Actifio Cloud Mobility

Actifio VDP 9.0

Copyright, Trademarks, and other Legal Matter

Actifio, Inc., is a provider of data protection and availability products. Actifio's technology is used in products sold by the company and products and services sold and offered by its commercial partners. The current list of Actifio patents is available online at: **http://www.actifio.com/patents/**

Actifio believes the information in this publication is accurate as of its publication date. Actifio reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Actifio strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to **docs@actifio.com**.

Contents

Preface

This document provides detailed instructions on how to use the Actifio Global Manager to virtualize physical servers and to migrate VMs from one cloud to another.

Actifio Appliances

Unless otherwise specified, all features and functions described in this document apply to all Actifio appliances.

The ActifioNOW Customer Portal

During the configuration and initialization of your Actifio appliance your Actifio representative provided you with a user name and password for the ActifioNOW customer portal.

From the ActifioNOW customer portal you can obtain detailed reports about your Actifio appliance, access the Actifio product documentation, including release notes, and search the knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

1. Go to: **https://now.actifio.com**.
2. When prompted, enter the user name and password provided by your Actifio representative.

Actifio Support Centers

To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:

  From anywhere: +1.315.261.7501

  US Toll-Free: +1.855.392.6810

  Australia: 0011 800-16165656

  Germany: 00 800-16165656

  New Zealand: 00 800-16165656

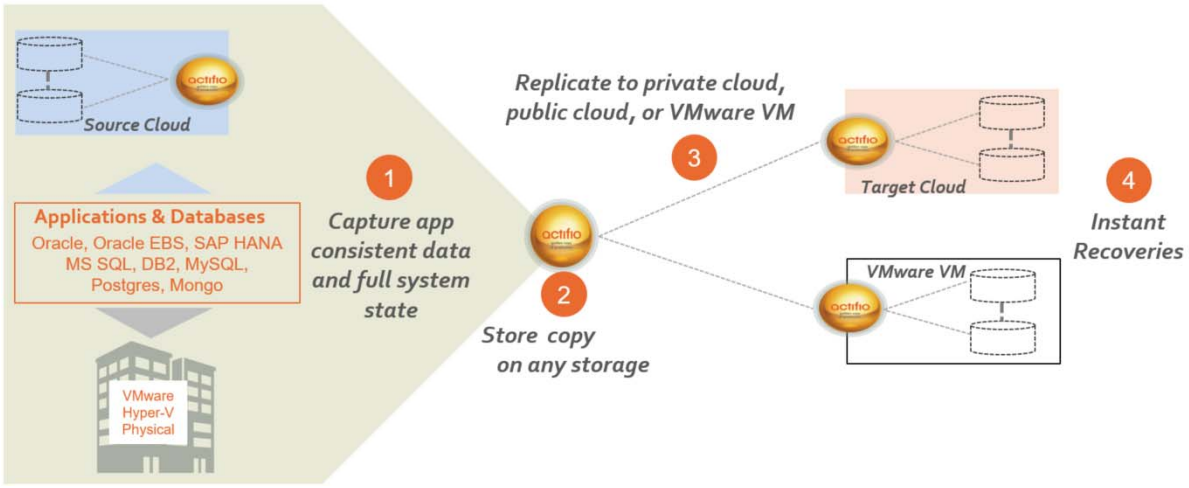
  UK: 0 800-0155019

1 Introducing Actifio Cloud Mobility

Actifio Cloud Mobility enables you to virtualize physical servers for migration to the cloud, and to capture local or cloud-based VMs for migration to other clouds from the AGM. ***Actifio Cloud Mobility*** details the two sides of cloud mobility, capturing the source and then recovering it to another state.

Virtualizing/capturing the source:

Recovering the virtualized source to the VM or cloud of your choice:

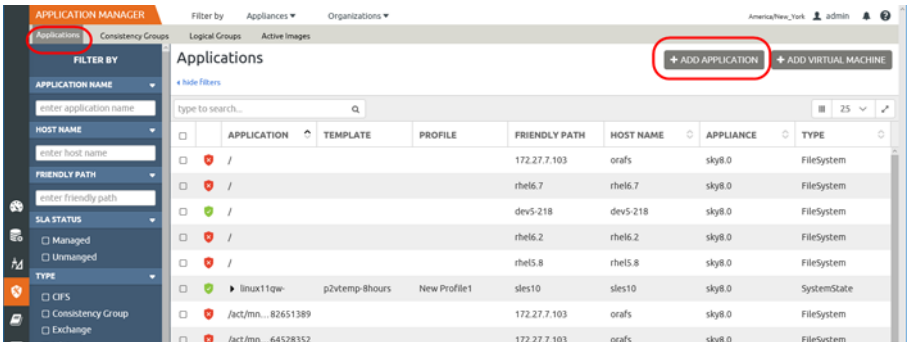


2 Capturing a VMware VM

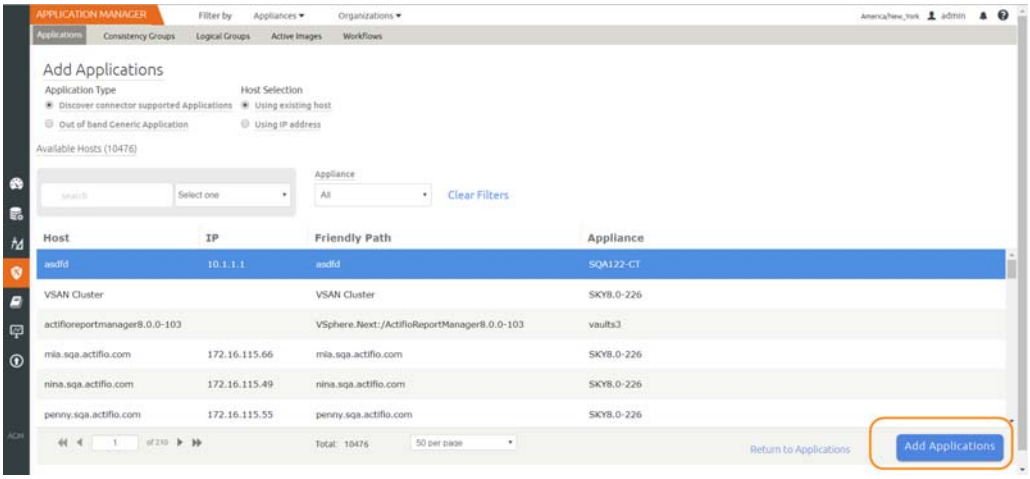
Before you can capture a VMware VM, the host that the VM is on must be added and the VM must be discovered with AGM version 8.0 or later.

To capture a VMware VM:

1. Open the Application Manager service in AGM to the Applications window.
2. Click **Add Application**.



3. The Add Applications window opens.



4. Select the host and click **Add Applications**. A progress spinner appears below the Application Type section under Add Applications. When the job is finished, the notification bell icon in the top right corner of the page becomes highlighted, and the applications appear in the Application Manager.
5. Select the host and click the arrow to the left of the name to expose the applications on the host.
6. Apply an SLA by selecting the VM and in the lower right corner selecting **Manage SLA**. The Manage SLA window appears.
    a. From the Manage SLA window, select from the Template and Profile drop-down lists.

b. Click **Apply SLA** to apply the SLA template and resource profile. The Apply SLA dialog box appears.

c. From the Apply SLA dialog box you can choose to make changes prior to applying an SLA. There are no application settings that are specific to protecting a system state. Apply application-specific settings and policy overrides suitable to this host. These settings may be useful or required in certain circumstances.

Note: *You can override policy settings in the Application Manager only if the policy template* ***Allow Overrides on Policy Settings*** *parameter has been set to* ***Yes***.

7. Click **Save Changes** when you finish modifying the settings in the Apply SLA dialog box.

8. To run the job immediately, click **Run SLA**.

Next Steps

When the job is finished (you can watch it in the System Monitor), the captured VM can be recovered or migrated to Amazon AWS, Google Cloud Platform, or Microsoft Azure as detailed in Chapter 6, Recovering a Captured Server or VM to a New VM in the Cloud.

3 Capturing and Virtualizing a Physical Host

This section details how to protect the system state, including the boot volume and all data disks, of a physical host and to recover it as a new VM. A system state includes basic metadata of the machine: number of CPUs, memory, number of disks, disk size, number of volumes per disk, volume size, number of network cards, network info of each interface, IP, and DNS.

Note: *This procedure is for virtualizing a physical host. To capture a VMware VM, see* Chapter 4, Capturing a VM in a Cloud for Migration*. Hyper-V VMs cannot be converted in this fashion.*

There are two steps to virtualizing a physical host:

1. Capture the system state as detailed in Capturing the System State of a Physical Host on page vii.
2. After you have captured the system state of the host, you can virtualize the host by recovering it as a new VMware VM as detailed in Recovering a Captured Server or Cloud VM to a New VMware VM.

   You can also recover the host as a VM in Amazon AWS, Microsoft Azure, and Google Cloud. These procedures are in Recovering a Captured Server or VM to a New VM in the Cloud on page xvii.

   Note: *SQL Cluster recovery is not automated; you must break the cluster, recover individual files and then form the cluster again.*

This section includes:

About the System State Container

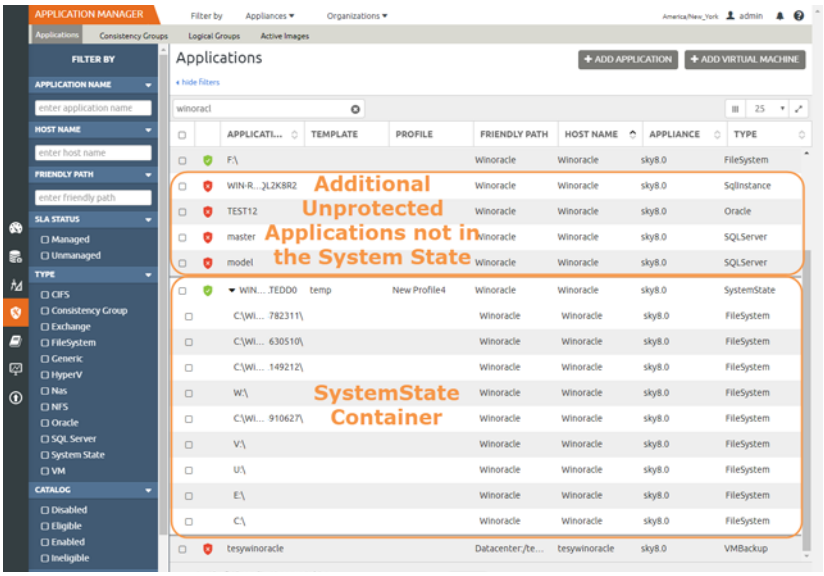
When you discover a new host, the Actifio Connector identifies any applications and file systems on it. The host's SystemState and its file systems appear in the Application Manager Applications list as a SystemState container. The Host has type SystemState and the name of the host has a black arrow beside it to indicate that there are file systems within the SystemState container.

File system applications on the host that are already protected do not go into the SystemState container, and applications that are not file systems do not go into the SystemState container.

This example shows a host Winoracle that includes (from the top):

- An already-protected FileSystem
- Unprotected applications of type SQLinstance, SQLServer, and Oracle
- The host as type SystemState, at the top of a SystemState Container
- Its root and boot drives and filesystems as type FileSystem inside the container

Databases and other applications with other types appear separately, outside of the SystemState container.



Everything in the SystemState container has the same protection policy, either unprotected or protected with the SystemState of the host. If you change the protection policy of a FileSystem included in a unprotected SystemState container by applying an SLA, then the filesystem is excluded from the SystemState container.

To change the protection of a FileSystem that is included in an already-protected SystemState, select the FileSystem and click Exclude from SystemState. The filesystem is removed from the SystemState container and appears with other FileSystem applications in the Applications list.

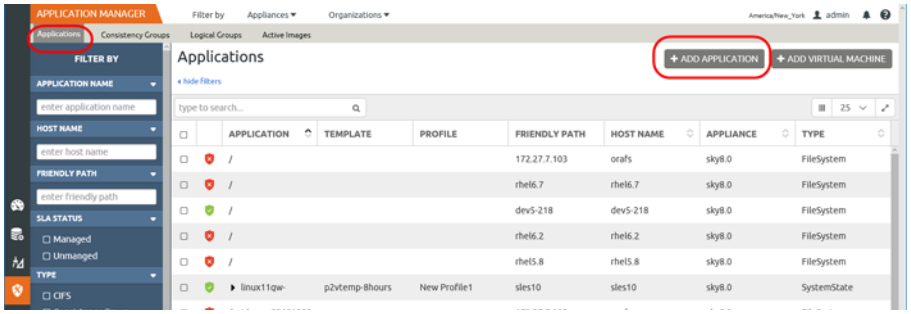
If you have a host that was discovered and protected with an Actifio Actifio Connector from before version 8.0, then any already-protected FileSystems appear with other protected FileSystems in the Applications list, not in the container.

Capturing the System State of a Physical Host

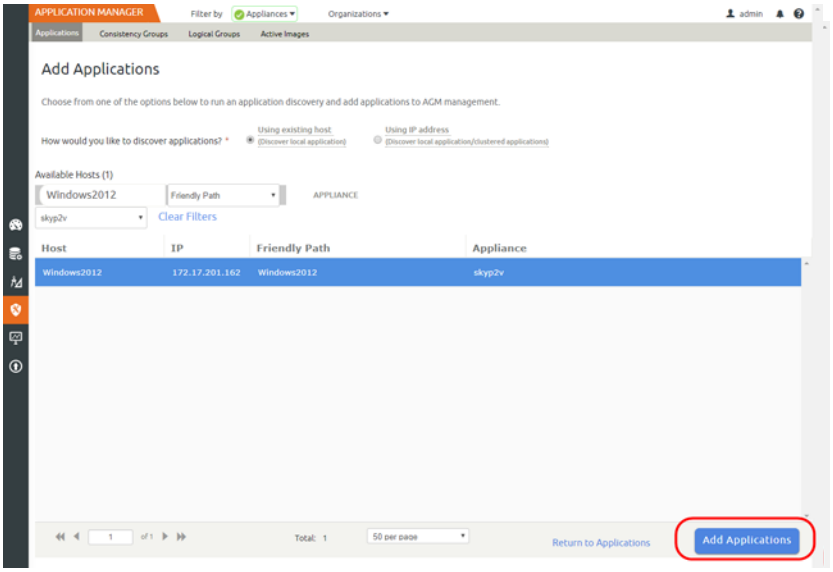
Note: *This procedure is for capturing the system state of a physical host. The procedure for capturing VMware VMs is in* Chapter 4, Capturing a VM in a Cloud for Migration.

To capture the system state of a physical host:

1. Open the Application Manager service in AGM to the Applications window.
2. Click **Add Application**.



3. The Add Applications window opens. Add the host as described in Application Discovery Overview.



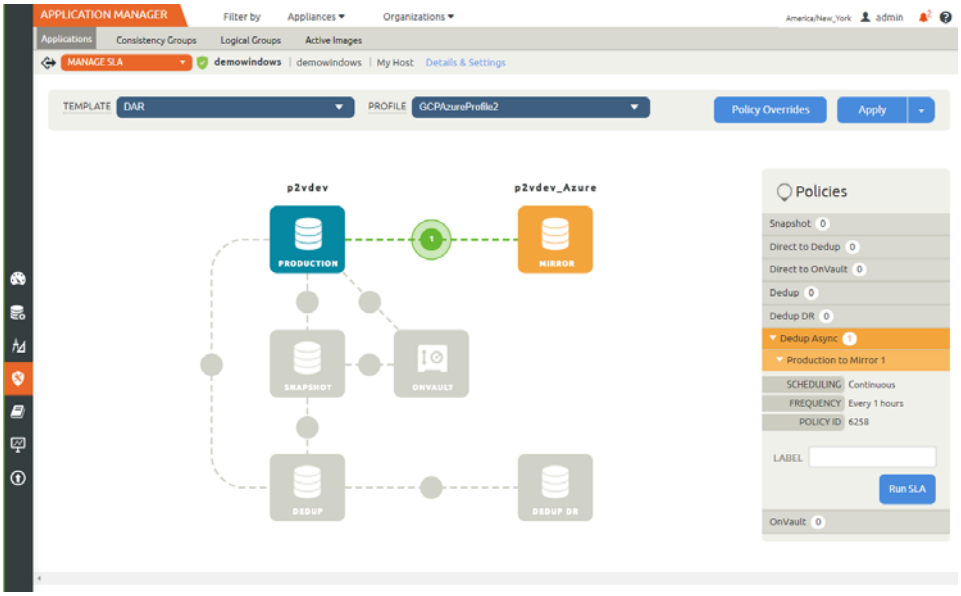
4. Select the host and click **Add Applications**. When the job is finished, the notification bell icon in the top right corner of the page becomes highlighted, and the applications appear in the Application Manager.
5. Select the host and click the arrow to the left of the name to expose the applications on the host. (You might want to review About the System State Container on page vi before continuing.)
    - If you are virtualizing an entire server, then sort the Applications list by Host Name, and then select the SystemState container with all file systems included. If the host includes additional unprotected applications such as databases, they will have the same Host Name, but they will not appear in the SystemState container. Check the boxes for those as well.
    - If you are virtualizing only the system state, then check the boxes for root (**/**) and **/boot** (Linux hosts) or **C:**(Windows hosts) only.
    - To change the protection of a FileSystem that is included in an already-protected SystemState, select the FileSystem and click Exclude from SystemState. The filesystem is removed from the SystemState container and appears with other FileSystem applications in the Applications list.

6. Apply an SLA by selecting the SystemState and in the lower right corner selecting **Manage SLA**. The Manage SLA window appears.

   a. From the Manage SLA window, select from the Template and Profile drop-down lists.

   b. Click **Apply SLA** to apply the SLA template and resource profile. The Apply SLA dialog box appears.

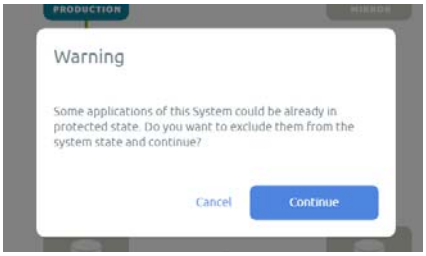
   c. From the Apply SLA dialog box you can choose to make changes prior to applying an SLA. There are no application settings that are specific to protecting a system state. Apply application-specific settings and policy overrides suitable to this host. These settings may be useful or required in certain circumstances.



Note: *You can override policy settings in the Application Manager only if the policy template* ***Allow Overrides on Policy Settings*** *parameter has been set to* ***Yes****.*

7. Click **Save Changes** when you finish modifying the settings in the Apply SLA dialog box.

   If you have already protected some data on the host, then you will see a warning. If you Continue, then the already-protected data will be excluded from this protection job.



   The Success message box appears.

   Note that the application is not captured until the scheduled job runs according to the hours of operation defined in the SLA template. For example, if at 10:00 am you assign a template that has hours of operation from 2:00 am to 5:00 am, then the first job will not start until the Actifio Appliance has an available job slot after 2:00 am. To run a job immediately, click **Run SLA**.

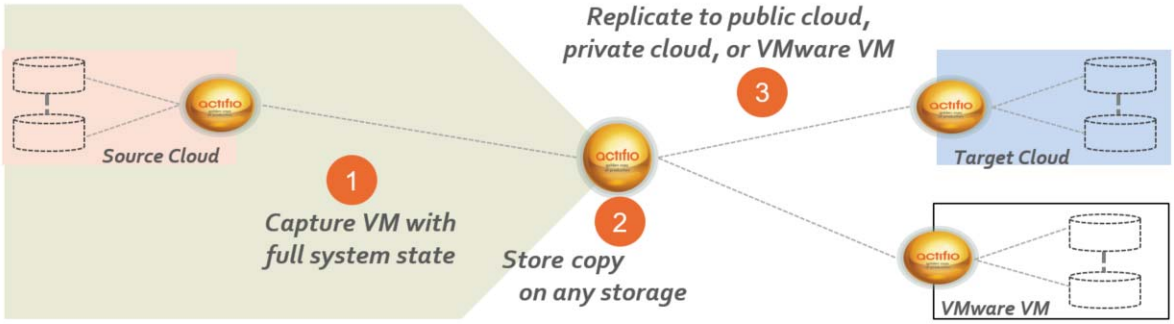
   Note: *To change settings for an application that is in a managed state, see* Modifying SLA Management of an Application.

8. To review the details of the managed application and/or modify any of the application-specific settings, click **Details & Settings**. When you are finished, or if you override advanced policy settings, click **Save Changes**.

4 Capturing a VM in a Cloud for Migration

If you have to migrate a VM from one cloud to another, then you must capture the system state of the source VM. When you capture a VM system state with boot and root directories:

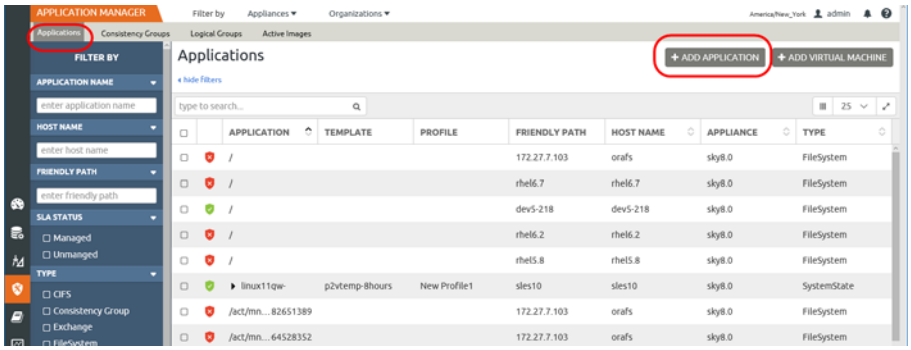
- If the VM had an Actifio Actifio Connector installed, the Connector will be copied and restored with no need for other steps.
- If the VM did not have a Connector installed, then when you recover the VM in the cloud, the Connector gets installed during the recovery process.



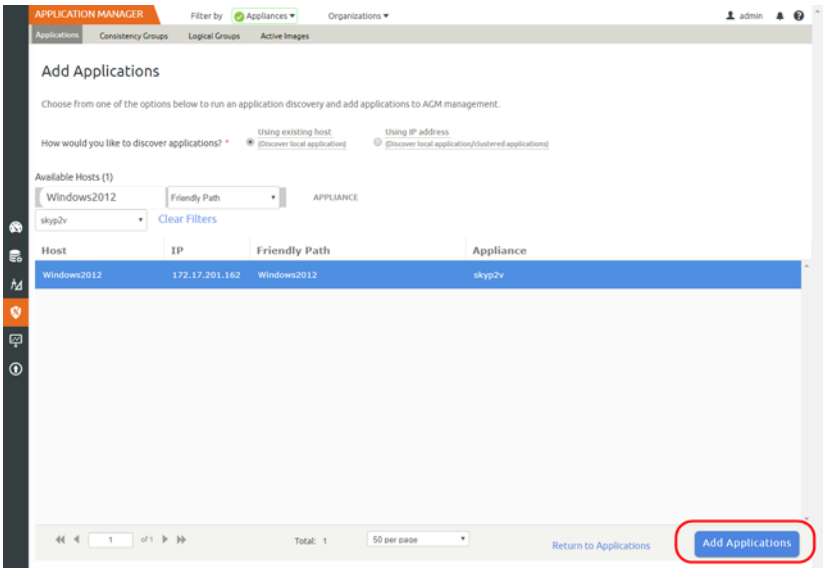
Before you can capture the system state of a VM, the host that the VM is on must be added and the VM must be discovered, with an Actifio Actifio Connector and AGM version 8.0 or later.

To capture the system state of a VM for migration:

1. Open the Application Manager service in AGM to the Applications window.
2. Click **Add Application**.



3. The Add Applications window opens. Add the host as described in Application Discovery Overview.



4. Select the host and click **Add Applications**. When the job is finished, the notification bell icon in the top right corner of the page becomes highlighted, and the applications appear in the Application Manager.

5. Select the host and click the arrow to the left of the name to expose the applications on the host.

    - If you are virtualizing an entire server, then sort the Applications list by Host Name, and then select the SystemState container with all file systems included. If the host includes additional unprotected applications such as databases, they will have the same Host Name, but they will not appear in the SystemState container. Check the boxes for those as well.
    - If you are virtualizing only the system state, then check the boxes for root (**/**) and **/boot** (Linux hosts) or **C:** (Windows hosts) only.
    - To change the protection of a FileSystem that is included in an already-protected SystemState, select the FileSystem and click Exclude from SystemState. The filesystem is removed from the SystemState container and appears with other FileSystem applications in the Applications list.

6. Apply an SLA by selecting the SystemState and in the lower right corner selecting **Manage SLA**. The Manage SLA window appears.

    a. From the Manage SLA window, select from the Template and Profile drop-down lists.

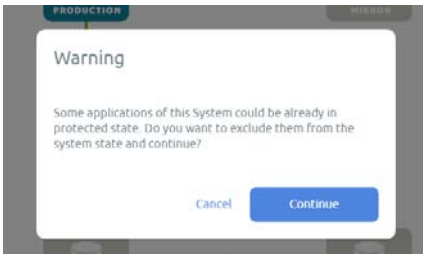
    b. Click **Apply SLA** to apply the SLA template and resource profile. The Apply SLA dialog box appears.

    c. From the Apply SLA dialog box you can choose to make changes prior to applying an SLA. There are no application settings that are specific to protecting a system state. Apply application-specific settings and policy overrides suitable to this host. These settings may be useful or required in certain circumstances.

    Note: *You can override policy settings in the Application Manager only if the policy template* ***Allow Overrides on Policy Settings*** *parameter has been set to* ***Yes***.

7. Click **Save Changes** when you finish modifying the settings in the Apply SLA dialog box.

    If you have already protected some data on the host, then you will see a warning. If you continue, then the already-protected data will be excluded from this protection job.



The Success message box appears.

8. To run the job immediately, click **Run SLA**.

Next Steps

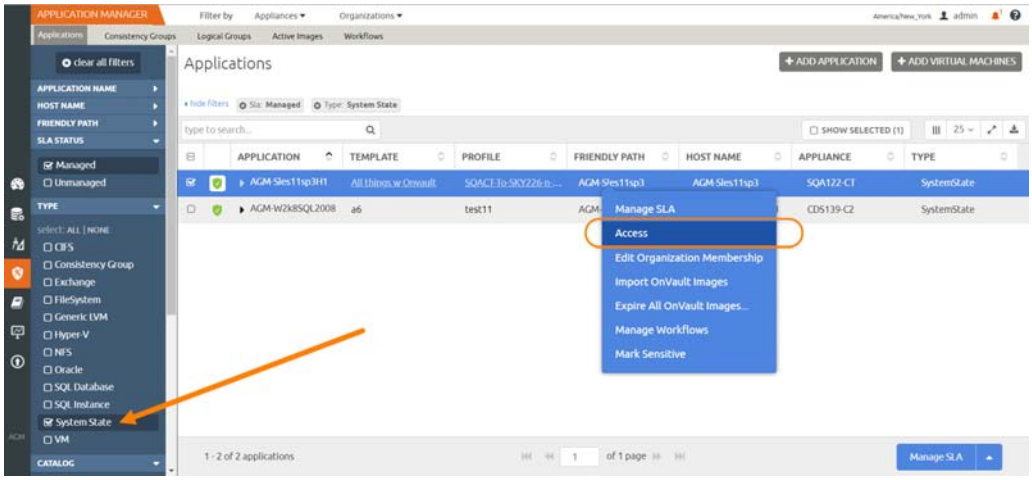
When the job is finished (you can watch it in the System Monitor), the captured VM with its system state can be recovered to Amazon AWS, Google Cloud Platform, or Microsoft Azure as detailed in Chapter 6, Recovering a Captured Server or VM to a New VM in the Cloud. The original can be deleted if you no longer need it, and any images expired.

5 Recovering a Captured Server or Cloud VM to a New VMware VM

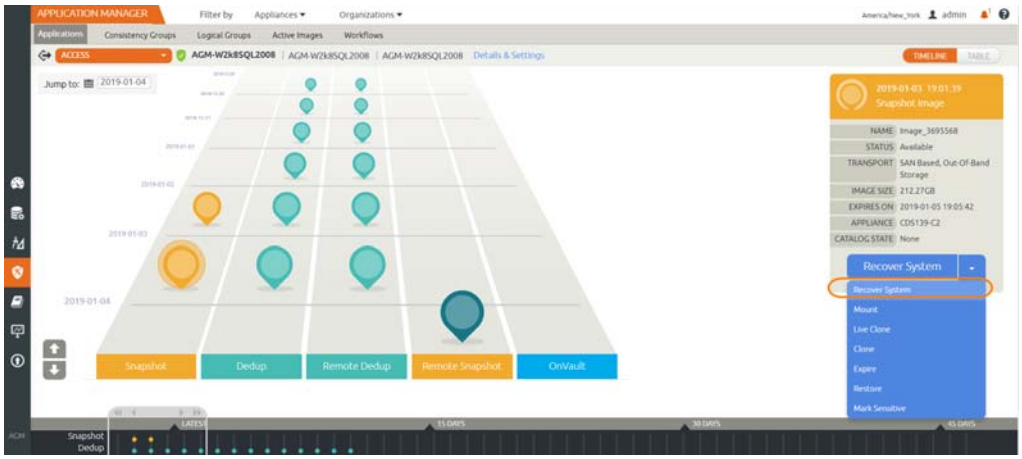
Recovering a host's SystemState enables you to create an on-premises VM with the system state information from a physical host captured according to the procedure in Capturing the System State of a Physical Host on page vii.

To restore a host's SystemState:

1. Open the Application Manager service in AGM to the Applications window.
2. Select the SystemState container of the host that you plan to restore. The System State filter can make this easier if you have many applications.
3. Either right-click the image or in the lower right corner, select **Access** from the dropdown list.

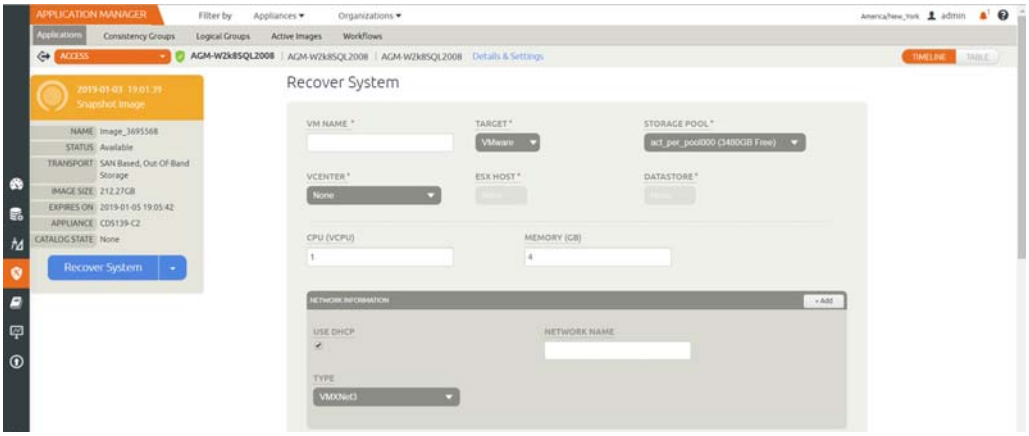


4. The timeline or table of images appears.



5. Select an image, then select **Recover System**. The Recover System window opens.

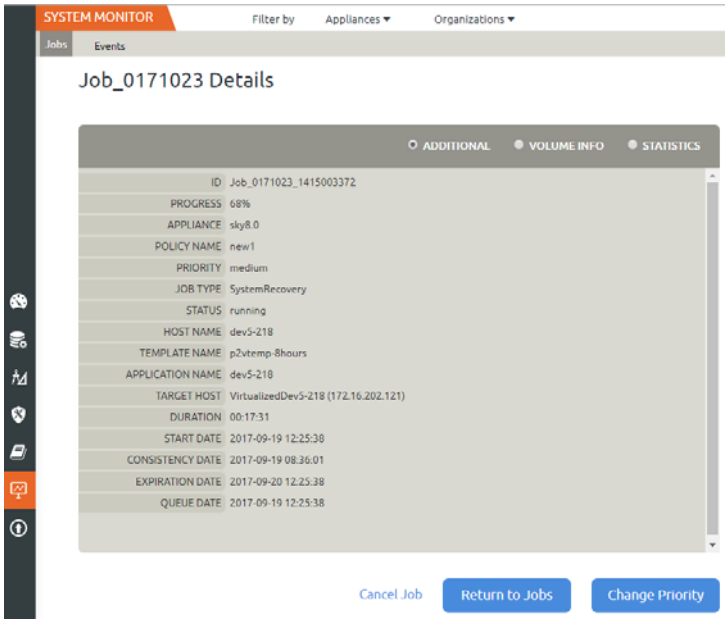
6. From the Target dropdown, select VMware to restore the physical host to a VMware VM.
If you want to restore the host to a VM in a cloud service, see Recovering a Captured Server or VM to a New VM in the Cloud on page xvii.



7. Fill in these network information values:
   - VM NAME: Enter a name for the new VMware/AWS virtual machine that you want to recover.
   - TARGET: VMware
   - STORAGE POOL: Select whether to use the Performance Pool or an external storage pool.
   - VCENTER: Select the vCenter that will manage the new VM.
   - ESX HOST: Select the ESX host that will host the new VM.
   - DATASTORE: Select the VMware Datastore.
   - CPU (VCPU): If you want to increase the number of CPUs used by the new VM, enter a value here.
   - MEMORY (GB): If you want to increase the memory available to the new VM, enter a value here.
   - USE DHCP: You can create the VM to use DHCP or a static IP. Check this box to use DHCP.
     If you will not use DHCP, then uncheck this checkbox and enter values for the IP Address, Subnet, Gateway, and DNS fields that appear.
   - NETWORK NAME: Network in which you want to recover the system.
   - TYPE: Select the virtual NIC type in use: VMXNet3 or E1000.

   Below the network information, an Applications/Data Volumes section shows FileSystems to be restored.

8. Click **Submit**. You can follow the progress of the SystemRecovery job in the system monitor. Click on the job to see the job details, including the IP address of the new host.



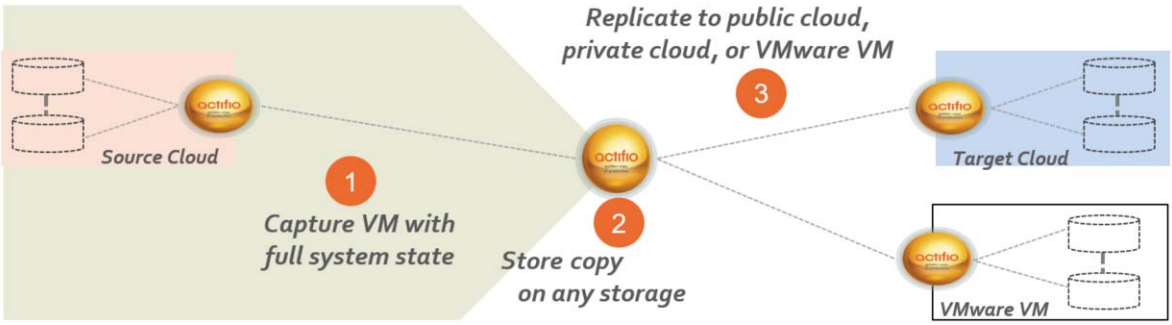
9. When the job is finished, the new VM will appear in the Applications list, unprotected.

6 Recovering a Captured Server or VM to a New VM in the Cloud

This chapter describes how to recover a host with its captured system state information to these targets:

When you capture a VM system state with boot and root directories:

- If the VM had an Actifio Actifio Connector installed, the Connector will be copied and restored with no need for other steps.
- If the VM did not have a Connector installed, then when you recover the VM in the cloud, the Connector gets installed during the recovery process.



Recovering a VM or a Physical Server to an Amazon AWS VM

Actifio Cloud Mobility allows you to recover a physical host's System State or a VM to a new VM in AWS.

Before You Begin

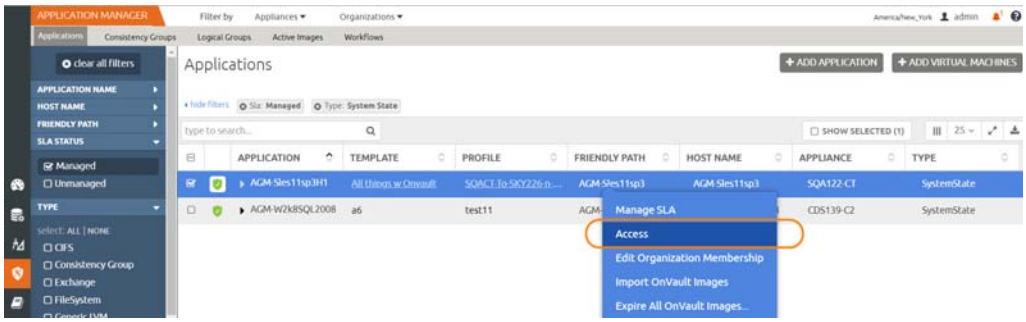
Before you begin, you will need:

- A target Sky Appliance in any of the regions in AWS, and the Region Code of the AWS region where the Sky Appliance is running.
- The target Sky Appliance must be joined to the source appliance from the Actifio Desktop Domain Manager System > Configuration > Appliance Settings page, and both must be managed by AGM.
- Base Template AMIs for Windows and Linux from your Actifio representative in your AWS account.
- An IAM user created from an Actifio-provided template, as described in Creating an Amazon IAM User with AWS Access Credentials on page xix.
- The target recovery security group requires these ports to be open both inbound and outbound for TCP: 80, 443, 5106, 3260

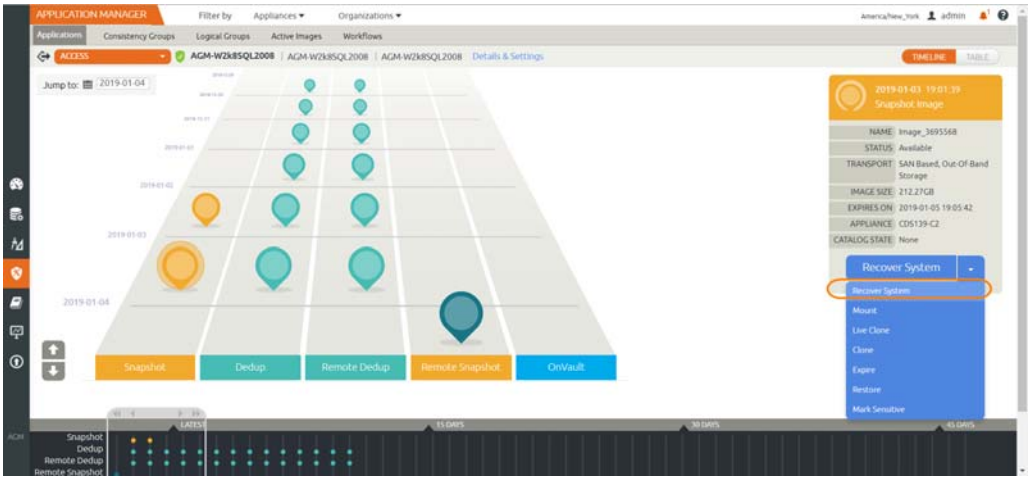
Procedure

To recover a VM or a physical host's System State to an Amazon AWS virtual machine:

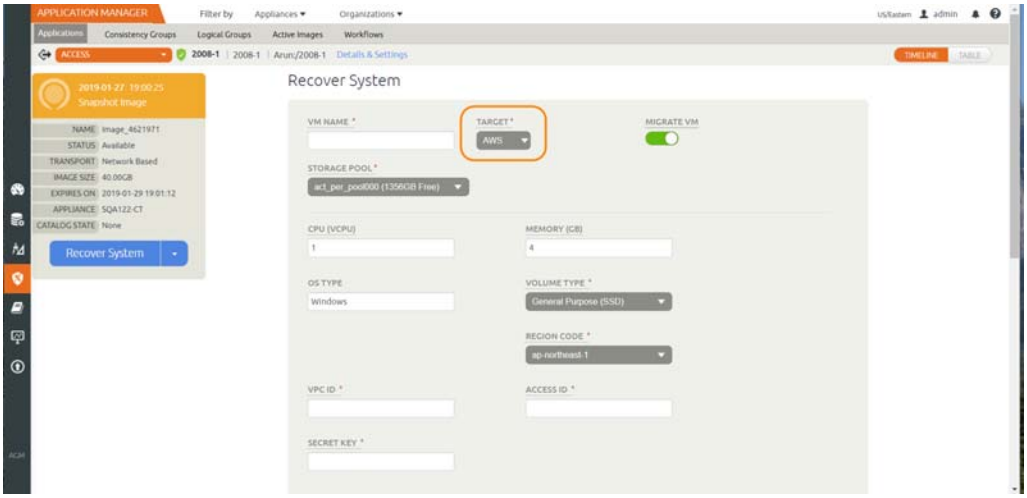
1. Open the Application Manager service in AGM to the Applications window.
2. Select the host that you plan to restore. The filters and the search tool can be helpful.
3. Either right-click the image or in the lower right corner, select **Access** from the dropdown list.



4. The timeline or table of images appears.

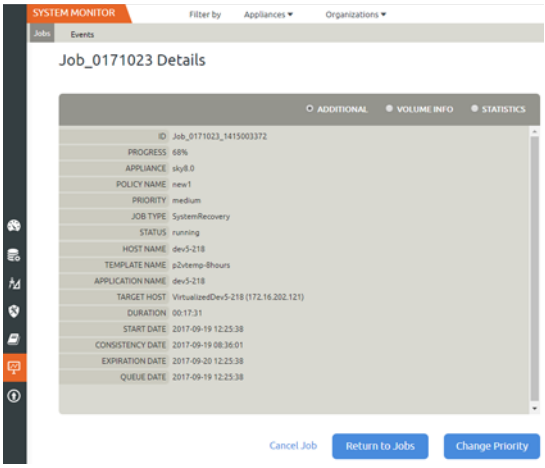


5. Select an image, then select **Recover System**. The Recover System window opens.
6. From the Target dropdown, select **AWS**.



7. Fill in these recover system values:
    - VM NAME: Enter a name for the new AWS virtual machine that you want to recover.
    - MIGRATE VM: As part of the system recovery operation, you can copy the boot drive and all of the file system files into a fully-functioning new VM that is unconnected to Actifio. Select this if you want to migrate the data from the image to AWS native volumes.
    - STORAGE POOL: Select whether to use the Performance Pool or an external storage pool.
    - CPU (VCPU): This is prepopulated from the source. If you want to increase the number of CPUs used by the new VM, enter a value here.
    - MEMORY (GB): This is prepopulated from the source. If you want to increase the memory available to the new VM, enter a value here.
    - REGION CODE: Enter the Amazon region code here.
    - VPC ID: Enter the VPC ID from Amazon.
    - ACCESS ID: Enter the Access Key ID.
    - SECRET KEY: Enter the Secret Access Key.
    - SUBNET ID: Enter the subnet ID from Amazon.
    - SECURITY GROUP ID: Enter the SecurityGroup ID from Amazon.
    - BOOT DISK SIZE (GB): Enter a size for the boot disk in GB (Windows only)

    Below the network information is an Applications/Data Volumes section that shows the FileSystems to be restored.
8. Click **Submit**.
9. Follow the progress of the SystemRecovery job in the system monitor. Click on the job to see the job details, including the IP address of the new host.



10. When the job is finished, the new VM will appear in the Applications list, unprotected.

    You must access the new host from an appropriate Amazon account in the right region.

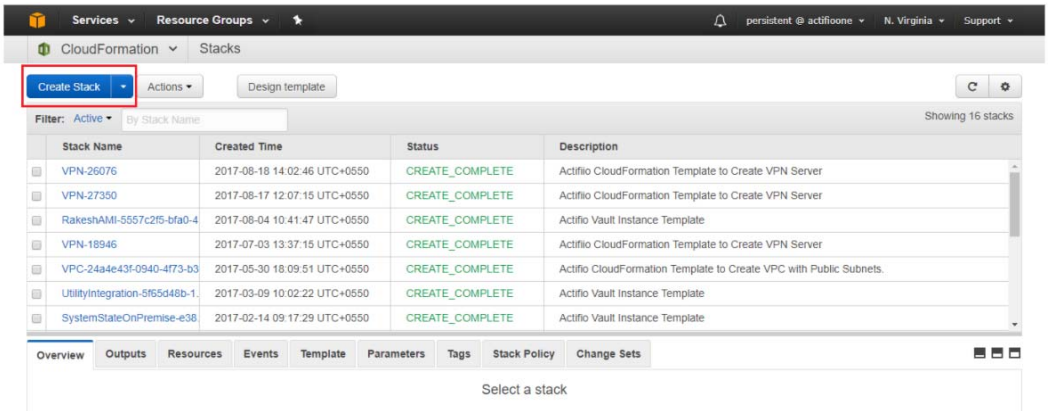
Creating an Amazon IAM User with AWS Access Credentials

The procedure for restoring a physical server or a VM to a new VM in Amazon AWS requires an Amazon IAM user with all the required permissions, an Access Key and a Secret Key.

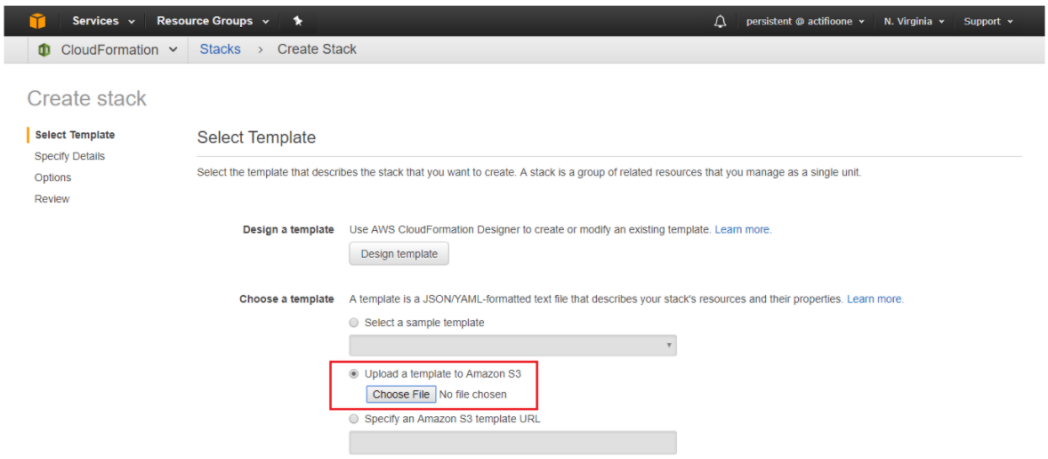
Actifio Support will provide you with an Amazon AWS Cloud Formation template that you can use to create an IAM group. An IAM user created inside this IAM group and AWS will have the permissions and an Access Key and a Secret Key.

To generate an IAM user with the required access credentials:

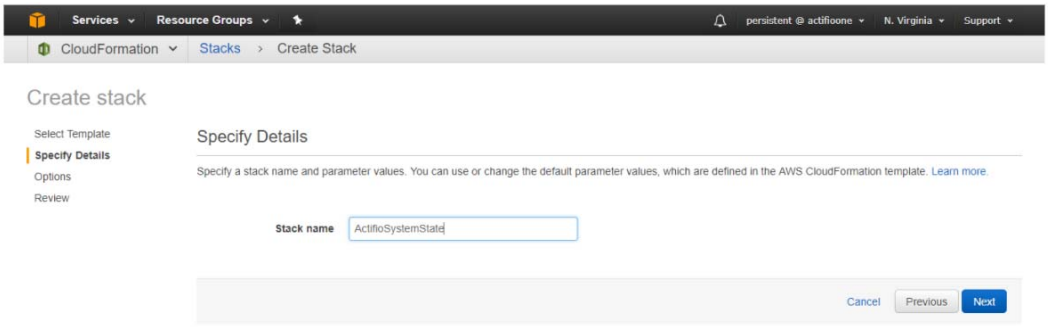
1. Log into your AWS account and go to the CloudFormation Service.
2. Click **Create Stack**.



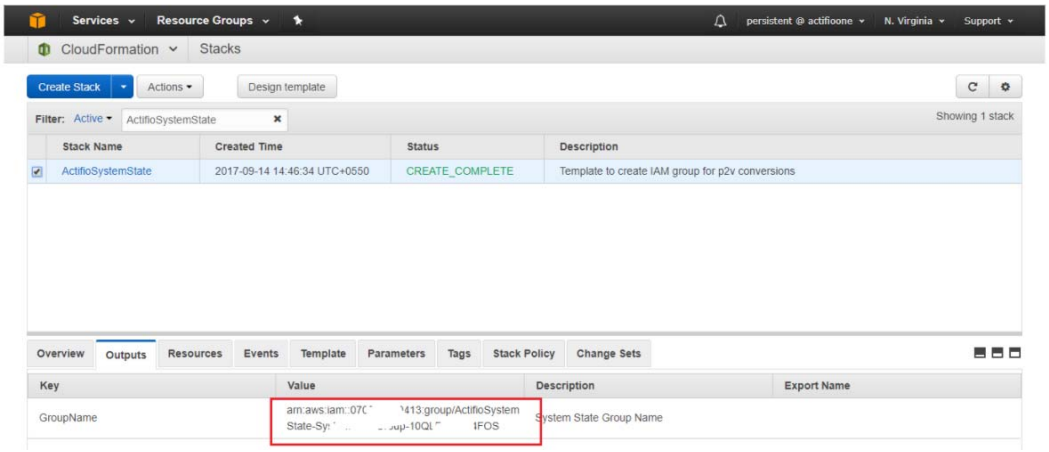
3. Click **Choose File** and upload the Cloud Formation template.



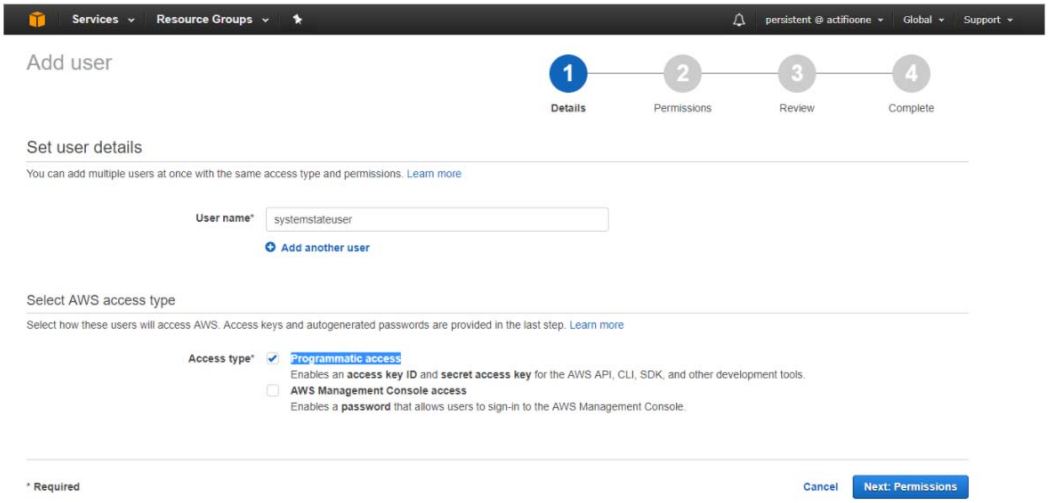
4. Give a stack name and click **Next** > **Next**. The stack will start running.



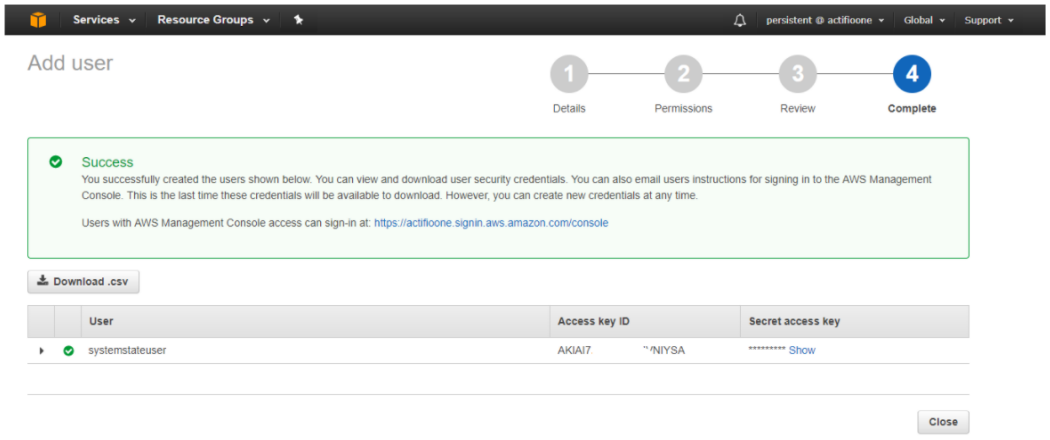
Once the stack status is completed, you can see the IAM group name created under the Outputs tab. You can also see the group if you navigate to IAM service -> Groups.



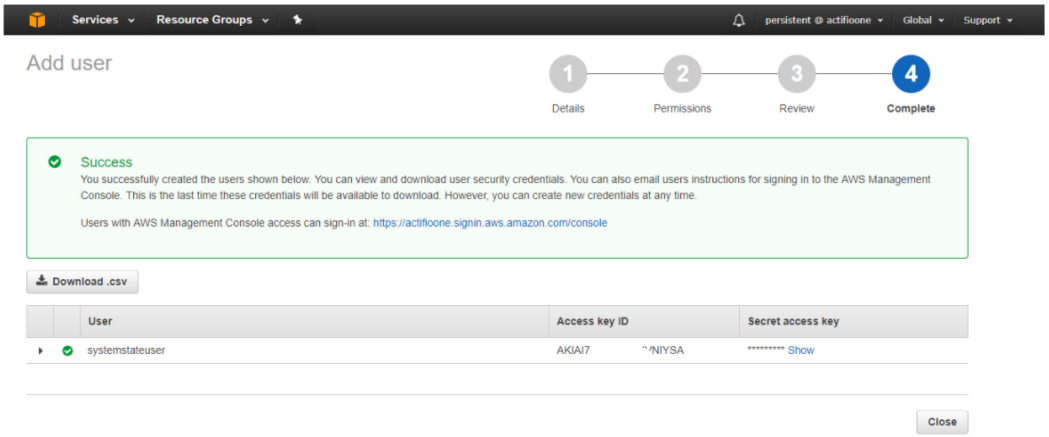
5. Go to IAM Service -> Users and click **Add User**.
6. Give any name to the IAM user and select only **Programmatic access**.



7. Click **Next:Permissions**, then select the newly created group under "Add user to group".



8. Click **Next** to create a new user. This will create an IAM user and you can get the access key id and secret key to use for running conversion to AWS.



After the user has been created, copy the Access Key ID and the Secret Key, then you can proceed with Recovering a VM or a Physical Server to an Amazon AWS VM on page xvii.

Recovering a VM or a Physical Server to a Microsoft Azure VM

Actifio Cloud Mobility allows you to recover a physical host's System State or a VM to a new VM in Microsoft Azure.

Before You Begin

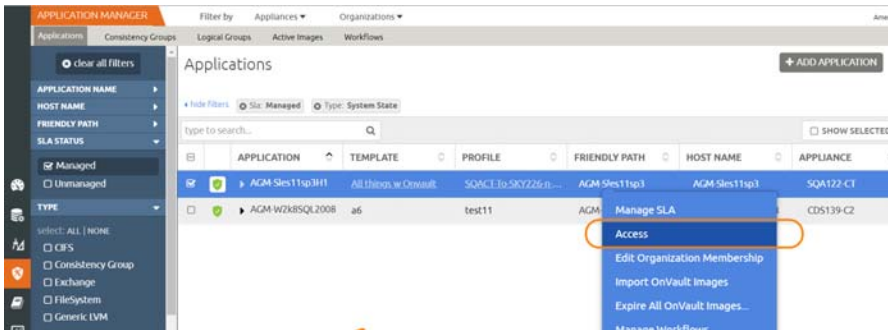
Before you begin, you will need:

- A target Sky Appliance in any of the regions in Azure, and the Azure Location of the Azure region where the Sky Appliance is running.
- The target Sky Appliance must be joined to the source appliance from the Actifio Desktop Domain Manager System > Configuration > Appliance Settings page, and both must be managed by AGM.
- A VHD file in your Azure account; see Getting the VHD on page xxv.
- Access credentials, as described in Generating Azure Access Credentials on page xxv.

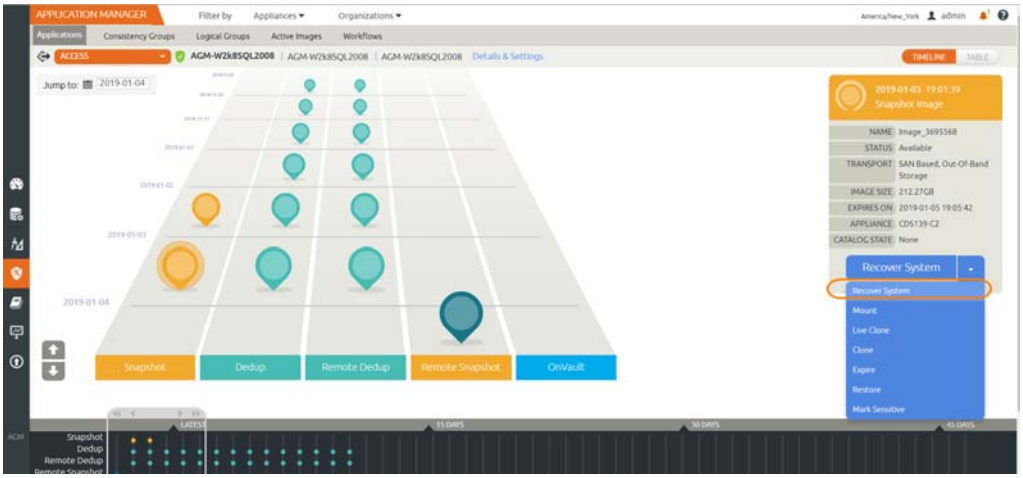
Procedure

To recover a VM or a physical host's System State to a Microsoft Azure virtual machine:

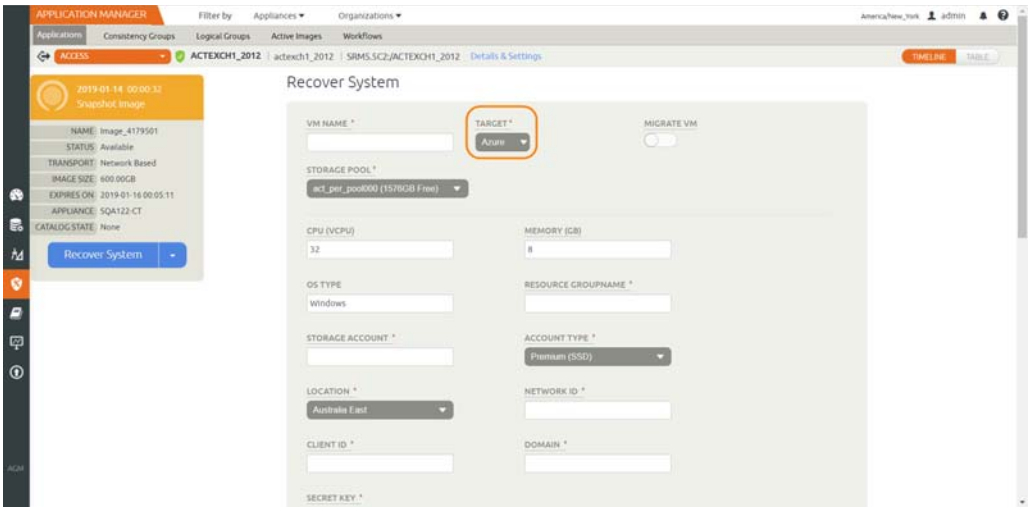
1. Open the Application Manager service in AGM to the Applications window.
2. Select the host that you plan to restore. The filters and the search tool can be helpful.
3. Either right-click the image, or in the lower right corner, select **Access** from the dropdown list.



4. The timeline or table of images appears.

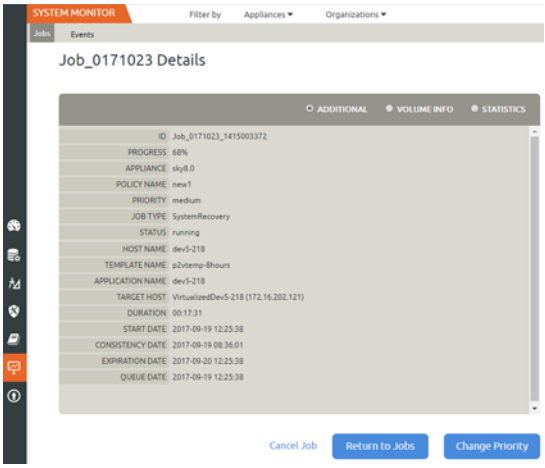


5. Select an image, then select **Recover System**. The Recover System window opens.
6. From the Target dropdown, select **Azure**.



7. Fill in these recover system values:
    - VM NAME: Enter a name for the new Azure virtual machine that you want to recover.
    - MIGRATE VM: As part of the system recovery operation, you can copy the boot drive and all of the file system files into a fully-functioning new VM that is unconnected to Actifio. Select this if you want to migrate the data from the image to a new VM in Azure.
    - STORAGE POOL: Select whether to use the Performance Pool or an external storage pool.
    - CPU (VCPU): This is prepopulated from the source. If you want to increase the number of CPUs used by the new VM, enter a value here.
    - MEMORY (GB): This is prepopulated from the source. If you want to increase the memory available to the new VM, enter a value here.
    - Resource Groupname: Enter the name of the Azure Resource Group.
    - Storage Account: Enter the name of your Azure Storage Account.
    - Location: Select the Microsoft Azure location where you want the VM.
    - Network ID: Enter the name of the network that the Azure VM is a part of.
    - Client ID, Domain (tenant ID), and Secret Key are the private keys required to make Azure API calls from the Sky Appliance.
    - SUBNET ID: Enter the subnet ID from Azure.
    - SECURITY GROUP ID: Enter the SecurityGroup ID from Azure.
    - BOOT DISK SIZE (GB): Enter a size for the boot disk in GB (Windows only)

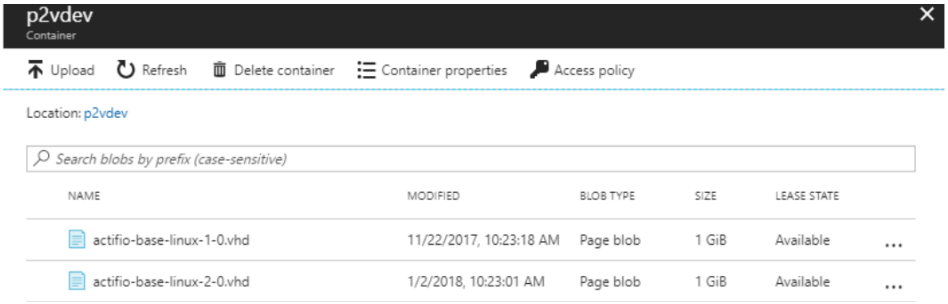
    Below the network information is an Applications/Data Volumes section with FileSystems to be restored.
8. Click **Submit**.
9. Follow the progress of the SystemRecovery job in the System Monitor. Click on the job to see the job details, including the IP address of the new host.



10. When the job is finished, the new VM will appear in the Applications list, unprotected. You must access the new host from an appropriate Azure account in the right region.

Getting the VHD

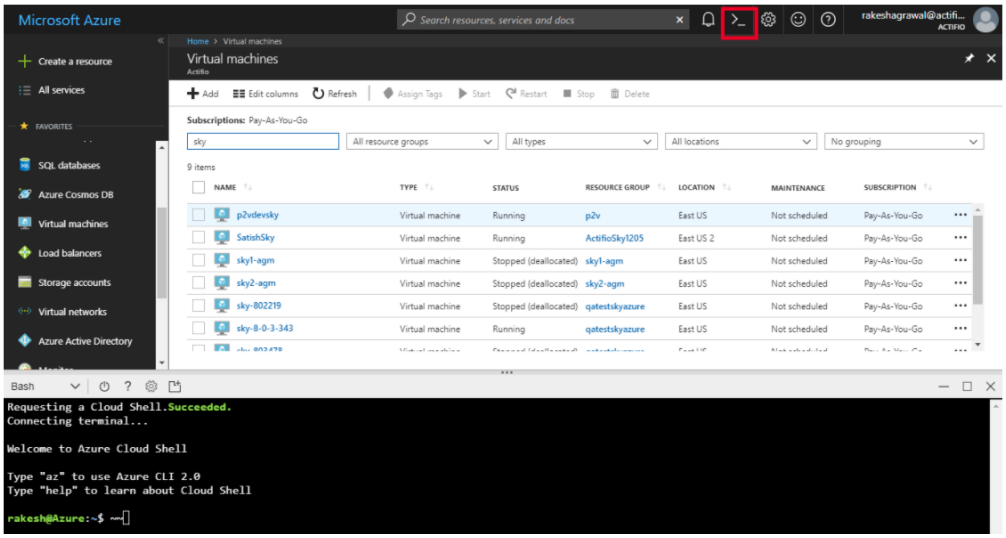
The first time you run a conversion, Actifio will copy the VHD into your Azure account using the shared-access URL that you provide.



Generating Azure Access Credentials

You need ClientId, Domain/tenant id and Secret Key for API authentication. To get these details:

1. Log in to the Azure portal as a user with the Virtual Machine Contributor and Storage Blob Data Contributor roles.
2. Get the subscription id of the account. You can get the subscription id by searching subscriptions in the Azure portal from Home -> Subscriptions.
3. Open cloud shell.



4. Execute:

```
az account set --subscription <Subscription_id>
az ad sp create-for-rbac --sdk-auth > my.azureauth
cat my.azureauth
```

This will create a file `my.azureauth` with all the details required for authentication via APIs.

Recovering a VM or a Physical Server to a Google Cloud VM

Actifio Cloud Mobility allows you to recover a physical host's System State or a VM to a new VM in Google Cloud.

Before You Begin

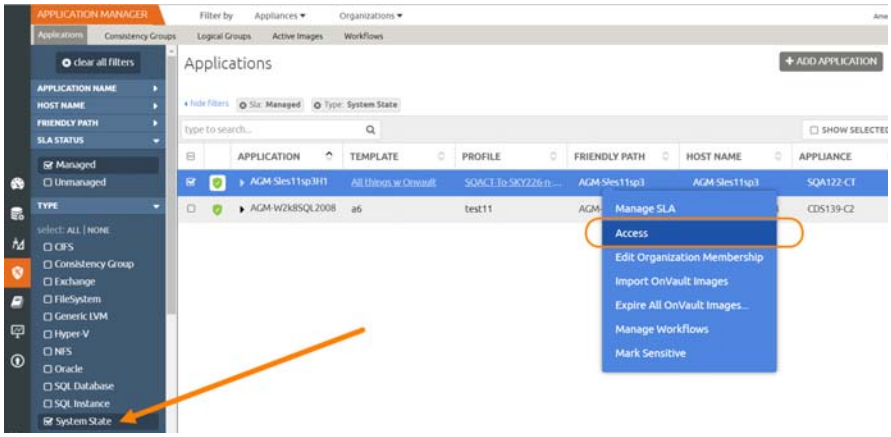
Before you begin, you will need:

- A target Sky Appliance in any of the Google Cloud regions, and the Region Code of the Google Cloud region where the Sky Appliance is running.
- The target Sky Appliance must be joined to the source appliance from the Actifio Desktop Domain Manager System > Configuration > Appliance Settings page, and both must be managed by AGM.
- Base Template Images for Windows and Linux from your Actifio representative in your Google Cloud Account.
- Private keys information for a user created from a service account with compute engine permissions, as described in Generating GCP Access Credentials on page xxix.

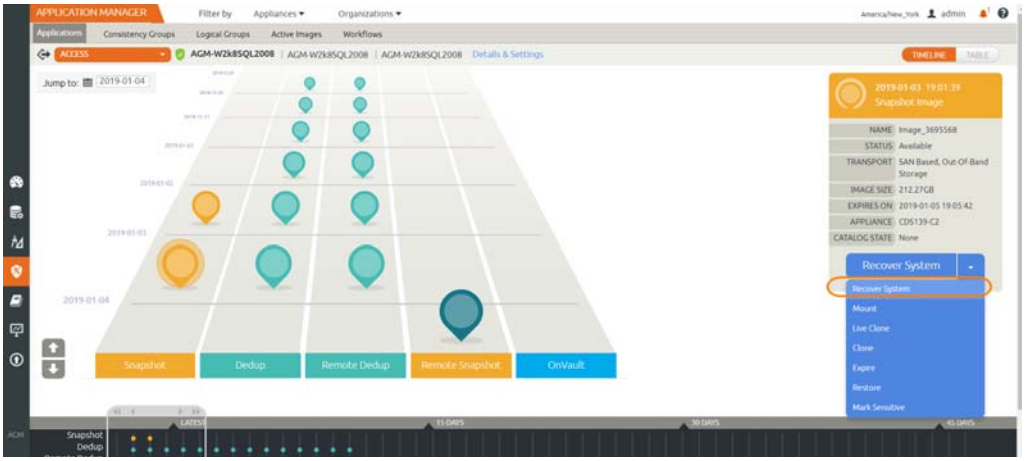
Procedure

To recover a VM or a physical host's System State to a Google Cloud virtual machine:

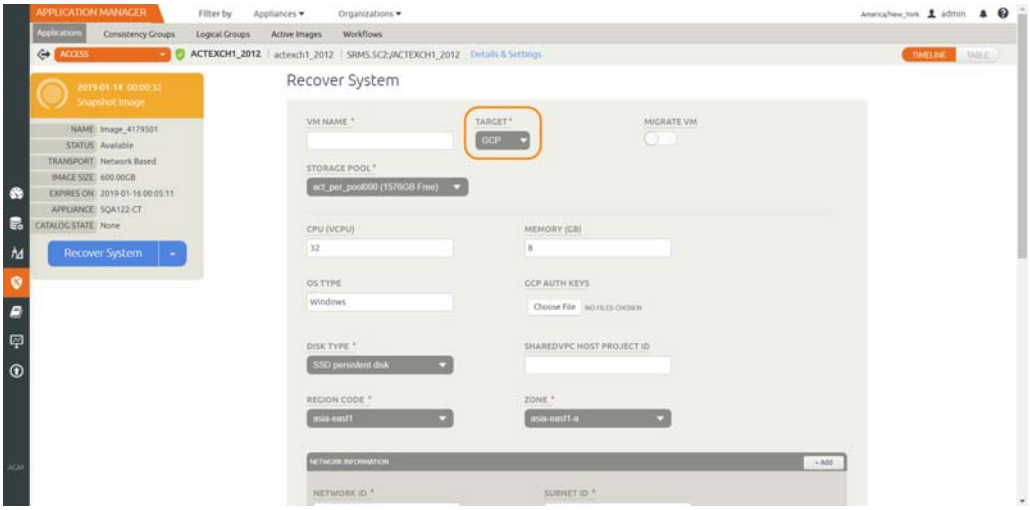
1. Open the Application Manager service in AGM to the Applications window.
2. Select the host that you plan to restore. The filters and the search tool can be helpful.
3. Either right-click the image or in the lower right corner, select **Access** from the dropdown list.



4. The timeline or table of images appears.

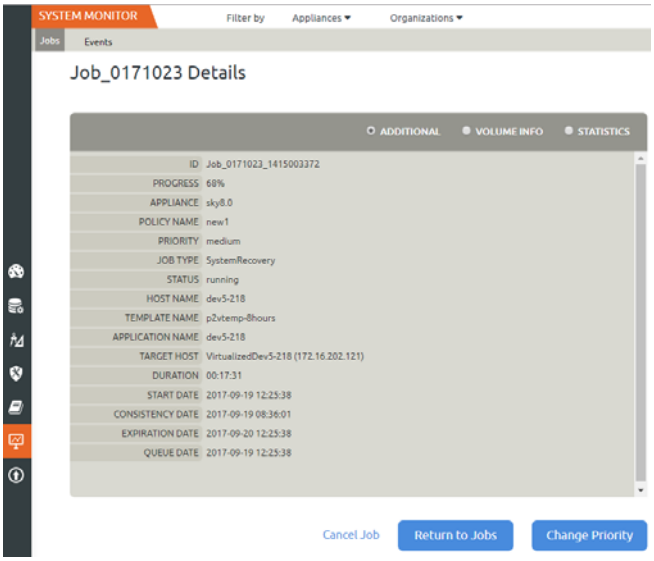


5. Select an image, then select **Recover System**. The Recover System window opens.
6. From the Target dropdown, select **GCP** to restore to Google Cloud.



7. Fill in these recover system values:
   - VM NAME: Enter a name for the new GCP virtual machine that you want to recover.
   - MIGRATE VM: As part of the system recovery operation, you can copy the boot drive and all of the file system files into a fully-functioning new VM that is unconnected to Actifio. Select this if you want to migrate the data from the image to a new VM in the Google Cloud Platform.
   - STORAGE POOL: Select whether to use the Performance Pool or an external storage pool.
   - CPU (VCPU): This is prepopulated from the source. If you want to increase the number of CPUs used by the new VM, enter a value here.
   - MEMORY (GB): This is prepopulated from the source. If you want to increase the memory available to the new VM, enter a value here.
   - GCP Auth Keys: Browse to and upload the authorization keys. See Generating GCP Access Credentials on page xxix.
   - Region Code: Select the Google Cloud region where you want the VM.
   - Zone: Select a zone within the Google Cloud region.
   - NETWORK ID: Enter the Network ID from GCP.
   - SUBNET ID: Enter the subnet ID from GCP.
   - BOOT DISK SIZE (GB): Enter a size for the boot disk in GB (Windows only).

   Below the network information is an Applications/Data Volumes section that shows the FileSystems to be restored.
8. Click **Submit**.
9. Follow the progress of the SystemRecovery job in the system monitor. Click on the job to see the job details, including the IP address of the new host.



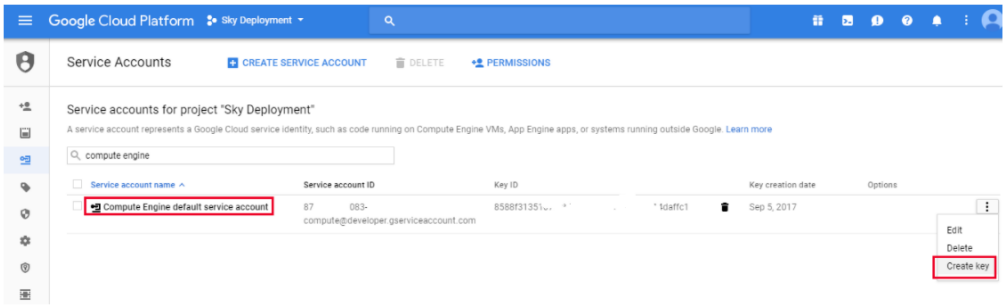
10. When the job is finished, the new VM will appear in the Applications list, unprotected.

    You must access the new host from an appropriate Google Cloud account in the right region.

Generating GCP Access Credentials

You need access credentials:

1. Create a service account from GCP Console > IAM & Admin -> Service Accounts. The Service account must have compute engine permissions. The Compute Engine Default service account can be used.
2. Download the JSON file which contains private keys information for the GCP account.



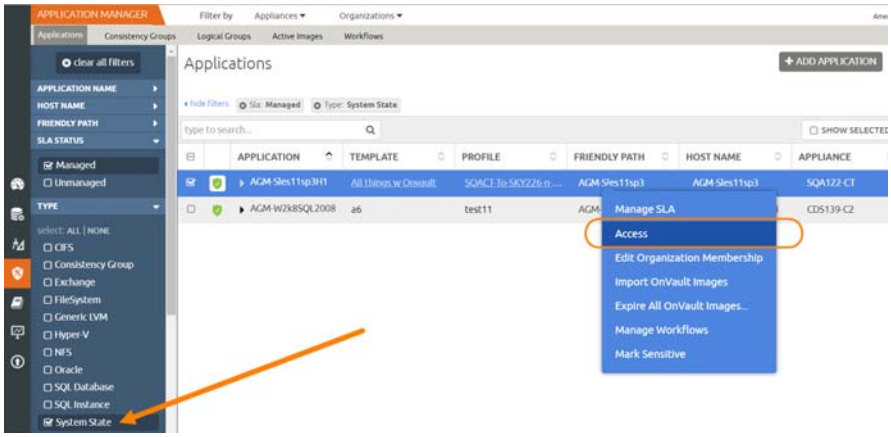
Recovering a Physical Server to a VMware VM

Actifio Cloud Mobility allows you to recover a physical host's System State or a VM to a new VMware VM.

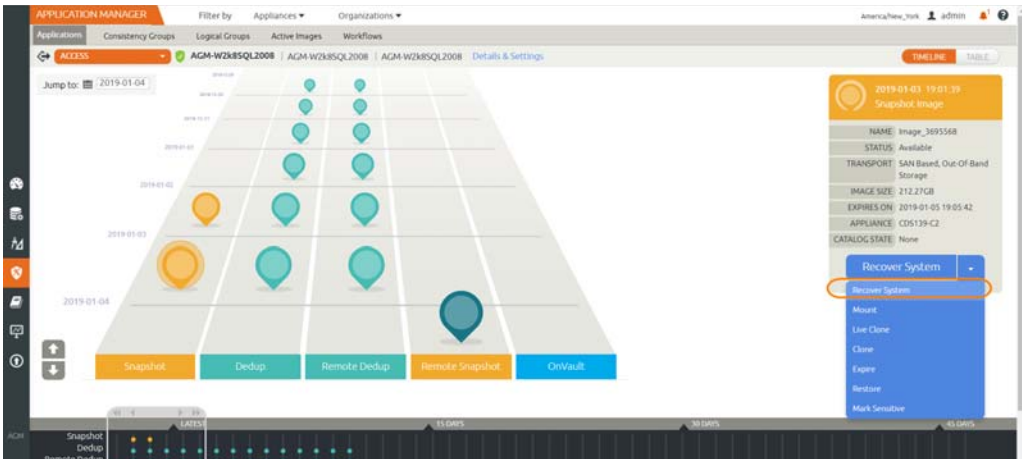
Procedure

To recover a physical host's System State to a VMware VM:

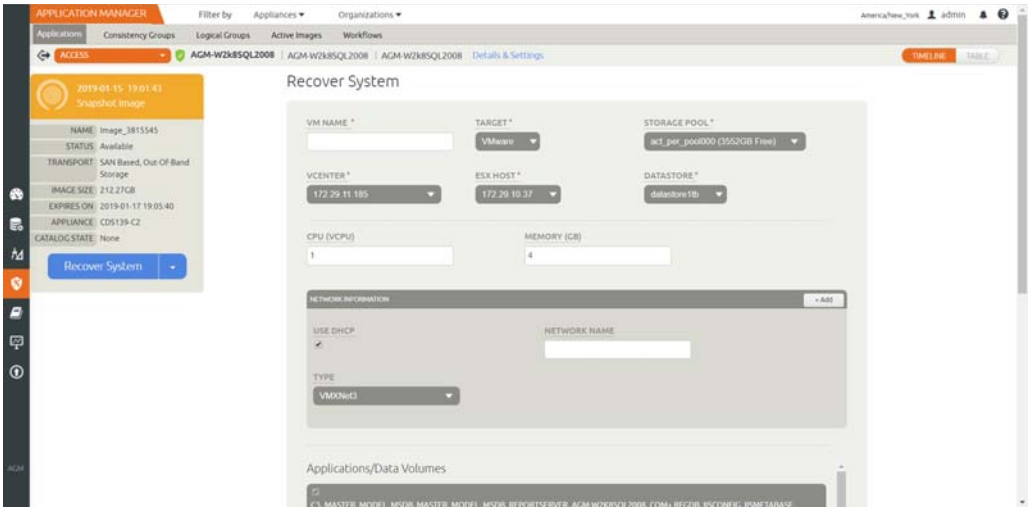
1. Open the Application Manager service in AGM to the Applications window.
2. Select the host that you plan to restore. The System State filter and the search tool can be helpful.
3. Either right-click the image or in the lower right corner, select **Access** from the dropdown list.



4. The timeline or table of images appears.



5. Select an image, then select **Recover System**. The Recover System window opens.
6. From the Target dropdown, select **VMware** to restore to a VMware VM.

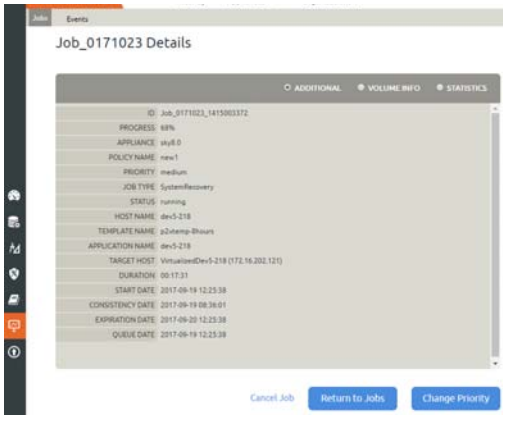


7. Fill in these recover system values:
   - VM NAME: Enter a name for the new virtual machine that you want to create.
   - STORAGE POOL: Select whether to use the Performance Pool or an external storage pool.
   - VCENTER: Select the vCenter that will host the new VM.
   - ESX HOST: Select the ESX server that will host the new VM.
   - DATASTORE: Select the Datastore that will host the new VM.
   - CPU (VCPU): This is prepopulated from the source. If you want to increase the number of CPUs used by the new VM, enter a value here.
   - MEMORY (GB): This is prepopulated from the source. If you want to increase the memory available to the new VM, enter a value here.
   - USE DHCP: Check this if you are using Dynamic Host Configuration Protocol.
   - NETWORK NAME: If you have multiple networks, record the name of the network for the new VM.
   - TYPE: Select the NIC in use, either VMXNet3 or E1000.

   Below the network information is an Applications/Data Volumes section that shows the FileSystems to be restored.

8. Click **Submit**.

9. Follow the progress of the SystemRecovery job in the system monitor. Click on the job to see the job details, including the IP address of the new host.



10. When the job is finished, the new VM will appear in the Applications list, unprotected.