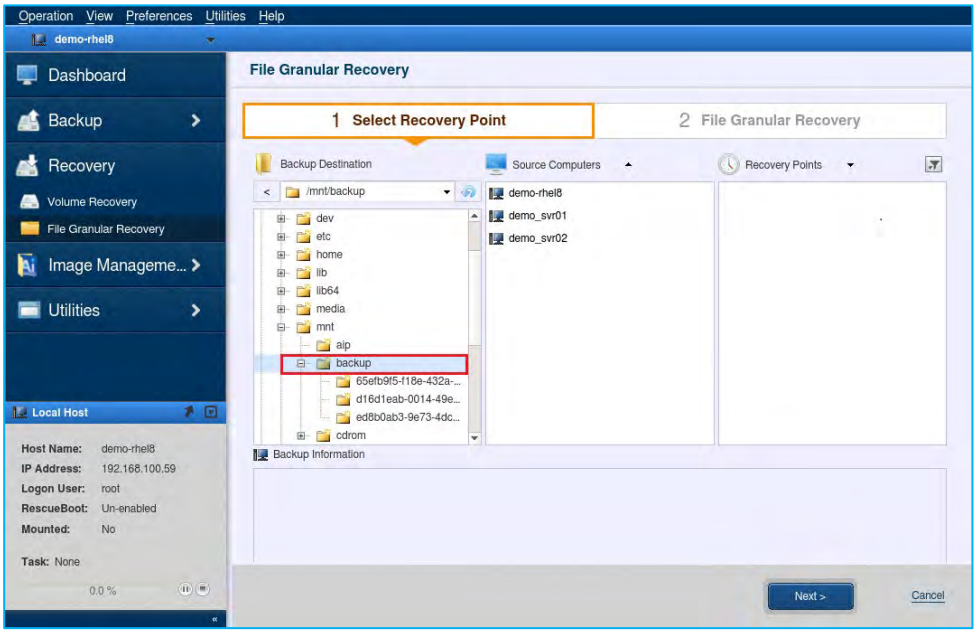
1. In this example we will create the directory “backup” under “/mnt” by running the following command from terminal. The mount command with mount the shared folder to the created directory.

```
# mkdir /mnt/backup
# mount -t cifs -o username=Administrator,password=xxxxxxxx //192.168.100.55/disk /mnt/backup
```

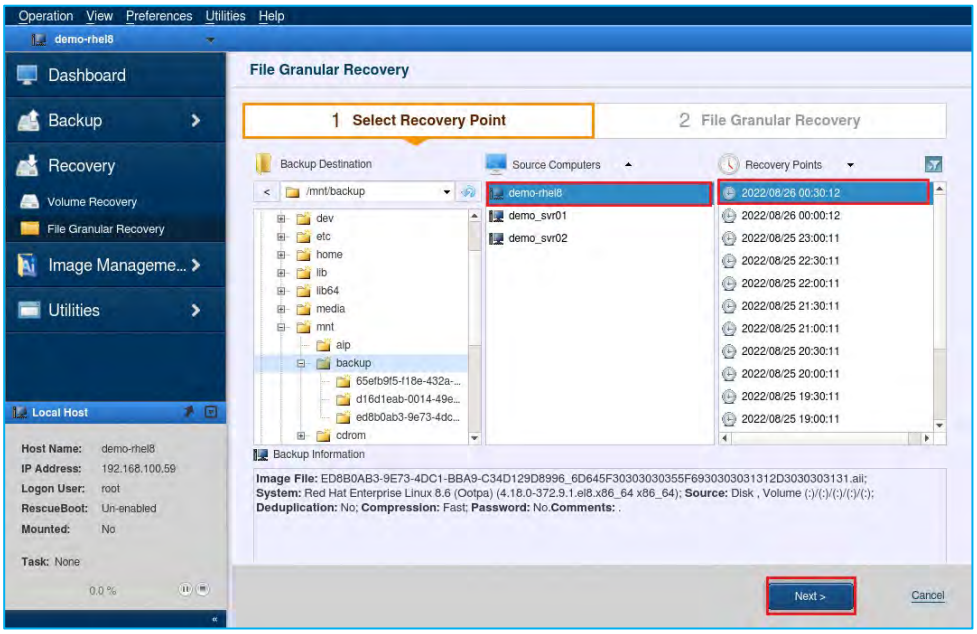
2. Start ActiveImage Protector and click **[Recovery]** → **[File Recovery]**.



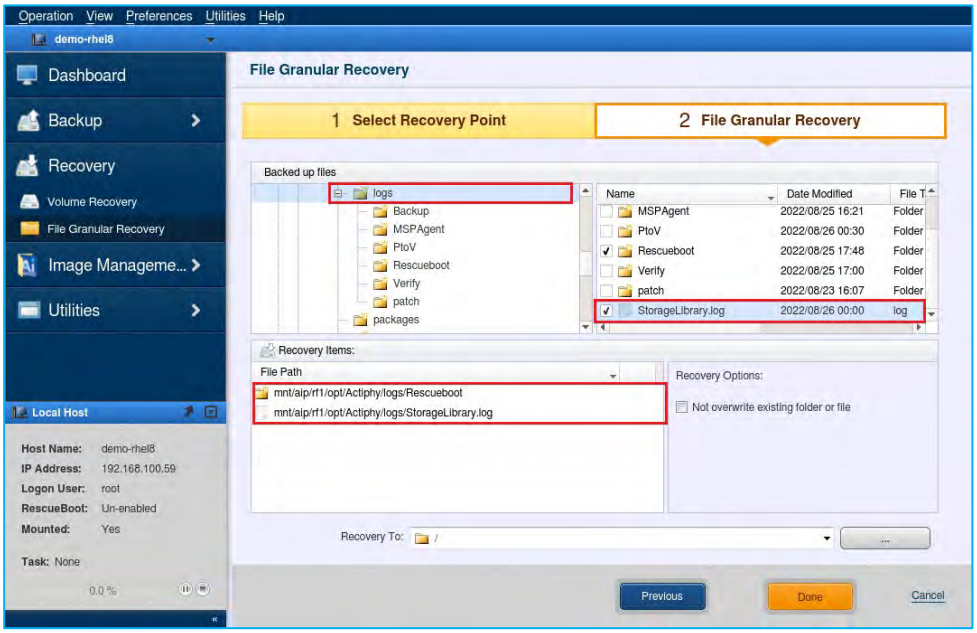
3. In **[Select Recovery Point]** window, please select the folder that contains image files. This example shows the directory "/mnt/backup" is selected on the mounted share.



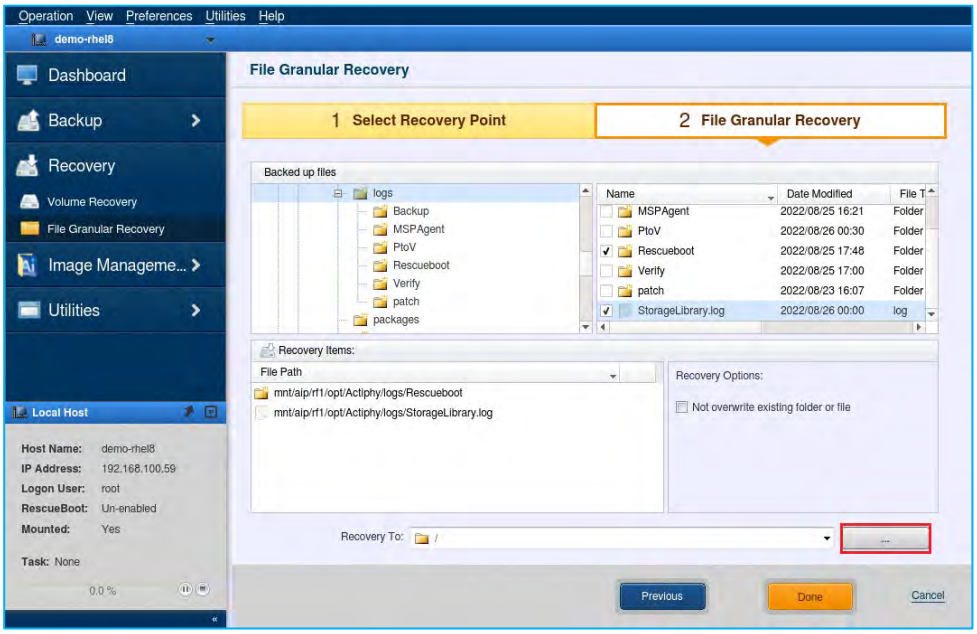
4. Select the source computer and the recovery point of the base (full) backup. Click **[Next]**. The information of the selected recovery point is displayed in **[Backup Information]**.



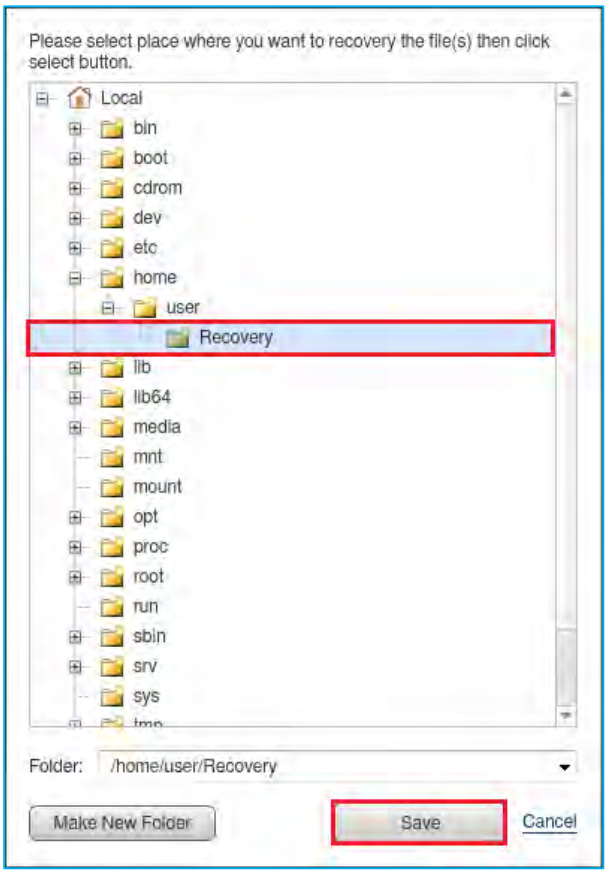
5. To exclude the listed items from restore source, click the **[X]** button (to display the [X] button, mouse over the blank column) or uncheck the checkbox in **[Backed up files]**.
   [Don't overwrite existing folder or file] option can be selected existing files or folders of the same name will not be overwritten.



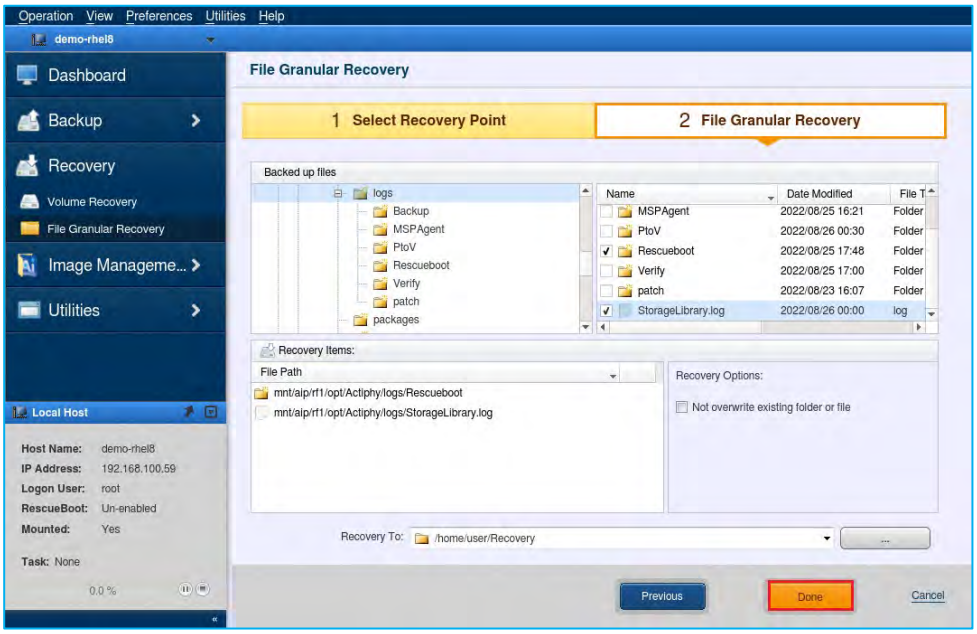
6. Specify a destination to restore the files in **[Recovery To]** by clicking [...].



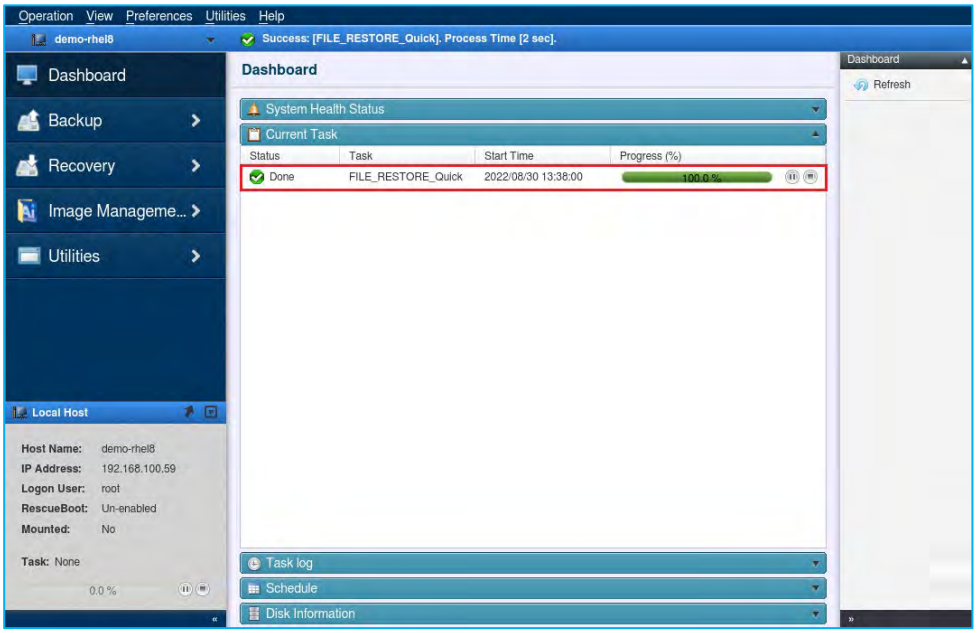
7. Select the destination folder to restore the items and click **[Select]**.



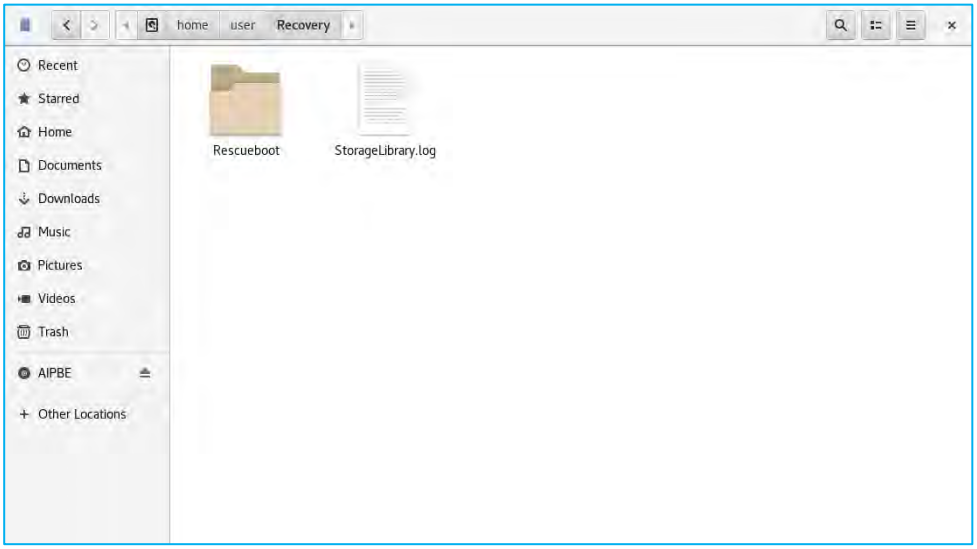
8. Click **[Run]** to start restore process.



9. When the progress bar reaches 100% the recovery is complete.



10. The restored files and folders are saved in the specified destination.

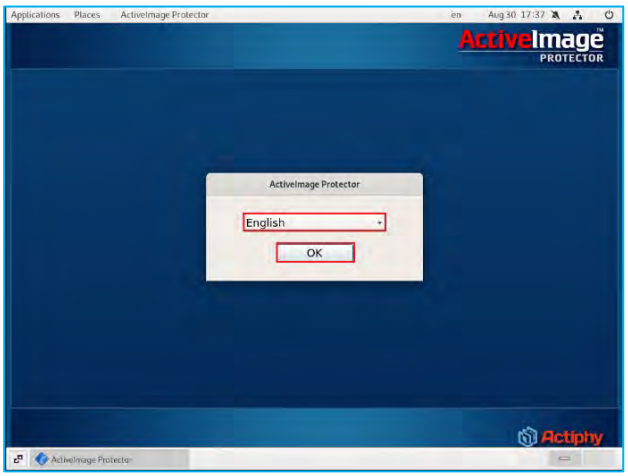


6-2. System Recovery : Standard Linux-based boot environment

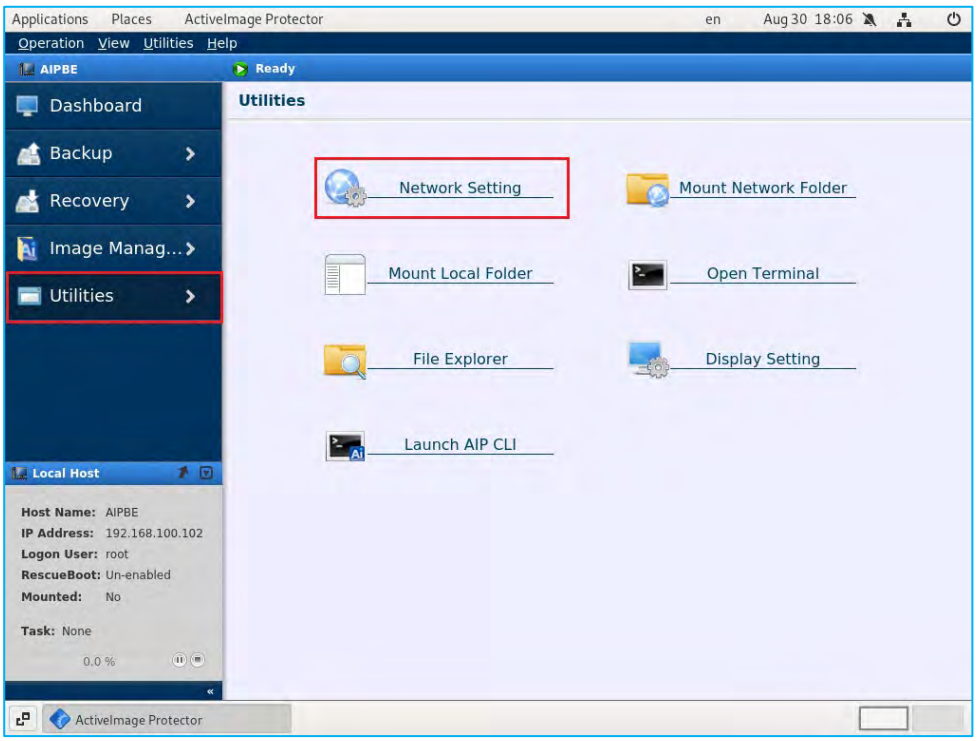
Use the following steps to recover a LVM configured system using the Linux-based Boot Environment. The boot environment can be created using the ActiveImage Protector 2022 Linux-based boot environment builder.

Note: ActiveImage Protector will purge all 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 and boot into ActiveImage Protector.
   - Select **[English]** (or whichever language you prefer).
   - Click the **[OK]** button.

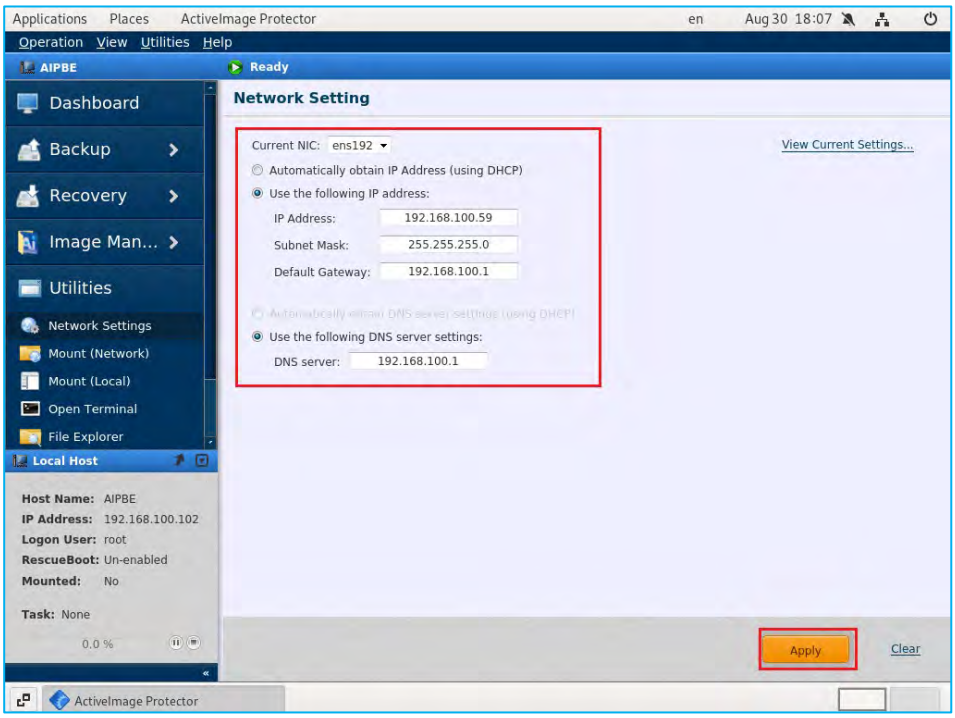


2. After the ActiveImage Protector GUI is displayed, click on **[Utilities]** → **[Network Setting]** to configure network settings. To access network shared folders containing image files, network configuration is required.

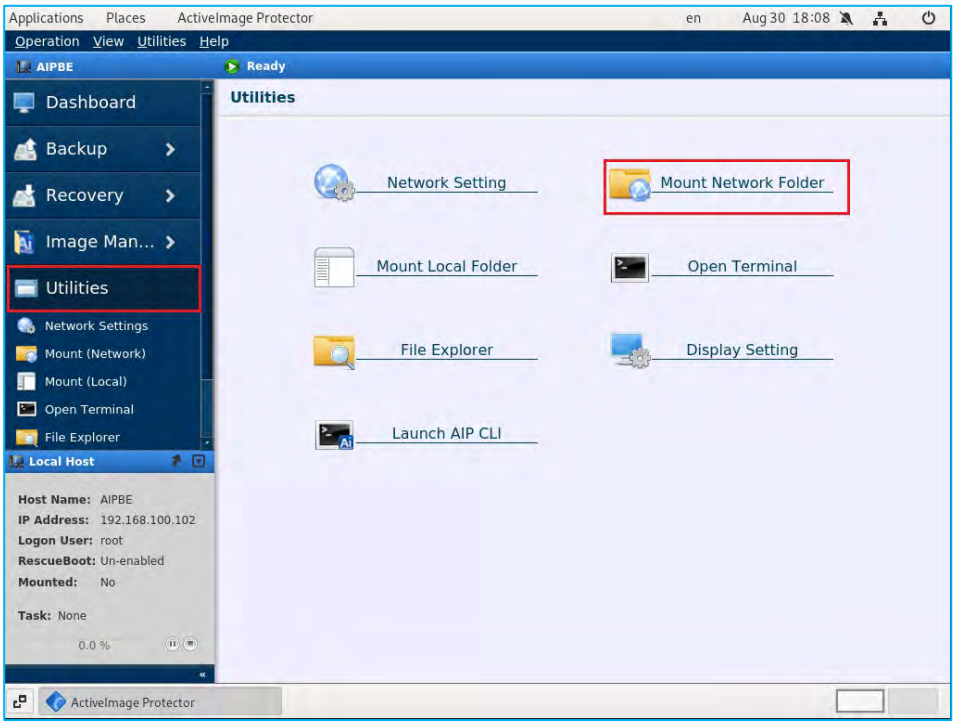


3. Select **[Use the following IP address]** radio button and enter your network information. We are going to use the following network information in our example:

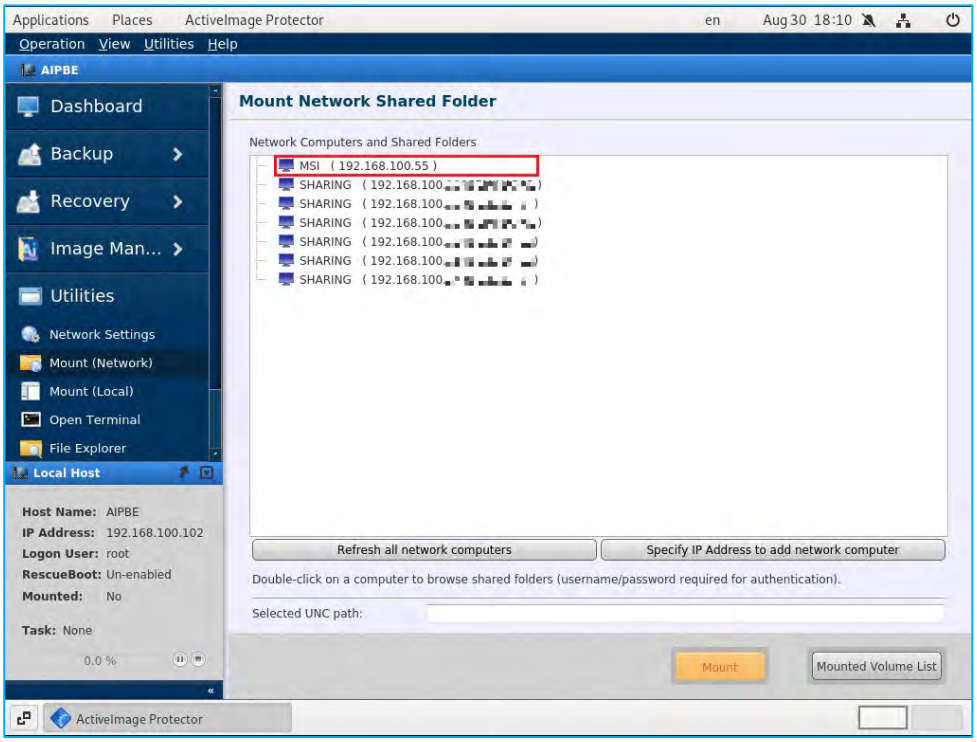
   - [IP Address]: 192.168.100. 59
   - [Subnet Mask]: 255.255.255.0
   - [Default Gateway]: 192.168.100.1
   - DNS Server: 192.168.100.1
   - Click the **[Apply]** button.



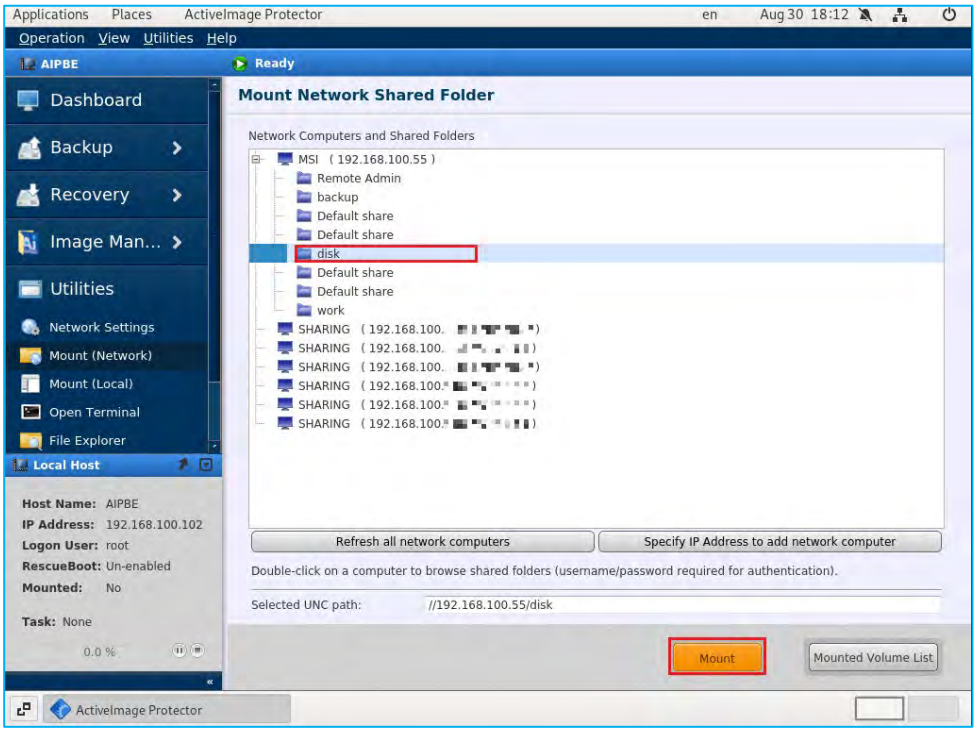
4. Click on **[Utilities]** → **[Mount Network Folder]** to mount the network shared folder containing image files.



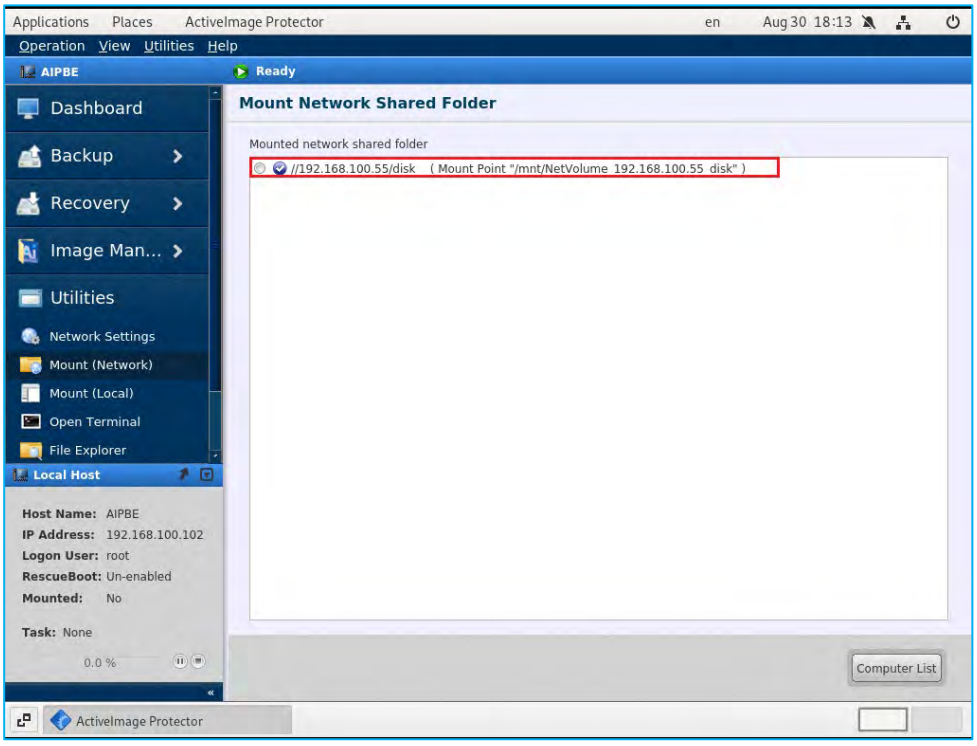
5. Networked computers that can be found are listed as below. Double-click on a computer has a network shared folder. Please enter **[User Name]** and **[Password]** for user authentication.
   *If the network computer is absent from the list, please add the computer by selecting **[Specify IP Address to add network computer]**.



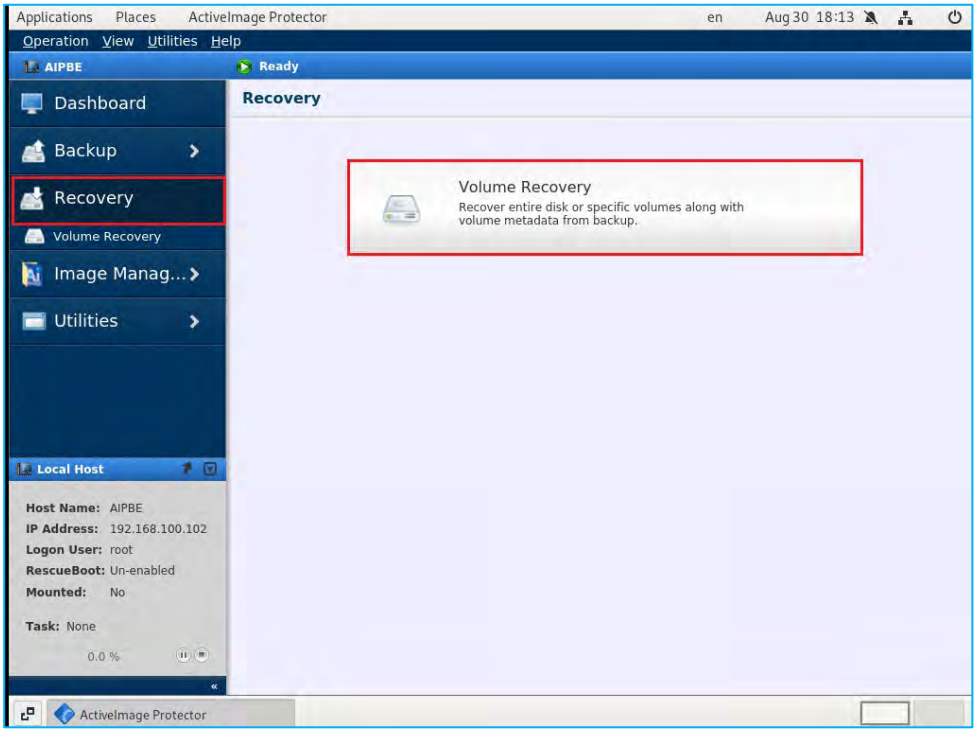
6. In this example, the shared folder “disk” is selected on “192.168.100.55”. Click **[Mount]**.



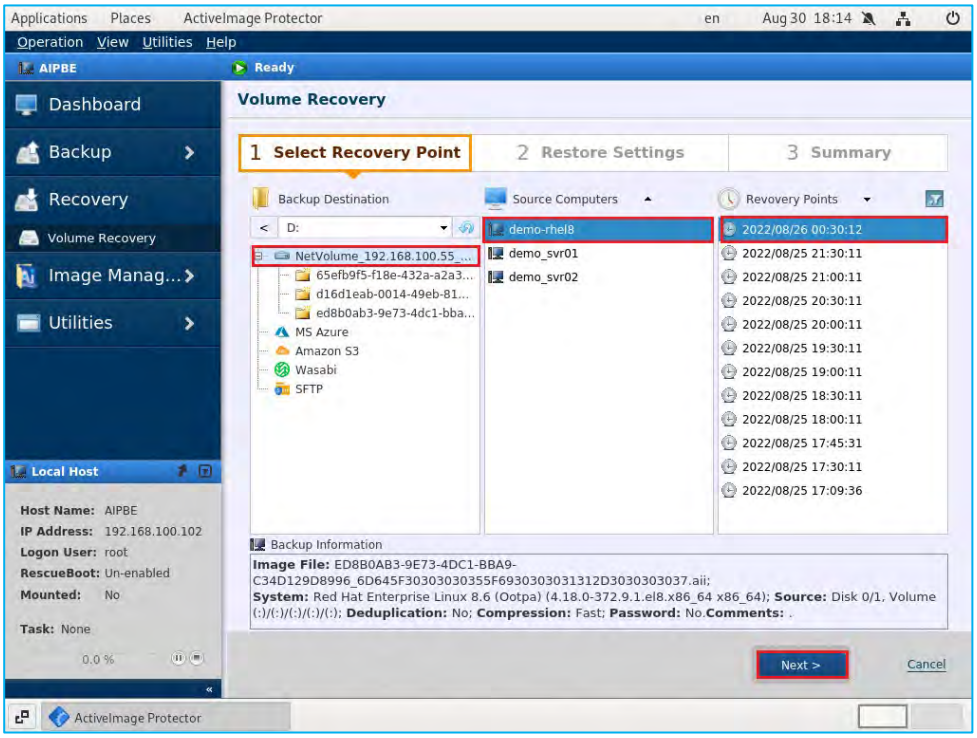
7. Once you have mounted the network shared folder, you'll see the mount point in the **[Mounted network shared folder]** list.



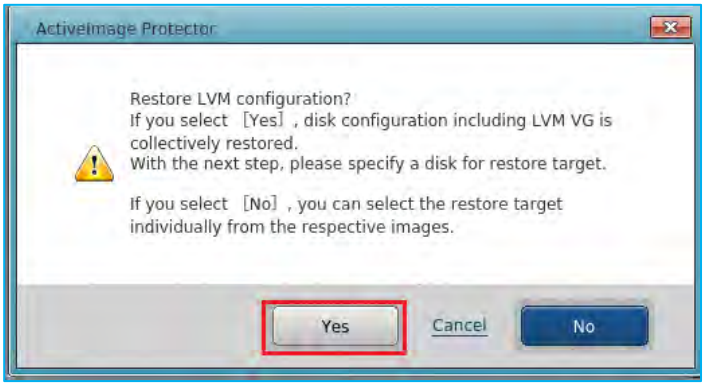
8. Click on **[Recovery]** → **[Volume Recovery]** to recover specific volumes (including volume metadata) or an entire disk, from a backup image.



9. Follow the steps below to select a backup recovery point.
   - Select the folder where the backup is located.
   - Select the backup **[Source Computer]**.
   - Select the **[Recovery Point]**.
   - Click **[Next]**.

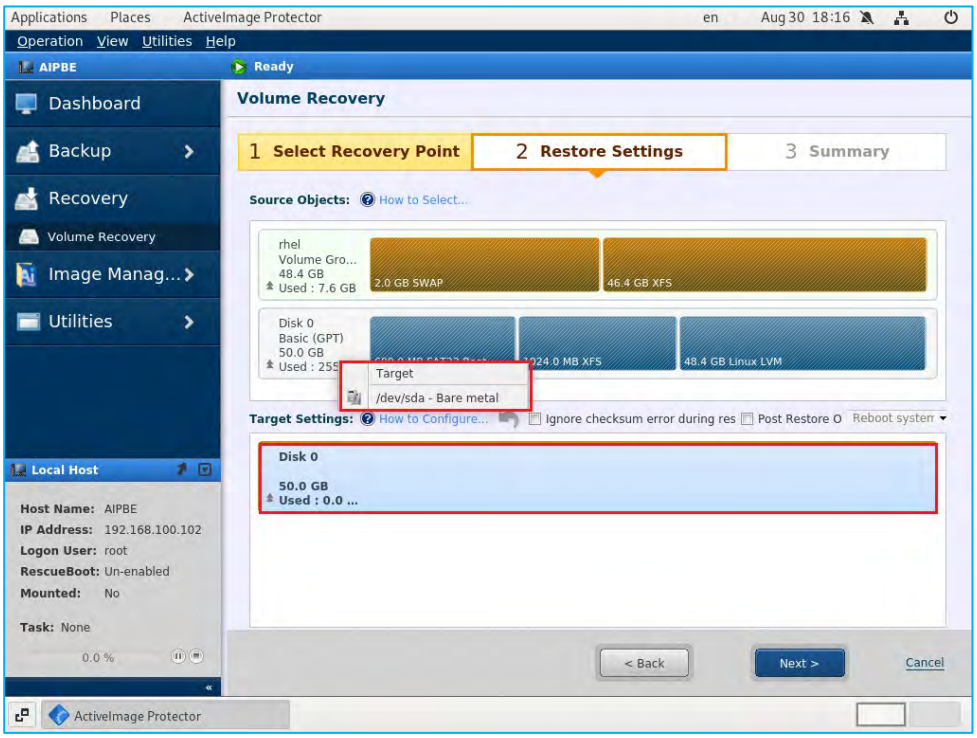


10. If restoring a LVM, click **[Yes]** in the dialog. In this example, all the disks, including the LVM VG,, are selected as restore source. The following explains how to perform system bare metal recovery and overwriting recovery operations.

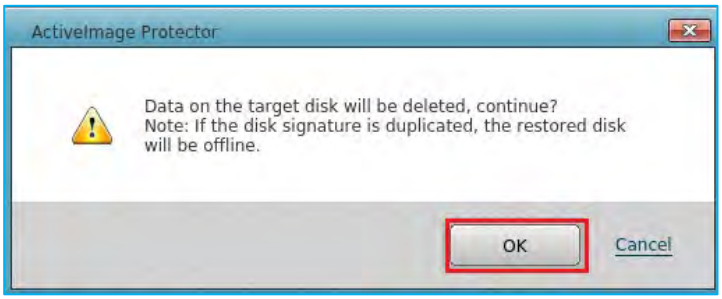


11. Bare Metal Recovery: Right-click on the left part of the disk map in **[Source Objects]**. Select the physical disk "/dev/sda – Bare metal" for **[Target]**. Alternatively, you can drag and drop the selected restore source to the restore target in the disk map at the bottom of the window. In this example, only the physical disk is selected for the restore target.

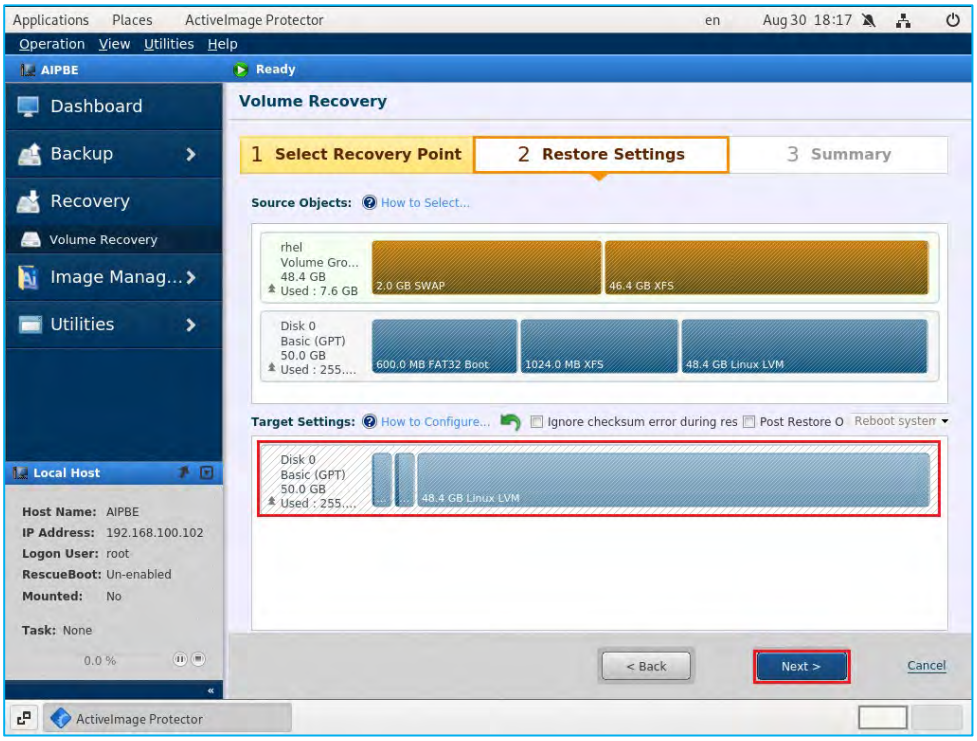
    Note: When the volume group (VG) is configured to span across multiple physical disks, please specify the all physical disks as the restore target.



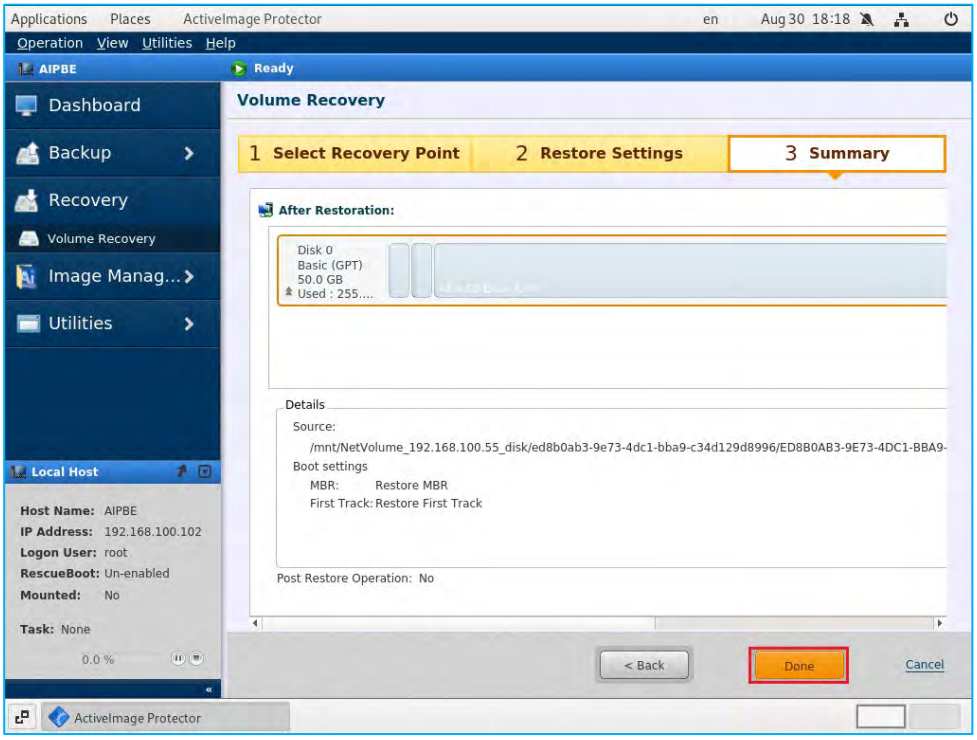
12. The following confirmation message is displayed. Click **[OK]**.



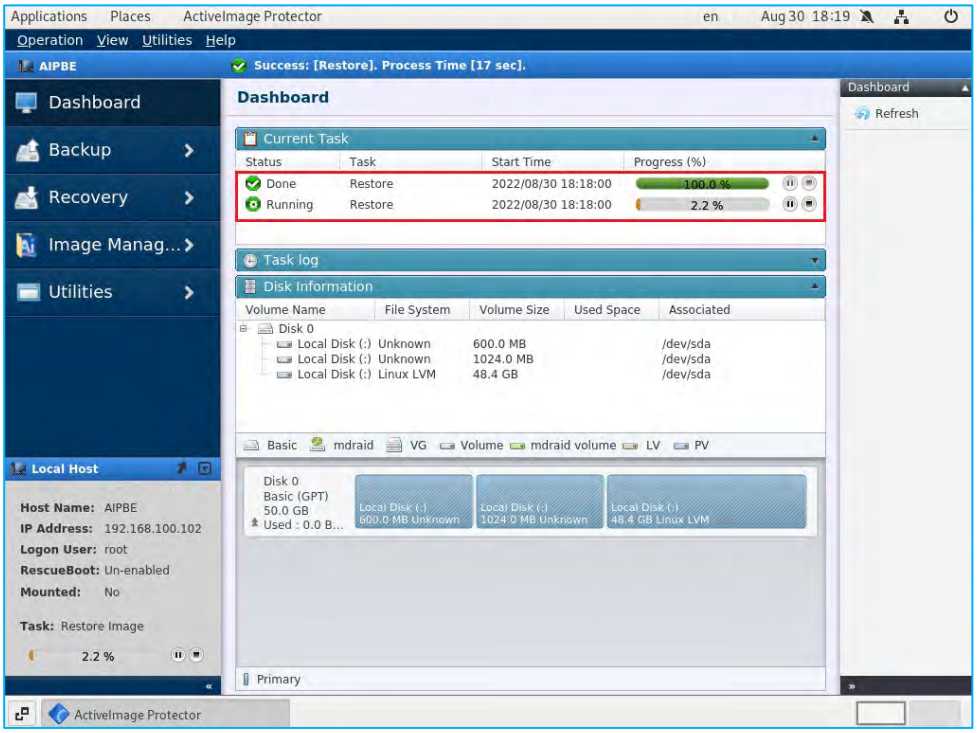
13. Please make sure the information displayed in **[Target Settings]** is correct and click **[Next]**.



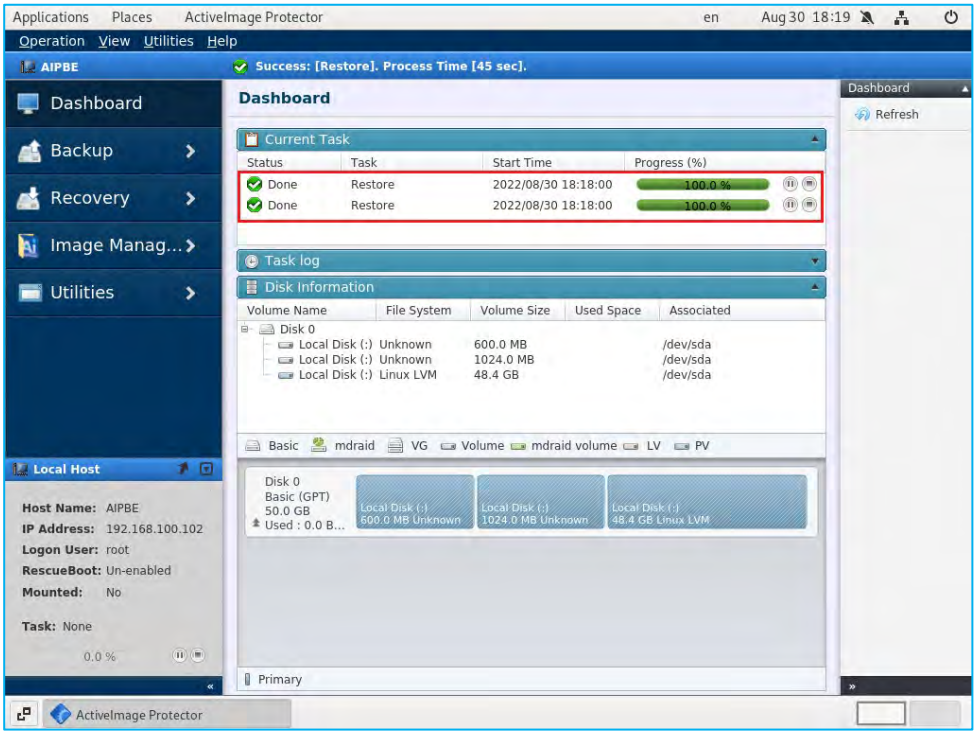
14. Please review the settings in **[Summary]** window and click **[Done]**.



15. When the recovery task starts, the console returns to Dashboard view indicating the progress of the tasks. After the physical disk is restored, a recovery task for the volume group (VG) will begin.



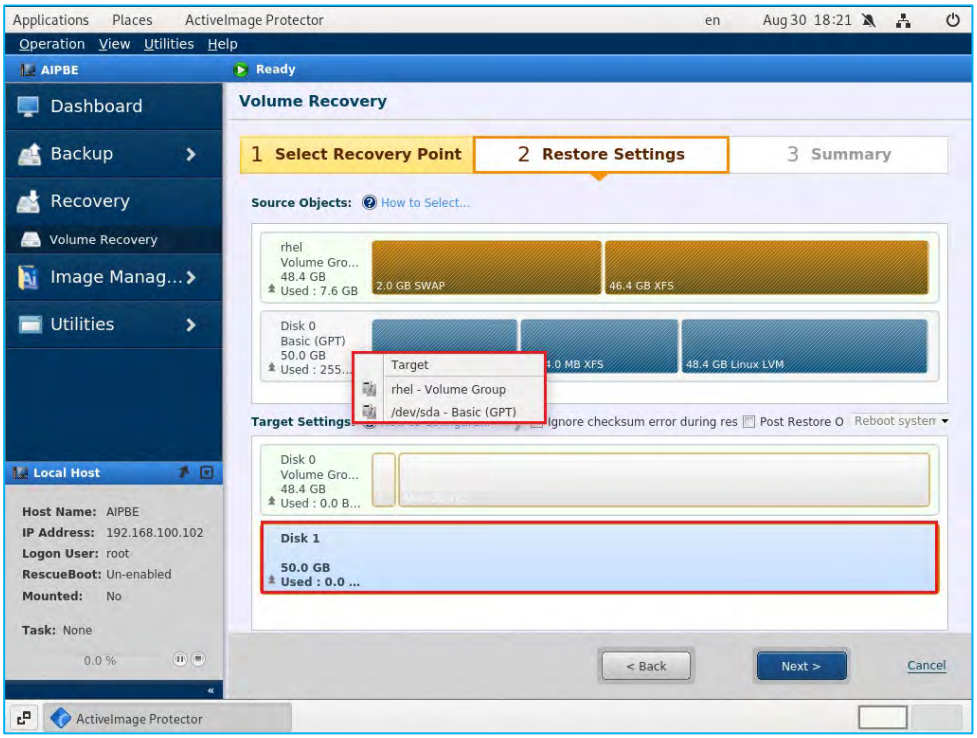
16. When the progress bar reaches 100% the recovery is complete. Please remove the boot environment media and select **[Operation]** -> **[Done]** in the console menu. Shut down or reboot the system. Verify the physical disk and VG are correctly restored.



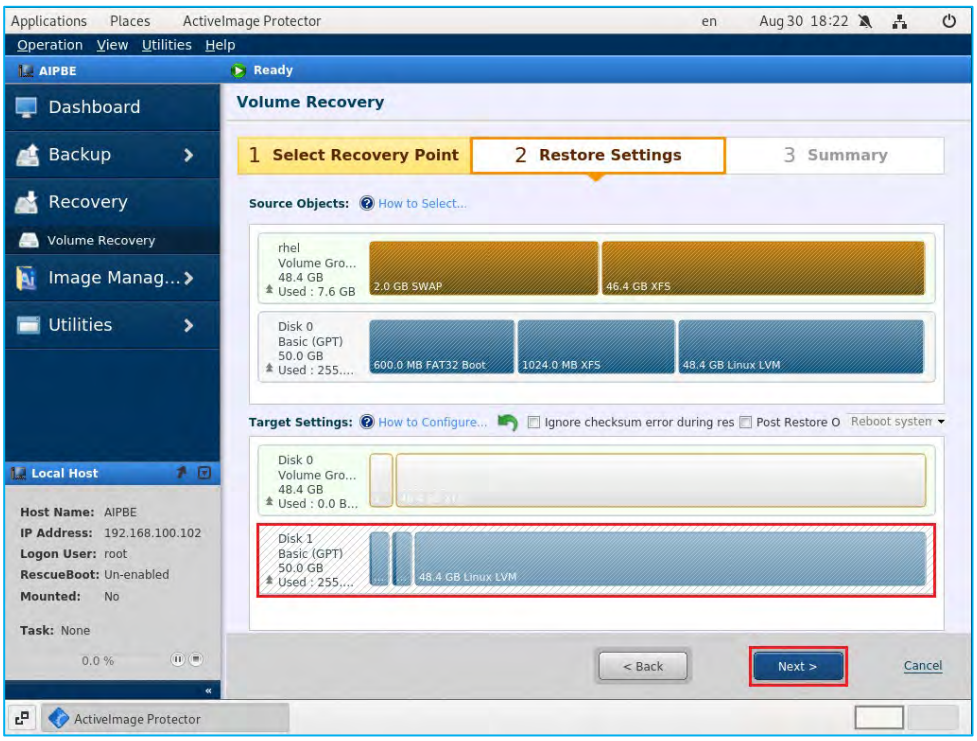
17. Overwrite Recovery

Using the same operating procedures as bare metal recovery, right-click on the left part of the disk map in [Source Objects]. Select the physical disk “/dev/sda – Basic (GPT)” as a [Target]. You can also drag and drop the selected restore source to the restore target in the disk map at the bottom of the window. In this example, only the physical disk is selected for the restore target.

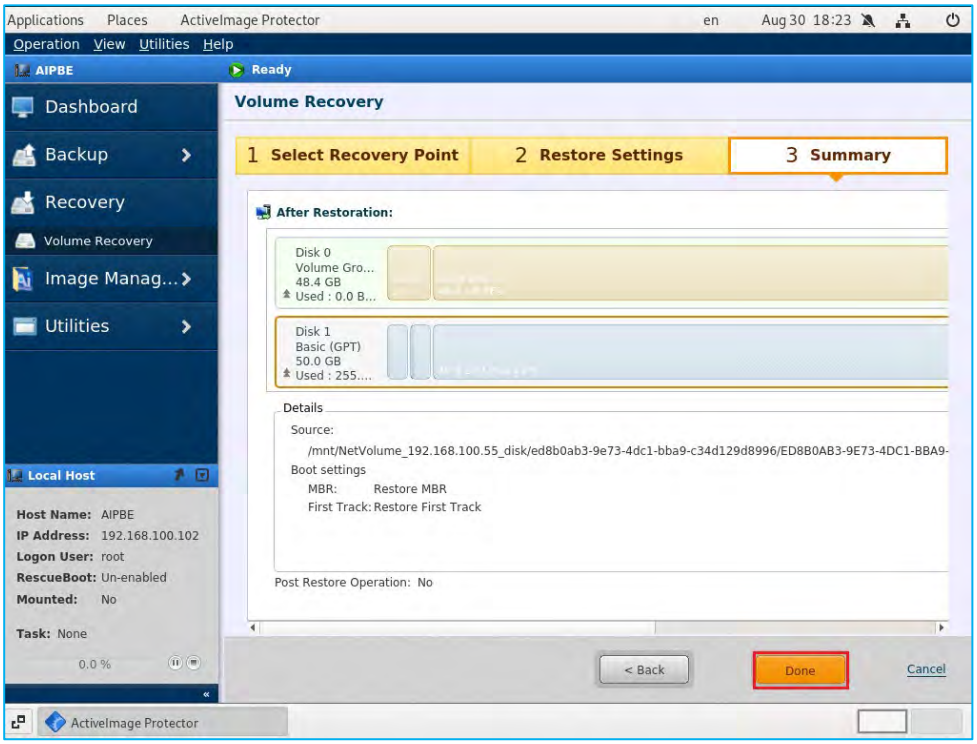
*When a volume group (VG) is configured with the volumes on multiple physical disks, please specify the entire physical disk as the restore target.



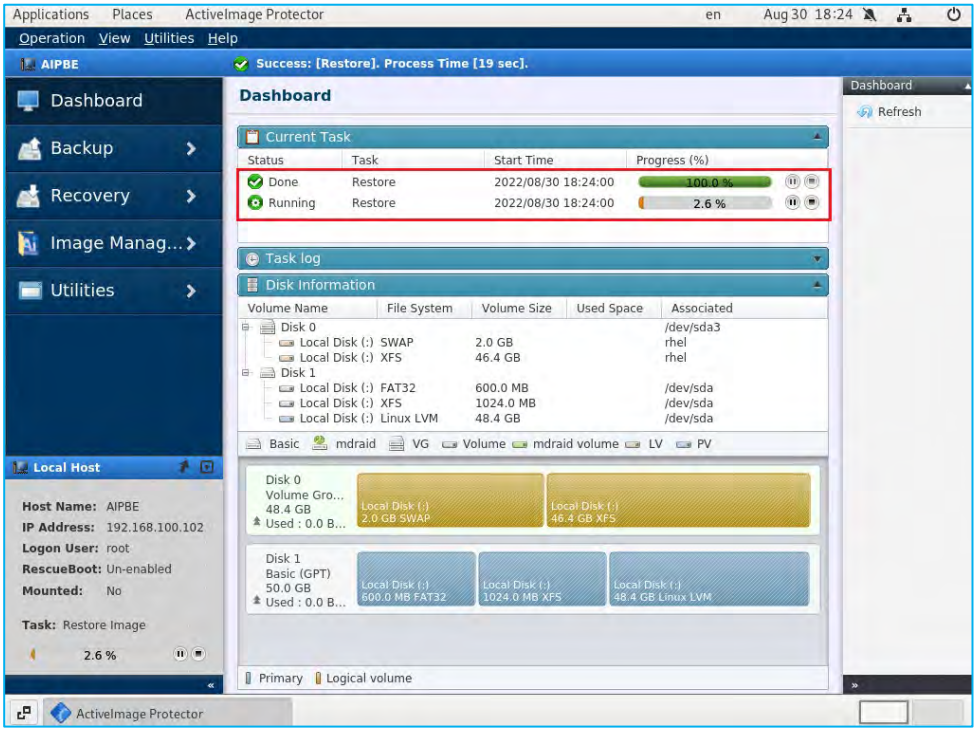
18. Please make sure the information displayed in **[Target Settings]** is correct and click **[Next]**.



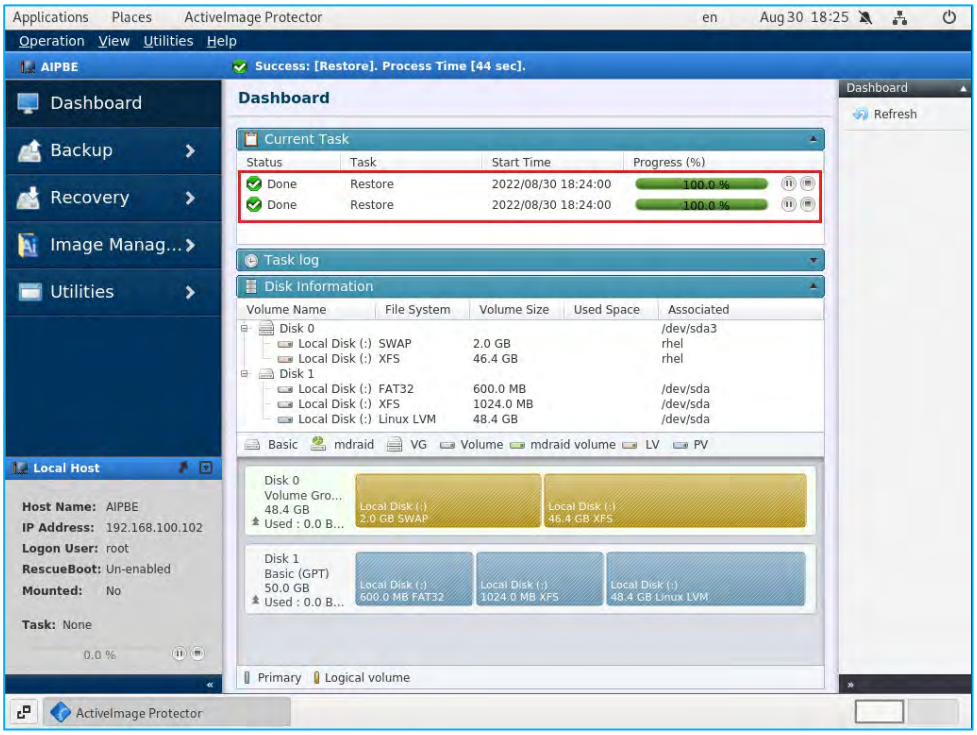
19. Please review the settings in **[Summary]** window and click **[Done]**.



20. When the recovery task starts, the console defaults to Dashboard view indicating the progress of the tasks. After the physical disk is restored, the recovery task for the volume group (VG) subsequently starts.



21. When the progress bar reaches 100% the recovery is complete. Please remove the boot environment media and select **[Operation]** -> **[Done]** in the console menu. Shut down or reboot the system.

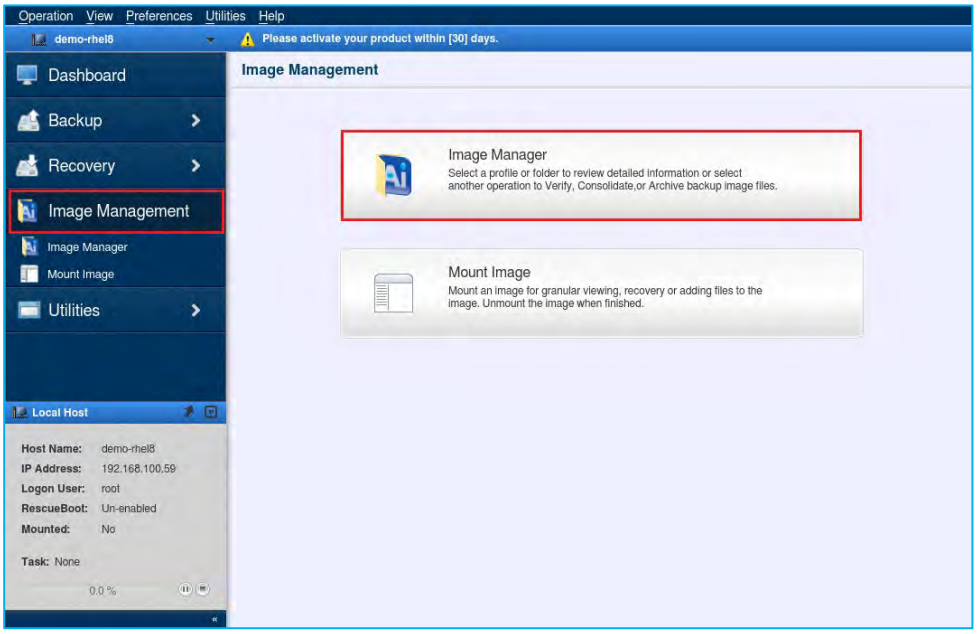


7. Image Management – Image Manager

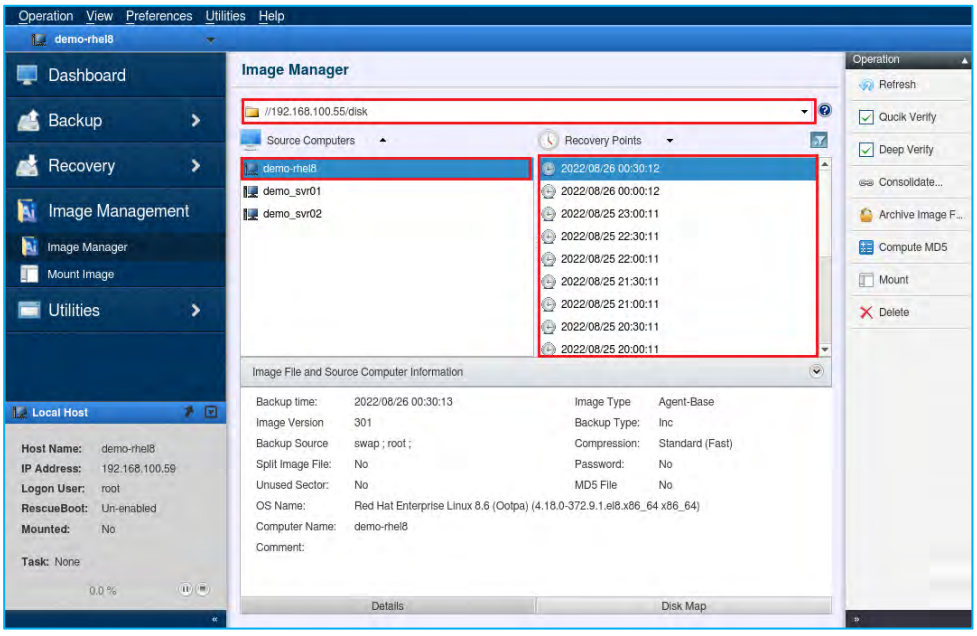
These tools are provided to enable you to manage various operations related to image files.

7-1. Image Manager

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



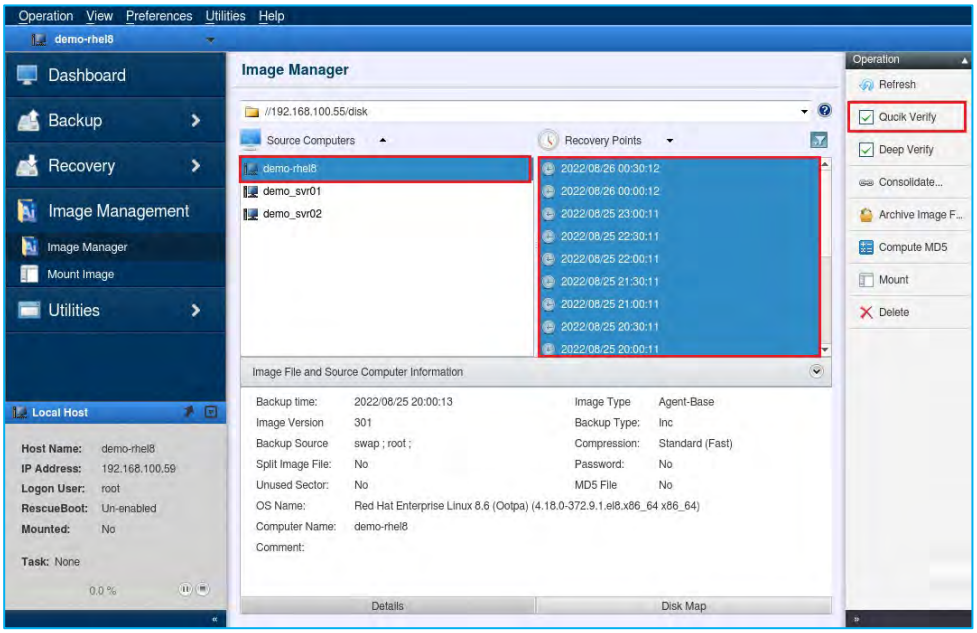
2. Please select a folder where backups are saved. Select **[Source Computer]** and **[Recovery Point]** for the backup to run an image management operation.



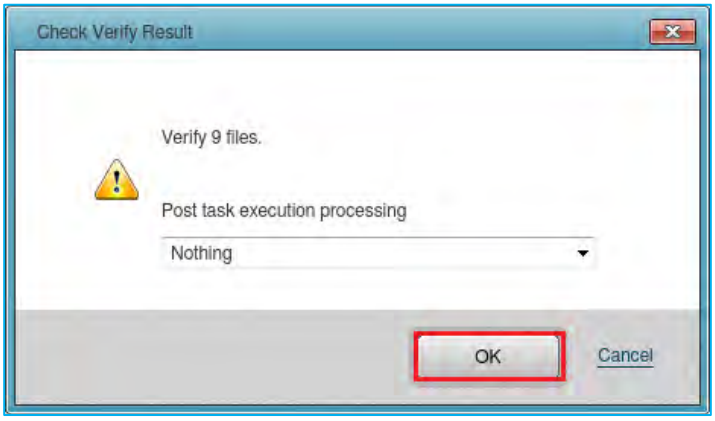
7-2. Quick Verify

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

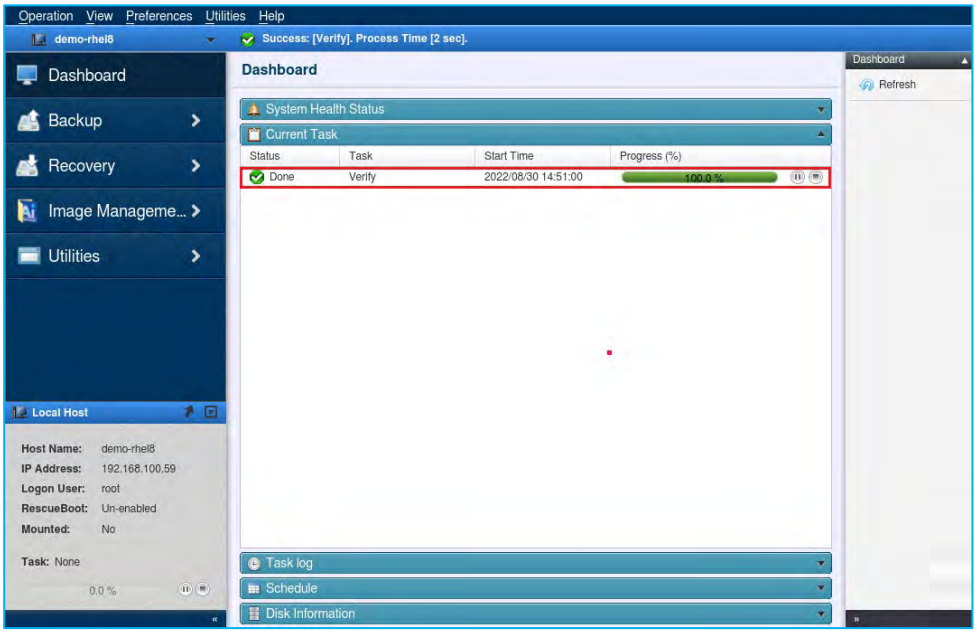
1. Select **[Source Computer]** and **[Recovery Point]** and click **[Quick Verify]** in the right pane. To select multiple recovery points, hold down the SHIFT/CTRL key and click on the starting and ending recovery points.



2. Click **[OK]** to start Quick Verify task.



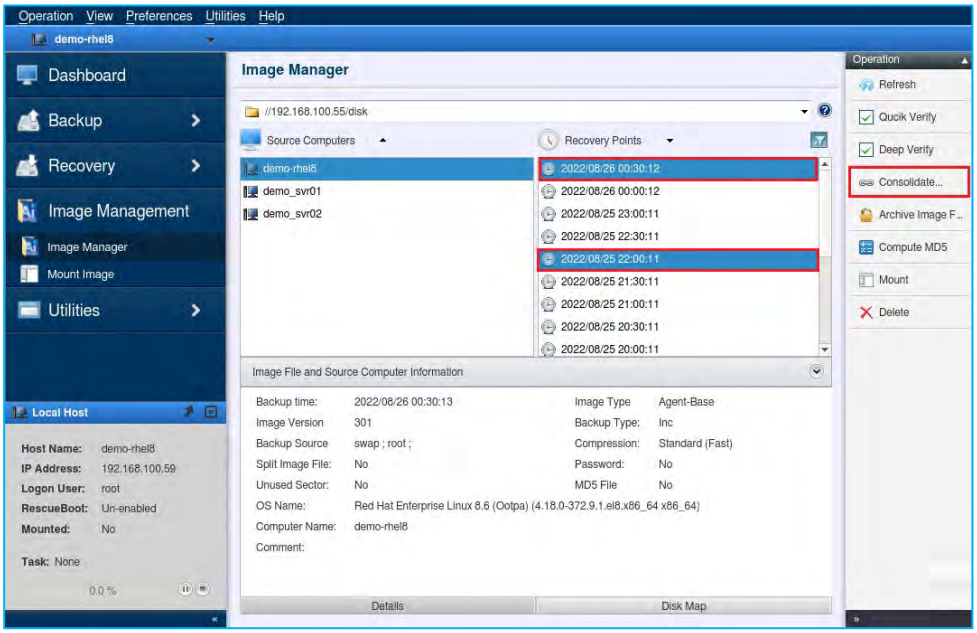
3. When Quick Verify task successfully completes, the following window will be displayed.



7-3. Consolidate backups

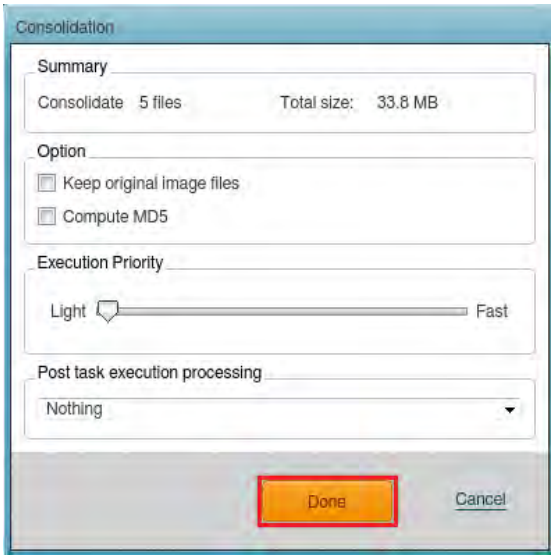
Reduce the number of files and save space using consolidation to consolidate your incremental backups.

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 “2022/08/26 4:30” is selected as the beginning and “2022/08/26 6:30” for the ending of incremental backups to consolidate.

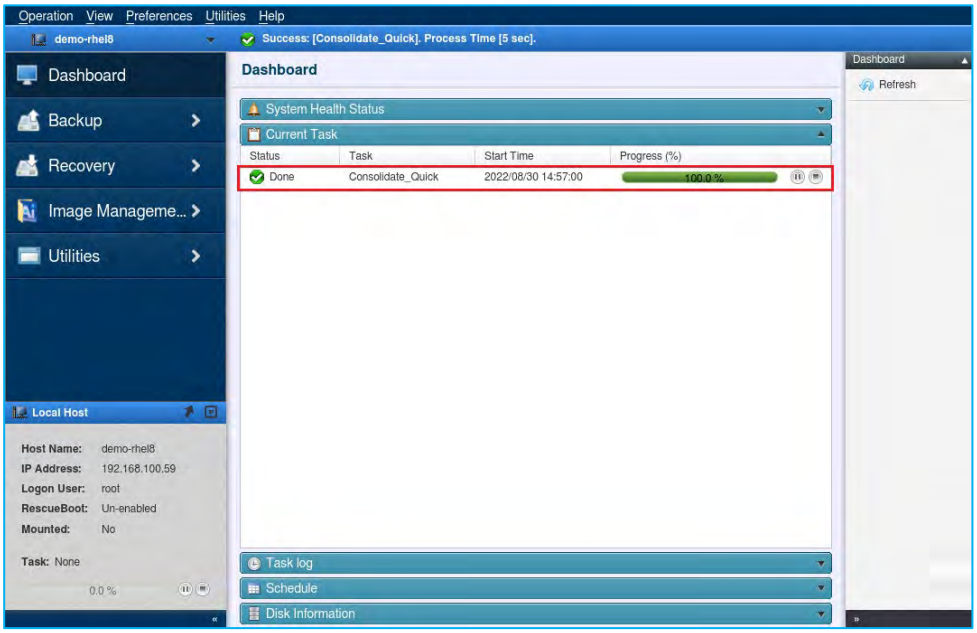


2. The following options can be set.

- **Keep original image files -** By default, the original backups will be deleted after the consolidated file is created. Check this box to retain the original files.
- **Compute MD5 -** Check this box to create an MD5 checksum file for the consolidated backups.
- After selecting the option, click **[Done].**



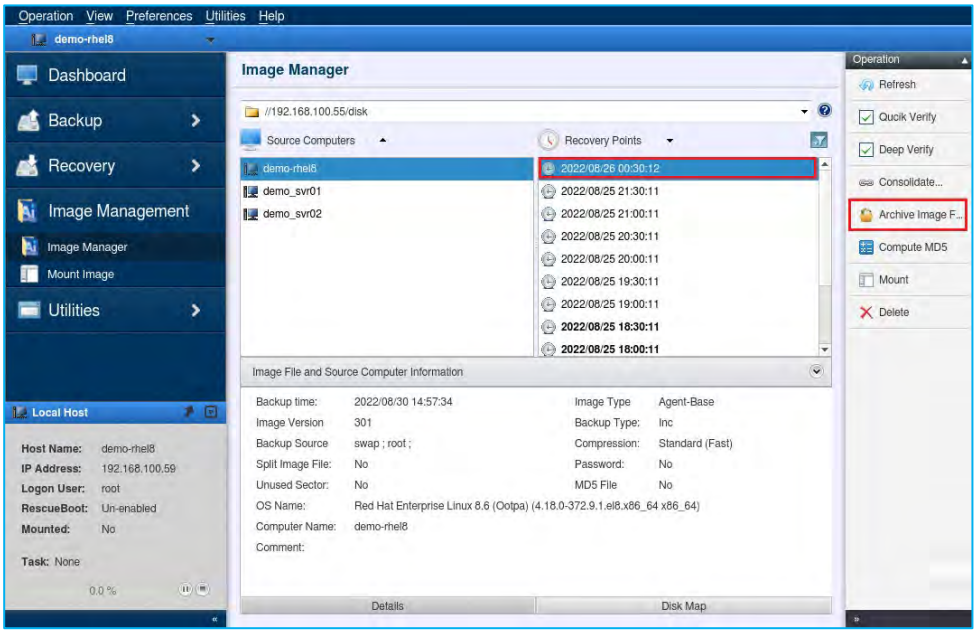
3. When Consolidation task successfully completes, the following window will be displayed.



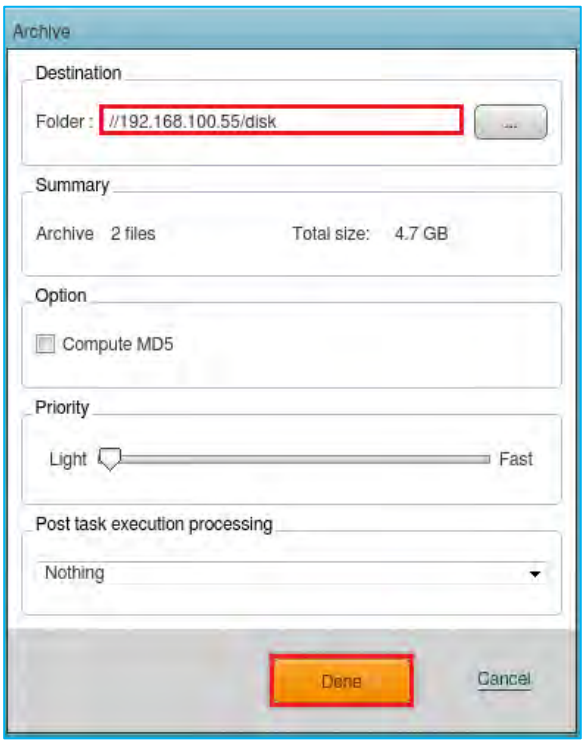
7-4. Archive backups

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

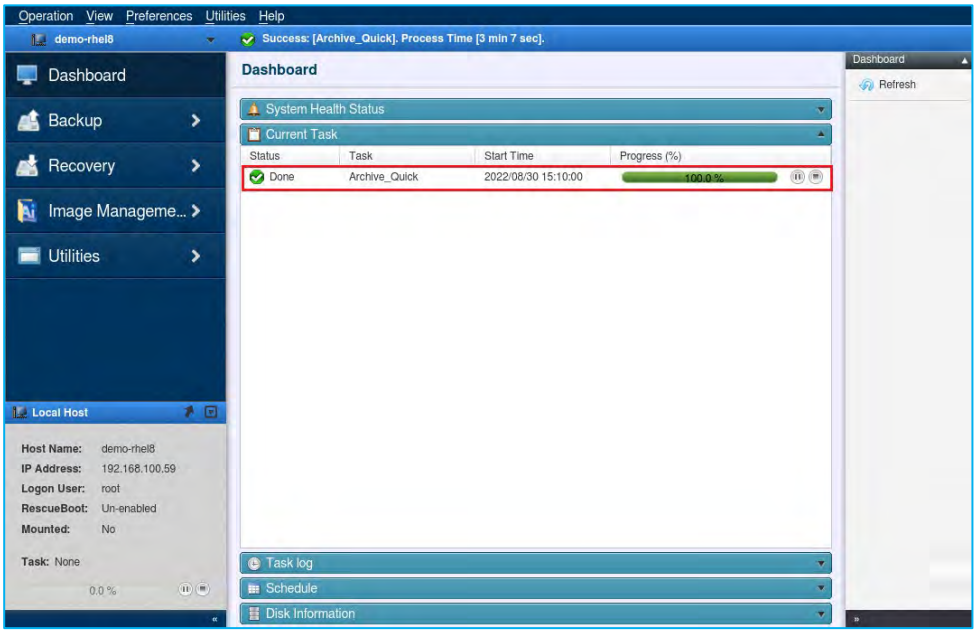
1. Select the latest [Recovery Point] and click [Archive Image] in the [Operation] menu.



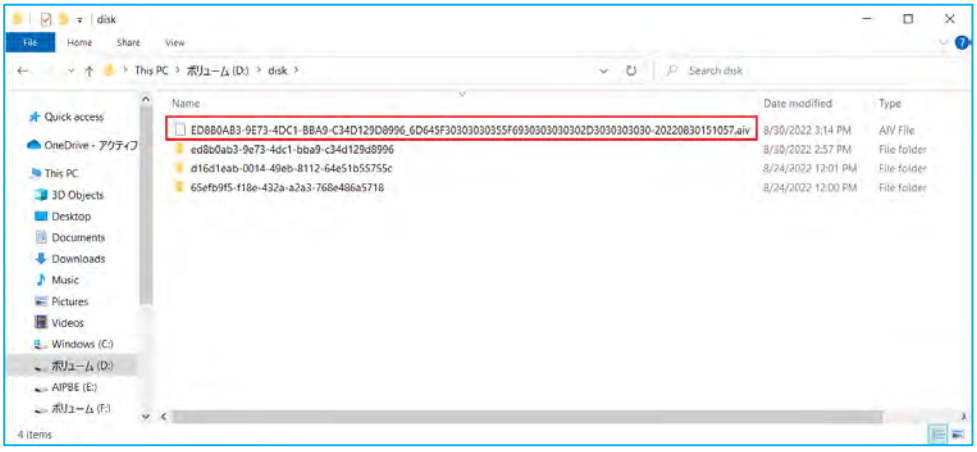
2. A popup dialog showing the number of selected backups and the total output size of the archive will be displayed. Please specify a destination that has enough space to save the archive file. Click [Done] to start the archival process.



3. When the archive is complete, the following window is displayed.



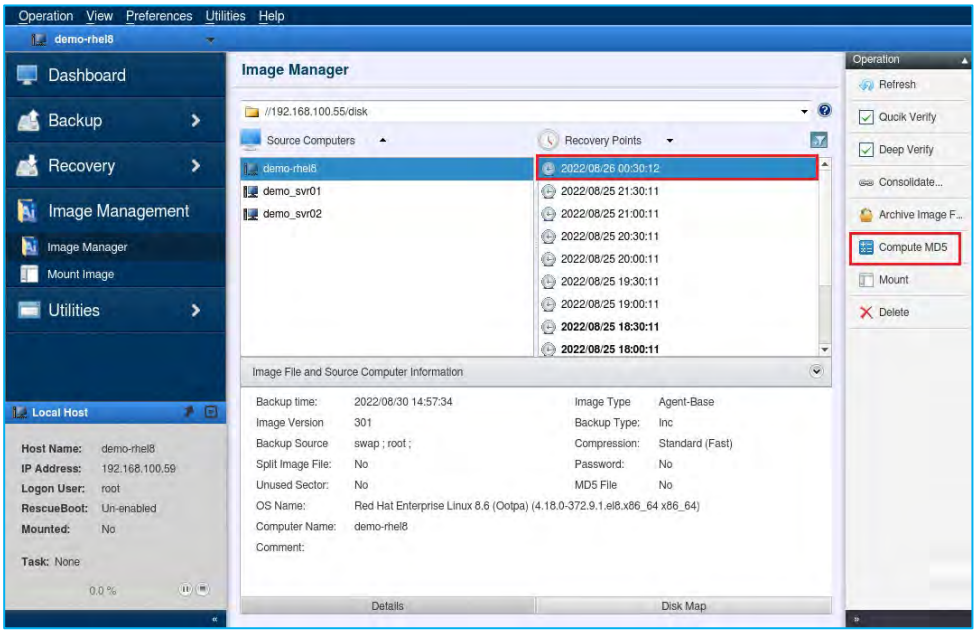
4. The archived file is created the location specified.



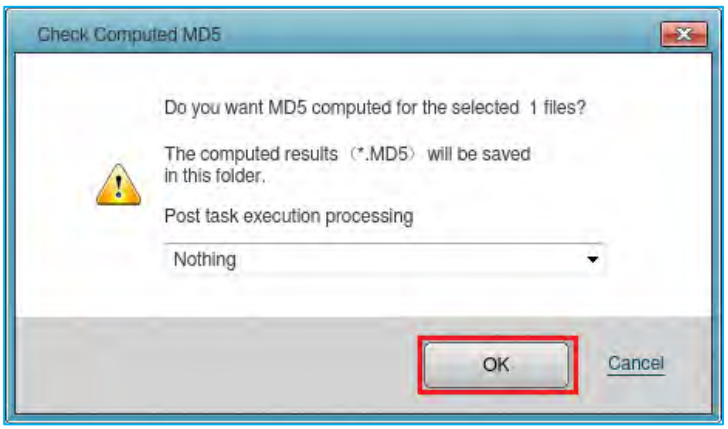
7-5. Create a MD5 file for the image (Compute MD5)

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 in a copy of the backup.

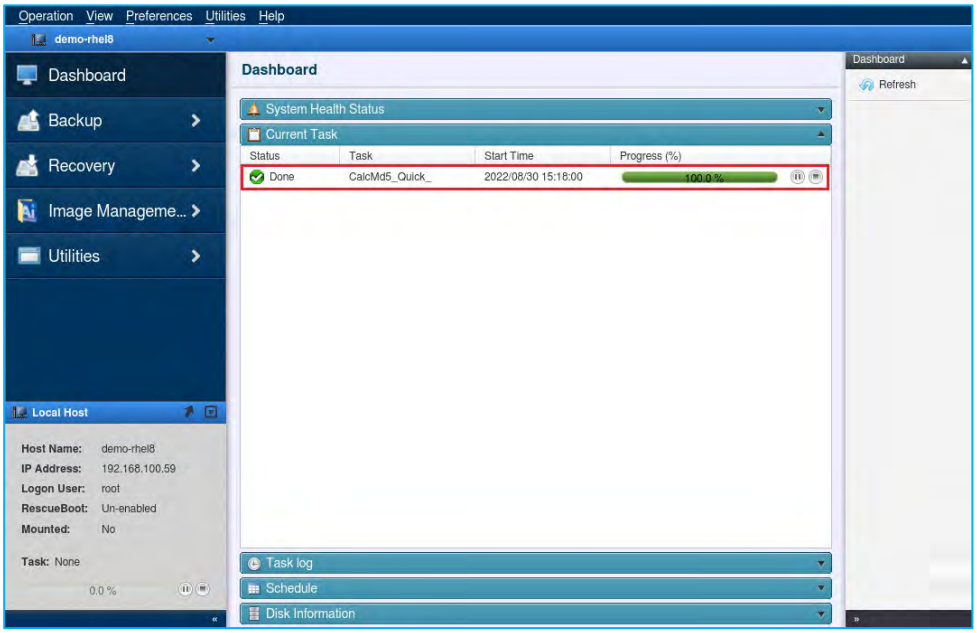
1. Select **[Source Computers]** and **[Recovery Points]**, and click **[Compute MD5]** in **[Operation]** menu. When creating MD5 checksum for multiple backups, hold down the SHIFT/CTRL key and click on the starting and ending recovery points.



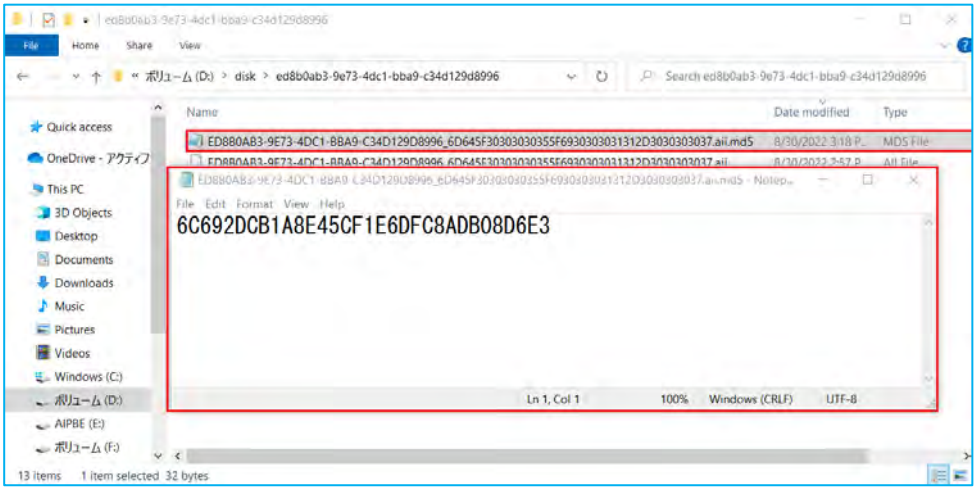
2. Click **[OK]**.



3. When the MD5 checksum file is complete, the following window is displayed.



4. You can verify the MD5 file was created on Windows OS by browsing to the folder.

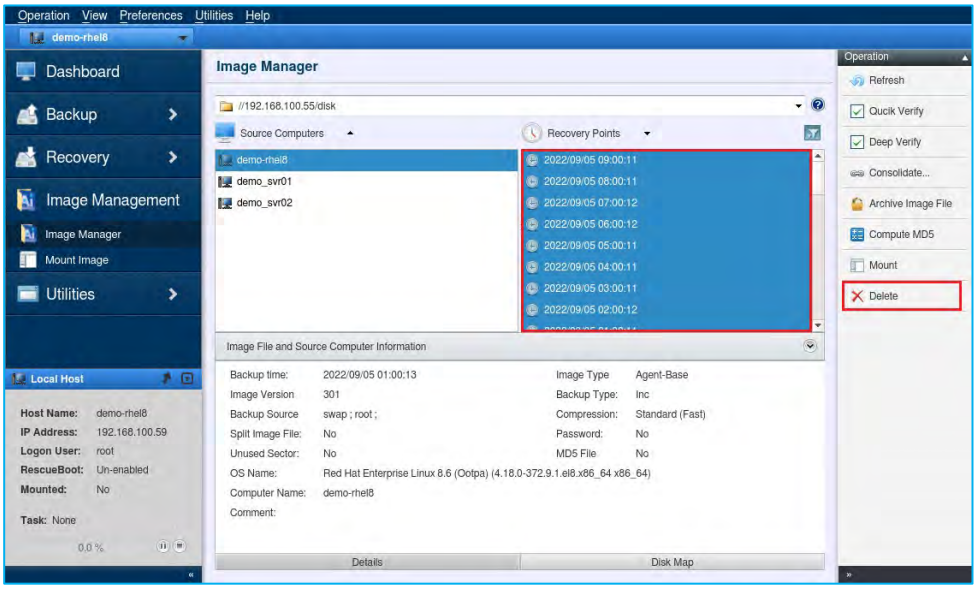


7-6. Delete Backup Files

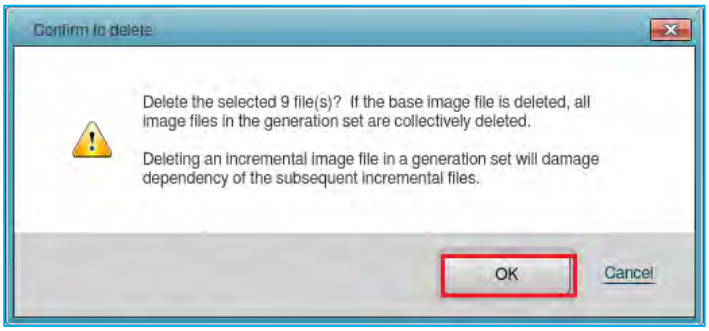
Specified backup files can be deleted.

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

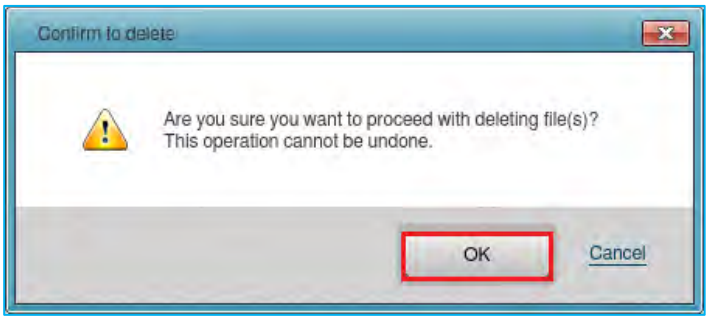
1. Select **[Source Computer]** and **[Recovery Point]** of a backup to delete. Click **[Delete]** in the **[Operation]** pane. To select multiple files, hold down the SHIFT/CTRL key and click on the starting and ending backup points.



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



3. The following confirmation message is displayed. Click **[OK]** to delete the backup file.



7-7. Image Manager: Mount Image

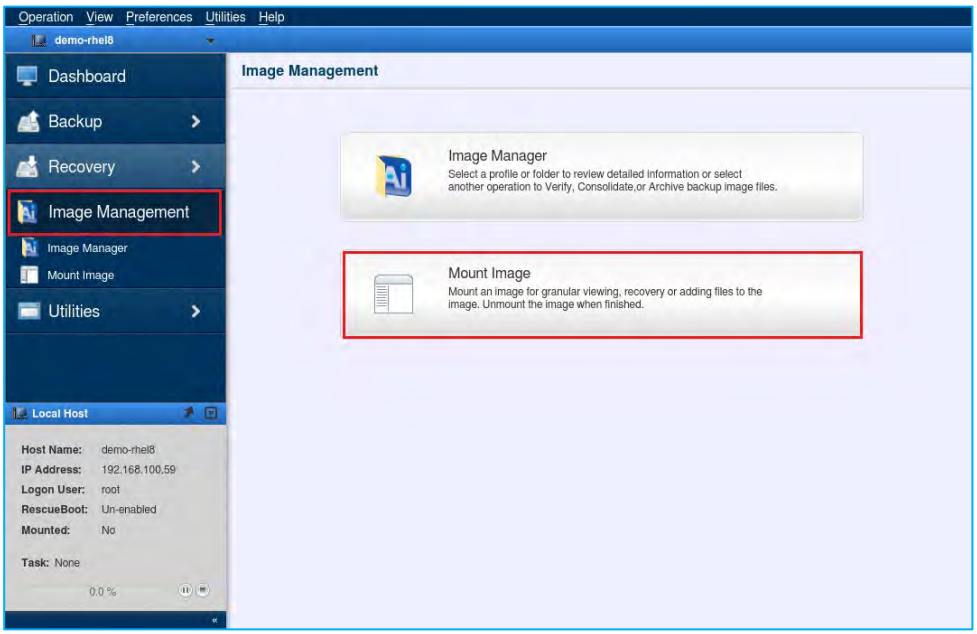
The Mount Image feature allows you to mount a backup on the OS file system and assign a drive letter. A mounted image can be browsed from file explorers and files and folders can be copied from ActiveImage Protector backups.

Note: When specifying a network shared folder as the backup destination, you need to mount the folder on the local system.

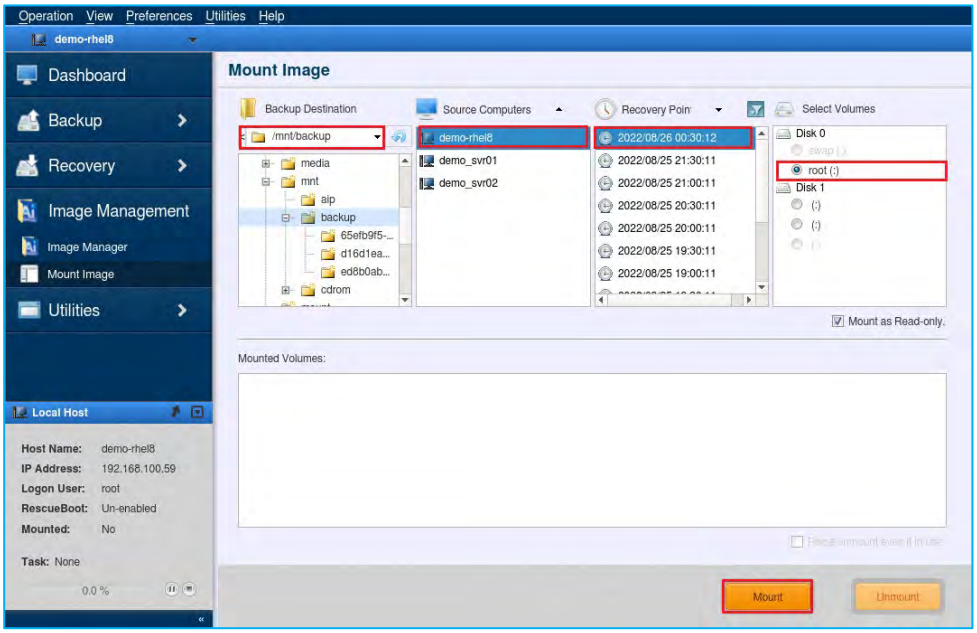
1. Please mount the network shared folders that are specified as backup destination on the local file system first. This example shows a folder mount “backup” is created under “/mnt” by running the following command from terminal, the shared folder specified as the destination is being mounted.

```
# mkdir /mnt/backup
# mount -t cifs -o username=Administrator,password=xxxxxxxx //192.168.100.55/disk /mnt/backup
```

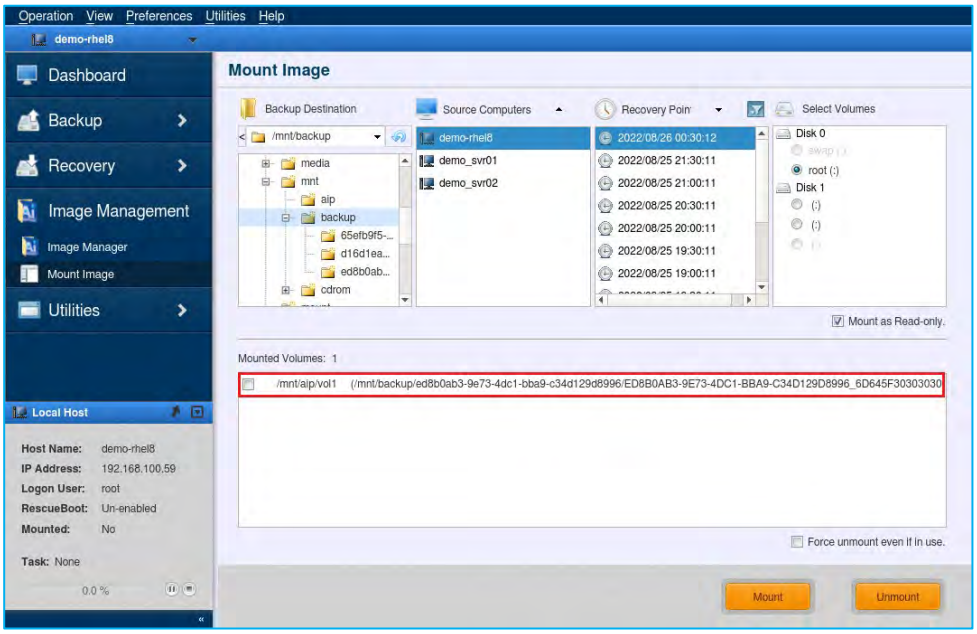
2. Start a Mount Image task. Select **[Image Management]** in the left pane and **[Mount Image]**.



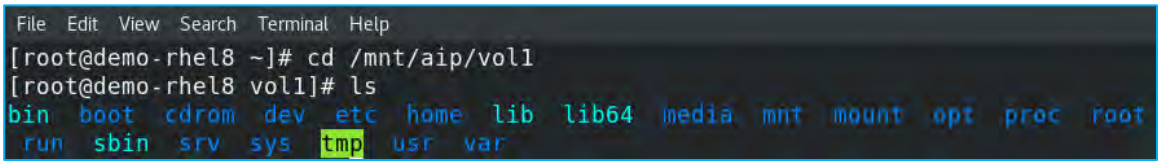
3. Mount a backup of a computer. In this example, "/mnt/backup" is selected for **[Backup Destination]** this was the destination shared folder mounted on "/mnt/backup" in the previous step. Select a **[Source Computer]** and a **[Recovery Point]** in the backup. Next, select the volume to mount in **[Select Volumes]** and click **[Mount]**.
   Note: The backup is mounted as writable by disabling the **[Mount as Read-only]** option. The changes made to the backup are saved in a differential backup (.aix) after the volume is unmounted.



4. The mounted volume is added to **[Mounted Volumes]** list.

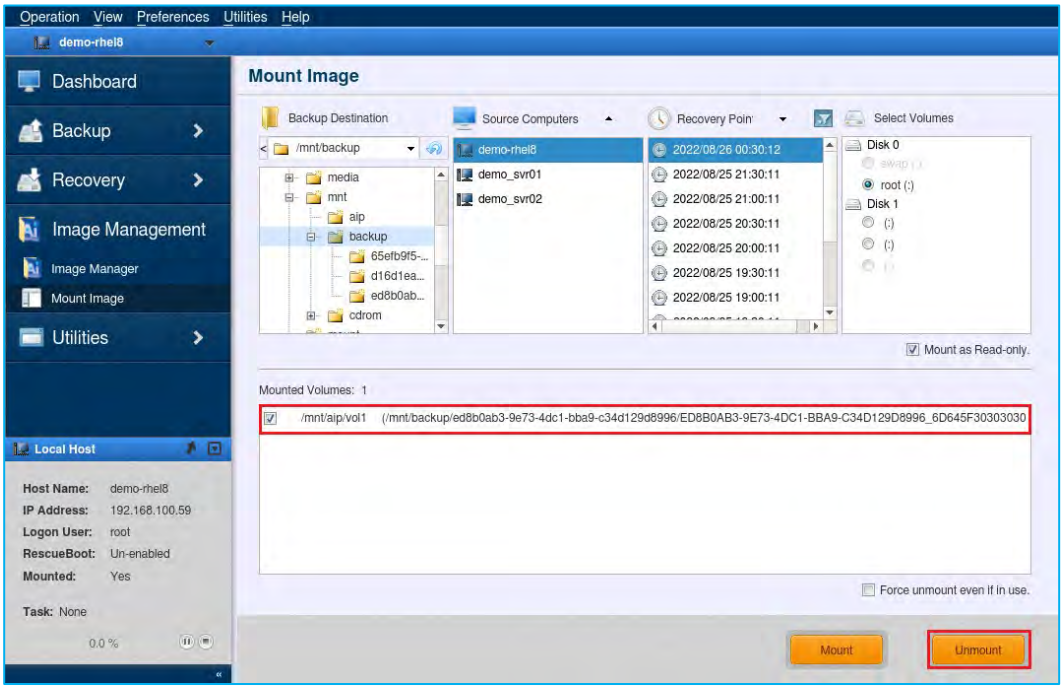


5. As shown below, the volume “root” is mounted to “/mnt/aip/vol”. When mounted, you can browse the contents, enabling you to open or copy files.



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

Note: If the volume fails to unmount, enable **[Force Unmount Volume]** and unmount the volume.

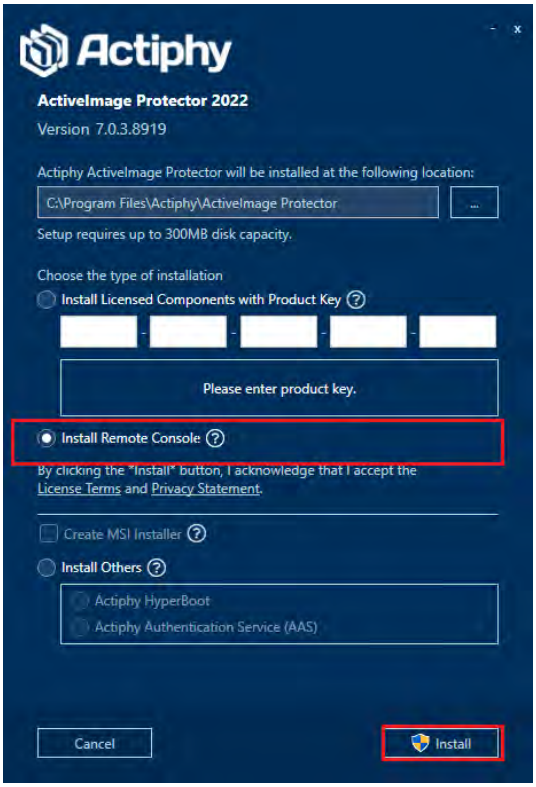


8. Remote Management Console

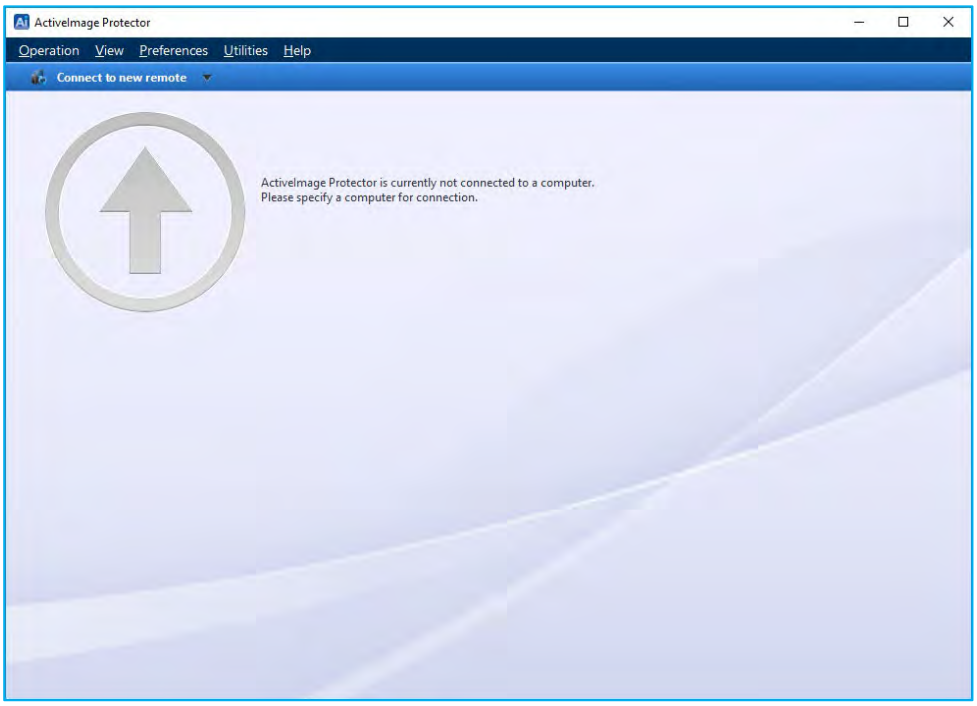
Please use the following steps to install ActiveImage Protector's remote console and connect to the remote console.

1. Install remote console

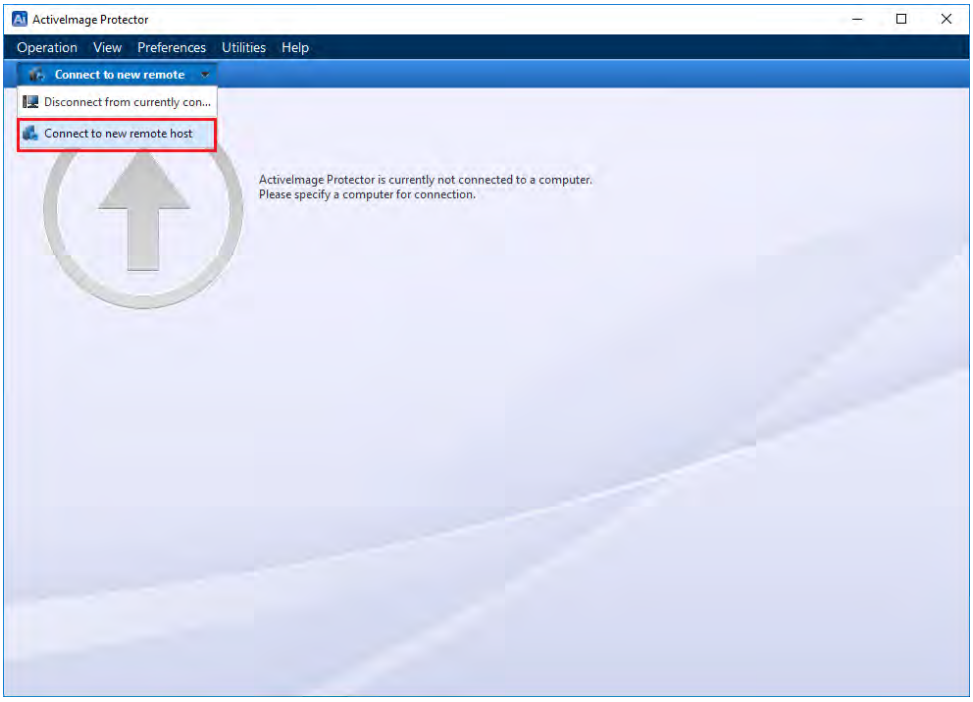
   Run ActiveImage Protector's installer "Setup.exe" in "Setup" folder in the product media on Windows computer and install the remote console. After running "Setup.exe", and the installer start up, please tick the checkbox for **[Install Remote Console]** and click **[Install]** to begin the installation.



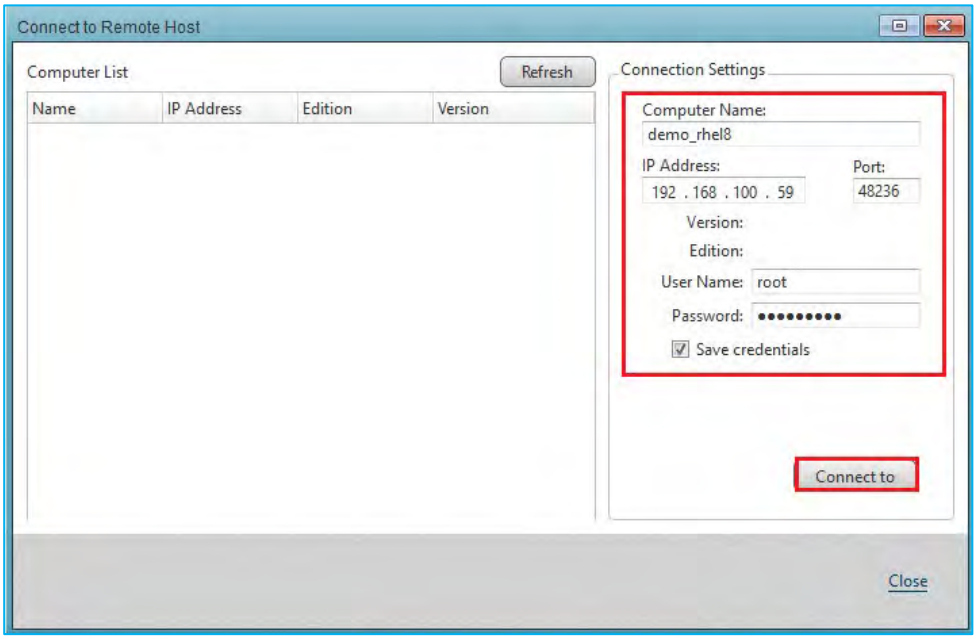
2. When the installation completes, go to Windows **Start** menu - **[Actiphy]** → **[ActiveImage Protector]** to start the remote console.



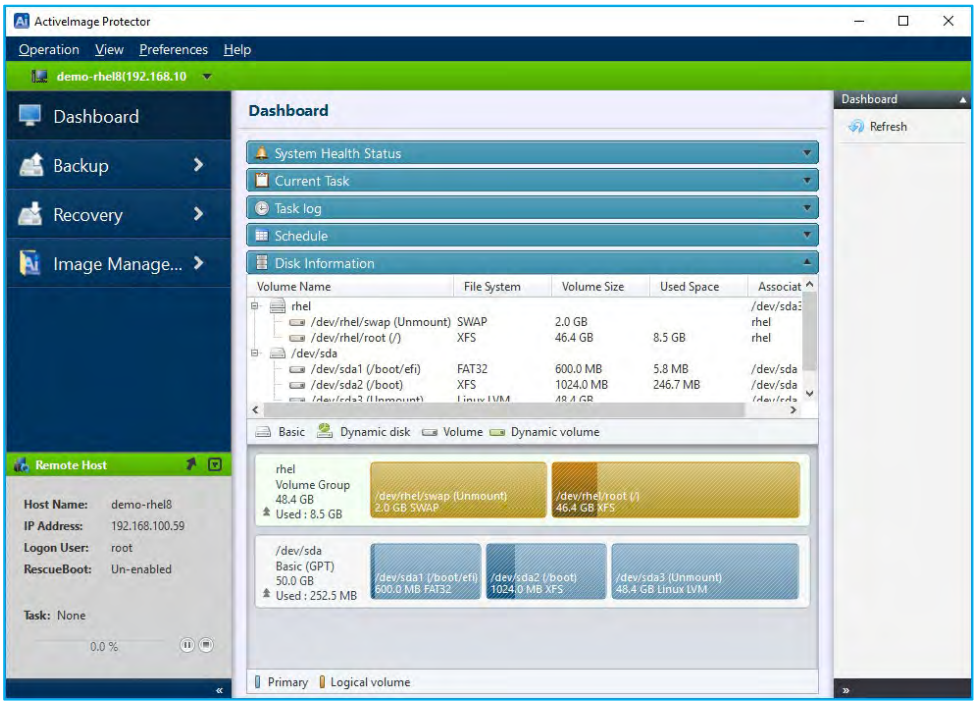
3. Click **[Connect to new remote host]** in the pull-down menu at the left upper corner of the console.



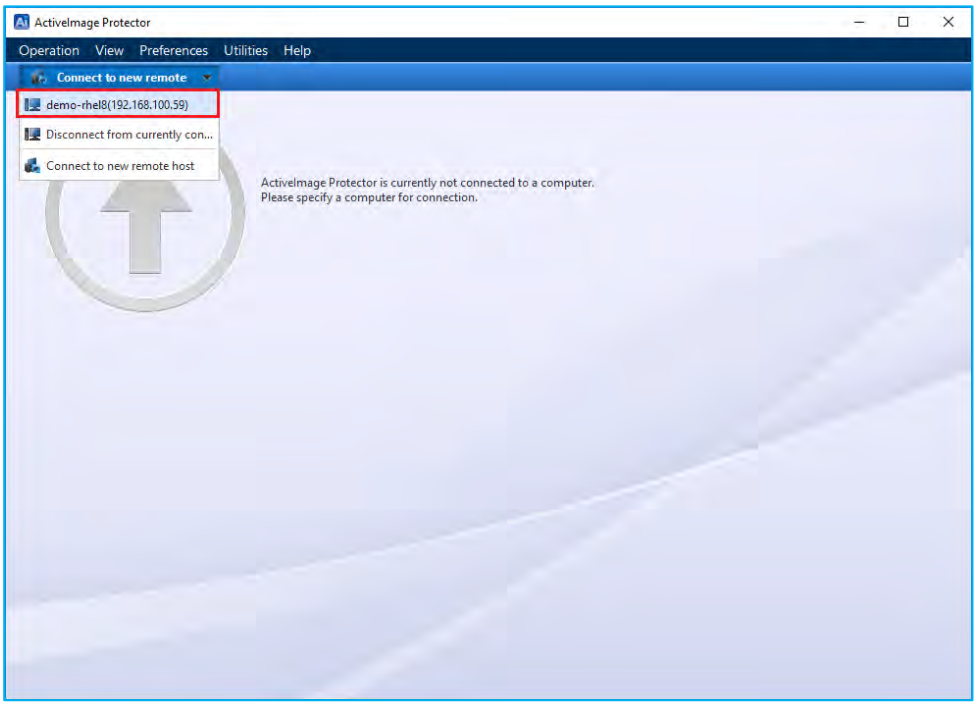
4. In **[Connection Settings]** enter your credential information to access the computer you want to manage remotely. Click **[Connect to]**.

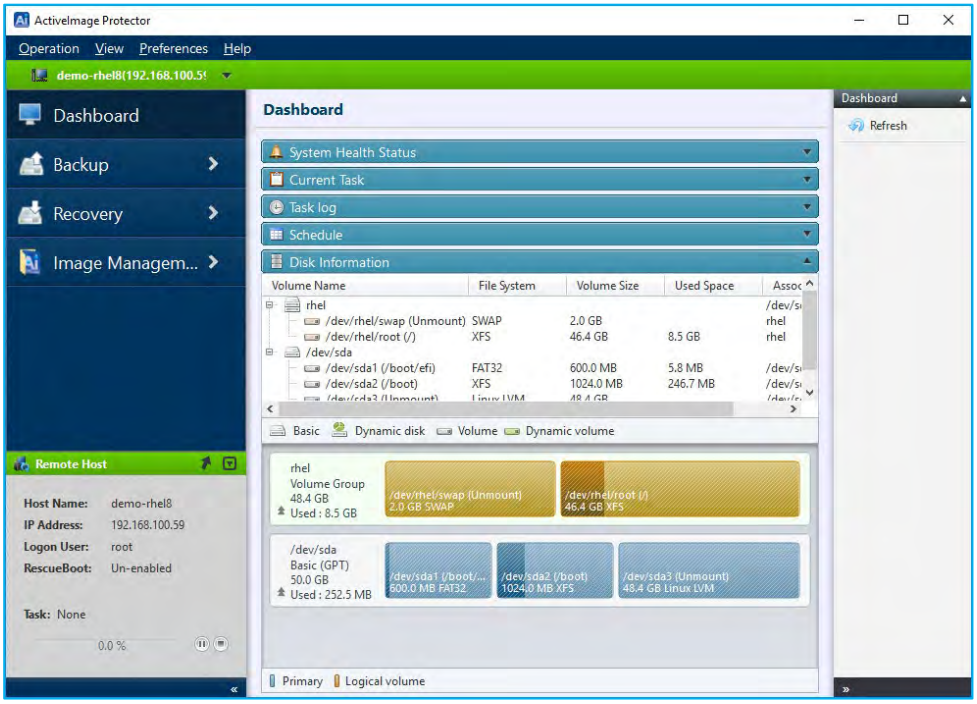


5. When the remote console is successfully established, the status bar will turn green. Most operations such as running backup/recovery tasks, image management operations and monitoring log information can be done on remote clients.



6. After having connected one time, the computer is registered as remote host in the pull down. To disconnect from the remote client and return to the local client, double click on the local host name





9. 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