
A VMware vCenter Administrator's Guide to Actifio GO

Actifio GO

Copyright, Trademarks, and other Legal Matter

Copyright © 2021 Google LLC. All rights reserved.

Actifio™, OnVault™, and VDP™ are trademarks of Google LLC.

All other brands, product names, goods and/or services mentioned herein are trademarks or property of their respective owners.

Contents

Preface	v
Actifio Appliances	v
The ActifioNOW Customer Portal	v
Actifio Support Centers	v
Chapter 1 – Introduction	1
Actifio Data Virtualization	1
Capture Mechanisms	2
Capturing Data	3
Setting Data Transport Mode to a Host in VMware	4
Capturing Virtual Server Data	6
Replicating Captured VMware Data	8
WH Monitoring	8
Accessing Data	8
Workflows to Automate Access to Data	9
Chapter 2 – Supporting VMware with Actifio VDP	11
Actifio Sky Appliance Networking Requirements	11
Ensuring iSCSI Connectivity from ESX to Storage	12
Ensuring iSCSI Connectivity with an ESX Server	12
Adding the iSCSI Actifio Definition to the ESX server	12
Configuring AGM to See the ESXi Host	13
Setting NFS Data Transport Mode to a Host in VMware	14
Renaming a vCenter	15
Chapter 3 – Discovering and Protecting VMware VMs	17
Create an SLA Template and Define Backup Policies	17
Creating a Template	17
Creating a Profile	18
Discovering VMs	19
Deleting VMs	21
Discovering Applications on a VM	22

Protect the VMs.....	23
Run an On-Demand Backup of the VM.....	24
Chapter 4 - Mounting a VMware VM Image	27
Mounting a VMware VM (Standard Mount).....	27
Recovering a Mounted VMware VM to Production Storage.....	30
Chapter 5 - Replicating VMware Data to a Datastore	31
Chapter 6 - Restoring Virtual Machines	33
Chapter 7 - Actifio VDP and VMware HA	35
Shutting Down a Managed Actifio Sky Appliance	36
Using VMware VMotion and Storage VMotion.....	37
VMotion for Host Migration of an Actifio-protected VM.....	37
Storage VMotion for Storage Migration of an Actifio-protected VM.....	37
VMware FT (Fault Tolerance) Configurations.....	37
Use of Resource Pools with Actifio Sky Appliance Instances.....	38
Licensing Considerations	38
Networking Considerations.....	39
Best Practices for Actifio Sky Appliance in an HA Failover Configuration.....	39
System Recovery Steps After an HA failover.....	39
Migrating Actifio Sky Appliances.....	40

Preface

This guide provides detailed instructions on how to capture and access VMware data with an Actifio appliance.

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: ActifioGO-CS@google.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 Introduction

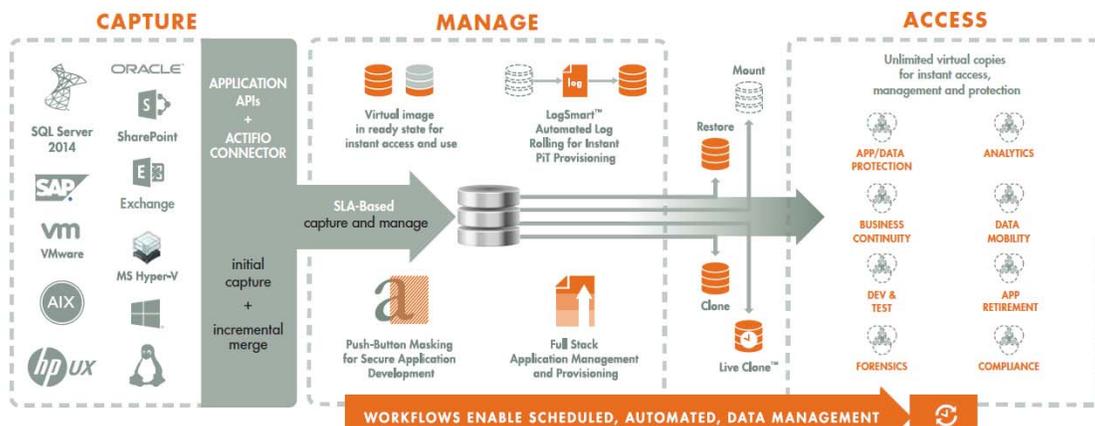
This chapter provides a high-level overview of basic Actifio concepts and procedures used to capture, manage, and access virtual machines (VMs). Specifically, this chapter describes:

- [Actifio Data Virtualization](#) on page 1
- [Capture Mechanisms](#) on page 2
- [Capturing Data](#) on page 3
- [Setting Data Transport Mode to a Host in VMware](#) on page 4
- [Capturing Virtual Server Data](#) on page 6
- [Accessing Data](#) on page 8
- [Workflows to Automate Access to Data](#) on page 9

Actifio Data Virtualization

An Actifio Appliance is a highly scalable copy data management platform that virtualizes application data to improve the resiliency, agility, and cloud mobility of your business. It works by virtualizing data in much the same way other technologies have virtualized servers and networks.

Actifio VDP on an Actifio Appliance enables you to capture data from production systems, manage it efficiently, and access virtual or physical copies of the data whenever and wherever they are needed.



Capture, Manage, and Use Application Data

Application data is captured at the block level in application native format, according to a specified SLA. A Golden copy of that data is created and stored once; it is updated incrementally with only the changed blocks of data in an “incremental forever” model. Unlimited virtual copies of the data can be made available instantly for use, without proliferating physical copies and taking up additional storage infrastructure.

Capture Mechanisms

An Actifio Appliance captures an initial full copy of an application's data or a VM. From then on, only the changed data is captured. To track changes, the Actifio Appliance uses either VMware API calls or the Actifio Connector.

VMware API Calls for Entire VMs

An Actifio Appliance can take advantage of VMware API for data protection (VADP) calls to capture an entire virtual server. Specifically, the API calls can:

Perform change block tracking: Makes an initial full snapshot of a database, then going forward only snapshots the changes to the database thereby enabling Actifio's incremental forever capture strategy.

Quiesce applications: Ensures application consistency during capture.

When an entire VM is captured, a fully functional VM (operating system, applications, and its data) is captured. Having a copy of the entire VM guarantees that the data can be accessed fast and without issues. Because the image presented is a fully functional VM, it can be started and run from an Actifio Appliance directly and then optionally migrated to a new, permanent location.

Virtual servers and their applications can be grouped and captured with a single SLA.

The Actifio Connector, for Individual Applications, Databases, and File Systems

The Actifio Connector is used to capture applications. The Actifio Connector is a small-footprint, lightweight service that can be installed on either virtual or physical servers.

The Actifio Connector provides a more granular capability than what is provided by VMware API calls. You can capture applications that cannot be snapped individually by VMware. It also offers options for handling individual database transaction logs.

Specifically, the Actifio Connector:

- Discovers applications
- Quiesces applications
- Where applicable, takes advantage of Microsoft VSS Writer for discovery, capture, and access operations.
- Identifies changes to application data for Actifio's incremental forever capture strategy.
- Captures databases in clustered application deployments.
- Captures database transaction logs:
 - o Captures database(s) and logs with one Policy Template
 - o Truncates database transaction logs as needed
 - o Rolls logs forward for point-in-time recovery
- Allows you to apply a single Policy Template to multiple VMs and/or applications.
- For VMware VMs:
 - o Captures databases that use pRDMs and vRDMs
 - o Avoids virtual server "stun" issues.

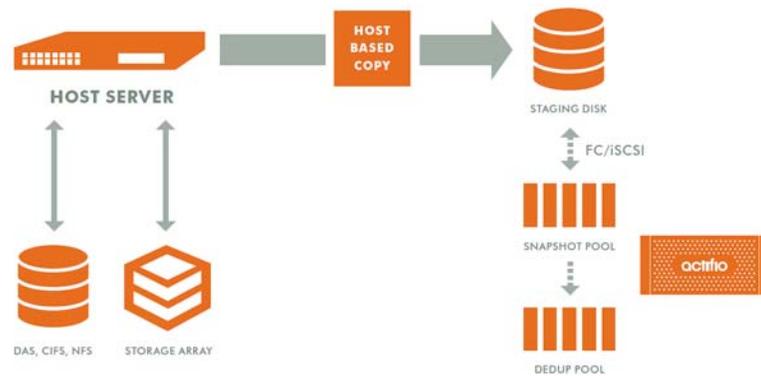
Capturing Data

When an Actifio Appliance protects an entire VM, it is not aware of the VM's contents so no application-specific actions are performed during either backup or restore. To capture selected applications on a VM, use the Actifio Connector as described in [The Actifio Connector, for Individual Applications, Databases, and File Systems](#) on page 2.

The Actifio Appliance captures and manages the application data separately from where the application writes its primary storage.

Snapshots of application data are captured and stored on a staging disk presented to the application host via Fiber Channel or iSCSI.

As shown in the following illustration, an Actifio Appliance presents a staging disk. That staging disk maintains a golden copy of the application's historical data.



Actifio Data Capture

When capturing data:

- A staging disk is automatically created and mounted on a server.
- An initial full copy is made to the staging disk. Subsequent copies consist only of incremental change blocks.
- The staging disk is unmounted from the server.
- A snapshot of the staging disk is made on the Actifio Appliance.

Setting Data Transport Mode to a Host in VMware

NFS Datastore Transport Mode with VMware is an alternative to iSCSI. NFS datastore enables simpler initial setup and fast onboarding of VMs into Actifio VDP. It is available starting with Sky 9.0 and enabled by default for new deployments. You can set the NFS transport mode to a VM host to avoid HBA scans that may cause the VM host to crash.

Before You Begin

To set NFS datastore support on VM:

- The ESX hosts involved in the restore must have the NFS protocol enabled in the Security Profile settings.
- The TCP ports for NFS between the Sky and ESX must be open.

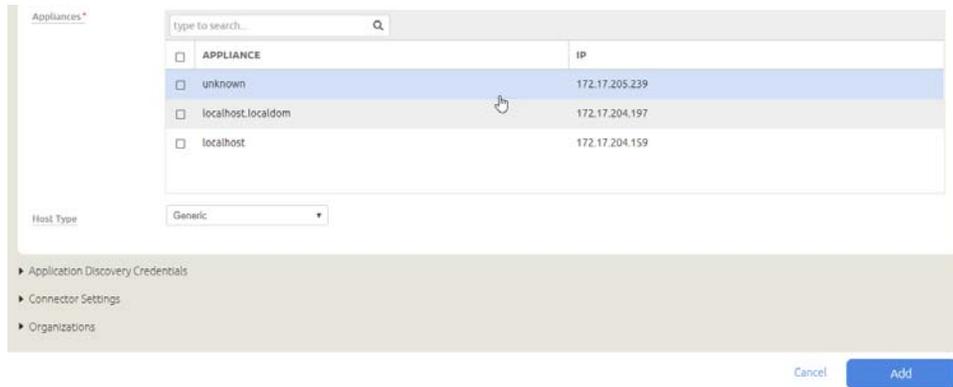
To convert the data transport for mounting staging disks to a Connector-based Windows or Linux host from iSCSI to NFS:

Note: Once the NFS datastore is mounted, you cannot unmount if any images exist.

1. In AGM, click the **Manage** tab and select **Hosts** from the drop-down menu. The Hosts page opens.
2. Select **Add Host**. The upper portion is for network and other identification information. Below that are dynamic sections for host connections and for organizations that the host belongs to.

The screenshot shows the 'Add Host' form in the AGM interface. The form is titled 'Add Host' and contains several input fields: 'Name *', 'Friendly Name', 'IP Address *', and 'Description'. Below these fields is a section for 'Appliances *' which includes a search box and a table of available appliances. The table has columns for 'APPLIANCE' and 'IP'. The 'unknown' appliance is selected. Below the table is a 'Host Type' dropdown menu set to 'Generic'. At the bottom of the form, there are three expandable sections: 'Application Discovery Credentials', 'Connector Settings', and 'Organizations'. At the very bottom right, there are 'Cancel' and 'Add' buttons.

3. Enter the host name and a friendly path for the host. The name of a host should start with a letter, and can contain letters, digits (0–9), and an underscore ('_').
4. Enter the IP address of the host, then click +. You can enter an additional IP address in IP Address. Click + to add each additional IP address for the host.
5. Optionally, add a description of this host.
6. In the Appliances section, select the AGM managed appliances that will serve this host. If the list is long, you can use the Search box to find a specific appliance or group of appliances.



7. Select the **Host Type**: vCenter, ESX Server, or Generic. Select Generic for hosts that are not one of the four VM types. This includes Windows and Linux hosts and all physical hosts. Generic hosts require an Actifio Connector of the type that matches their OS.

For vCenter or ESX Server selections, you also get the option to select a Transport Mode. You see the Transport Mode option only during adding a host. This option can be edited after the host has been added:

- o **NFS** (default): Select NFS if you are in an NFS network. Transport will be Network Based in the Application Manager image details and in the System Monitor Transport column.
- o **SAN** (block storage): Select SAN if you are using Fibre Channel or iSCSI networking. Transport will be SAN Based in the Application Manager image details and in the System Monitor Transport column.

Note: vCenter hosts default to the transport type NFS. This may be incompatible with External Storage Pools (ESP) under certain circumstances. If you plan to use ESP, change the transport type to SAN. For more information, see **Transport Setting for External Snapshot Pools** in the AGM Online help.

8. If you must override the connection settings from the appliance, then click **Connector Settings**, **vCenter Settings**, or **ESX Settings** as appropriate. For more information, refer to Connector Settings Overrides in the AGM Online help.
9. Click **Organizations**. Select one or more organizations for the host to join. For details on Organizations, see Viewing Organizations in the AGM Online help.
10. Click **Submit** to save the host information.

The Edit Host page opens where additional steps are required if you are adding a host that will use NFS storage or Oracle database authentication. If the new host is defined on multiple appliances and if the information is not identical for them all, then you will see the Host Reconciliation page first. Refer to the AGM Online help for more information.

Capturing Virtual Server Data

When capturing virtual machine data, you can capture:

- Applications on a VM
- Applications in a Consistency Group
- Application(s) along with the VM's boot volume
- Entire VMs individually or in groups

Capturing VMs consists of four steps in the VM Onboarding Wizard in the AGM App Manager:

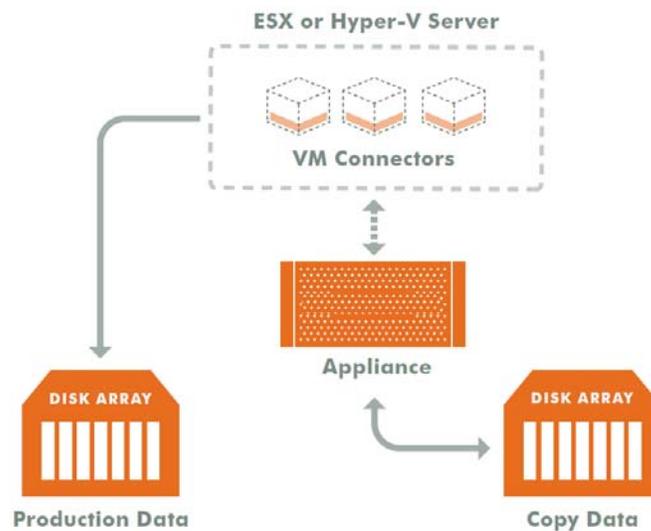
1. Choose the Server for VM Discovery
2. Select Virtual Machines
3. Manage VMs
4. Approve the Onboarding Summary

Note: You can create Production Direct-to-Dedup policies VMware VMs without keeping a snapshot in the Snapshot Pool. Capturing VMware VMs directly to a Dedup Backup Pool is meant for long term retention when instant access from a Snapshot Pool is not required. See the AGM online help for details.

Note: If you capture an entire VM with one policy and also capture individual applications on that VM with another policy, ensure that one capture operation completes before the other capture operation completes.

Capturing Applications on a VM

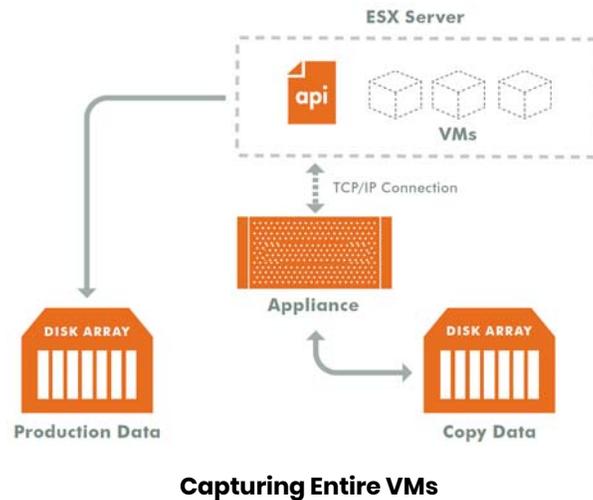
Installing the Actifio Connector on a VM allows you to capture applications on that VM. Multiple applications can be captured with a single policy template, or multiple policies can be used to capture individual applications.



Connectors on Multiple Virtual Machines

Capturing VMs Individually or in Groups

To capture entire VMware VMs, the Actifio Appliance takes advantage of VMware APIs.



Note: A Sky Appliance is a VMware VM. It can be on the same ESX server as the VMs it manages.

When an entire virtual server is captured, a fully functional virtual server (operating system, applications, and its data) is captured. Having a copy of the entire virtual server guarantees that the data can be accessed quickly and without issues. Because the image presented is a fully functional virtual server, it can be migrated to a new, permanent location.

Capturing whole virtual servers allows groups of virtual servers and their applications to be captured with a single SLA Policy Template.

Capturing Applications in Actifio Consistency Groups

A consistency group is enabled by the Actifio Connector. As the name implies, consistency groups ensure consistent point-in-time capture and recovery across multiple applications on the same host.

To achieve application consistency, members of a consistency group are quiesced and captured together via a single policy.

If the Actifio Appliance captures database logs along with the associated database, then all databases in that group can be recovered to the same point-in-time. Recovery and rolling forward of the logs (for databases) in a group is performed via the Actifio user interface with a single action.

In addition to making capture and recovery operations easy and fast, consistency groups consume fewer system resources (VDisks).

Capturing Applications and Boot Volumes

When capturing application data on VMs you have the option of also capturing the VM's boot volume.

When a VM's boot volume is captured along with its application data, if needed, an image can be presented that is a fully functional VM and its applications. The image can then be migrated to a new, permanent location.

Replicating Captured VMware Data

To replicate data, at least two Actifio Appliances must be joined and have exchanged certificates. Details on joining Actifio Appliances can be found in AGM Online Help.

Once Actifio Appliances are joined, Actifio Resource Profiles are used to control where data is replicated.

Actifio Resource Profiles can specify replication of data from either:

- A local Snapshot Pool to a remote Snapshot Pool
- A local Dedup Backup Pool to a remote Dedup Backup Pool
- A local Snapshot Pool to a remote OnVault pool
- A local Snapshot Pool to a remote VMware datastore. See [Replicating VMware Data to a Datastore](#) on page 31 for details.

WH Monitoring

Datastore space utilization is checked before creating the snapshot and also monitored throughout the data movement process while data is copied from VMware snapshot to Actifio staging disks/direct dedup objects.

In the case where the data is being replicated to a remote VMware datastore, the local datastore and the remote datastore space usage are monitored during data movement. If a critical threshold is crossed in any of the data movement jobs, all subjobs are canceled and the job fails.

Critical threshold and the frequency at which datastore usage is monitored are defined in: **Manage > Storage Pools.**

Accessing Data

Role-based Access Control

Actifio administrators can control which users have access to data, Actifio features, processes, and resources. In addition, captured data can be defined as sensitive or non-sensitive. Actifio users can be granted permission to access sensitive or non-sensitive data.

Captured VMs, VM data, or applications on a VM can be accessed in these three ways:

Mounts

The Actifio mount function provides instant access to data without moving data. Captured copies of databases can be rolled forward via the Actifio user interface and mounted on any database server.

An Actifio Appliance provides two ways to mount data:

- **The standard mount** presents and makes the captured data available to a target server as a file system, not as a VM or application. This is useful if a VM or application is corrupt, lost, or if a server is being replaced. In such cases you cannot use a restore operation to recover the application or VM. Instead, you can mount an image and copy the data from the mounted image to their original location on a server.
- **The Application Aware mount** presents and makes a captured database available to a target server as a database. This allows you to address the unique challenges associated with creating and managing copies of production databases for non-production use. Application Aware mounts are performed from the Actifio Appliance and do not require manual intervention by database, server, or storage administrators. Application Aware mounts can be used for such things as database reporting, analytics, integrity testing, and test and development.

LiveClones

The LiveClone is an independent copy of a VM or an application on a VM that can be refreshed when the source data changes. The advantage of a LiveClone is that it is an independent copy of data that can be incrementally refreshed and masked before being made available to users. This allows teams such as development and test to ensure they are working on the latest set of data without having to manually manage the data or access the production environment.

Restores

The restore function reverts production data to a specified point in time. Restore operations actually move data. Typically restore operations are performed to restore a VM or application to a valid state after a massive data corruption or storage array failure. The amount of time required to complete a restore operation depends on the amount of data involved.

Note: Actifio provides the flexibility to restore to the original server or to an alternate server. To restore to an alternate server, the Actifio Connector must be installed on the alternate server before initiating the restore operation.

To restore a database and then apply logs, the restored database must be in Restoring Mode. Actifio's log capture and restore functionality allows you to, from the Actifio user interface, restore the database in Restoring Mode and then roll the logs forward to a specific point in time.

If you restore a database without specifying Restore with no Recovery, the database will be restored and brought on line without applying logs.

Workflows to Automate Access to Data

Workflows are built with captured data. Workflows can present data as either a direct mount or as a LiveClone:

- Direct mounts (standard or application aware) work well for application data that does not need to be masked prior to being presented. A mounted copy of data can be refreshed manually or automatically on a schedule. Direct mounts allow you to instantly access captured data without actually moving the data.
- A LiveClone is a copy of your production data that can be updated manually or on a scheduled basis. You can mask sensitive data in a LiveClone prior to making it available to users.

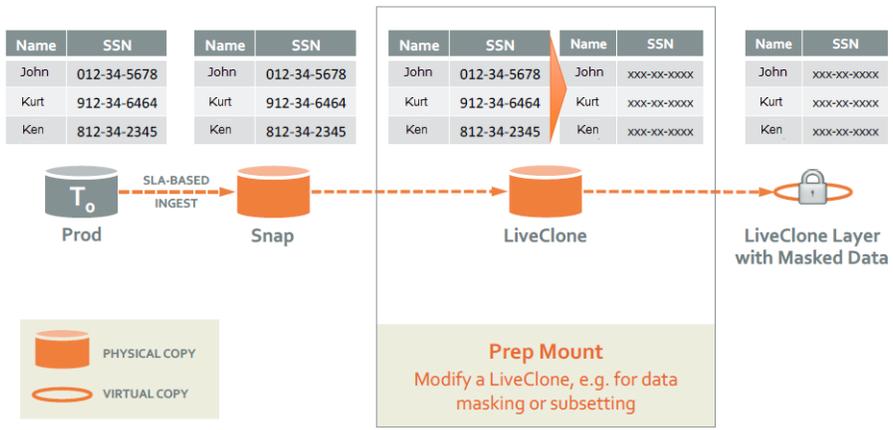
Combining Actifio's automated data capture and access control with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait weeks for DBAs to update test and development environments, users can provision their own environments almost instantly.

For example, an Actifio administrator can create an SLA Template Policy that captures data according to a specified schedule. Optionally, the administrator can mark the captured production data as sensitive and only accessible by users with the proper access rights.

After access rights have been defined and data has been captured, the administrator can create a Workflow that:

- Makes the captured data available as a LiveClone or a direct mount
- Updates the LiveClone or mountable data on a scheduled or on demand basis
- Optionally automatically applies scripts to the LiveClone's data after each update. This is useful for masking sensitive data.

Once the Workflow completes, users with proper access can provision their environments with the LiveClone or mountable data through the AGM.



Workflow With Masked Social Security Data

2 Supporting VMware with Actifio VDP

This includes:

- [Actifio Sky Appliance Networking Requirements](#) on page 11
- [Ensuring iSCSI Connectivity from ESX to Storage](#) on page 12
- [Ensuring iSCSI Connectivity with an ESX Server](#) on page 12
- [Setting NFS Data Transport Mode to a Host in VMware](#) on page 14

Actifio Sky Appliance Networking Requirements

Sky Appliances installed in a vCenter require the following network settings:

- **Static IPs:** You must provide static IPs for the NIC on the Sky Appliance.
- **VMXNET3:** Sky Appliance must use the VMXNET3 Ethernet adapter. These adapters enable 10GB performance.

Actifio Sky Network Protocol support

Actifio Sky installed in a VMware environment supports storage presentation (as part of backup/recovery and mount operations) over iSCSI or NFS. The configuration requirements for each of these protocols are:

- **NFS:** As long as you have a network connection from both the Sky Appliance and the vSphere host that the VM resides on, all backups and mounts using NFS will proceed normally. You can use NFS over your network without configuring iSCSI.
- **iSCSI:** The Sky Appliance uses iSCSI to mount data. Ensure that iSCSI is on for the Sky Appliance's vSphere host, and for the servers that host the data the Sky Appliance will capture and manage.

When capturing an entire vSphere VM, iSCSI does not need to be configured on the vSphere host that hosts the VM to be captured. Once the VM has been captured, to present the VM to another vSphere host, including the vSphere host from which it was captured, the vSphere host must have iSCSI configured.

When capturing individual applications on a VM, rather than capturing the entire VM, iSCSI must be configured on the VM's vSphere host.

Note: For best iSCSI network traffic results, see [Ensuring iSCSI Connectivity on a Linux Host](#) on page 35.

Each Sky Appliance can support up to 100 iSCSI sessions.

Ensuring iSCSI Connectivity from ESX to Storage

To test the iSCSI connection from an ESXi server to a Sky appliance:

1. Enable ESXi Shell and connect to ESXi as root.
2. Use netcat (nc) command to confirm connectivity:

```
~ # nc -z 123.45.67.89 3260  
Connection to 123.45.67.89 3260 port [tcp/*] succeeded!
```

This example confirms that the device is listening on that port. If a port is unreachable then you return to the prompt with no output.

Note: ESXi does not have telnet, so issuing a ping does not prove that connectivity for iSCSI is available.

Ensuring iSCSI Connectivity with an ESX Server

This has two parts:

1. [Adding the iSCSI Actifio Definition to the ESX server](#) on page 12
2. [Configuring AGM to See the ESXi Host](#) on page 13

Before You Begin

In order to ensure connectivity to ESX servers reached via iSCSI:

- Check that the network ports are as described in **Network Administrator's Guide to Actifio GO**.
- Check each ESX server to be sure that these are set to the following recommended values:

Setting	Recom. Value	Description
LoginTimeout	60	When iSCSI establishes a session between initiator and target, it must log into the target. It will try to log in for a period of LoginTimeout. If the login attempt exceeds LoginTimeout, then the login fails.
Noopinterval	30	iSCSI uses the noop timeout to passively discover if this path is dead when it is not the active path.
Nooptimeout	30	This is tested on non-active paths every NoopInterval. If no response is received by NoopTimeout, the path is marked dead.

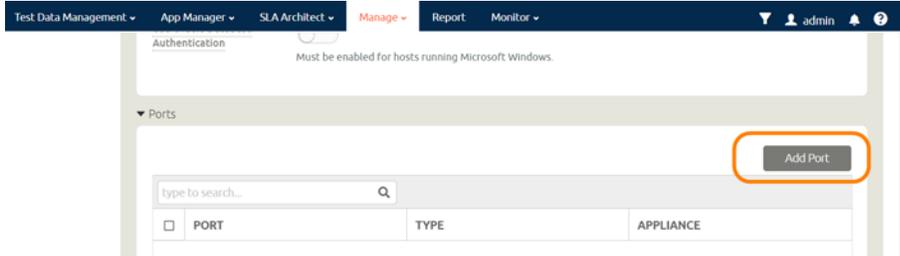
This procedure is for a single Actifio Ethernet iSCSI connection to a single iSCSI Ethernet connection on the ESX server. Actifio Professional Services can help you with any other configuration.

Adding the iSCSI Actifio Definition to the ESX server

1. Highlight the ESX server in vCenter and select the **Configuration** tab.
2. Select the iSCSI Software Adapter and then **Properties**. A pop up window appears to discover the Actifio iSCSI connection.
3. Select Dynamic Discovery tab and click **Add** to add the iSCSI IP of the Actifio Appliance.
4. Enter the IP address of the Actifio iSCSI port and click **OK**. It is added to the target listing.
5. Right click on the iSCSI software adapter and click **Rescan**.
Continue to [Configuring AGM to See the ESXi Host](#) on page 13.

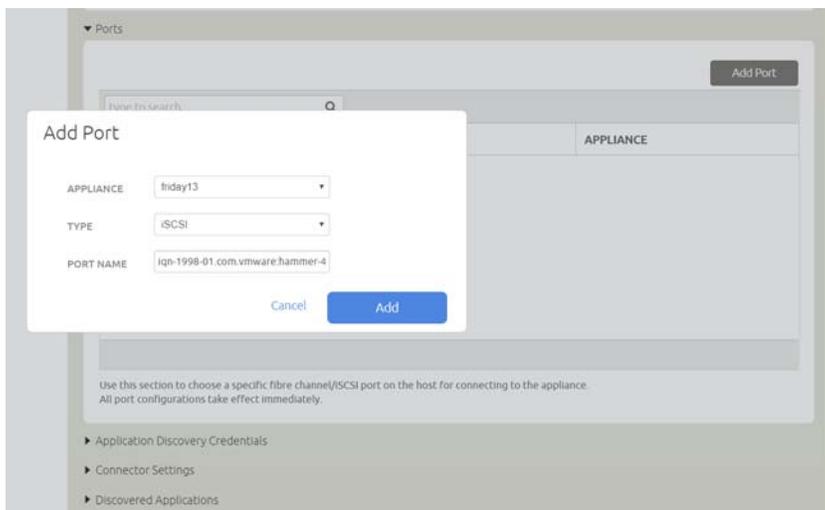
Configuring AGM to See the ESXi Host

1. Open AGM to **Manage > Hosts**.
2. Right-click the ESXi server and select **Edit**.
3. Scroll down the right side to the Ports section and click **Add Port**.



Configuring AGM to Recognize an ESX Server

4. From the Type menu, select **iSCSI**.
5. At Port Name, enter the iSCSI iqname, and click **Add**. This will configure the iSCSI relationship on Actifio to the ESX server.



Adding the Port

Setting NFS Data Transport Mode to a Host in VMware

NFS Datastore Transport Mode with VMware is an alternative to iSCSI. NFS datastore enables simpler initial setup and fast onboarding of VMs into Actifio VDP. It is enabled by default for new deployments. You can set the NFS transport mode to a VM host to avoid HBA scans that may cause the VM host to crash.

Before You Begin

To set NFS datastore support on VM:

- The ESX hosts involved in the restore must have the NFS protocol enabled in the Security Profile settings.
- The TCP ports for NFS between the Sky and ESX must be open.

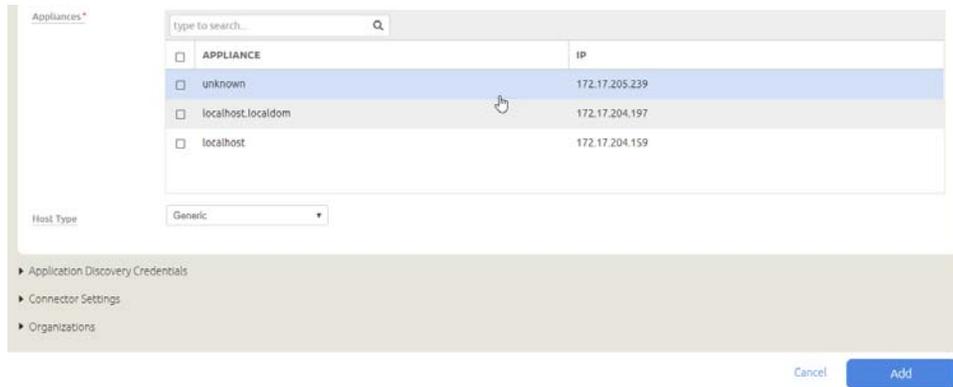
To convert the data transport for mounting staging disks to a Connector-based Windows or Linux host from iSCSI to NFS:

Note: Once the NFS datastore is mounted, you cannot unmount if any images exist.

1. In AGM, click the **Manage** tab and select **Hosts** from the drop-down menu. The Hosts page opens.
2. Select **Add Host**. The upper portion is for network and other identification information. Below that are dynamic sections for host connections and for organizations that the host belongs to.

APPLIANCE	IP
<input type="checkbox"/> unknown	
<input type="checkbox"/> localhost.localdom	
<input type="checkbox"/> localhost	

3. Enter the host name and a friendly path for the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Enter the IP address of the host, then click +. You can enter an additional IP address in IP Address. Click + to add each additional IP address for the host.
5. Optionally, add a description of this host.
6. In the Appliances section, select the AGM managed appliances that will serve this host. If the list is long, you can use the Search box to find a specific appliance or group of appliances.



7. Select the **Host Type**: vCenter, ESX Server, or Generic. Select Generic for hosts that are not one of the four VM types. This includes Windows and Linux hosts and all physical hosts. Generic hosts require an Actifio Connector of the type that matches their OS.

For vCenter or ESX Server selections, you also get the option to select a Transport Mode. You see the Transport Mode option only during adding a host. This option can be edited after the host has been added:

- o **NFS** (default): Select NFS if you are in an NFS network. Transport will be Network Based in the Application Manager image details and in the System Monitor Transport column.
- o **SAN** (block storage): Select SAN if you are using Fibre Channel or iSCSI networking. Transport will be SAN Based in the Application Manager image details and in the System Monitor Transport column.

Note: vCenter hosts on appliances default to the transport type NFS. This may be incompatible with External Storage Pools (ESP) under certain circumstances. If you plan to use ESP, change the transport type to SAN. For more information, see *Transport Setting for External Snapshot Pools in the AGM Online help*.

8. If you must override the connection settings from the appliance, then click **Connector Settings**, **vCenter Settings**, or **ESX Settings** as appropriate. For more information, refer to Connector Settings Overrides in the AGM Online help.
9. Click **Organizations**. Select one or more organizations for the host to join. For details on Organizations, see Viewing Organizations in the AGM Online help.
10. Click **Submit** to save the host information.

The Edit Host page opens where additional steps are required if you are adding a host that will use NFS storage or Oracle database authentication. If the new host is defined on multiple appliances and if the information is not identical for them all, then you will see the Host Reconciliation page first. Refer to the AGM Online help for more information.

Renaming a vCenter

If you change the name of a vCenter, then remember to rename the vCenter within AGM.

If the UUID of a captured VM changes, then a new full copy will occur on the next backup job.

3 Discovering and Protecting VMware VMs

This chapter details:

- [Create an SLA Template and Define Backup Policies](#) on page 17
- [Discovering VMs](#) on page 19
- [Deleting VMs](#) on page 21
- [Discovering Applications on a VM](#) on page 22
- [Protect the VMs](#) on page 23
- [Run an On-Demand Backup of the VM](#) on page 24

Create an SLA Template and Define Backup Policies

To back up a VM, you need a Policy Template and a Profile. Once you have the Policy Template and Profile in place, you can discover the VMs and back them up with your defined policy. This step involves [Creating a Template](#) and [Creating a Profile](#).

Creating a Template

Now create an SLA Template to set how to backup, how frequently to backup, and how long to retain the backup image.

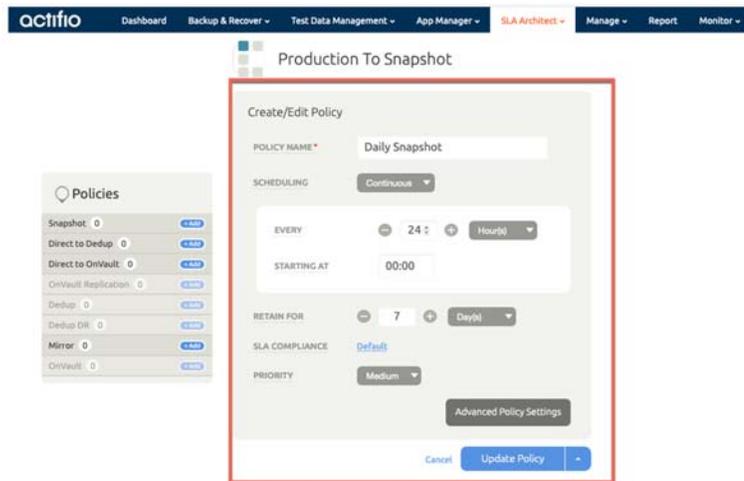
1. In the AGM, navigate to the SLA Architect, Templates page and click CREATE TEMPLATE.



2. This opens a new template page. Enter a meaningful template name and description. It is common to use “Gold” templates (backup policies) to protect tier 1 applications with RPO of less than an hour, and “Silver” for tier 2 applications that have RPO needs between 1 to 12 hours.



- Click on the **+** button between the production and snapshot box (or click on Policies, Snapshot, + Add button). This opens the “Production to Snapshot” page. Give the backup policy a name.



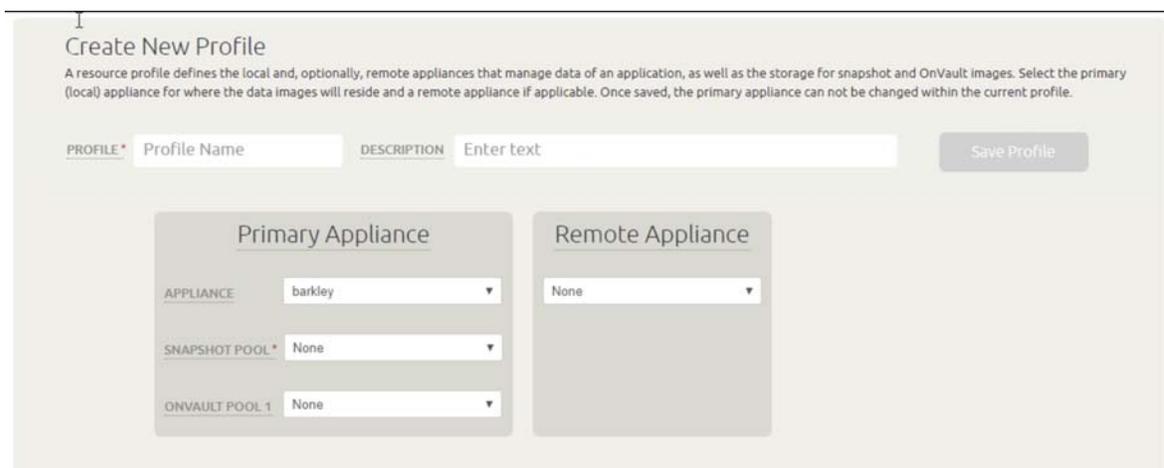
- Change the scheduling to **Continuous**.
 - Every: Specify how frequently you want to backup the data. Since we said we would want to snapshot once a day, set the backup frequency to be **Every 24 hours**.
 - Starting At: Specify the start time at which you want the backup policy to trigger.
 - Retain For: Specify the duration for which these backups should be retained. (If you use 7 days retention, then each snapshot will expire after 7 days).
- There is no need to set Advanced Policy Settings.
- Click **Update Policy**. This takes you back to the previous page.
 - Click **Save Template**.

Now you have a template with a policy that will snapshot images of your VM and retain the images for the retention period before expiring them automatically. Now you need a Resource Profile.

Creating a Profile

Profiles determine which storage pool in an Actifio Appliance is used to hold images of applications that Actifio created from VMware API integration.

Go to **SLA Architect, Profiles**. Select a snapshot or OnVault pool on the local appliance and optionally a pool on a remote appliance.



Discovering VMs

Use the VM Onboarding Wizard from the App Manager to discover virtual machines (VMs) managed by a vCenter or by an individual ESXi server. Once you have discovered one or more VMs, you can protect them all at once by applying an SLA Template and Profile or you can simply add them to the Applications list as unmanaged or ignored VMs.

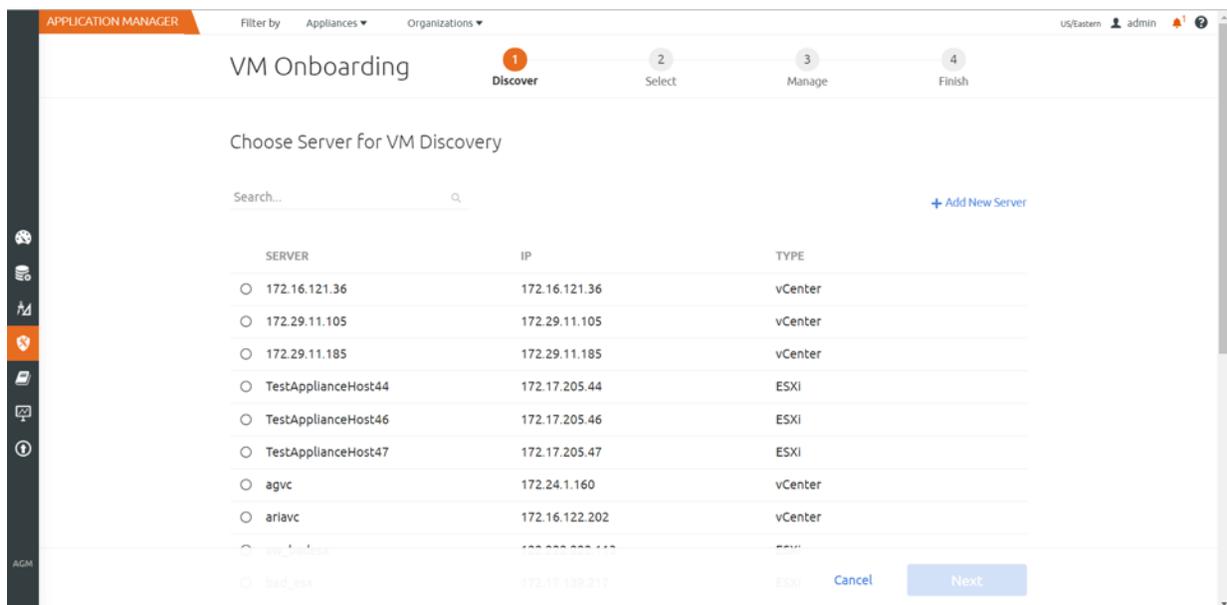
During AGM configuration, you may have already added the ESXi servers and vCenters as hosts to Sky Appliances. See **Network Administrator's Guide to Actifio GO** for more information. The VM Onboarding Wizard also allows you to add a server in case it was not added before.

Note: When you discover a VMware vCenter, all ESXi hosts are automatically discovered.

Note: Virtual machine discovery on a hypervisor requires an Actifio user with 'Host Manage' Actifio rights.

To discover a VM:

1. In AGM, go to **App Manager** and click **Add Virtual Machine**. The VM Onboarding Wizard opens and shows the Choose Server for VM Discovery page.



Page 1 of the Onboarding Wizard

2. Follow the Wizard to the Onboarding Summary at the end and click Finish. After discovery, the virtual machines and hypervisors are added as hosts in the **Manage** Hosts list.

APPLICATION MANAGER Filter by Appliances Organizations US/Eastern admin

VM Onboarding

1 Discover 2 Select 3 Manage 4 **Finish**

Onboarding Summary

- 1 VM will have an SLA applied

VM	ACTION	STATUS
actsky08 Datacenter/Rd_Cluster/actsky08	Apply SLA	--

Cancel Previous **Finish**

The Onboarding Summary for a Simple Job

Note: The Sky Appliance relies on synchronicity between an Sky Appliance and its discovered hosts. Hosts that are not connected to an NTP server can drift, resulting in differences between the host's record and the Sky Appliance's record of the time snapshots taken or other actions performed by the Sky Appliance.

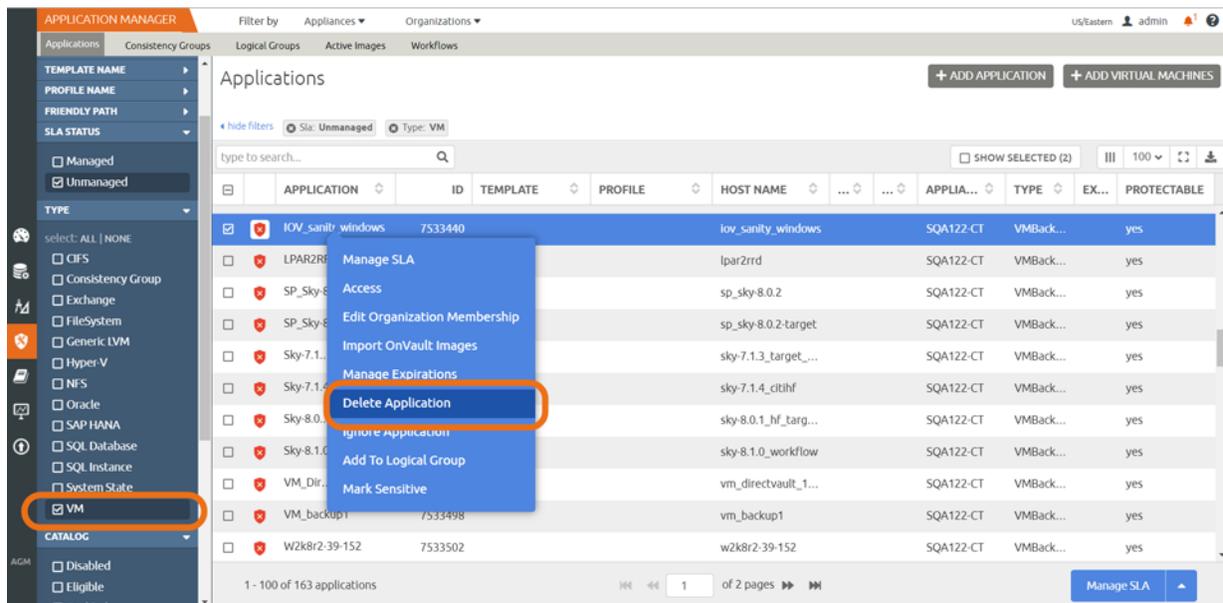
Deleting VMs

You can delete unprotected VMs. To delete protected VMs, first unprotect them by disassociating all SLAs.

Note: Remote VMs that appear in the App Manager Applications list under the Remote category should be deleted from the remote Sky Appliance.

To delete a VM:

1. In AGM, go to **App Manager > Applications**.
2. Click the VM filter tab from the filters on the left side.
3. Select the VM to delete.
4. Right-click it to open the service menu, and click **Delete Application**.



The Application Manager Navigation Pane List Filter

5. Click **Yes** in the confirmation dialog.

Images from a deleted application appear as orphans in the navigation pane under Orphan. You can see an application in the orphan section only if there are any images of that application.

You can delete a resource profile or a policy template only when the resource profile or policy template is not used to protect an application.

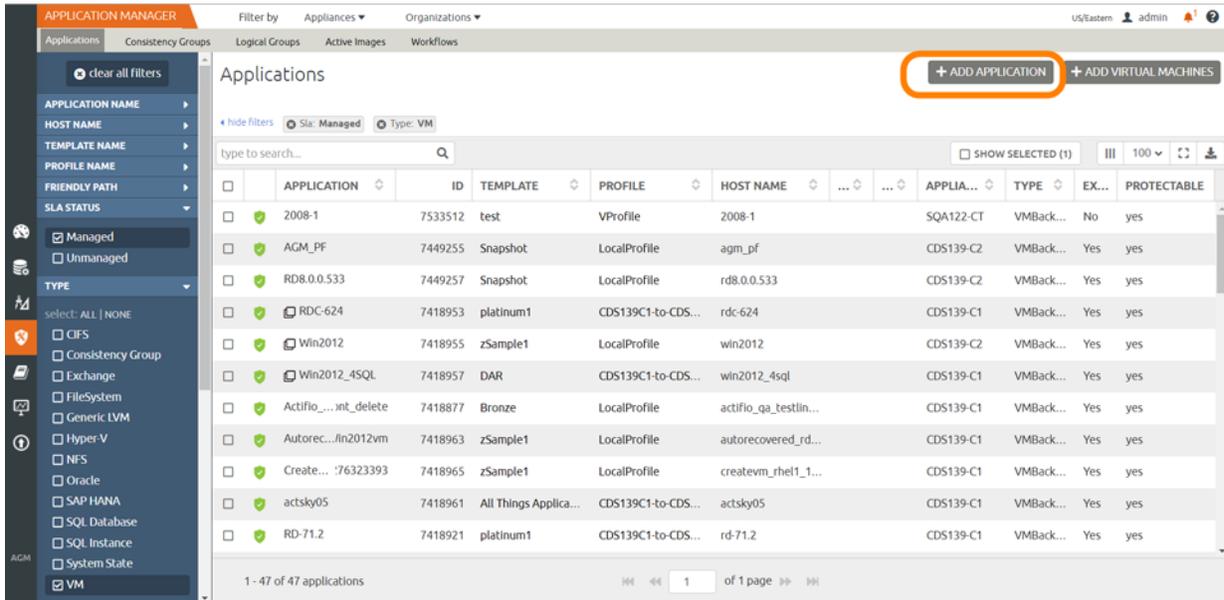
Note: Deleting a VM or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that VM). If any stale images are left on a Sky Appliance (usually due to a remote appliance unavailability), in the left bottom menu list of Appliance Configuration, under the gear icon, you will see an operation called **Cleanup Dedup Async** or **Cleanup StreamSnap**. For more information, see the AGM Online Help.

Discovering Applications on a VM

You can discover applications on VMs that are known to the Sky Appliance. You must have the 'Host Manage' or 'Application Manage' rights to discover applications and the Actifio Connector must be installed and configured on the host.

To discover an application:

1. Open the AGM and go to the **App Manager**. In the upper right corner, click **+ Add Application**.



Adding Applications from the App Manager

2. The Add Applications page appears. Select **Discover connector supported Applications and Using Existing Host**.
3. From the Appliance drop-down list, select the Actifio appliance that connects to the host(s) that includes the applications you would want AGM to discover. You can choose All for multiple appliances or select a specific appliance.
4. Select the host that includes the application you would like to protect. If you have many hosts, then you can use the filters to make the list more manageable.
5. Select one or more hosts from the Available Hosts table, then click **Add Applications**.

Note: The application discovery process can take some minutes, depending on the number of hosts and the applications associated with the selected hosts.

6. Verify the application discovery status in the Notification Center.
7. Add additional applications or proceed to the application list in the App Manager. The discovered applications are added to the list of applications in the Application List window of the App Manager.

Note: Instructions for installing and configuring the Actifio Connectors are in **Network Administrator's Guide to Actifio GO**.

Protect the VMs

Note: Application-consistent backups require VMware Tools.

The AGM Onboarding Wizard brings you to the Manage VMs page, where you can protect the VMs.

1. In AGM's **Backup and Recover** menu, select **Backup**. The onboarding wizard displays a variety of supported application types. Select **VM**.
2. In the Manage VMs window, under Choose action, select **Apply SLA**.
3. The Choose template drop-down list opens. Select a template, then select a profile when the Choose profile drop-down list opens.



The screenshot shows a window titled "Manage VMs". Below the title bar, there is a label "For 1 VM:" followed by three dropdown menus. The first dropdown menu is set to "Apply SLA", the second to "New Template9", and the third to "LocalProfile". To the right of these dropdowns is a blue button labeled "OK".

4. Click **OK** to assign the profile and template to the selected VMs.
You can place your mouse over the Preview section to look at detailed information about the policies contained in the template. Information includes policy name, the frequency in which each policy is run, whether it runs continuously or within a window, and whether it has retention capability.
5. Click **Next**.
6. A Summary screen will display. Select **Finish** to complete the onboarding process which will start backing up the selected VMs based on the Policy Template you attached.
7. After onboarding is complete, a pop-up appears. Click **Finish** again. Once the policy template is attached to the selected VMs, the status changes to a green check mark.

Actifio GO will ensure that the chosen VMs get backed up as per the frequency set in the backup policy. With a continuous backup policy, the first (full) backup job will be automatically triggered. Subsequent backup jobs will be triggered according to the frequency/schedule.

Run an On-Demand Backup of the VM

We can now run an on-demand backup of our VM.

1. In the AGM, go to **App Manager, Applications** and select the VM for which you want to trigger an on-demand backup. Right-click the Application and select **Manage SLA**.



2. On the Manage SLA page, in the Policies section on the right side of the page, expand **Snapshot** and then **Daily Snapshot**. This exposes the **Run SLA** button. Enter a meaningful label and use that button to run an on-demand backup of your VM.

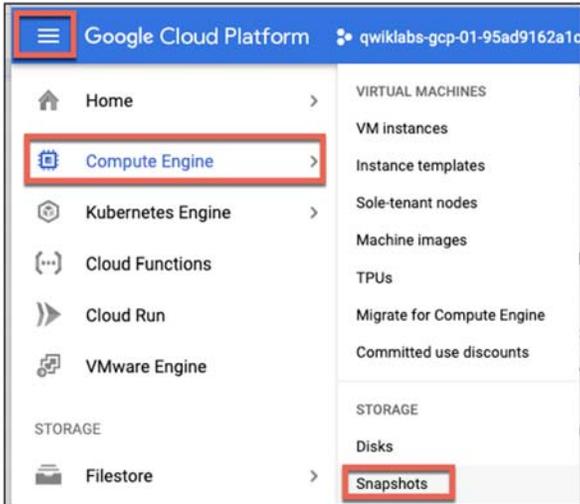


3. Now go to the **Monitor** menu and select **Jobs**. A scheduled job may have run already (is Scheduled is Yes) and an on-demand should have run (Is Scheduled is No). The duration of both jobs should be short although the first one will be longer as it was a full copy (from Persistent Disk to Object storage).

JOB	STATUS	HOST	APPLI...	APPLI...	QUEU...	START...	ENDED	DURA...	TYPE	TEMP...	POLICY	PRIOR...	TRAN...	IS SCH...
Job_0...	Succeeded	centos-7	centos-7	skybas...	2021-0...	2021-0...	2021-0...	00:00:23	snapshot	PD Sna...	Daily S...	medium	netwo...	No
Job_0...	Succeeded	centos-7	centos-7	skybas...	2021-0...	2021-0...	2021-0...	00:00:33	snapshot	PD Sna...	Daily S...	medium	netwo...	Yes

If you see no jobs listed, see if a Filter is set (they are listed above the search box).

You can also see your snapshots in the Google Cloud Console at **Compute Engine, Snapshots**.



If there were two Actifio generated snapshots, then you see two Snapshots in Pantheon. The Creation type for both snapshots is Manual because they were generated by an API call sent by the Actifio Appliance.

A screenshot of the Google Cloud Snapshots page. The page shows a table of snapshots with columns for Status, Name, Location, Snapshot size, Creation time, Creation type, Source disk, and Disk size. Two snapshots are listed, both with a 'Manual' creation type, which is highlighted with a red box. The first snapshot is 'snap-centos-7-002' (731.89 MB) and the second is 'snap-centos-7-810' (12.91 MB).

Status	Name	Location	Snapshot size	Creation time	Creation type	Source disk	Disk size
<input type="checkbox"/>	snap-centos-7-002	us	731.89 MB	May 26, 2021, 3:34:07 PM UTC+10:00	Manual	centos-7	20 GB
<input type="checkbox"/>	snap-centos-7-810	us	12.91 MB	May 26, 2021, 3:35:46 PM UTC+10:00	Manual	centos-7	20 GB

4 Mounting a VMware VM Image

This chapter provides instruction for mounting VMware VMs:

- [Mounting a VMware VM \(Standard Mount\)](#) on page 27
- [Recovering a Mounted VMware VM to Production Storage](#) on page 30

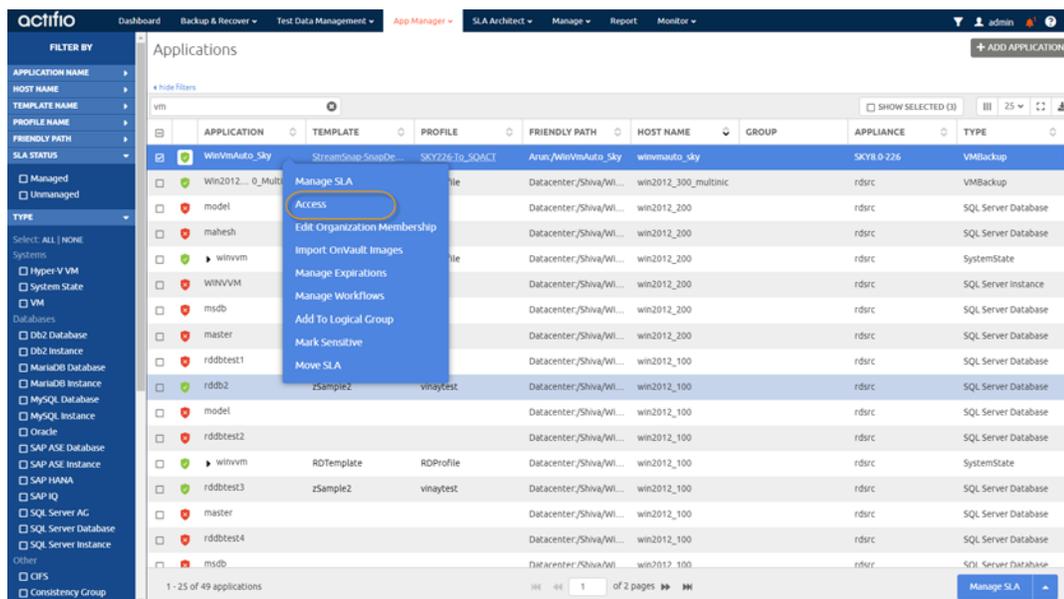
When mounting to an existing VM, no settings are preserved. Captured VMDK volumes are presented as vRDM/pRDM disks to the target VM.

The Actifio Appliance can present 45 LUNs to a VM, and a VM can have a maximum of 60 LUNs (including existing ones and mounted volumes).

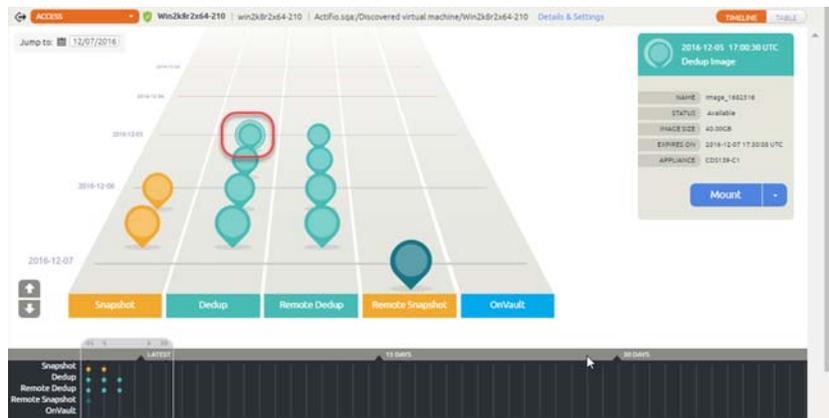
Mounting a VMware VM (Standard Mount)

To mount an active image to a VMware VM:

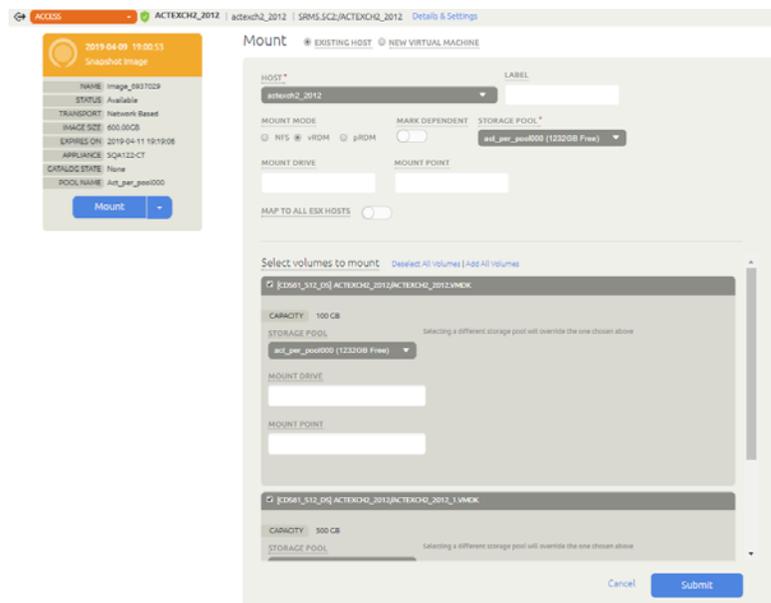
1. Go to AGM and click **App Manager** and then select **Applications**. The Applications page opens.
2. Right-click the VM image that you want to mount, then choose **Access** from the drop-down list at the bottom of the Applications page.



The Timeline ramp view is a time-based visualization of 7 days of captured images for the selected application. You can use your mouse scroll wheel or the up and down arrows in the bottom left corner of the page to move the timeline through the captured images and make a selection.



3. Select an image, then select **Mount** from the list of access operations. The Mount page opens.



4. Select a host to mount to: **Existing Host** or **New Virtual Machine**.
 - If you select Existing Host, select a physical or virtual host from Host drop-down list. You can select any known host from the drop-down list, grouped into Physical Machines and Virtual Machines. If you need a host that has not yet been added, add it from the **Manage > Hosts**.
 - If you select New Virtual Machine, make the following selections specific to the virtual machine:
 - o **VM Name:** Enter a name for the new VM that you want to mount,
 - o **VCENTER:** Select a vCenter from the drop-down list for the new VM you want to mount.
 - o **ESX HOST:** Select an ESX Host from the drop-down list for the new VM you want to mount.
 - o **DATASTORE:** Select a datastore that has the required storage available from the drop-down list for the new VM you want to mount.

Note: The target Actifio appliance must write configuration data to the selected datastore to point to the mounted volumes, but no storage will be consumed by the image virtual copy.

When mounting as a new VM, the VM version, Guest Id, Number of CPUs, Memory, and Hardware details are preserved. Backed up VMDK volumes are presented as vRDM/pRDM disks to the new VM.

5. For Mount Mode, select one of the following:
 - o **NFS** if you are in an NFS network environment.
 - o **vRDM** (virtual raw device mapping) if you need the ability to move the mounted image with VMware VMotion without taking down the VM. The maximum vRDM size for ESXi 5.0 and 5.1 is 2 TB minus 512 B. In ESXi 5.5, the size was increased to 62 TB. By default vRDM mode is selected.
VMware snapshots treat mounted vRDMs as Independent and are not included in snapshots. Because of this, by default, Actifio does not include vRDMs when protecting a mounted VM. Actifio does provide an option where you can mark vRDMs as Dependent. Although rarely used, when this option is enabled, vRDMs will be included in VMware snapshots. Actifio SLA templates will capture vRDMs marked as Dependent and the captured data will be counted in MDL usage.
 - o **pRDM** (physical raw device mapping) is used for file level restore operations, and if you want to share the mounted image. pRDMs can be up to 64 TB. In many cases, pRDM is your best choice.
6. For **Mark Dependent**, VMware snapshots treat mounted vRDMs as Independent and are not included in snapshots. Because of this, by default, Actifio does not include vRDMs when protecting a mounted VM. Use this setting to mark vRDMs as Dependent. Although rarely used, when this option is enabled, vRDMs will be included in VMware snapshots. Actifio SLA templates will capture vRDMs marked as Dependent and the captured data will be counted in MDL usage.
7. If necessary, change the default storage pool from the Storage Pool drop-down list. The default storage pool is `act_per_pool` (the Snapshot Pool).
8. If desired, enter a unique name associated with the mount in **Label**.
9. Specify the following mount selections:
 - o **Mount Drive:** (Windows only). Specifies a drive letter to be assigned to the volume. If the drive letter is not available, the job fails. If multiple volumes are found, then it assigns subsequent drive letters. If no Mount Drive is specified, the Actifio Connector chooses a drive letter itself, if available.
 - o **Mount Point:** The full path at which you want to mount the volume. If the path exists as an empty folder, the Actifio Connector will use it. If it does not exist, the Actifio Connector will create it. If it exist as a file or as a folder that is not empty, then the job will fail. If there are multiple volumes to be mounted, the Actifio Connector chooses the user specified for one of the volumes and for the remaining it appends an underscore (`_`) followed by a number (for example, `<user_specified>_#`).
10. Click **Map to All ESX Hosts** to instruct AGM to map the mount settings to all ESX hosts.
11. Select a single volume or multiple volumes to mount from the **Select Volumes To Mount** area. By default, all the volumes are selected, and the first volume cannot be deselected. If you mount to an existing VM, the VM disks will show up as a new filesystem drive on the VM.

Note: AGM assumes that the first volume of the VM is the boot volume. If the selected first volume is not the boot volume, contact Actifio support for further assistance.

Specify the Storage Pool, Mount Drive, and Mount Point for each volume you want to mount.

12. If you are mounting an image from the dedup pool that was captured by an Actifio Sky appliance, you have the option of:
 - o Mounting to a host directly from the Dedup Pool. With this option, the mount operation is almost instant, however, because the data in the dedup pool is deduplicated, access performance is impacted because data must be rehydrated before it can be accessed.

- o Rehydrating the data to the Actifio Snapshot Pool before mounting. With this option, the mount operation is delayed until rehydration is complete. Access performance is fast because the data is already rehydrated and ready for access.
13. Click **Submit**. A job is submitted to mount the image to the selected host. Once completed, the image becomes active and is available in the Active Images view (Manage Active Images) of the Application Manager.

Recovering a Mounted VMware VM to Production Storage

To mount a VMware VM and then migrate the VM data via VMware ESX VMotion:

1. Choose the datastore for the RDM files and VM configuration files. Do not choose the datastore that will be the permanent home of the VM. For example, if you want the VM to be on DS1 after the VMotion operation, then choose DS2 as the datastore for the mount.
2. Use VMotion to migrate the VM to the production array:
 - o Change the datastore. The new datastore cannot be the same as the source datastore.
 - o Change the format of the virtual disk. Leaving it as same format as source will not work.

Note: *If both of the above criteria are not met, you will have a very fast VMotion that only moves RDM files or has no action because the source datastore and destination datastore are the same.*

3. Unmount & Delete the mount:
 - a. In AGM, go to **App Manager, Active Mounts** and right-click the image that you want to unmount and delete.
 - b. Click **Unmount & Delete**.
 - c. Click **Yes** in the confirmation dialog.

Note: *VMware snapshots treat mounted vRDMs as Independent and are not included in snapshots. Because of this, by default, Actifio does not include vRDMs when protecting a mounted VM. Actifio does provide an option where you can mark vRDMs as Dependent. Although rarely used, when this option is enabled, vRDMs will be included in VMware snapshots. Actifio SLA templates will capture vRDMs marked as Dependent and the captured data will be counted in MDL usage.*

5 Replicating VMware Data to a Datastore

A VMware VM can be replicated to a datastore. To replicate data, at least two Actifio Appliances must be joined and have exchanged certificates. Details on joining Actifio Appliances can be found in the AGM online help.

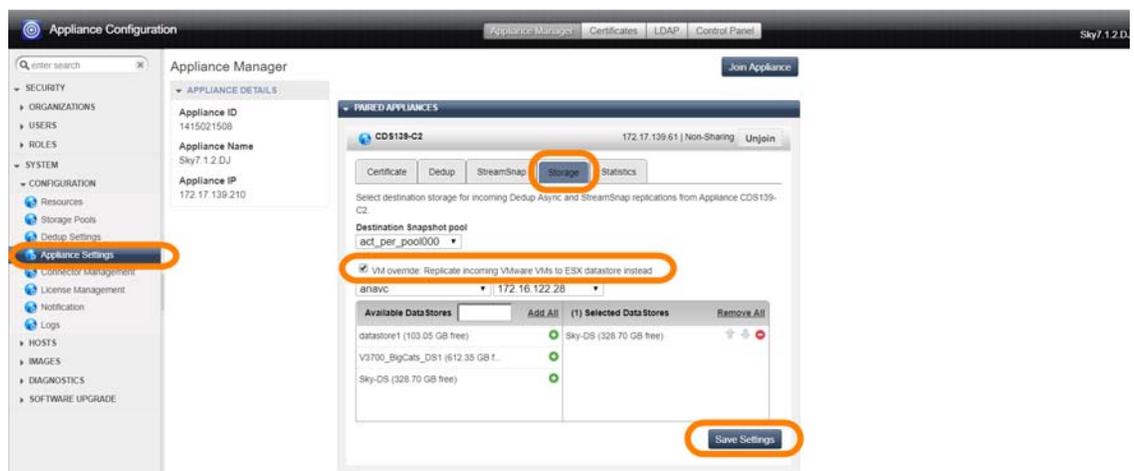
Resource Profiles define where to replicate data. By default, Resource Profiles replicate data to either a Snapshot Pool or a Dedup Backup Pool on a remote site. When coupled with a Production to Mirror Policy, a Resource Profile can replicate VMware data directly to a datastore. To use this option:

- The datastore must be part of an ESX server/vCenter added/discovered by the remote Actifio Appliance to which the local Actifio Appliance is joined. See the AGM online help for details.
- Data must be replicated via a Production to Mirror Policy that uses either Dedup-Async or StreamSnap replication. See the AGM online help for details.

Note: Once defined, the local Actifio Appliance's Resource Profiles that include the remote Actifio Appliance will replicate VMware data to the specified datastore.

To replicate VMware data directly to a datastore:

1. In AGM, go to **Manage > Appliances**. Right-click the appliance and select **Configure Appliance**. The Application Configuration page opens.
2. In the Appliance Configuration page, go to **System > Configuration > Appliance Settings > Storage** tab:



Storage Options

If the local Actifio Appliance is joined with multiple remote Actifio Appliances, select the remote Actifio Appliance needed.

3. Click the **VM override** check box.
4. From the drop-down menus, select a vCenter host/ESX host.
5. Click the green plus sign next to the required datastore name. When selecting datastores:
 - o Select as many datastores as needed. When multiple datastores are selected, VMDKs will be written to the datastores in round robin fashion.
 - o Ensure the datastore(s) free space equals the amount of data that will be replicated plus enough extra space to accommodate future growth
6. Click **Save Settings**. Resource Profiles on this Actifio Appliance that include the remote Actifio Appliance set up with the VM override will replicate VMware data to the selected datastore.

If you exceed the capacity of the selected datastore(s), you can add more. Replicated VMDKs will be written to the new datastore(s). Data will not be balanced across datastores when new datastores are added.

In the case where the data is being replicated to a remote VMware datastore, the local datastore and the remote datastore space usage are monitored during data movement. If a critical threshold is crossed in any of the data movement jobs, all subjobs are canceled and the job fails.

6 Restoring Virtual Machines

You can restore a VM to its original host or to a replacement host at the same IP address, overwriting the existing VM. Restoring always involves some data loss: any data that came in between the last snapshot job and the application failure is lost. The Actifio Appliance offers other options for recovering data.

Applications on VMs that are protected through the Actifio Connector can be protected and restored as individual applications. See the AGM online help for details.

When you restore an image, the SLA options (Run Schedule, Expire Data) of the protected VM are turned off.

Cloning VMware VMs

VMware VMs can also be restored by cloning a VM to a new VM. In most cases, that is the better way to restore the VM. Cloning is detailed in the AGM online help.

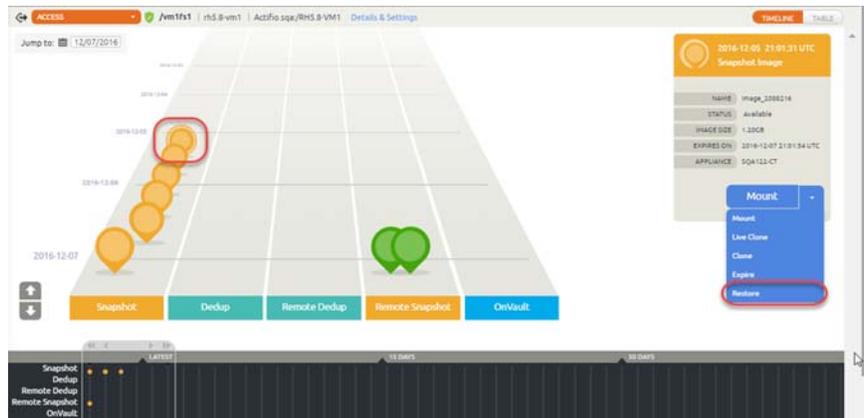
Restoring VMware VMs

Restoring from a dedup image requires space in your snapshot pool for rehydration. The space required is equal to the full Backup Size of your application as shown in the application information. If you need to add a new snapshot pool see the AGM online help for details.

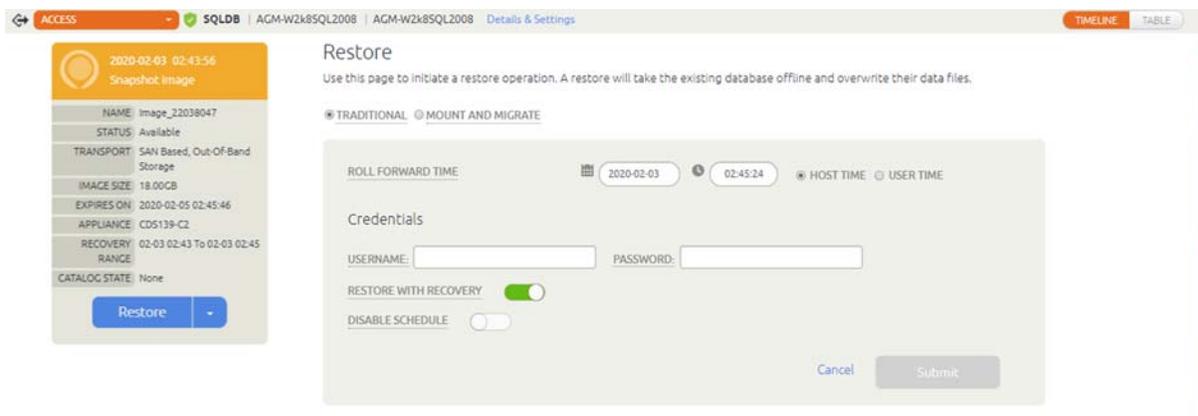
To restore a point-in-time image from a managed VM:

1. Go to AGM and click **App Manager > Applications**. The Applications page opens.
2. Select the managed VM that you want to restore, then choose **Access** from the drop-down list at the bottom right corner of the Applications page. The Access page opens listing captured images in the Timeline ramp view.

The Timeline ramp view is a time-based visualization of 7 days of captured images for the selected application. You can use your mouse scroll wheel or the up and down arrows in the bottom left corner of the page to move the timeline through the captured images and make a selection.



3. Select the image type by clicking the corresponding Snapshot, Dedup, Remote Dedup, or Remote Snapshot (Dedup Async or StreamSnap) image in the Access page.
4. Select **Restore** from the list of operations. The Restore page opens.
5. Check the **Power On Virtual Machine After Restore** check box if you want the restored VM to be powered on after the restore operation is complete.



6. Select a single volume or multiple volumes to restore. By default all the volumes are selected.
7. Click **Submit**. A warning dialog appears. Read it and then enter **DATA LOSS** to confirm. A second warning appears. Enter **OVERWRITE OTHER APPS** to confirm the restore operation.

The restore job starts. You can verify that the restore operation is successful by viewing the job status in System Monitor. When the image is restored, the Actifio appliance creates new VMs populated with data copied from the selected point-in-time image.

Note: The Restore operation cannot be performed from a remote appliance. However, you can use a remote- dedup image for a restore operation on the source appliance itself.

7 Actifio VDP and VMware HA

This chapter describes:

- [Shutting Down a Managed Actifio Sky Appliance](#) on page 36
- [VMotion for Host Migration of an Actifio-protected VM](#) on page 37
- [VMware FT \(Fault Tolerance\) Configurations](#) on page 37
- [Use of Resource Pools with Actifio Sky Appliance Instances](#) on page 38
- [Licensing Considerations](#) on page 38
- [Networking Considerations](#) on page 39
- [Best Practices for Actifio Sky Appliance in an HA Failover Configuration](#) on page 39
- [System Recovery Steps After an HA failover](#) on page 39
- [Migrating Actifio Sky Appliances](#) on page 40

Actifio Sky Appliance is VMware HA and DRS/DPM friendly, and is supported in environments configured with these VMware services. There are some special handling considerations for HA failover with Sky Appliance and potential functional/performance degradation while the dedup store goes through its recovery and integrity checks, post Sky Appliance VM restart.

Once an Actifio Sky Appliance instance has failed over and is running on a new ESX host in the cluster due to an ESX HA failover, snapshot operations should resume within several minutes.

Recovery and integrity checks on the dedup store can take a significant amount of time to perform. The dedup engine keeps a large index in memory which is lost in the event the Sky Appliance VM experiences an HA Failover where the Sky Appliance VM is shutdown/powered off without flushing the cache.

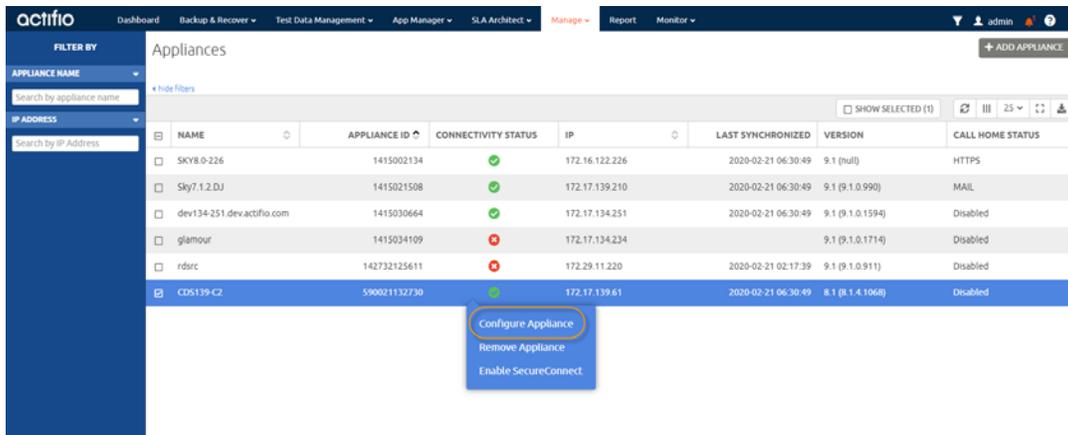
So while VMware HA failover can be used to restart a Sky Appliance VM instance in the event of a ESX host failure, it is best to configure the ESX environment and Actifio Sky Appliance instance to minimize the need for HA failover that requires the Sky Appliance VM to shut down without the proper quiesce and shutdown procedure.

Shutting Down a Managed Actifio Sky Appliance

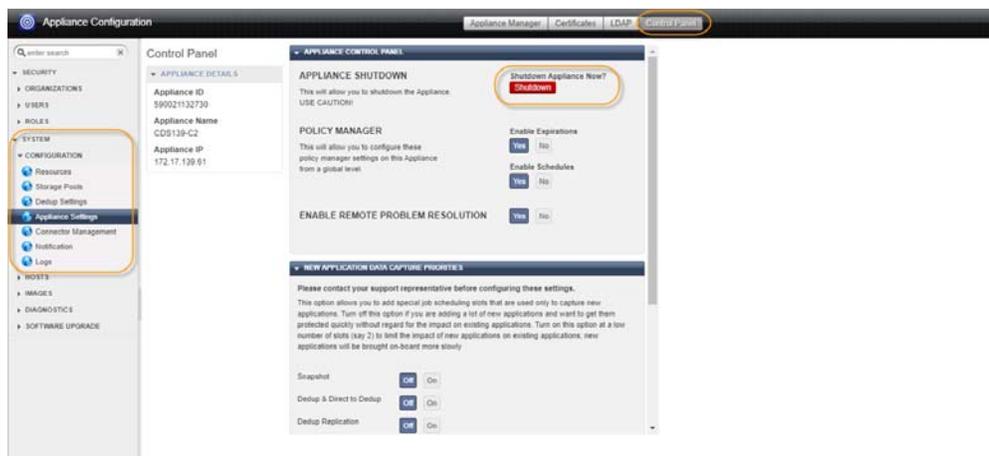
It is of the utmost importance that the Actifio Sky Appliance instance does not get powered down without flushing its memory cache to disk!

It is critical that you always shut down the Actifio Sky Appliance instance from within the Actifio Sky Appliance itself:

1. In AGM, go to **Manage > Appliance**.
2. Right-click the appliance to shut down and select **Configure Appliance** to open the Appliance Set up page.



3. Go to **System > Configuration > Appliance Settings**.
4. Click the **Control Panel** tab. The control panel opens.
5. Click **Shutdown**. Complete shutdown can take 10 to 20 minutes.



The Actifio Sky Appliance does **not** necessarily shut down the dedup engine cleanly from the vSphere interface (Shutdown Guest/Restart Guest) via VMware tools. While Actifio Sky Appliance VMs are hooked into the vSphere VM guest OS shutdown process, the dedup engine sometimes takes longer to quiesce and shutdown than VMware allows, which will result in a kill -9 being executed after a period of time. The procedure above allows time for dedup to shutdown.

6. Shut the Actifio application down inside the Sky Appliance guest, and then when the application has completed its shutdown procedure, you can power the VM off via the vSphere interface.

Using VMware VMotion and Storage VMotion

[VMotion for Host Migration of an Actifio-protected VM](#)

[Storage VMotion for Storage Migration of an Actifio-protected VM](#)

VMotion for Host Migration of an Actifio-protected VM

Movement of an Actifio-protected VM that has one or more mounted images from one ESX host to another via VMotion is supported when all of the ESX hosts in the cluster can reach all the disks used by the VM. Selecting "Map to all ESX hosts" during the mount will allow a migration to any host in the ESX cluster. VMotion between hosts shows very little performance impact at normal operating loads; the best practice is to perform the migration during relatively low workloads on the ESX servers.

Note: DRS (*Distributed Resource Scheduler*) is subject to the same restriction; it can only migrate a VM to hosts that can reach all the disks used by the VM, including any mounted disks.

Storage VMotion for Storage Migration of an Actifio-protected VM

Movement of storage for an Actifio-protected VM that has one or more mounted images from one datastore to another datastore via Storage VMotion is supported. All hosts must have access to both datastores.

Performance may be degraded during the storage migration resulting in SLA misses; the best practice is to perform the migration during low workloads on the Actifio Appliance and on the ESX servers.

Do not perform a Storage VMotion while the Sky Appliance is powered on.

Sky Appliance disk devices should be located on storage that is accessible to all hosts in the ESX cluster.

VMware FT (Fault Tolerance) Configurations

The VMware Fault Tolerance feature is not currently supported with Actifio Sky Appliance instances.

Use of Resource Pools with Actifio Sky Appliance Instances

Actifio Sky Appliance instances can be installed and have their resources managed via resource pools.

It is important not to memory starve the Actifio Sky Appliance VM for dedup processing, which can be time sensitive, and through which any deduplicated data must pass for remote data movement. The memory limits represent the minimum resources required to run the Actifio Sky Appliance instance at expected levels.

While it is important not to vCPU starve the Actifio Sky Appliance instance as well, memory reservation is more important than vCPU reservation for a Actifio Sky Appliance instance.

For production deployments, use CPU and Memory reservations where possible, or ensure resources are not shared on the ESX host to ensure reliable performance is achieved.

For the latest specifications on Actifio Sky Appliance CPU and memory requirements, see ***Installing and Upgrading Actifio Global Manager on a VMware Server.***

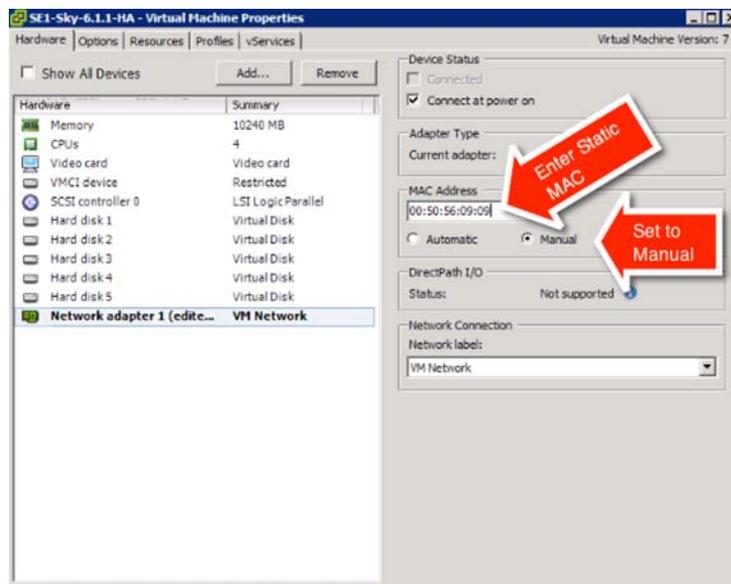
Licensing Considerations

Actifio Sky Appliance licensing uses some portion of the MAC address of eth0 (or the first available NIC if eth0 is replaced) to generate the unique ID - which is then used for creating licenses. Make sure the MAC addresses remain the same for the Sky Appliance VM regardless of where it is running in the HA cluster.

Most HA and VMotion operations (including VM and Storage movement) should not cause the Sky Appliance VM to change its MAC address. There are operations and conditions that can cause the MAC address to change, including Cloning of the VM and MAC address conflicts occurring because ESX does not check MAC addresses on powered down VMs for conflicts with running or suspended VMs, when MAC addresses are assigned.

There are several options for managing MAC address assignment at both the vCenter and ESX level. These are discussed in detail in the VMware Networking documentation.

Set a static MAC address for Sky Appliance VMs, to ensure that you retain the MAC address regardless of conditions within the cluster. Enable this for all Sky Appliance VMs. Without this, if a MAC address change occurs, the Sky Appliance VM will run in an evaluation mode (without a license) for 15 days and will require re-applying that license. Make a note of all Sky Appliance VM MAC addresses for reference. If a MAC address conflict occurs, resolve it by changing the MAC address assigned to the conflicting VM, not the Sky Appliance VM.



Networking Considerations

Ensure that the network implementation for the HA cluster allows for seamless failover of Actifio Sky Appliance instances. If you have a dedicated backup network to all hosts being protected with a Sky Appliance for data movement, make sure all eligible hosts in the HA cluster have access to this network. If you have multiple networks through which a Sky Appliance is protecting VMs or physical hosts, again, make sure that infrastructure is available and named consistently across all ESX hosts in the HA cluster. Ensure all Sky Appliance required network infrastructure is accessible to Actifio Sky Appliance instances during failover, for instance, DNS and NTP.

Best Practices for Actifio Sky Appliance in an HA Failover Configuration

- When adding an Actifio Sky Appliance to a Resource Pool, do not over-commit the pool resources. Consider configuring a dedicated resource pool for the Actifio Sky Appliance instance.
- Ensure that the VMware HA cluster nodes have sufficient resources to handle all recovered Actifio Sky Appliance instances. Actifio Sky Appliance instances consume a fair amount of CPU and Memory depending on License size. It is important that VMware HA slot calculations for the HA cluster Sky Appliance is running take these values into consideration. For more on HA slot calculations, see this excellent article by Duncan Epping on the Yellow-Bricks Blog. <http://www.yellow-bricks.com/vmware-high-availability-deepdiv/>
- When installing multiple Actifio Sky Appliance instances into the same VMware HA cluster:
 - Balance multiple Actifio Sky Appliance instances between the hosts in an HA cluster rather than installing them all on the same host. This will minimize downtime and SLA impact from a single ESX host failure.
 - Use DRS affinity rules with Actifio Sky Appliance instances to help ensure they are always on different hosts (“VM/VM anti-affinity”).

System Recovery Steps After an HA failover

There are two primary failover use cases with Actifio Sky Appliance:

Planned Failover: This includes DRS, DPM, and vMotion migrations of the Sky Appliance VM to other clusters due to operational requirements, maintenance windows, and so on.

- These operations should be expected to succeed and running jobs will continue and complete during the Sky Appliance VM migration. The Sky Appliance should continue to operate normally during this operation though performance may be impacted.

ESX Host failure: This assumes that the host Sky Appliance VM’s ESX has failed and the Sky Appliance instance was not shut down cleanly. VMware HA can restart the Sky Appliance instance on another host in the HA cluster.

- When the Sky Appliance VM restarts, backup jobs that were in-flight during the failure will be failed and discarded. Restore points for these failed jobs will not be available.
- New snapshot backups start based on the normal SLA schedule. These accumulate until the dedup engine is available to ingest the snapshot images. If more than one snapshot is taken for the same application during this time only the latest will be ingested into dedup. If the snapshot expires before the dedup engine is available to process it, those restore points are lost.
- Dedup can take from two to several hours to recover on a large, very busy Actifio Sky Appliance instance. As stated previously, when a Sky Appliance VM goes down without following the proper shutdown procedure, the in-memory cache that the dedup engine uses is lost and a recovery and integrity check is initiated before restarting.
- When the dedup engine comes back online, snapshots accumulated between the Sky Appliance instance starting up and dedup coming online will begin their dedup ingest process. Subsequent remote dedup jobs will process if configured.

Migrating Actifio Sky Appliances

Migrate Actifio Sky Appliance instances as infrequently as possible. Only move Actifio Sky Appliance instances between cluster hosts when necessary for maintenance operations or for long term migrations. Configure the instance to ensure DRS and DPM are not moving Sky Appliance around the cluster on a frequent basis.

- DRS/DPM initiated movement of Actifio Sky Appliance VMs will succeed assuming resource availability. Allowing for these automated Actifio Sky Appliance instance migrations is supported and should perform well on clusters migrated during periods of minimal load. It is not a recommended configuration for heavily loaded Actifio Sky Appliance instances. Performance impact on the Actifio application will vary significantly during these migrations based on the VMotion speed (1GB, 10GB or multi-NIC) and cluster resource management strategies in place.
- The recommended configuration for heavily utilized Actifio Sky Appliance instances requires setting the Sky Appliance VM Automation level to **Manual**. In the cluster settings, under vSphere DRS -> Virtual Machine Options, change the Virtual Machine Automation Level to **Manual** from the default of **Fully Automated**. When a migration event is generated for the Actifio Sky Appliance instance, placement and migration recommendations are displayed, but do not run until you manually apply the recommendation. This will allow the Sky Appliance VM to be VMotioned and restarted by VMware HA services, but will not allow the instance to be automatically moved by DRS or DPM when the ESX Host is under performance load or relatively idle. This should result in DRS choosing to move other VMs rather than the Sky Appliance to relieve over subscription of resources. It is important to maintain a high level of performance in order for Actifio to meet SLA targets.

