



ActiveImageTM 2018 Update **PROTECTOR**

Server / Desktop Edition (Update)/for Hyper-V Startup Guide

3rd Edition June, 2019

Table of Contents

1. Overview	1
2. Installation	3
3. Product Activation	9
4. Backup.....	12
4-1. Backup Now	12
4-2. Scheduled Backup	20
5. Boot Environment Builder	36
Build Windows-PE based Boot Environment	36
6. Restore	42
6-1. File Recovery	42
6-2. System Recovery	47
7. Image Manager	56
7-1. Verify Image.....	58
7-2. Consolidate Image Files	59
7-3. Archive Backup Image File	61
7-4. Compute MD5 hash value	62
7-5. Delete	65
8. Mount Backup Image.....	66
9. Image Management –iSCSI Target Server	69
9-1. Mount Backup Files to Local Disk	70
9.2 Attach virtual disk to virtual machine	85
10. Manage Remote Host	96
10-1. Push Install	96
10-2. Network client management console.....	101

11. vStandby.....	105
12. ImageBoot.....	113
APPENDIX.....	121

1. Overview

ActiveImage Protector is a backup and recovery solution designed with the latest sector-based disk imaging technology to flexibly support Windows machines in a variety of system environments ranging from legacy machines to the latest virtual machines.

ActiveImage Protector provides features essential for a backup solution such as Hot Imaging feature allowing you to back up a running system, Cold Imaging feature enabling you to create a backup image of a clean Windows system before starting it up, fast Incremental Backup that includes only the sectors that have changed since the last full or incremental backup image was written, Command Line Interface allowing backups to be administered by third-party system management tools.

System Requirements

The following are the system requirements for ActiveImage Protector Server Edition / Desktop Edition (Update) and for Hyper-V Enterprise.

Before you start using ActiveImage Protector Server Edition / Desktop Edition, please ensure that the following system requirements are met.

CPU	Pentium 4 or above CPU
Main Memory	1024MB or more is required.
Hard Disk	1.5GB or more of available disk space is required.
DVD-ROM Drive	Necessary to install the product, boot or start up ActiveImage Protector boot environment
Supported Operating System (Server Edition Update)	Windows: Windows Server 2019, Windows Server 2016, Windows Server 2012 and 2012 R2, Windows Server 2008 (x86/x64) and 2008 R2, Windows Storage Server 2016, Windows Storage Server 2012 and 2012 R2, Windows Storage Server 2008 and 2008 R2, Windows Server 2003 SP2 (x86/x64) R2 Hypervisor: Windows Server 2016 Hyper-V (Hot & Cold Imaging), Windows Server 2012 and 2012 R2 Hyper-V (Hot & Cold Imaging), Windows Server 2008 R2 Hyper-V (Hot & Cold Imaging)

Supported Operating System (for Hyper-V Enterprise)	Windows Server 2008 R2 or later server OS (including Hyper-V Server) on which Hyper-V is configured. *As for Windows Server 2008 R2, please make sure that Microsoft .Net Framework 4.5 or later is already configured.
--	--

* As to the limitations for using the product, please refer to the release note included in ActiImage Protector's media.

* This document includes the screen shots captured in Server Edition, the operating procedures are the same for Desktop Edition.

2. Installation

The following are the operating procedures required to install ActiveImage Protector on the machine specified as backup source.

1. Set the product media to the machine to start the installation launcher. Click on **[Install]**. If the launcher does not start, please execute Launch.exe in the product media.



Note) Server/Desktop Edition:

When you click on [ActiveVisor], you can install “ActiveVisor” . When you click on [Other products], you can install “ImageCenter LE” or “vStandby AIP” or “ImageBoot”.



Note) for Hyper-V Enterprise:

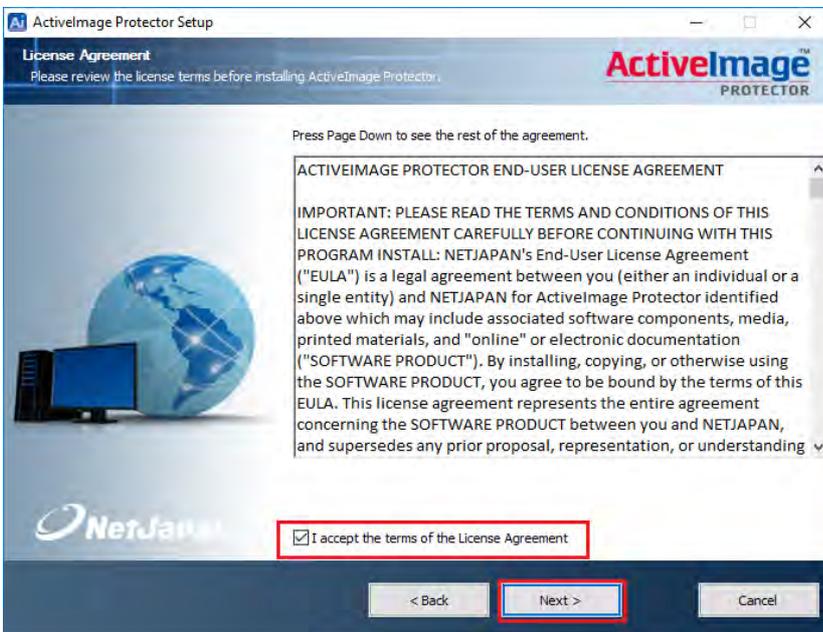
When you click on [ActiveVisor], you can install “ActiveVisor” . When you click on [Other products], you can install “ImageCenter LE” or “ReZoom it!”.



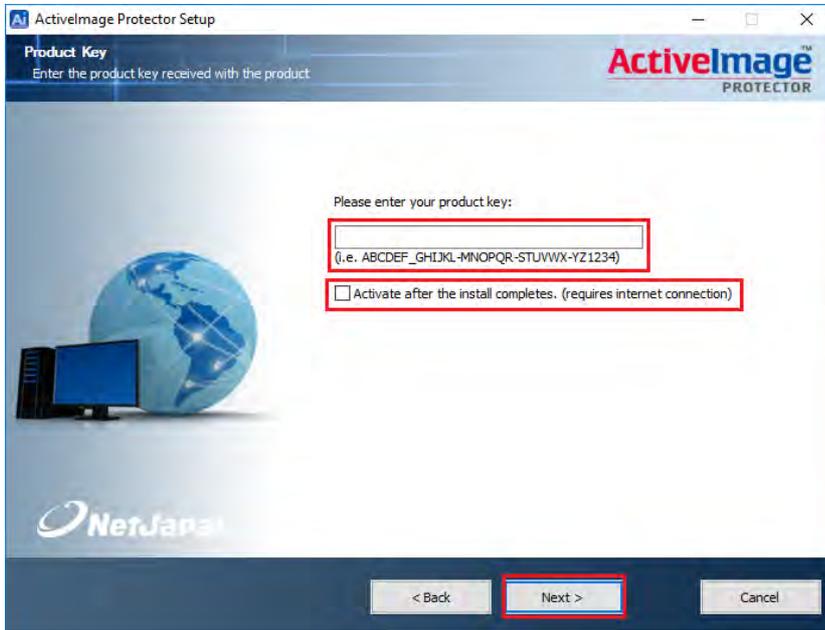
2. Click **[Next]**.



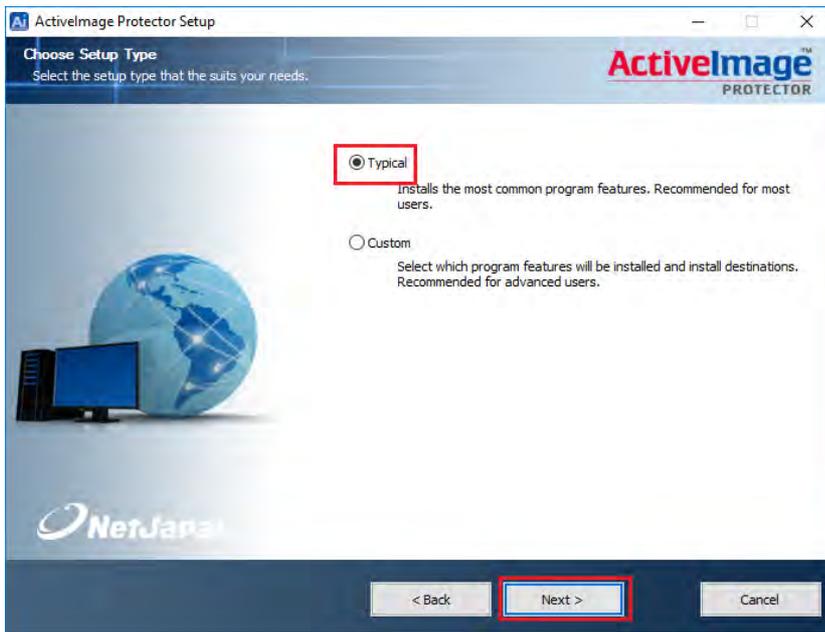
3. Please review the End User's License Agreement.
Check the box next to **[I accept the terms of the License Agreement]** to continue the installation. Click **[Next]**.



4. Enter the product key. **[Activate after the install completes]** option may be selected to automatically activate the product upon completion of the installation process. Click **[Next]**.



5. Select **[Typical]** for the setup type and click **[Next]**.



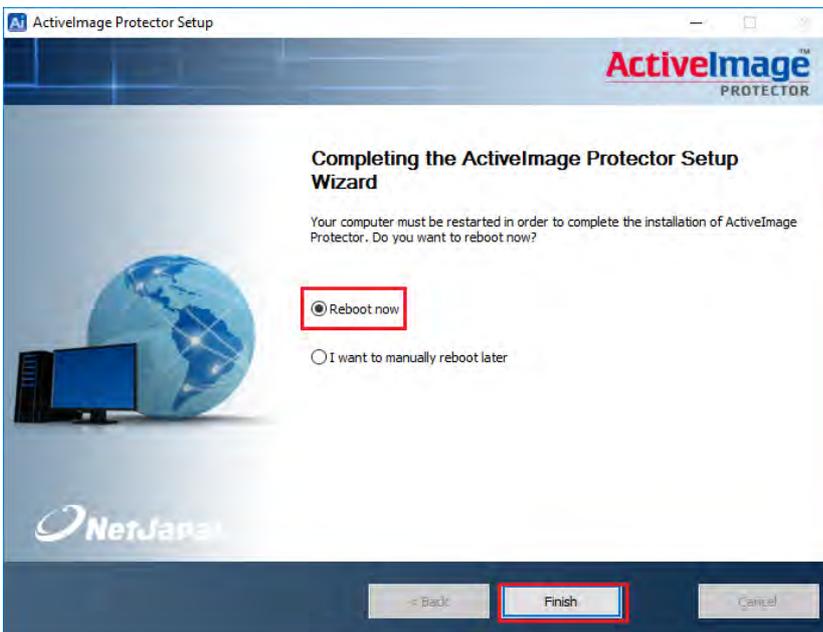
6. Review the installation settings and click **[Install]** to complete the installation.



7. Please wait until installation of ActiveImage Protector completes.



8. Upon completion of the product installation, eject the product media and select **[Reboot now]** to reboot the machine immediately and **[Finish]**. The machine is automatically rebooted.



3. Product Activation

Manual activation of the installed ActiveImage Protector terminates the live trial period. If the **[Activate after the install completes...]** was checked to automatically activate the product upon completion of installation, the following procedures are not required.

Two types of activation practices are supported; one is traditional online activation over the internet and the other is offline activation on standalone machine with no internet connection due to security reason.

Offline activation:

- No auto-update over network
- No E-Mail communication updating you with the latest information about ActiveImage Protector is provided from NetJapan.

The following are the operating procedures for online activation.

1. Start ActiveImage Protector

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

Windows 7 or earlier Desktop OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

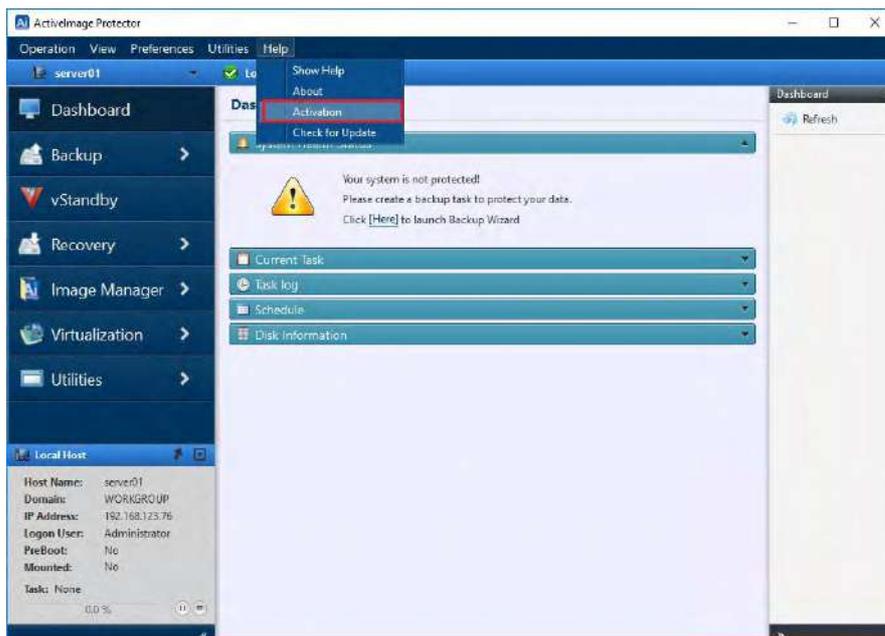
Windows Server 2012 or later server OS:

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

Windows Server 8 or later Desktop OS :

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

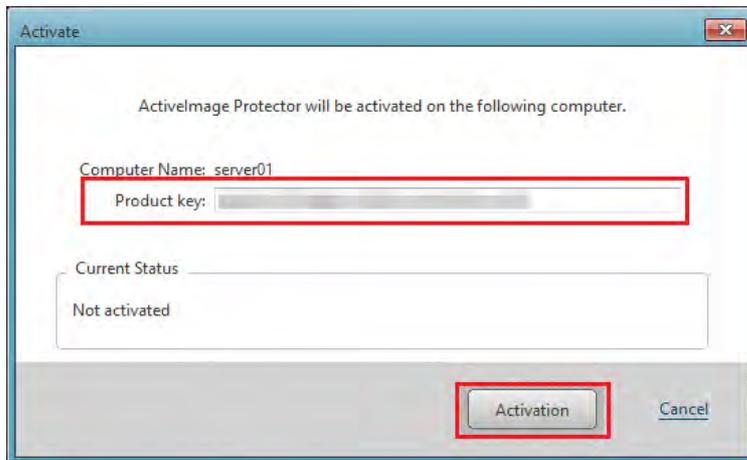
2. Click **[Help]** and select **[Activation]** from the drop down menu.



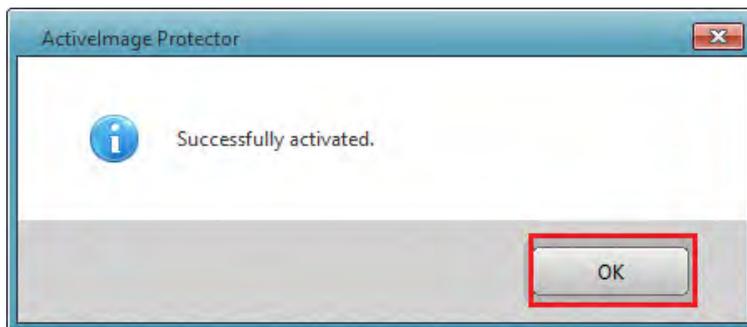
Note) The left pane of ActivImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



3. Enter the product key and click **[Activation]**.



4. When you get the following message, activation process completes. Click **[OK]**.



4. Backup

4-1. Backup Now

The following are the operating procedures for Backup Now.

1. Start ActivelImage Protector

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActivelImage Protector]**.

Windows 7 or earlier Desktop OS:

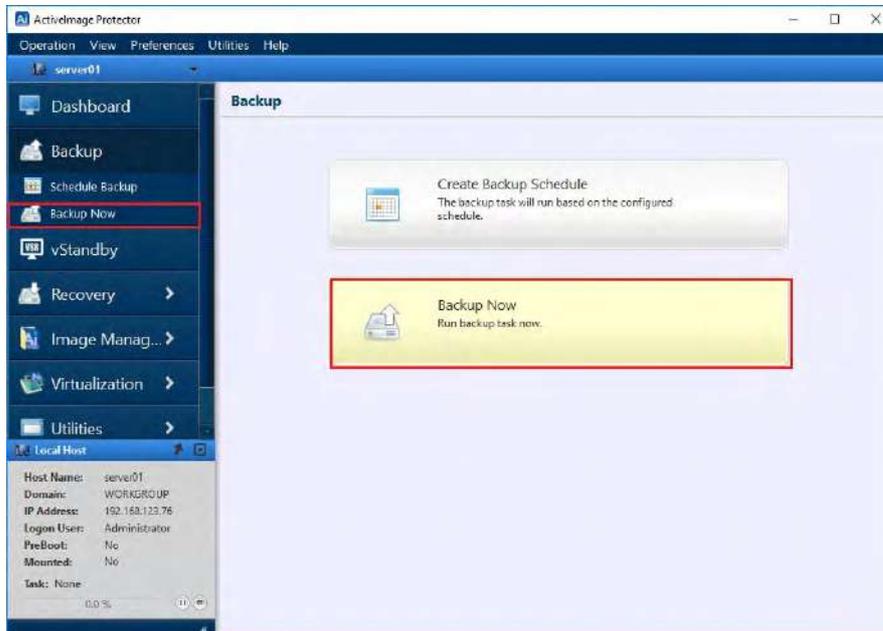
Click **[Start] – [All Programs] – [NetJapan] – [ActivelImage Protector]**.

Windows Server 2012 or later server OS: Click **[Start] – [Applications] – [NetJapan] – [ActivelImage Protector]**.

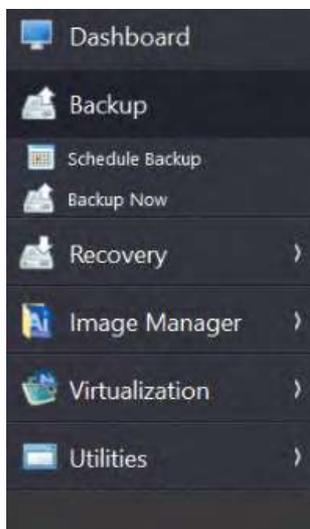
Windows Server 8 or later Desktop OS :

Click **[Start] – [Applications] – [NetJapan] – [ActivelImage Protector]**.

2. Click [Backup] – [Backup Now].



Note) The left pane of ActiVImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.

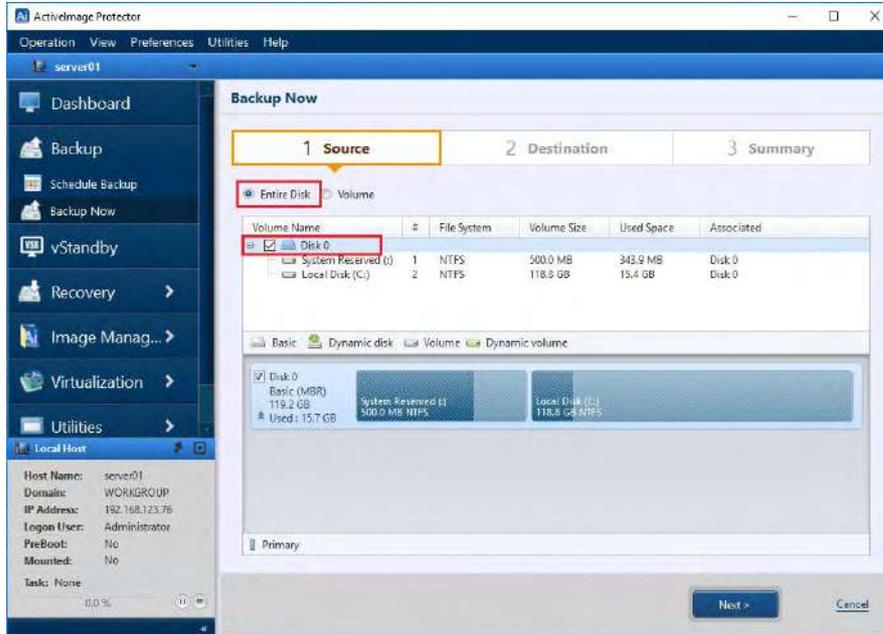


3. Select backup source.

The following example shows that the entire disk is selected for the backup source.

Click [Entire Disk] and check the checkbox for [Disk 0].

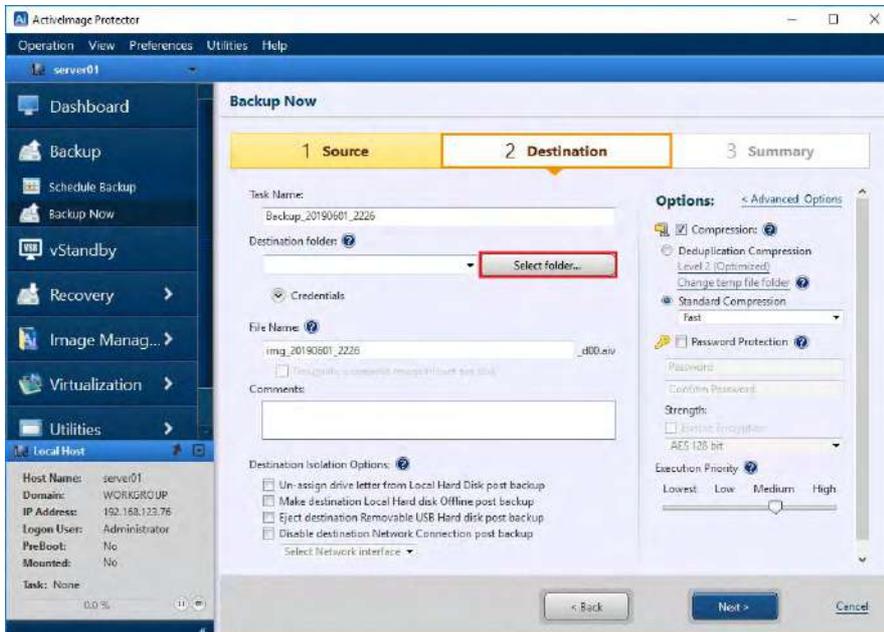
When the backup source is selected, click [Next].



4. Select a target destination for the backup image.

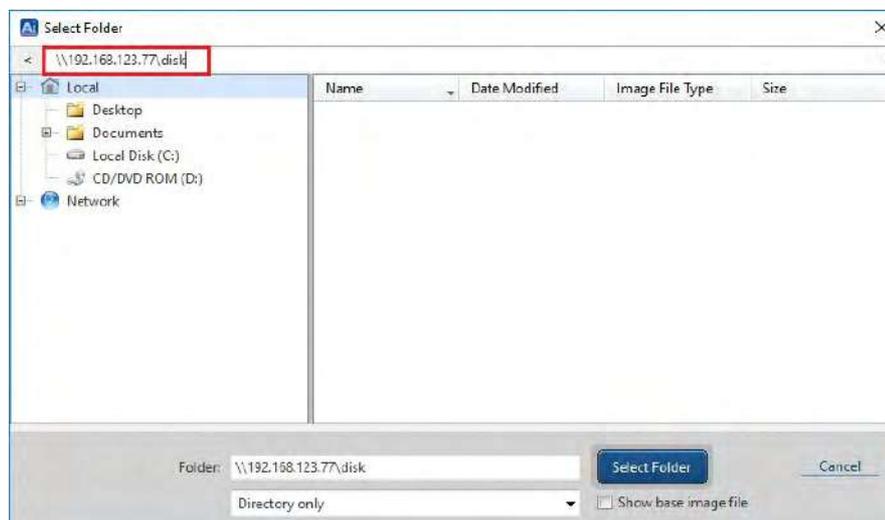
The following example show that “ [\\192.168.123.77\disk](#) “ in the network shared folder is specified for the target destination.

Click **[Select Folder]**.

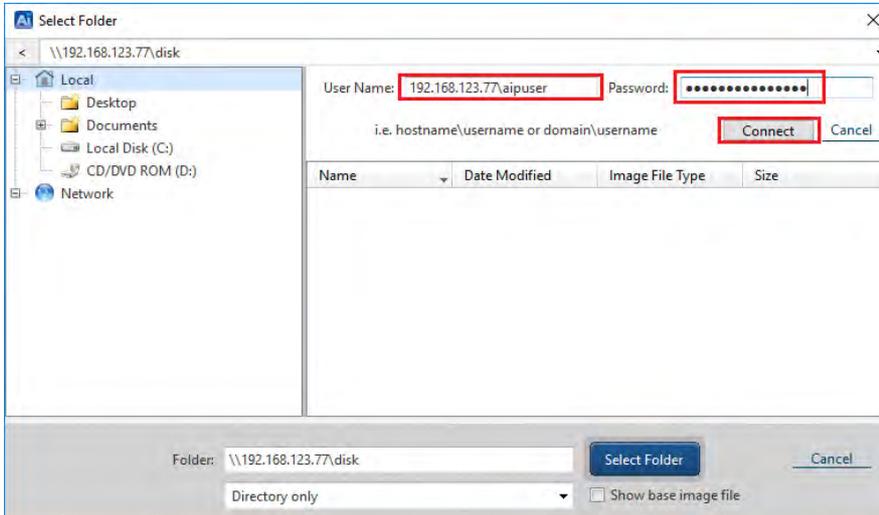


5. Please specify the path for the location of the target destination.

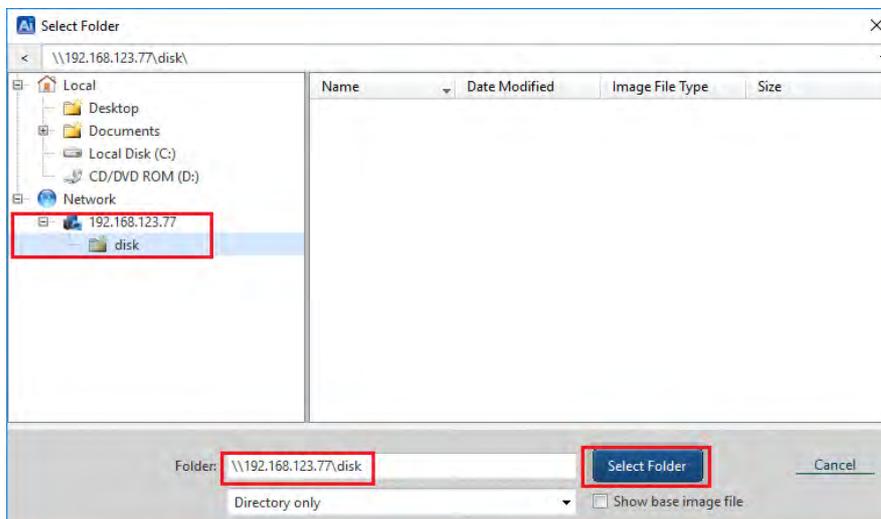
Please enter the following path “ [\\192.168.123.77\disk](#) “ for the target destination and press Enter key.



6. Please enter the credentials to access the target destination.
User Name must be specified in “Host Name \ User Name” format.
The following example shows that the host name “192.168.123.77” and user name “aipuser” are entered. The credentials are predefined to access the destination folder. Enter “ \\192.168.123.77\aipuser” for **[User Name]** and the password for **[Password]**. Click **[Connect]**.



7. Ensure the target destination is correctly specified and click **[Select Folder]**.

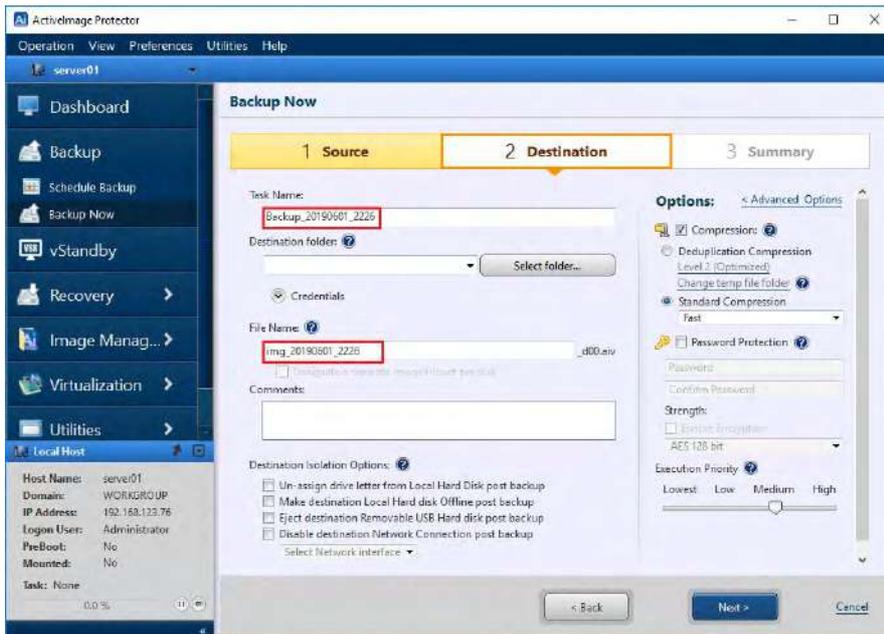


8. Specify the backup image file name.

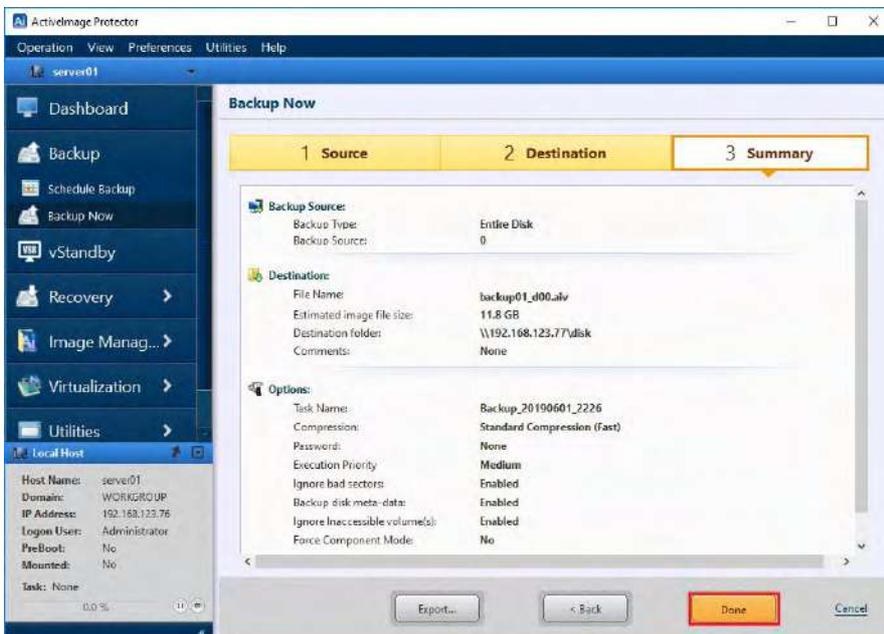
The following example shows that “backup01” is specified for the image file (the file extension is automatically entered.)

Destination Isolation feature is available only in ActiveImage Protector Update, disconnecting network access to backup image storage drives after backups complete. For more detailed description about **[Destination Isolation Options]**, please refer to “Scheduled Backup”.

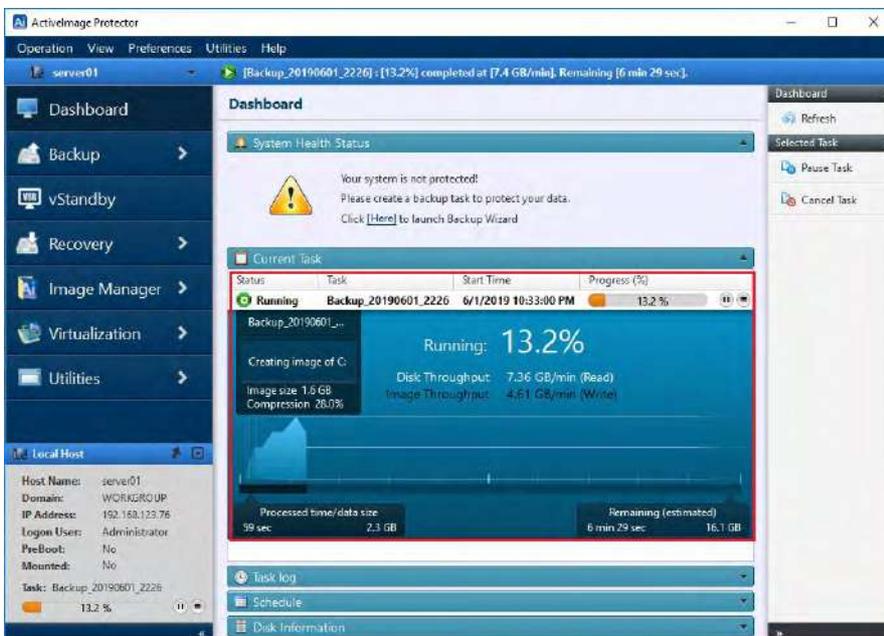
Enter “backup01” for **[File Name]** and click **[Next]**.



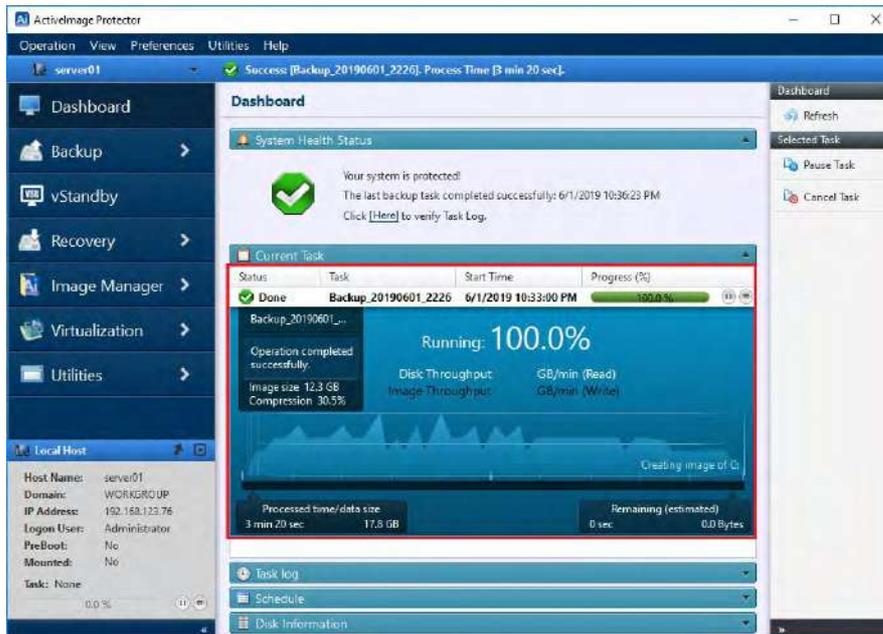
9. The backup configuration and option settings are displayed. Review the settings and click **[Done]** to start the backup task.



10. When the backup task is started, the current task information is displayed in **[Dashboard]**.



11. When the progress of **[Running]** task indicates “100%”, the backup process is completed.



4-2. Scheduled Backup

The following are the operating procedures for Scheduled Backup.

1. Start Activelmage Protector.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [Activelmage Protector]**.

Windows 7 or earlier Desktop OS:

Click [Start] – [All Programs] – [NetJapan] – [Activelmage Protector].

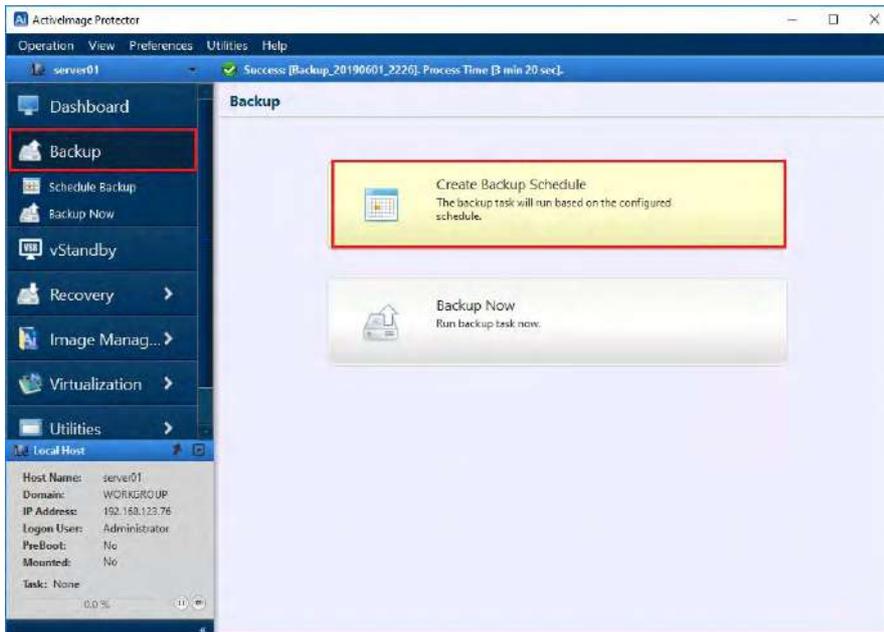
Windows Server 2012 or later server OS:

Click **[Start] – [Applications] – [NetJapan] – [Activelmage Protector]**.

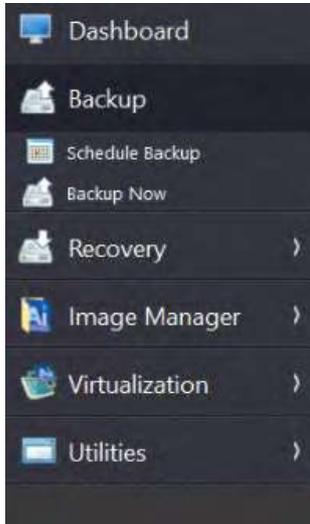
Windows Server 8 or later Desktop OS :

Click [Start] – [Applications] – [NetJapan] – [Activelmage Protector].

2. Click [Backup] – [Create Backup Schedule].

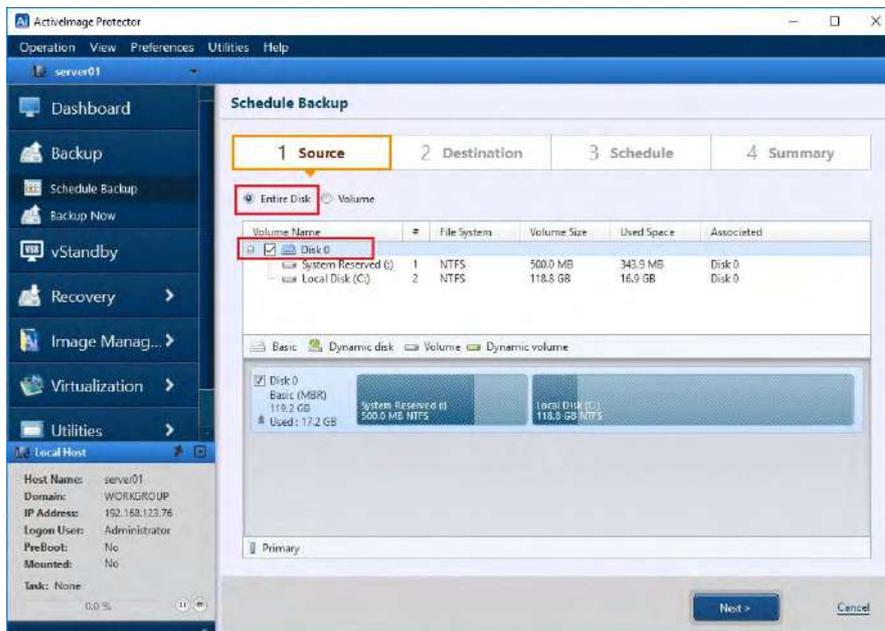


Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



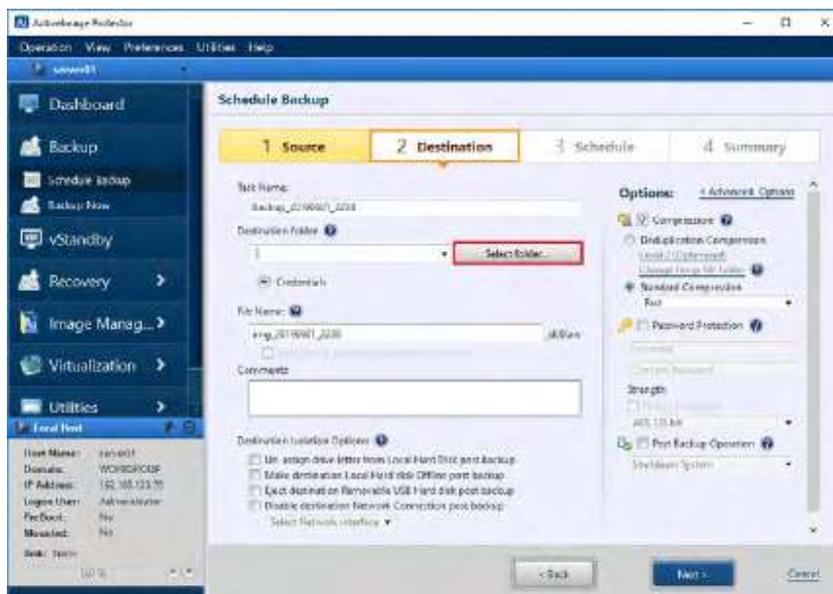
3. Select backup source.

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

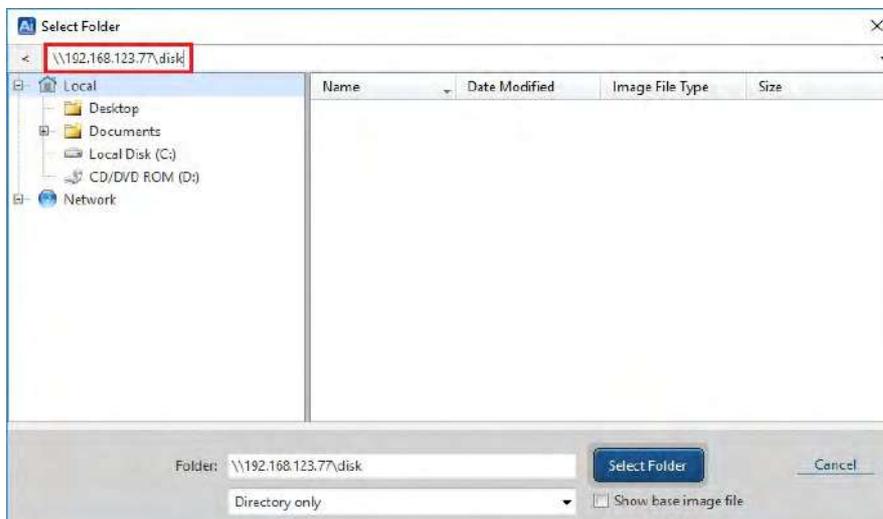


4. Select a target destination for the backup image.

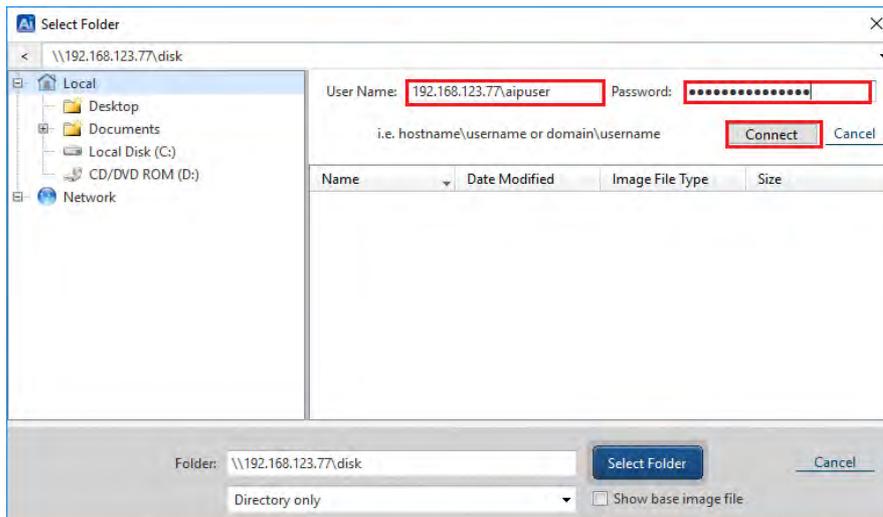
The following example shows that “[\\192.168.123.77\disk](#)” in the network shared folder is specified for the target destination. Click **[Select Folder]**.



5. Please specify the path for the location of the target destination.
Please enter the following path “ \\192.168.123.77\disk “ for the target destination and press Enter key.

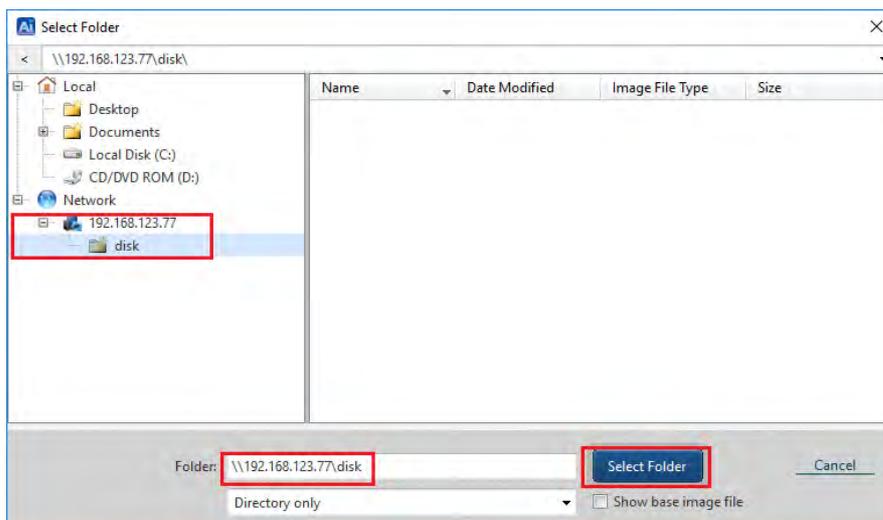


6. Please enter the credentials to access the target destination.
User Name must be specified in “Host Name \ User Name” format.
The following example shows that the host name “192.168.123.77” and user name “aipuser” are entered. The credentials are predefined to access the destination folder.
Enter “192.168.123.77\aipuser” for **[User Name]** and the password for **[Password]**. Click **[Connect]**.



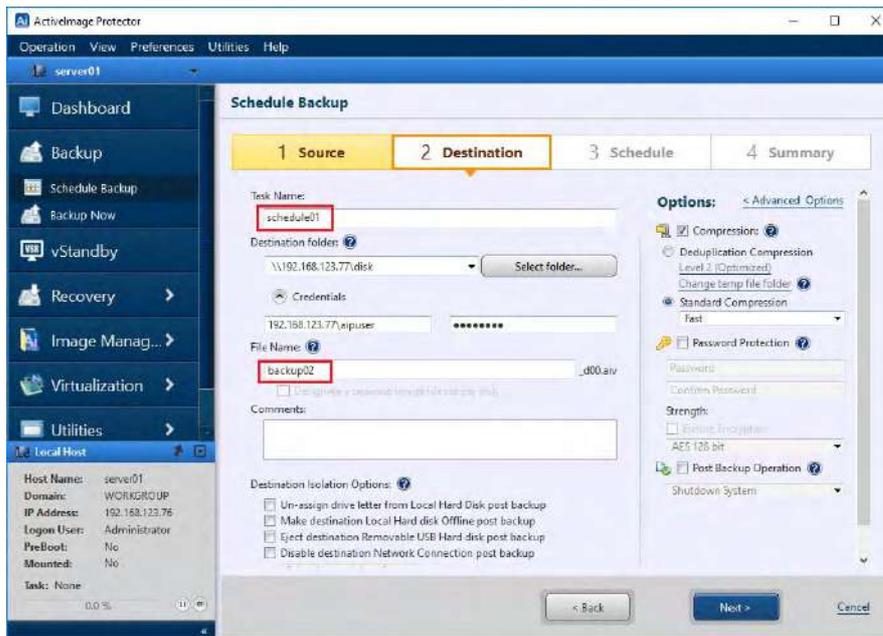
If you specify the same target destination that you selected before, since the credentials are saved, the windows for the above step 5 and 6 are skipped.

7. Ensure the target destination is correctly specified and click **[Select Folder]**.

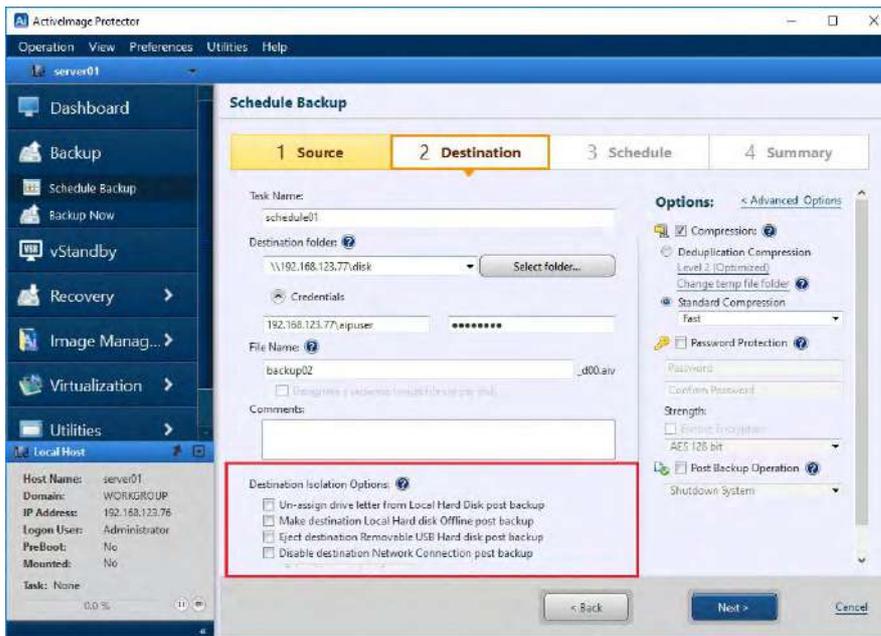


8. Specify the backup image file name.

The following example shows that “schedule 01” is specified for the task name, “backup02” for the image file name (the file extension is automatically entered.) Enter “schedule 01” for **[Task Name]**, “backup02” for **[File Name]**.



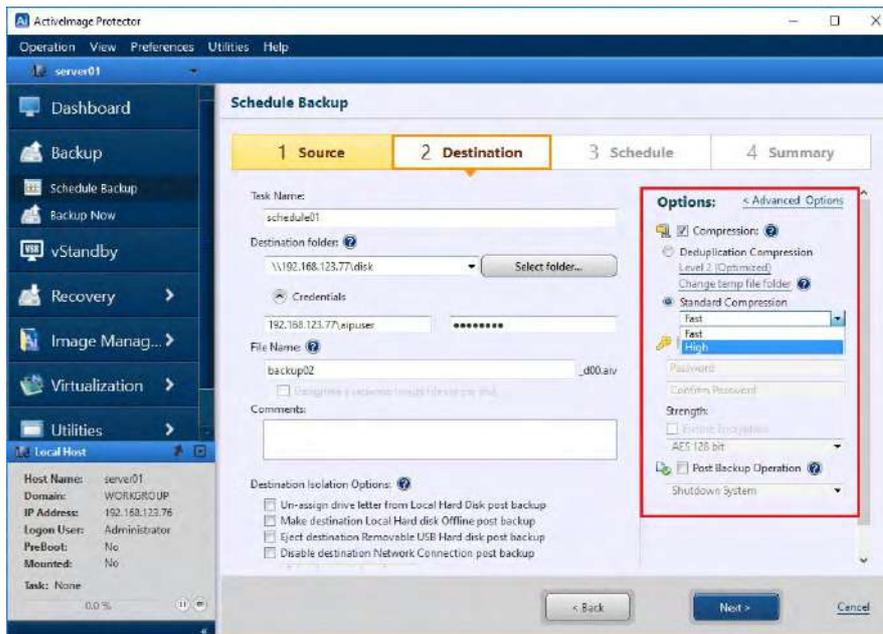
9. Next, configure the setting for **[Destination Isolation Options]**. Destination Isolation feature, available only in ActiveImage Protector Update, disconnects network access to backup image storage drives or setting the destination disk to offline upon completion of backup process. Imagelsolate™ technology protects the backup storage and backup files from potential malware or ransomware attacks. **[Destination Isolation]** provides four options. Enabling **[Un-assign drive letter from Local Hard Disk post backup]**, the drive letter assigned to the local hard disk is de-assigned upon completion of backup process. Selection of **[Make destination Local Hard disk offline post backup]** sets the destination disk to offline upon completion of backup process (same behavior as **[Disk Management]** in Disk Management Tool). When **[Eject destination Removable USB Hard disk post backup]** is enabled, a removable hard disk such as USB hard disk become removable upon completion of backup process. If **[Disable destination Network Connection post backup]** is enabled, network connection to backup destination is disconnected upon completion of backup process. You can select the network interface to block in the selection box at the bottom.



10. Configure Compression settings. ActiveImage Protector provides two compression types.

One is Standard Compression that offers the common file / folder compression tool same as ZIP. The other is Deduplication Compression designed to create index for every block of backup stream and delete duplicated blocks when identified while creating a backup image file. Deduplication Compression feature efficiently and dramatically reduces backup storage space requirements on a server hosting multiple virtual machines.

Check the checkbox for **[Compression]** in **[Option]** pane. When **[Deduplication Compression]** option is selected, **[Level 2 (Optimized)]** and **[Change temp folder]** are enables.



The compression level goes up according to the compression ratio.

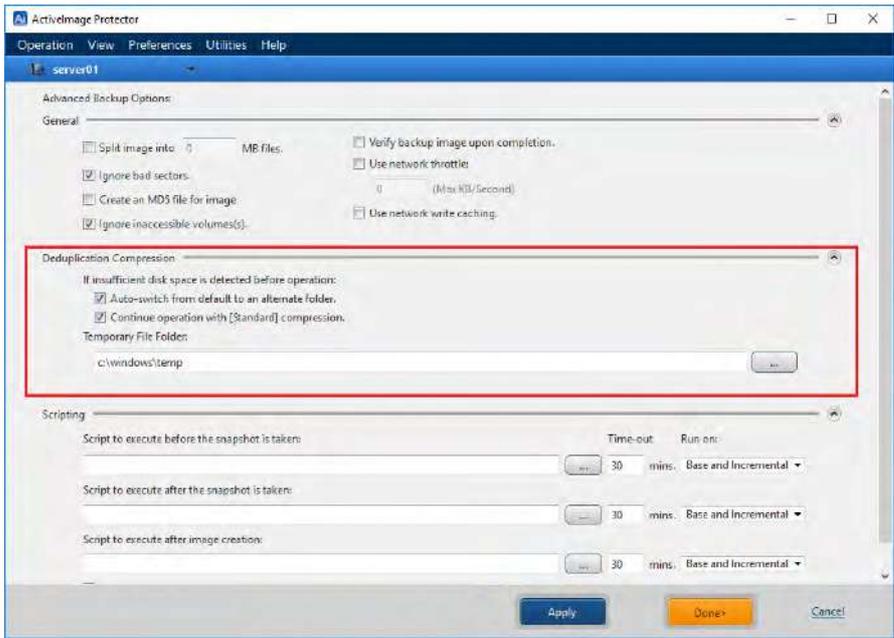
When a backup task runs in boot environment, the temporary work folder is located on memory by default, therefore, please be aware that the available space in the temporary work folder may be insufficient. If the backup source includes large data volume, please change the temporary work folder to other location such as the target destination.

Click **[Advanced Option]** to configure the advanced option settings.

In **[General]**, please select **[Split image into xx MB files]** to split and save the created backup files.

In **[VSS Setting]**, You can edit the VSS setting for a backup task if you need to forcefully run VSS in component mode or exclude specific files from backup source.

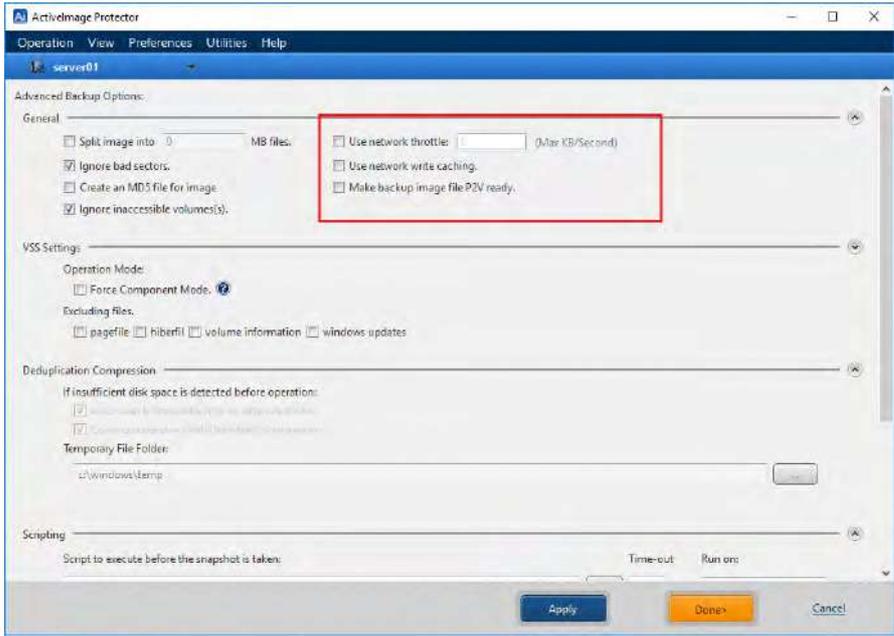
In **[Deduplication Compression]**, you can select an option ensuring that the backup task completes without interruption if insufficient disk space is detected in the temporary file folder before operation. You can also specify the location for deduplication to process temporary files. Since the execution of a backup task in boot environment processes the temporary files in memory space, by default, it may cause insufficient available memory. If the backup source is large in data size, please change the location of temporary file folder.



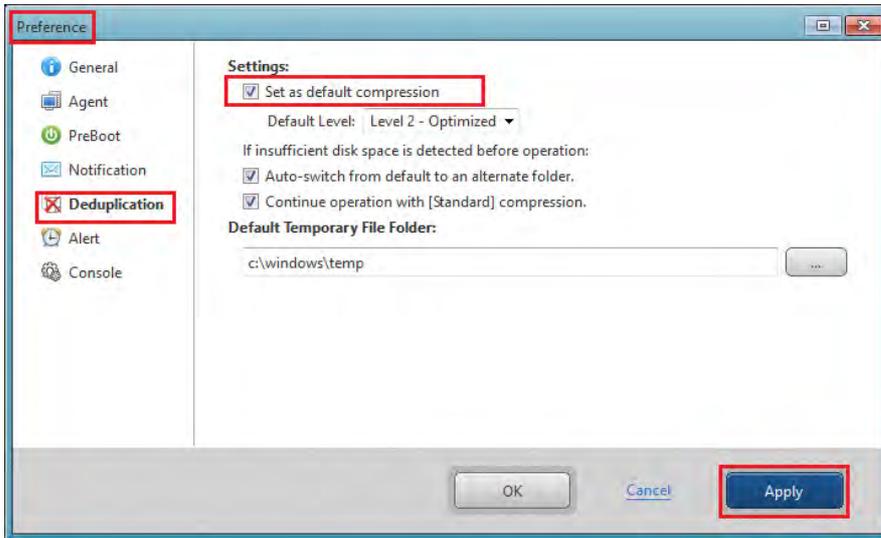
Backing up multiple number of virtual machines at a time increases backup traffic over the network. Network throttle defines the maximum throughput over the network and the use of cached data shortens data access time.

Enable **[Use network throttle]** option to define the maximum throughput in KB/second to reduce traffic over the network while saving backup image files to network shared folder.

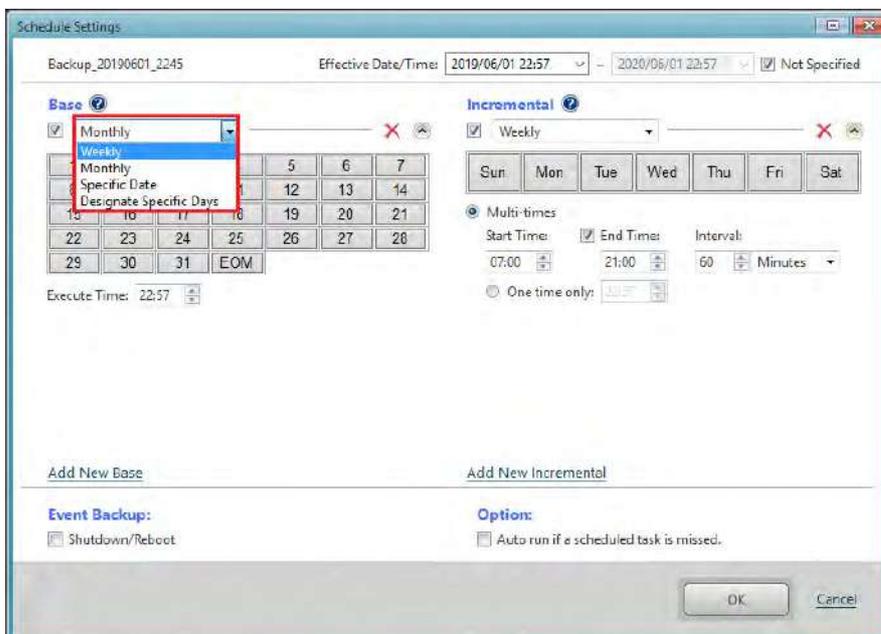
Enable **[Use network write caching]** option to use cached data and shorten data access time in saving backup image files to the destination over network.



11. To enable Deduplication Compression feature by default, go to [Preference] – [Deduplication] and check the checkbox for **[Set as default compression]** and select **[Deduplication Compression]** for **[Default Level]**. Click **[Apply]**.

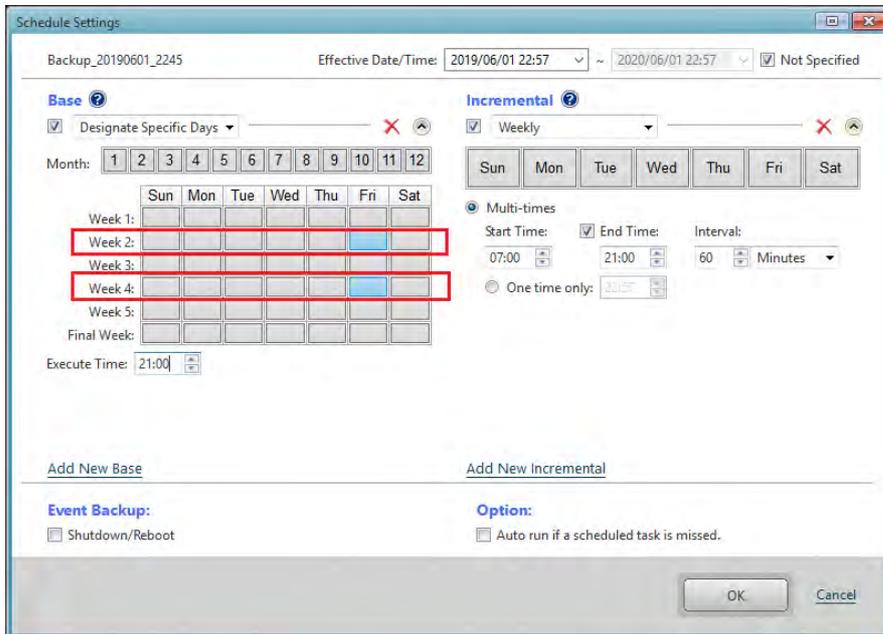


12. Schedule type can be selected to configure the backup schedule. Begin by specifying **[Effective Date/Time]** that the scheduled task becomes live. The [Effective Date/Time] defaults 10 minutes from the time of beginning the configuration in the wizard. **[Not Specified]** option may be selected so that the scheduled task is live for unlimited period. Options include **[Weekly]**, **[Monthly]**, **[Specific Date]**, **[Designate Specific Days]** for full base backup.



[Designate Specific Days] is a new schedule type ActiveImage Protector 2018 Update provides. For example, you can specify “Every second Friday from

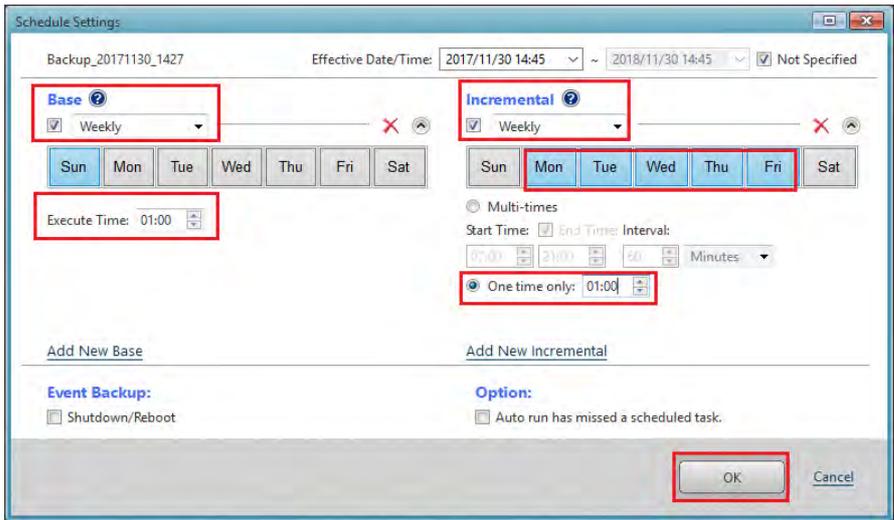
January to December” for the schedule setting. In case you have a routine of business operations such as financial closing or inventory management which requires to make significant changes on a specific day of a specific week every month, you will find this schedule type very convenient.



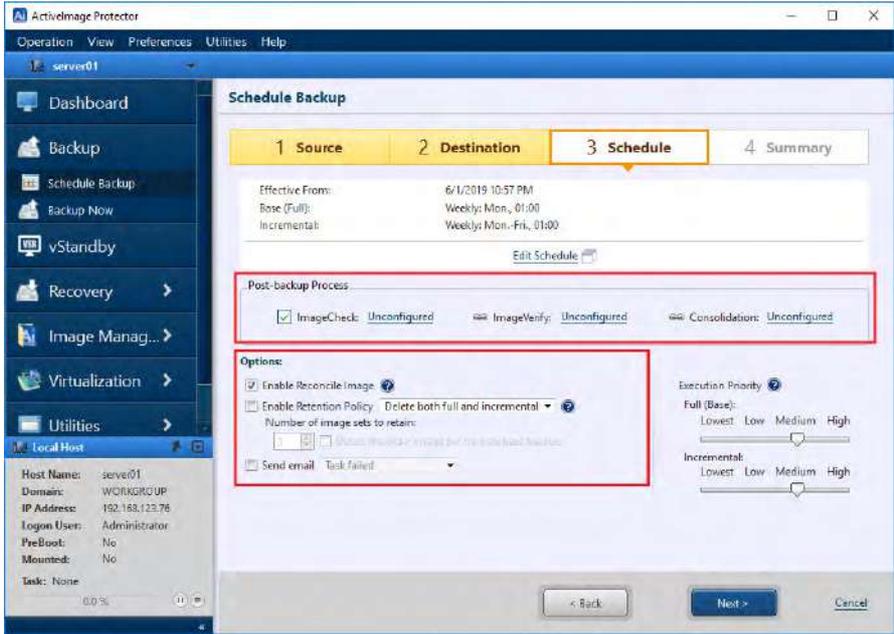
The following example shows the weekly backup schedule settings.

- Base backup: Weekly
- Incremental backup: Weekly
- Base backup: Every Sunday at 1:00 AM
- Incremental backup: From Monday to Friday at 1:00 AM

After configuring the settings, click **[OK]**.

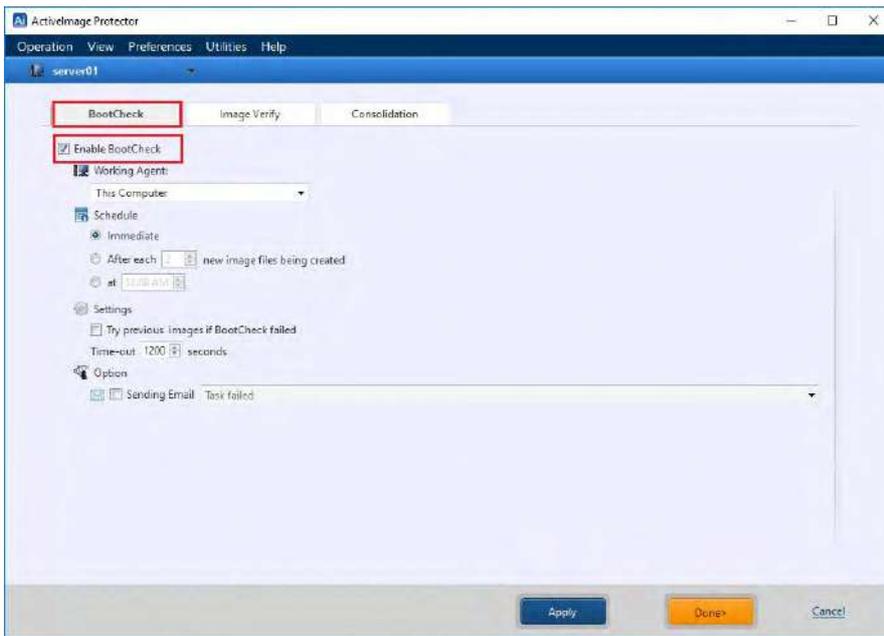


13. Configure the option settings including Retention Policy, BootCheck and Consolidation for post backup processing. Check the checkbox for **[Enable Retention Policy]** option and enter “3” for [Number of image sets to retain:] (3 sets of incremental backup files are retained in the target destination before deletion).

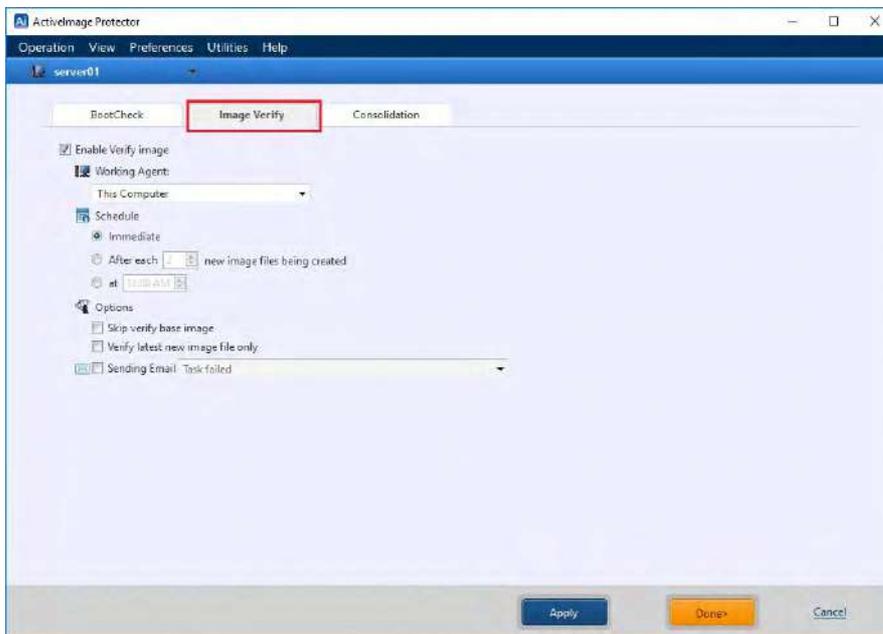


You can select an option for Post-backup Process, i.e., **[BootCheck]**, **[Image Verify]**, **[Consolidation]**. **[BootCheck]** tests that backup images can successfully boot by using virtual machine on the specified host. Click **[Unconfigured]** to display the setting window.

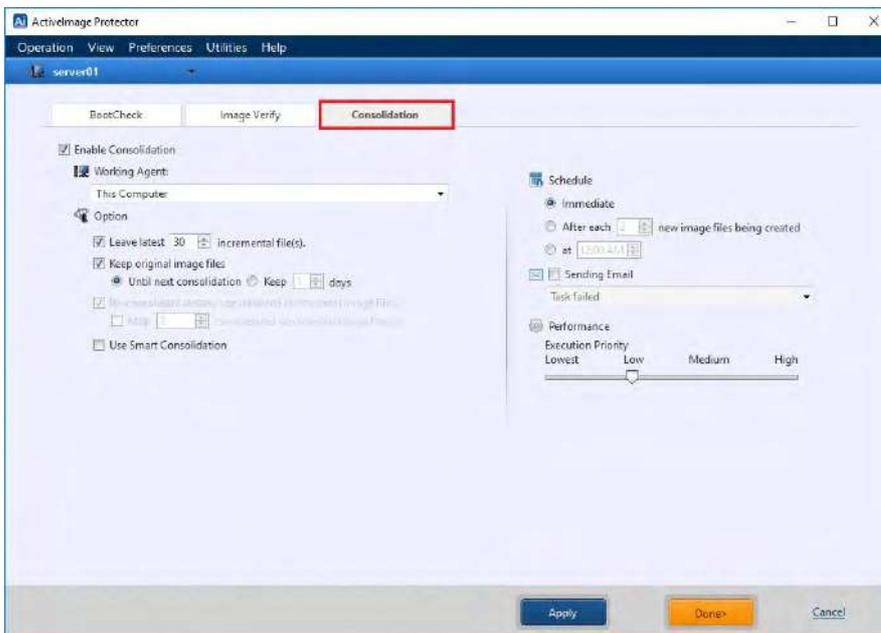
14. In **[BootCheck]** tab, check the checkbox for **[Enable BootCheck]**.



15. Click **[Image Verify]** tab. Check in the check box for **[Enable Verify Image]** to verify the integrity of a created backup image. Please configure the setting for **[Schedule]**.



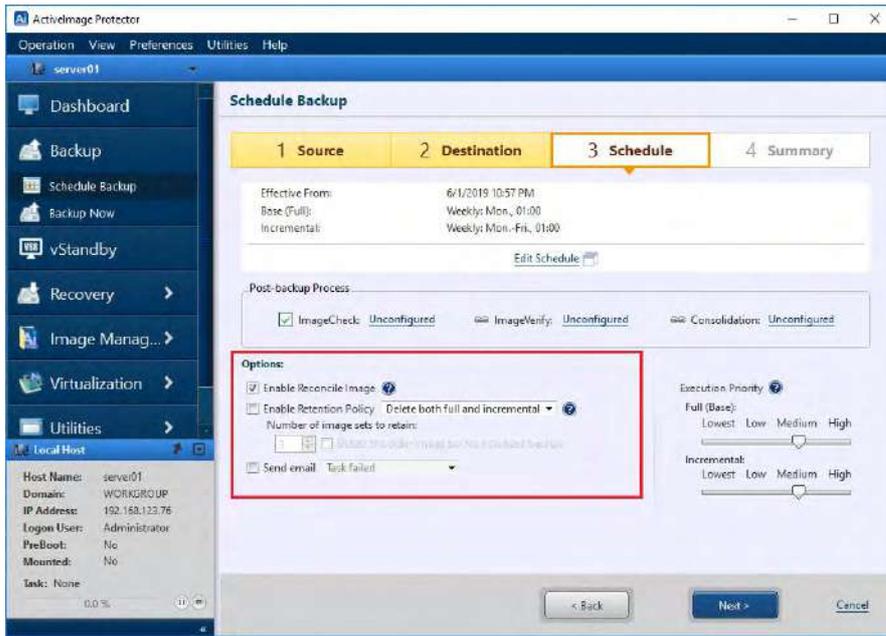
16. Click **[Consolidation]** tab. Check the checkbox for **[Enable Consolidation]**. Incremental backup saves processing time, however, recurring scheduled backup tasks creates a growing and sometimes unmanageable number of incremental files. Consolidation consolidates an uninterrupted series of backup image files in the same generation set to facilitate file management. The following example shows that 15 consolidated files are retained while the latest 30 incremental files are saved. Consolidation task runs whenever a new incremental backup file is created. Click **[Done]** to go back to **[Schedule]** window.



17. In **[Option]** section, the following options are provided.

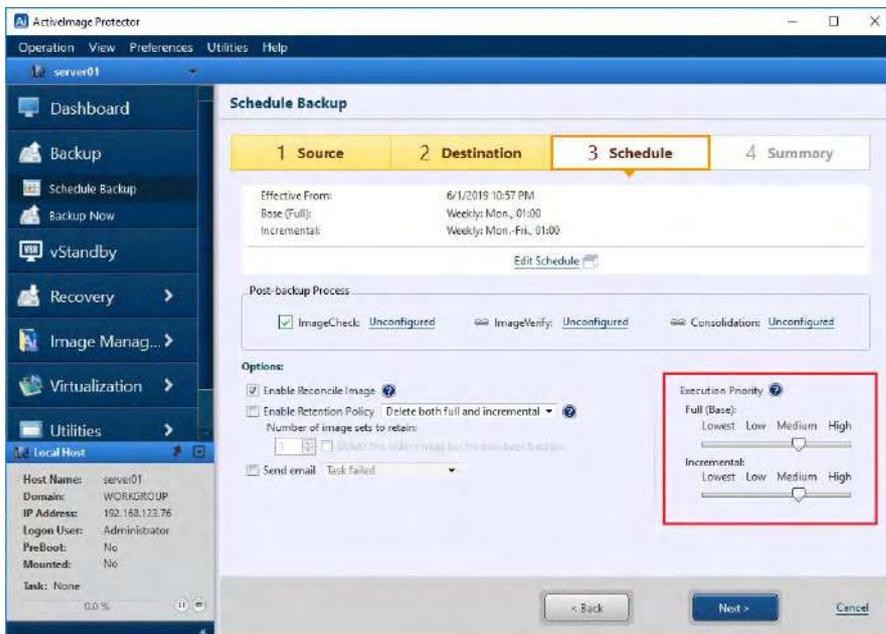
- Enable Retention Policy
- Send email

Retention Policy defines how many sets of backup files to retain before deletion. Enabling Retention Policy, you can configure the setting for the number of image sets to retain as well as which backup image files to delete. Enable **[Send email]** option to send E-Mail informing you of a task completed with a specified status.



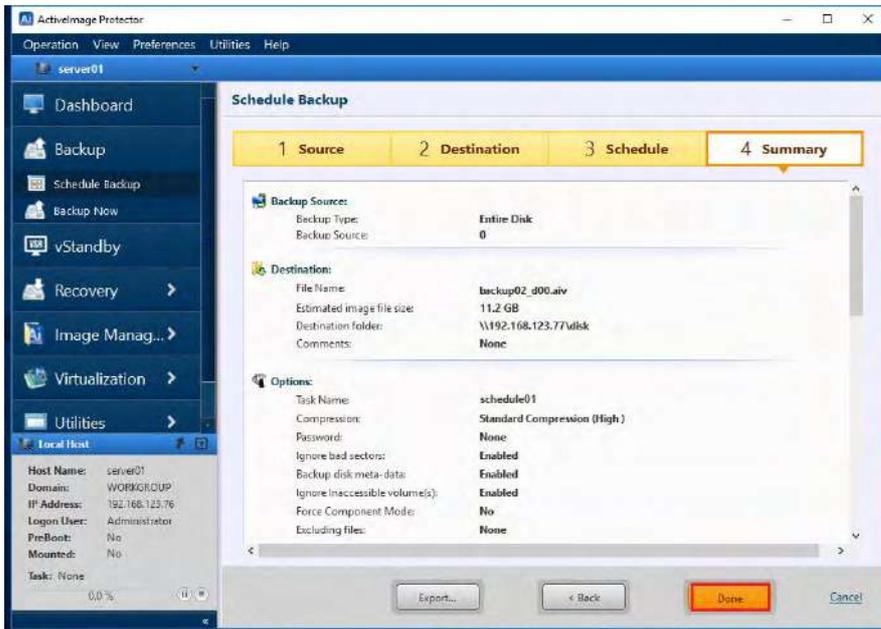
Backing up multiple number of virtual machines at a time increases backup traffic over the network. Network throttle defines the maximum throughput over the network and the use of cached data shortens data access time.

You can also select a level of task Execution Priority for CPU usage.

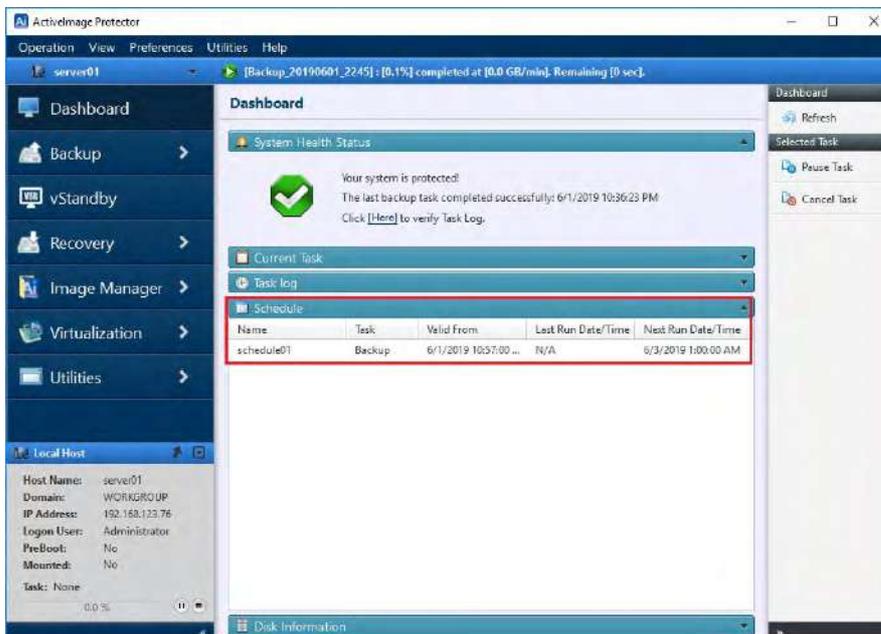


When the option settings are configured, click **[Next]**.

18. In **[Summary]** window, review the backup configuration and options.
Click **[Done]** to complete backup setting.



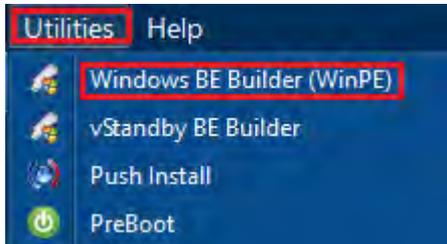
19. Go to **[Dashboard]** – **[Schedule]** to monitor the created schedule. The scheduled backup task runs according to the schedule you specified.



5. Boot Environment Builder

Build Windows-PE based Boot Environment

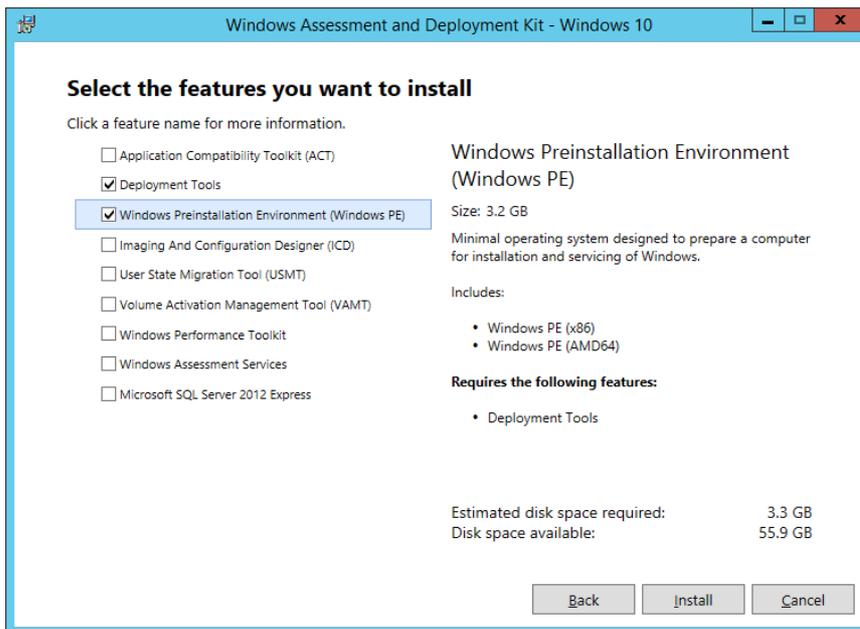
1. Start by selecting **[BE Builder (Windows PE)]** from the **[Utilities]** menu bar.



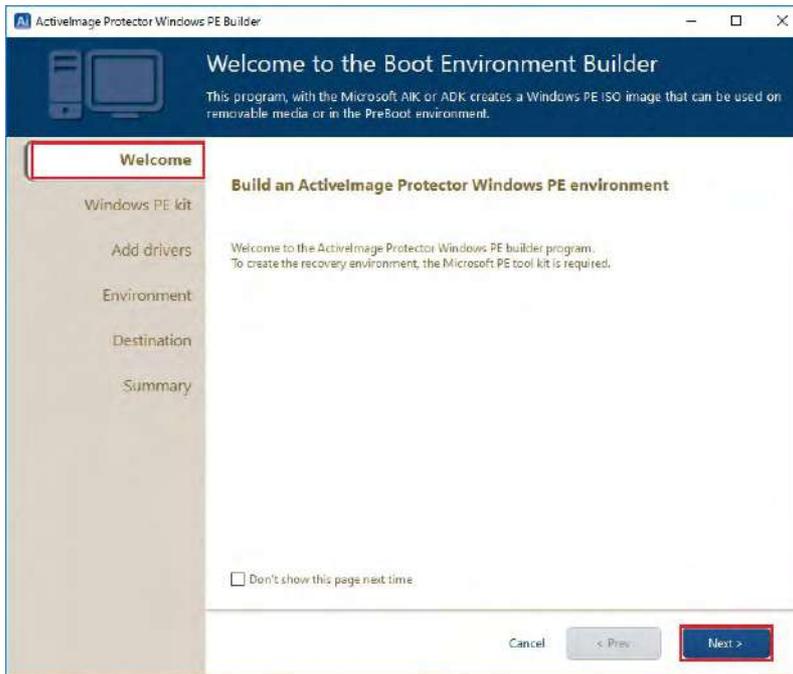
2. Microsoft Windows ADK or AIK is required to be installed on the host to build the Windows PE based boot environments.

As for Windows ADK, please select the following components to install:

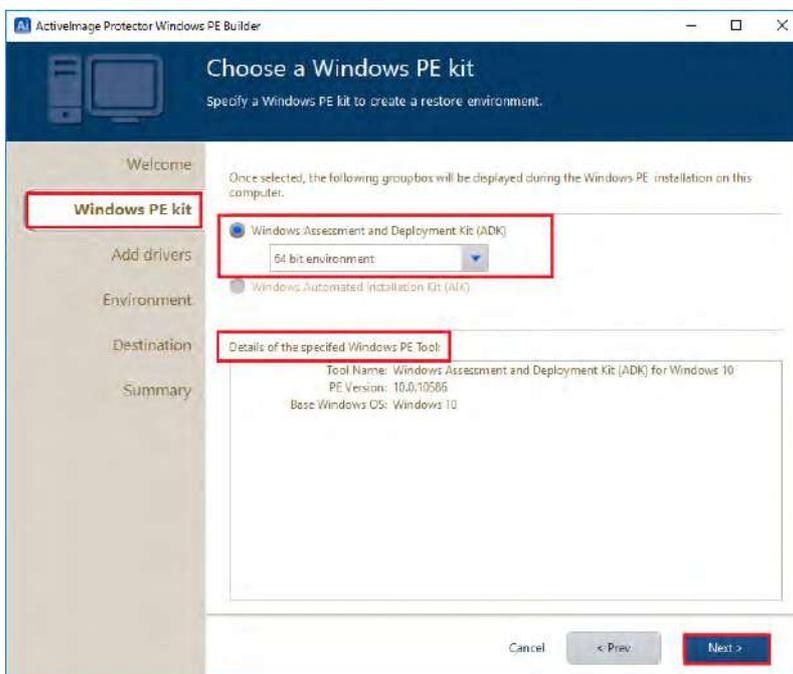
- Deployment Tools
- Windows Preinstallation Environment (Windows PE)



3. **[Welcome to Boot Environment Builder]** window comes up, then click on **[Next]**.



4. Specify the Windows PE toolkit needed for the installed operating system by clicking the appropriate radio button. The 32-bit version of Windows PE boot environment can be built on 64-bit host. The information of a specific Windows PE toolkit can be displayed. Click **[Next]**.

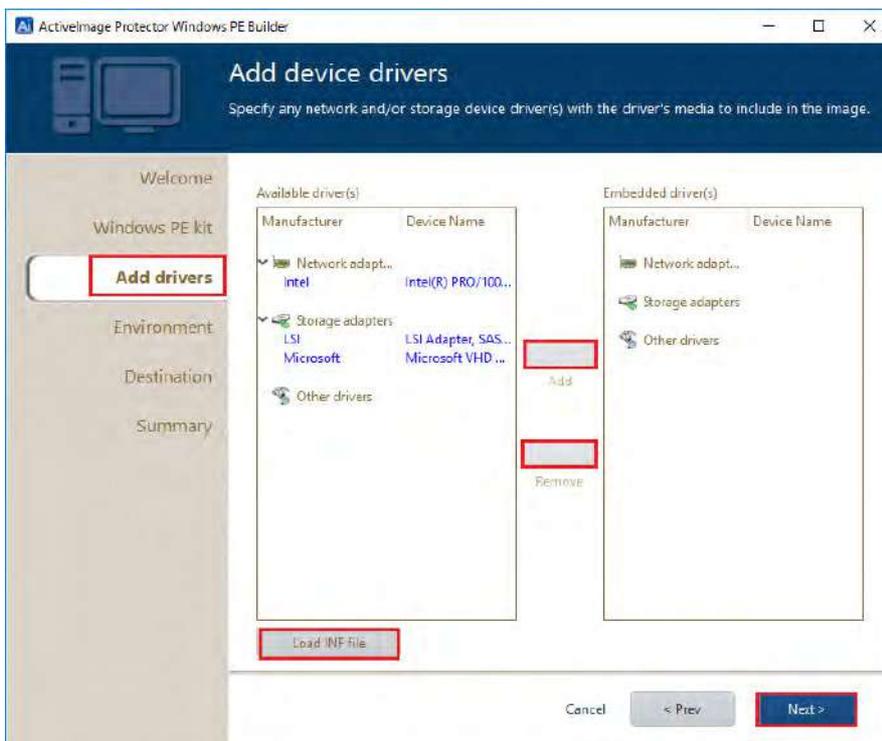


5. Specify device driver(s) to include in the boot environment.

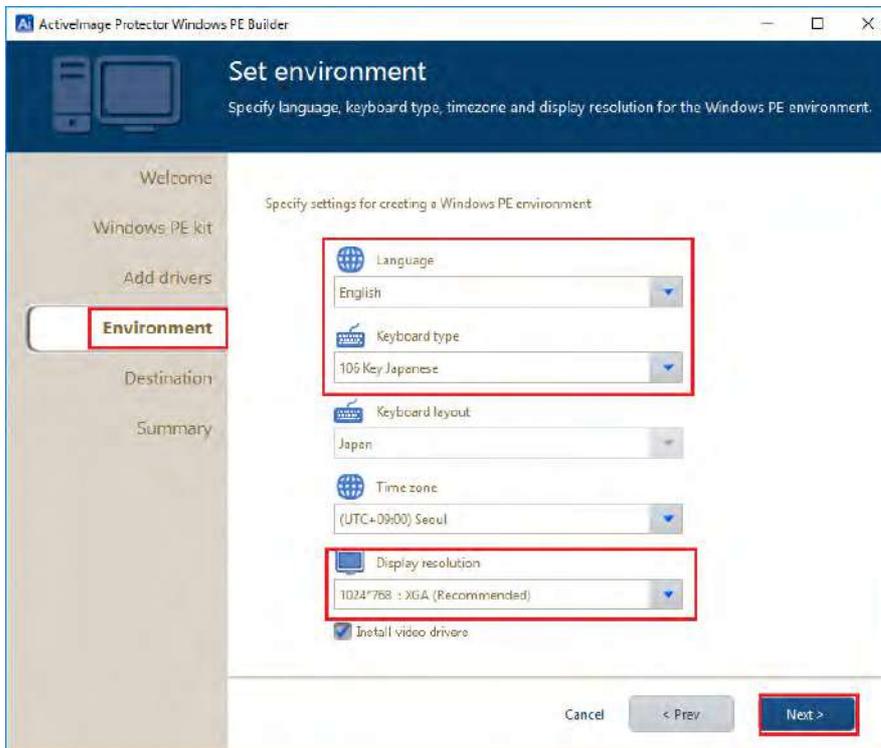
Network and storage device drivers included in the current system are detected and listed on the left pane. Click **[Load INF file]** to add a driver by selecting INF file if the driver is not listed.

After selecting a driver to add, click on **[==>]** to include the driver in **[Embedded driver(s)]**. To exclude a driver from **[Embedded driver(s)]**, select the driver and click on **[<==]**. Click **[Next]**.

* Only LAN (Ethernet) driver is supported as network driver.



6. Specify the Language, Keyboard type, Time zone and/or Display resolution for the Windows PE boot environment by selecting the preferred option from the drop-down menu. Click **[Next]**.



7. Select the bootable media to build the boot environment.

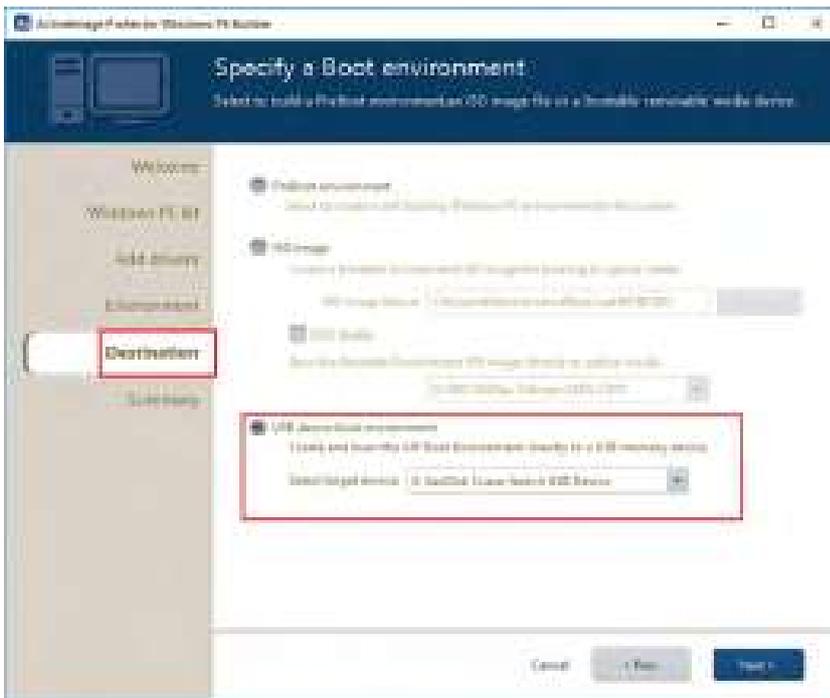
PreBoot environment - Creates the boot environment in the system volume to boot from the hard disk.

ISO Images - Creates an ISO image file in the specified location. The created ISO file may be burned to DVD media at a later time.

* [DVD media] option is not provided for Windows XP/2003. After creating ISO image, please use a third-party writing software to burn the ISO image to DVD media.

USB device boot environment - Creates boot environment on a USB memory device. The USB media currently connected to the PC may be selected. All data on the selected USB media device will be erased. * [USB device boot environment] option is not provided for Windows XP/2003.

Click **[Next]**.



8. Please review the configured settings. Click [**< Prev**] to make changes to previous settings. Click on a node to go back to a specific page. Click on [**Build Windows PE environment**] to display the confirmation message. Click on [**OK**] to start building Windows PE environment. You can monitor the progress in the following window.



9. When boot environment creation completes, the following message is displayed. Click on **[OK]** to close the window.



6. Restore

6-1. File Recovery

A specific file or folder can be restored from a backup image file to a specified location. Please take the following procedures.

1. Start ActivelImage Protector.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActivelImage Protector]**.

Windows 7 or earlier Desktop OS:

Click [Start] – [All Programs] – [NetJapan] – [ActivelImage Protector].

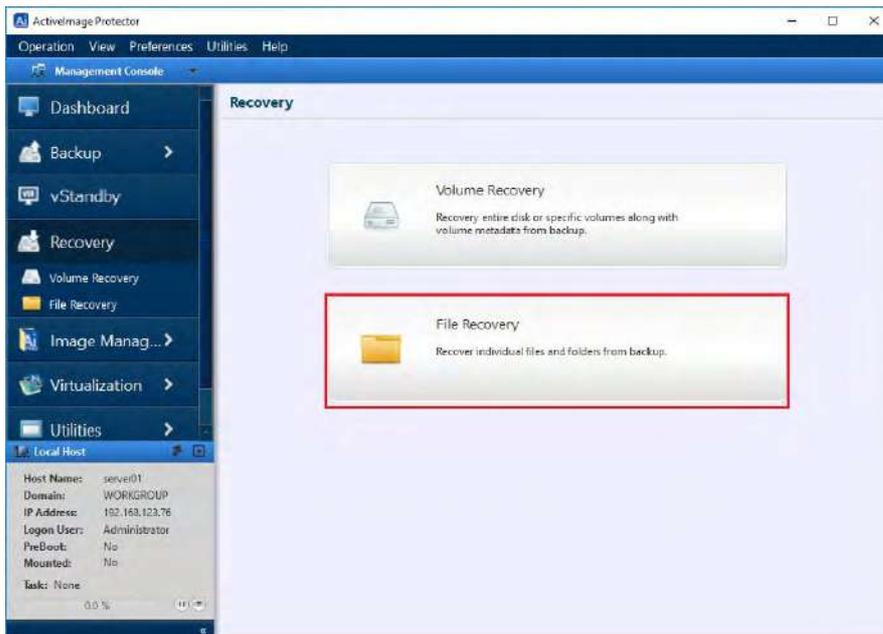
Windows Server 2012 or later server OS:

Click [Start] – [Applications] – [NetJapan] – [ActivelImage Protector].

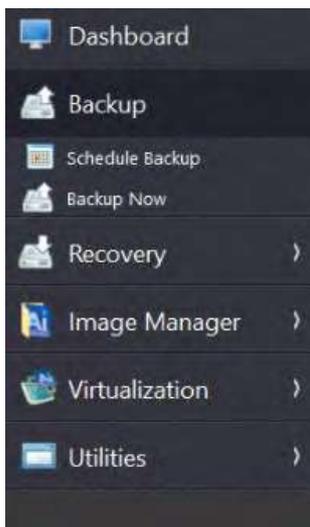
Windows Server 8 or later Desktop OS :

Click [Start] – [Applications] – [NetJapan] – [ActivelImage Protector].

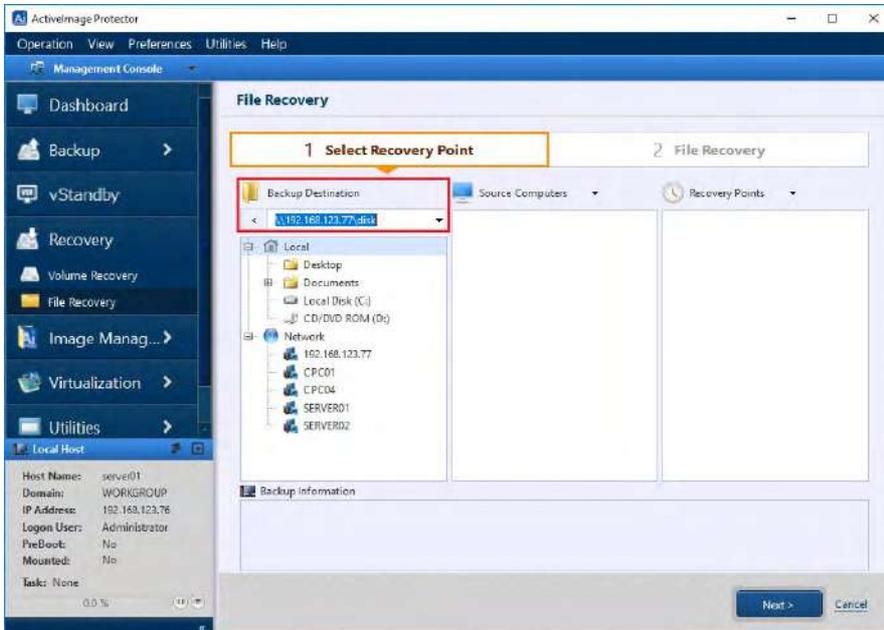
2. Select [Recovery] – [File Recovery].



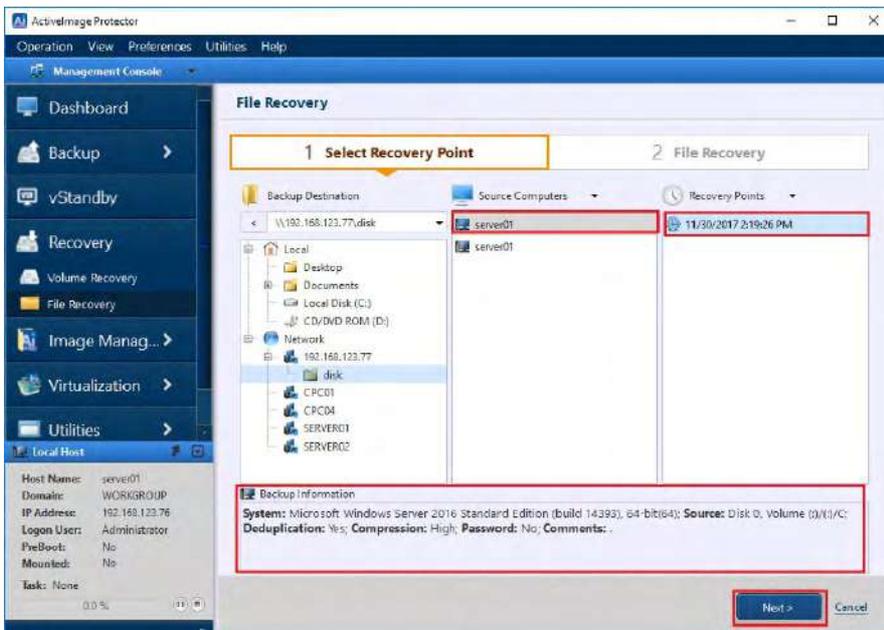
Note) The left pane of ActiImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



3. Select the backup image file in **[Backup Destination]**. You can specify the path for the destination. This example shows that “ \\192.168.123.77\disk “ is specified for the destination. Press Enter key.



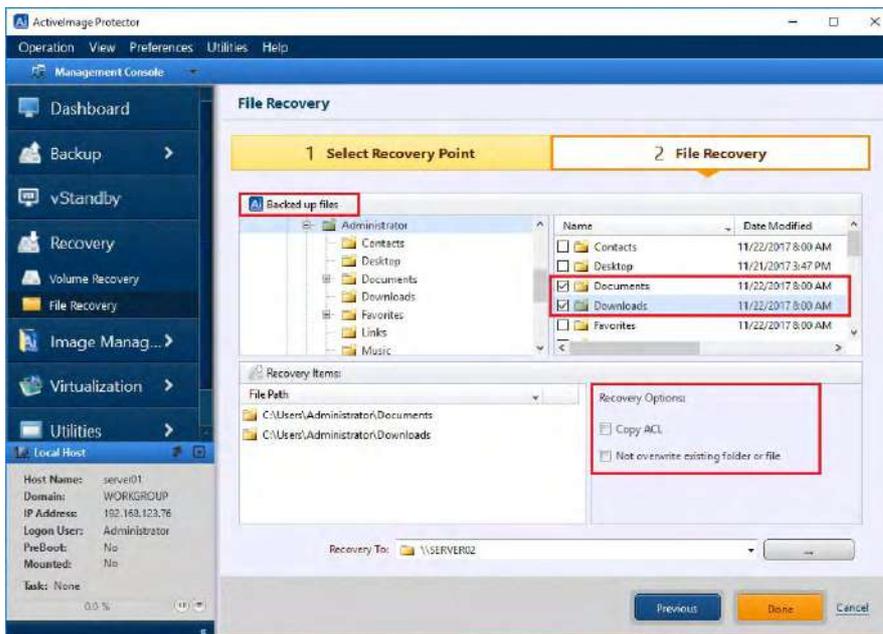
4. Select the backup source host from the list and recovery point. Click **[Next]**. The information of the selected recovery point (image) is displayed in **[Backup Information]**.



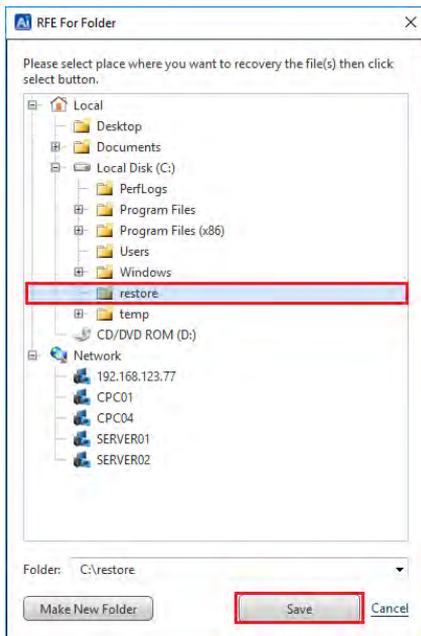
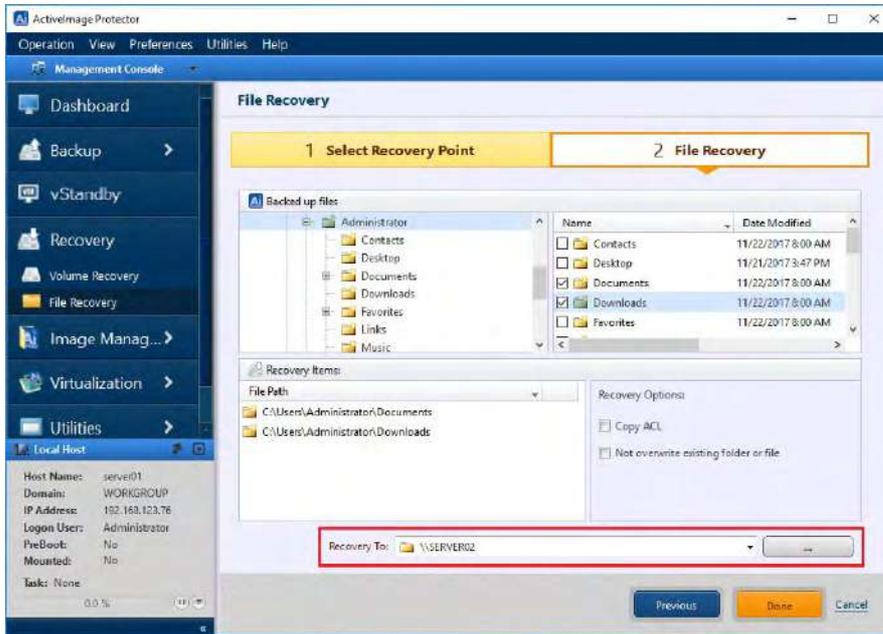
5. Check the checkbox for the items in **[Backed up files]** to restore. The selected items are listed in **[Recovery Items]**.

The following **Recovery Options** may be configured.

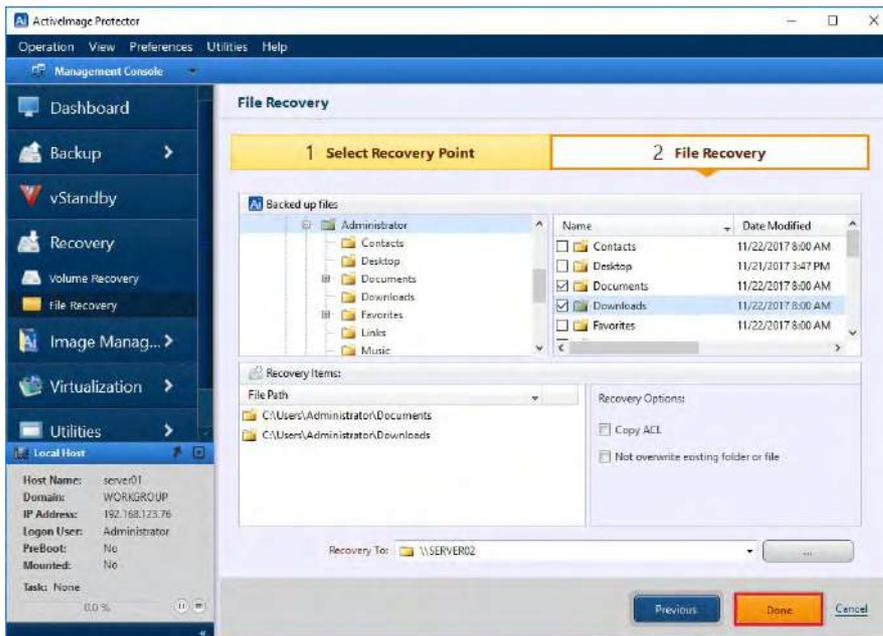
- **Copy ACL** - The selected file is restored keeping Access Control List (ACL) configured for restore source file.
- **Not overwrite existing folder or file** – If there already exists a file / folder in the destination, the file / folder is restored under a unique name instead of overwriting the existing file.



6. Click [...] (Browse) to select the destination to save the restored item. Click **[Save]**.



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



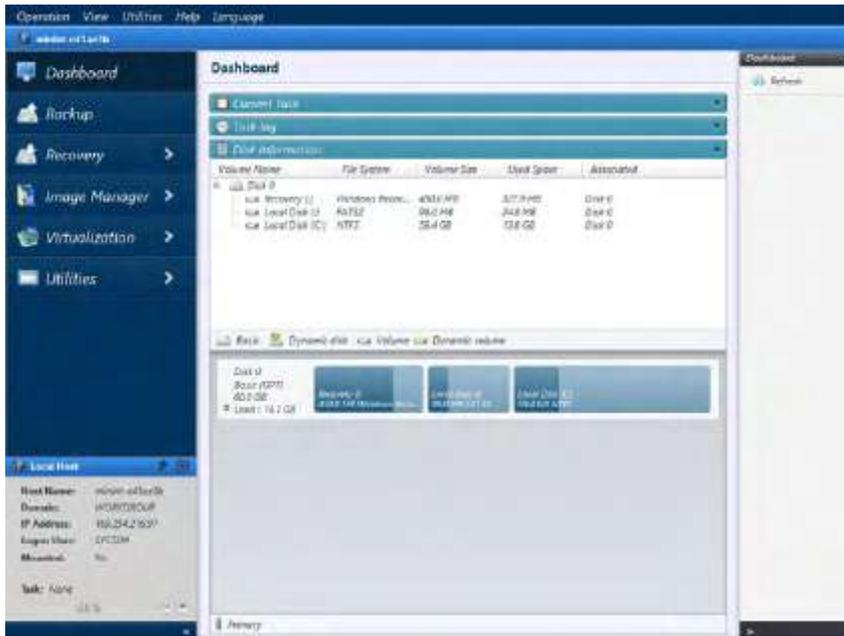
6-2. System Recovery

The following are the operating procedures for system recovery by using boot environment in USB device or optical media built with AOMEI Backupper BE Builder.

Note: Please be aware that, as a result of system recovery, the data stored in local folder are entirely purged.

1. Set the boot media to your machine and boot into the boot environment from the boot media. Please wait until boot environment completely boots up.

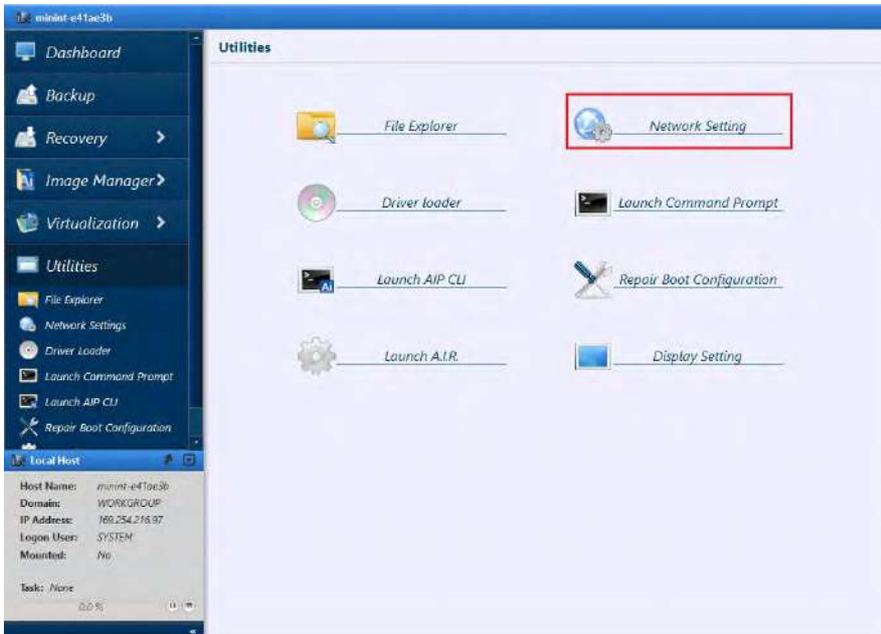




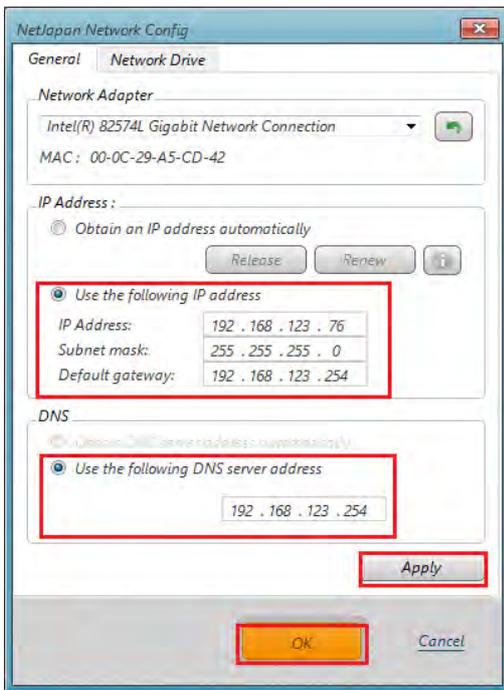
Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition.



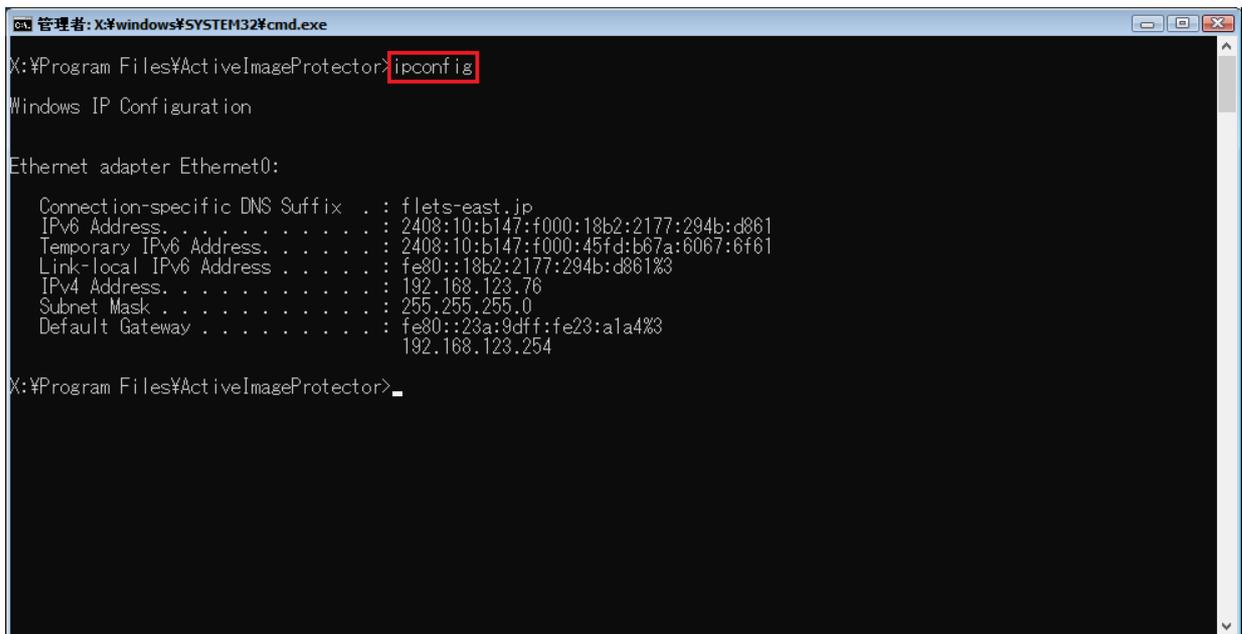
2. Please configure the network settings in order to access the network shared folder specified for the target destination.
Select **[Utilities] – [Network Setting]**.



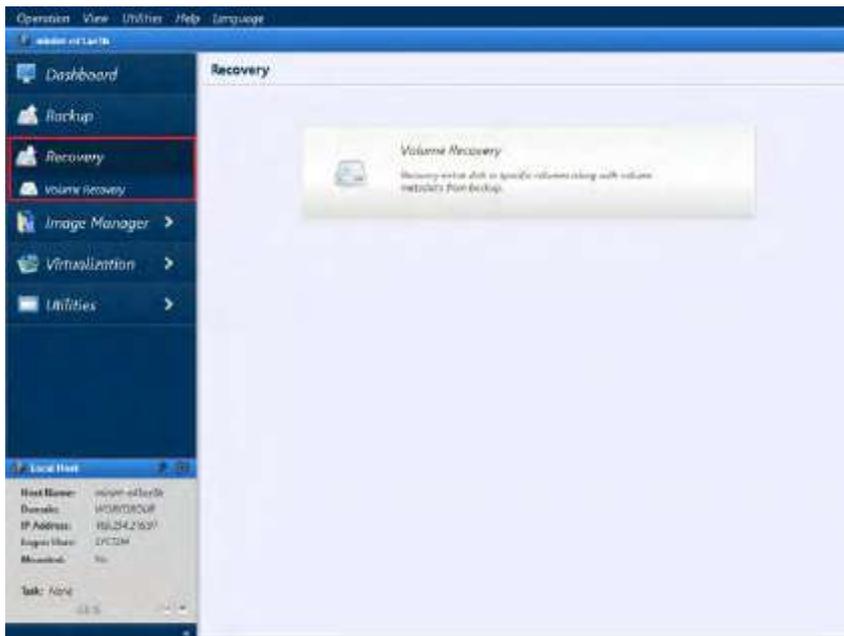
3. **[NetJapan Network Config]** windows is displayed. This example shows that **[Use the Following IP address]** is selected. Please configure the settings according to your network environment. Specify “192.168.123.76” for **[IP Address:]**, “255.255.255.0” for **[Subnet mask]**, “192.168.123.254” for **[Default gateway]**, Select **[Use the following DNS server address]** and enter “192.168.123.254”. Click **[Apply]** and **[OK]** to complete the settings.



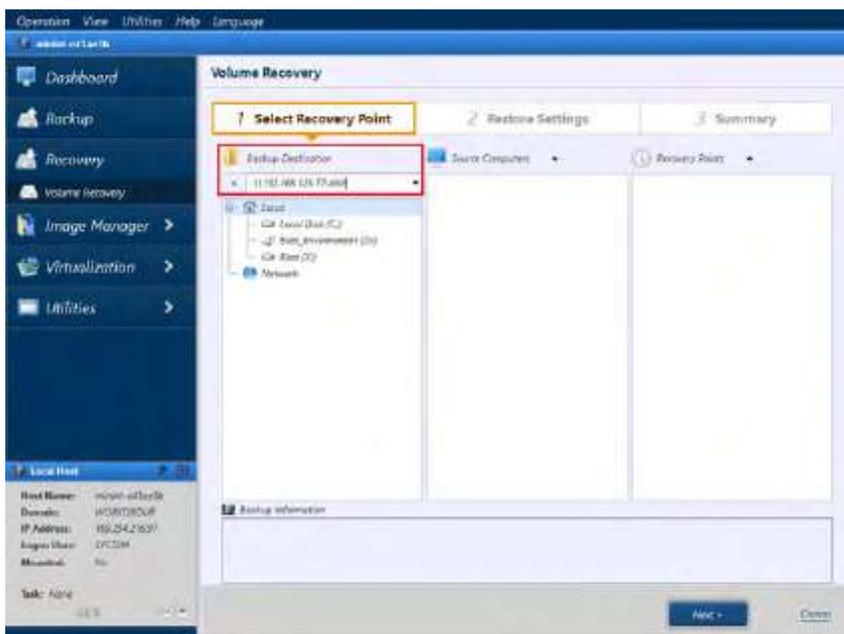
4. Go to **[Option] – [Launch Command Prompt]** and ensure that the settings such as IP Address are correctly configured. Enter “ipconfig” command and press Enter key. Make sure that the IP address is correctly specified.



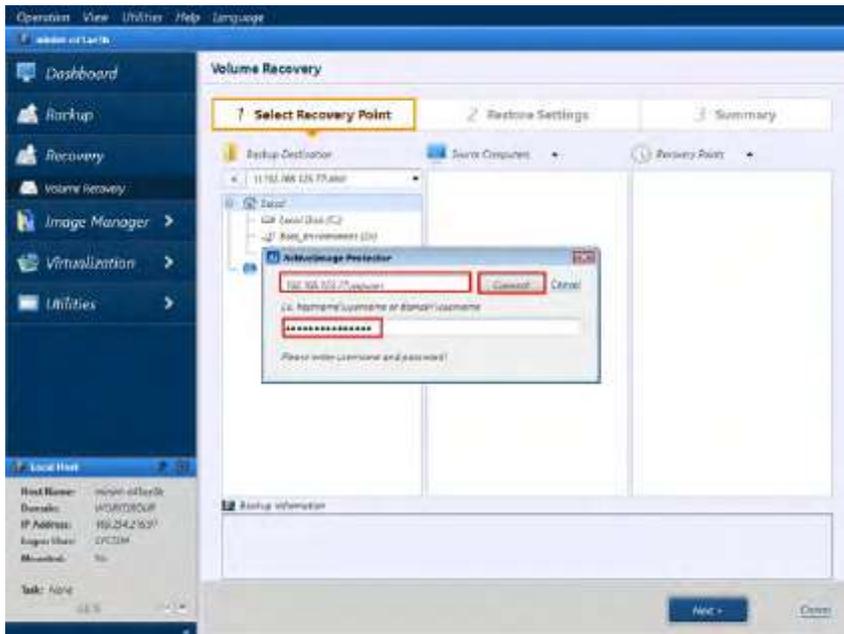
5. Select [Recovery] – [Volume Recovery].



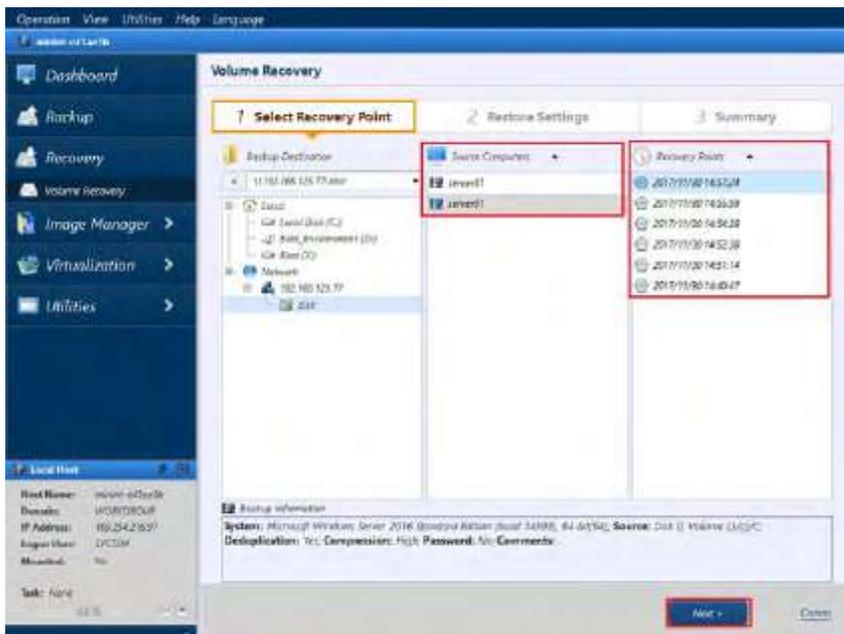
6. Enter “\\192.168.123.77\disk” for [Backup Destination] and press Enter key.



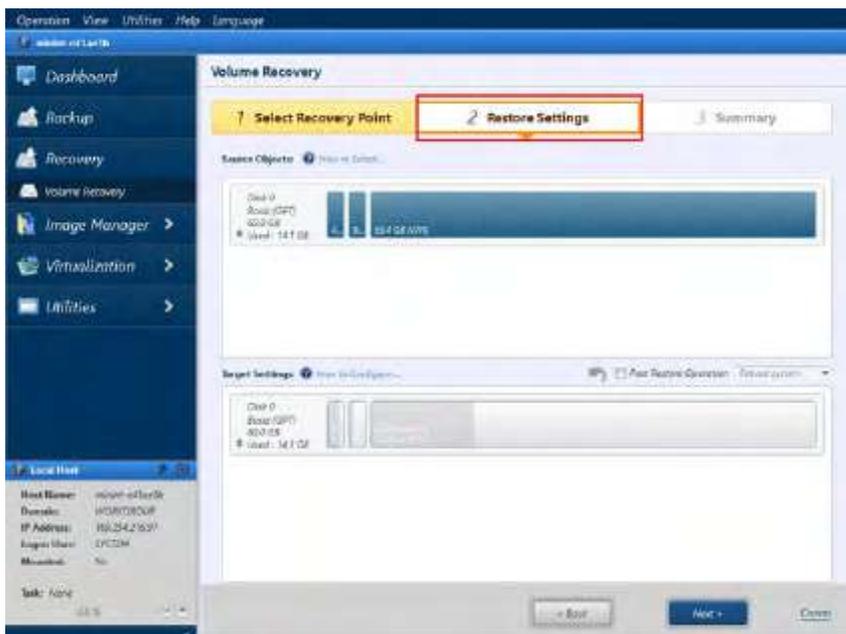
7. For user authentication, please enter “192.168.123.77\aipuser” for user name and predefined password. Click **[Connect]**.



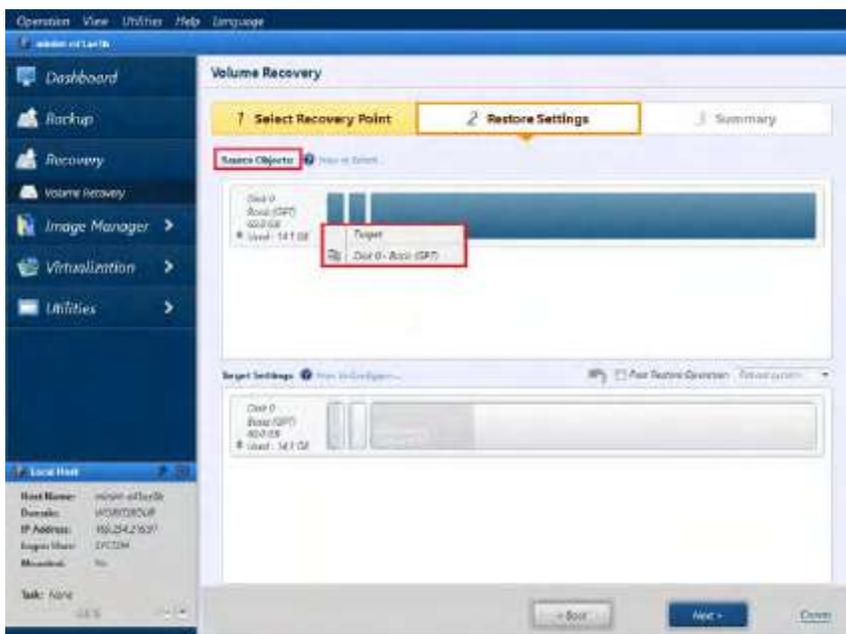
8. Select Source Computer and Recovery Point. Click **[Next]**.



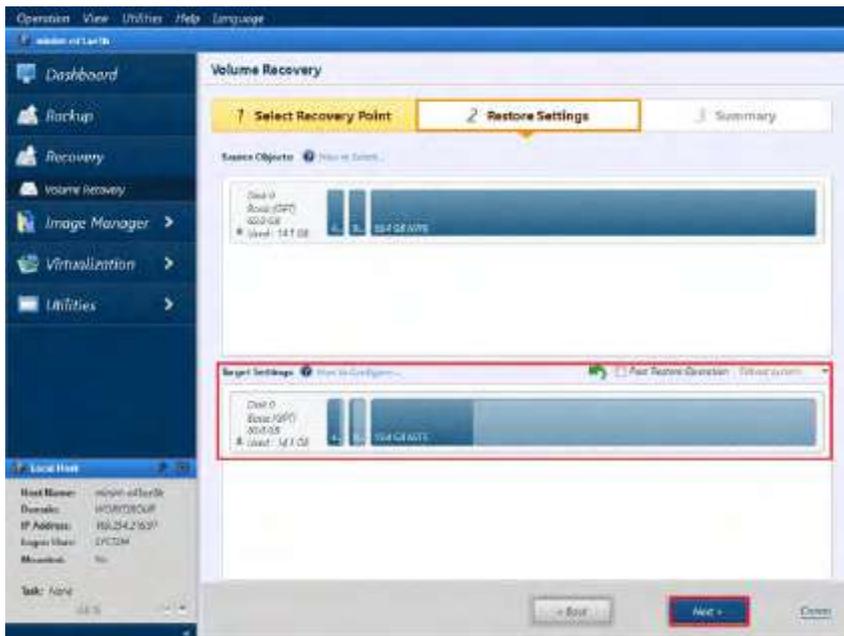
9. [Restore Settings] window is displayed.



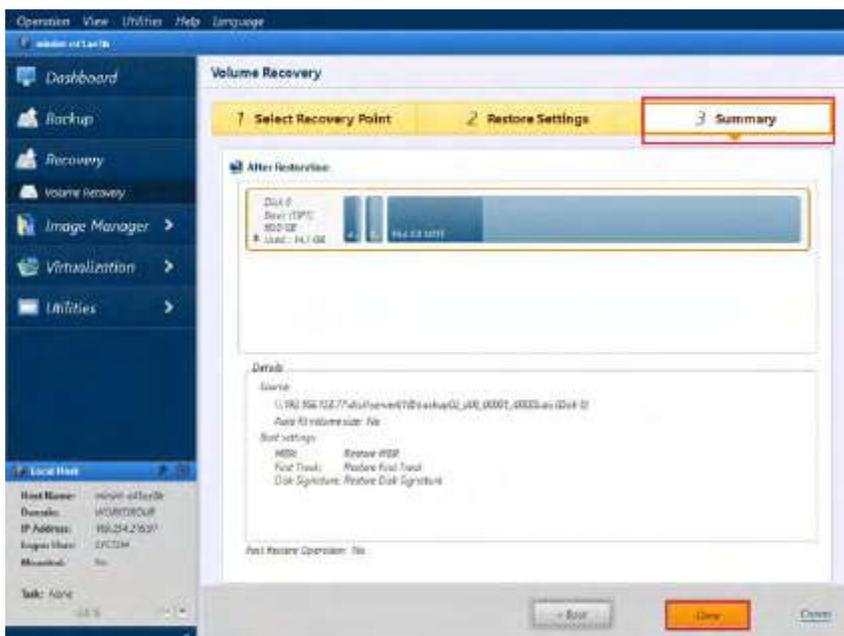
10. Right-click on the restore source selected in [Source Objects] and select “Disk 0 - Basic (GPT)” for [Target].



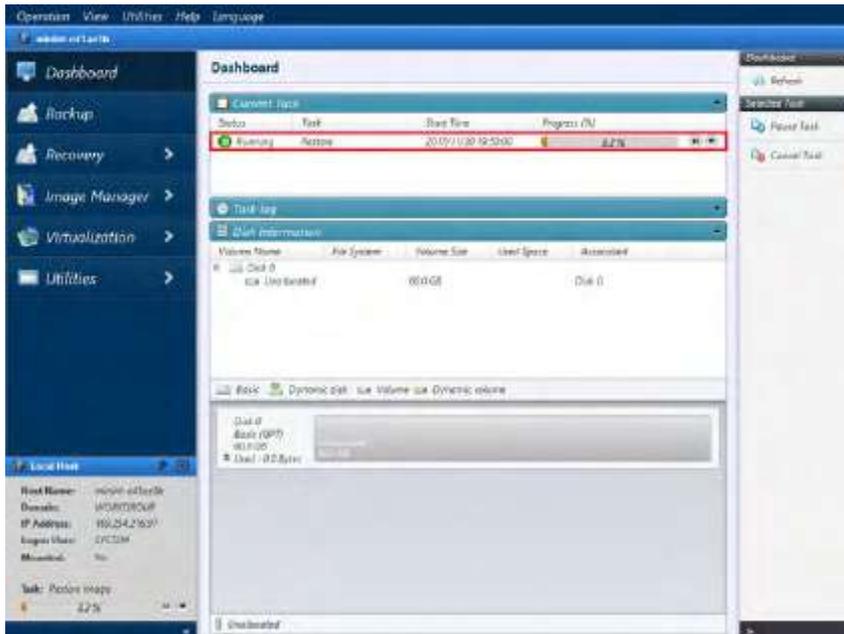
11. Please review the settings in **[Target Settings]** and click **[Next]**.



12. Review the summary and click **[Done]** to complete.

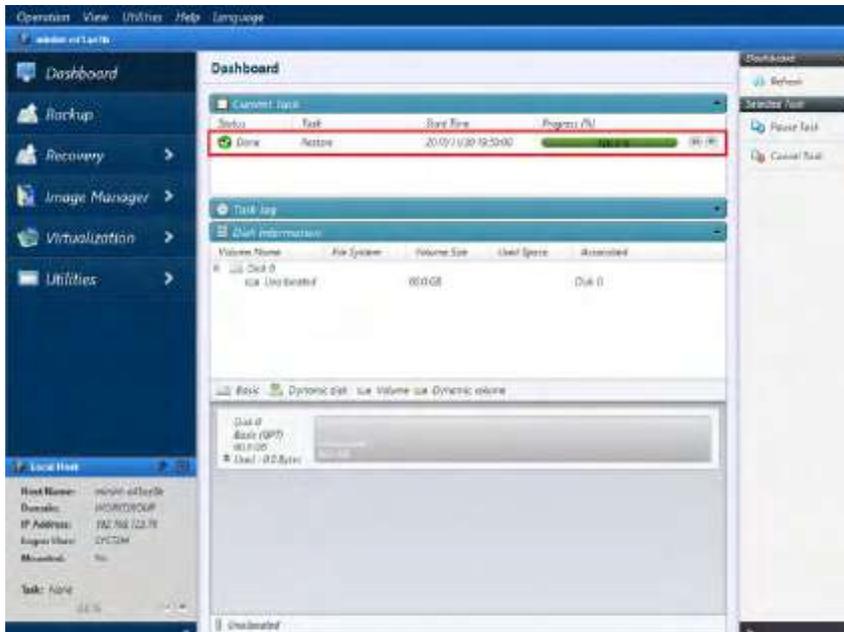


13. Restore task started.



14. When the Progress reaches “100%”, the recovery task completed. Select **[Operation]** – **[End]** to shut down or reboot the machine.

Ensure that the restore task successfully completed.



7. Image Manager

Image Manager tools provide a number of options that provide efficient management of backup image files.

1. Start ActivelImage Protector.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActivelImage Protector]**.

Windows 7 or earlier Desktop OS:

Click [Start] – [All Programs] – [NetJapan] – [ActivelImage Protector].

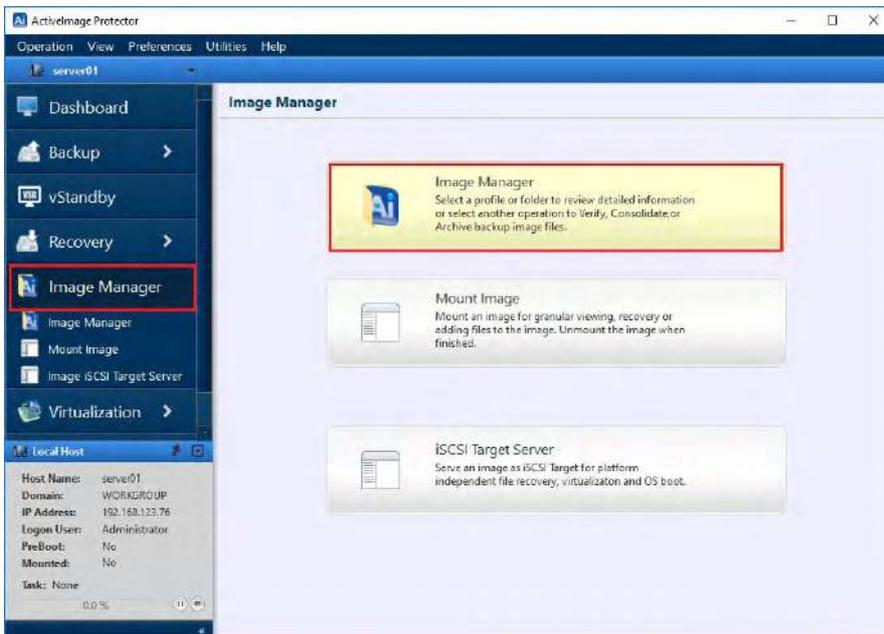
Windows Server 2012 or later server OS:

Click [Start] – [Applications] – [NetJapan] – [ActivelImage Protector].

Windows Server 8 or later Desktop OS :

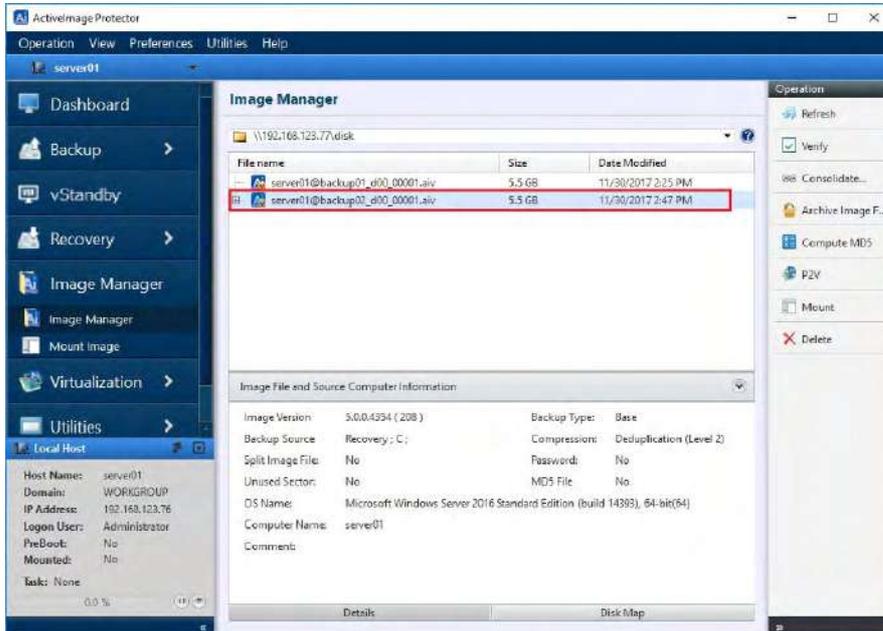
Click [Start] – [Applications] – [NetJapan] – [ActivelImage Protector].

2. Select [Image Manager] - [Image Manager].



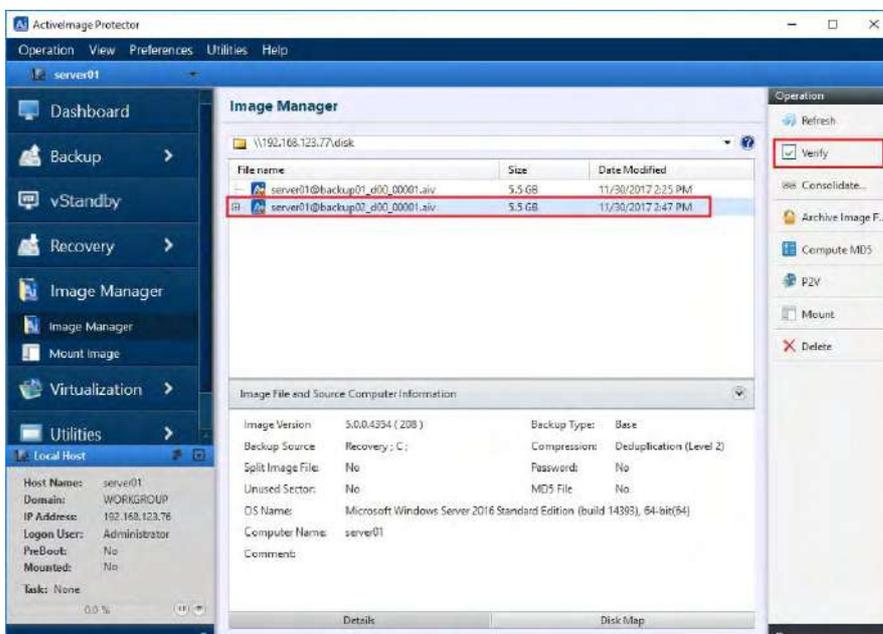
Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.

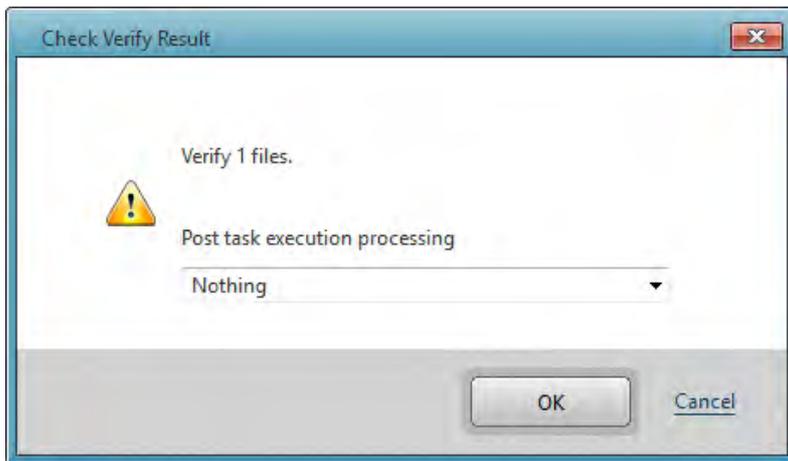
3. Select a backup image file.



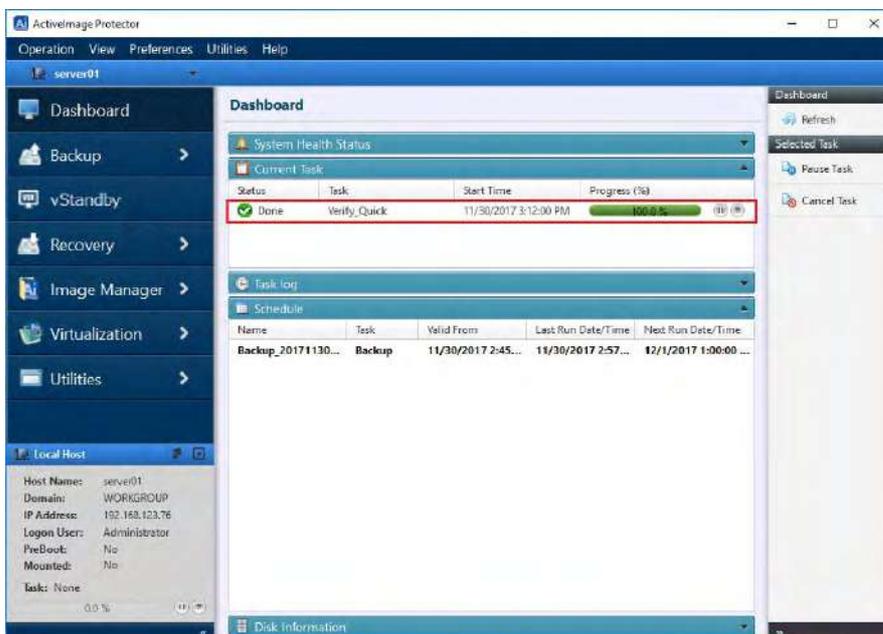
7-1. Verify Image

1. Verify the integrity of a backup image. Select a file then click **[Verify]**.



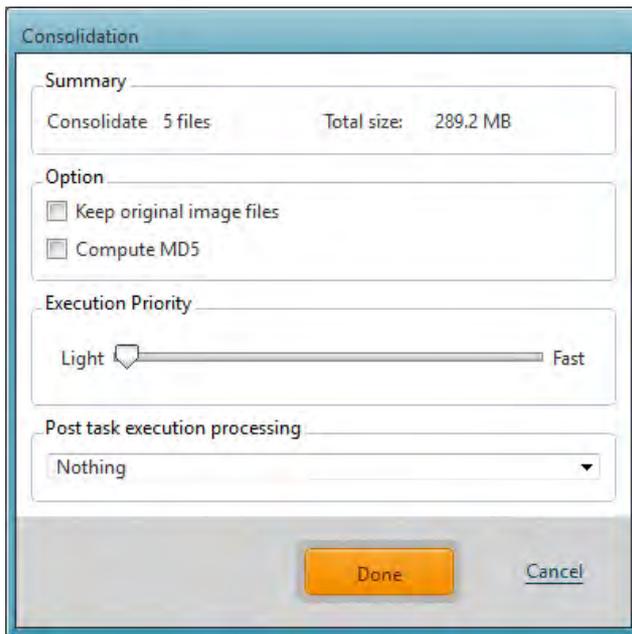


2. Upon completion of Verify task, the status and progress are displayed as follows.

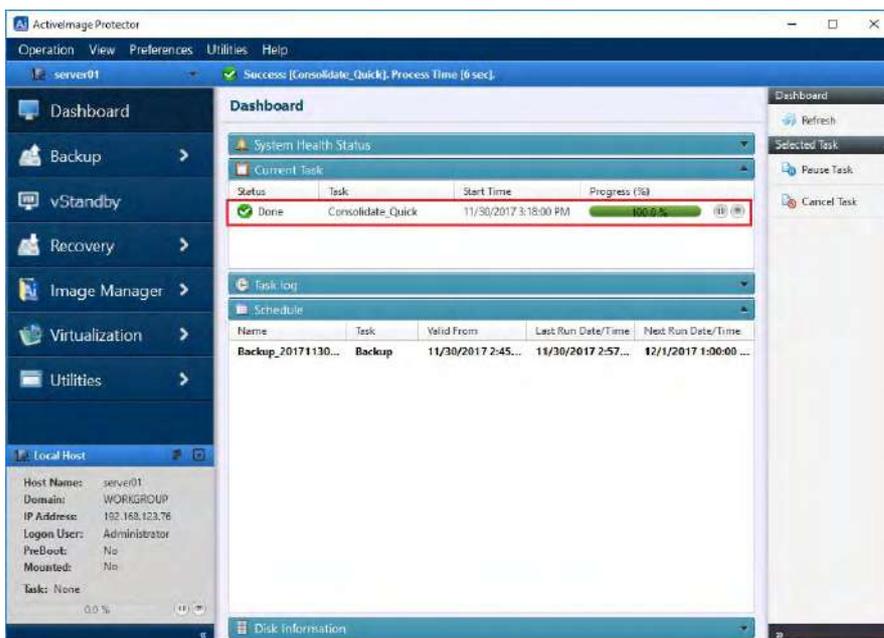


7-2. Consolidate Image Files

1. Select multiple incremental backup images to consolidate them into a single incremental file. Select the files and click **[Consolidate]** in the right pane. You can configure the following option settings.
 - Keep original image files** - By default, the original image files 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 image file.
 - Execution Priority** - Depending on the number of processes running on the system, adjust the execution priority for the consolidation process.
 - Post task execution processing** - Choices included are to **[Reboot]** or **[Shutdown]** once the consolidated file is created.

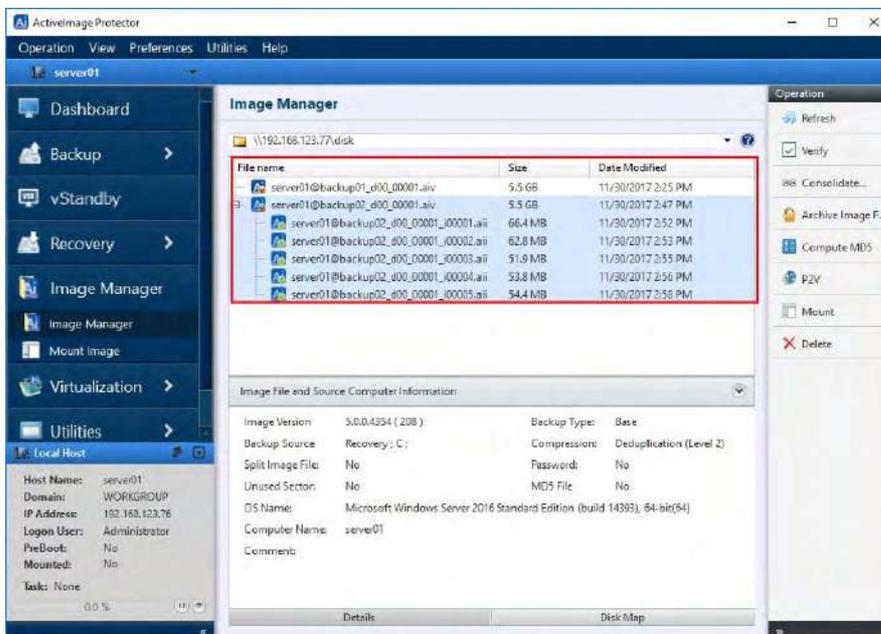


2. Upon completion of the consolidation task, the following window is displayed.



7-3. Archive Backup Image File

1. Archive feature unifies a base image file and an uninterrupted series of incremental files in the same generation set into a full backup file and saves it under a different name. Select a full (base image file) and incremental files from the same generation set.

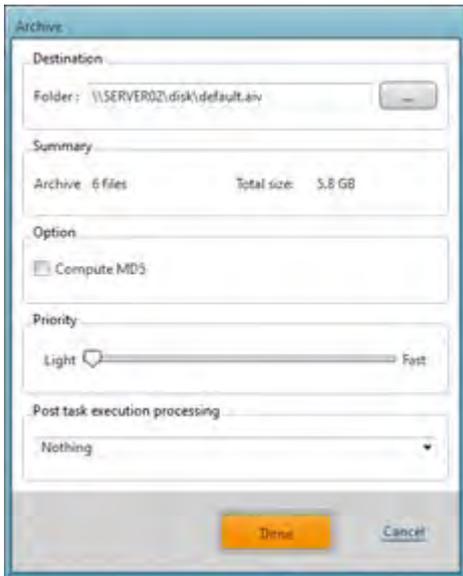


2. You can configure the following option settings.

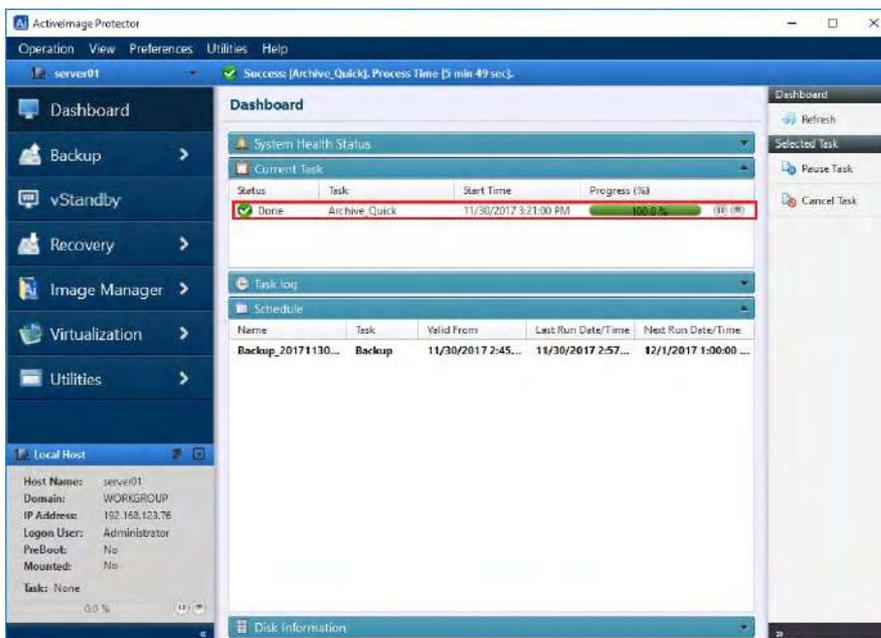
Compute MD5 - Creates an MD5 checksum file for the archived file.

Priority - Depending on the number of processes running on the system, adjust the execution priority for the archiving process.

Post task execution processing - Choices included are to [Reboot] or [Shutdown] once the archived file is created.

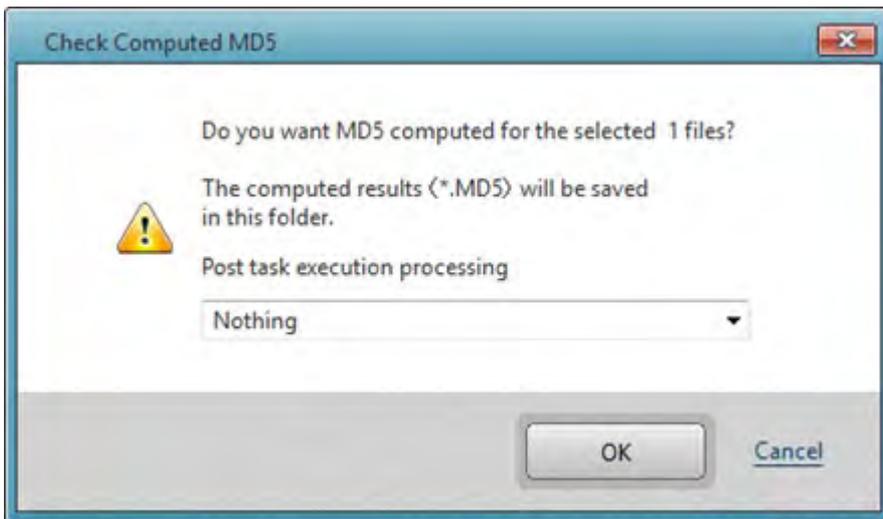


3. Upon completion of Archive task, the following information is displayed in Dashboard window.

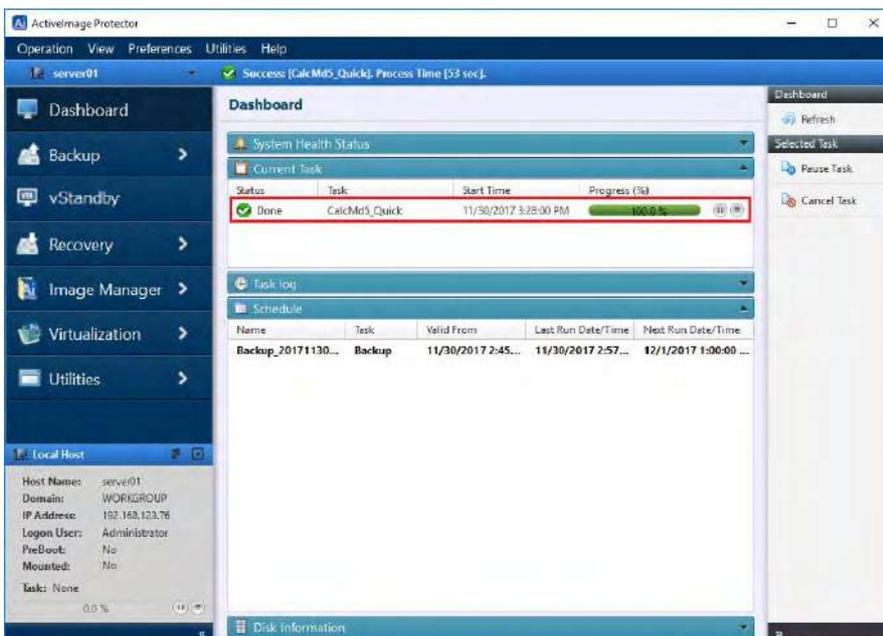


7-4. Compute MD5 hash value

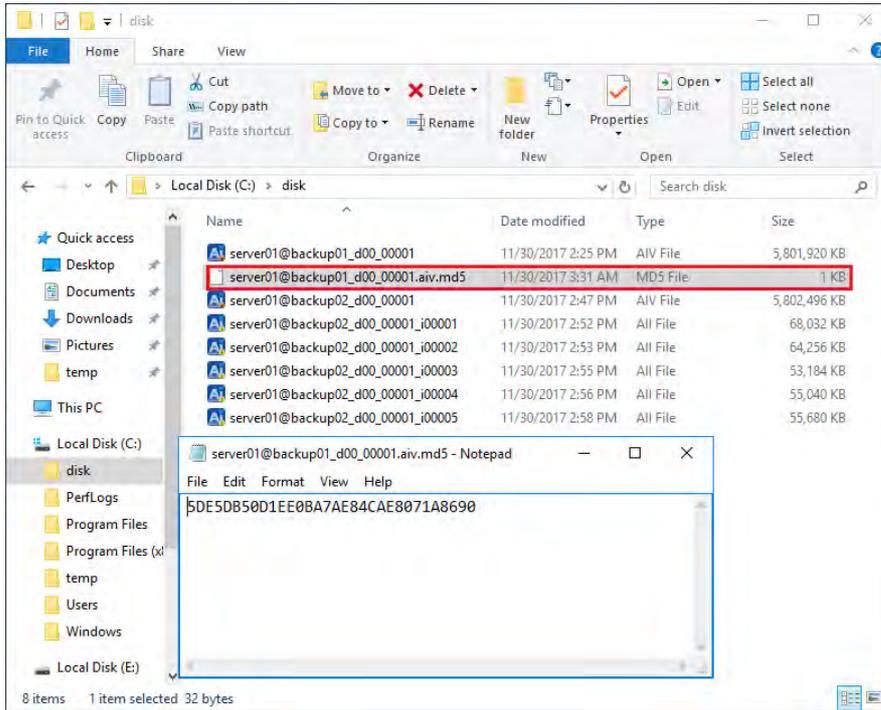
1. Create an MD5 checksum for the selected image file. This can be used as a security measure to check if internal tampering of the image file has occurred in a copy of the image.



2. Upon completion of computing MD5, the following information is displayed in Dashboard window.

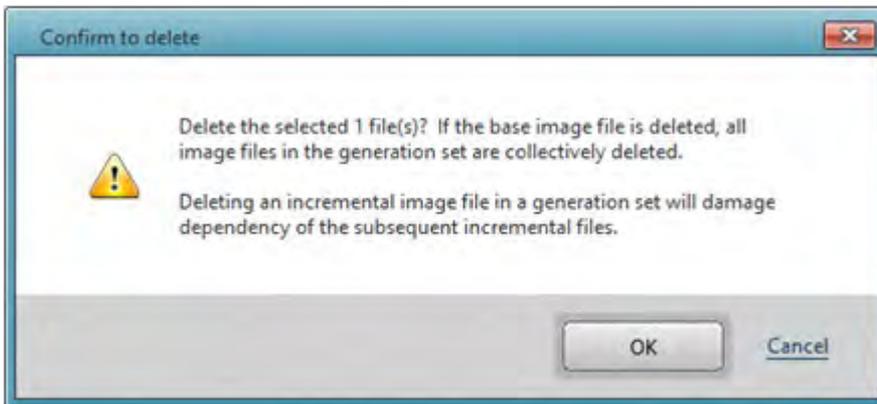


3. Please make sure that the MD5 file is created by using Windows Explorer.



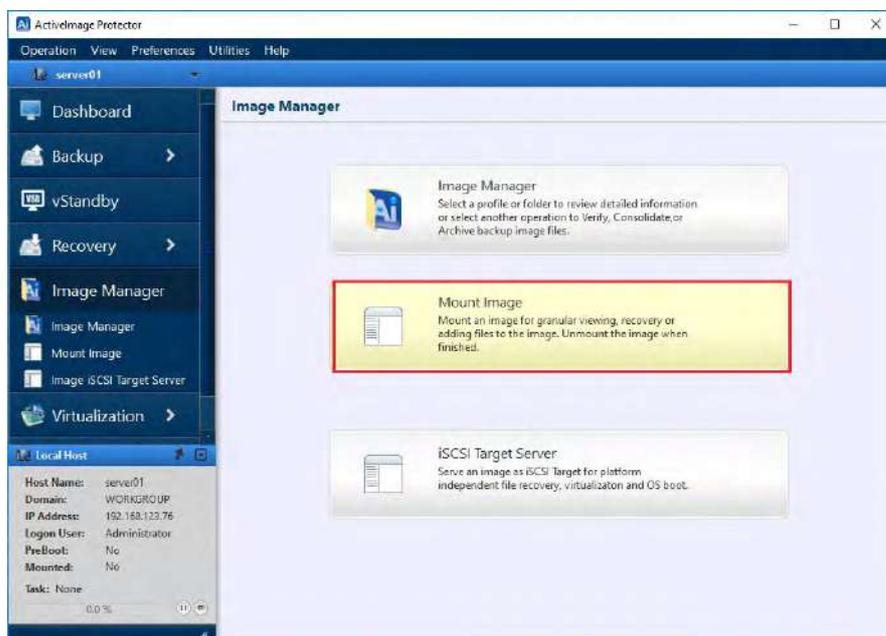
7-5. Delete

You can select to delete a base or incremental image file(s). Please keep in mind that this type of deletion cannot be undone.



8. Mount Backup Image

1. Go to [Image Manager] and select [Mount Image].



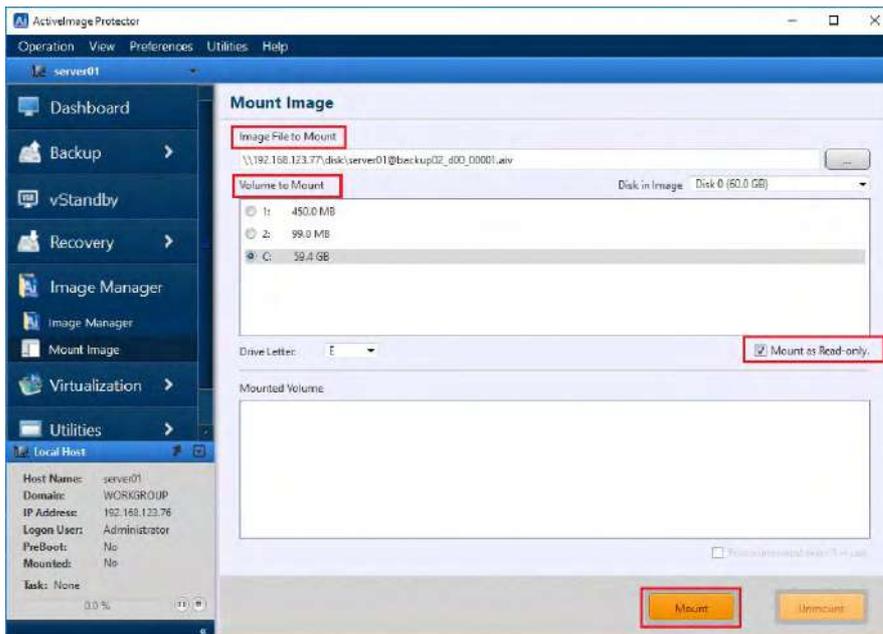
Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.



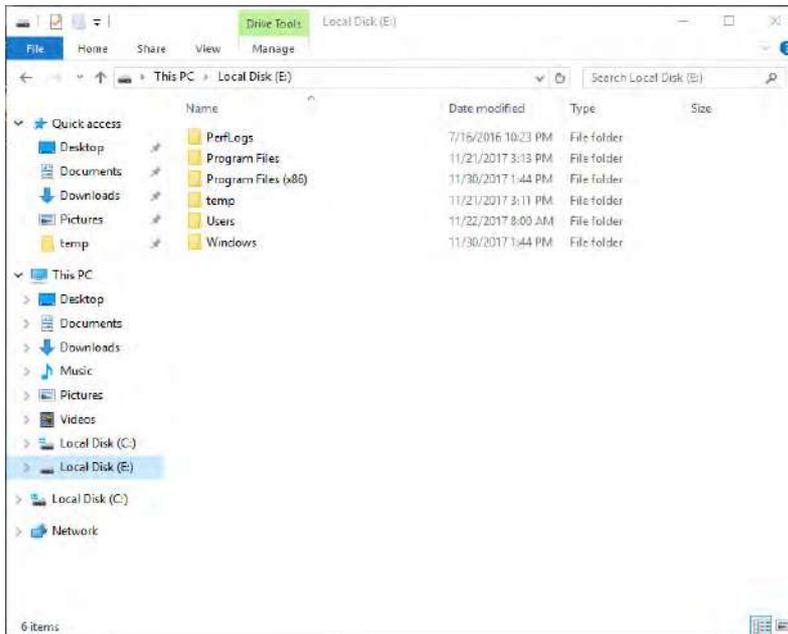
2. Select the backup image to mount. If the selected image includes multiple disks, select a disk.

Select a volume to mount from the image.

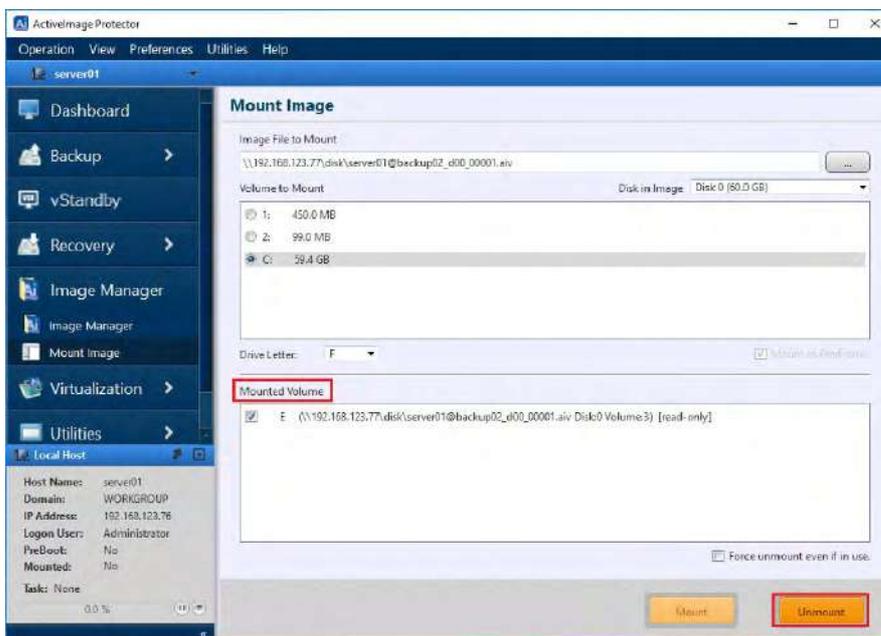
Specify the drive letter and click **[Mount]**. The image file can be mounted as read-only (default) by selecting the **[Mount as Read-only]** option.



3. In the mounted image file, you can select and open or copy a file / folder in the same manner as you operate read-only drive in Windows Explorer.



4. To unmount the image file, Select a mount point from the **[Mounted Volume]**. Click **[Unmount]**.



*Uncheck **[Mount as Read-only]** option to mount the image file as writable. The changes made to the image file are saved in a differential image file (.aiv) after the volume is unmounted.

9. Image Management –iSCSI Target Server

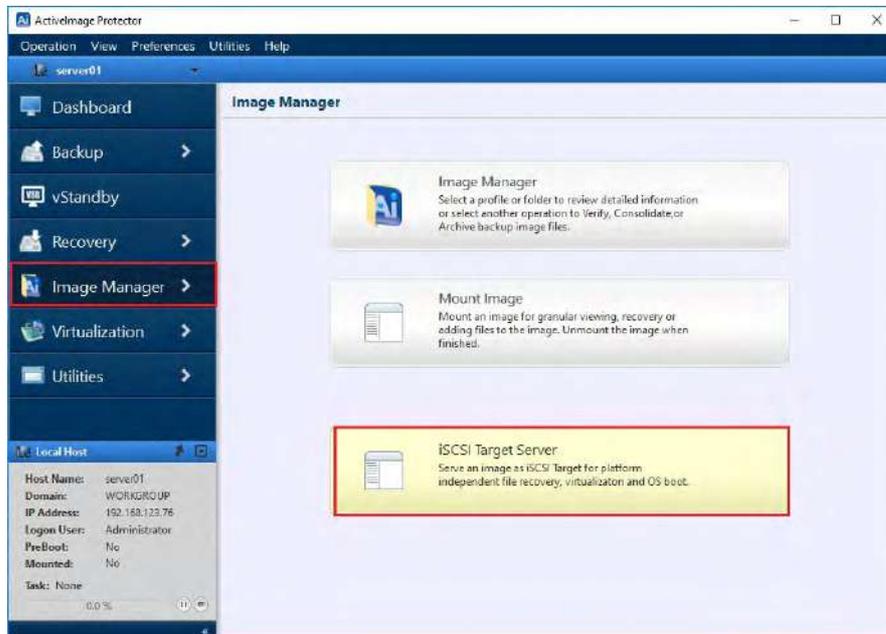
Networked data storage (Network Attached Storage) includes SAN (Storage Area Network), NAS (Network Attached Storage), etc. FC-SAN (Fibre Channel Storage Area Network) provides high-speed data communication. However, they are expensive in cost and complex to configure and manage.

In the meantime, iSCSI contributes to solve those problems. iSCSI provides direct access to storage devices over network and TCP/IP packet transmission carrying SCSI commands and data. The use of your IP connectivity enables to freely configure iSCSI targets. iSCSI targets may be recognized and utilized to serve as a local drive. It may consume extra CPU resources and increase the load on the network. However, the advantages are that iSCSI targets can be freely deployed in your system environment and the existing network devices can be used without modification.

ActiveImage Protector Update provides a new feature to utilize any backup image file serving as an iSCSI target.

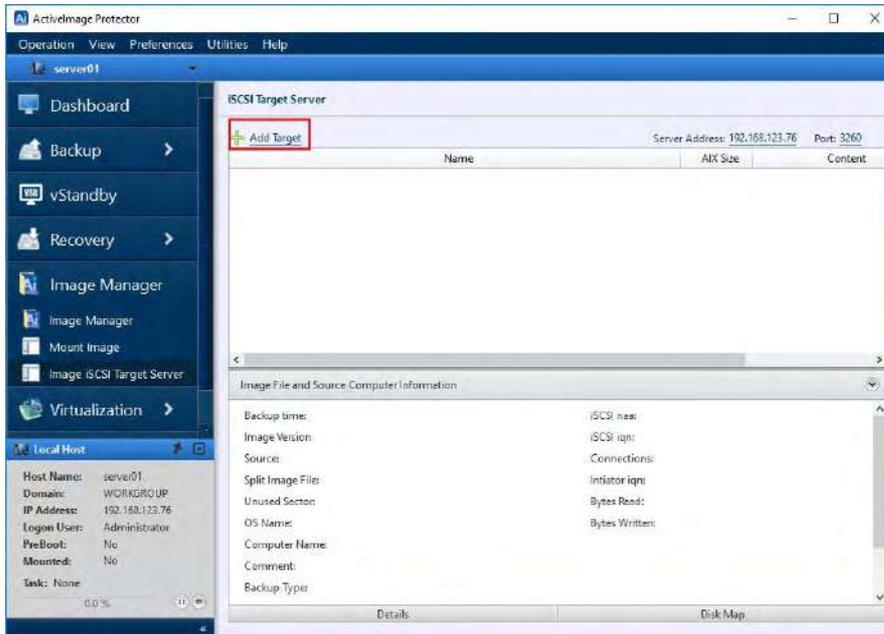
9-1. Mount Backup Files to Local Disk

1. Select **[Image manager] – [Image iSCSI Target Server]** in the left menu in ActiveImage Protector.

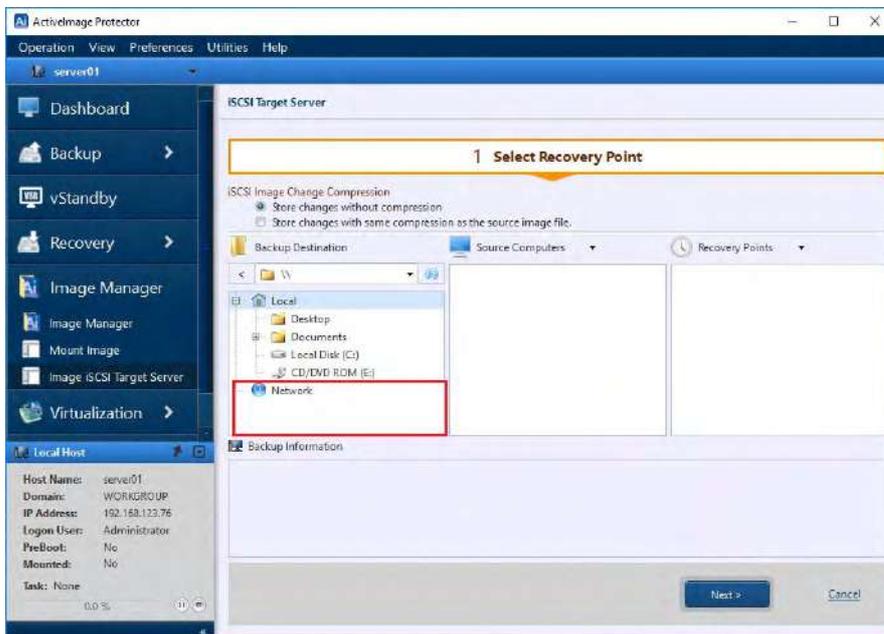


Note) The left pane of ActiveImage Protector for Hyper-V Enterprise screen is different from the one of Server Edition. There is no “iSCSI Target Server” menu.

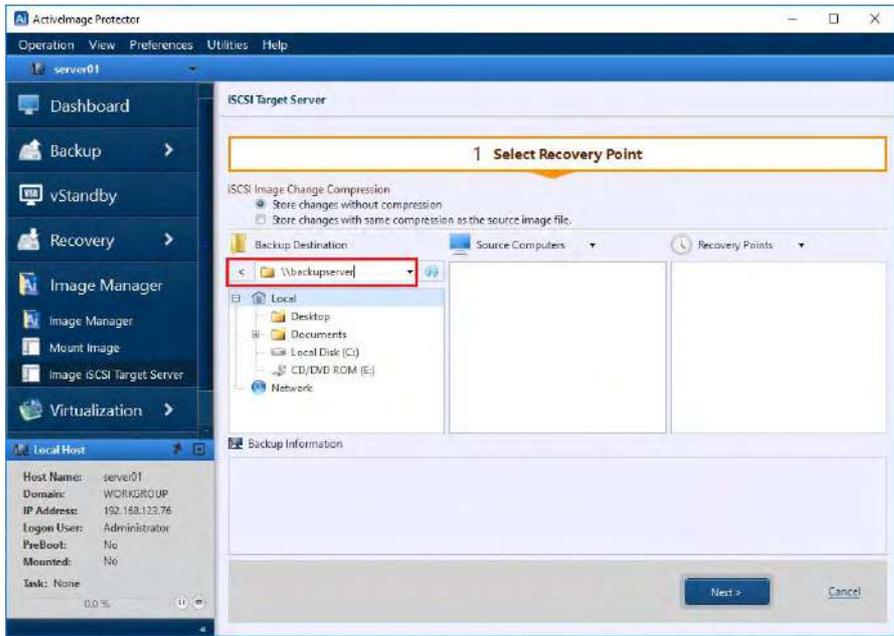
2. **[iSCSI Target Server]** window is shown as below. iSCSI targets will be listed in the window. To add a target, click **[Add Target]** at the upper left corner of the list.



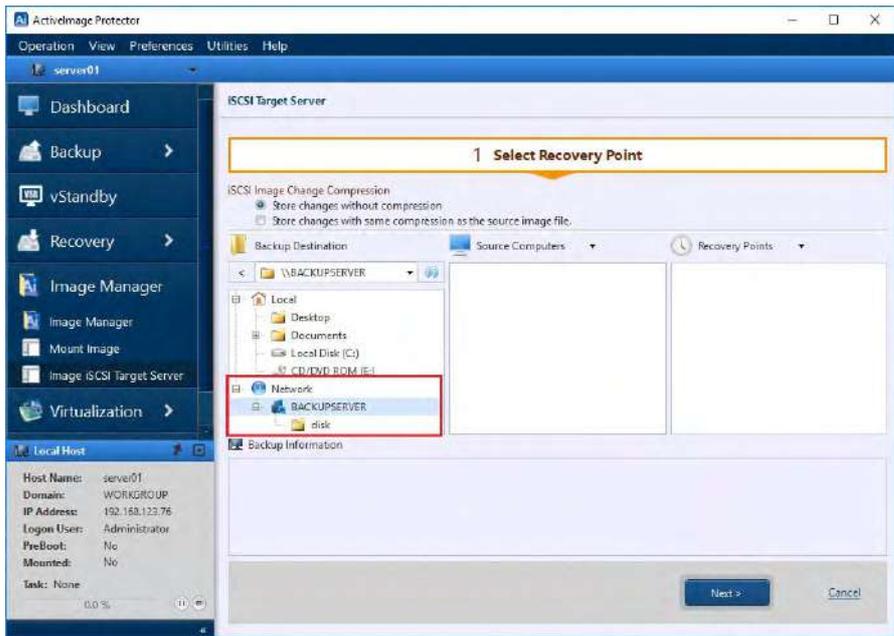
3. Select a backup image file and recovery point.



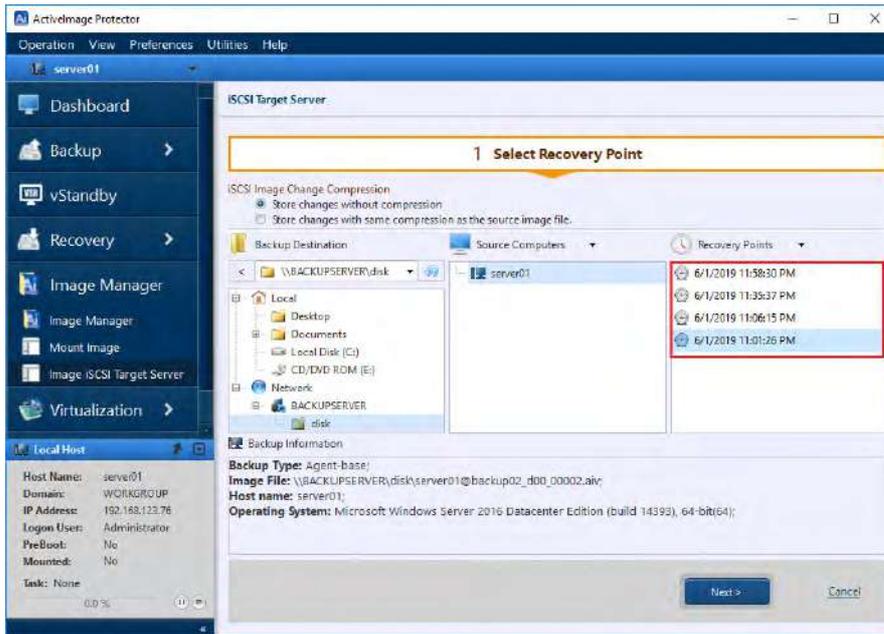
If no network shared folder is displayed under “Network” in [Backup Destination] column, enter a server name following “\\” in the text box.



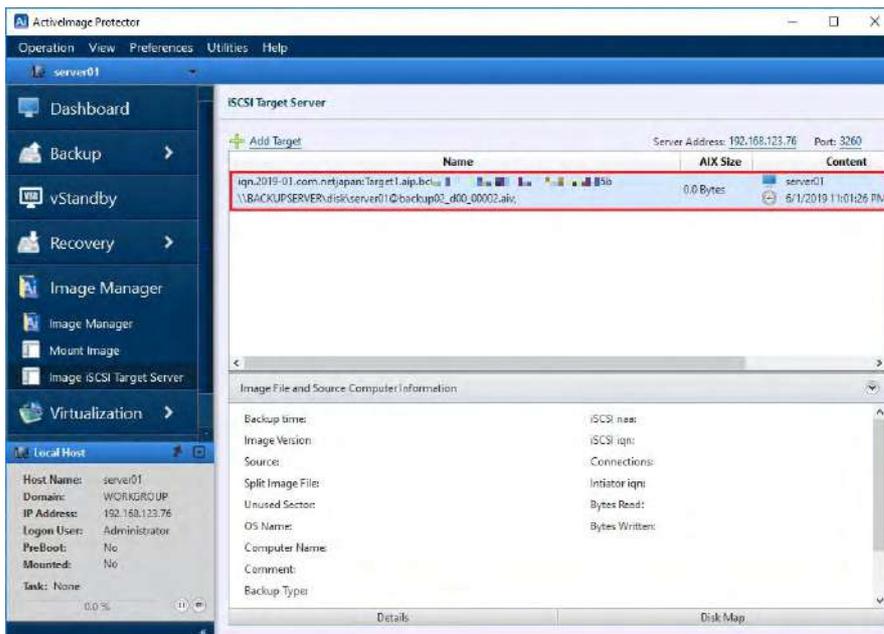
4. Upon completion of a search, shared folders are found under “Network”.



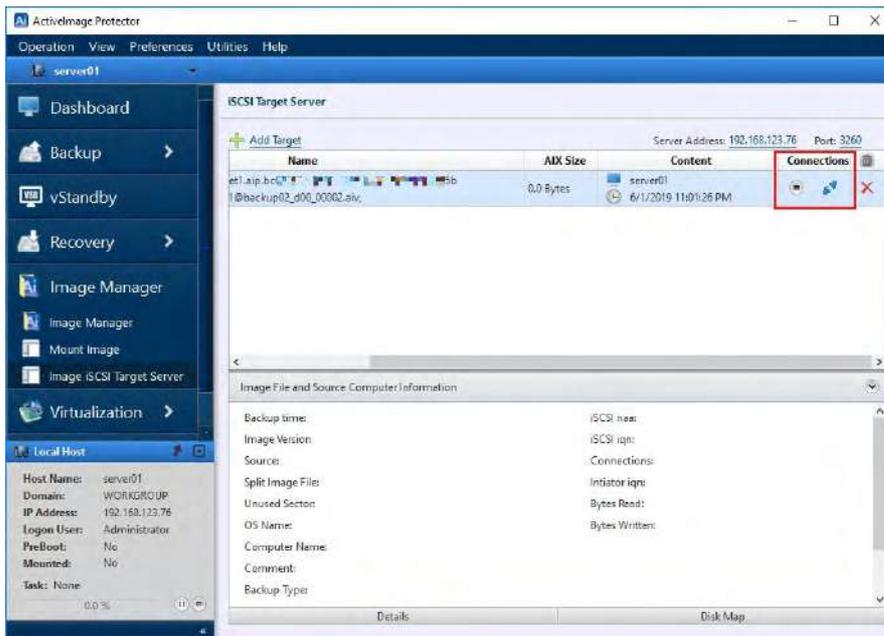
5. Select a backup file and a recovery point.



6. The backup file serving as iSCSI target is listed.

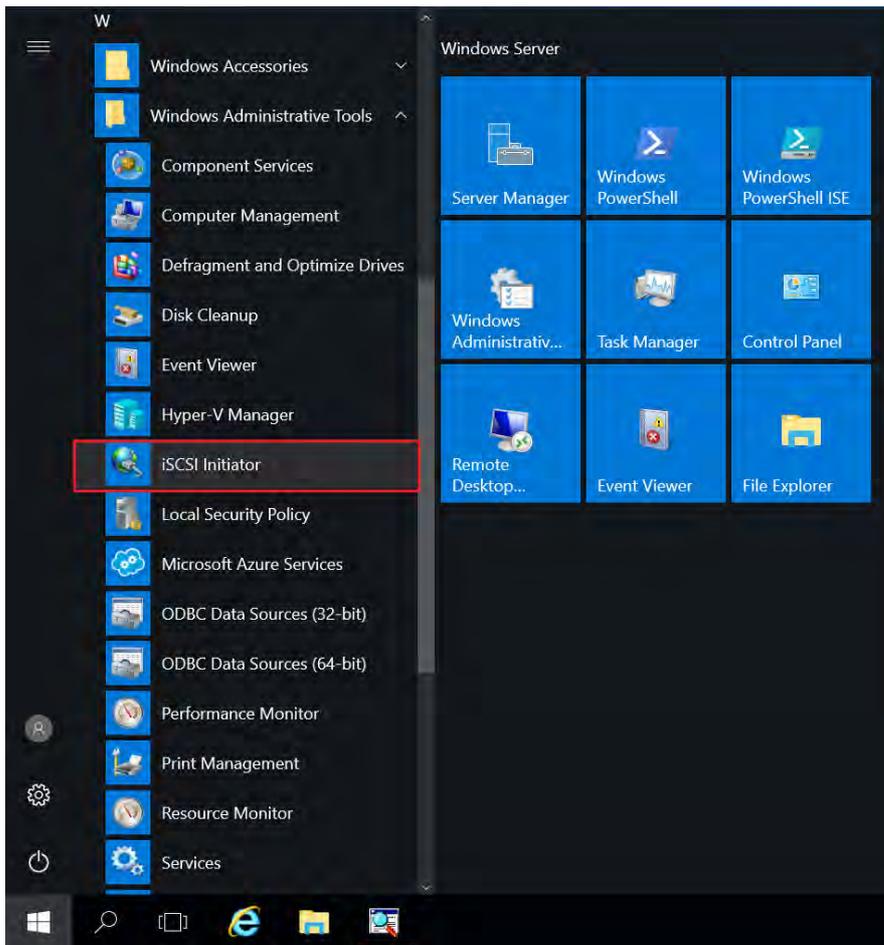


7. Move the slide bar to the right and display the **[Connection]** column.

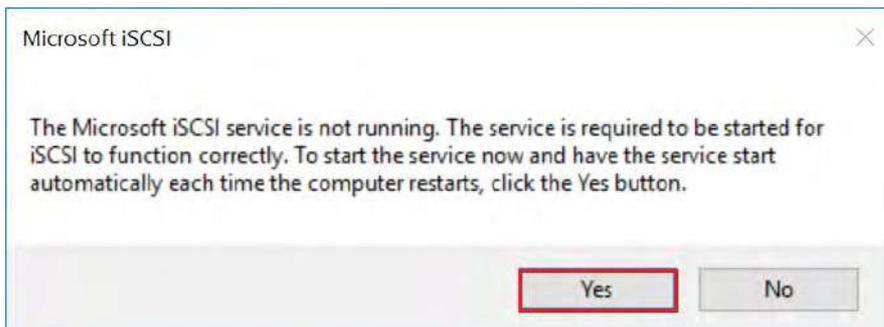


Please be aware of the detached connector icon indicating that the iSCSI target is not network connected.

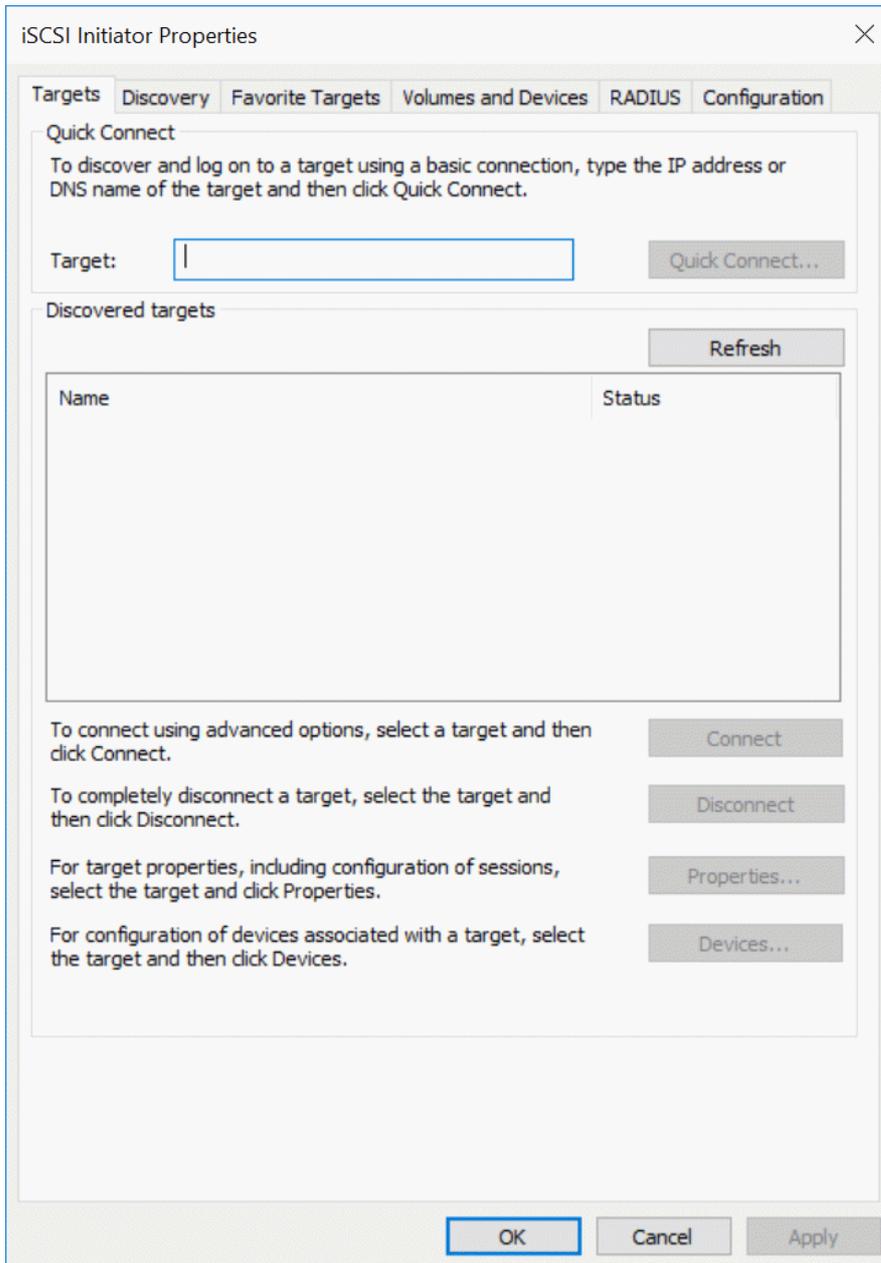
8. Next, select **[iSCSI Initiator]** in Start menu to discover iSCSI target.



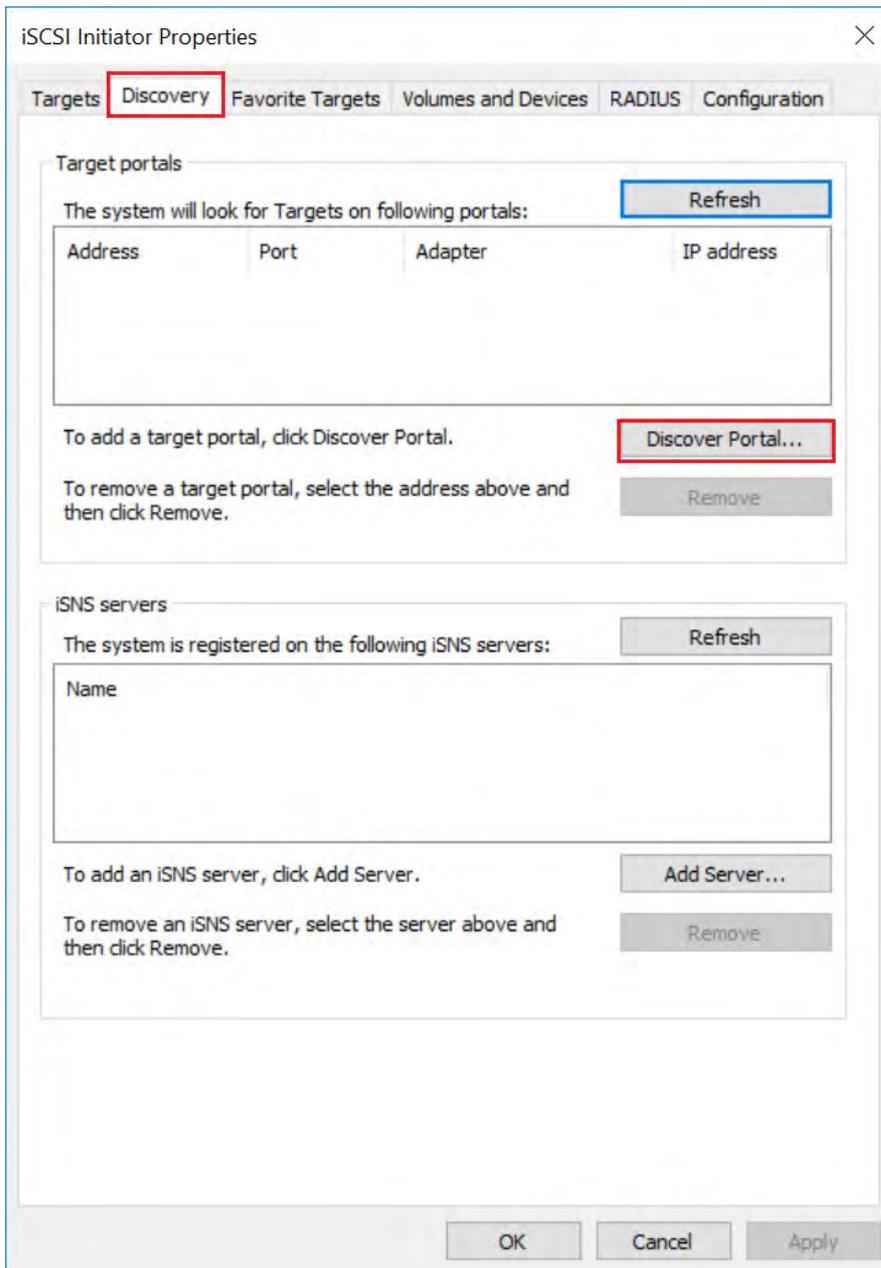
9. When you try to start Microsoft iSCSI Service for the first time, you will get the following confirmation message as shown below. Click **[Yes]**.



10. iSCSI Initiator is started and iSCSI Initiator Properties window is displayed as shown below.

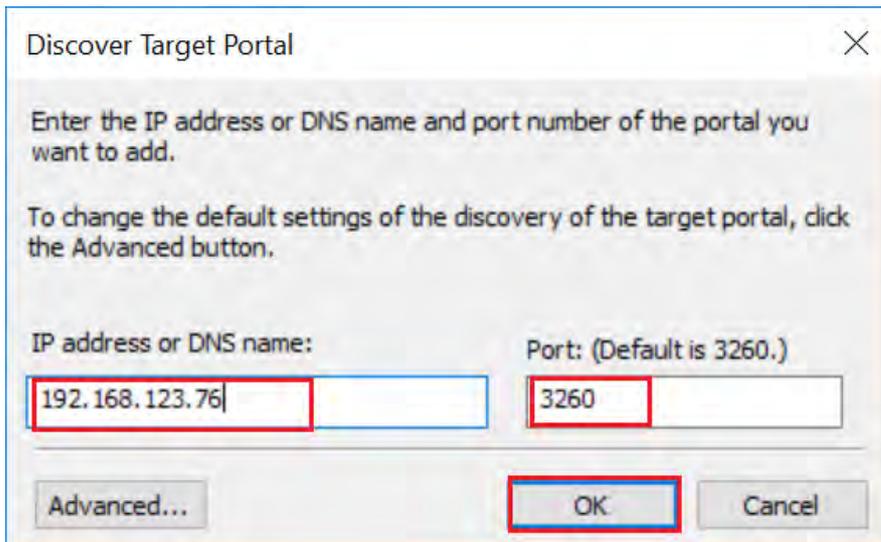


11. At present, no iSCSI target is added to the list. Select **[Discovery]** tab.

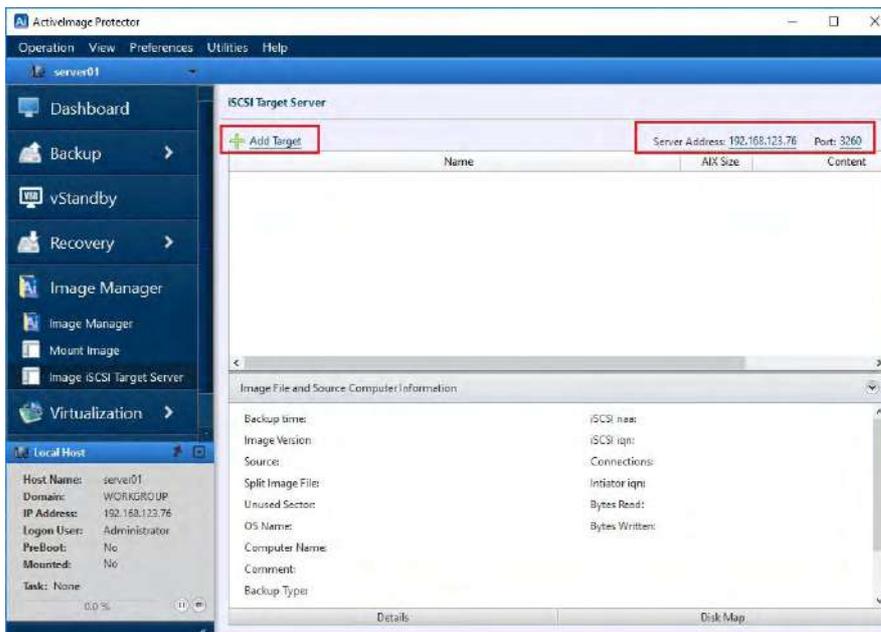


iSCSI target created by using ActiveImage Protector is searched for and added to the list. Click **[Discover Target Portal]**.

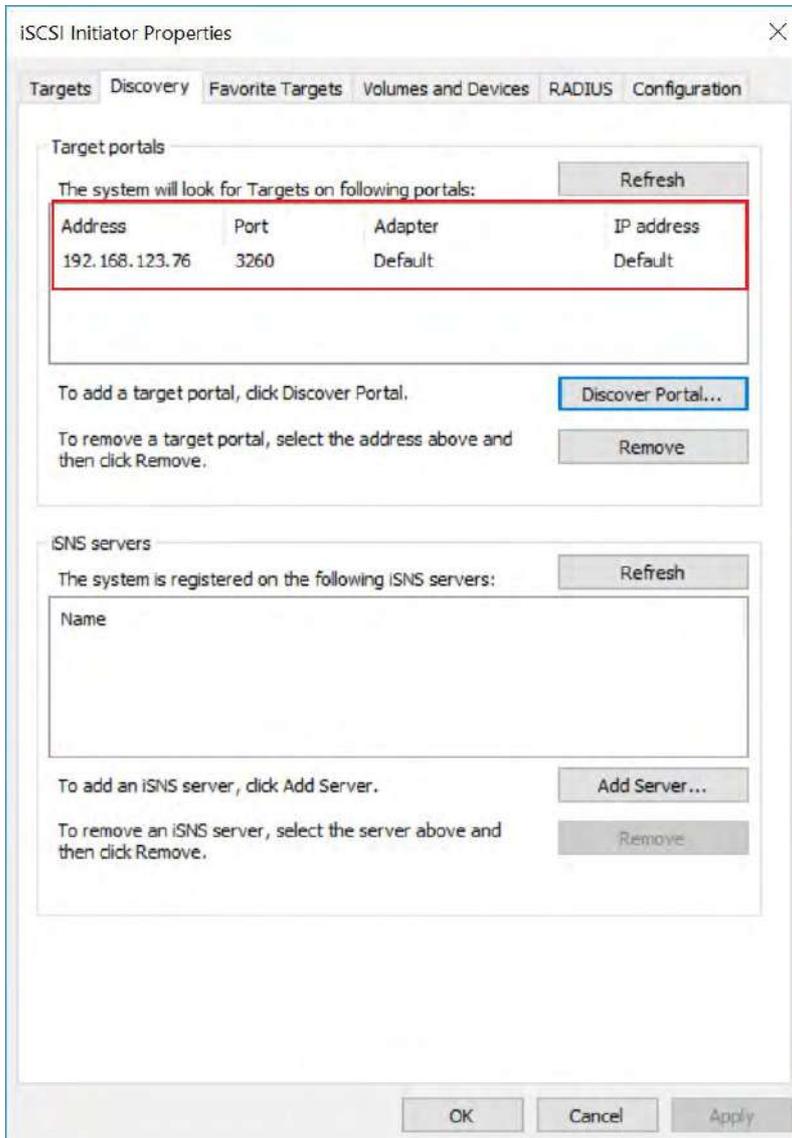
12. Target portal is searched for.



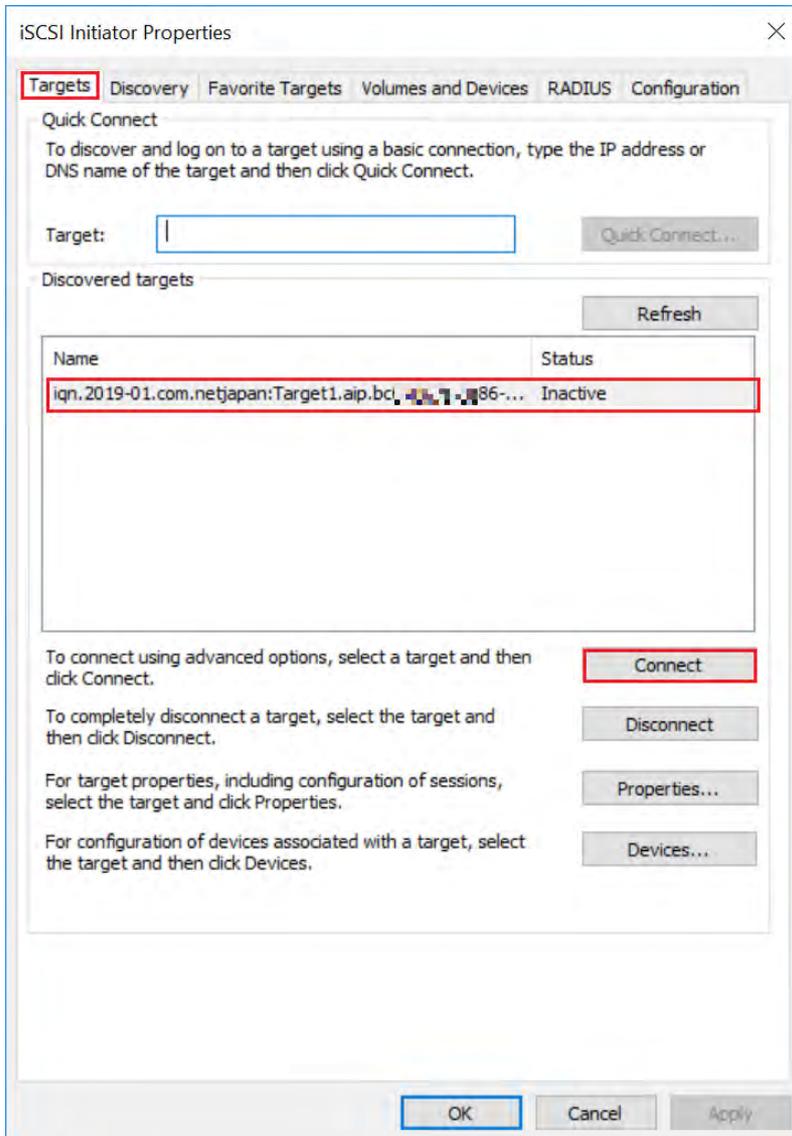
Enter “192.168.123.11” in the blank field for **[IP address or DNS name]**. This IP address was indicated for **[Server Address]** at the upper right in **[iSCSI Target Server]** window of ActiveImage Protector. “3260” was indicated, by default, for **[Port]**. Please make sure these numbers are identical.



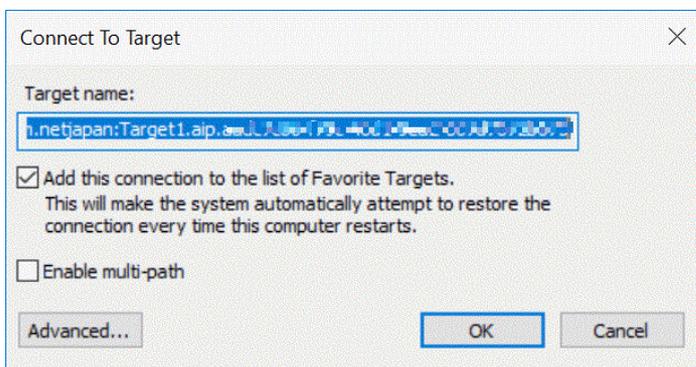
13. Click **[OK]** and the entered IP address is indicated under **[The system will look for Targets on following portals:]**.



14. Go back to **[Target]** tab. iSCSI target indicated in the following screen is listed in **[Discovered targets]**.

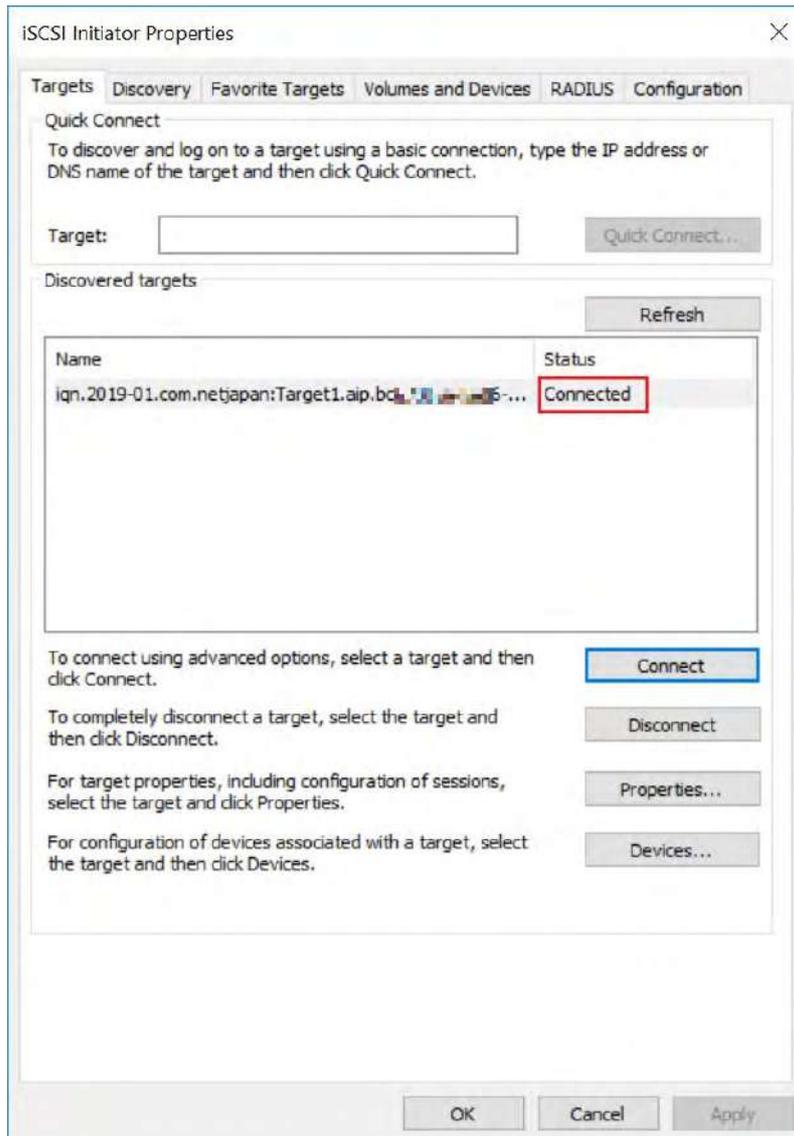


15. The name of the discovered target is the same as the backup file name added to iSCSI target list shown blow. click **[Connect]** to connect to the target.

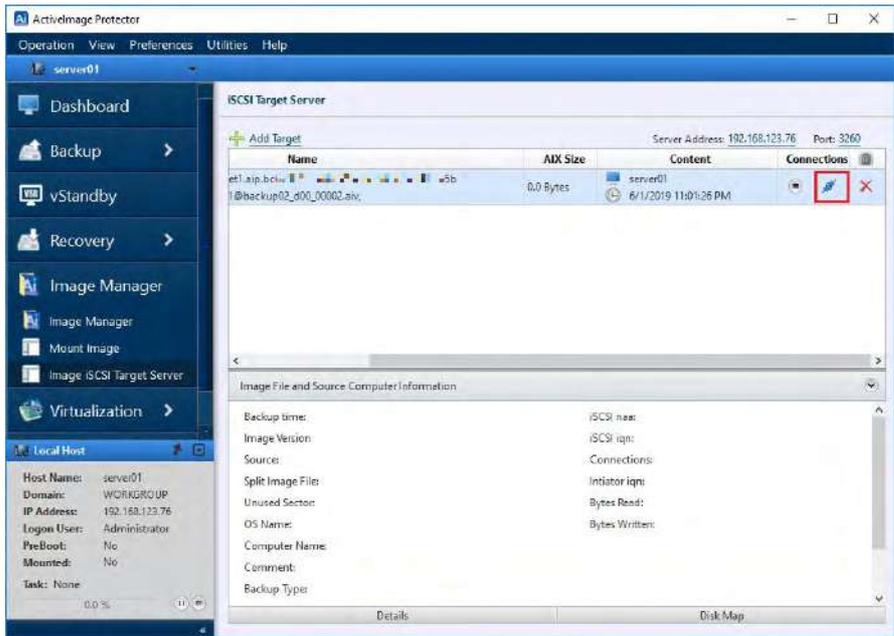


16. By default, **[Add this connection to the list of Favorite Targets]** option is enabled. As explained under the option, the system automatically attempts to restore the connection every time the computer restarts. Click **[OK]** to connect to the target.

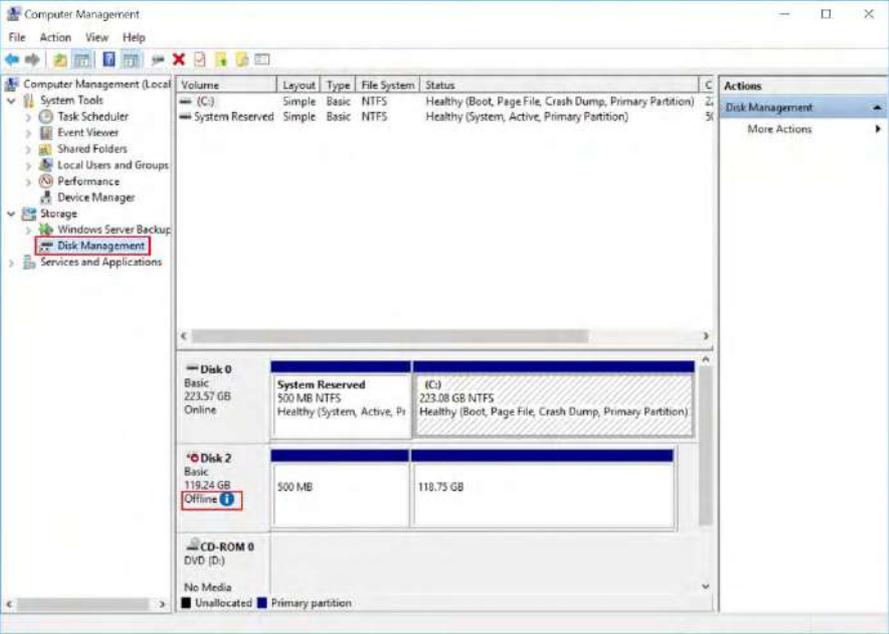
The **[Status]** of the **[Discovered target]** is **[Connected]** in **[Target]** tab.



Now, go back to ActiveImage Protector. The detached connector icon is attached now as you see in the following screen.

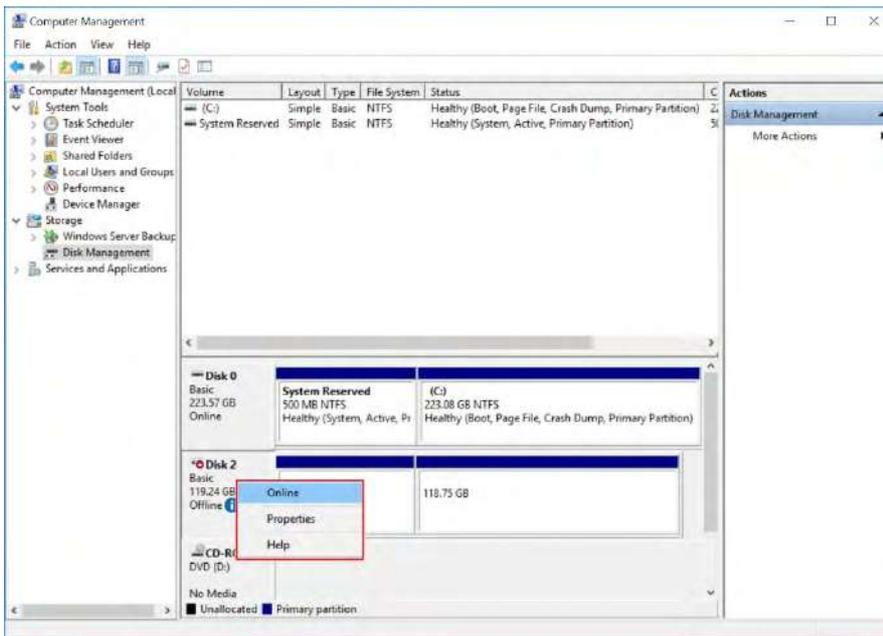


17. Go to [Management Tool] and launch [Computer Management] to select [Disk Management] in the left menu.

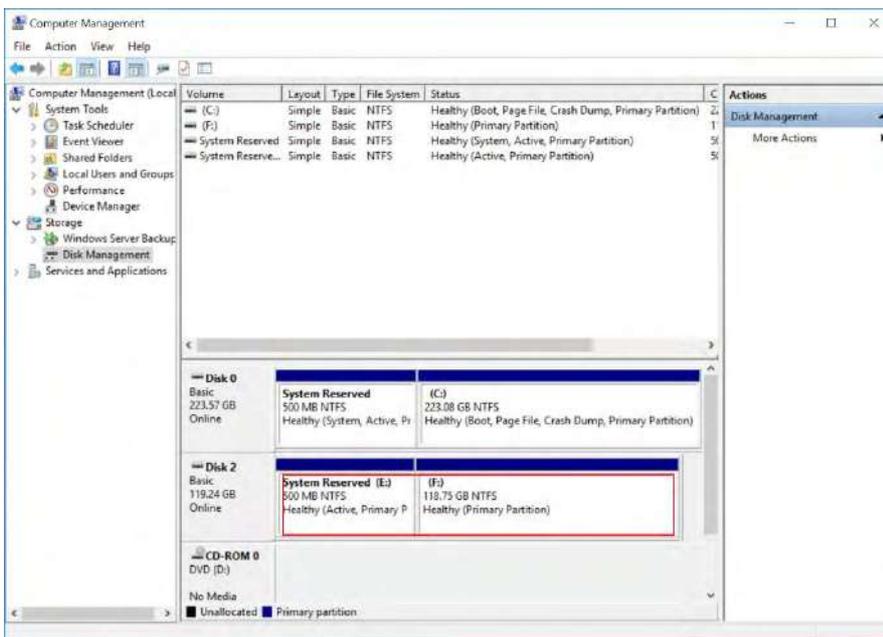


Disk 1 is added under offline condition.

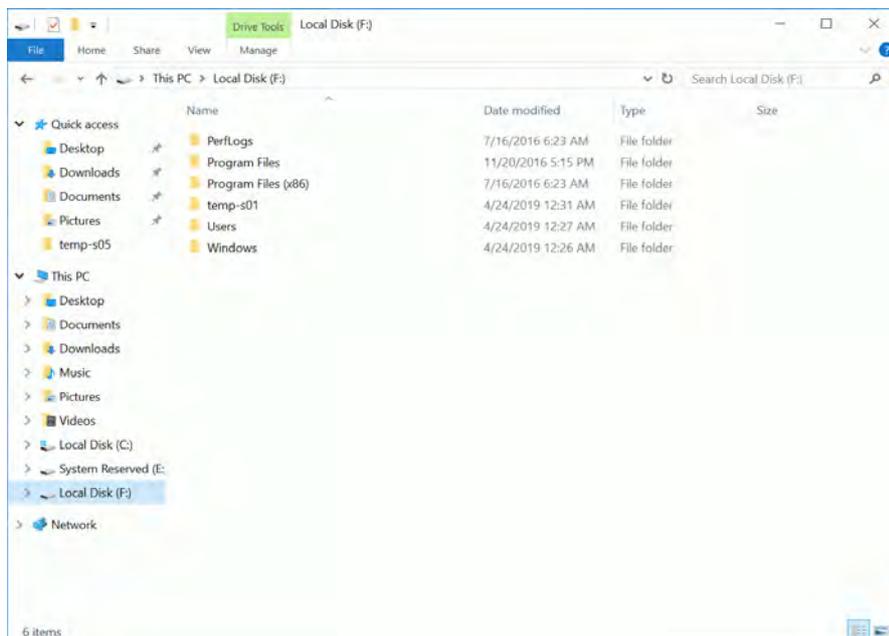
18. Right-click on Disk 1 to display the context-menu as shown below.



19. Select **[Online]** in the context menu and Disk 1 will be recognized as a local disk. The drive letter is assigned to the partition.

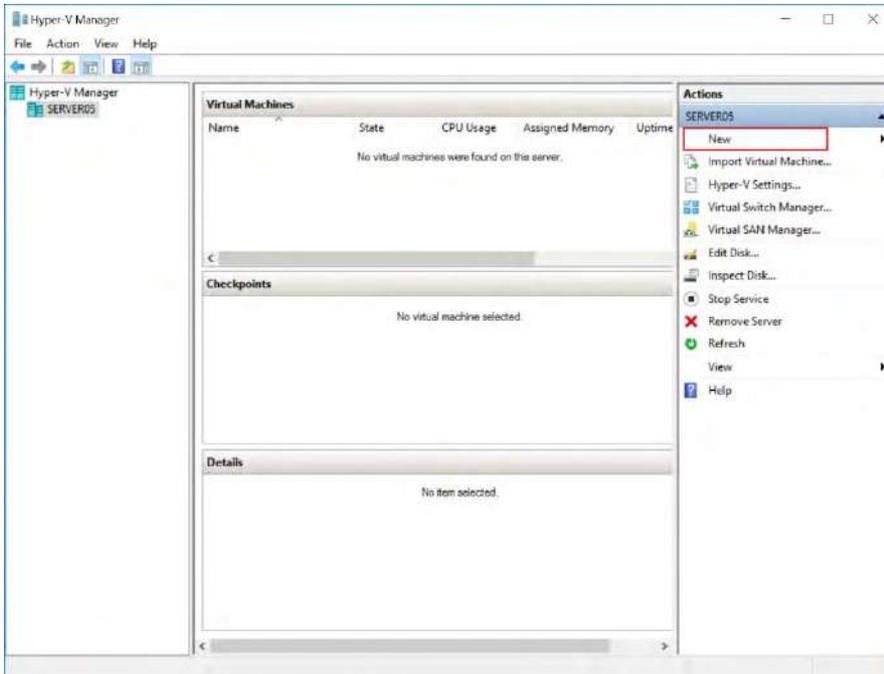


20. You can browse the disk in File Explorer as shown below:

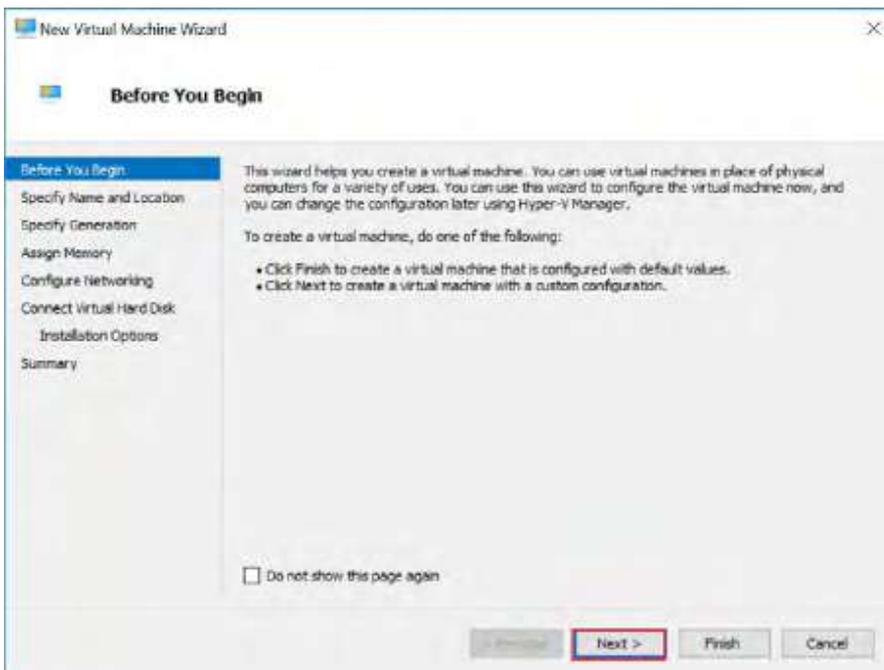


ActiveImage Protector provides Mount Image feature, which, however, enables you to mount a backup image via ActiveImage Protector. A local disk serving as iSCSI target offers a local file system in data area, which provides disaster recovery solution in the event of a system failure.

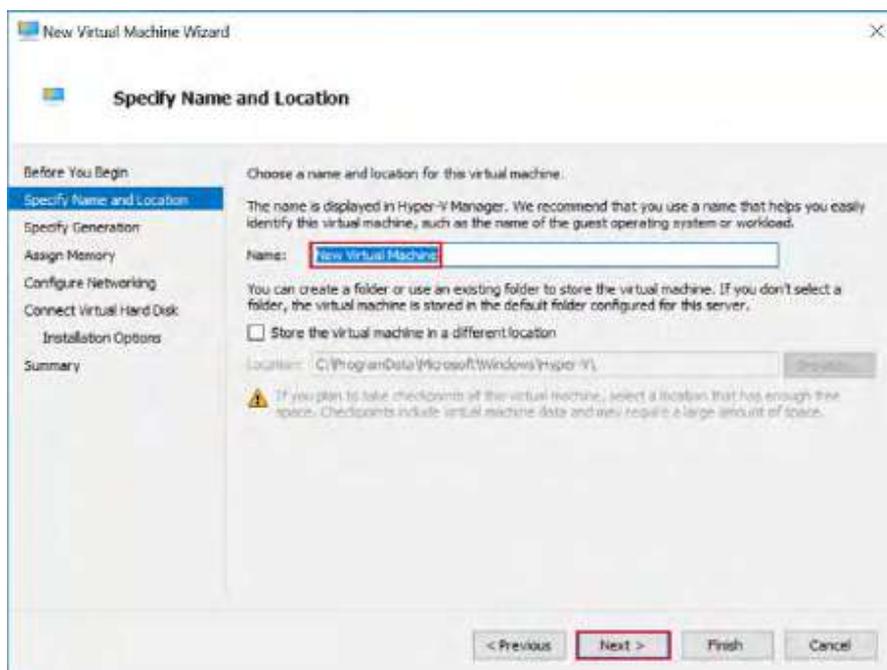
- At present, there exists no virtual machine. Select **[New]** in the right menu to create a new virtual machine.



- New Virtual Machine Wizard is launched as follows.

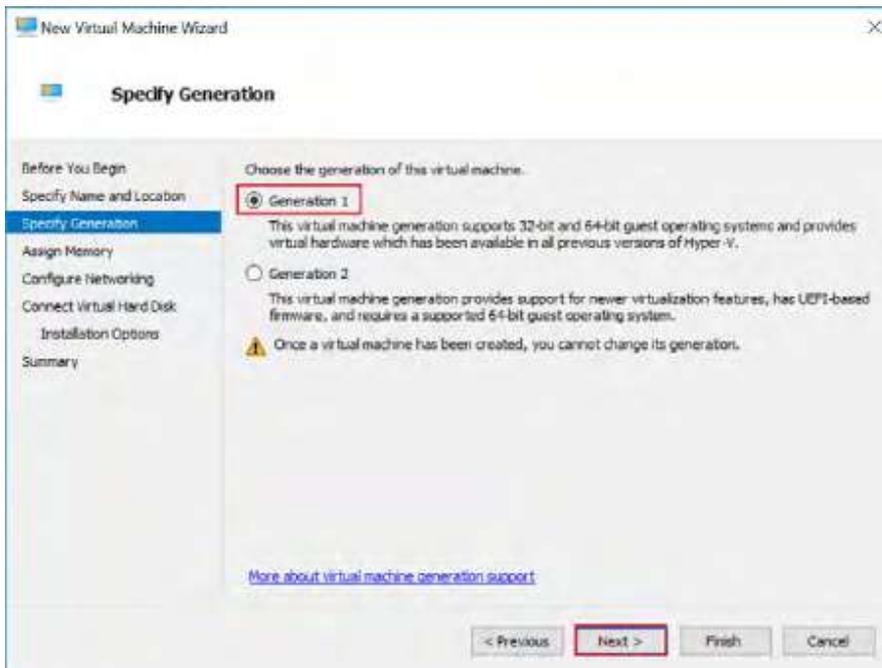


4. Click [Next] to display [Specify Name and Location].



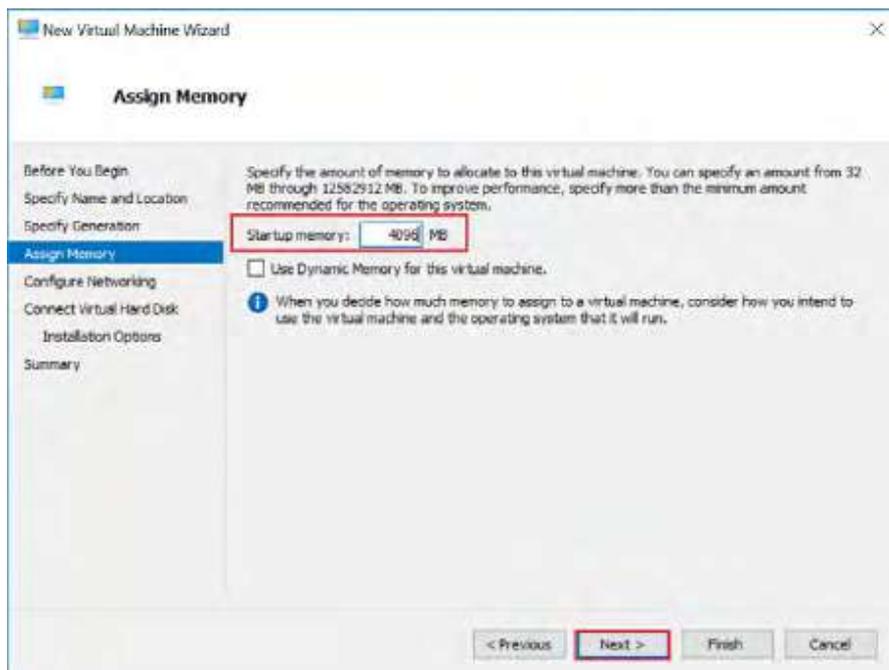
In this example, the default name “New Virtual Machine” is used for [Name] and the default destination location is used.

5. Click **[Next]** to display **[Specify Generation]** window.



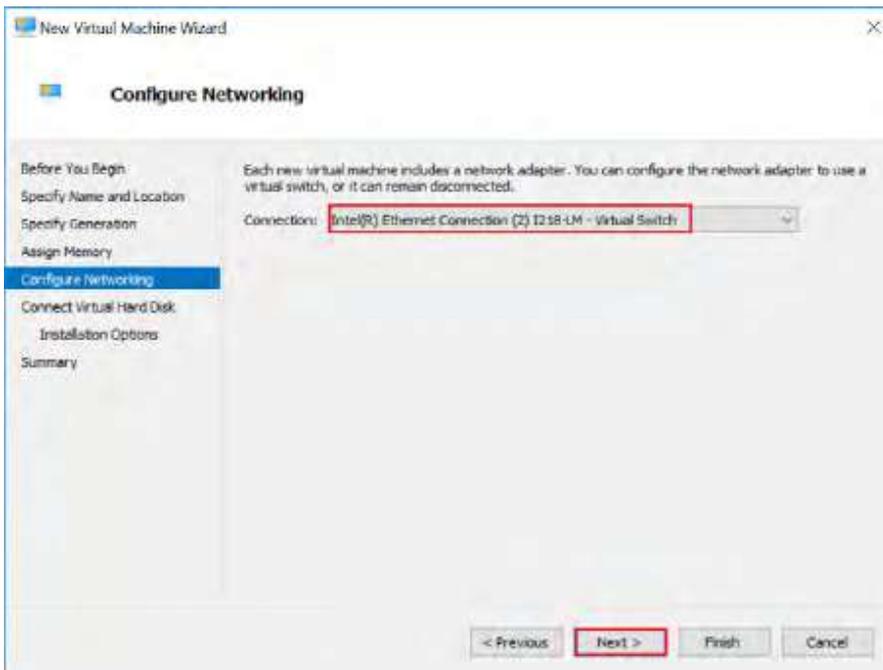
By default, **[Generation 1]** is selected.

6. Click **[Next]** to display **[Assign Memory]** window.

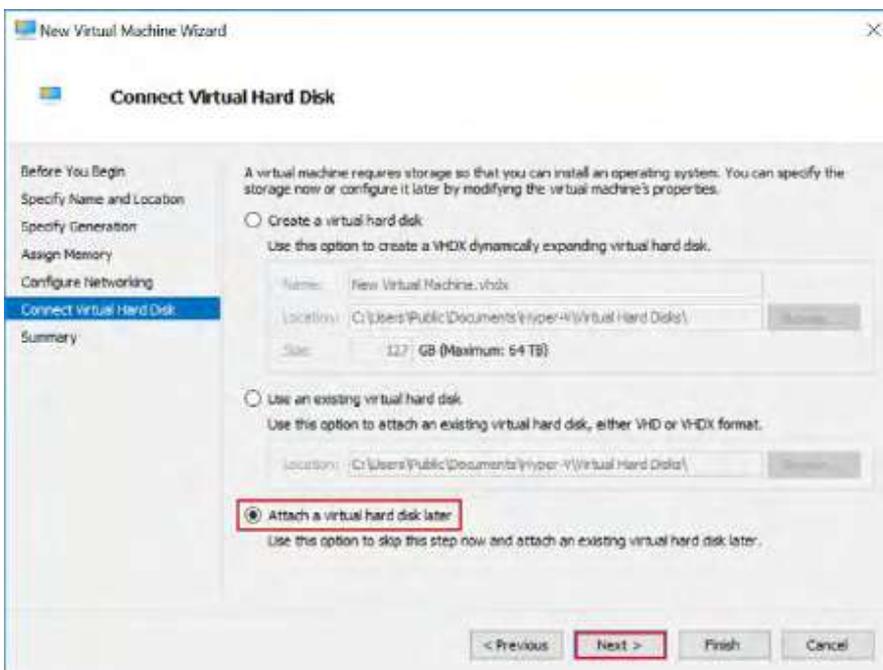


Here, “4096MB”, the same memory size as the backup source virtual machine, is assigned in **[Startup memory]**.

7. Click [Next] to display **[Configure Networking]** window.

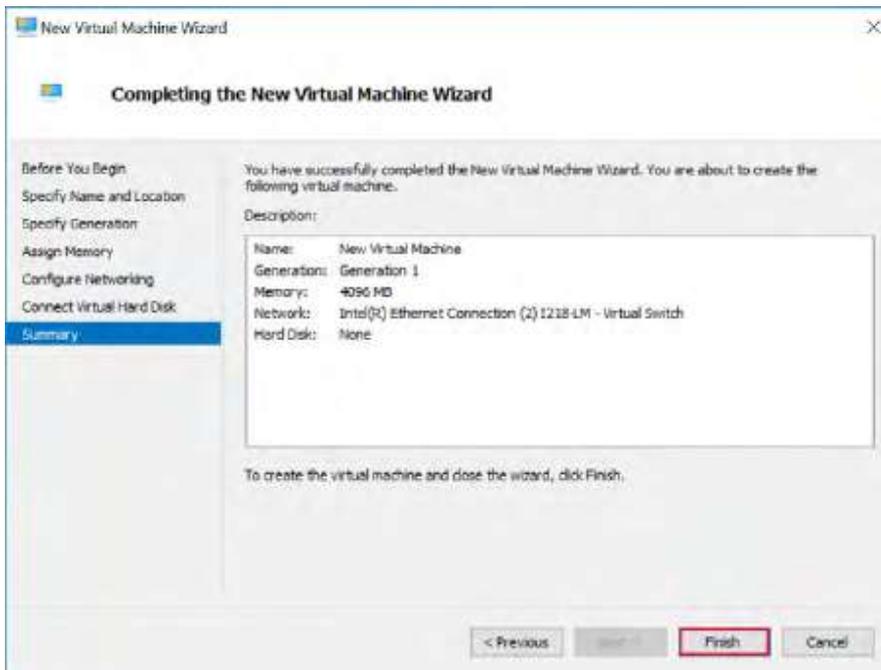


8. Here, “Intel(R) Ethernet Connection (2) I218-LM - Virtual Switch”, the same virtual switch as for the backup source virtual machine, is selected. Click **[Next]** to display **[Connect Virtual Hard Disk]**.



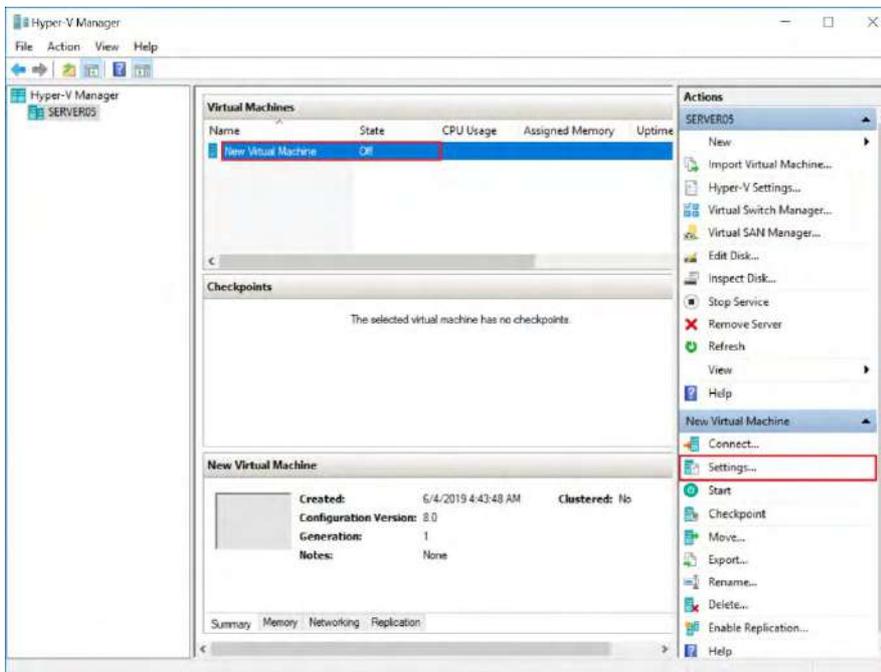
In this example, [Attach a virtual hard disk later] is selected to skip selection of a virtual disk. Please be aware you are taking different operating procedures from the regular routine.

- Click [Next] to display [Completing the New Virtual Machine Wizard].



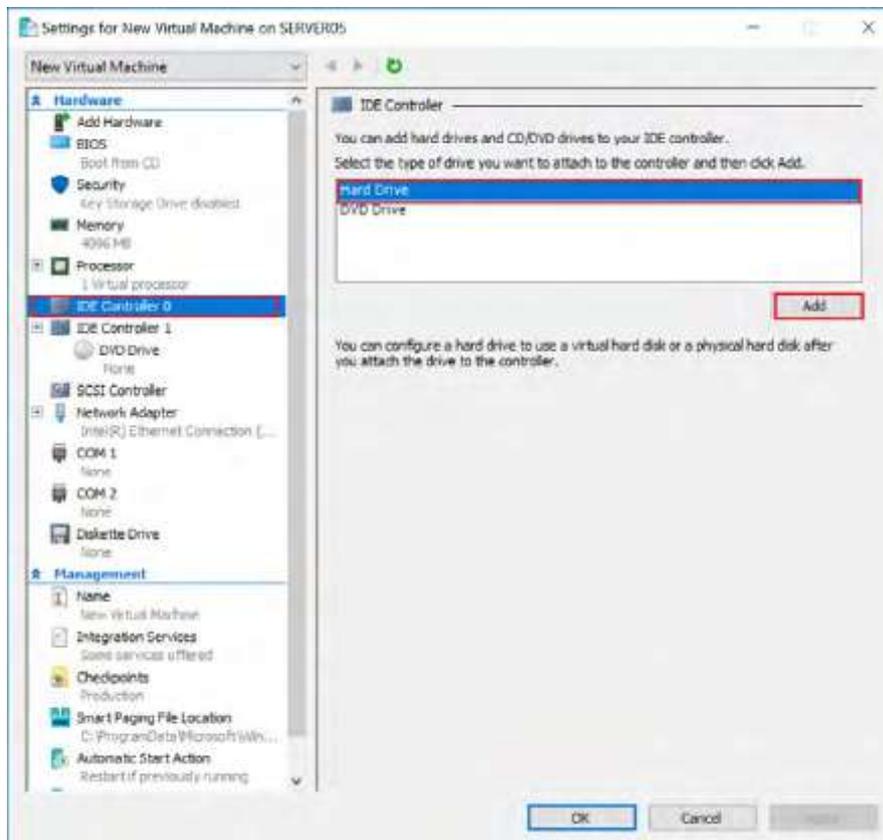
Please review the configured settings and click **[Finish]** to create a new virtual machine.

- Configure the settings for the new virtual machine.

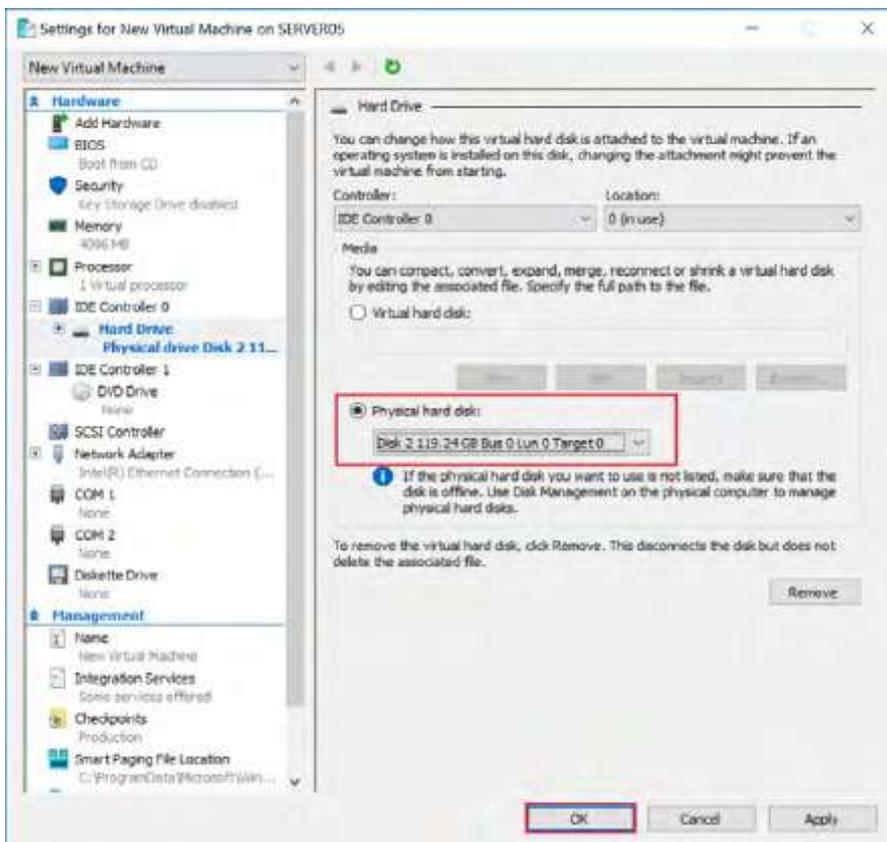


11. Select **[IDE Controller 0]** in [Hardware].

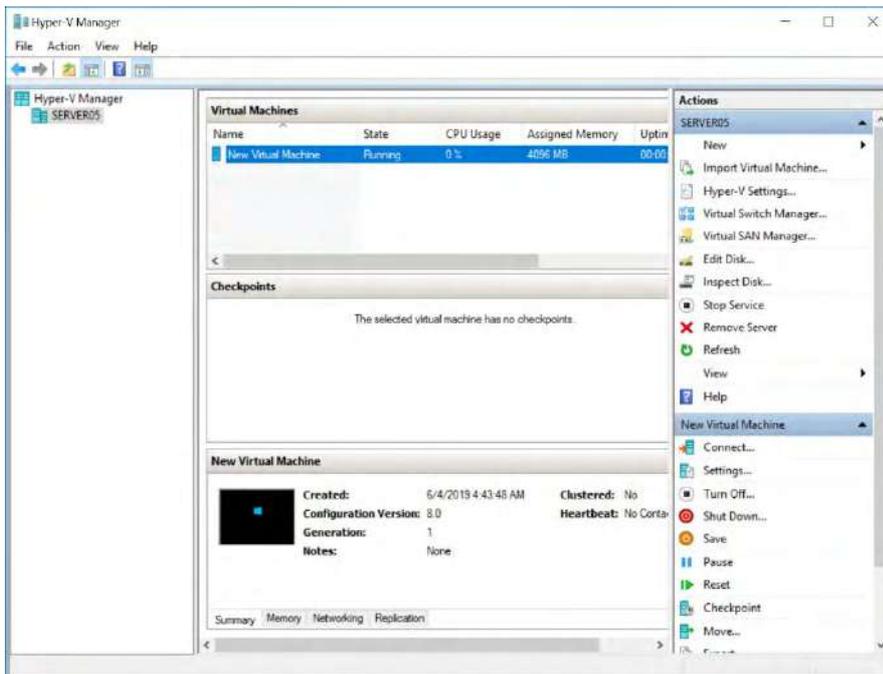
Select **[Hard Drive]** for [IDE Controller] and click **[Add]**.



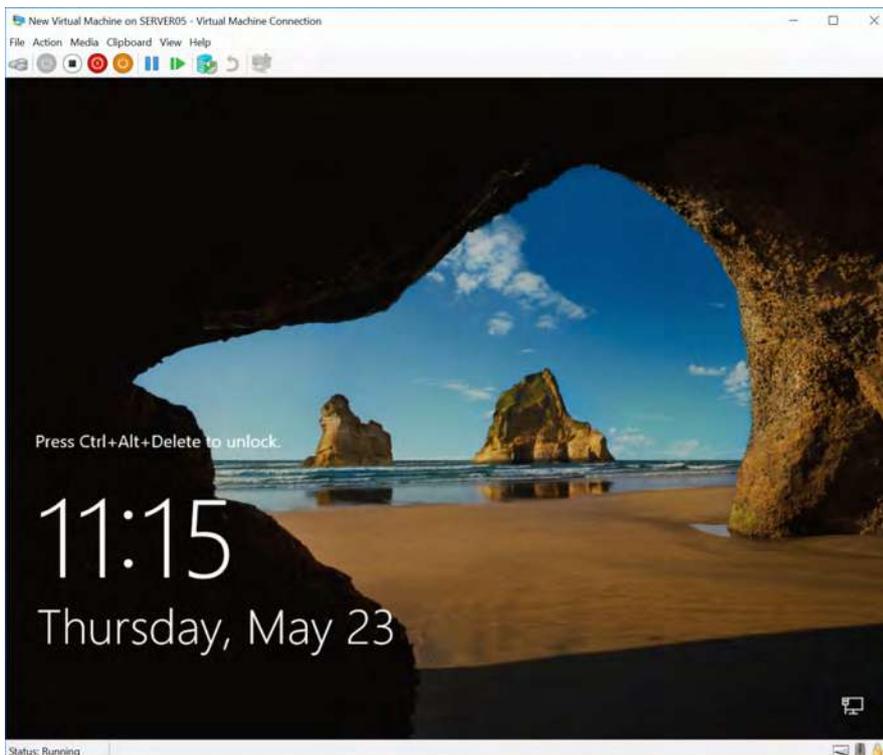
12. In **[Hard Drive]** section, select **[Physical hard disk]** and “Disk 1 20.00GB Bus 0 Lun 0 Target 0” by default. If no other iSCSI target is listed, this is the only option you are allowed to select. Click **[OK]**.



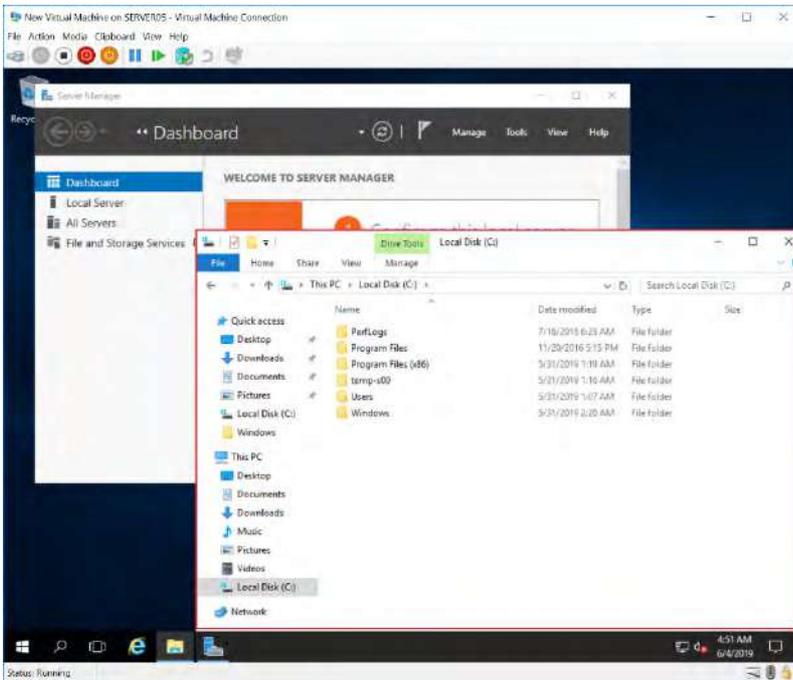
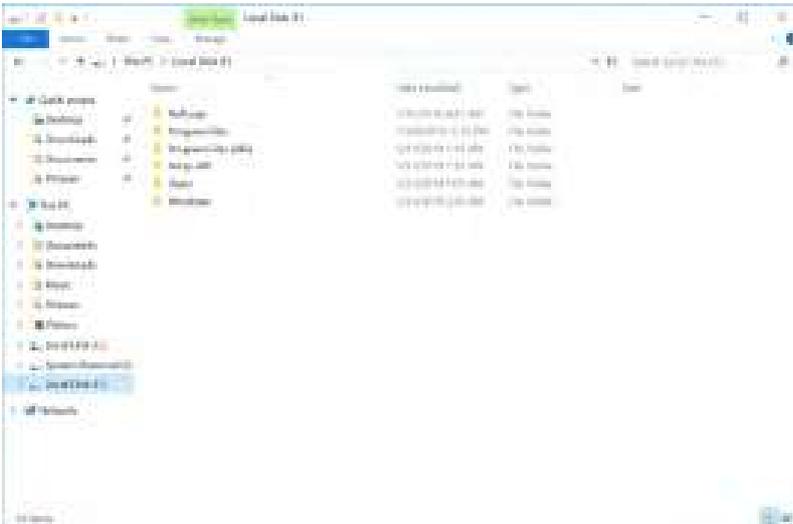
13. Run the new virtual machine in the following window.



14. When the virtual machine is connected to the server system, the following window is displayed.



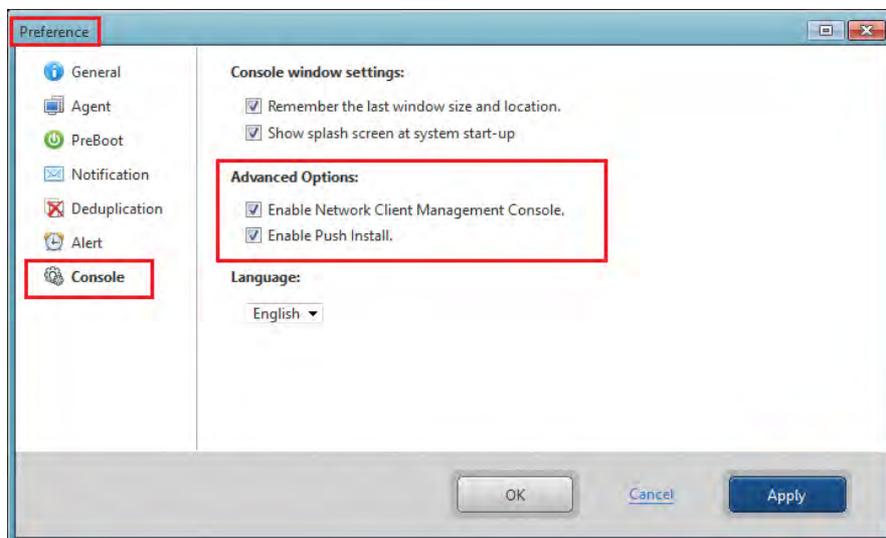
15. Please make sure that the folder structure is configured the same as previous Explorer screen.



16. The use of this feature enables you to attach a backup image of the failed virtual machine to another virtual machine as a virtual disk and immediately recover the failed virtual machine. Though this document has not provided a detailed description, the use of VMware vMotion streamlines the backup / recovery process by seamlessly migrating live virtual machines booted from the iSCSI target to a hypervisor in a production environment.

10. Manage Remote Host

This topic describes Push Install and Network Client Management Console. These features are enabled by selecting [Console] in [Preferences] menu.



10-1. Push Install

Note) The Push Install function is invalid on ActiveImage Protector for Hyper-V Enterprise

Please select **[Enable Push Install]** option in **[Advanced Options]** in the above **[Preference]** Window.

1. Start ActiveImage Protector.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

Windows 7 or earlier Desktop OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

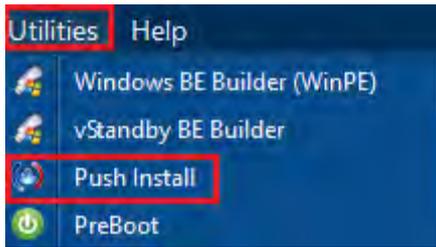
Windows Server 2012 or later server OS:

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

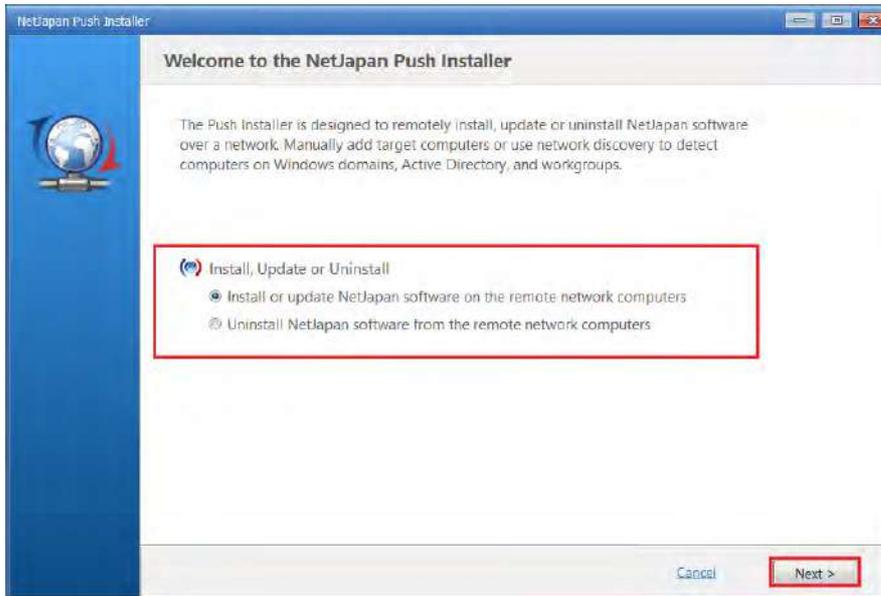
Windows Server 8 or later Desktop OS :

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

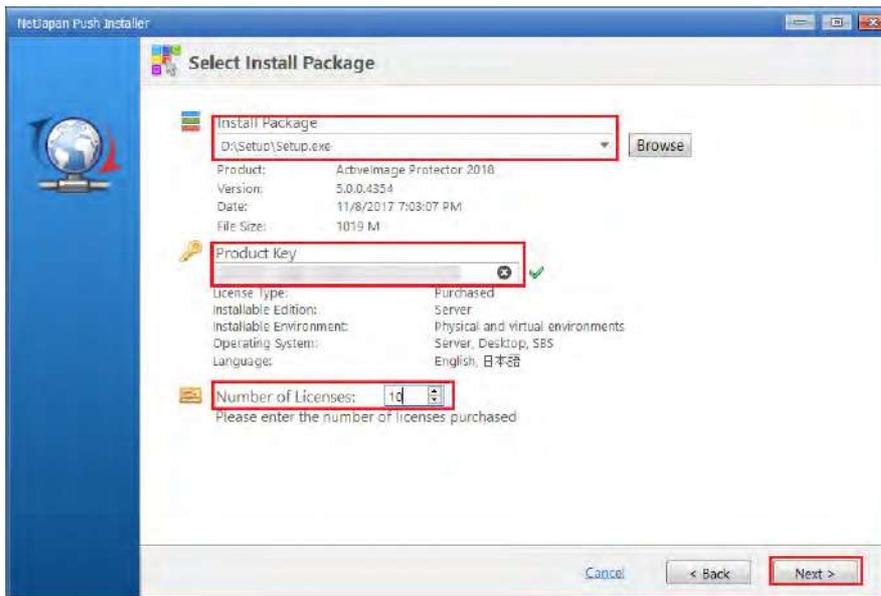
2. Select [Push Install] in [Utilities] menu.



3. To install ActiveImage Protector, select [Install or upgrade NetJapan software on the remote network computers] and click [Next].



4. Select [Install Package]. Enter [Product Key] and [Number of Licenses] and click [Next].



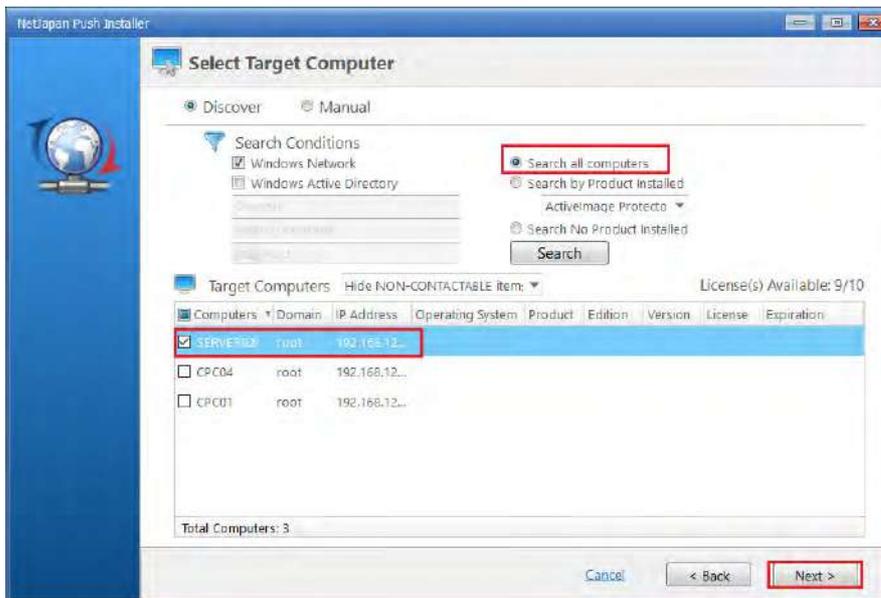
5. Please specify the host to install the product.

You can search for the host name from the networked hosts or directly enter the host name.

You can specify the criteria and filtering conditions to search for a specific networked host.

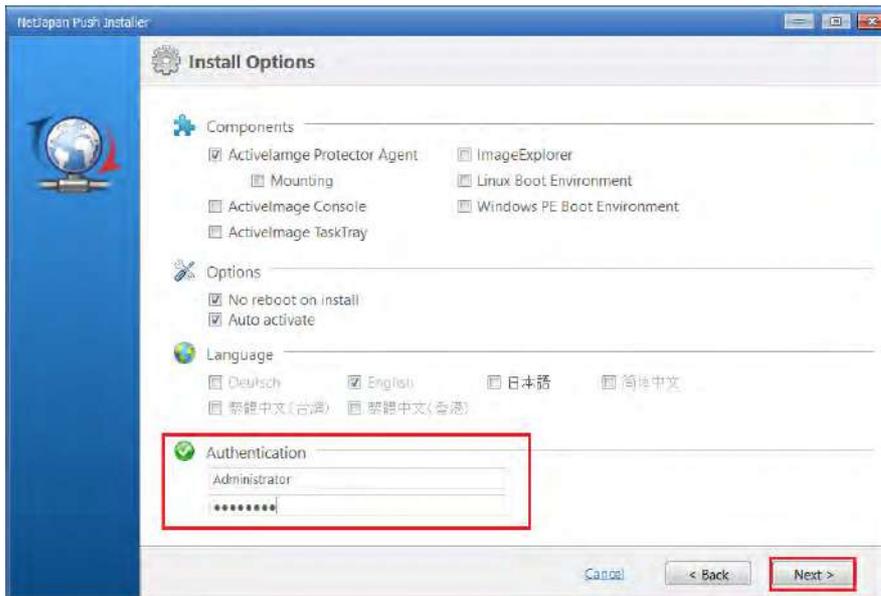
- **Windows network** : A search for host computers on the same network is performed.
- **Windows Active Directory** : A list of host computers in the specified Active Directory is obtained.
- **Search all computers** : All hosts are searched.
- **Search by Product Installed** : The hosts on which ActiveImage Protector is installed are listed.
- **Search No Product Installed** : The hosts on which ActiveImage Protector is not installed are listed

This example shows that [Search all computers] option is selected. Check the checkbox for “SERVER02” in the host list on which ActiveImage Protector is not installed, and click [Next].

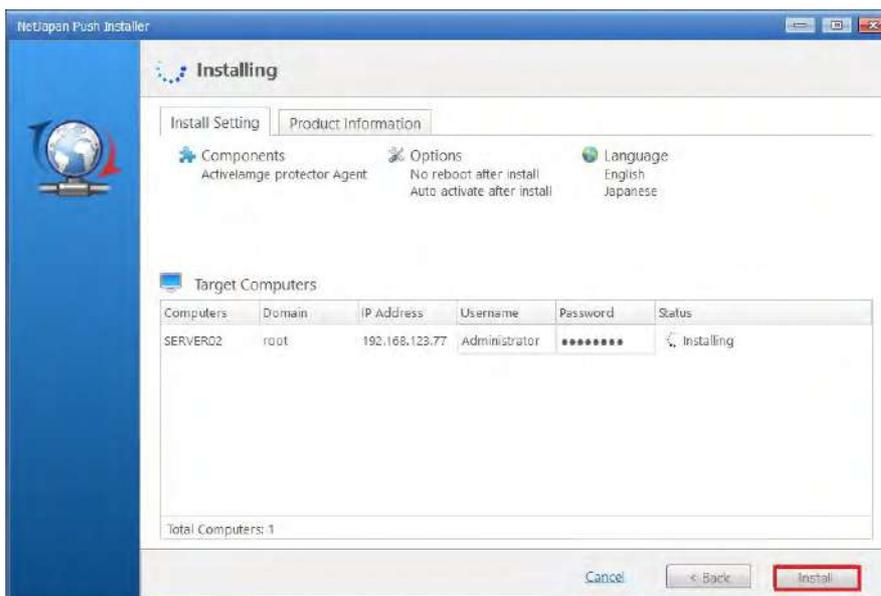


6. You can configure the installation option settings. Please select the components to install in **[Component]** option. **[Options]** provides the options for post-installation behavior (reboot / activate).
- **Do not reboot the system** : Select this option not to reboot the system upon completion of the product installation. Your computer must be restarted to complete the installation and start operation of the ActiveImage Protector agent even when this option is enabled.
 - **Automatically activate** : Upon completion of the product installation you can predefine whether the product is automatically activated.

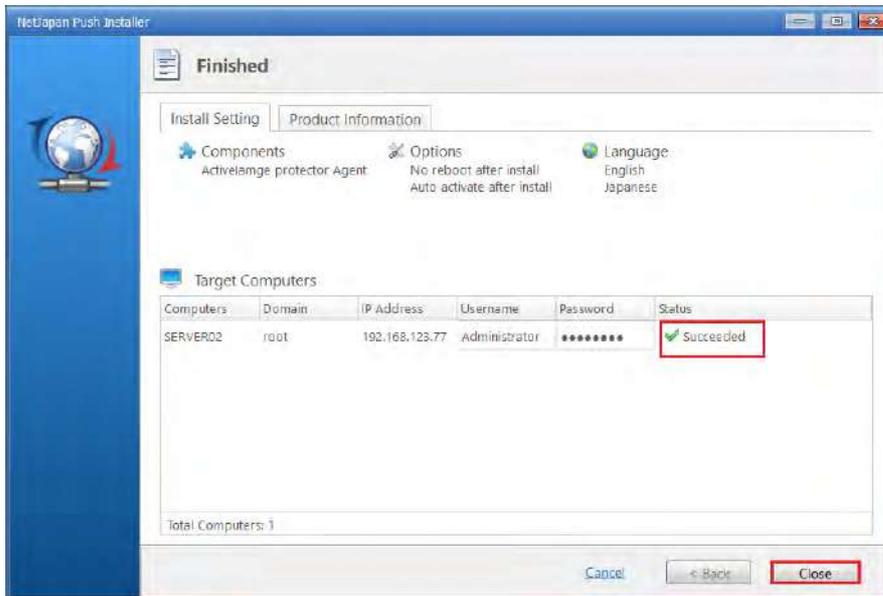
Enter credentials and click **[Next]**.



7. Review the settings and click **[Install]**. Installation of Activelange Protector starts.



8. Upon completion of installation, **[Succeeded]** is indicated for **[Status]** in the following window. Click **[Close]** to end Push Install.



10-2. Network client management console

You can monitor the status and manage ActiveImage Protector installed on a networked remote host.

1. Start ActiveImage Protector.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

Windows 7 or earlier Desktop OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

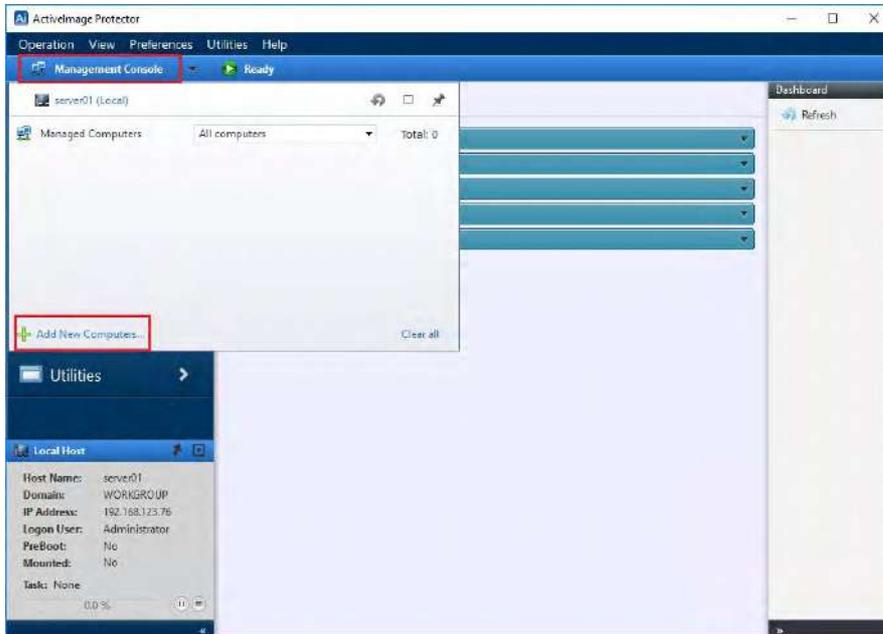
Windows Server 2012 or later server OS:

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

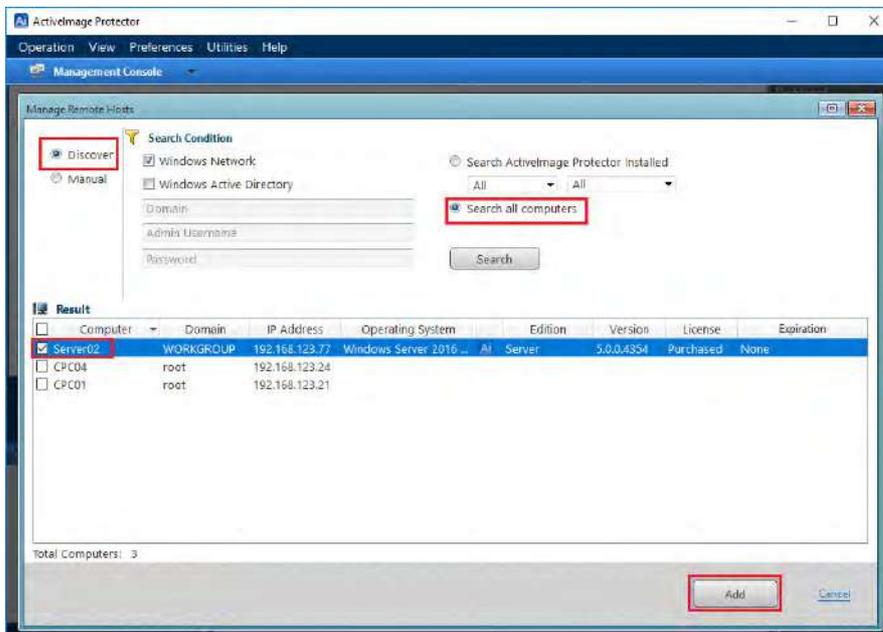
Windows Server 8 or later Desktop OS :

Click **[Start] – [Applications] – [NetJapan] – [ActiveImage Protector]**.

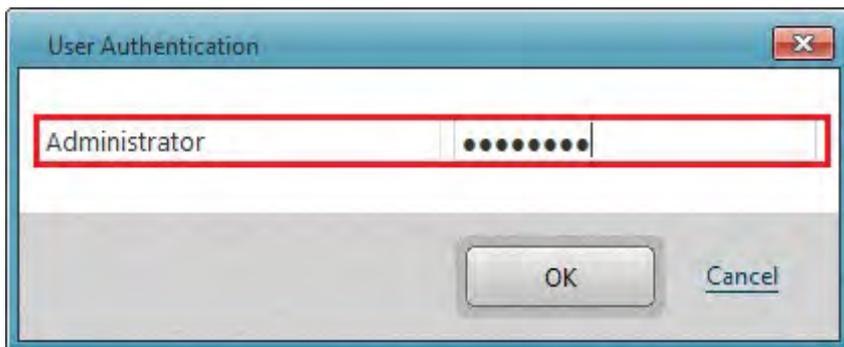
2. Before you start using Remote Control feature, you need to display a list of remote hosts in **[Management Console]** window. Click **[Add New Computers]**.



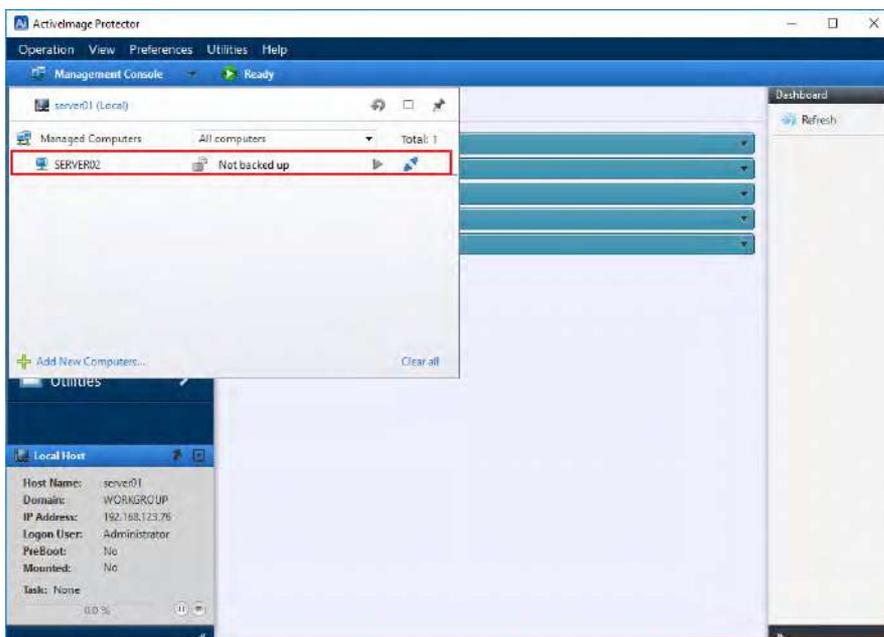
3. Specify the host to add to the list. You can add a new computer by selecting **[Discover]** or **[Manual]**. This example show that **[Discover]** and **[Search all computers]** option are selected. Check the checkbox for "Server02" in the host list and click **[Add]**.



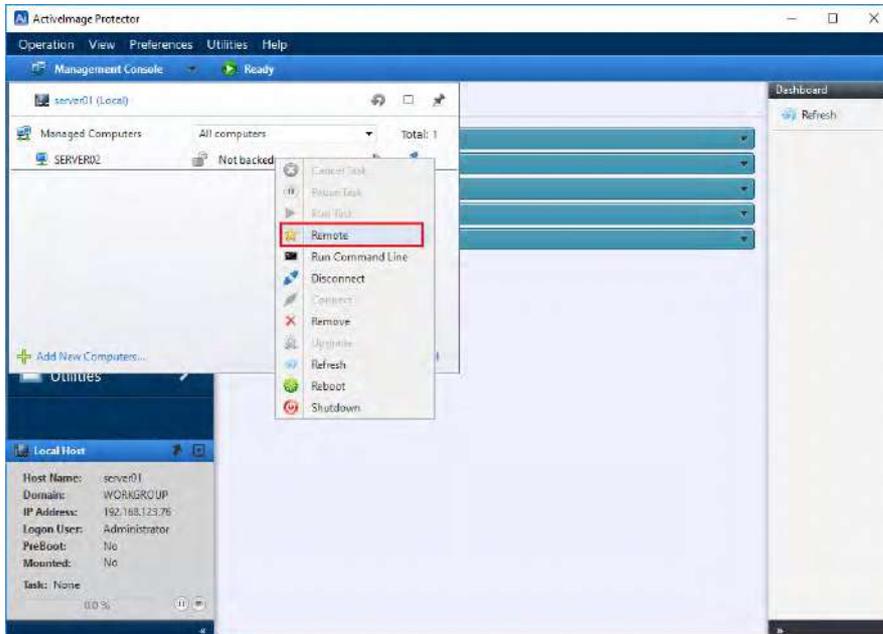
4. Enter the credentials to access the host.



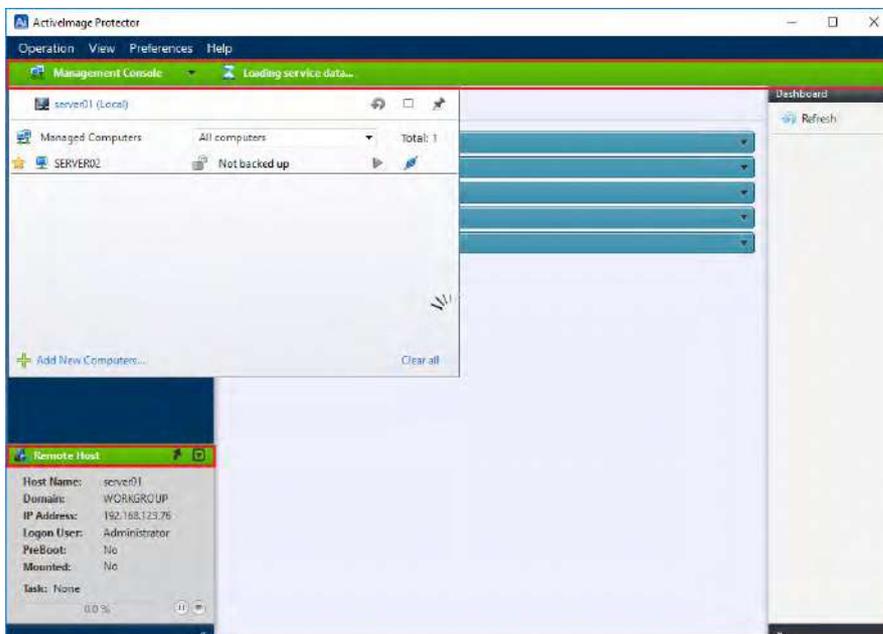
5. "Server02" is added to the Managed Computers list.



6. Select a host from the list and double-click or right-click on the host. Select [Remote] from the context menu to directly connect to agent installed on remote host from the console.



7. When connection is successfully established, the status bar is green-colored. Now one-click offers execution of scheduling backup tasks on remote network hosts and monitoring log information.



8. Double-click on the local host name to disconnect from the remote host.

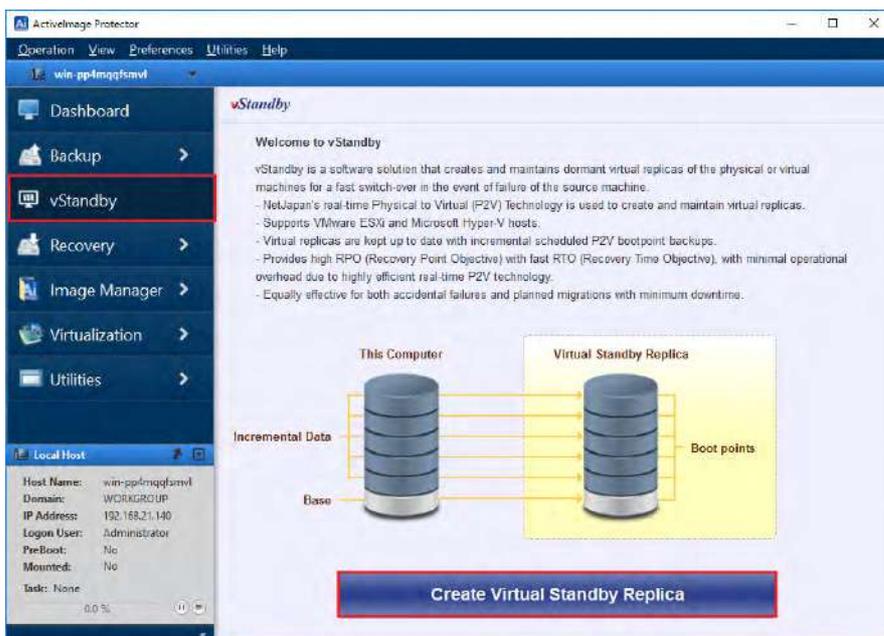
11. vStandby

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 virtual replica is kept current by taking scheduled incremental P2V boot points of the source machine. This ensures a successful start-up of the standby virtual machine created at the point in time before the system failure. vStandby is equally valuable as a tool for migrating legacy physical machines to an ESXi or Hyper-V host in real-time. Minimal downtime is expected as NetJapan's P2V technology is utilized for the migration of the legacy machines.

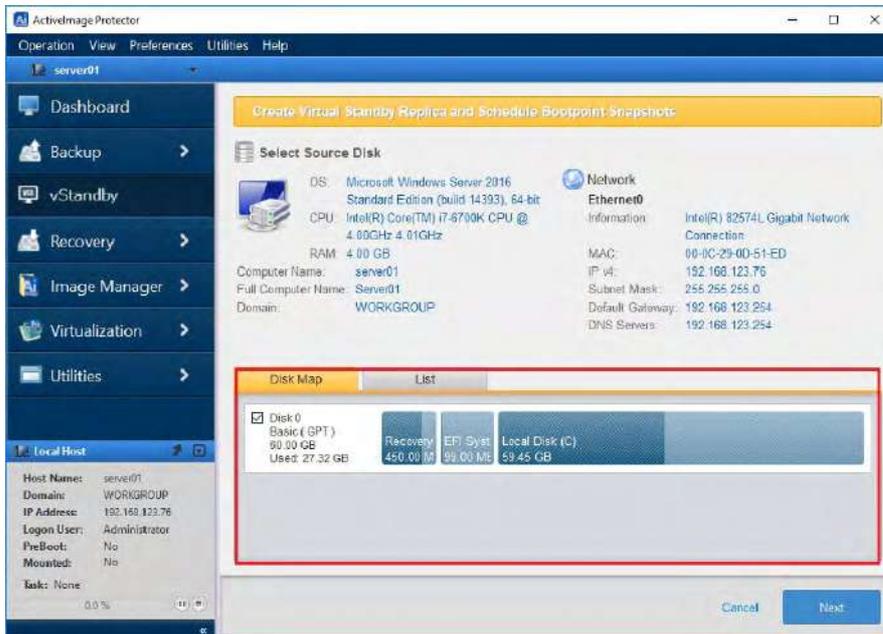
Note) The vStandby function is invalid on ActiveImage Protector for Hyper-V Enterprise.

For detailed system requirements, please refer to NetJapan web site.

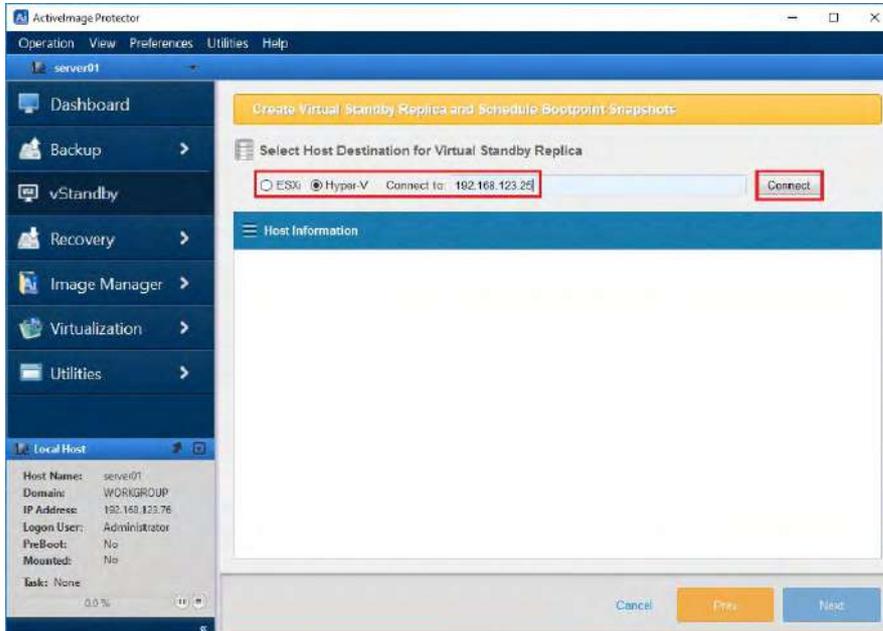
1. To start creating a virtual standby replica, click **[vStandby]** from the left menu. **[Welcome to vStandby]** window is displayed. Click **[Create Virtual Standby Replica]**.



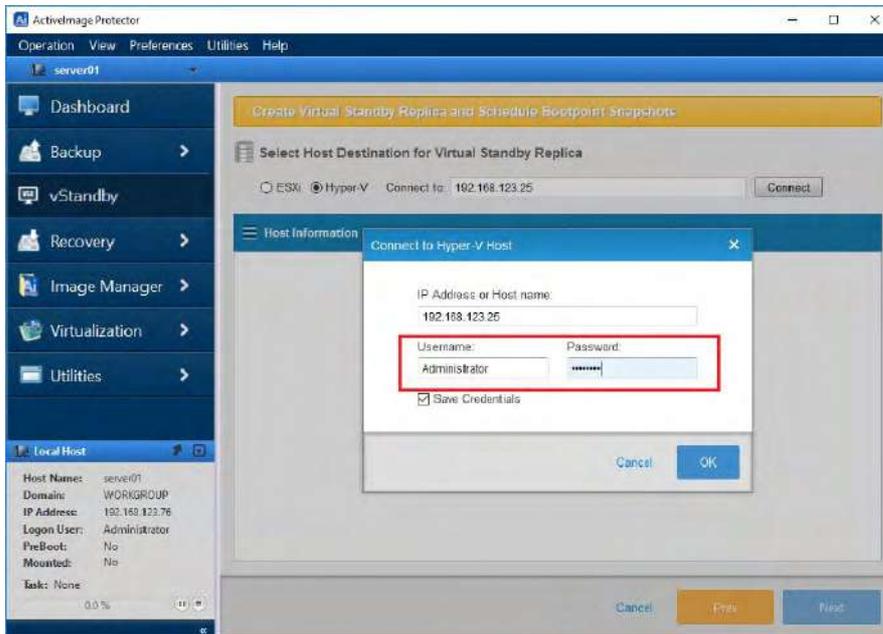
2. Select the source disk to create the standby virtual machine by checking the checkbox for the source disk in the disk map or the list. Click **[Next]**.



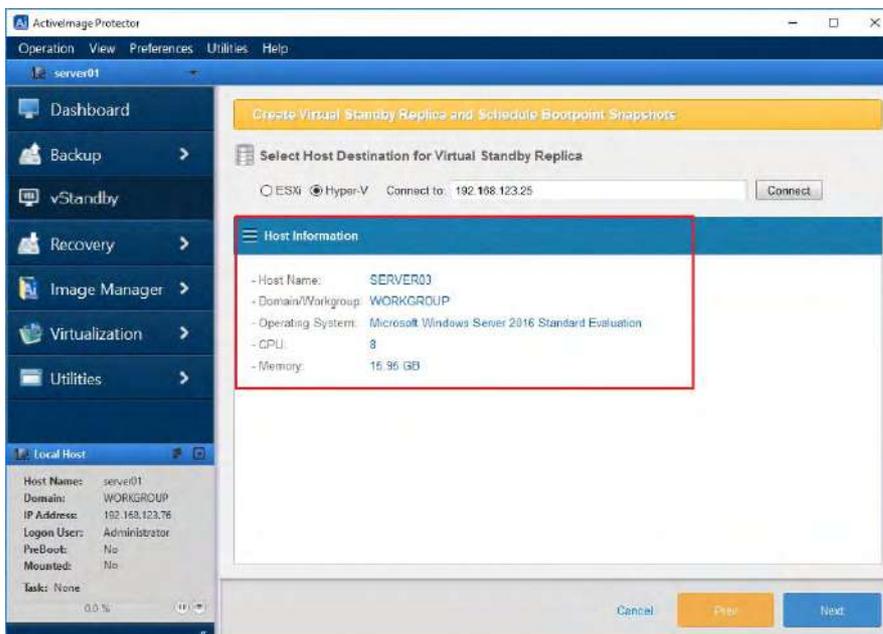
3. Select ESXi or Hyper-V for the target host to create virtual standby replica. This example shows that [Hyper-V] is selected. Enter "192.168.123.25" and click [Connect].



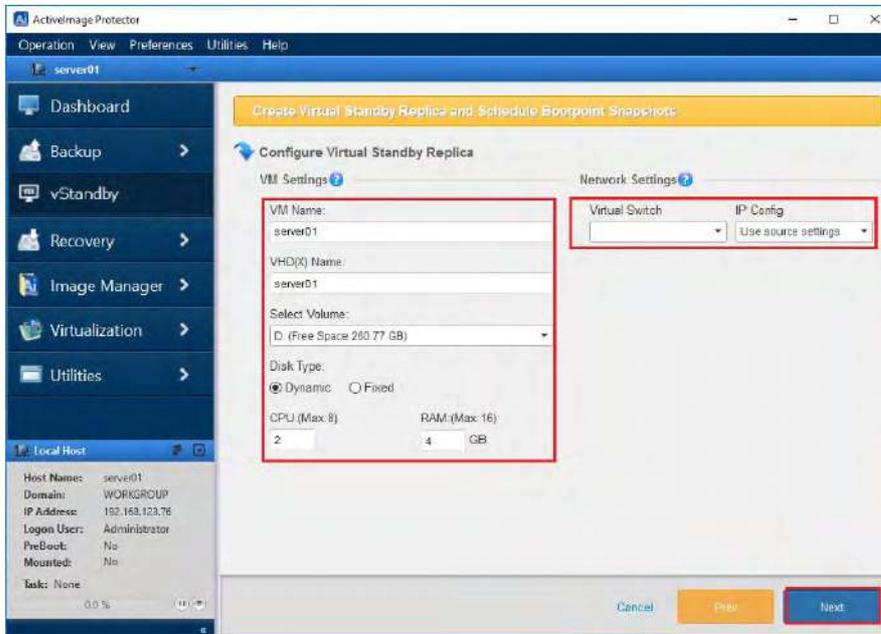
4. Enter credentials to log in Hyper-V host. Enter “Administrator” for [User Name] and the predefined password for [Password].



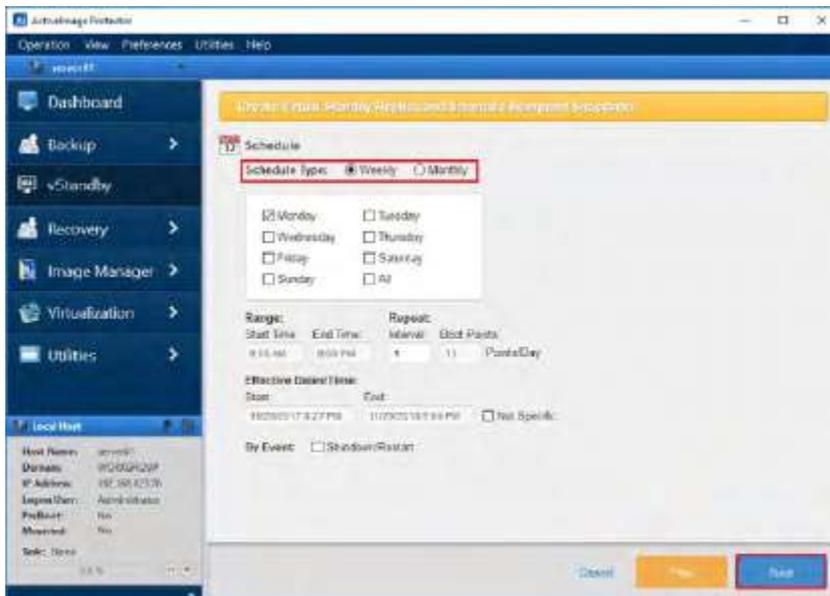
5. Hyper-V Host Information is displayed. Click [Next].



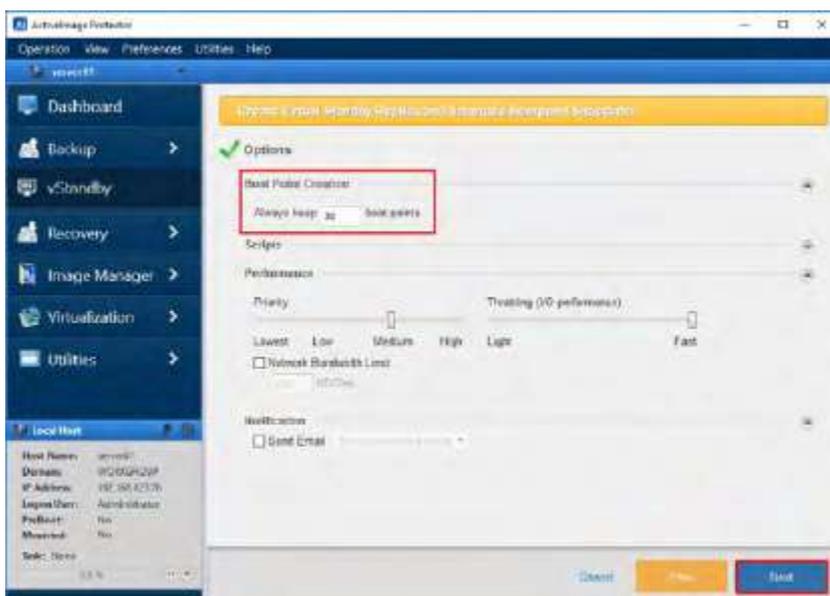
6. **[Configure Virtual Standby Replica]** window is displayed. Please configure the virtual standby replica settings. In **[VM Settings]** please enter **[VM Name]**, **[VHD(X) Name]**, **[Select Volume]**, **[Disk Type]**. In Network Settings please enter **[Virtual Switch]**, **[IP Config]**. Click **[Next]**. **[Virtual Switch]** is configured on host machine and **[IP Address]** configured on source machine.



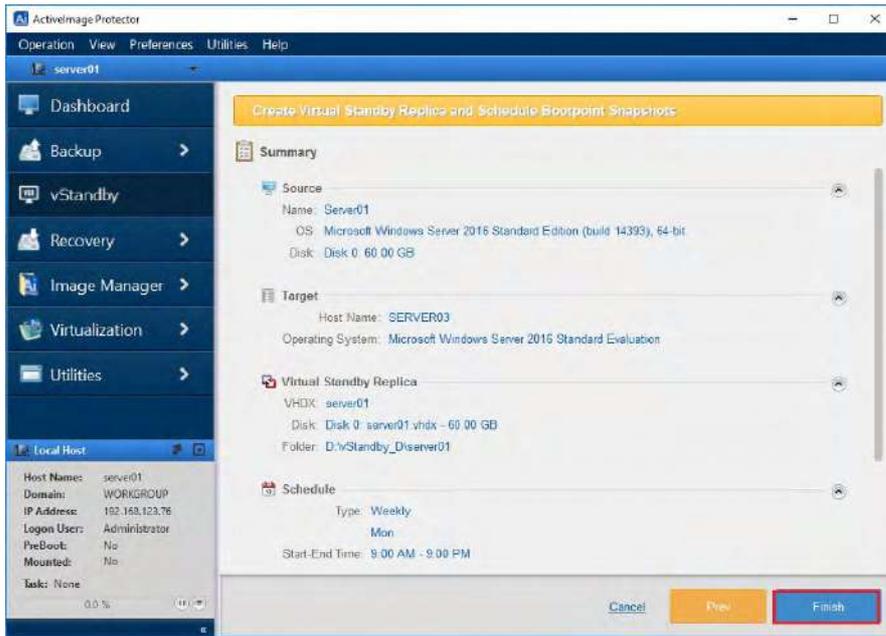
- You can configure weekly or monthly intervals for creating incremental boot points of the standby virtual machine. The following example shows Weekly schedule setting window. Click **[Next]**.



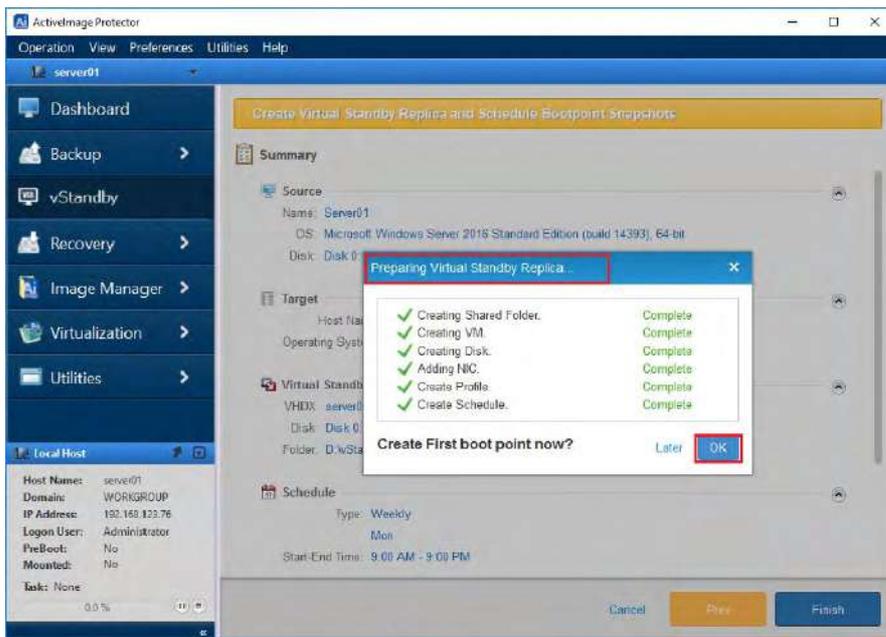
- Please configure the option settings. You can configure the maximum limit (up to 30) for the number of boot points to create for a virtual standby replica. When the number of the boot points reaches the predefined limit, the most and the second obsolete boot points are merged. Set the priority for the vStandby Windows process. Adjusting the priority setting can allocate more or less CPU time for the vStandby processes. This is all dependent on the number of other mission critical applications running on the protected machine. Click **[Next]**.



9. **[Summary]** window is displayed. Review the settings and click **[Finish]**.



10. vStandby task is created. If you want to run the task immediately, click **[OK]**.



11. Dashboard monitors scheduled recurring tasks.

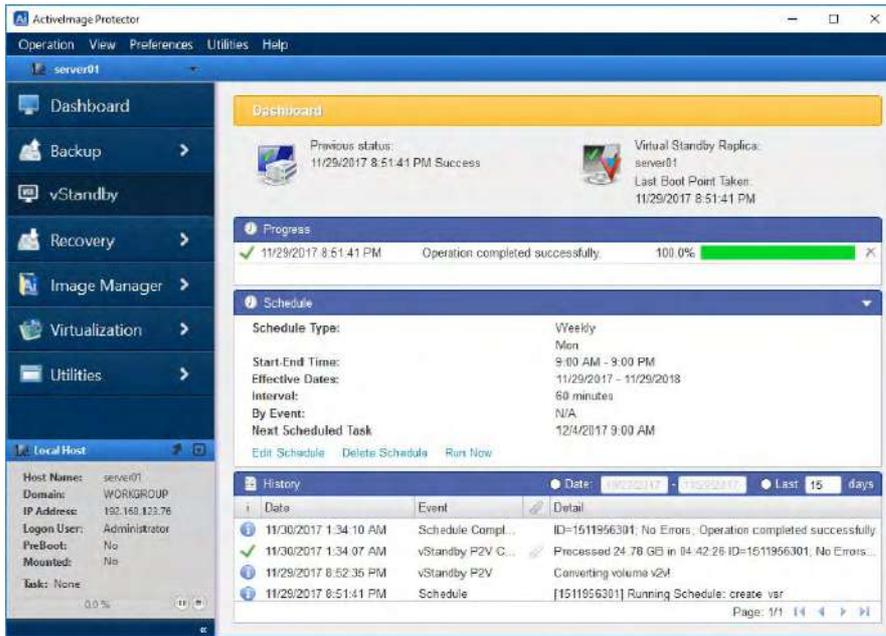
The screenshot displays the ActiVimage Protector software interface. The main window is titled "server01" and features a navigation sidebar on the left with options: Dashboard, Backup, vStandby, Recovery, Image Manager, Virtualization, and Utilities. The main content area is divided into several sections:

- Dashboard:** Shows "Previous status: 11/29/2017 8:29:38 PM Success" and "Virtual Standby Replica: server01" with "Last Boot Point Taken: 11/29/2017 8:29:38 PM".
- Progress:** A progress bar indicates "Converting volume 3 to virtual image" at 20.3% completion, starting at 11/29/2017 8:51:41 PM.
- Schedule:** A red-bordered box highlights the following details:
 - Schedule Type:** Weekly, Mon
 - Start-End Time:** 9:00 AM - 9:00 PM
 - Effective Dates:** 11/29/2017 - 11/29/2018
 - Interval:** 60 minutes
 - By Event:** N/A
 - Next Scheduled Task:** 12/4/2017 9:00 AM
- History:** A table showing recent events:

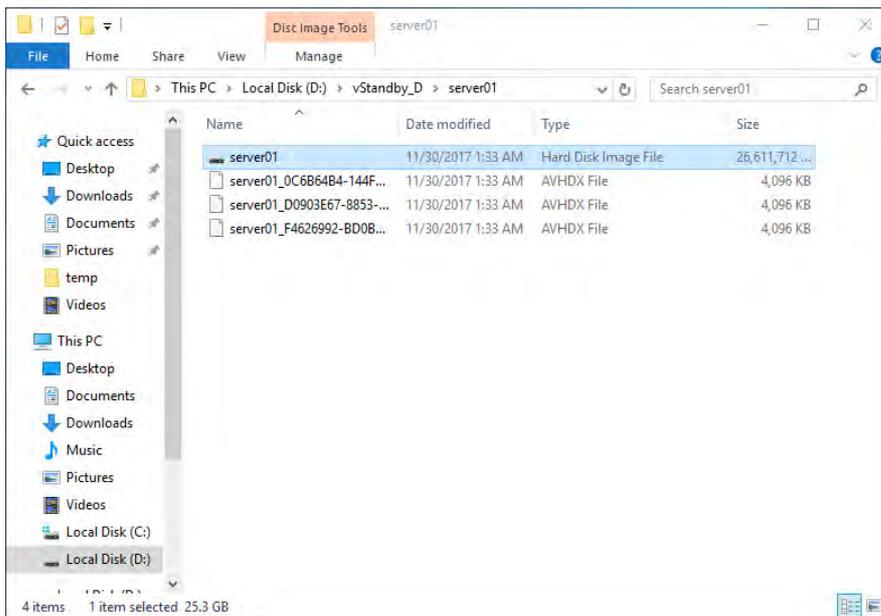
Date	Event	Detail
11/29/2017 8:52:35 PM	vStandby P2V	Converting volume: v2yl
11/29/2017 8:51:41 PM	Schedule	[1611966301] Running Schedule: create_vsr
11/29/2017 8:48:48 PM	Schedule Compl...	ID=1511964978: No Errors, Operation completed successfully.
11/29/2017 8:48:46 PM	vStandby P2V C...	Processed 2.03 GB in 00:19:07 ID=1511954978: 1 Errors, T...

At the bottom left, system information for "Local Host" is shown, including Host Name (server01), Domain (WORKGROUP), IP Address (192.168.123.76), Logon User (Administrator), PreBoot (No), and Mounted (No). A task named "create_vsr" is shown with a progress bar at 20.3%.

12. When a virtual standby replica is created, the following window is displayed.



13. On Hyper-V host, you can monitor the virtual standby replica as follows.



12. ImageBoot

ImageBoot immediately starts a virtual machine from any ActiveImage Protector backup image file. ImageBoot is developed based on NetJapan's virtual conversion technology but bypasses lengthy physical to virtual conversion and recovery process. As is often the case, it takes about a couple of hours to restore a 1TB backup image file. The use of ImageBoot enables you to boot a backup image file as a virtual machine in as little as two minutes.

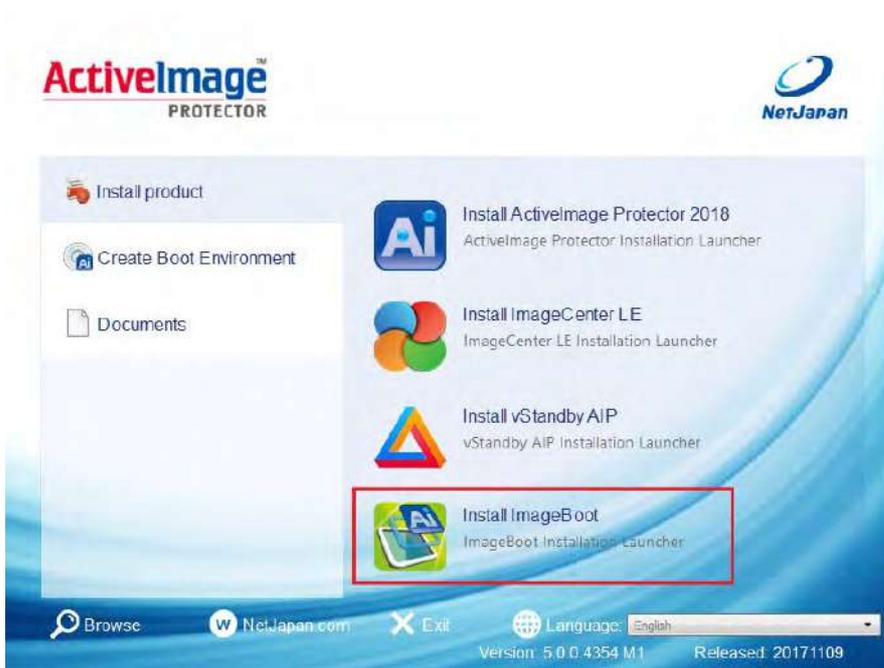
Microsoft Hyper-V, VMware Workstation/Player are supported for hypervisor.

Note) When you wish to use ImageBoot, please visit our website and download it at free of charge.

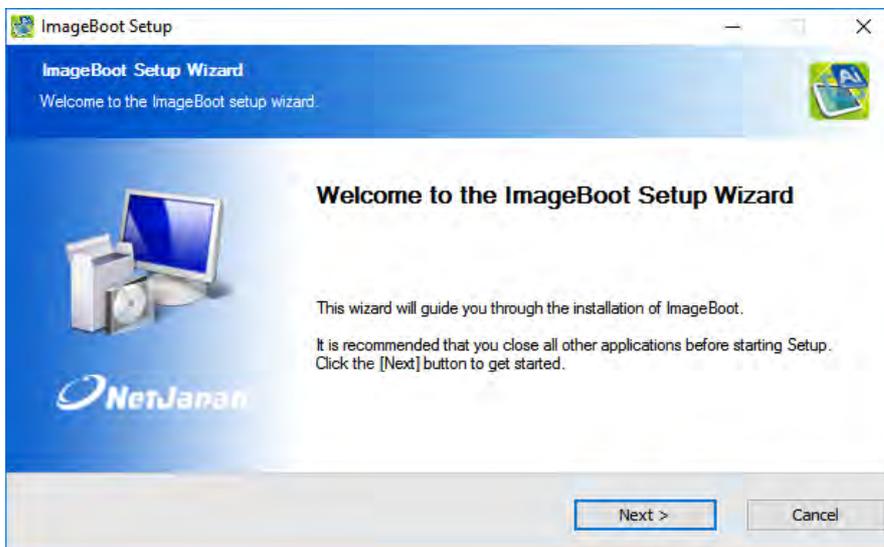
The following are the examples for practical use of ImageBoot.

- Common disaster recovery approaches include backup image boot test to provide confidence that your backup images are bootable. However, it's time consuming and cumbersome process. The use of ImageBoot lets you bypass the lengthy test process.
- The use of incremental backup images enables to locate the point of a system failure. However, you need to check the entire incremental backup files to identify the cause of the problem. Combined with the recovery process, it takes quite long. The use of ActiveImage Protector's regularly scheduled backups and ImageBoot help you identify the point of failure bypassing recovery process.
- ImageBoot facilitates verification of P2V migration. ImageBoot provides confidence in P2V migration by using a backup image file.
- vStandby, as stated above, also provides immediate start-up of the standby virtual machine. The difference between the two products is that ImageBoot immediately starts a ActiveImage Protector backup image file. Without the need for making changes to the backup image files, a backup image file of the source machine can be booted. ImageBoot lets you perform testing upgraded version of an application or updated services.

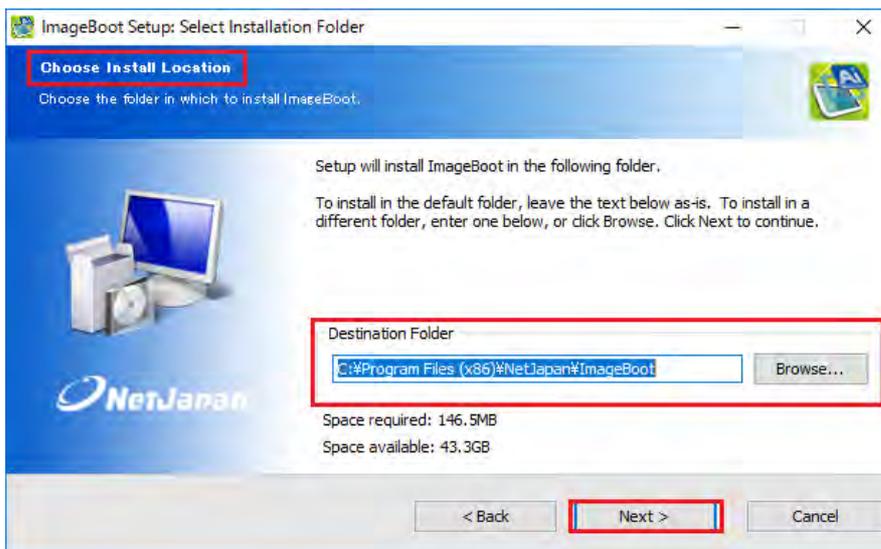
1. ImageBoot has to be installed from the product media or the setup file downloaded from NetJapan's Web Site. When you use the launcher, please select **[Install ImageBoot]**.

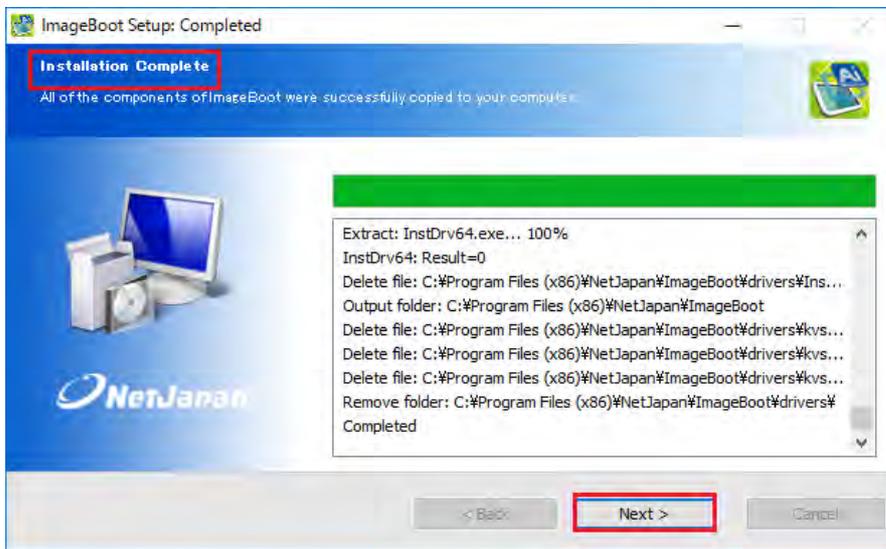
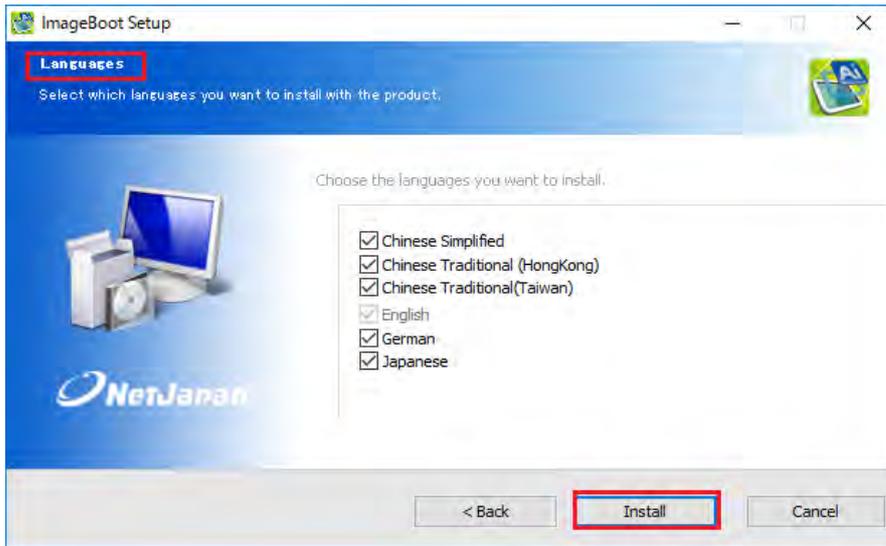


Setup Wizard is launched as follows.

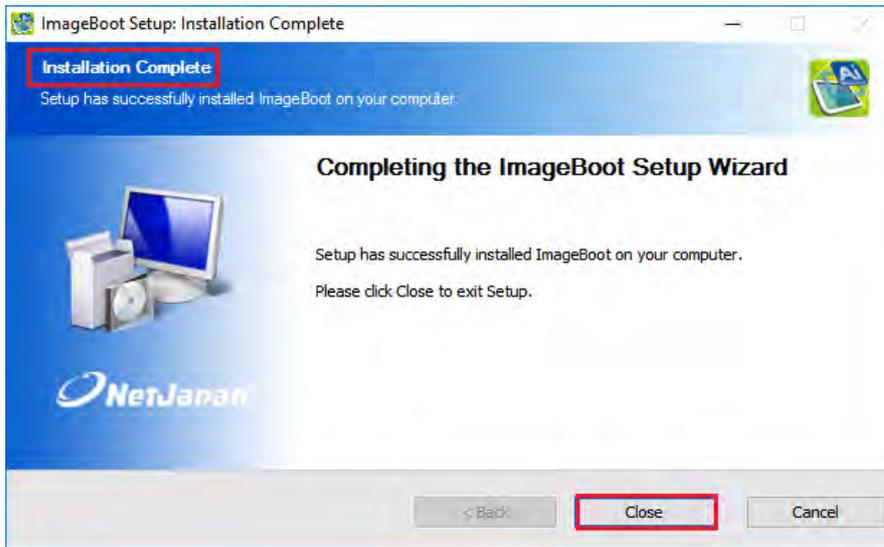


2. Please carefully review the End User's License Agreement. Specify the installation folder and the preferred language to install the package (you may not need to change the default settings.)





3. The installation completes with the following window of the setup wizard. Click **[Close]** to end the setup wizard.



4. Start ImageBoot.

Windows Server 2008 R2 or earlier server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

Windows 7 or earlier Desktop OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

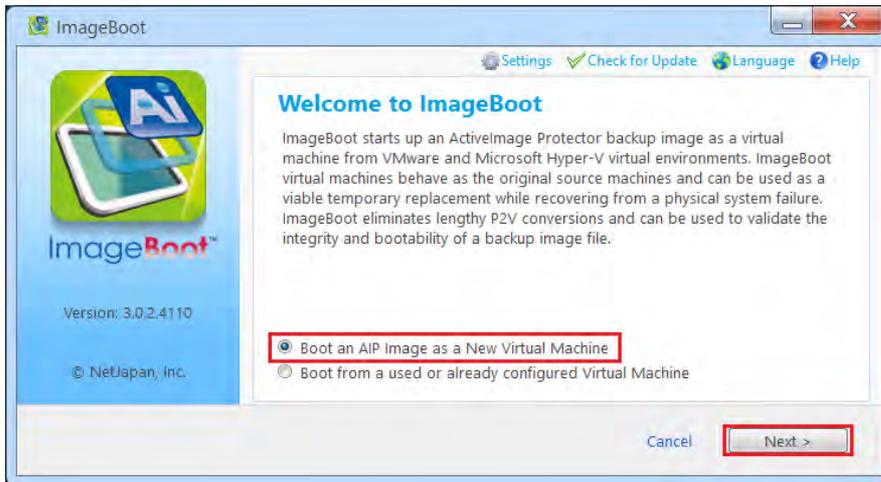
Windows Server 2012 or later server OS:

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

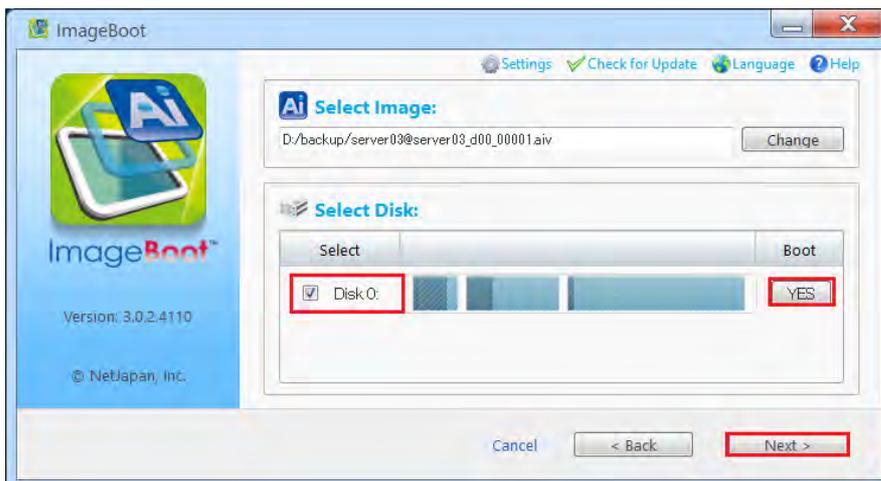
Windows Server 8 or later Desktop OS :

Click **[Start] – [All Programs] – [NetJapan] – [ActiveImage Protector]**.

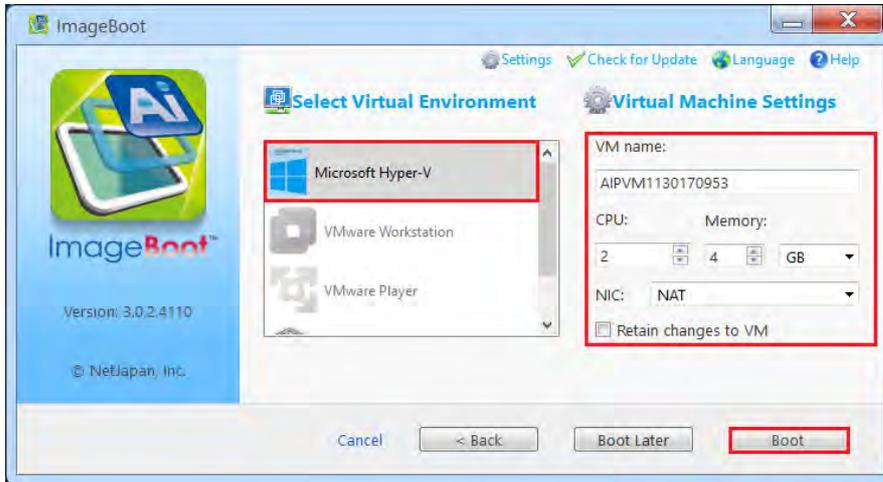
5. ImageBoot starts. This example shows that **[Boot an AIP image as a New Virtual Machine]** is selected. Click **[Next]**.



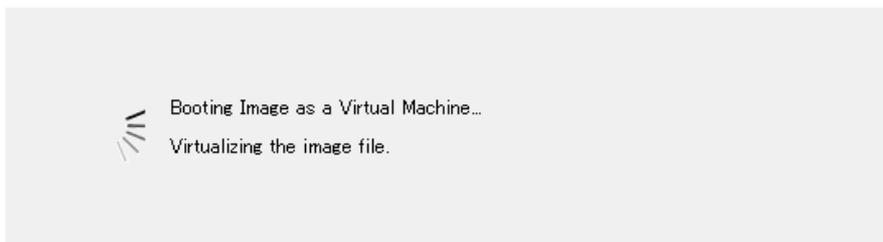
6. Select a backup image file created by using ActiveImage Protector in **[Select Image]**. Check in the checkbox for “Disk 0” in **[Select Disk]**. Please make sure that “Yes” is indicated for **[Boot]**. Click **[Next]**.



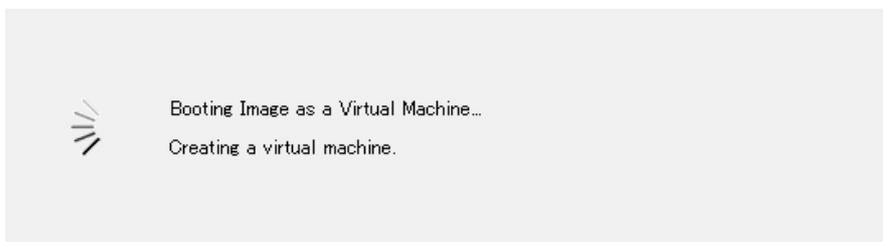
7. Select a hypervisor. This example shows that **[Microsoft Hyper-V]** is selected. Please configure the settings, i.e., **[VM name]**, **[CPU]**, **[Memory]**, **[NIC]**. Click **[Boot]**.



8. P2V process starts.

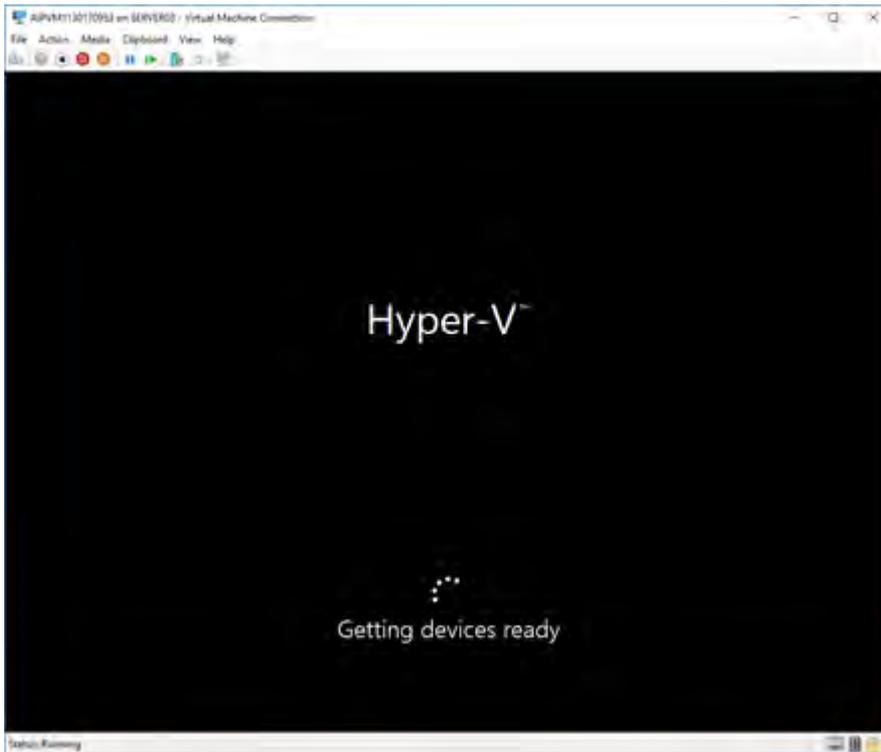


9. Virtual machine, virtual network adapter are created.

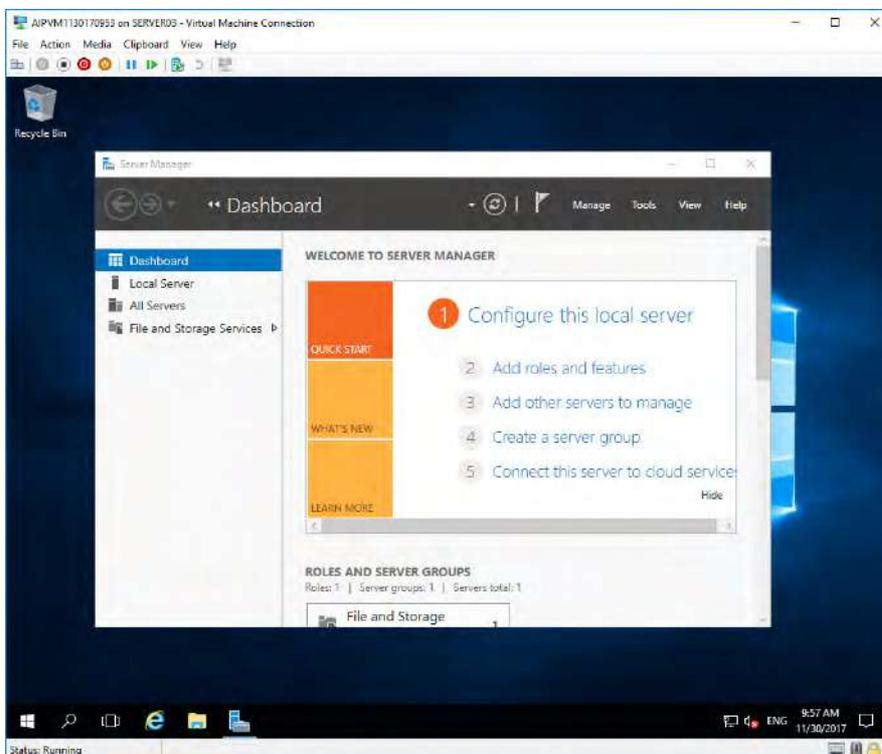


10. Thereafter, Windows system boots up.

When Windows OS boots up, device preparation phase may take place.



11. This example shows that a virtual machine is booted from a backup image file of Windows Server 2016.



APPENDIX

ActiveImage Protector & Support Information

●NetJapan's Web Site

You will find the product information as well as direct links to download documentation, our full installers or update installers, etc:

<https://www.netjapan.eu/en-us/>

●ActiveImage Protector FAQ

You can access the support FAQ.

<https://kb.netjapan.com/>

For your inquiry about ActiveImage Protector, please contact:

NetJapan, Inc. Global Sales Dept.,

E-mail: global-info@netjapan.com

Phone: +81-3-5256-0877

Fax: +81-3-5256-0878

The software and the related documentation are proprietary products of NetJapan, Inc., and are copyrighted to the company.

Copyright©2008-2019 NetJapan, Inc. All rights reserved.

ActiveImage Protector, ActiveImage Protector Server, ActiveImage Protector Desktop, ActiveImage Protector IT Pro, ActiveImage Protector for Hyper-V Enterprise, ReZoom it!, ActiveImage Protector Linux, ActiveImage Protector Virtual, ActiveImage Protector Cluster, ActiveImage Protector Cloud, ActiveImage Protector Basic, ImageBoot, ImageCenter LE, BootCheck, ActiveImage Deploy USB, ActiveVisor, HyperAgent, HyperBack, HyperRestore, and HyperStandby are trademarks of NetJapan, Inc.

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