

# ActiveImage Protector 2022 Cloud Setup Guide

3rd Edition (February, 2024)



# Contents

---

1. Overview.....	3
System Requirements.....	3
2. Installation.....	5
3. Configure backup settings and run backup tasks.....	6
3-1. Volume Backup: One Time Only.....	6
3-2. Volume Backup: Scheduled Backups .....	12
4. Restore .....	21
4-1. File / Folder Recovery .....	21
4-2. In-Cloud Recovery .....	26
4-3. System Recovery (RescueBoot) .....	34
5. In-Cloud Standby.....	45
5-1. Create a snapshot from a backup file .....	45
5-2. Create a volume from a snapshot and attach to newly created instance .....	53
6. Remote Management Console.....	62
7. Reference .....	67

# 1. Overview

---

ActiveImage Protector is a system / data protection solution supporting various system environments, including physical and virtual machines and cloud environments. This set-up guide will show you how to install and configure ActiveImage Protector 2022 Cloud on virtual machines on public cloud (Amazon Web Services (hereinafter “AWS”), Microsoft Azure (hereinafter “Azure”), Google Cloud Platform (hereinafter “Google Cloud”), Oracle Cloud Infrastructure (hereinafter “Oracle Cloud”). We recommend you read this manual before using ActiveImage Protector 2022 Cloud to configure backups. Please visit our online help for more detailed information at the following sites:

- For Windows environment:  
[https://webhelp.actiphys.com/AIP/2022/en\\_US/](https://webhelp.actiphys.com/AIP/2022/en_US/)
- For Linux environment:  
[https://webhelp.actiphys.com/AIP/linux/2022/en\\_US/](https://webhelp.actiphys.com/AIP/linux/2022/en_US/)

## System Requirements

The following are computer system requirements to install ActiveImage Protector 2022 (Version 7.0.3,8919 for Windows, Version 7.0.3.8919 for Linux). Please ensure your computer meets these minimum system requirements before using ActiveImage Protector 2022. For the latest system requirements, please visit our Web site at: (<https://www.actiphys.com/global/support/system-requirements/>)

Windows Virtual Machine	
<b>CPU</b>	Pentium 4 or newer.
<b>Main Memory (RAM)</b>	4GB of RAM or greater. (8GB is recommended.)
<b>Hard Disk</b>	1.5GB of available disk space or greater.
<b>Internet</b>	An internet connection is required to activate the product, issue license file and update the product.
<b>Supported OS</b>	<ul style="list-style-type: none"> <li>• Windows Server 2022</li> <li>• Windows Server 2019</li> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server IoT 2019 / 2022 for Storage</li> <li>• Windows Storage Server 2016</li> <li>• Windows Storage Server 2012 R2</li> </ul>

Linux Virtual Machine	
<b>CPU</b>	Pentium 4 or newer. * Only x86_64 architecture is supported. * Secure Boot is not supported.
<b>Main Memory (RAM)</b>	2GB of RAM or greater.
<b>Hard Disk</b>	2GB of available disk space or greater.
<b>Internet</b>	An Internet connection is required to activate the product.
<b>Supported OS</b>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux : 9.0 – 9.3 / 8.0 – 8.9 / 7.0 – 7.9</li> <li>• CentOS : 8.1 – 8.4 / 7.0 – 7.9</li> <li>• Oracle Linux : 9.0 – 9.3 / 8.1 – 8.9 / 7.0 – 7.9</li> <li>• AlmaLinux 9.0 – 9.3 / 8.3 – 8.9</li> <li>• MIRACLE LINUX 9.0, 9.2 / 8.4, 8.6, 8.8</li> <li>• Rocky Linux 9.0 – 9.3 / 8.3 – 8.9</li> <li>• Amazon Linux 2</li> <li>• SUSE Linux Enterprise Server 15 / Desktop 15</li> <li>• OpenSUSE Leap 15</li> <li>• Ubuntu 18.04LTS / 20.04LTS / 22.04LTS</li> <li>• Debian 9 – 12</li> </ul>

## 2. Installation

---

ActiveImage Protector Cloud is designed to back up Windows / Linux virtual machines on public clouds (AWS, Azure, Google Cloud, Oracle Cloud). For more detailed operating procedures regarding how to install and configure the basic settings, please refer to the following setup guide.

\*When installing ActiveImage Protector on virtual machines in a Cloud environment, please use a “Cloud product key”.

- Windows: ActiveImage Protector 2022 Server Setup Guide

[https://www.actiphy.com/global/setup\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_server](https://www.actiphy.com/global/setup_guide/actiphy_activeimage_protector_2022_server)

- Linux: ActiveImage Protector 2022 Linux Setup Guide

[https://www.actiphy.com/global/setup\\_guide/actiphy\\_activeimage\\_protector\\_2022\\_linux](https://www.actiphy.com/global/setup_guide/actiphy_activeimage_protector_2022_linux)

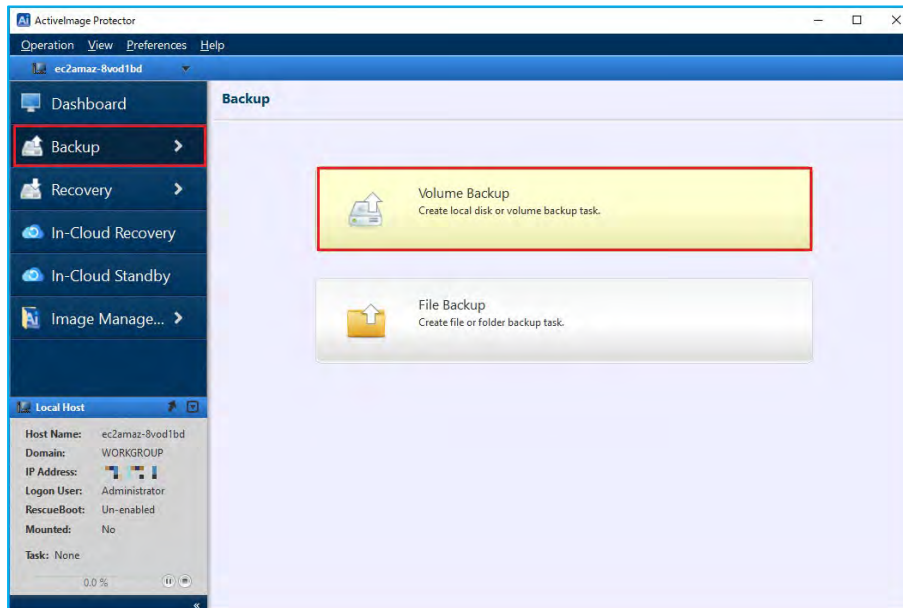
### 3. Configure backup settings and run backup tasks

#### 3-1. Volume Backup: One Time Only

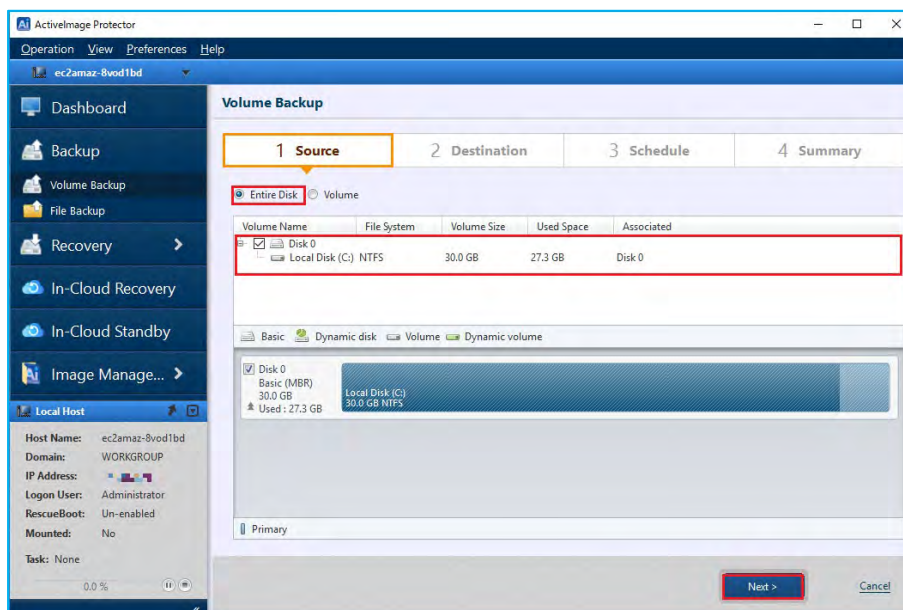
Use the following steps to run ad hoc backup tasks:

1. Launch ActiImage Protector by clicking on the Windows Start menu and then navigating to **[Actipty]** → **[ActiImage Protector]**.

Once inside ActiImage Protector, click on **[Backup]** → **[Volume Backup]**.

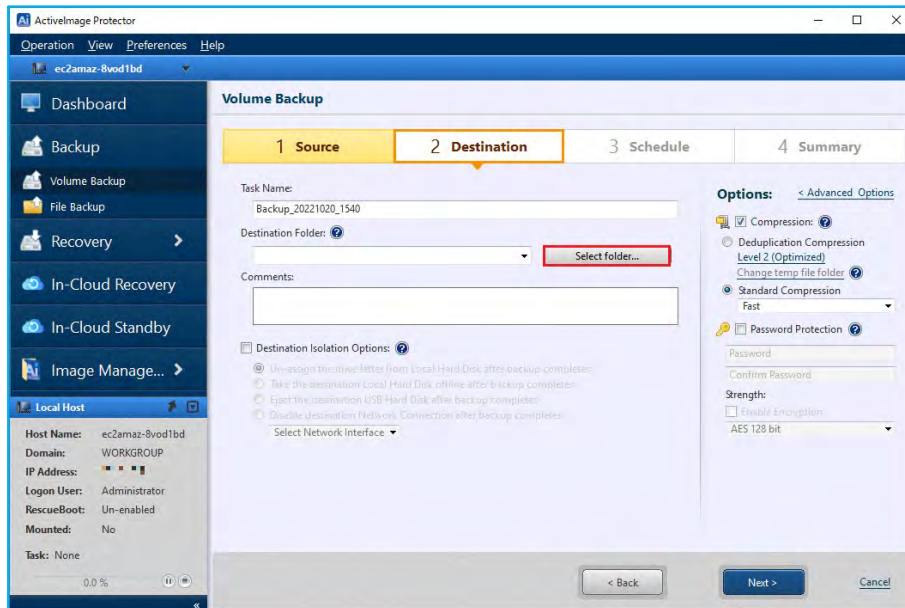


2. Select a backup source. The following example shows the entire disk selected for the backup source. Click **[Entire Disk]** and check the checkbox for **[Disk 0]**. When the backup source is selected, click **[Next]**.

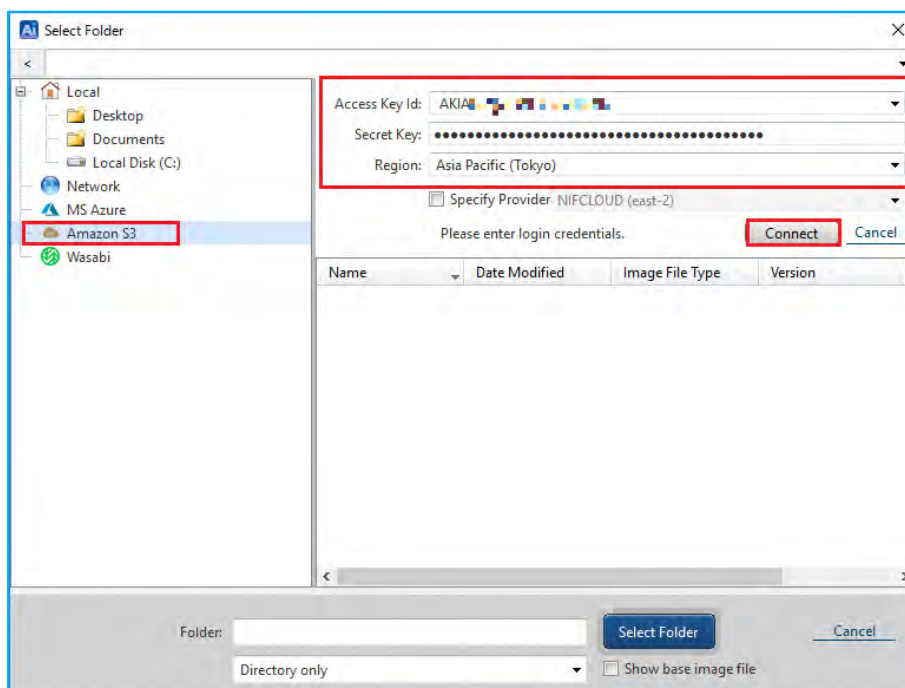


## Configure backup settings and run backup tasks

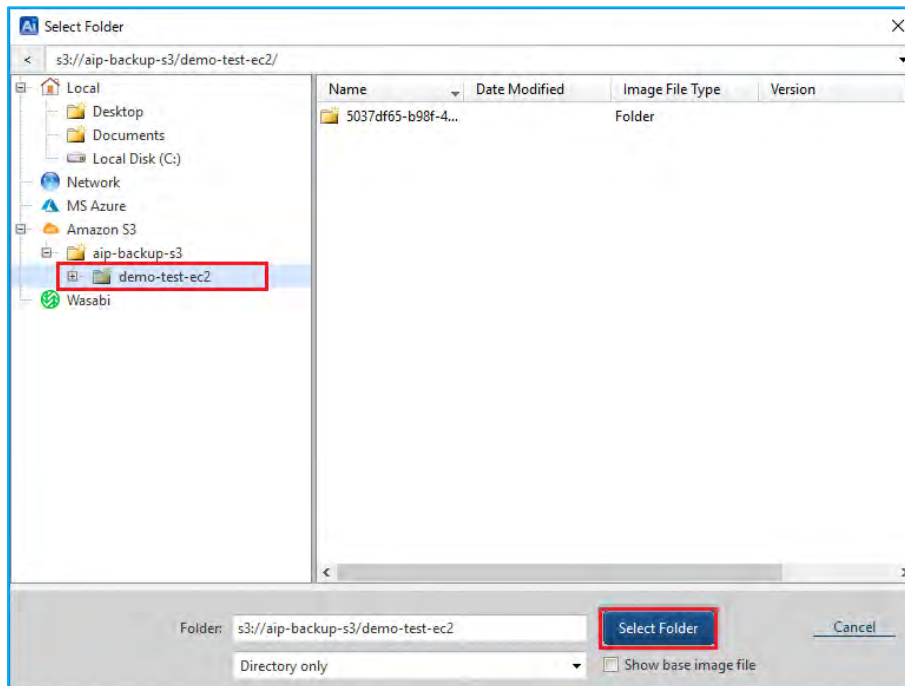
3. Select a destination folder for the backup image. Supported storage locations include local disks, network shared folder in the cloud, cloud storage (Azure Storage, Amazon S3, Wasabi). The following example shows “Amazon S3” is selected as the destination. Click the **[Select Folder]** button.



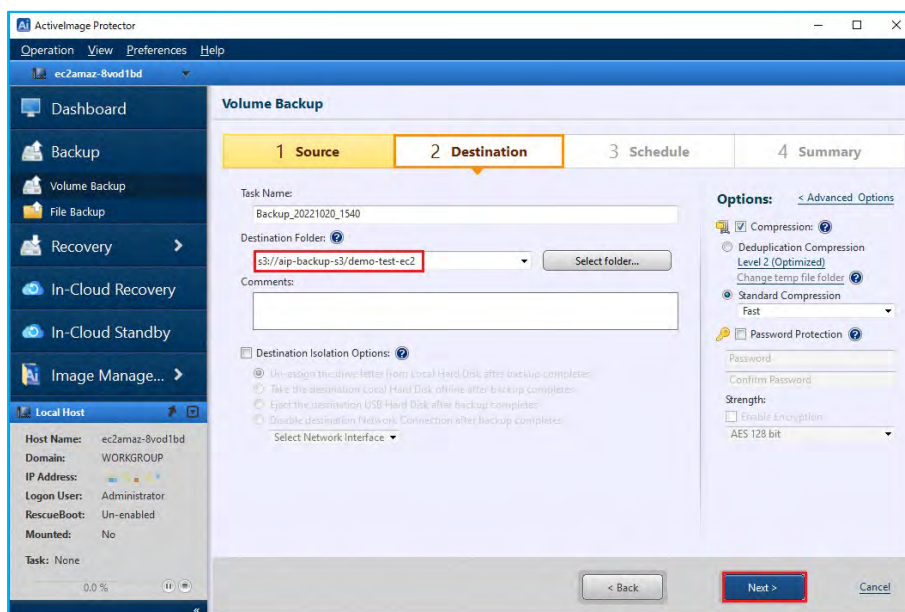
4. Select “Amazon S3” in **[Select Folder]** window. Next, enter your credentials to log into Amazon S3. Enter **[Access ID:]**, **[Secret Key:]** for AWS and select **[Region:]** and click **[Connect]**.



- When the connection to Amazon S3 is successfully established, bucket information is shown. The following example shows we are selecting folder “demo-test-ec2” in the bucket “aip-backup-s3” pre-configured in Amazon S3. Click the **[Select Folder]** button.



- Ensure you have selected a folder in Amazon S3 for the **[Destination Folder]**. Then, click the **[Next]** button. The Destination Isolation feature, and compression & encryption options are available at the bottom and the right side of the screen. Please refer to section 3-2 Volume Backup: Scheduled Backups of this document for more information.





## Configure backup settings and run backup tasks

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

Schedule Settings

Backup\_20221020\_1540 Effective Date/Time: 2022/10/20 16:05 ~ 2023/10/20 16:05 ☒ Not Specified

Task Type: **Backup Once** Schedule Backup

Base ?

☒ Monthly ☒ Weekly

1 2 3 4 5 6 7  
8 9 10 11 12 13 14  
15 16 17 18 19 20 21  
22 23 24 25 26 27 28  
29 30 31 EOM

Execute Time: 16:05

Incremental ?

☒ Weekly ☒ Multi-times

Start Time: 07:00 End Time: 16:00 Interval: 60 Minutes

☒ One time only: 16:05

Add New Base Add New Incremental

Event Backup: ☐ Shutdown/Reboot Base and Incremental

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

OK Cancel

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

ActiveImage Protector

Operation View Preferences Help

ec2amaz-8vod1bd

Dashboard Backup Volume Backup File Backup Recovery In-Cloud Recovery In-Cloud Standby Image Manage...

Local Host

Host Name: ec2amaz-8vod1bd  
Domain: WORKGROUP  
IP Address: 172.31.1.1  
Logon User: Administrator  
RescueBoot: Un-enabled  
Mounted: No  
Task: None 0.0 %

Volume Backup

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

Task type: Backup Once  
Effective From: 2022/10/20 16:05  
Base (Full): Incremental  
Edit Schedule

Options:

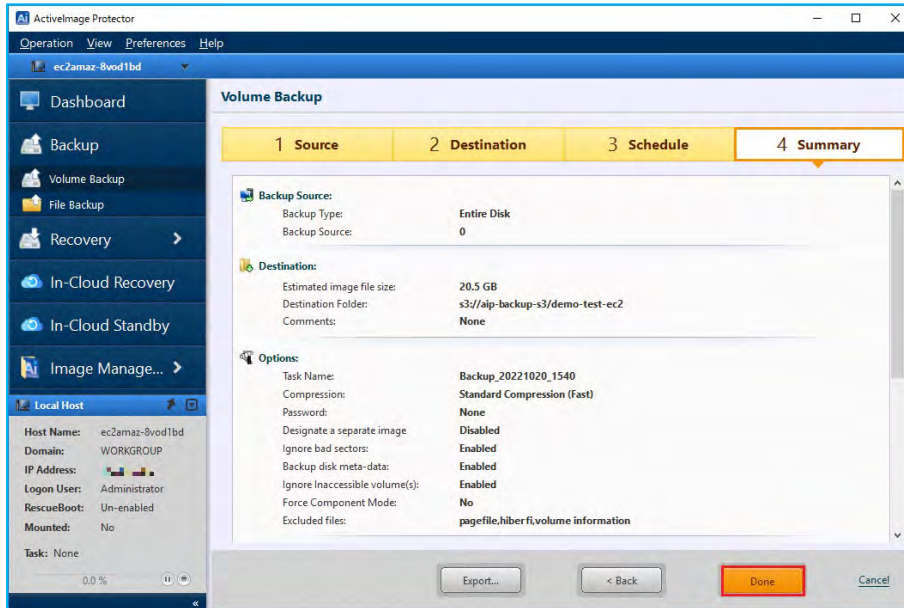
☐ Enable Retention Policy Delete both full and incrementals  
Number of image sets to retain: 3  
☐ Send email Task failed

Execution Priority

Full (Base): Lowest Low Medium High  
Incremental: Lowest Low Medium High

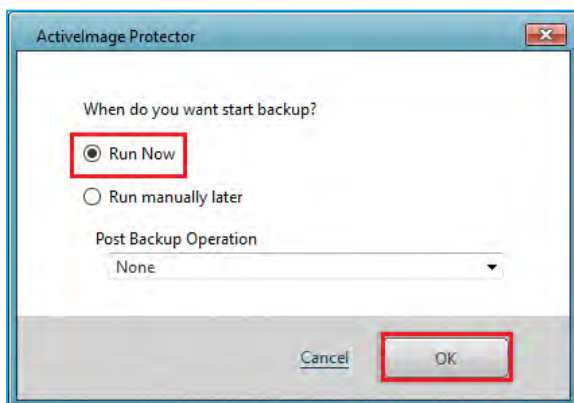
< Back Next > Cancel

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



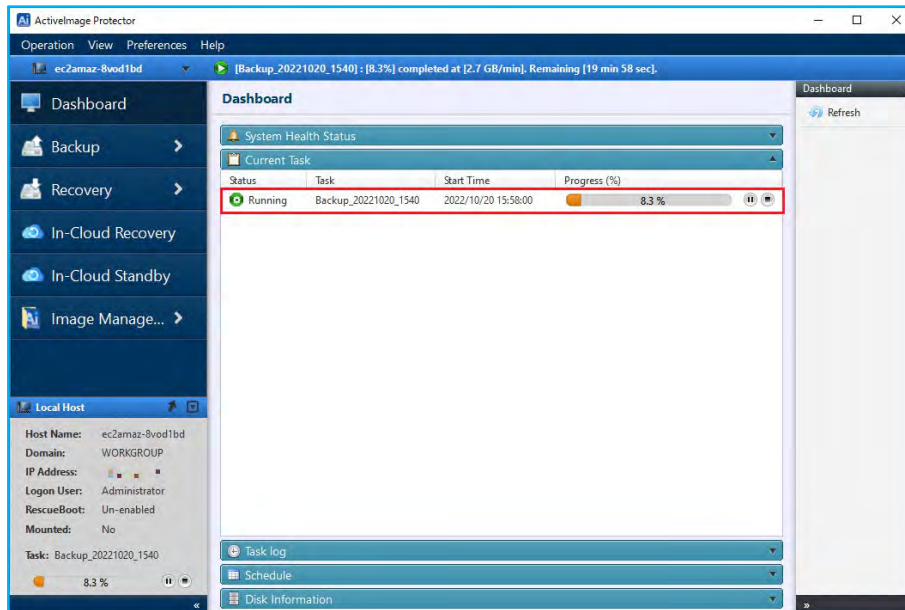
10. Select **[Run Now]** and click **[OK]** to start backup task.

**[Post Backup Operation]** may be selected to shut down or restart the system upon the completion of backup.

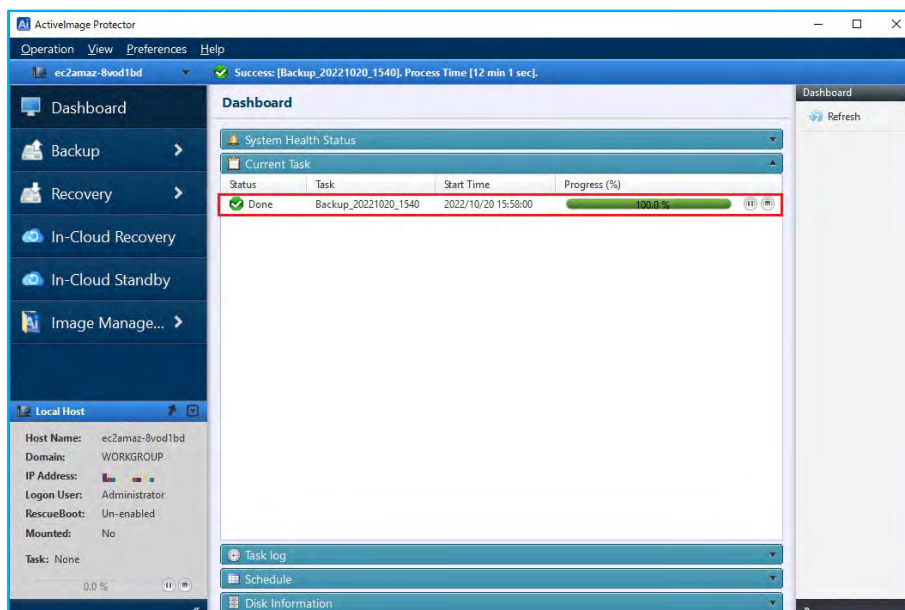


## Configure backup settings and run backup tasks

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



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

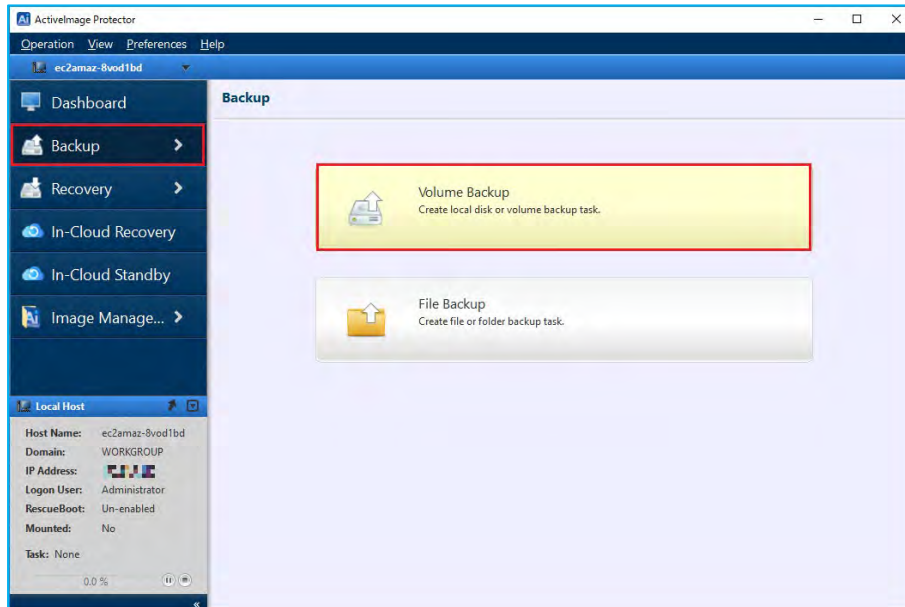


## 3-2. Volume Backup: Scheduled Backups

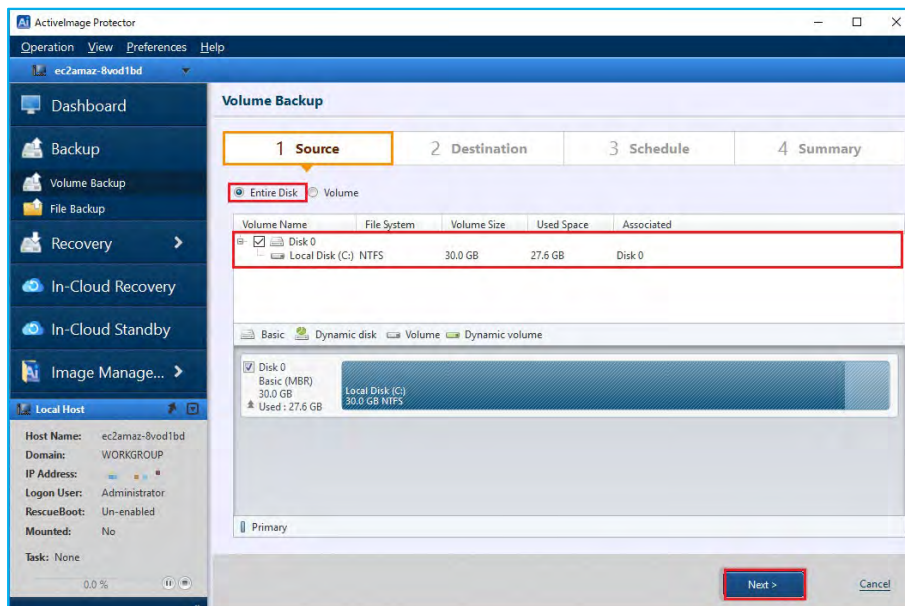
Please use the following steps to configure regularly scheduled backups.

1. Start ActiImage Protector by clicking on the Windows Start menu and selecting **[Actiphy]** → **[ActiImage Protector]**.

Once in ActiImage Protector, click on **[Backup]** → **[Volume Backup]**.

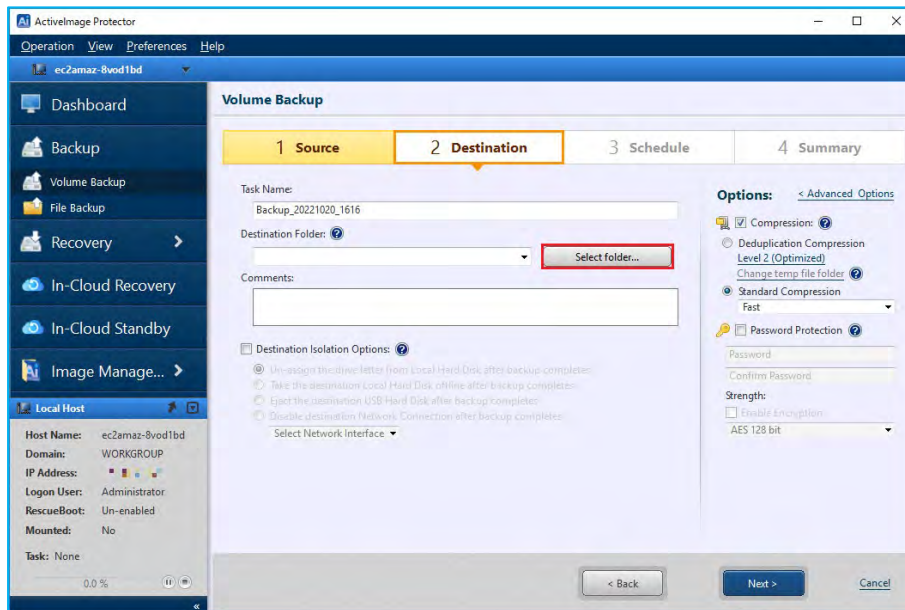


2. Select the backup source from the list of volumes. We will select the entire disk as the backup source in this example. Click **[Entire Disk]** and then click the checkboxes for **[Disk 0]**. Once you have selected the backup source(s), click the **[Next]** button.

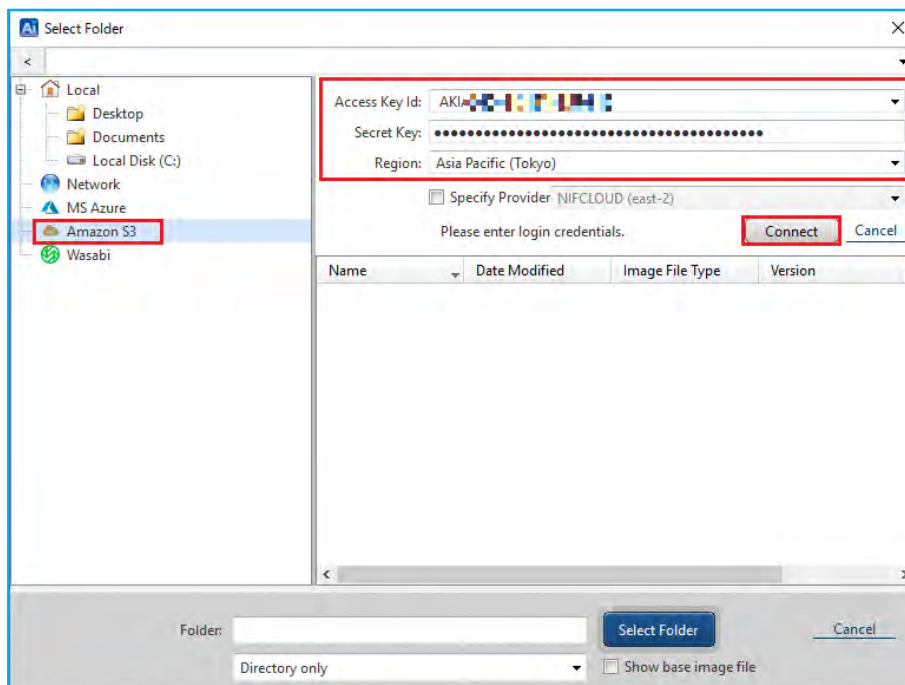


## Configure backup settings and run backup tasks

3. Select a destination folder to save the backup image files to. In this example, we have selected the cloud storage “Amazon S3” as the destination. Click **[Select Folder]** or click on the “▼” icon on the right-hand side of the **[Destination folder]** text box to select a location to save your backup. Click **[Select Folder]** when specifying a new destination folder.



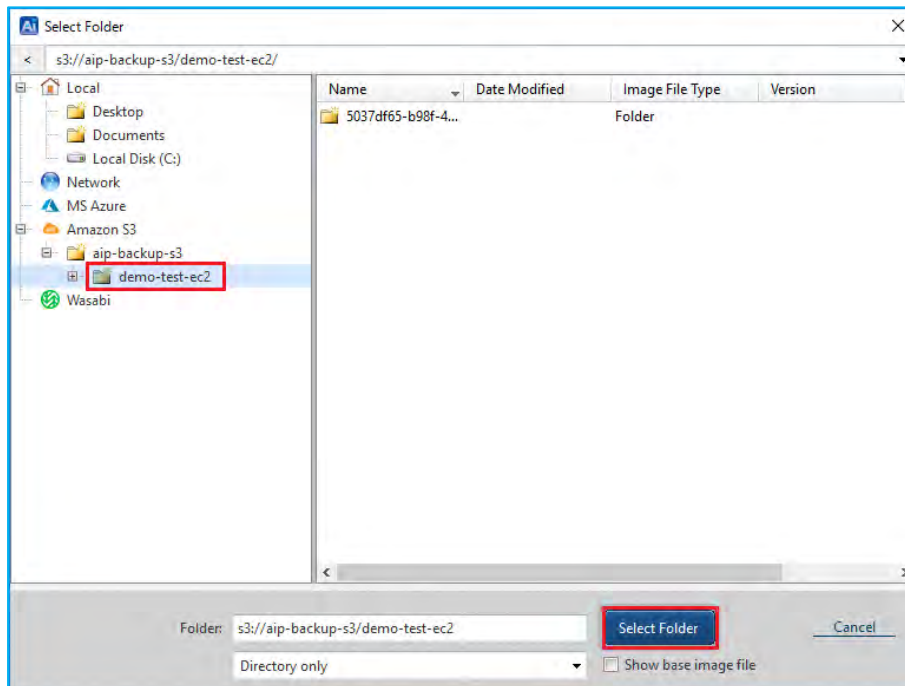
4. Select “Amazon S3” in **[Select Folder]** window. Next, enter your credentials to log into Amazon S3. Enter **[Access ID:]**, **[Secret Key:]** for AWS and select **[Region:]** and click **[Connect]**.



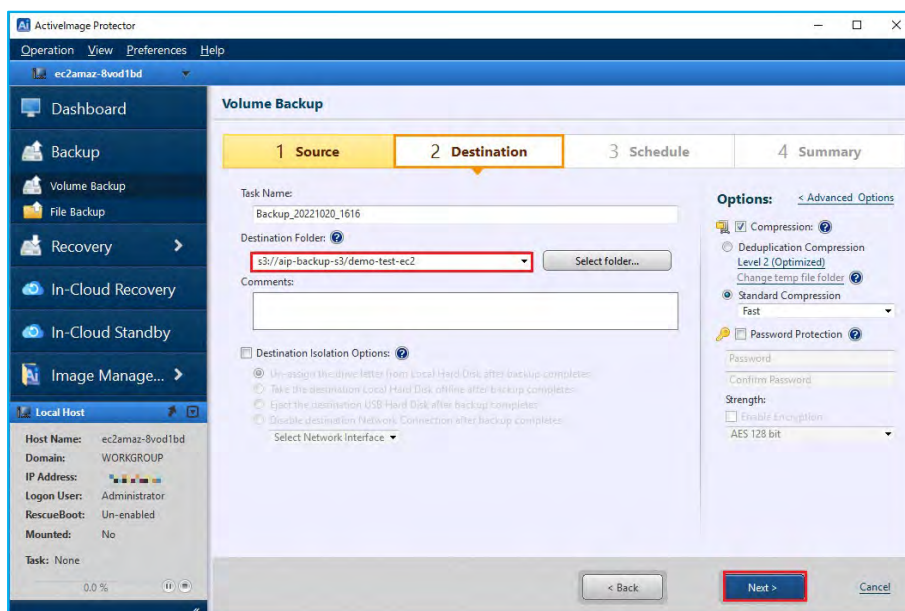


## Configure backup settings and run backup tasks

- When the connection to Amazon S3 is successfully established, bucket information is shown. The following example shows selecting the folder “demo-test-ec2” in the bucket “aip-backup-s3” pre-configured in Amazon S3. Click the **[Select Folder]** button.



- Ensure you have selected a folder in Amazon S3 for the **[Destination Folder]**. Then, click the **[Next]** button. We will review the **[Options]** sections later in this document.



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

The screenshot shows the 'Schedule Settings' dialog box for 'Backup\_20221020\_1616'. The 'Task Type' is set to 'Schedule Backup'. The 'Base' schedule is configured as 'Weekly' with 'Execute Time' set to '01:00' on 'Sun'. The 'Incremental' schedule is also set to 'Weekly' with 'Execute Time' set to '01:00' on 'Mon' through 'Sat'. The 'Event Backup' section is set to 'Shutdown/Reboot' and 'Base and Incremental'. The 'Option' section has 'Auto run if a scheduled task is missed' checked. The 'OK' button is highlighted with a red box.

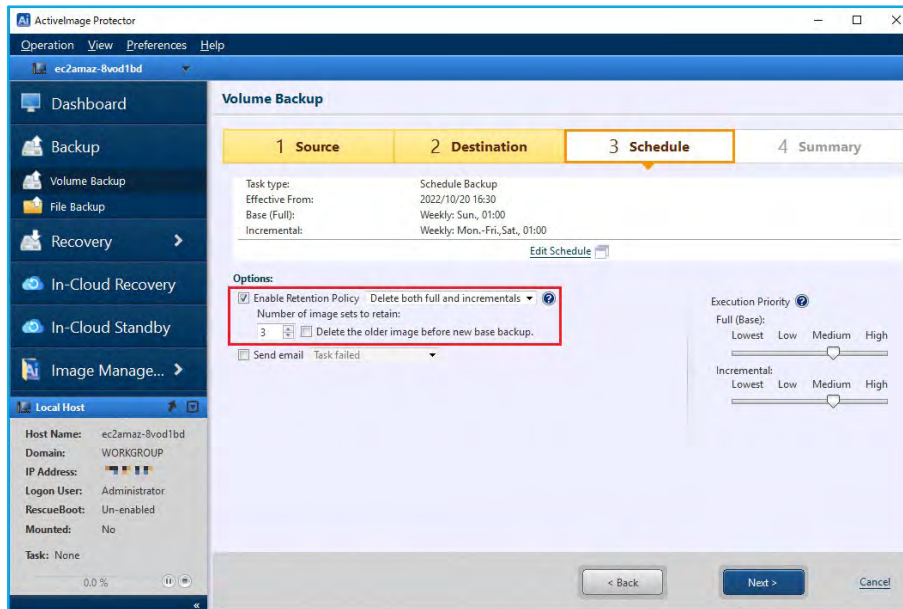
8. The following example shows how to set up a multi-scheduled backup:
  - Click the **[Add New Base]** link on the Schedule Settings page.
  - Configure the settings for your additional schedule.
  - In addition to a weekly schedule, you can configure monthly backups to regularly occur at the end of the month.

The screenshot shows the 'Schedule Settings' dialog box for 'Backup\_20221020\_1616'. The 'Task Type' is set to 'Schedule Backup'. The 'Base' schedule is configured as 'Monthly' with 'Execute Time' set to '01:00' and 'EOM' (End of Month) selected. The 'Incremental' schedule is set to 'Weekly' with 'Execute Time' set to '01:00' on 'Sun' through 'Sat'. The 'Event Backup' section is set to 'Shutdown/Reboot' and 'Base and Incremental'. The 'Option' section has 'Auto run if a scheduled task is missed' checked. The 'OK' button is highlighted with a red box.

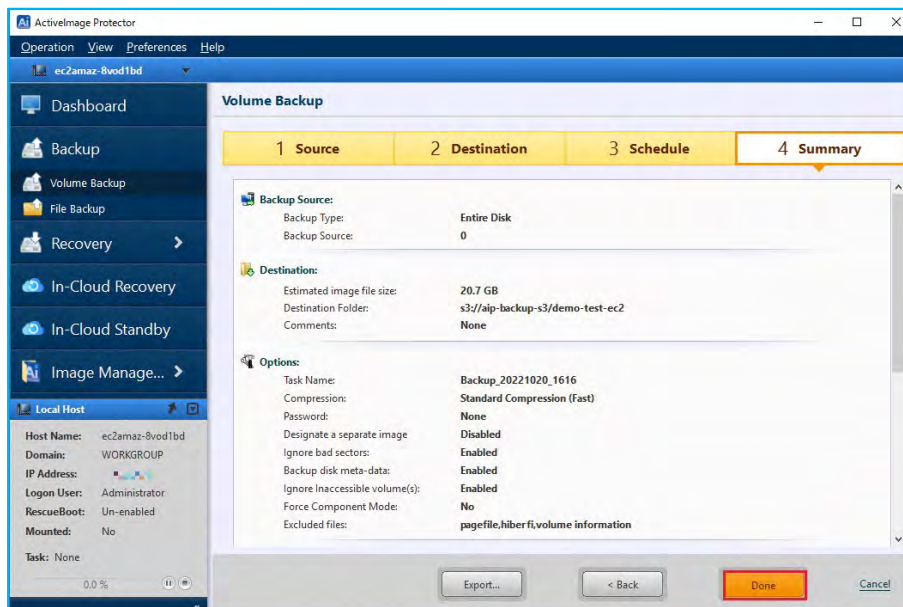
9. You can configure **[Enable Retention Policy]** and **[Send Email]** settings on the **[Schedule]** tab.

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

**NOTE:** Each set of ActiveImage Protector backup files consists of one base backup image and any associated incremental backup files.

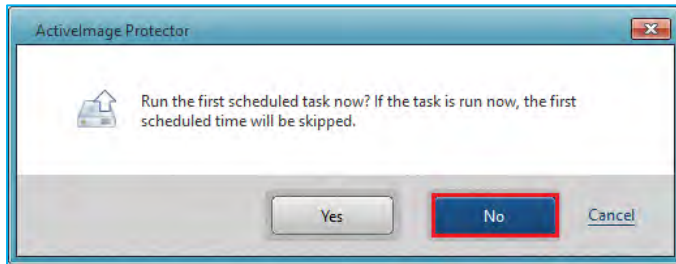


10. After configuring the backup schedule, you should see a summary of your configuration. Please review your backup configuration. If everything looks correct, click the **[Done]** button.

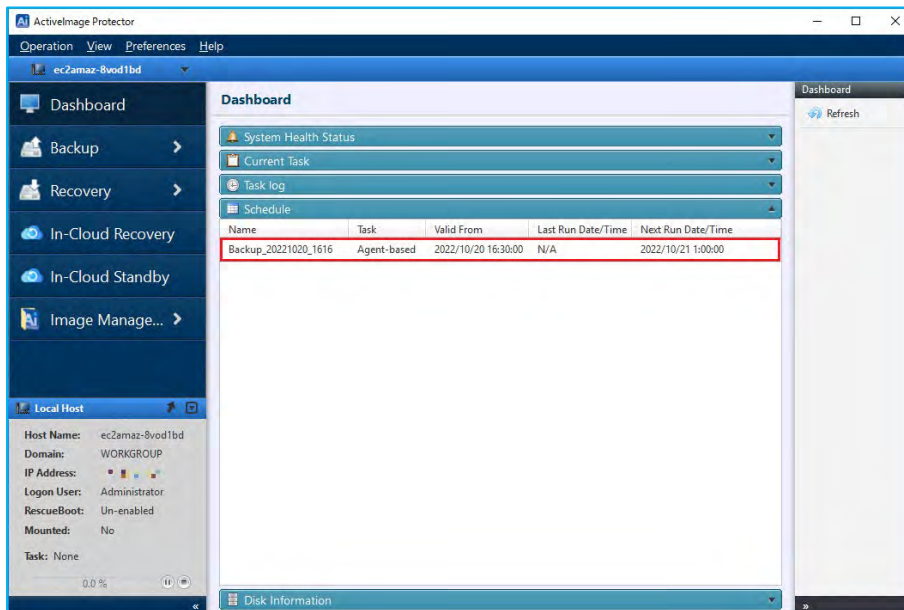




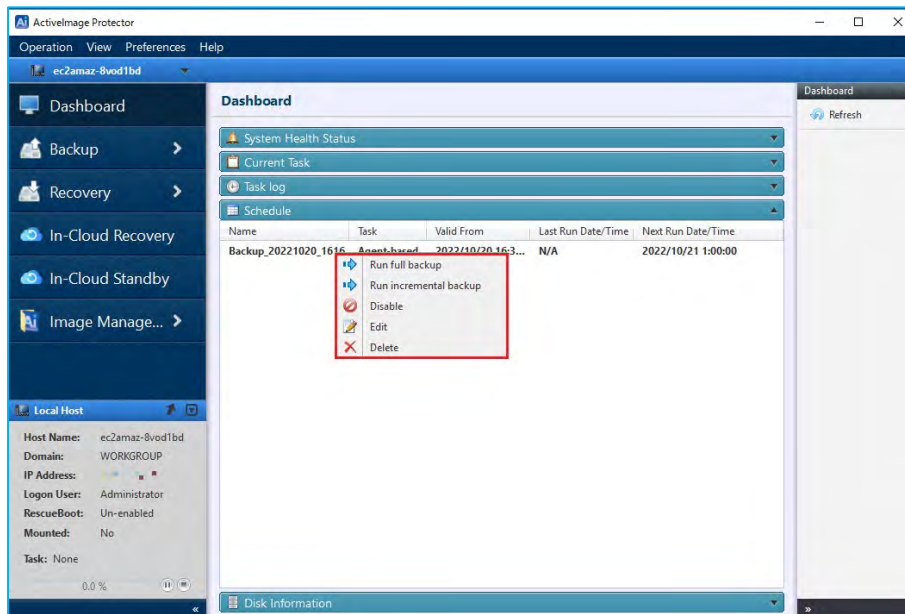
11. Next, you'll see a dialog asking if you want to run the initial backup now. If you click the **[No]** button, the system will take you back to the Dashboard, and your initial backup will run according to your schedule. If you click the **[Yes]** button, the system will immediately run the initial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



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



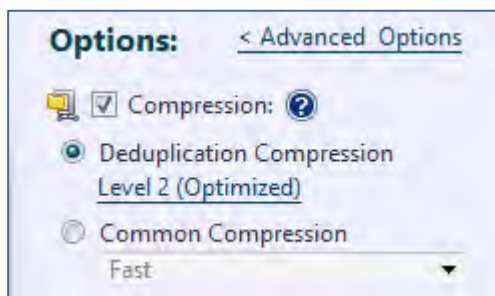
13. Right-click on **[Schedule Name]** to immediately run a full or incremental backup task or edit the schedule settings.



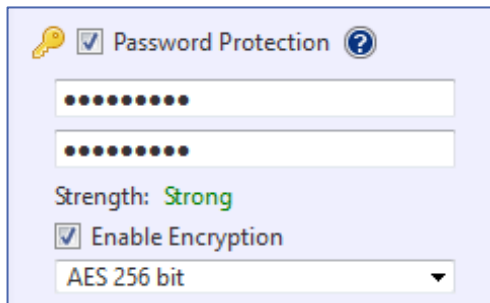
14. When necessary, you can enable the **[Options]** and **[Advanced Settings]**. Here are some examples:

(1) **Options:**

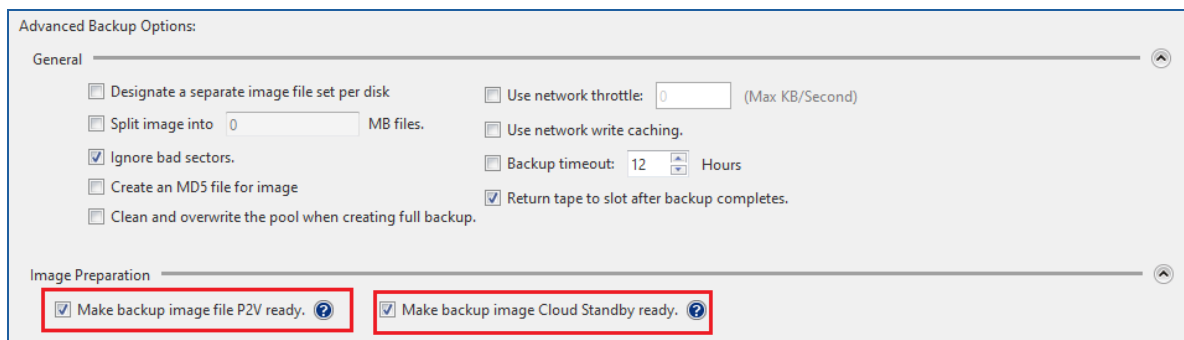
- **Compression:** ActiveImage Protector provides two types of compression: **[Standard Compression]** and **[Deduplication Compression]**. The compression ratio differs depending on the type of compression you choose. The **[Standard Compression]** option will produce a backup image around 70% of the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



- (2) **Password Protection:** Enabling this option protects the backup image file by assigning a unique password. This additional security prevents anyone from mounting, exploring, or restoring the image file without a password.
- (3) **Enable Encryption:** There are three levels of encryption to choose from: "RCS," "AES128 bit", and "AES256 bit." Encrypting your backups will help protect any backup image files you save to a remote location from cyber attacks.



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



- **Make backup image file P2V ready:** This option tells ActiveImage Protector to prepare an image file for virtualization later. Please note that this option does not virtualize the file. It only prepares the image so you can virtualize it at a later time, however it includes the installation of the drivers required for virtualization on (VMware ESXi / Microsoft Hyper-V), and modifying registry settings, etc.
- **Make backup image Cloud Standby ready:** This option prepares the image for booting via In-Cloud Standby by installing required drivers and modifying the registry. Please enable this option when using In-Cloud Standby.

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



The screenshot shows the 'Scripting' tab in a configuration window. It contains two sections: 'Script to execute before the snapshot is taken:' and 'Script to execute after the snapshot is taken:'. Each section has a text input field for a script path, a 'Time-out' field set to '30 mins.', and a 'Run on:' dropdown menu set to 'Base and Incremental'. The entire configuration area is highlighted with a red border.

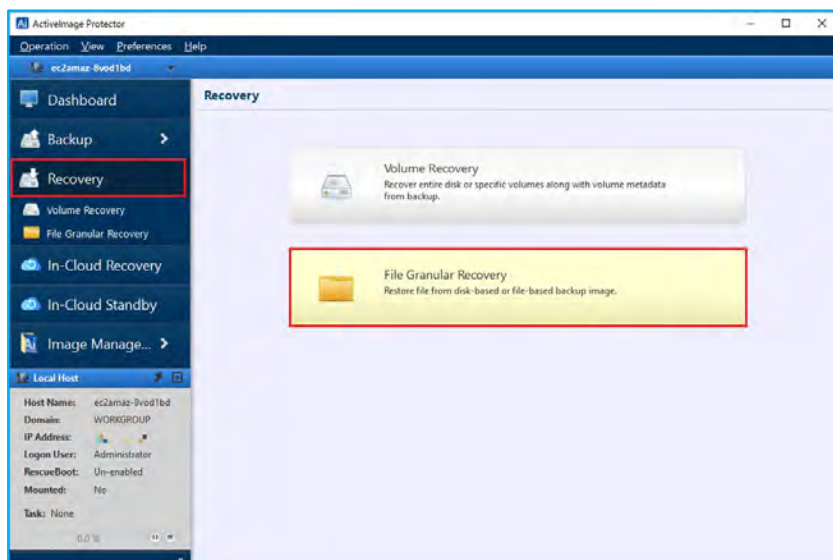
Script to execute before the snapshot is taken:	Time-out	Run on:
c:\temp\DB_shutdown.ps1	30 mins.	Base and Incremental
Script to execute after the snapshot is taken:	Time-out	Run on:
c:\temp\DB_startup.ps1	30 mins.	Base and Incremental

## 4. Restore

### 4-1. File / Folder Recovery

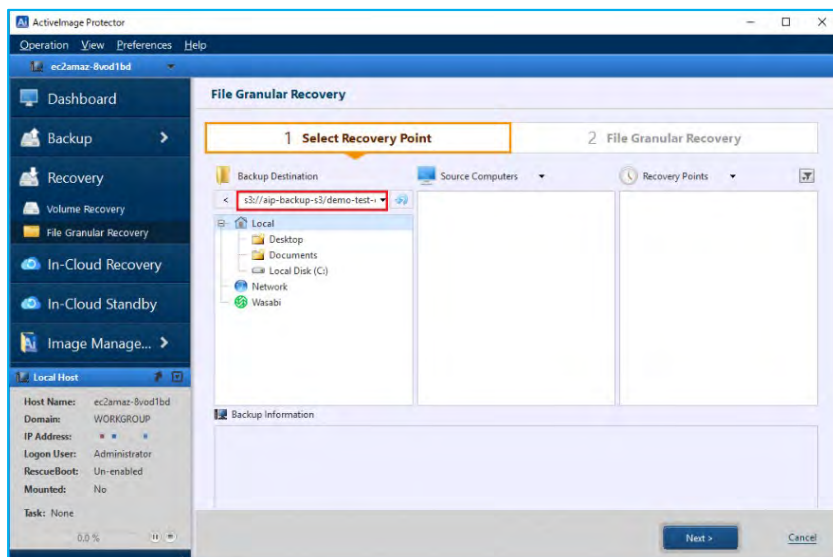
Please use the following steps to restore a specific file or folder from a disk backup image:

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



2. Next, on the [File Granular Recovery] screen:

- Click on the [▼] icon under **[Backup Destination]**.
- Select the folder of the backup image file from which you want to restore a file or folder.
- You can also specify the path to the backup image. In this example, we're entering "S3://aip-backup-s3/demo-test-ec2" as the instance of Amazon S3 containing our backup image.
- Press the **[Enter]** key to set your selection. When you are prompted to enter credential information for accessing AWS, please enter **[Access ID:]**, **[Secret Key:]**, **[Region:]** and click **[Connect]**.

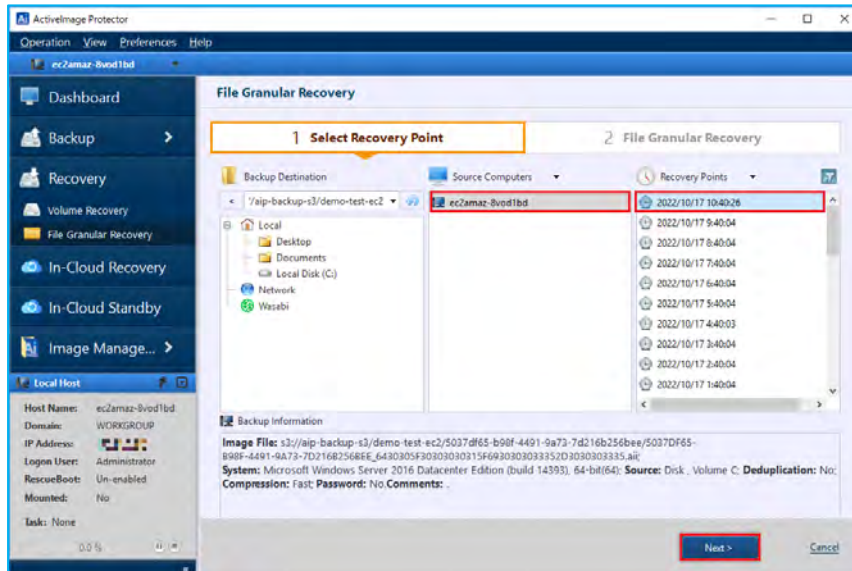


## Restore

3. ActiImage Protector will populate the **[Source Computers]** list with all the images in the directory you specified.

Select the source computer you want to restore a file or folder from in the list. ActiImage Protector will display information about your selected backup image in the **[Backup Information]** section of the screen.

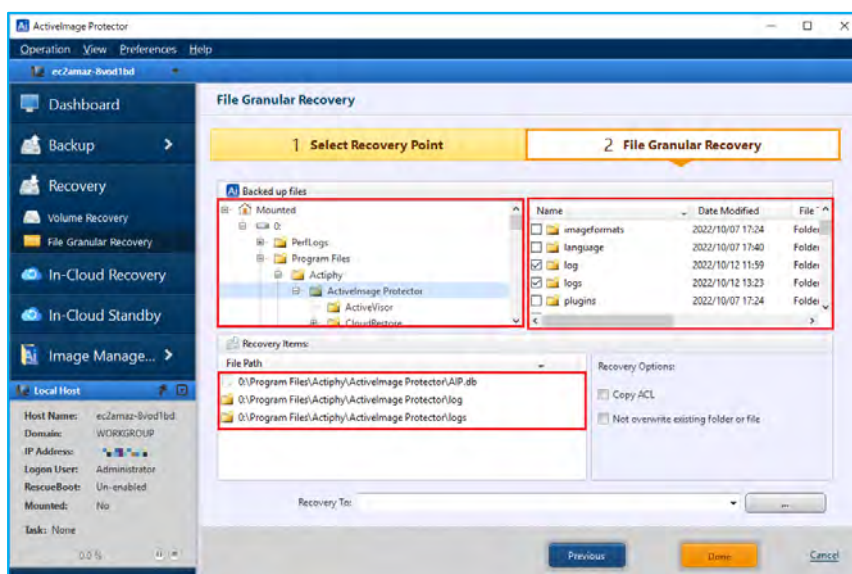
Click the **[Next]** button.



4. Now, click the checkbox next to each file or folder you want to restore in the **[Backed up files]** list. ActiImage Protector will list each item you've selected in the **[Recovery Items]** section of the page.

Once you have selected all the files and folders you want to restore from the **[Backup up files]** list, you may choose the following recovery options:

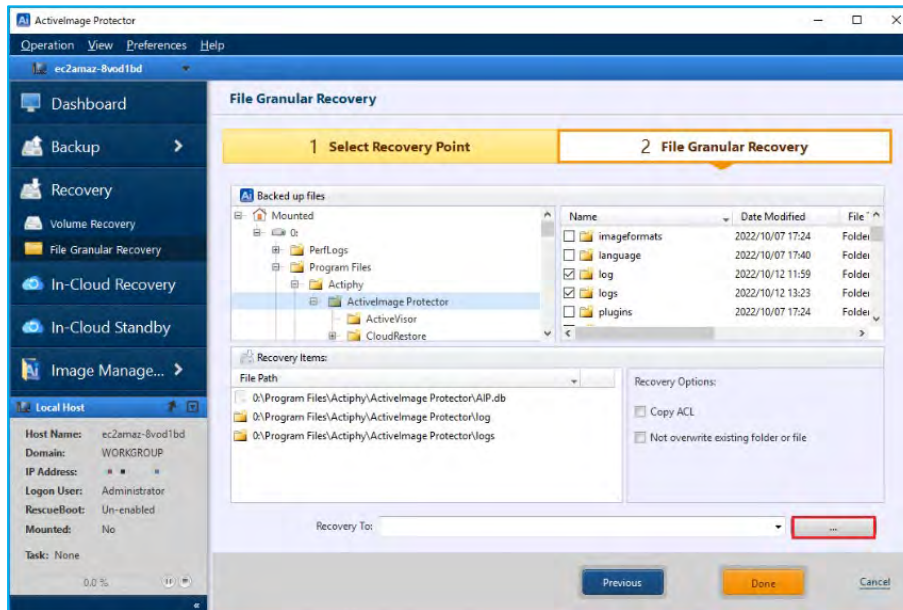
- **[Copy ACL]** will copy the Access Control List data from the backup image to the recovered file or folder.
- If **[Not overwrite existing folder of file]** is selected, ActiImage Protector will safely recover your selected files without overwriting existing files and folders. If you don't choose this option, ActiImage Protector will overwrite any files or folders on your computer that have the same name as the files and folders you are recovering from your backup image.



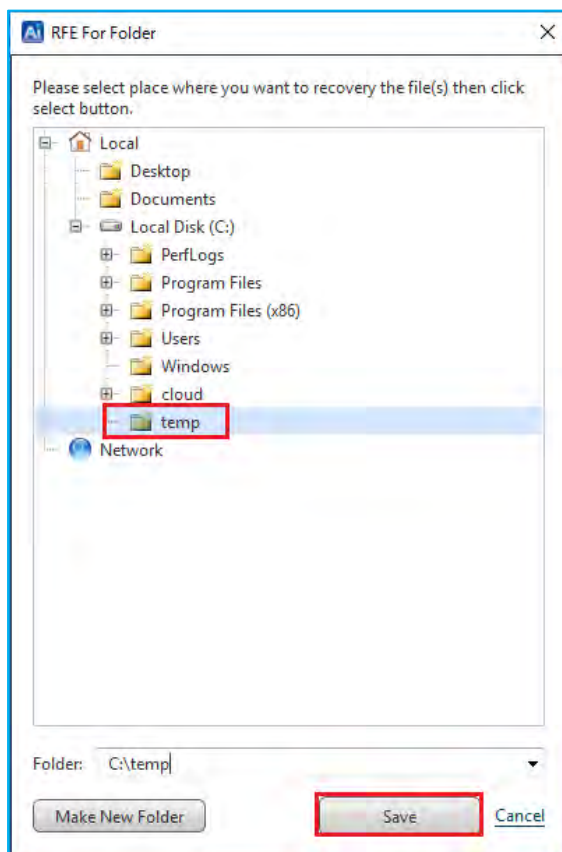


## Restore

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

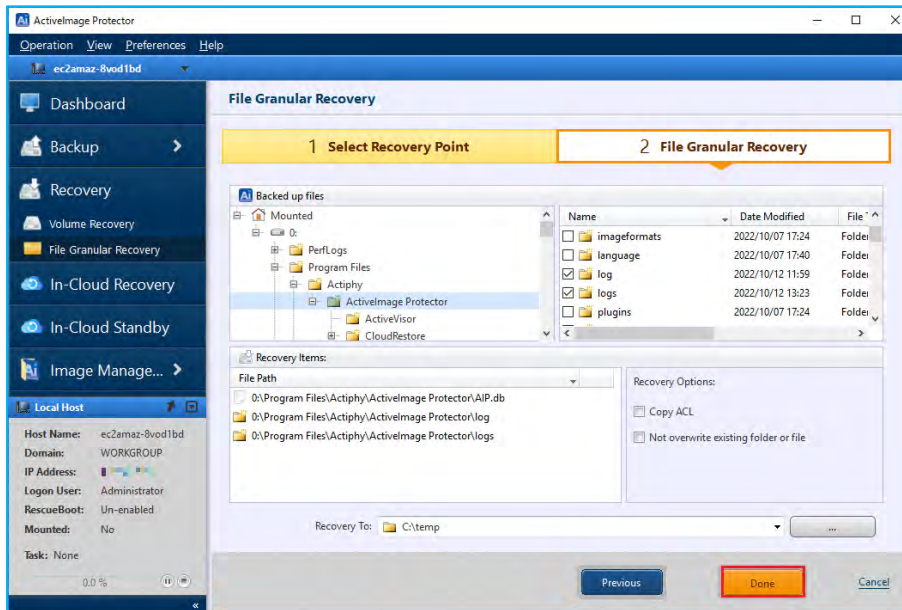


- Select the folder and click **[Save]**.

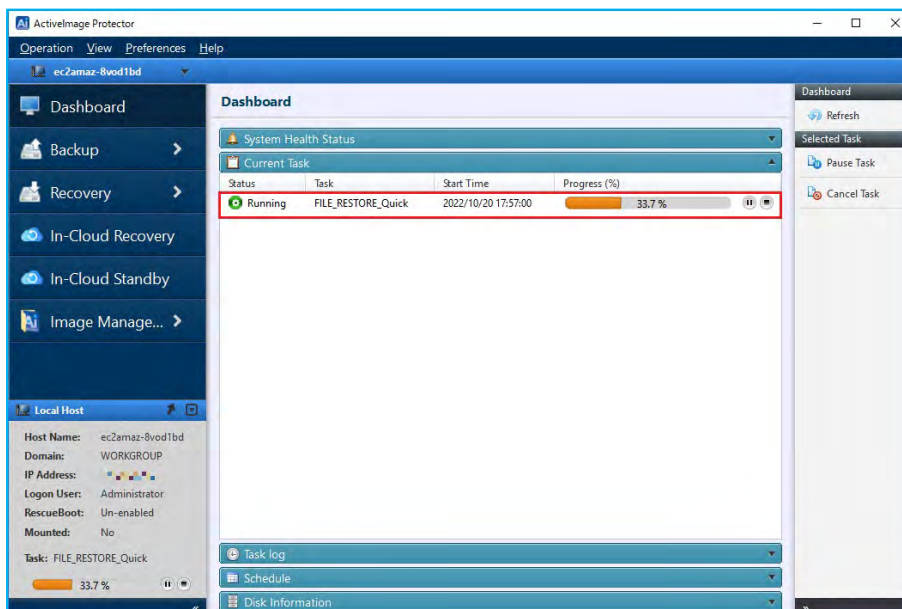


## Restore

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



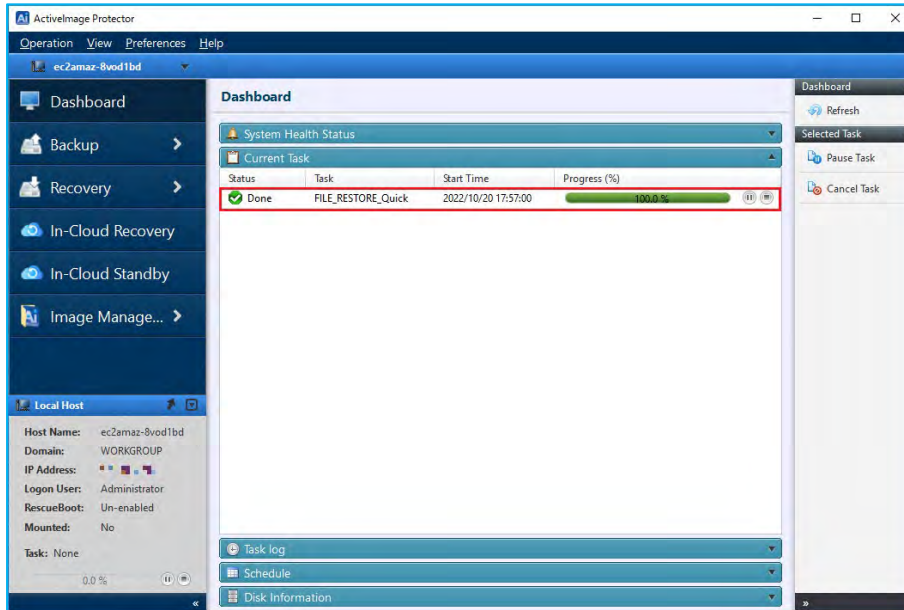
- ActiveImage Protector will display the restoration progress in the **[Current Task]** section.



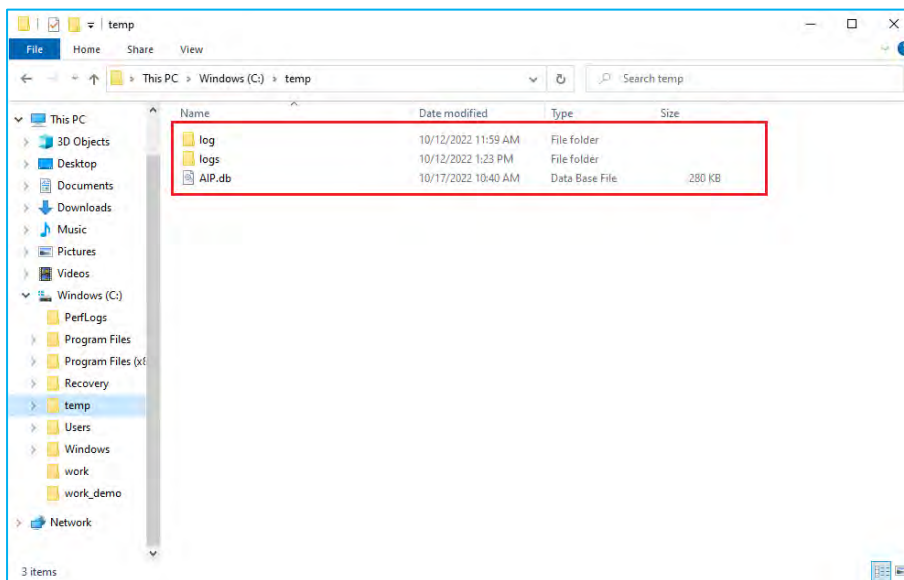


## Restore

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



10. The files and folders specified to restore are saved to the specified location.



## 4-2. In-Cloud Recovery

The In-Cloud Recovery feature restores an entire system from a backup virtual machine configured in an Amazon Web Service (AWS), or Microsoft Azure cloud environment. This feature restores the backup via a temporary instance appliance and does not require the use of cloud management consoles or command line tools.

In-Cloud Recovery enables users to restore a system from a backup to an instance of AWS EC2 by using the following steps.

\* In-Cloud Recovery™ does not support Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) . When restoring a virtual machine, boot environment booted from RescueBoot is used. (Ref. "4-3 System Recovery (RescueBoot))

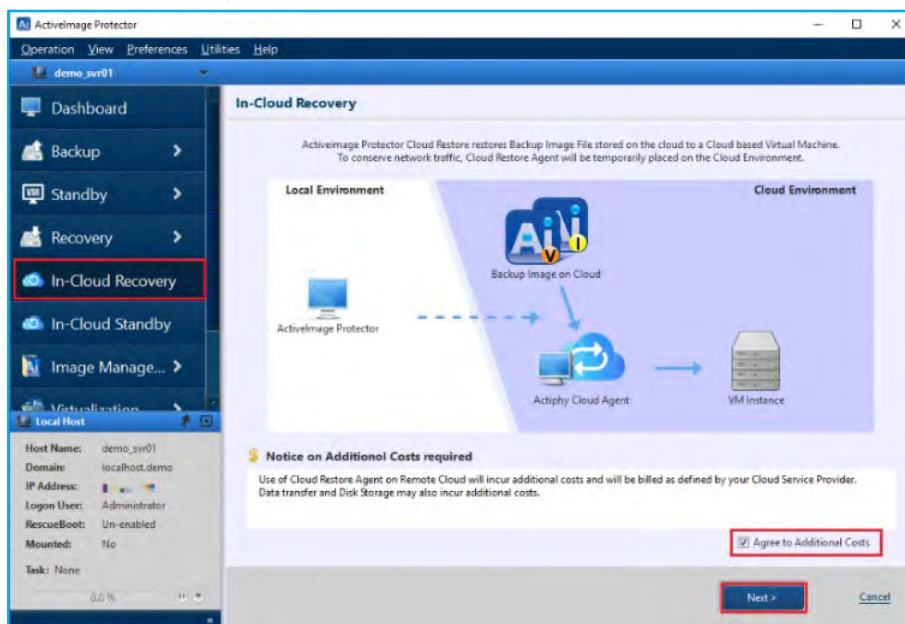
1. Go to Windows Start menu - **[Actiphy]** → **[ActiveImage Protector]**. Start ActiveImage Protector.

Select **[In-cloud Recovery]** in the left menu.

**Note:** In-Cloud Recovery does not run on a target virtual machine.

In-Cloud Recovery must be used on a computer that has access to the cloud environment.

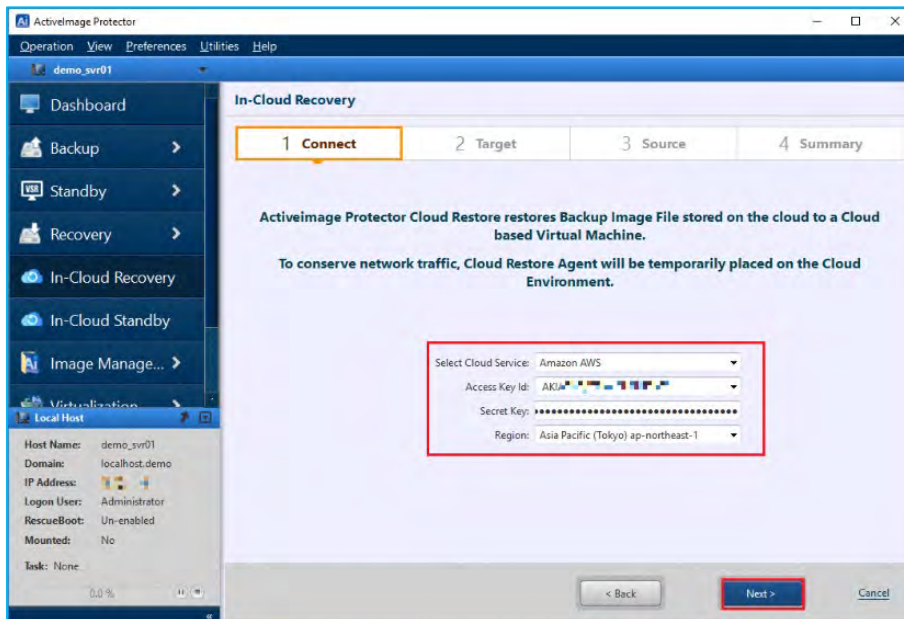
The use of any of the cloud services may incur additional costs and will be billed as defined by your Cloud Service Provider. In addition a temporary appliance called "Actiphy Cloud agent" will be deployed in the respective regions in cloud environment. Data transfer and storage for a volumes created in restore process may also incur additional costs as determined by the cloud provider. To proceed with operation, please click the checkbox to **[Agree to additional cost]** and click **[Next]**.



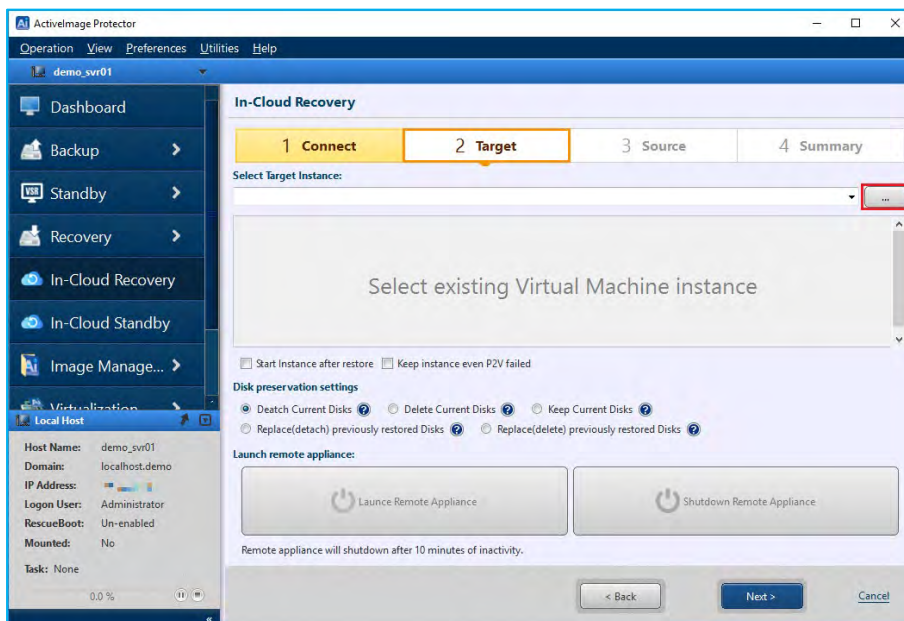
## Restore

2. Select the cloud service and enter credential information.

In this example we have selected **[Amazon AWS]** for **[Select Cloud Service]** and entered **[Access Key]** and **[Secret Key]** for AWS. Select **[Region]** and click **[Next]**.

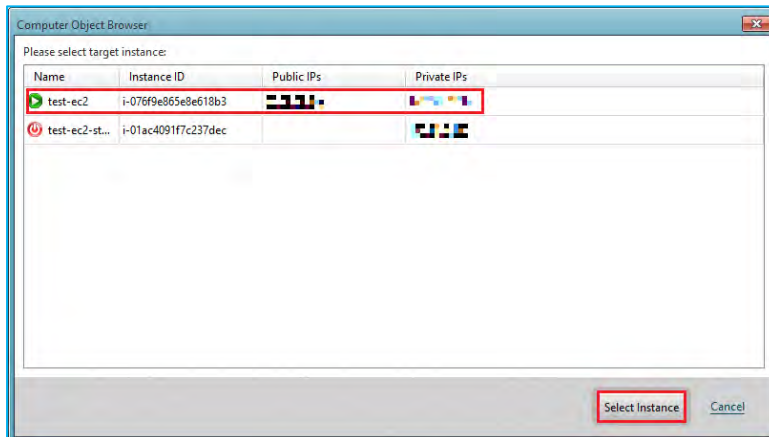


3. Click **[...]** and specify the instance for the restore target. Please make sure that the instance is not running.

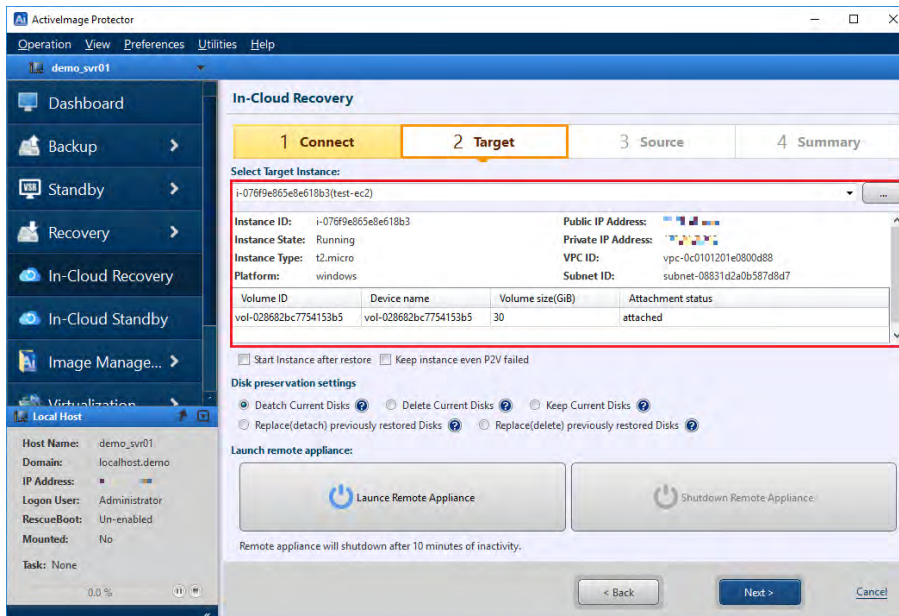


## Restore

- Please select the target instance and click **[Select instance]**. In this example we have selected backup source instance "test-ec2".



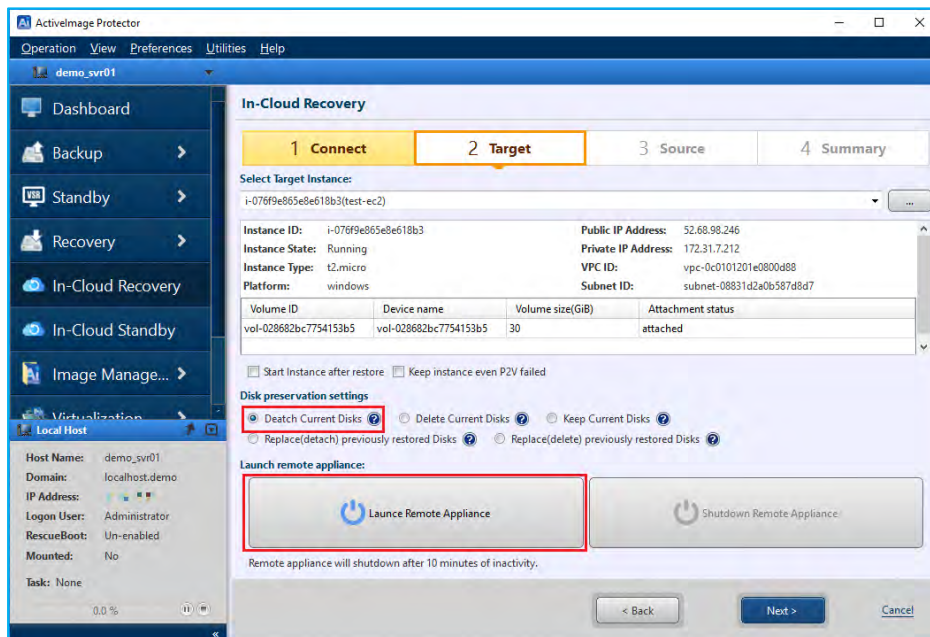
- The information of the target instance is displayed.



## 6. Configure the option settings for the restored disk.

In this example, we have selected **[Detach current disk]** for **[Disk preservation settings]**. Then, click **[Launch Remote Appliance]** to run “**ActiPhy Cloud Agent (boot environment)**”.

Please wait for a while...



### Disk preservation settings:

#### (1) Detach Current Disks:

Detach the disk connected to the instance and connect the restored disk to the instance.

The detached disk is not deleted but remains in storage.

#### (2) Delete Current Disks:

Detach and delete the disk(s) connected to the instance and attach the restored disk to the instance.

#### (3) Keep Current Disks:

The disk attached to the instance is not detached and the restored disk is attached as an additional disk.

#### (4) Replace (Detach) previously restored disks:

Detach previously restored disks and attach the newly restored disk to the instance.

The detached disk is not deleted but remains in storage.

Disks that are not restored when using this option are not detached from the instance.

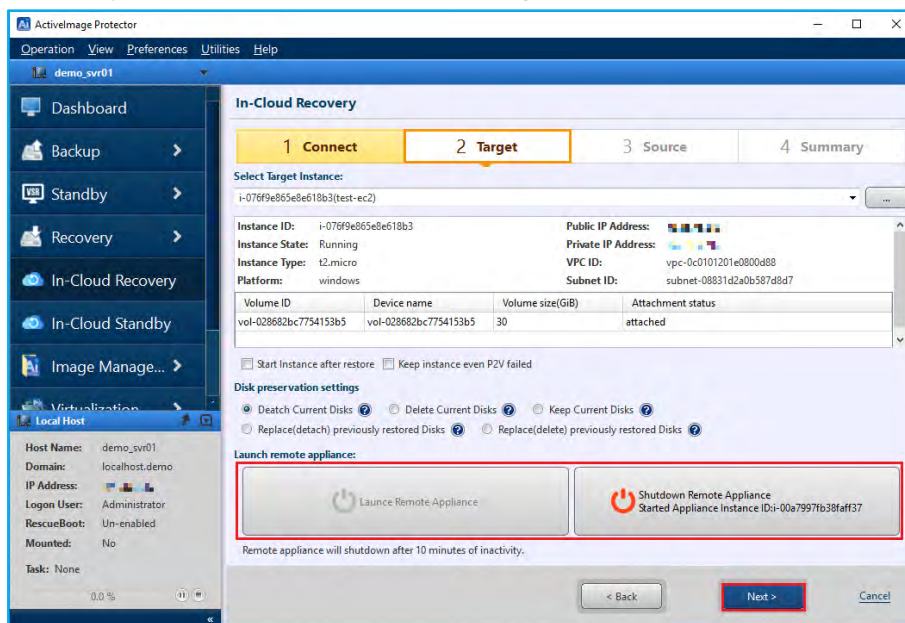
#### (5) Replace (Delete) previously restored disks:

Detach and delete previously restored disks on the instance and attach the newly restored disk to the instance. Disks that are not restored when using this option are not detached from the instance.

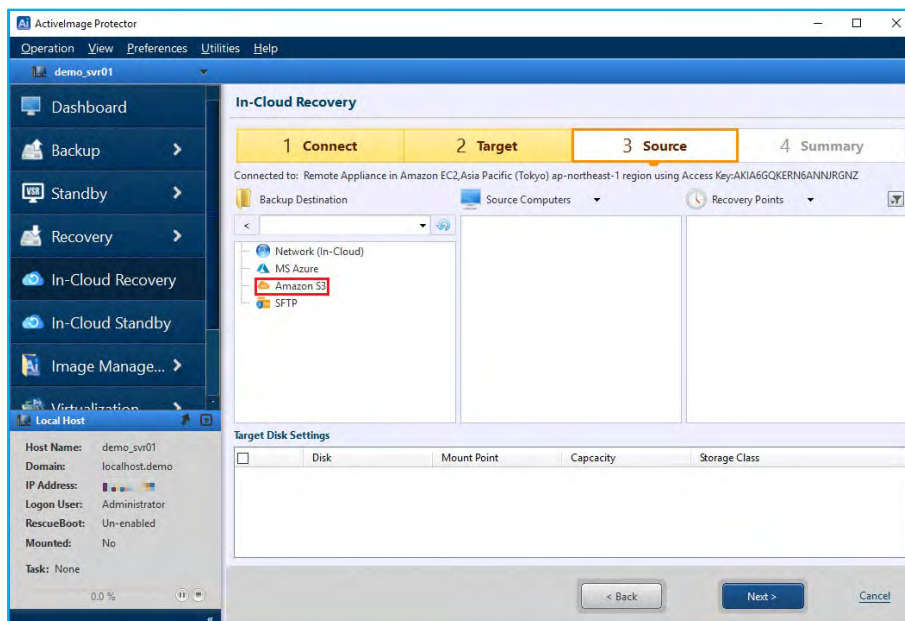


## Restore

- When **[Launch Remote Appliance]** is grayed out and **[Shutdown Remote Appliance]** is enabled, “**Actiphys Cloud Agent (boot environment)**” is running. Click **[Next]**.

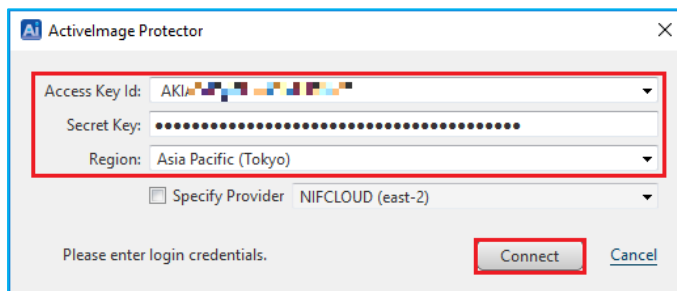


- Please specify the folder on which the source backup file is located. In this example we have selected **[Amazon S3]** for **[Backup Destination]**.

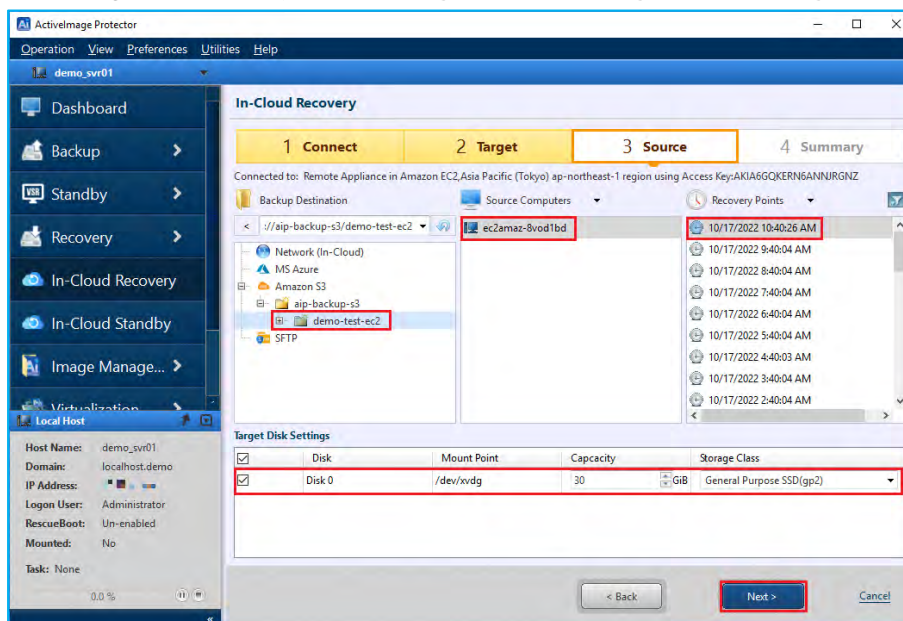


## Restore

9. Enter **[Access Key]** and **[Secret Key]** to access Amazon S3 of AWS. Select **[Region]** and click **[Connect]**.



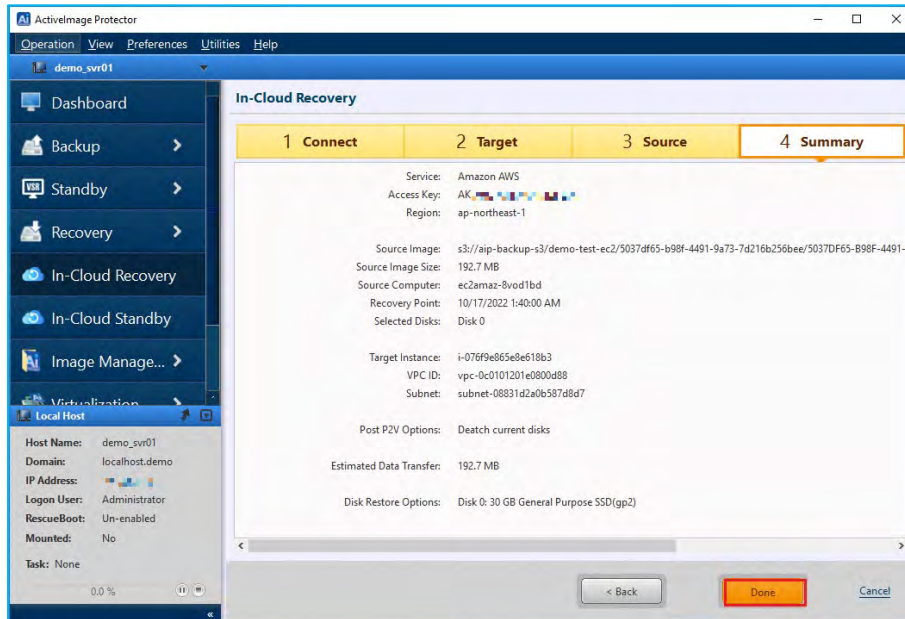
10. Please select **[Folder]** -> **[Source Computer]** -> **[Recovery Point]** and click **[Next]**. You can also configure the settings for **[Capacity]** and **[Storage Class]** in **[Target Disk Setting]**.



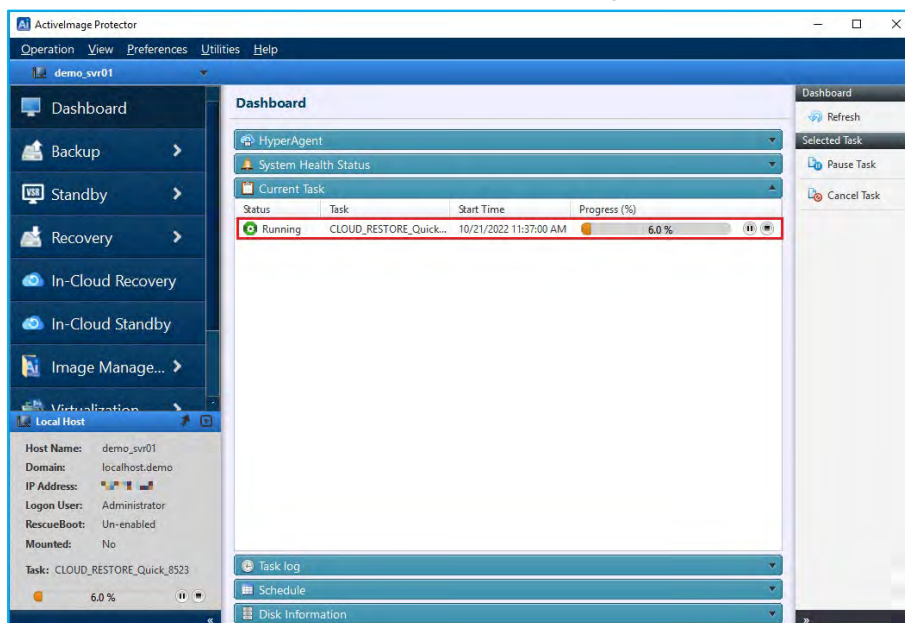
Disk	Mount Point	Capacity	Storage Class
Disk 0	/dev/xvdd	30	General Purpose SSD(gp2)

## Restore

11. Please review the configured settings and click **[Done]** to start the recovery process.



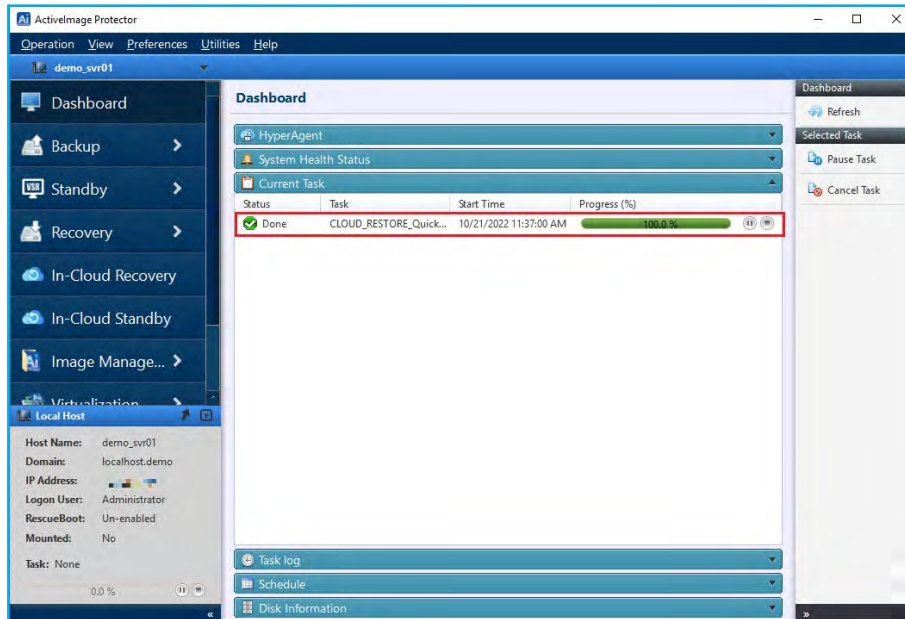
12. When a recovery task starts, you can monitor the progress in the Dashboard window.





## Restore

13. ActiImage Protector has finished the recovery process when the progress bar reaches 100%.



14. Once the recovery is complete, the disk connected to the instance is detached from AWS management console. You can verify the restored disk is connected to the restore target instance.

- (1) A new disk is created from the backup. The disk name is "<instance name>\_disk\_YYYYMMDDhhmmss". When you verify the restored disk is connected to the target instance is running normally, please delete the detached disk.

Volumes (1/2)						
Search						
	Name	Volume ID	Size	Created	Availability ...	Volume state
<input type="checkbox"/>	test-ec2-vol1	vol-028682bc7754153b5	30 GiB	2022/10/06 16:15 GMT+9	ap-northeast-1c	Available
<input checked="" type="checkbox"/>	test-ec2_Disk_20221021113753	vol-066b6372a135bf0b3	30 GiB	2022/10/21 11:38 GMT+9	ap-northeast-1c	In-use

- (2) The created disk is connected as the root device of the instance.

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

☒

Name

Instance ID

Instance state

Instance type

Status check

Availability Zone

Public IP

☒

test-ec2

i-076f9e865e8e618b3

Stopped

t2.micro

-

ap-northeast-1c

ec2-...

Instance: i-076f9e865e8e618b3 (test-ec2)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Root device details

Root device name

Root device type

EBS optimization

/dev/sda1

EBS

disabled

▼ Block devices

Filter block devices

Volume ID

Device name

Volume size (GiB)

Attachment status

Attachment time

Encrypted

vol-066b6372a135bf0b3

/dev/sda1

30

Attached

Fri Oct 21 2022 14:38:45 GM...

No

### 4-3. System Recovery (RescueBoot)

ActiveImage Protector™ includes RescueBoot, enabling to start up the Actiphy Boot Environment directly from a virtual machine in AWS, Azure, Google Cloud, Oracle Cloud without the use of external device of Actiphy Boot Environment. You can also remotely access boot environment booted from RescueBoot and restore the system of virtual machine in cloud. The following example shows the operating procedures of system recovery for AWS EC2 instance (virtual machine) using RescueBoot.

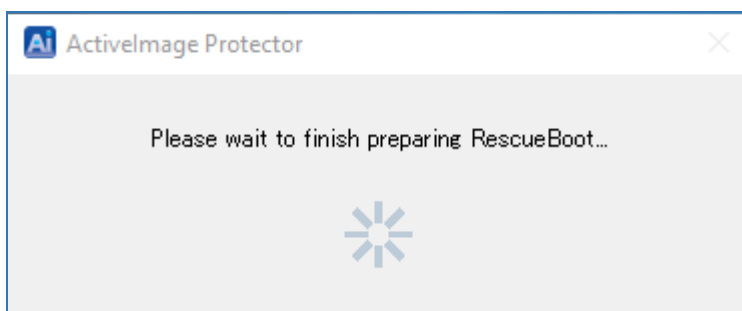
#### 1. Boot up RescueBoot

Please use the following operating procedures on the restore target virtual machine on which ActiveImage Protector is installed.

- (1) Go to Windows Tray icon (at the lower right of the desktop window) and click **[Run RescueBoot]** in ActiveImage Protector's icon menu.



- (2) When RescueBoot boots up, boot environment is built in the internal disk. Please wait until boot environment will be built (2-3 minutes).



## Restore

- (3) When the boot environment is built, you will get the following dialog notifying you that the system is shutting down and boot environment will boot up. At this point, remote connection is disconnected.



## 2. Accessing boot environment

When boot environment boots up on the restore target virtual machine, access the boot environment from ActiVImage Protector's Remote Management console.

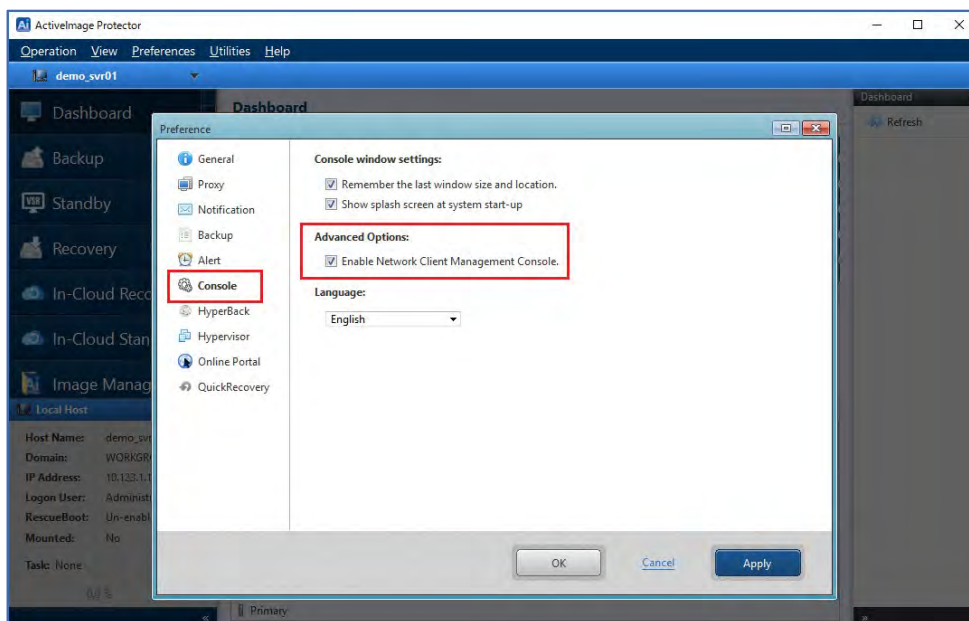
\*In this example, the following ports are opened in Security Settings for AWS instance.

- TCP port 48236
- UDP port 48238
- UDP port 48239

- (1) Please use the following operating procedures to launch ActiVImage Protector's console window.

Click **[Actiphy]** – **[ActiVImage Protector]** in Windows Start menu.

- (2) First, in order to launch ActiVImage Protector's Remote Management console, go to **[Preference]** - **[Console Window Settings]** and check in the checkbox for **[Enable Network Client Management Console]** and click **[Apply]** button. Click **[OK]** and the system will take you back to the Dashboard.

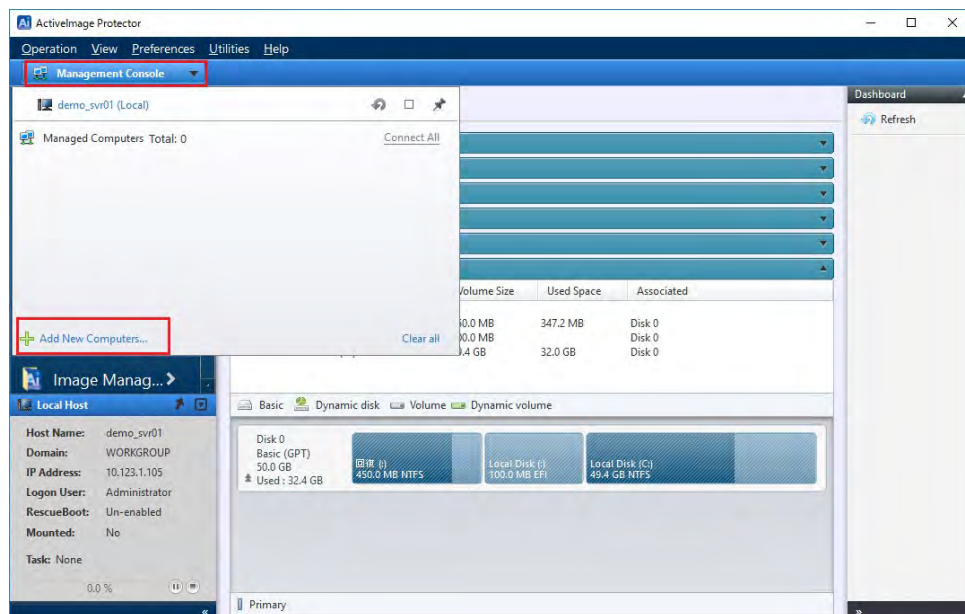


## Restore

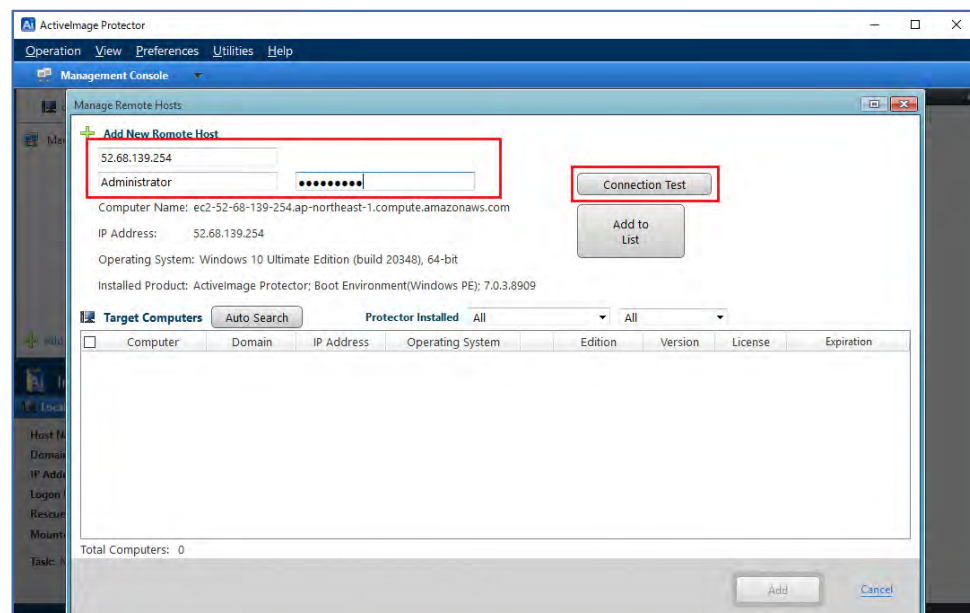
- (3) Click **[Management Console]** located in the upper left of the window.

Before using the Remote Management feature, you need to add any clients you wish to manage to the list of Managed Computers.

Click **[Add New Computers]**.

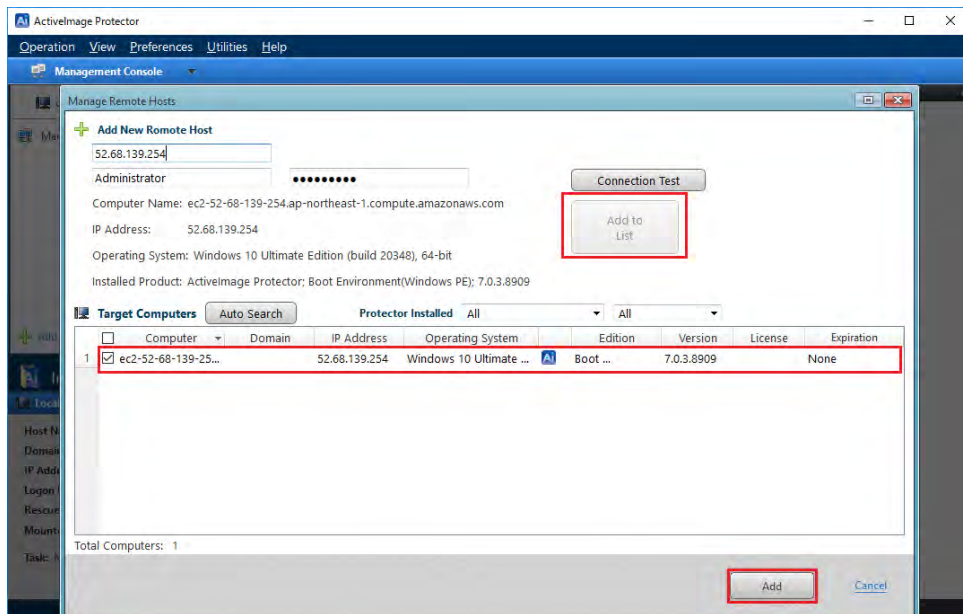


- (4) You need to select restore target virtual machine on which boot environment is booted. Enter **[Public IP Address]** of the instance, Administrator's **[User Name]** and **[Password]** and click **[Connect Test]** in **[Add New Remote Host]** dialog. When the connection test succeeds, **[Host Name]**, **[IP address]** and **[Installed Product]** (Actiphy Boot Environment) are displayed.

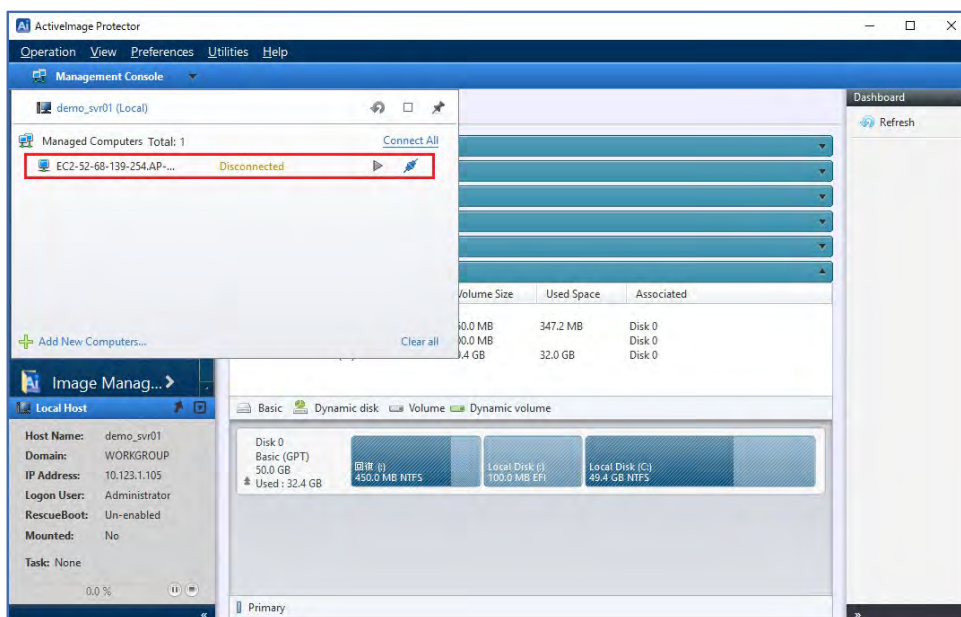


## Restore

- (5) Click **[Add to list]** and the remote host is added to the list of **[Target Computers]**. Click **[Add]** and the target remote host is added to the list of Managed Computers.



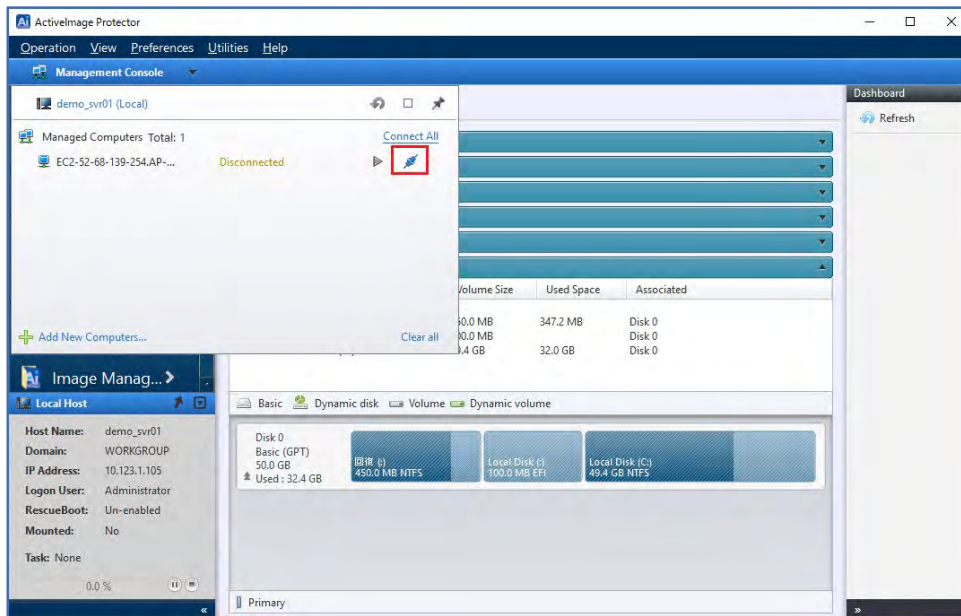
- (6) The remote host is added as a managed computer.



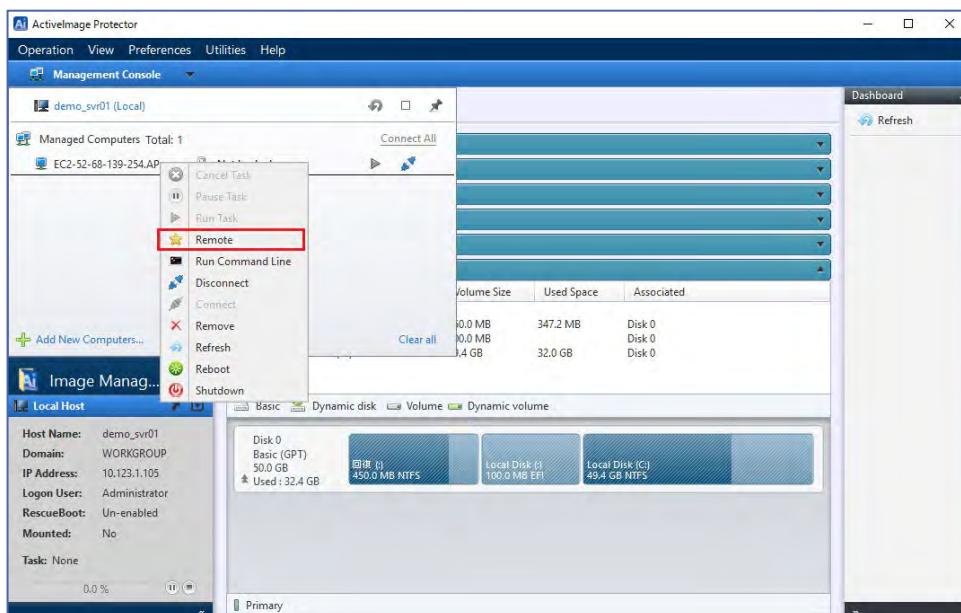


## Restore

- (7) Select and right-click on a host in the host list. The following context menu is displayed. Click the Connector mark.



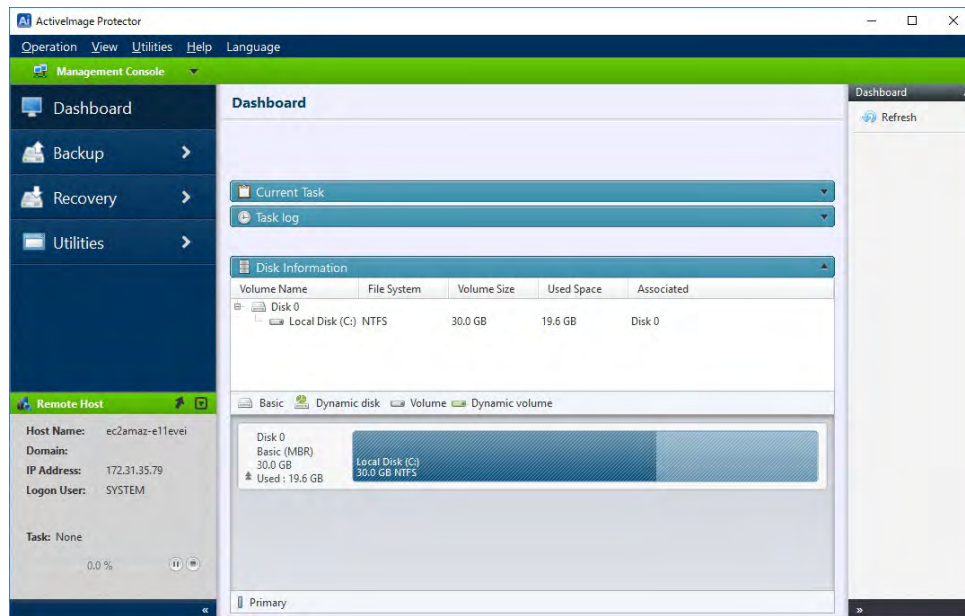
- (8) Select a host in the host list and click **[Remote]** in the right-click menu. The connection from Management Console window to the boot environment is established.



## Restore

(9) When the connection is successfully established, the status bar is green.

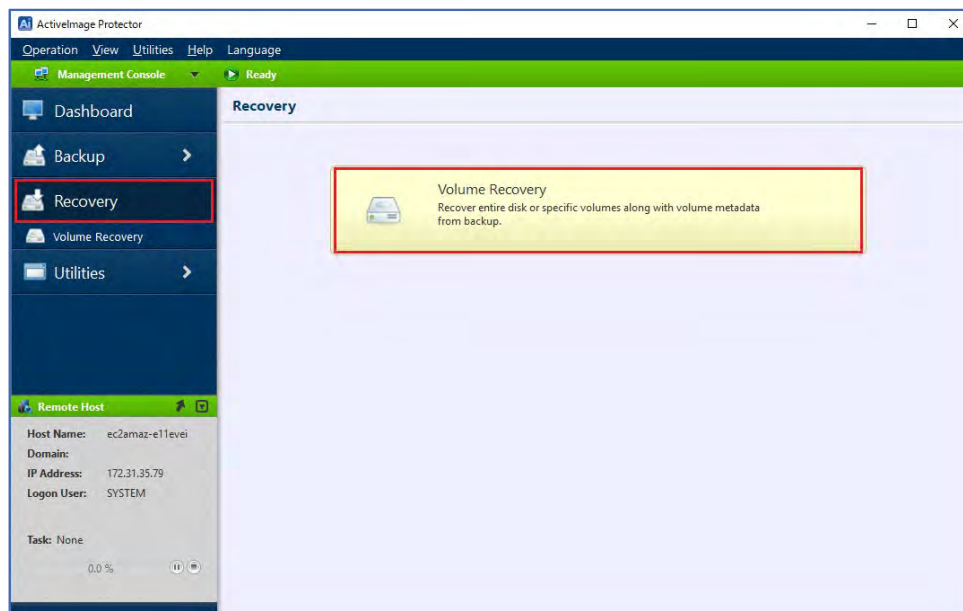
\*When disconnecting the access to remote host, double-click the local host name.



### 3. System Recovery

The following is an explanation of performing a restore operation from remote Management Console while accessing the boot environment on the remote host.

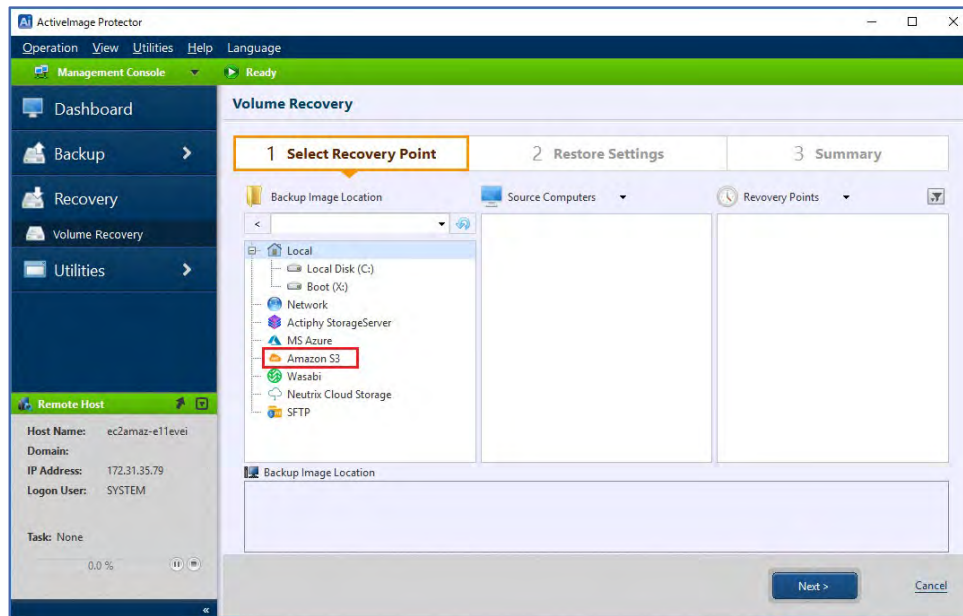
(1) Select **[Recovery]** – **[Volume Recovery]**.



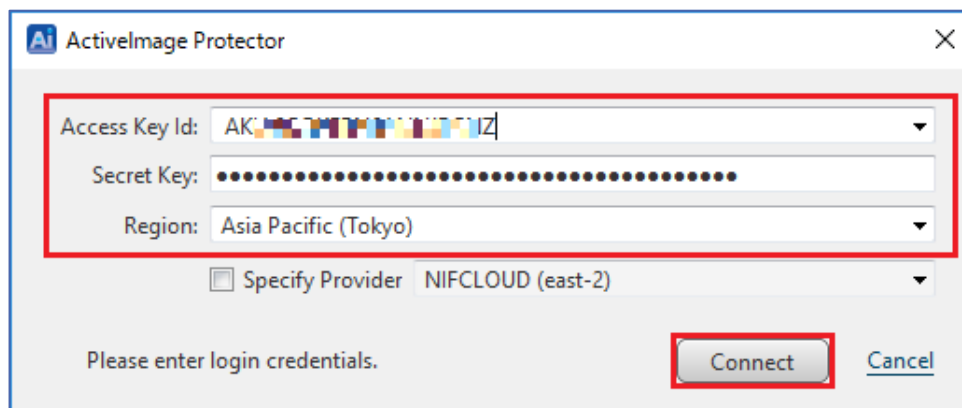
## Restore

- (2) Select the backup destination for the virtual machine to restore.

In this example **[Amazon S3]** is selected for **[Backup Destination]**.



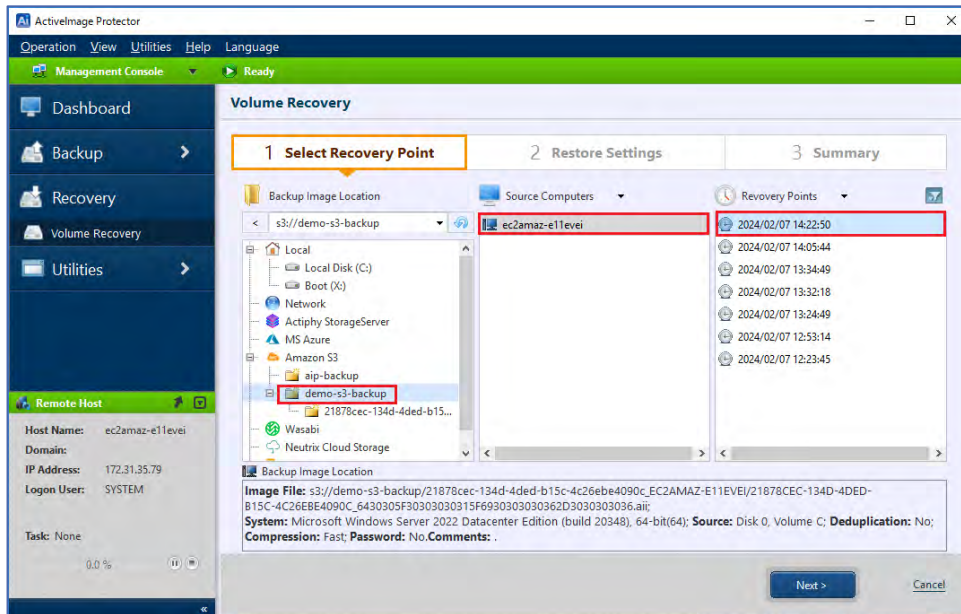
- (3) Enter AWS **[Access Key ID]** and **[Secret Key]** for Amazon S3. Select **[Region]** and click **[Connect]**. Or click **[▼]** to the right of the text box for **[Access Key ID]**. The destinations previously selected in the backup processes and backup tasks are listed. You can select one from the list.



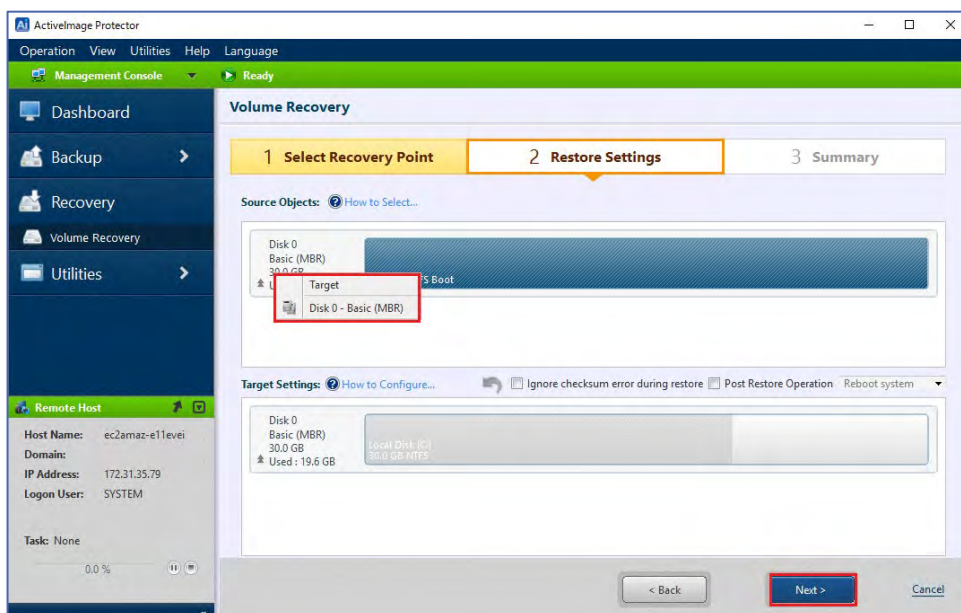


## Restore

- (4) Select **[Folder]** – **[Computer]** – **[Recovery Point]** and click **[Next]**.

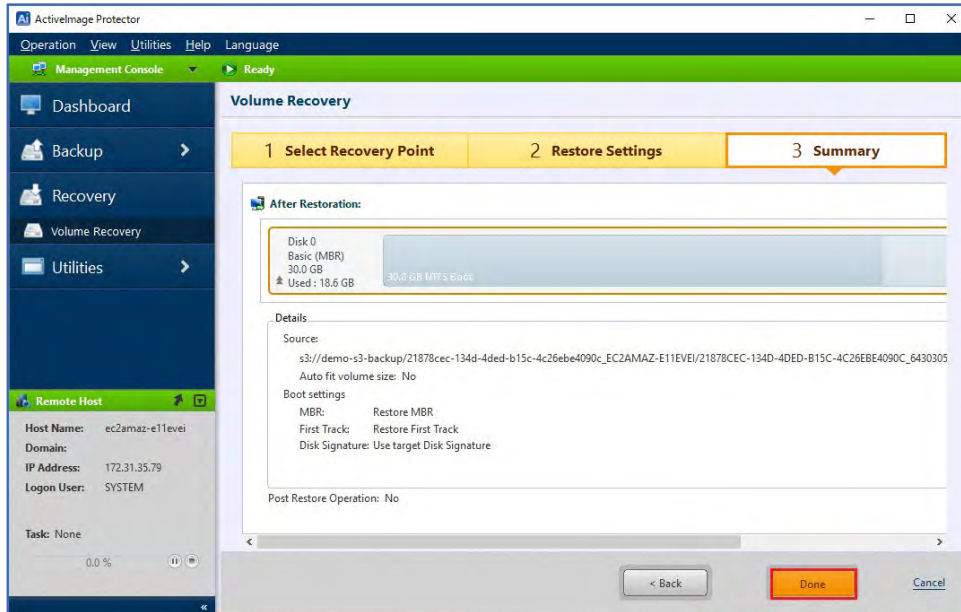


- (5) Right-click on the left part of disk map in **[Source Objects]**. From the context menu select **[Disk 0 – Basic (MBR)]** for **[Target]**. The details are displayed in **[Target Settings]**. Click **[Next]**.

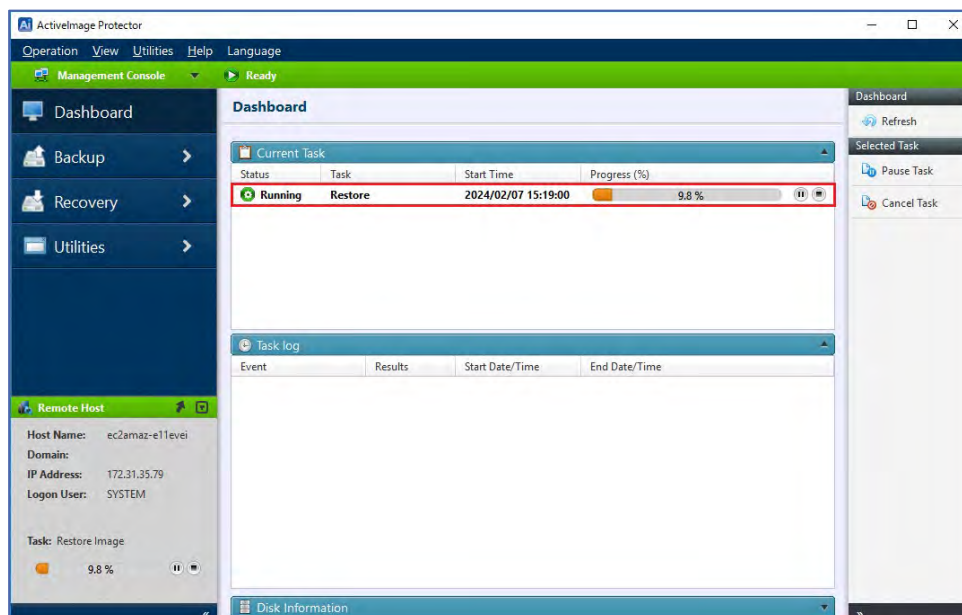


## Restore

- (6) Please review the configured settings in the **[Summary]** window. Click **[Done]**.

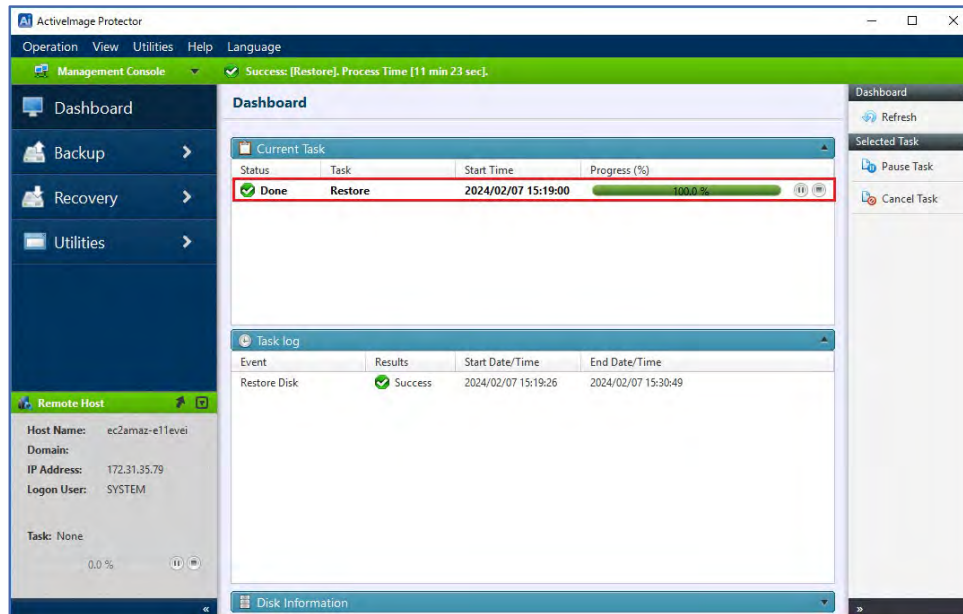


- (7) When the recovery task starts, the progress is displayed.

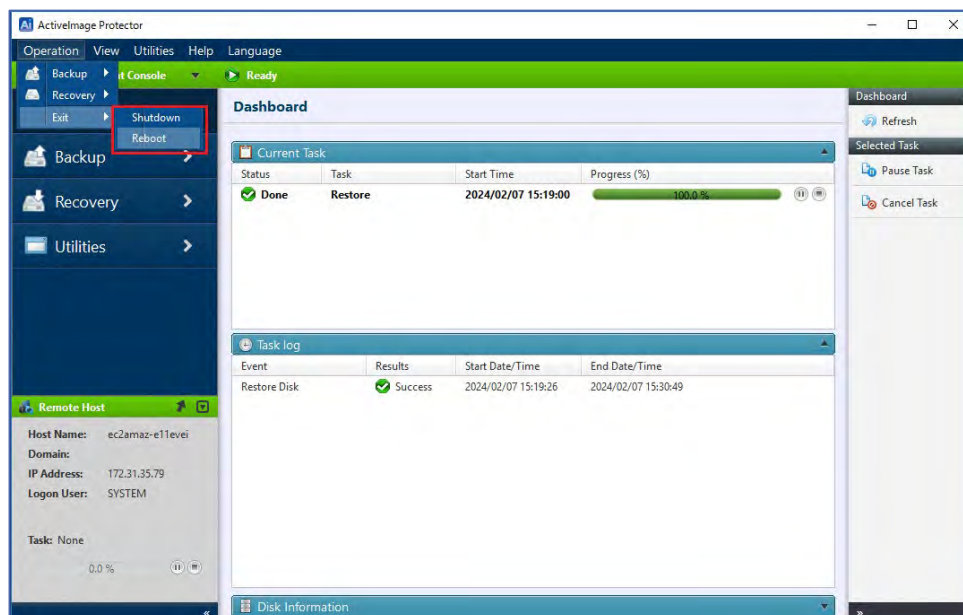


## Restore

- (8) When the Progress reaches “100%”, the recovery task for cloud virtual machine has completed.

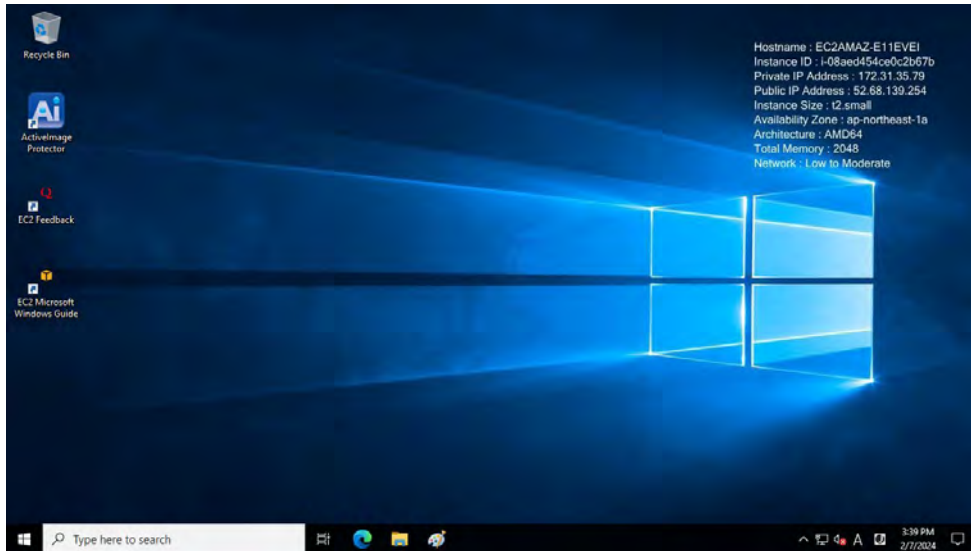


- (9) Click on **[Operation]** - **[End]** to shut down or reboot the machine.



## Restore

(10) Please access the restored virtual machine and make sure recovery process successfully completed.



## 5. In-Cloud Standby

In-Cloud Standby feature creates snapshots on a predetermined schedule for machine instances that exist on Amazon Web Service (AWS) or Microsoft Azure. If an emergency arises, the snapshot is available in the cloud for booting and instance to a specific point in time.

The following explains how to use this feature in a system recovery scenario including how to create a backup snapshots from an instance of AWS EC2, create a volume from a snapshot by using AWS management console, attach the volume to a newly created instance.

### 5-1. Create a snapshot from a backup file

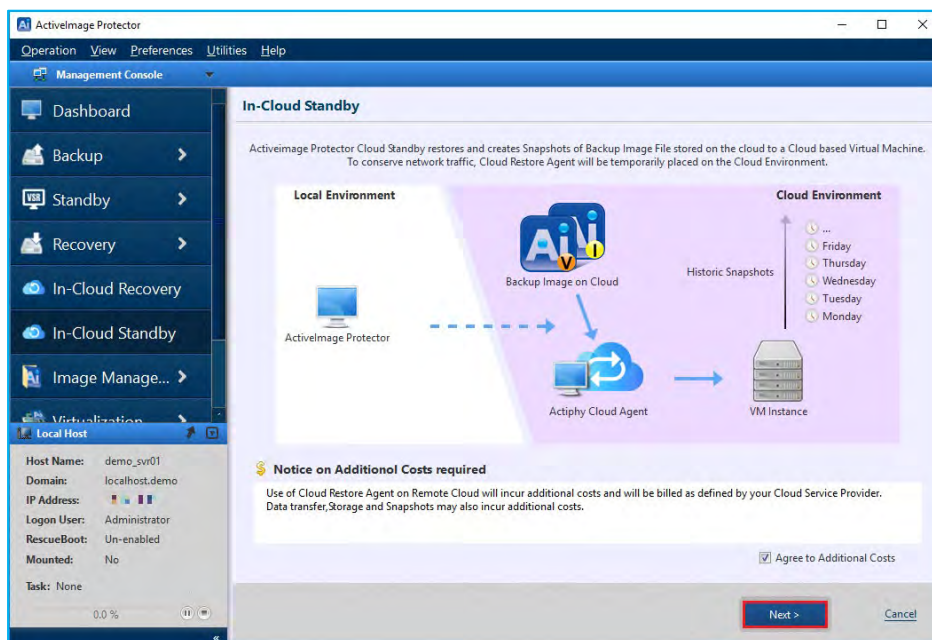
**Note:** To create snapshots using the In-Cloud Standby feature, the backup image files from which the snapshots are created require that the option **[Make backup image Cloud Standby ready]** is enabled.

Please refer to section **3-2 Volume Backup: Scheduled Backups** of this document for more information.

1. Start ActiveImage Protector. Go to Windows Start menu - **[Actiphy]** → **[ActiveImage Protector]**.

Select **[In-Cloud Standby]** in the left menu.

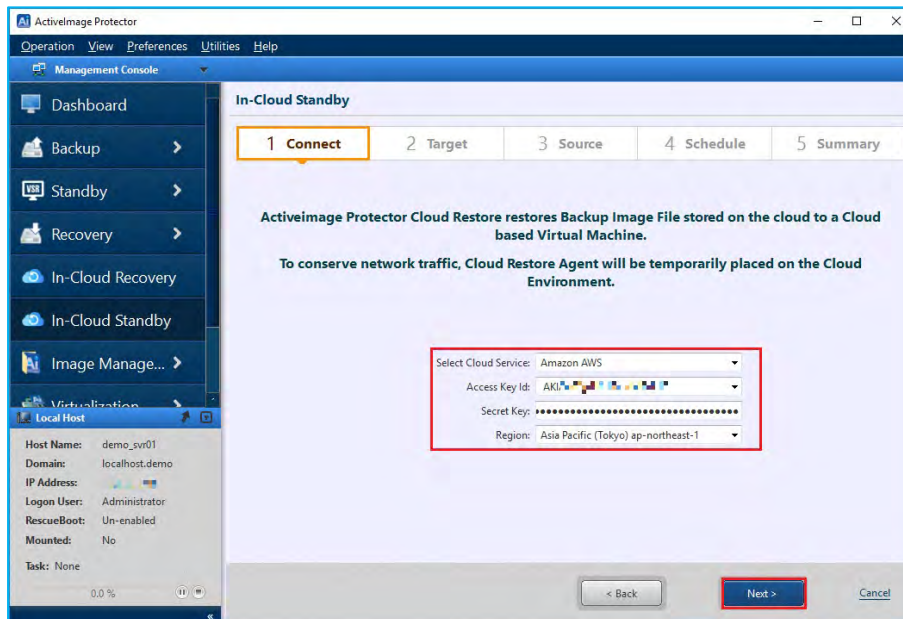
**Note:** The use of any of the cloud services may incur additional costs and will be billed as defined by your Cloud Service Provider. In addition a temporary appliance called "Actiphy Cloud agent" will be deployed in the respective regions in cloud environment. Data transfer and storage for a volumes created in restore process may also incur additional costs as determined by the cloud provider. To proceed with operation, please click the checkbox to **[Agree to additional cost]** and click **[Next]**.



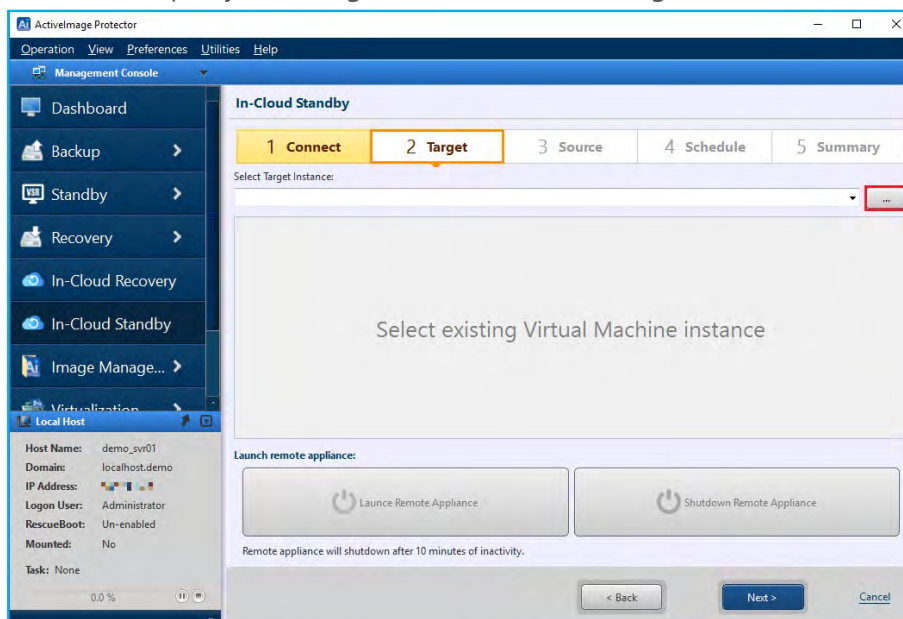


2. Select the cloud service and enter credential information.

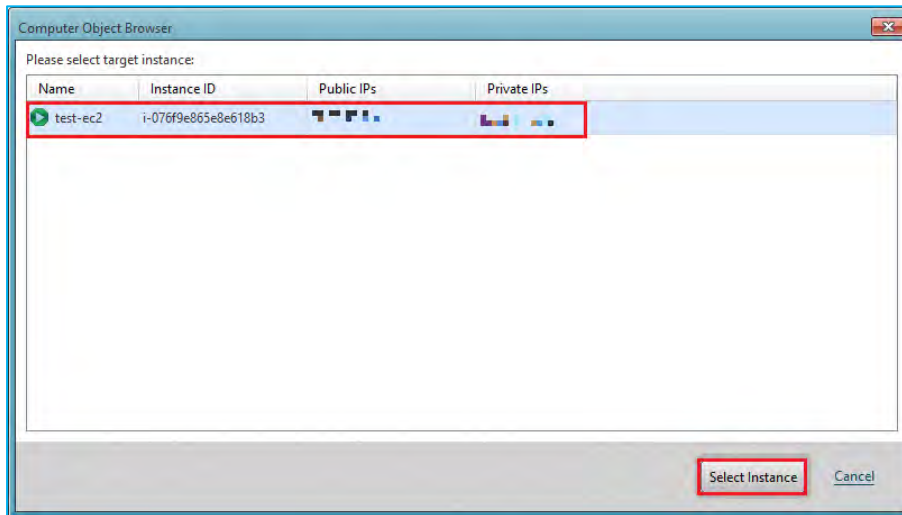
In this example we have selected **[Amazon AWS]** for **[Select Cloud Service]** and entered **[Access Key]** and **[Secret Key]** for AWS. Select **[Region]** and click **[Next]**.



3. Click **[...]** and specify an existing instance as the restore target. Please make sure that the instance is not running.

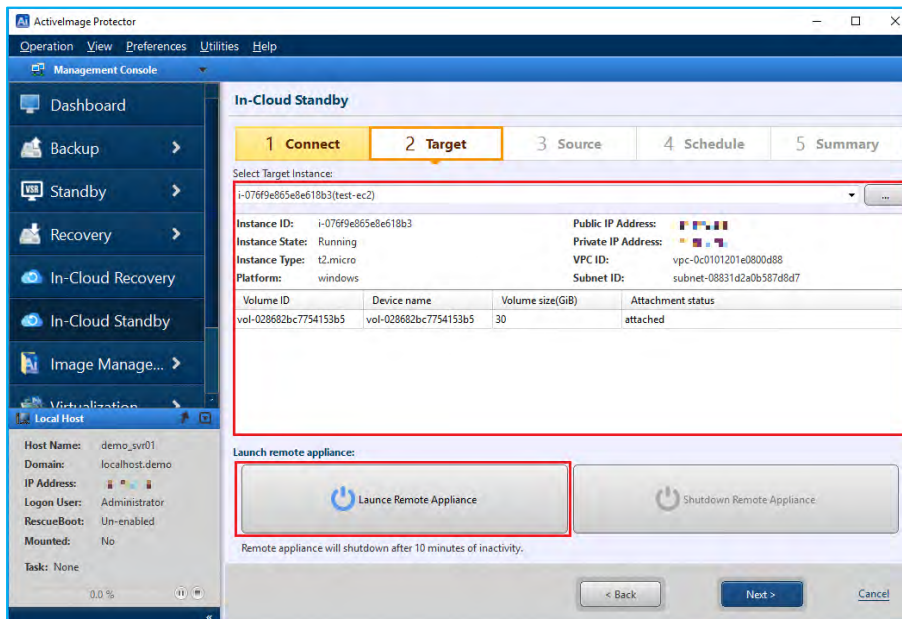


4. Select the instance. In this example, we selected “test-ec2” for the backup source instance. Click **[Select]**.

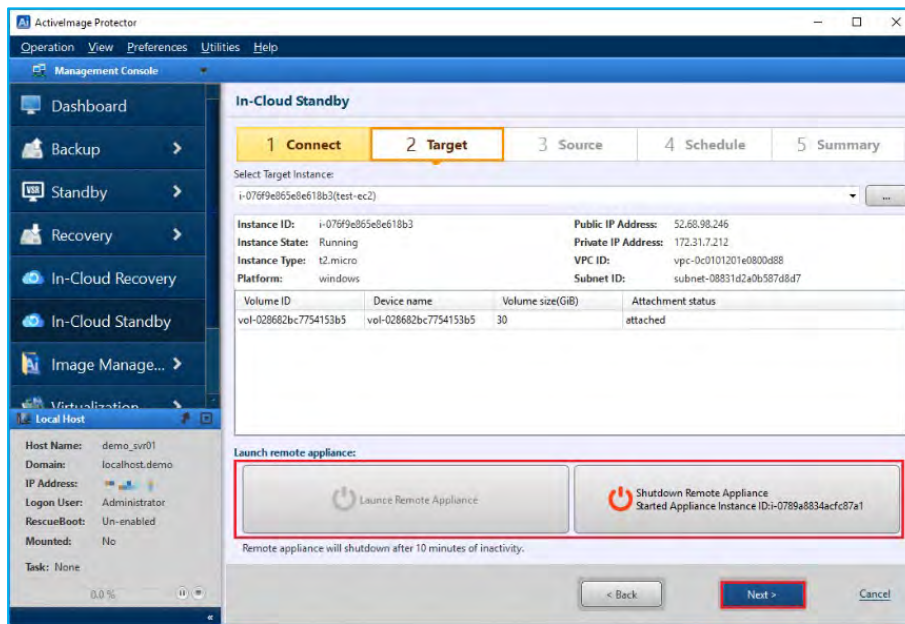


5. The information of the instance is displayed. Click **[Launch Remote Appliance]** to boot **[Actiphy Cloud agent (boot environment)]**.

Please wait ...



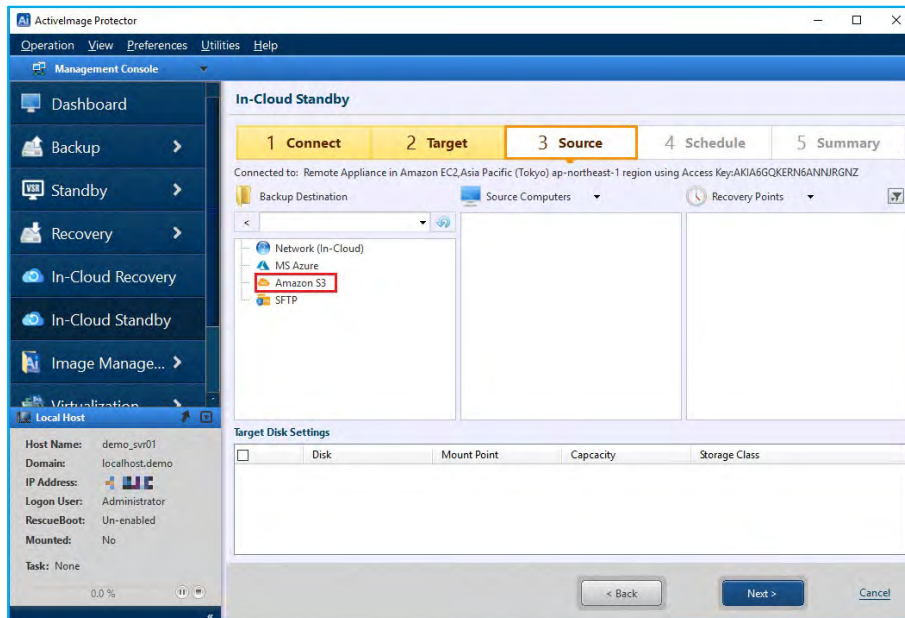
6. When **[Launch Remote Appliance]** is grayed out and **[Shutdown Remote Appliance]** is enabled, “**ActiPHY Cloud Agent (boot environment)**” is running. Click **[Next]**.



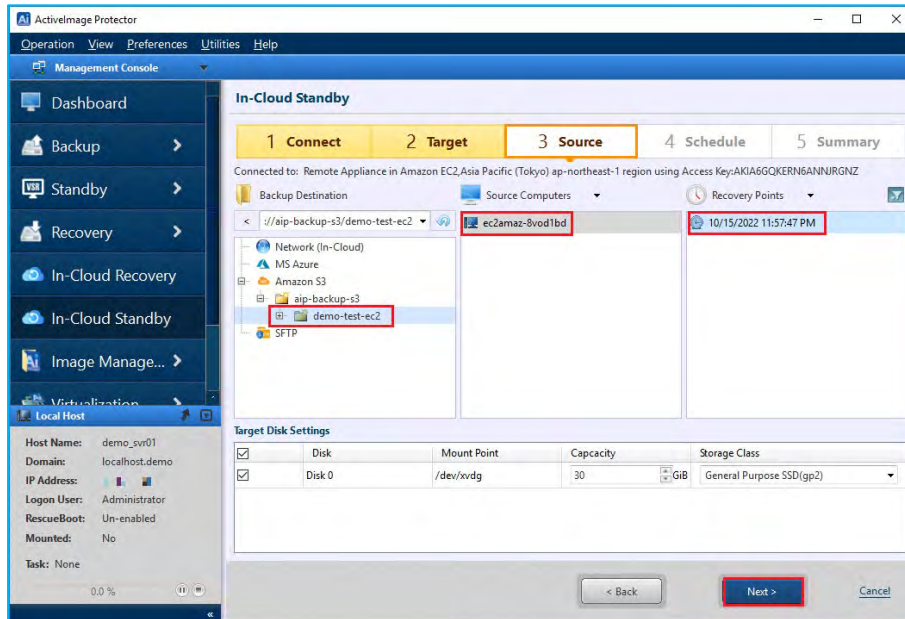
7. Please specify the location of the backup files.

In this example we have selected **[Amazon S3]** for **[Backup Destination]**.

When you are prompted to enter the credential information for Amazon S3, please enter **[Access Key]** and **[Secret Key]** to access AWS. Select **[Region]** and click **[Connect]**.



8. Please select **[Folder]** -> **[Source Computer]** -> **[Recovery Point]** (base backup) and click **[Next]**.

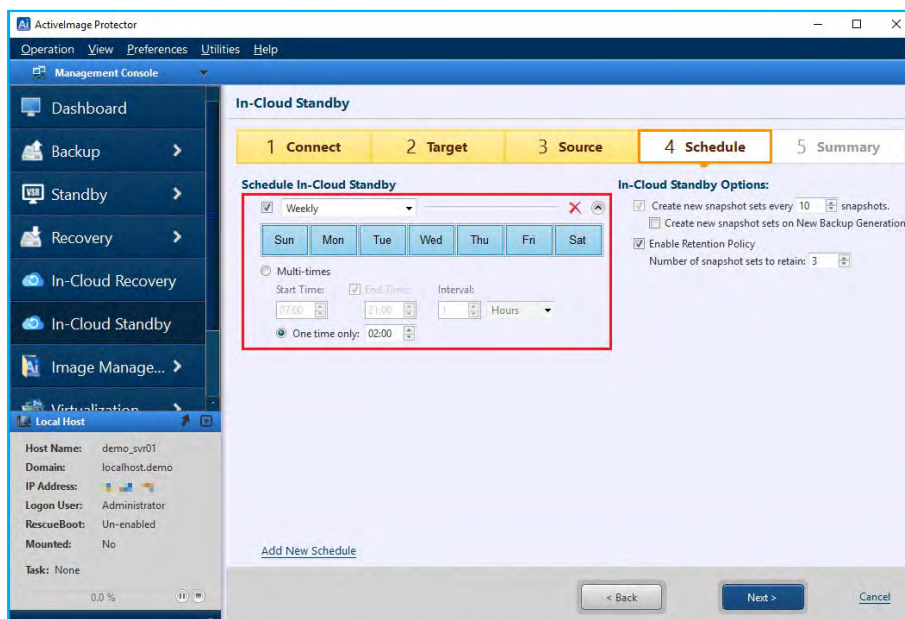


9. Please select the schedule type. Options include **[Weekly]**, **[Monthly]**, **[Designate Specific Days]**.

The steps below shows an example of configuring a weekly schedule:

- Under **[Schedule In-Cloud Standby]**, use the drop-down menu to select the schedule type for the designated interval for creating snapshots.
- Set the snapshot schedule to **[Weekly]**.
- Specify the daily interval of snapshots created by clicking specific days of the week.
- Set the execute time interval for **[One Time Only]** at 2:00am.

Virtual snapshots are created on the instance based on the In-Cloud Standby Schedule when a new full or incremental backup file(s) is detected. If multiple new backup files are detected at the time of the scheduled task, then snapshots are created for each file. If there are no new backup or incremental files available, the scheduled task is skipped.





10. The following example explains the configuration settings for the Retention Policy.

**(1) Create a snapshot set for a designated number of snapshots taken:**

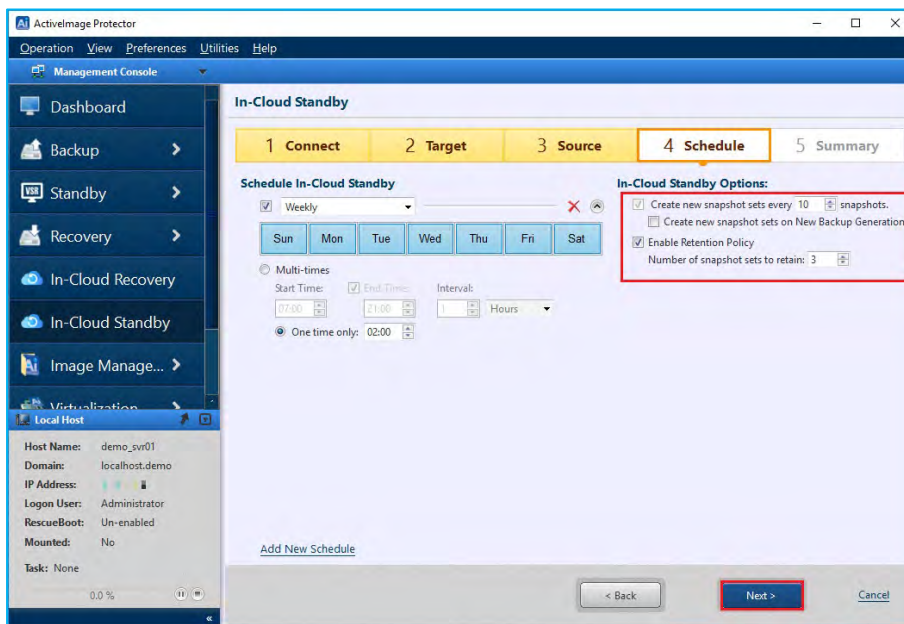
When enabled, a new virtual snapshot set is created every time the designated number of snapshots have reached that designated threshold.

**(2) Enable Retention Policy**

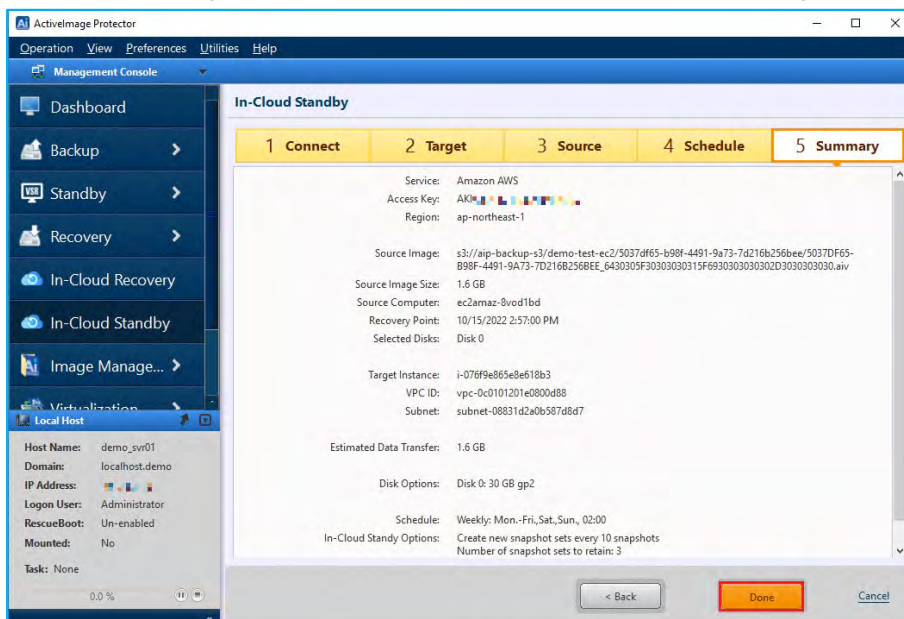
Specify the number of snapshot sets to retain. This example shows by default that the last three snapshot sets are retained in the cloud.

**Note:** When a fourth snapshot set is created, then the oldest set is deleted.

Once configured, click **[Next]**.



11. Confirm the settings in the Summary window. If satisfied with the configuration, click **[Done]**.



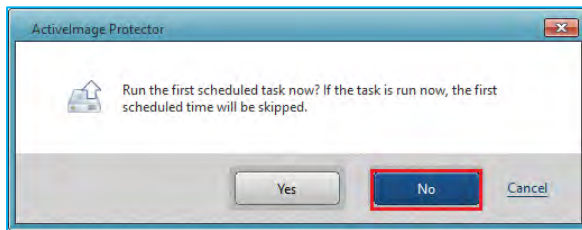
12. A dialog box is displayed asking if you would like to run the initial snapshot creation task now.

By clicking **[No]**, the system returns to the dashboard, and your initial snapshot creation task will run according to the configured schedule.

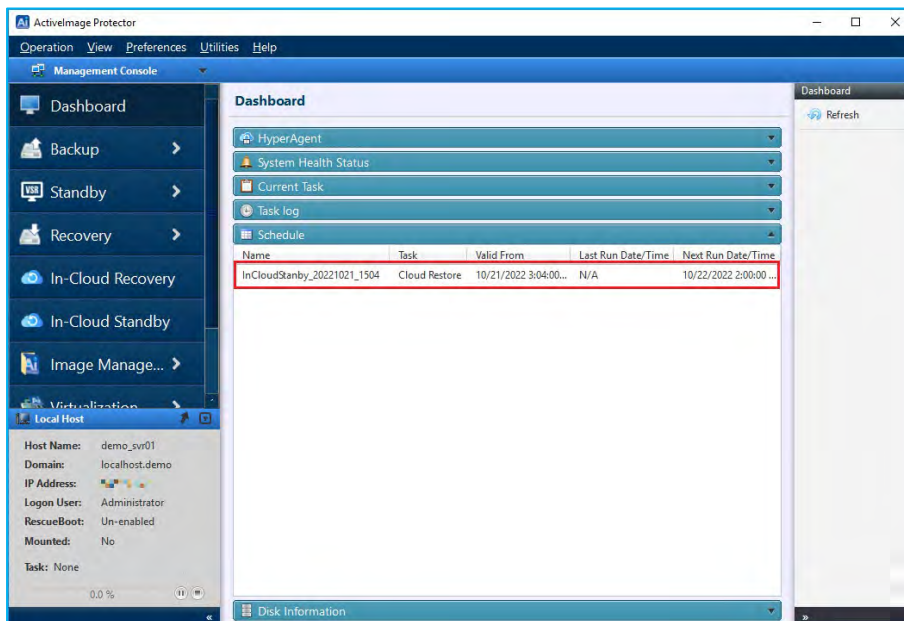


## In-Cloud Standby

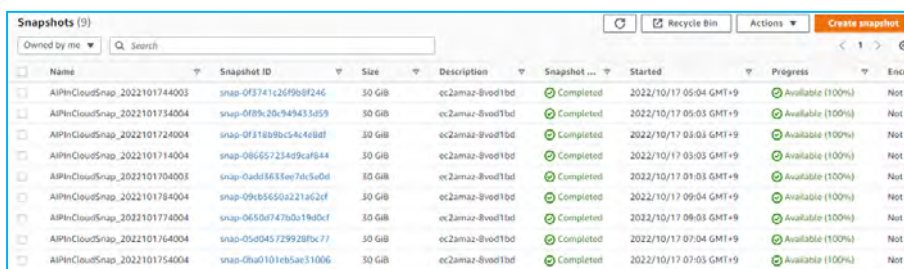
By clicking **[Yes]**, the system will run the initial snapshot creation task immediately and will thus skip the first scheduled task.



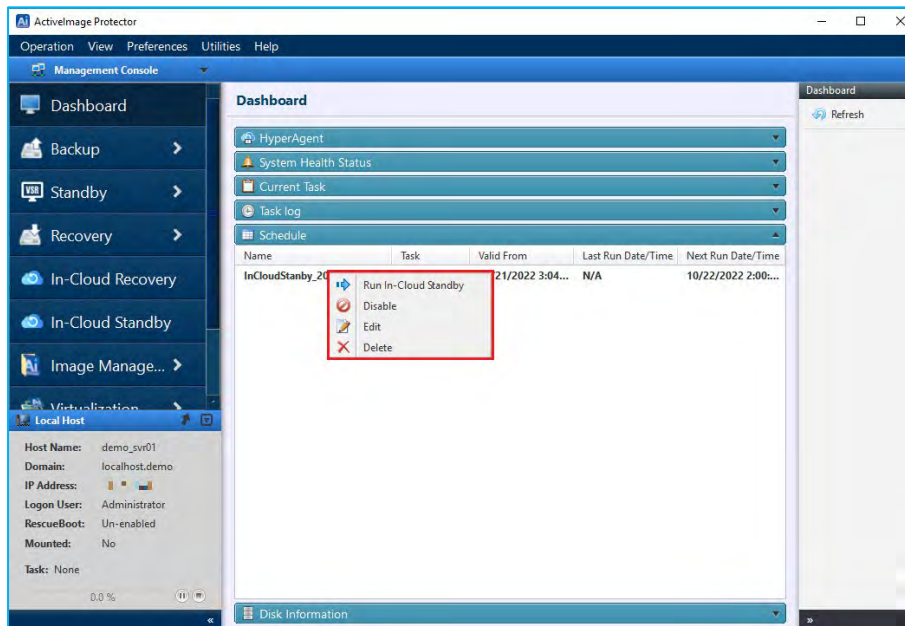
13. Go to the **[Dashboard]** and expand the **[Schedule]** tab to modify or monitor your scheduled tasks. A snapshot is created from a backup based on the predefined backup schedule.



14. In this example, the created snapshot is named accordingly using this naming convention: **[AIPInCloudSnap\_YYYYMMDDhhmmss]**.



15. You can run tasks immediately or edit settings by right-clicking on the **[Schedule Name]**.



## 5-2. Create a volume from a snapshot and attach to newly created instance

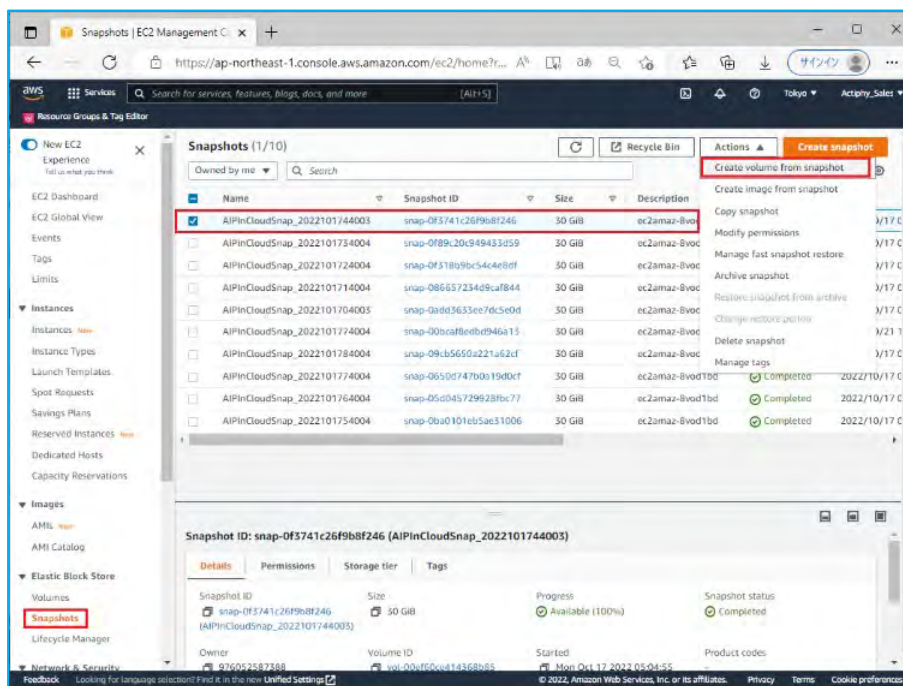
The following explains how to do a system recovery, including how to create a volume from the Cloud Standby snapshot and attaching the volume to a newly created instance.

\*AWS Management Console screens may have changed from the time of this documents creation, however the following explains the basic instructions even if the user interfaces have changed.

### 1. Create a volume from the snapshot.

Please select **[EC2] -> [Snapshot]** from the menu on AWS management console. Check in the checkbox for the snapshot created at the point of time to restore to. Click **[Create volume from snapshot]** in the pull-down menu of **[Action]**.

In this example we have selected the latest snapshot of the host “ec2amaz-8vod1bd” created by In-cloud Standby.



2. Configure the settings in **[Create volume]** window.

**(1) Volume settings**

Please specify the same availability zone as the target instance to attach the volume. In this example, we selected “ap-northeast-1c” for **[Availability Zone]**. No changes are made to the other default settings.

**Create volume** [Info](#)

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

**Volume settings**

Snapshot ID  
 snap-0f3741c26f9b8f246 (AIPlnCloudSnap\_2022101744003)

Volume type [Info](#)  
General Purpose SSD (gp2)

Size (GiB) [Info](#)  
30  
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS  
100 / 3000  
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) [Info](#)  
Not applicable

Availability Zone [Info](#)  
ap-northeast-1c

Fast snapshot restore [Info](#)  
 Not enabled for selected snapshot

Encryption [Info](#)  
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances...  
☐ Encrypt this volume

**(2) Tags - optional**

In this example, we specified “Name” for **[Key]** and “test-ec2-standby” for **[Value - optional]**. After configuring the settings, click **[Create volume]** button.

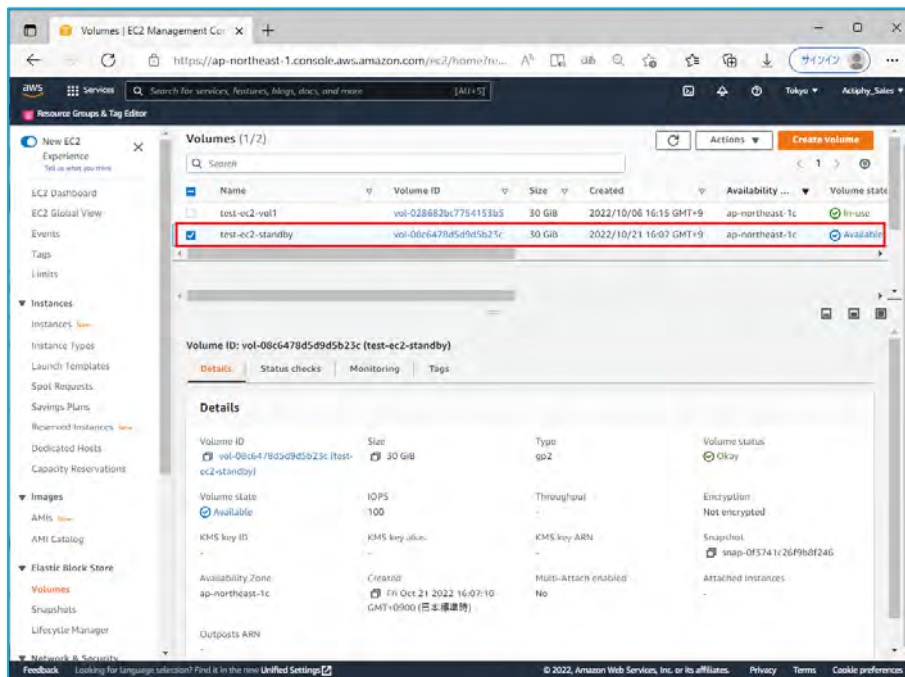
**Tags - optional** [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	test-ec2-standby	Remove

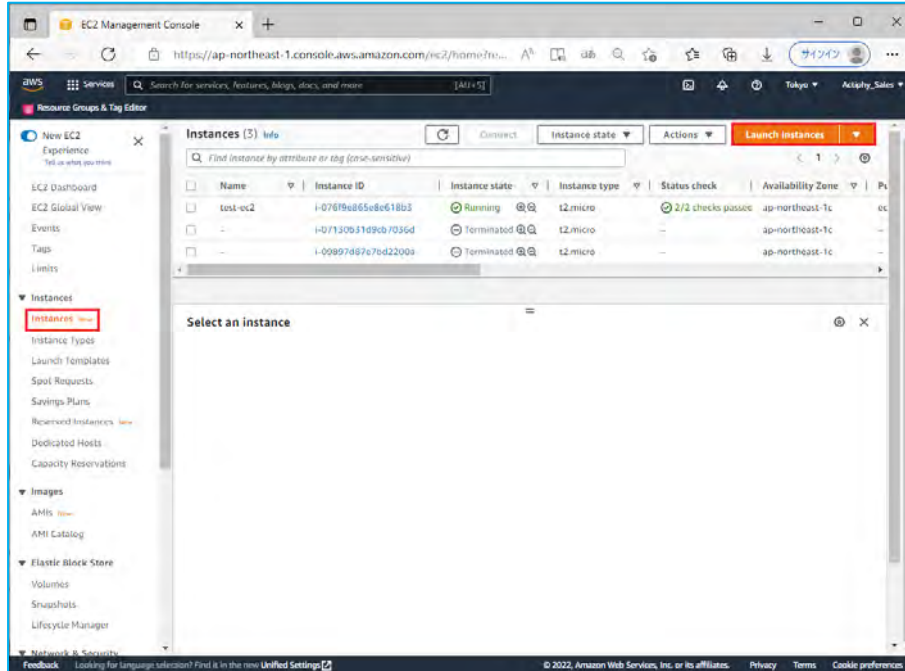
You can add 49 more tags.

### (3) The volume named “test-ec2-standby” is created.



### 3. Create a new instance.

Go to AWS Management Console and select **[EC2] -> [Instance]** in the menu. Click **[Launch Instances]** to display the window for creating an instance.





- (1) In **[Name and tags]**, please specify any name of the instance. In this example, specified “test-ec2-standby” for the name of the instance.

**Name and tags** [Info](#)

Name

test-ec2-standby [Add additional tags](#)

- (2) In **[Application and OS Images (Amazon Machine Image)]**, please select the backup image of the virtual machine. In this example, we selected “Windows\_Server 2016-Japanese-Full-Base” which is the same as the backup source instance.

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

AMI from catalog Recents Quick Start

Amazon Machine Image (AMI)

Windows\_Server-2016-Japanese-Full-Base-2022.09.14 [Verified provider](#)

ami-0e5e6cd3680e5aa0e [Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled
Community AMIs	2022-09-14T19:00:09.000Z	x86_64	hvm	ebs	Yes

- (3) Please select the instance type. In this example. We selected “t2.micro” with the same name as the backup source instance.

▼ **Instance type** [Info](#)

Instance type

t2.micro [Free tier eligible](#) [Compare instance types](#)

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0152 USD per Hour

On-Demand Windows pricing: 0.0198 USD per Hour

- (4) In **[Key pair (login)]** window, select key pair. In this example, we selected the existing key pair “test-ec2-key” named the same as backup source instance.

**▼ Key pair (login)** Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

test-ec2-key ▼

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

- (5) In **[Network settings]** window, specify the security group. In this example, the existing security group same as the backup source instance is selected.

**▼ Network settings** Info Edit

Network Info

vpc-0c0101201e0800d88 | test-ec2-vpc

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

**Firewall (security groups)** Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups Info

Select security groups ▼

launch-wizard-1 sg-0ab413092c7e90814 X  
VPC: vpc-0c0101201e0800d88

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

- (6) In **[Configure storage]** window, you do not need to change the default settings. When you have finished configuring the instance, click **[Launch Instance]** to begin the creation process of the instance.

**▼ Configure storage** Info Advanced

1x 30 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems Edit

**► Advanced details** Info

t2.micro

Firewall (security group)

launch-wizard-1

Storage (volumes)

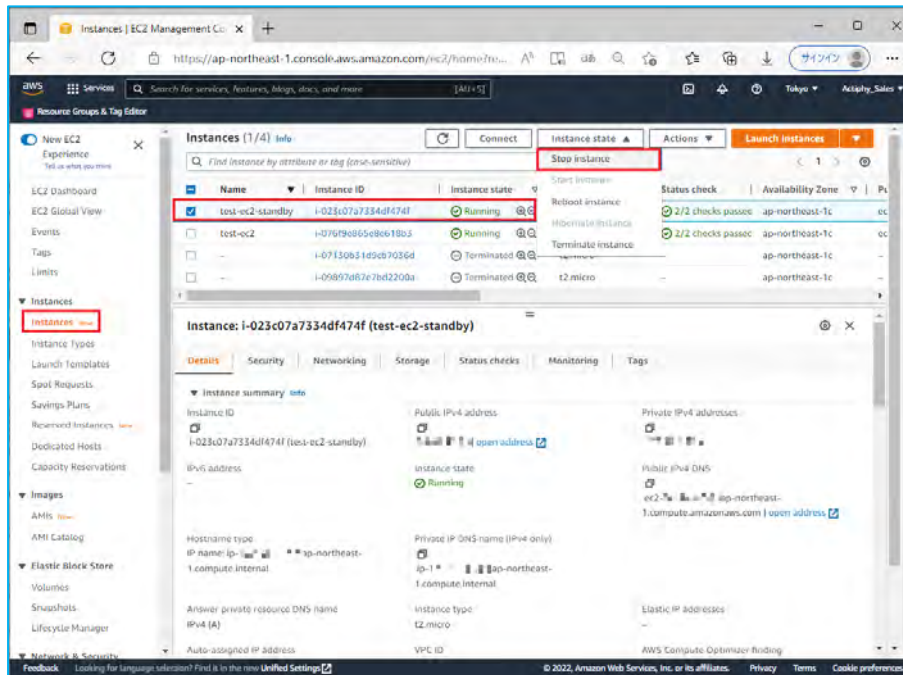
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. X

Cancel Launch Instance

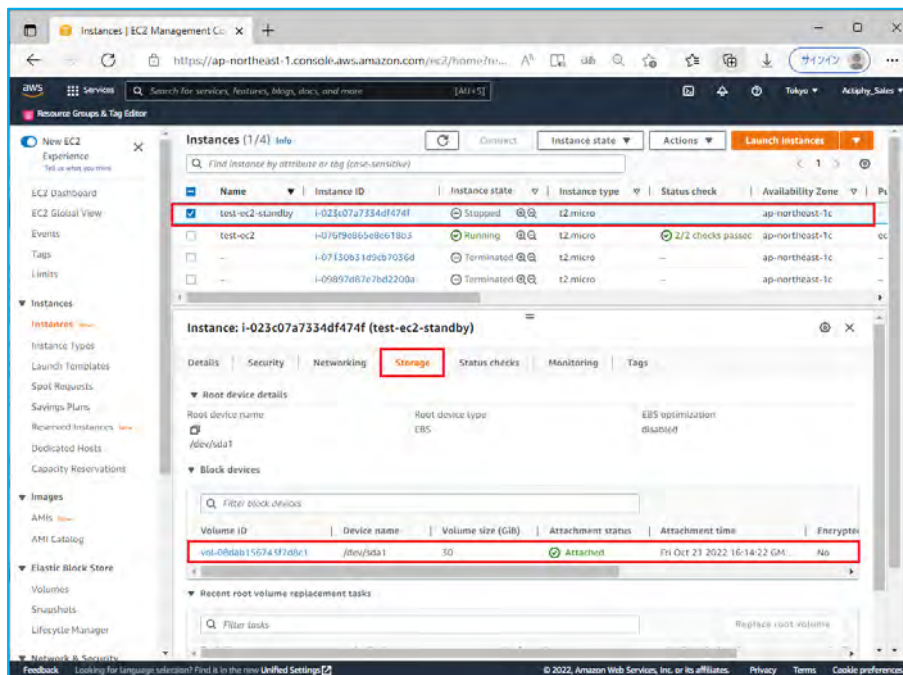
- Before replacing the volumes, stop the newly created instance.

In this example, we selected **[Instance]**, check in the checkbox for the newly created instance “test-ec2-standby” and click **[Stop Instance]** in the pull-down menu of **[Instance State]**.

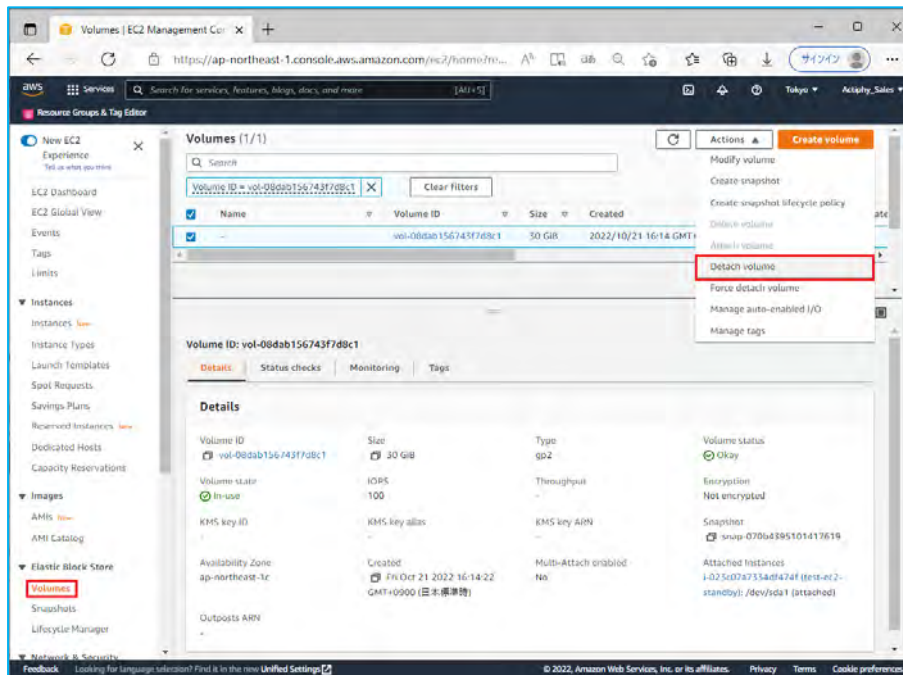


- Detach the root volume of the newly created instance.

Before detaching the root volume, check the root device name (in this example, “/dev/sda1”) in **[Storage]** tab of the instance and click **[Volume ID]**.

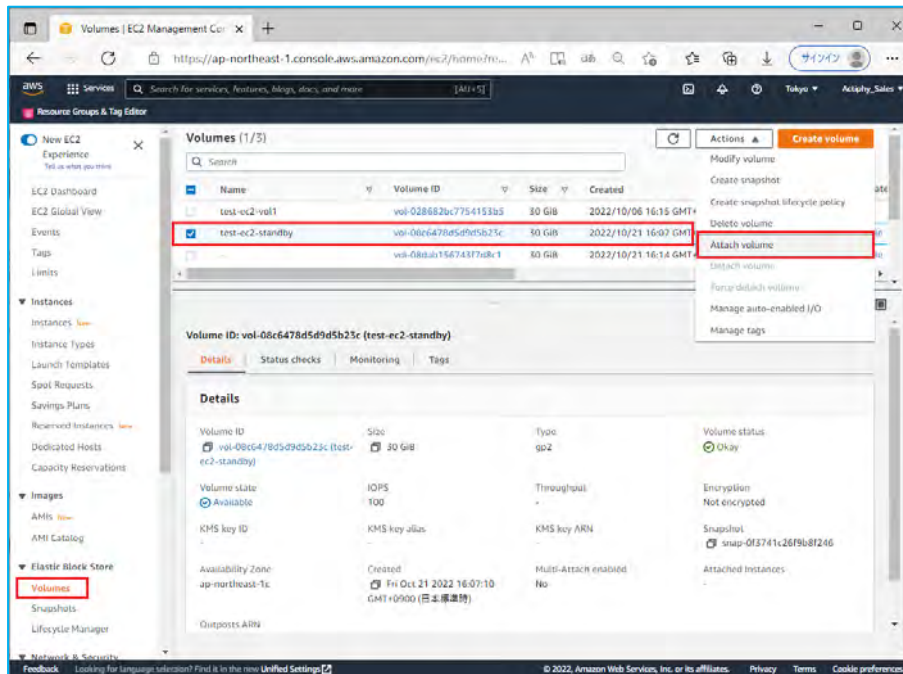


6. When **[Volumes]** window is displayed, click **[Detach volume]** in the pull-down menu of **[Action]**.



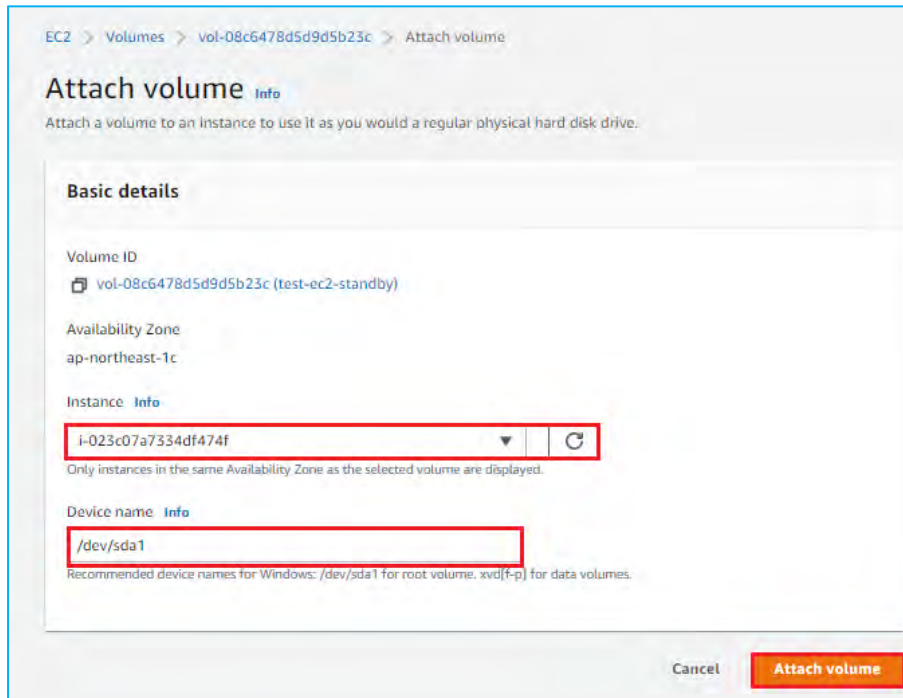
7. Attach the volume created from a snapshot.

Go to AWS Management Console and select **[EC2]** -> **[Volume]** in the menu. Check in the checkbox for the volume created from a snapshot. Click **[Attach Volume]** in the pull-down menu of **[Action]**.

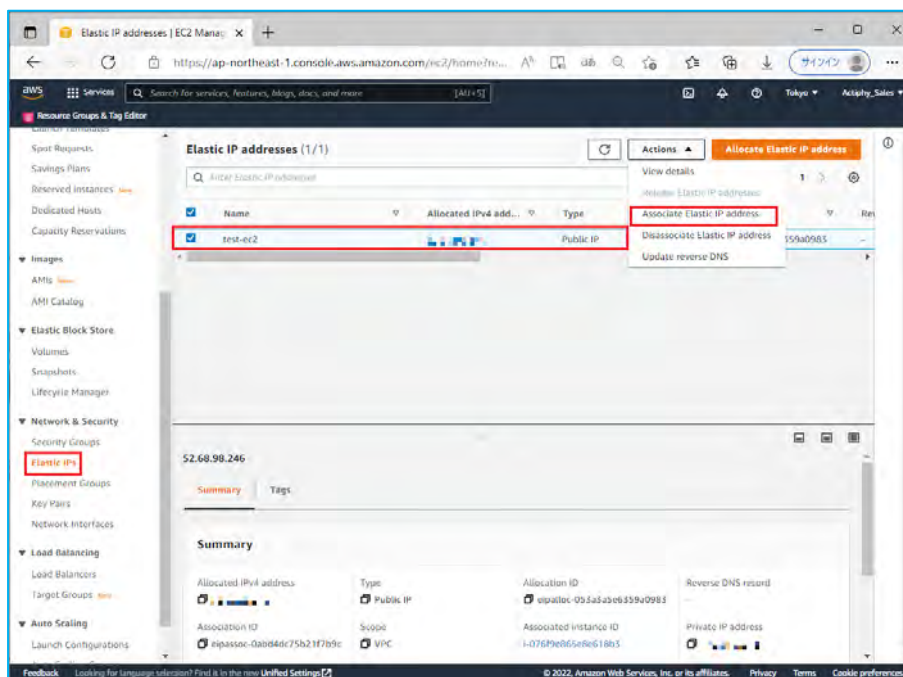




- Attach the created volume to the newly created instance. The device name is “/dev/sda1” as identified above.

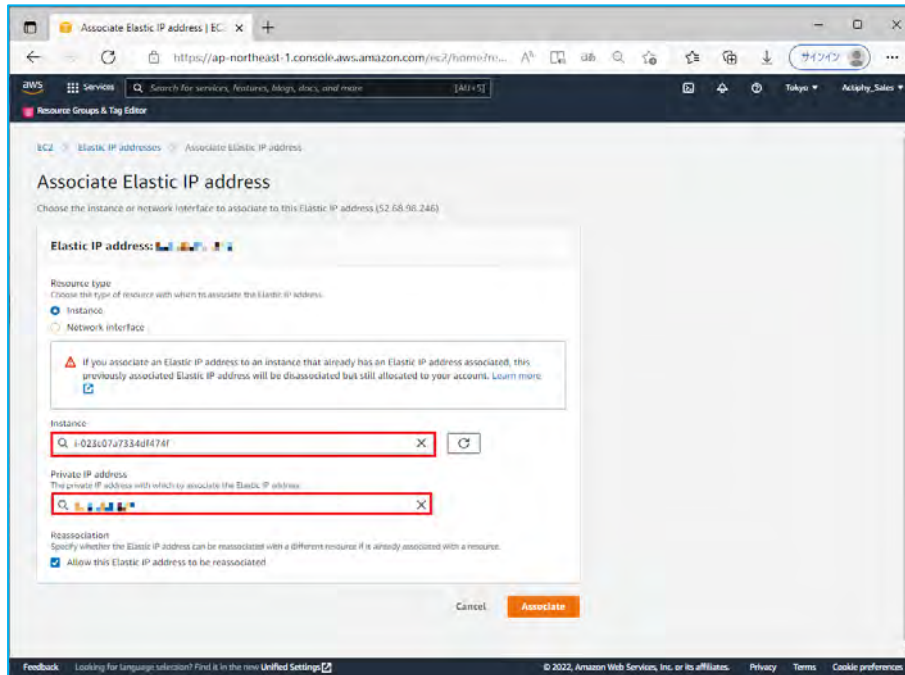


- Detach “Elastic IP” from the existing instance and attach it to the new instance.  
Go to AWS Management Console and select **[EC2]** -> **[Elastic IP]** in the menu. Check in the checkbox for “Elastic IP” attached to the existing instance and click **[Associate Elastic IP address]** from the pull-down menu of **[Action]**.



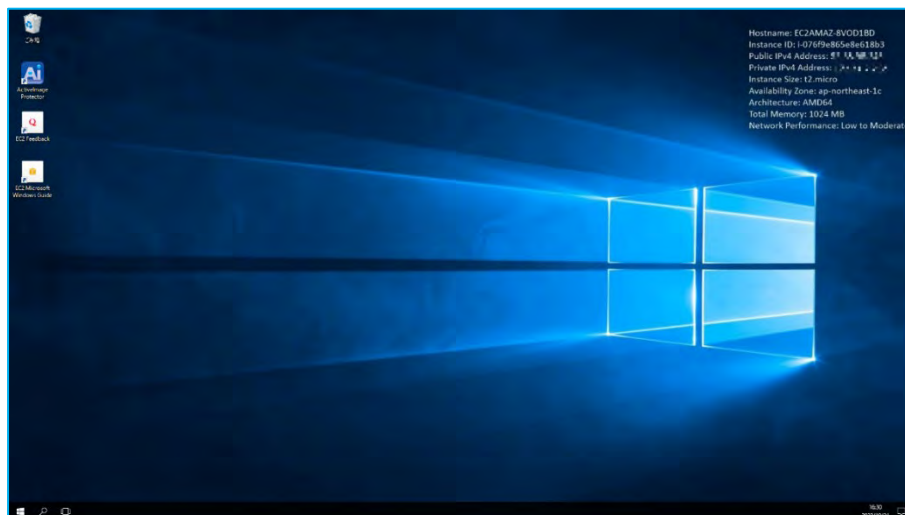


10. Select the newly created instance for **[Instance]**, check in the checkbox for **[Allow this Elastic IP address to be reassociated]** and click **[Associate]**.



11. Boot the newly created instance.

The snapshot created from backup is now restored to the new instance.



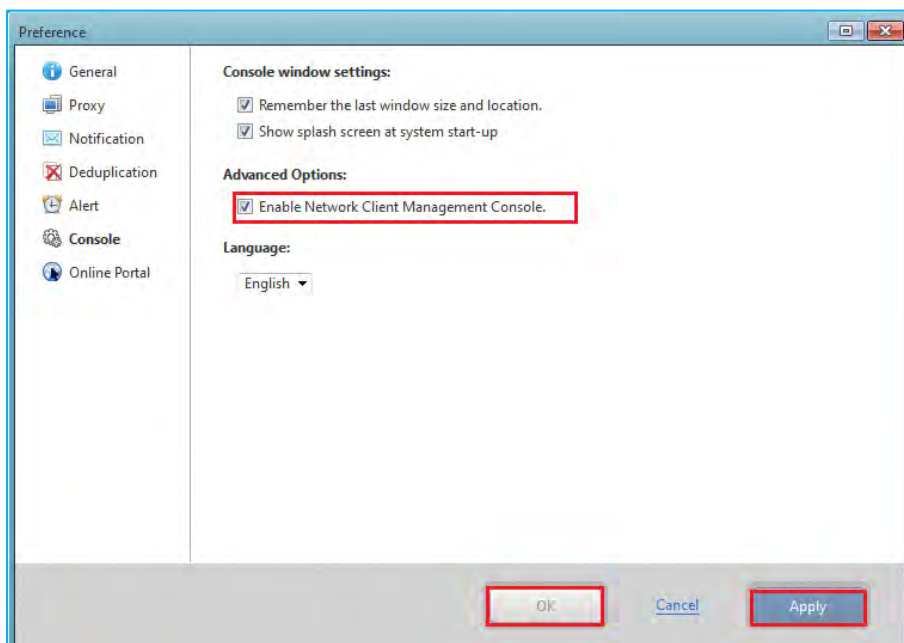
## 6. Remote Management Console

Remote Management Console enables you to remotely manage ActiveImage Protector agents installed on the instances of AWS EC2 and Azure.

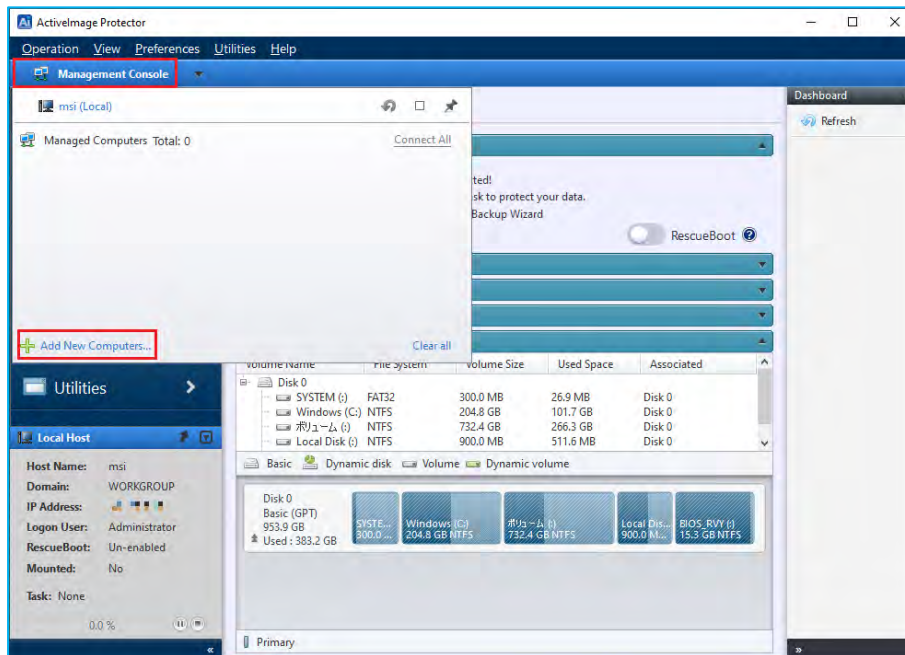
1. Launch ActiveImage Protector by clicking on the Windows Start menu and then navigating to **[Actiphy]** → **[ActiveImage Protector]**.
2. Go to **[Preference]** -> **[Console]**, check in the checkbox for **[Enable Network Client Management Console]** and click **[Apply]**. Click **[OK]** and the system will take you back to the Dashboard.

Please open the following ports in security settings for the instance (add them to the inbound rules of security policy with AWS.)

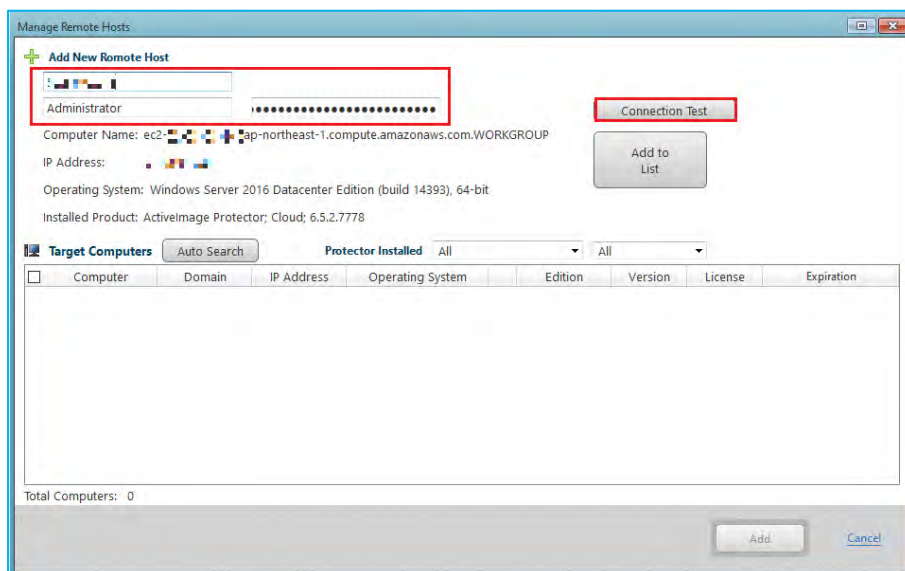
- TCP port 48236
- UDP port 48238
- UDP port 48239



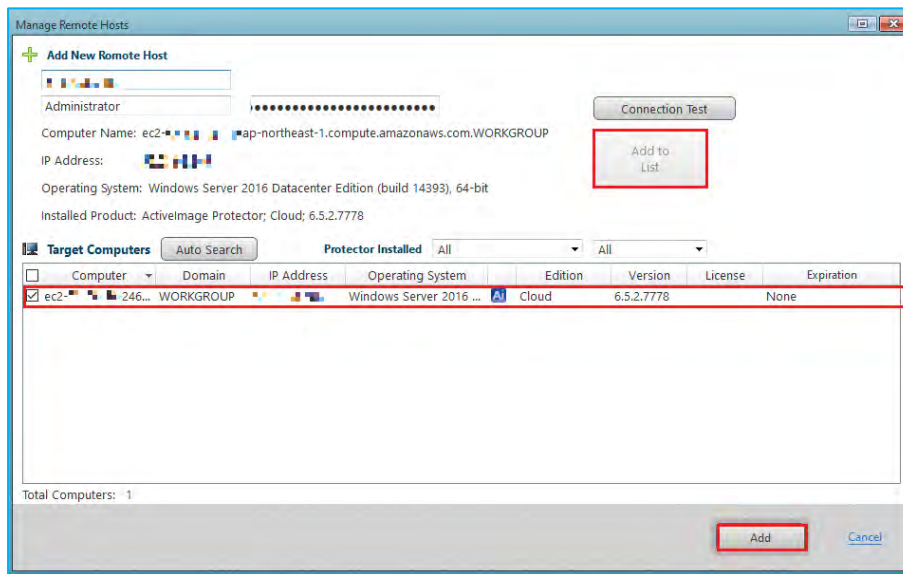
- Click **[Management Console]** in the upper left of the window. Click **[Add new computers]** to add the new computer to the host list.



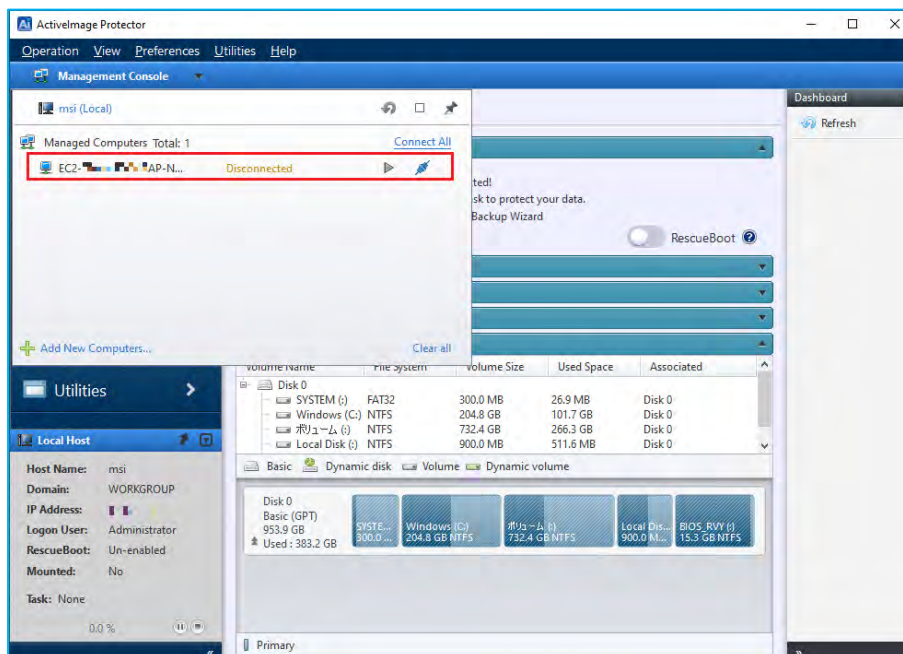
- Select the host names to add to the list by selecting **[Auto Search]** or **[Manual Search]**.  
In this example, we entered “IP address of the instance of Cloud”, “Administrator’s user name”, “Password” in **[Add New Remote Host]** window, and click **[Connection Test]**. When the connection test succeeds, **[Host Name]** and **[IP address]** are displayed.



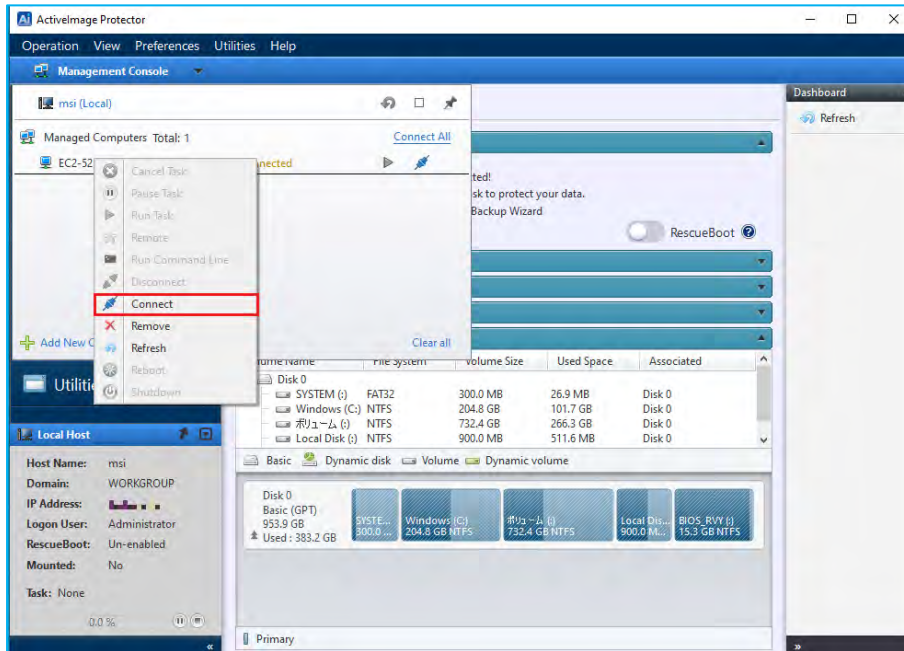
- Click **[Add to List]** and the remote host is added to the **[Target Computers]** list. Click **[Add]** to register the remote host as the target computer.



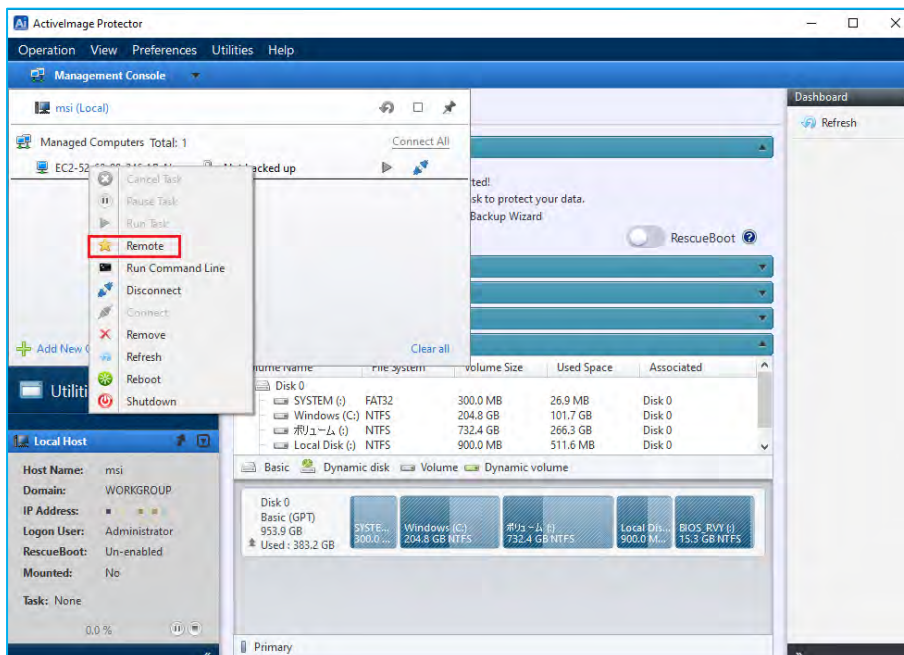
- The remote host is added to the managed computer.



- Right-click on a host in the list and click **[Connect]** in the context menu.

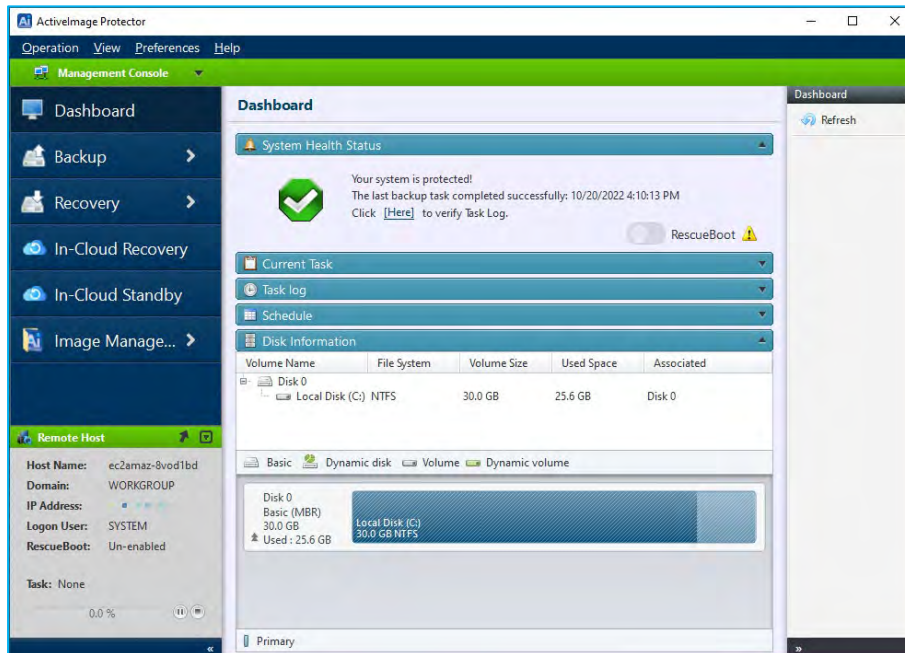


- Right-click on a host in the list, and select **[Remote]** in the right-click menu to establish the connection to the agent.

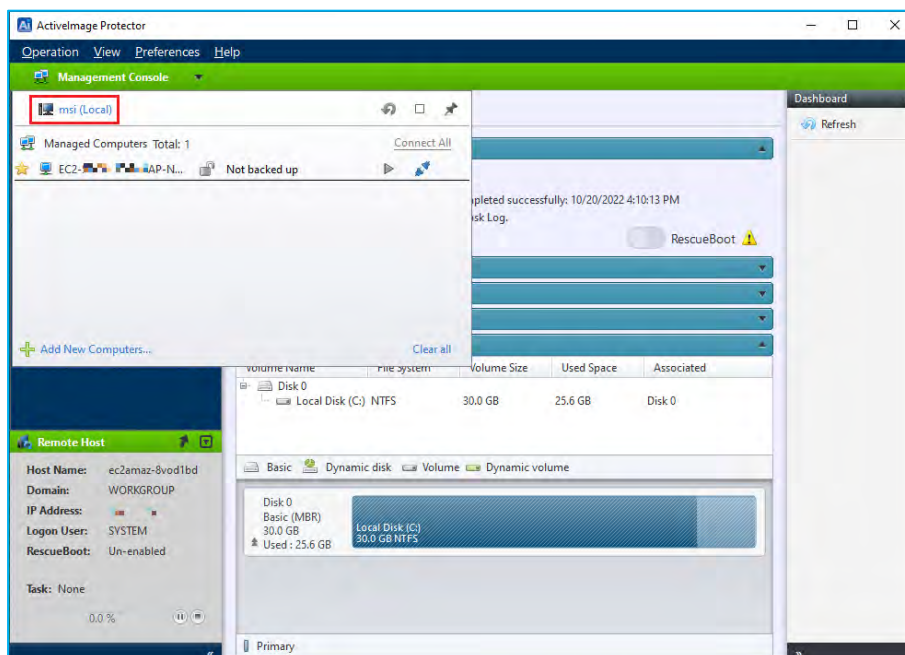




9. When connection is successfully established, the status bar is green. Now one-click offers execution of scheduled backup tasks on networked remote computers and monitoring of log information.



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



## 7. Reference

---

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

© 2024 Actiphy, Inc. All rights reserved.

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

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