A VMware vCenter Administrator's Guide to Actifio VDP

Actifio VDP 10.0

Copyright, Trademarks, and other Legal Matter

Contents

Preface vii

Actifio Appliances vii

The ActifioNOW Customer Portal vii

Actifio Support Centers vii

..... vii

Chapter 1 - Introduction 1

Actifio Data Virtualization 1

Capture Mechanisms 2

Capture Methods 3

Setting Data Transport Mode to a Host in VMware 5

Capturing Virtual Server Data 7

Replicating Captured VMware Data 9

WH Monitoring 9

Accessing Data 9

Workflows to Automate Access to Data 10

Chapter 2 - Supporting VMware with Actifio VDP 13

Actifio Sky Appliance Networking Requirements 13

Ensuring iSCSI Connectivity from ESX to Storage 14

Ensuring iSCSI Connectivity with an ESX Server 14

Adding the iSCSI Actifio Definition to the ESX server 15

Configuring AGM to See the ESX Host 15

Ensuring NFS Connectivity from ESX to Storage 16

Setting NFS Data Transport Mode to a Host in VMware 17

Specifying the NIC for NFS Mounts 18

Renaming a vCenter 18

Chapter 3 - Discovering and Protecting VMware VMs 19

Discovering VMs 19

Deleting VMs 21

Discovering Applications on a VM 22

Chapter 4 - Mounting a VMware VM Image 23

Mounting a VMware VM (Standard Mount) 23

Recovering a Mounted VMware VM to Production Storage 26

Chapter 5 - Replicating VMware Data to a Datastore 27

Chapter 6 - Restoring Virtual Machines 29

Chapter 7 - Actifio VDP and VMware HA 31

Shutting Down a Managed Actifio Sky Appliance 32

Using VMware VMotion and Storage VMotion 33

VMotion for Host Migration of an Actifio-protected VM 33

Storage VMotion for Storage Migration of an Actifio-protected VM 33

VMware FT (Fault Tolerance) Configurations 33

Use of Resource Pools with Actifio Sky Appliance Instances 34

Licensing Considerations 34

Networking Considerations 35

Best Practices for Actifio Sky Appliance in an HA Failover Configuration 35

System Recovery Steps After an HA failover 35

Migrating Actifio Sky Appliances 36

Chapter 8 - VMware Permissions 37

Creating the VDPReadOnly vCenter Role 39

Creating the VDPOperations vCenter Role 40

The vCenter Permissions List, vCenter 6.0 41

The vCenter Permissions List, vCenter 6.5 42

The vCenter Permissions List, vCenter 6.7 43

The vCenter Permissions List, vCenter 7.0 44

Assigning Minimum Permissions 45

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: 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 Introduction

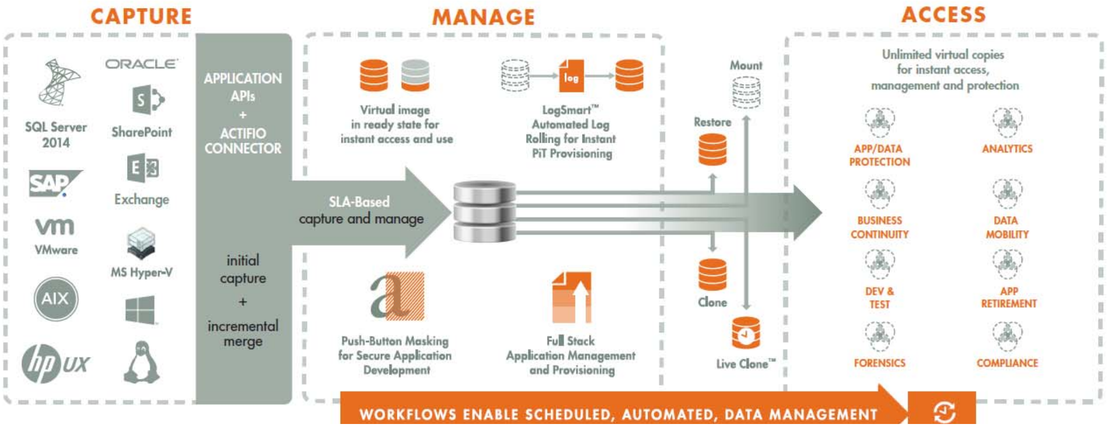
This chapter provides a high-level overview of basic Actifio concepts and procedures used to capture, manage, and access virtual machines (VMs). Specifically, this chapter describes:

- Actifio Data Virtualization on page 1
- Capture Mechanisms on page 2
- Capture Methods on page 3
- Setting Data Transport Mode to a Host in VMware on page 5
- Capturing Virtual Server Data on page 7
- Accessing Data on page 9
- Workflows to Automate Access to Data on page 10

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
ACCESS
SQL Server 2014
ORACLE
SharePoint
SAP
Exchange
vm VMware
MS Hyper-V
AIX
hp UX
APPLICATION APIs + ACTIFIO CONNECTOR
initial capture + incremental merge
SLA-Based capture and manage
Virtual image in ready state for instant access and use
log
LogSmart™ Automated Log Rolling for Instant PiT Provisioning
Push-Button Masking for Secure Application Development
Full Stack Application Management and Provisioning
Mount
Restore
Clone
Live Clone™
Unlimited virtual copies for instant access, management and protection
APP/DATA PROTECTION
ANALYTICS
BUSINESS CONTINUITY
DATA MOBILITY
DEV & TEST
APP RETIREMENT
FORENSICS
COMPLIANCE
WORKFLOWS ENABLE SCHEDULED, AUTOMATED, DATA MANAGEMENT

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:
    - Captures database(s) and logs with one Policy Template
    - Truncates database transaction logs as needed
    - 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:
    - Captures databases that use pRDMs and vRDMs
    - Avoids virtual server "stun" issues.

Capture Methods

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.

Actifio supports three capture methods:

Out-of-Band on page 3

In-Band (CDS Appliance only) on page 4

LAN-Free (CDS Appliance only) on page 4

Out-of-Band

Out-of-Band is the most common method used when capturing data. The Actifio Appliance operates outside of the application's data path and leverages the IP network. Production data is controlled by a non-Actifio storage controller on your existing storage arrays. 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.

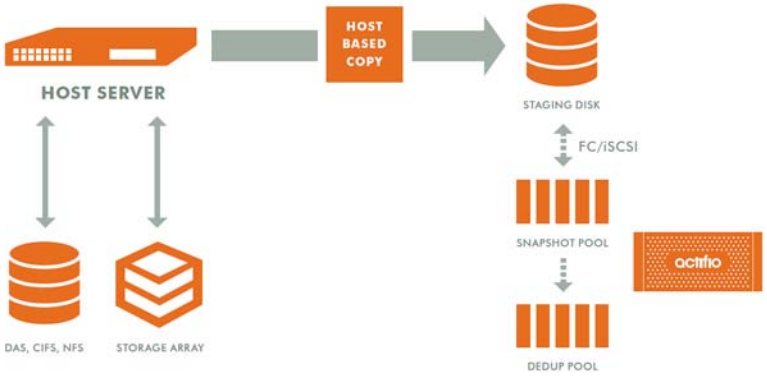
The Out-of-Band method will meet the needs of most users who want to capture:

Hypervisors: VMware, Hyper-V

Applications: Oracle, SQL, Exchange, SharePoint, SAP on Oracle

File Systems: Windows, Unix, Linux file systems.

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.

In-Band (CDS Appliance only)

With the In-Band method, production data storage is controlled by an CDS Appliance. Snapshots and changed-block tracking are native to the CDS Appliance. The CDS Appliance is in the data path between the SAN and the application host.

The In-Band method will meet the needs of those customers whose production data is on Fiber Channel LUN(s) on an Actifio supported storage array AND one or more of the following conditions apply:

- The application is not a supported Out-of-Band application. For example, Db2 or a custom application.
- The local RPO requirements are shorter than what is practical for Out-of-Band. For example, when snapshots are required every 15 minutes.
- The remote RPO requirements are shorter than what Actifio Dedup Async Replication (DAR) allows. For example, requirement states instant sync/async.
- There is a large amount of data. For example, a 10TB database.
- The applications and the files on them need to be managed. It is more efficient to manage blocks of data rather than applications and their files. For example, a Linux file system with 21million files.

LAN-Free (CDS Appliance only)

To capture VMware VMs, an CDS Appliance can employ LAN-Free data capture. With this method, data is moved over the SAN and the LAN is used for command and control.

To use the LAN-Free data capture method the SAN administrator simply has to:

1. Use Fibre Channel SAN zoning to provide the CDS Appliance access to the storage controller that manages the ESXi datastores.
2. Ensure that the storage controller is supported by the CDS Appliance.
3. Define the CDS Appliance as a host
4. LUN Mask all datastore LUNs to the CDS Appliance host.

The CDS Appliance will detect whether the ESXi datastore LUNs are accessible via Fibre Channel. If they are available, data will be moved across the Fibre Channel SAN automatically.

In all other aspects LAN-Free is the same as Out-of-Band.

Note: *If the SAN administrator fails to map the required datastores or maps a required datastore away from the CDS Appliance, then the CDS Appliance will switch to LAN based data capture.*

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

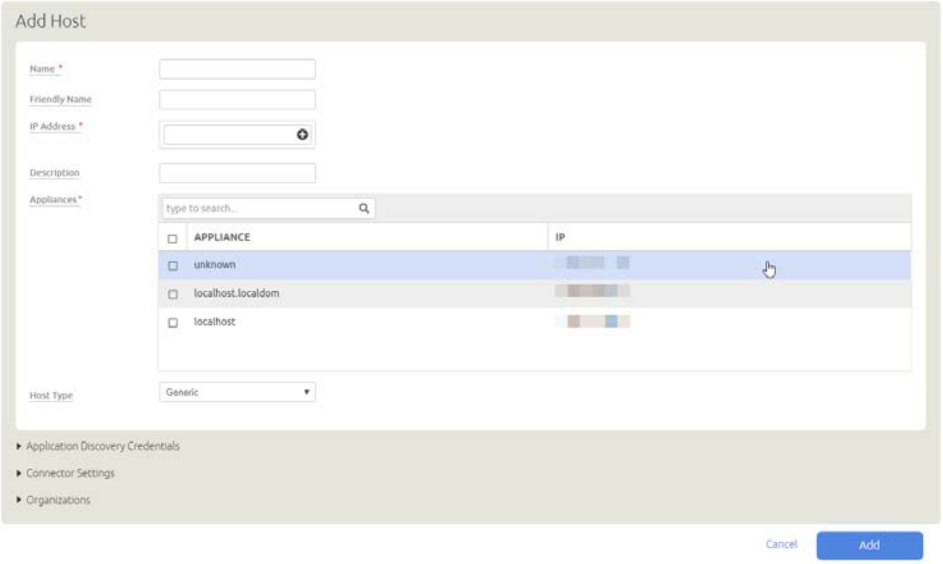
To set NFS datastore support on VM:

- 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.*

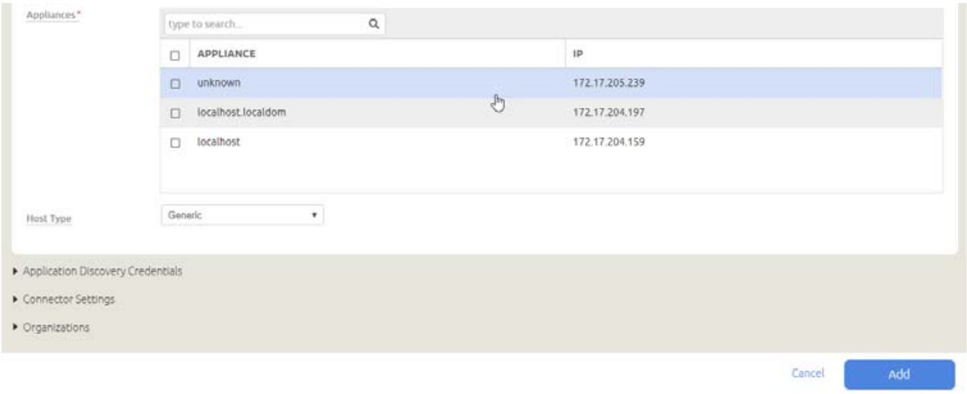
1. In AGM, click the **Manage** tab and select **Hosts** from the drop-down menu. The Hosts page opens.
2. Select **Add Host**. The upper portion is for network and other identification information. Below that are dynamic sections for host connections and for organizations that the host belongs to.



APPLIANCE	IP
unknown	[redacted]
localhost.localdom	[redacted]
localhost	[redacted]

Host Type: Generic

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.



Appliances*

type to search...

□	APPLIANCE	IP
□	unknown	172.17.205.239
□	localhost.localdom	172.17.204.197
□	localhost	172.17.204.159

Host Type: Generic ▾

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:

   - **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.
   - **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:** As of v9.0, 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.

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:

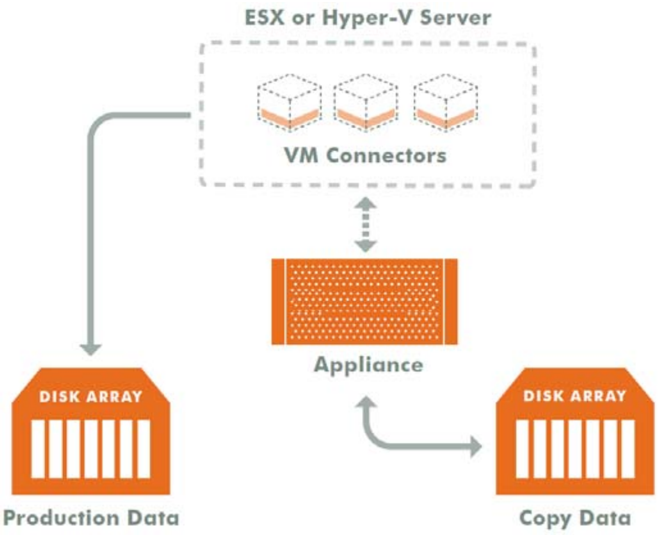
1. Choose the Server for VM Discovery
2. Select Virtual Machines
3. Manage VMs
4. Approve the Onboarding Summary

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

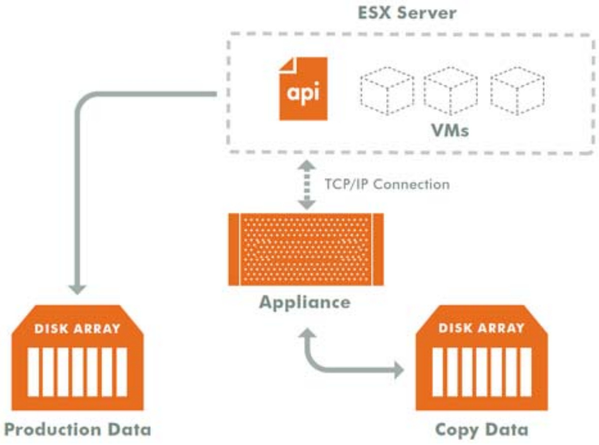
Installing the Actifio Connector on a VM allows you to capture applications on that VM. Multiple applications can be captured with a single policy template, or multiple policies can be used to capture individual applications.



Connectors on Multiple Virtual Machines

Capturing VMs Individually or in Groups

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



Capturing Entire VMs

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 27 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.

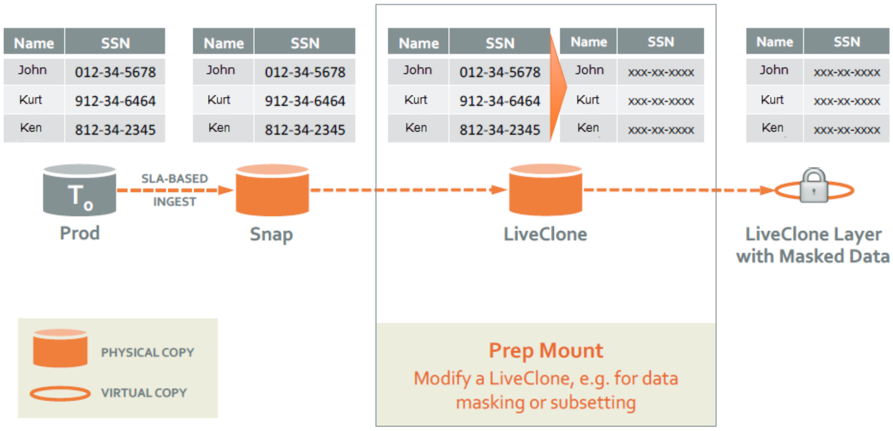
Combining Actifio's automated data capture and access control with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait weeks for DBAs to update test and development environments, users can provision their own environments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



Name	SSN
John	012-34-5678
Kurt	912-34-6464
Ken	812-34-2345

Name	SSN
John	012-34-5678
Kurt	912-34-6464
Ken	812-34-2345

Name	SSN
John	012-34-5678
Kurt	912-34-6464
Ken	812-34-2345

Name	SSN
John	xxx-xx-xxxx
Kurt	xxx-xx-xxxx
Ken	xxx-xx-xxxx

Name	SSN
John	xxx-xx-xxxx
Kurt	xxx-xx-xxxx
Ken	xxx-xx-xxxx

T_0
Prod
SLA-BASED INGEST
Snap
LiveClone
LiveClone Layer with Masked Data
PHYSICAL COPY
VIRTUAL COPY
Prep Mount
Modify a LiveClone, e.g. for data masking or subsetting

Workflow With Masked Social Security Data

2 Supporting VMware with Actifio VDP

This includes:

- Actifio Sky Appliance Networking Requirements on page 13
- Ensuring iSCSI Connectivity from ESX to Storage on page 14
- Ensuring iSCSI Connectivity with an ESX Server on page 14
- Ensuring NFS Connectivity from ESX to Storage on page 16
- Setting NFS Data Transport Mode to a Host in VMware on page 17

Actifio Sky Appliance Networking Requirements

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

- **Static IPs**: You must provide static IPs for all NICs on Sky Appliances.
- **VMXNET3**: Sky Appliance models 30, 50, 120, and 200 must use the VMXNET3 Ethernet adapter. These adapters enable 10GB performance.
- **Adding NICs**: By default, the Sky Appliance comes with a single NIC. To add additional NICs, see Appendix A, Adding and Configuring Additional Network Interfaces.

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.

  The Snapshot pool and the Dedup pool each need their own SCSI controller set to VMware Paravirtual.

***Note:** For best iSCSI network traffic results, see NIC Usage for Each Actifio Appliance Type on page 4.*

Each Sky Appliance and CDX Appliance can support up to 100 iSCSI sessions. A CDS Appliance can support 275 sessions. You can support an additional 100 sessions by adding a NIC card to a Sky Appliance.

Ensuring iSCSI Connectivity from ESX to Storage

To test the iSCSI connection from an ESXi server to a V3700 or V7000 storage array or to an Actifio CDS 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 SAN transport of data to an external storage pool

A newly created vCenter will default to Transport Type NFS. This is incompatible with ESP, and should be changed to SAN. This setting is visible in AGM and from the Command Line, but is not displayed in the Actifio Desktop.
You can also do this from the CLI:

```
[root@sky812-900-RC2 ~]# udsinfo lshost 207823
udstask chhost -transport san <id>'\
```

The -transport parameter is detailed in the ***Actifio CLI Reference***.

Ensuring iSCSI Connectivity with an ESX Server

This has two parts:

1. Adding the iSCSI Actifio Definition to the ESX server on page 15
2. Configuring AGM to See the ESX Host on page 15

Before You Begin

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

- Check that the NICs are as described in NIC Usage for Each Actifio Appliance Type on page 4.
- Check that the network ports are as described in Firewall Rules on page 13.
- 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.

For CDX Appliance cluster (which is high availability), these parameters are different to ensure the iSCSI connection survives a failover event.

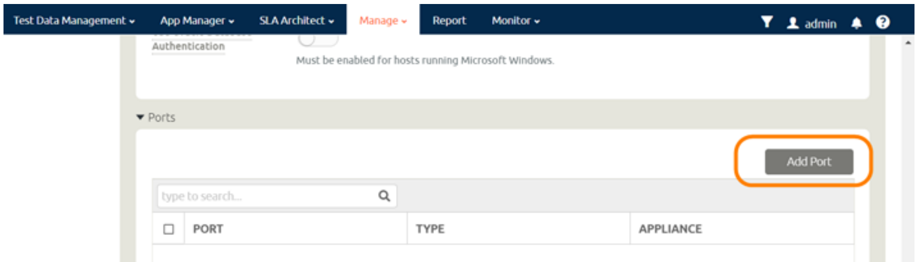
Adding the iSCSI Actifio Definition to the ESX server

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 ESX Host on page 15.

Configuring AGM to See the ESX Host

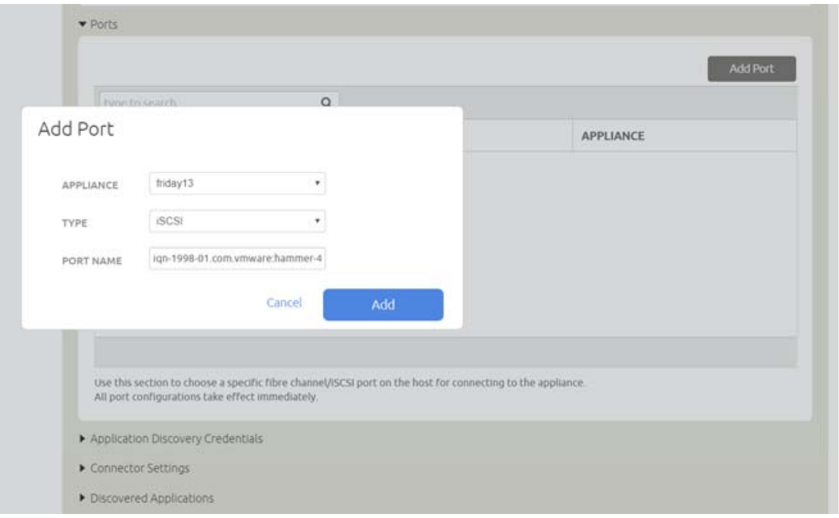
1. Open AGM to **Manage** > **Hosts**.
2. Right-click the ESX server and select **Edit**.
3. Scroll down the right side to the Ports section and click **Add Port**.



Must be enabled for hosts running Microsoft Windows.

Configuring AGM to Recognize an ESX Server

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



APPLIANCE friday13

TYPE iSCSI

PORT NAME iqn-1998-01.com.vmware:hammer-4

Use this section to choose a specific fibre channel/iSCSI port on the host for connecting to the appliance.
All port configurations take effect immediately.

Adding the Port

Ensuring NFS Connectivity from ESX to Storage

Minimum ESX versions

ESXi hosts must be running these minimum levels to support NFS client.

- ESXi Version 5.5 Patch 5 (Build 2718055) OR
- ESXi Version 6.0 U1a (Build 3073146)

Increasing the NFS datastore limit in ESX

The vSphere ESXi/ESX default configuration allows for only eight NFS mounts per ESXi/ESX host. There are three advanced configuration options which control the maximum number of NFS mounts. These settings enable the maximum number of NFS mounts for vSphere ESXi/ESX, listed in Table 1: ESX Advanced Configuration Options, Limits per ESX Version on page 16.

To edit advanced configuration options, select the ESXi/ESX host in the Inventory Panel, then navigate to Configuration > Software > Advanced Settings to launch the Settings window.

Set the following values:

1. The number of NFS datastores which can be mounted by the vSphere ESXi/ESX host concurrently is limited. The default value is 8.
   Under NFS, Select **NFS.MaxVolumes**: Limits the number of NFS datastores which can be mounted by the vSphere ESXi/ESX host concurrently.
2. When increasing the number of NFS datastores, increase the *maximum* amount of heap memory as well.
   Under Net, Select **Net.TcpipHeapMax**: The maximum amount of heap memory, measured in megabytes, which can be allocated for managing VMkernel TCP/IP network connectivity.
3. When increasing the number of NFS datastores, increase the *default* amount of heap memory.
   Under Net, Select **Net.TcpipHeapSize**: The amount of heap memory, measured in megabytes, which is allocated for managing VMkernel TCP/IP network connectivity.

Table 1: ESX Advanced Configuration Options, Limits per ESX Version

Version	NFS.MaxVolumes	Net.TcpipHeapMax	Net.TcpipHeapSize
ESXi/ESX 3.x	32	120	30
ESXi/ESX 4.x	64	128	32
ESXi 5.0/5.1	256	128	32
ESXi 5.5	256	512	32
ESXi 6.0	256	1536	32

Note: *Changing Net.TcpipHeapSize and/or Net.TcpipHeapMax requires a host reboot.*

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

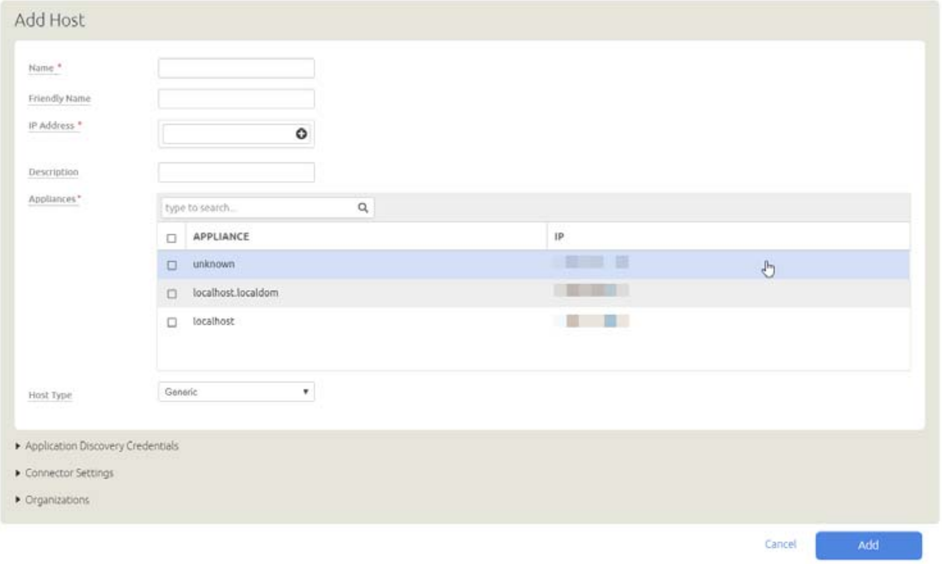
To set NFS datastore support on VM:

- 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.



Add Host

Name *

Friendly Name

IP Address *

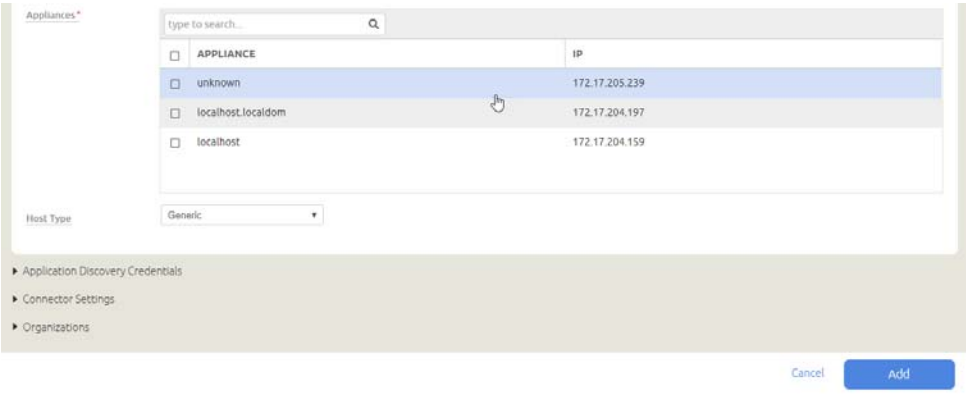
Description

Appliances *

□	APPLIANCE	IP
□	unknown	[redacted]
□	localhost.localdom	[redacted]
□	localhost	[redacted]

Host Type: Generic

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.



Appliances*

type to search...

☐	APPLIANCE	IP
☐	unknown	172.17.205.239
☐	localhost.localdom	172.17.204.197
☐	localhost	172.17.204.159

Host Type: Generic

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:

   - **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.
   - **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: *As of v9.0, 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.

Specifying the NIC for NFS Mounts

Specify the NIC for an NFS mount at the ESX level:

```
udstask chhost -nfsoption server:serverip=1.1.1.1 <hostid>
```

The -nfsoption parameter is detailed in the ***Actifio CLI Reference***.

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:

Discovering VMs on page 19

Deleting VMs on page 21

Discovering Applications on a VM on page 22

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.

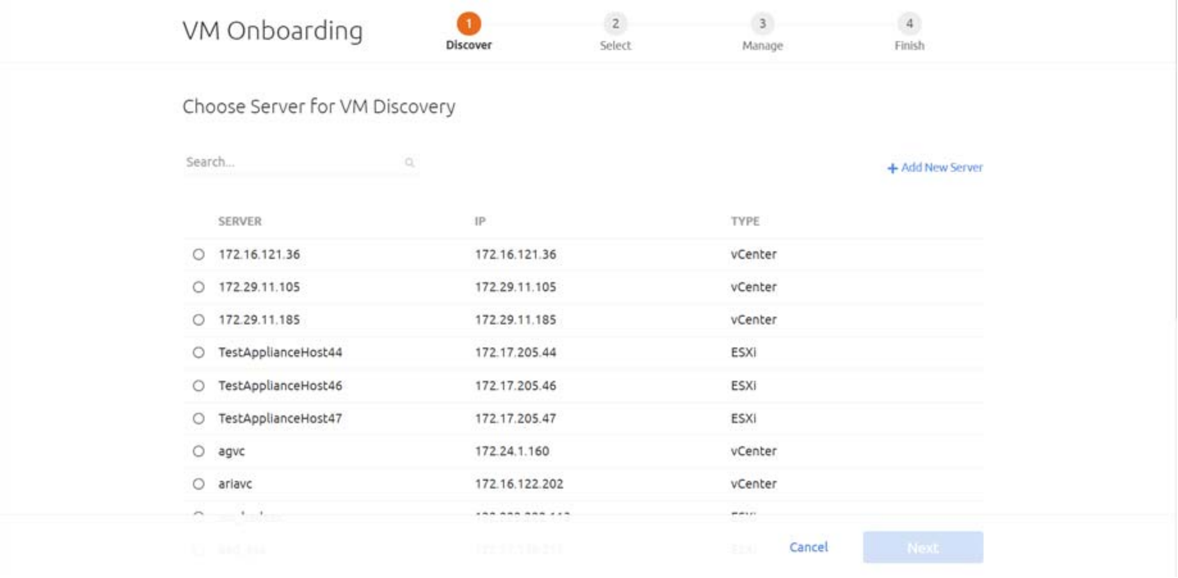
During AGM configuration, you may have already added the ESXi servers and vCenters as hosts to Actifio Appliances. See ***Network Administrator's Guide to Actifio VDP*** for more information. The VM Onboading Wizard also allows you to add a server in case it was not added before.

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.

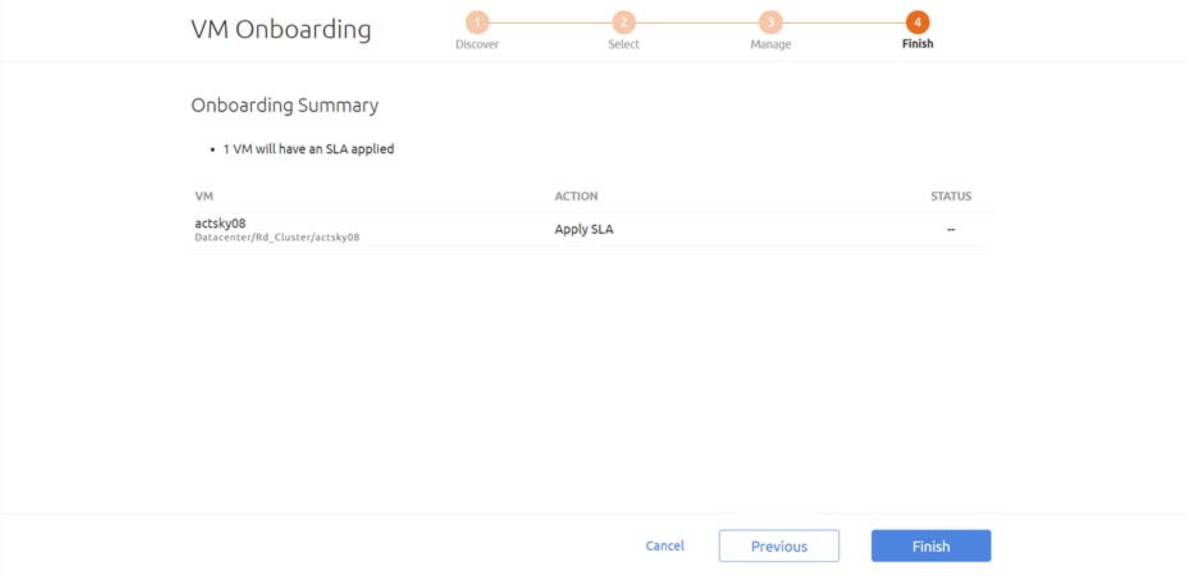


Choose Server for VM Discovery

	SERVER	IP	TYPE
○	172.16.121.36	172.16.121.36	vCenter
○	172.29.11.105	172.29.11.105	vCenter
○	172.29.11.185	172.29.11.185	vCenter
○	TestApplianceHost44	172.17.205.44	ESXi
○	TestApplianceHost46	172.17.205.46	ESXi
○	TestApplianceHost47	172.17.205.47	ESXi
○	agvc	172.24.1.160	vCenter
○	ariavc	172.16.122.202	vCenter

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.



Onboarding Summary

- 1 VM will have an SLA applied

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

The Onboarding Summary for a Simple Job

Note: *The Actifio Appliance relies on synchronicity between an Actifio 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 Actifio Appliance's record of the time snapshots taken or other actions performed by the Actifio Appliance.*

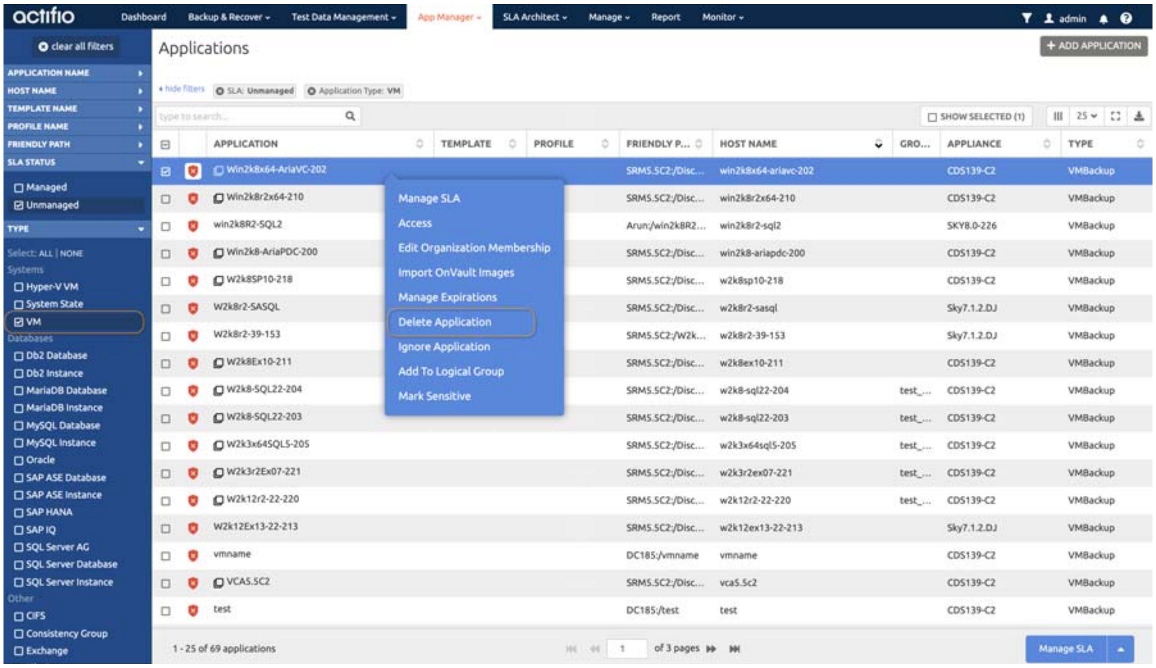
Deleting VMs

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 Actifio 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**.



	APPLICATION	TEMPLATE	PROFILE	FRIENDLY P...	HOST NAME	GRO...	APPLIANCE	TYPE
☑	Win2k8x64-AriaVC-202			SRM5.5C2:/Disc...	win2k8x64-ariavc-202		CDS139-C2	VMBackup
□	Win2k8r2x64-210			SRM5.5C2:/Disc...	win2k8r2x64-210		CDS139-C2	VMBackup
□	win2k8R2-SQL2			Arun:/win2k8R2...	win2k8r2-sql2		SKY8.0-226	VMBackup
□	Win2k8-AriaPDC-200			SRM5.5C2:/Disc...	win2k8-ariapdc-200		CDS139-C2	VMBackup
□	W2k8SP10-218			SRM5.5C2:/Disc...	w2k8sp10-218		CDS139-C2	VMBackup
□	W2k8r2-SASQL			SRM5.5C2:/Disc...	w2k8r2-sasql		Sky7.1.2.DJ	VMBackup
□	W2k8r2-39-153			SRM5.5C2:/W2k...	w2k8r2-39-153		Sky7.1.2.DJ	VMBackup
□	W2k8Ex10-211			SRM5.5C2:/Disc...	w2k8ex10-211		CDS139-C2	VMBackup
□	W2k8-SQL22-204			SRM5.5C2:/Disc...	w2k8-sql22-204	test_...	CDS139-C2	VMBackup
□	W2k8-SQL22-203			SRM5.5C2:/Disc...	w2k8-sql22-203	test_...	CDS139-C2	VMBackup
□	W2k3x64SQL5-205			SRM5.5C2:/Disc...	w2k3x64sql5-205	test_...	CDS139-C2	VMBackup
□	W2k3r2Ex07-221			SRM5.5C2:/Disc...	w2k3r2ex07-221	test_...	CDS139-C2	VMBackup
□	W2k12r2-22-220			SRM5.5C2:/Disc...	w2k12r2-22-220	test_...	CDS139-C2	VMBackup
□	W2k12Ex13-22-213			SRM5.5C2:/Disc...	w2k12ex13-22-213		Sky7.1.2.DJ	VMBackup
□	vmname			DC185:/vmname	vmname		CDS139-C2	VMBackup
□	VCA5.5C2			SRM5.5C2:/Disc...	vca5.5c2		CDS139-C2	VMBackup
□	test			DC185:/test	test		CDS139-C2	VMBackup

1 - 25 of 69 applications

1 of 3 pages

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.

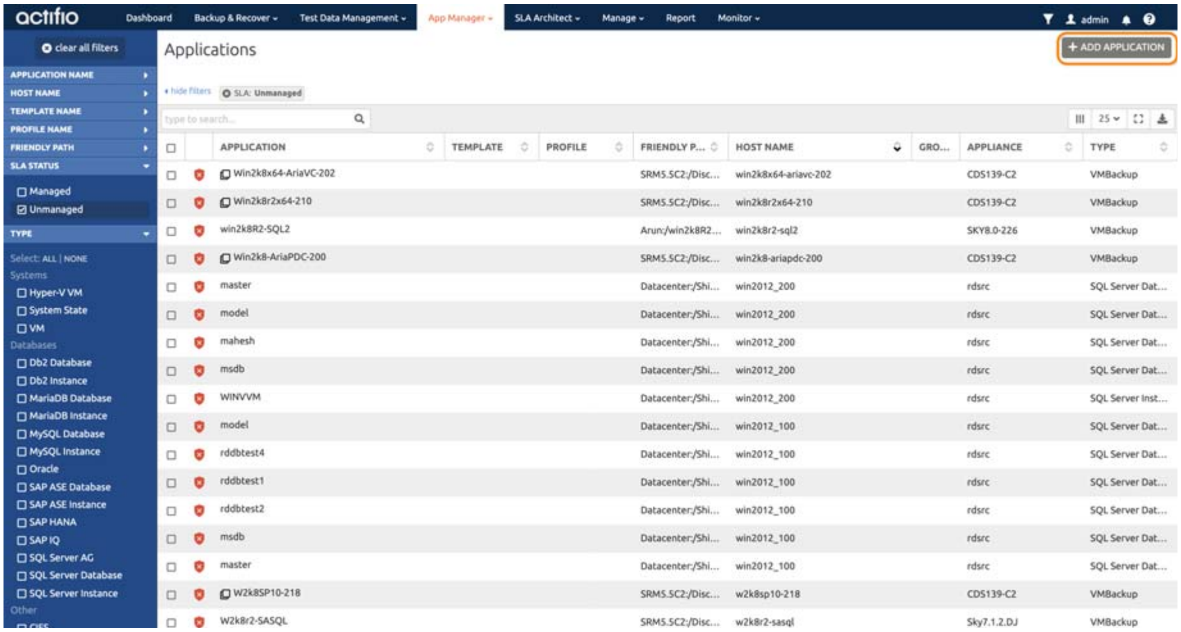
Note: *Deleting a VM or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that VM). If any stale images are left on an Actifio Appliance (usually due to a remote appliance unavailability), in the left bottom menu list of Appliance Configuration, 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 Actifio 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**.



□	APPLICATION	TEMPLATE	PROFILE	FRIENDLY P...	HOST NAME	GRO...	APPLIANCE	TYPE
□	Win2k8x64-AriaVC-202			SRM5.5C2:/Disc...	win2k8x64-ariavc-202		CDS139-C2	VMBackup
□	Win2k8r2x64-210			SRM5.5C2:/Disc...	win2k8r2x64-210		CDS139-C2	VMBackup
□	win2k8R2-SQL2			Arun:/win2k8R2...	win2k8r2-sql2		SKY8.0-226	VMBackup
□	Win2k8-AriaPDC-200			SRM5.5C2:/Disc...	win2k8-ariapdc-200		CDS139-C2	VMBackup
□	master			Datacenter:/Shi...	win2012_200		rdsrc	SQL Server Dat...
□	model			Datacenter:/Shi...	win2012_200		rdsrc	SQL Server Dat...
□	mahesh			Datacenter:/Shi...	win2012_200		rdsrc	SQL Server Dat...
□	msdb			Datacenter:/Shi...	win2012_200		rdsrc	SQL Server Dat...
□	WINVVM			Datacenter:/Shi...	win2012_200		rdsrc	SQL Server Inst...
□	model			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	rddbtest4			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	rddbtest1			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	rddbtest2			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	msdb			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	master			Datacenter:/Shi...	win2012_100		rdsrc	SQL Server Dat...
□	W2k8SP10-218			SRM5.5C2:/Disc...	w2k8sp10-218		CDS139-C2	VMBackup
□	W2k8r2-SASQL			SRM5.5C2:/Disc...	w2k8r2-sasql		Sky7.1.2.DJ	VMBackup

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 VDP****.*

4 Mounting a VMware VM Image

This chapter provides instruction for mounting VMware VMs:

- Mounting a VMware VM (Standard Mount) on page 23
- Recovering a Mounted VMware VM to Production Storage on page 26

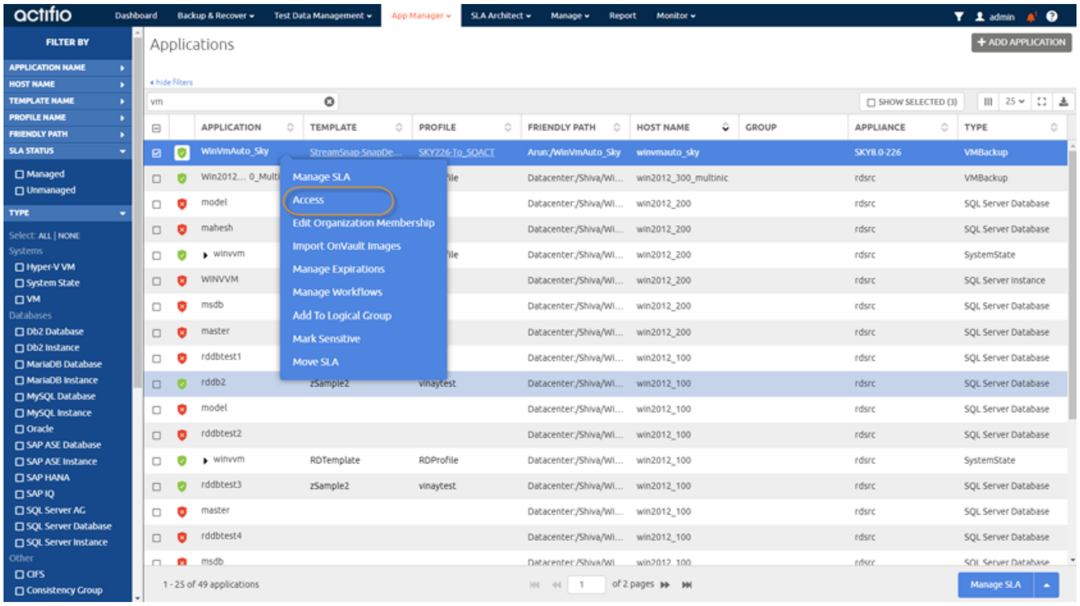
When mounting to an existing VM, no settings are preserved. Captured VMDK volumes are presented as vRDM/pRDM disks to the target VM.

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)

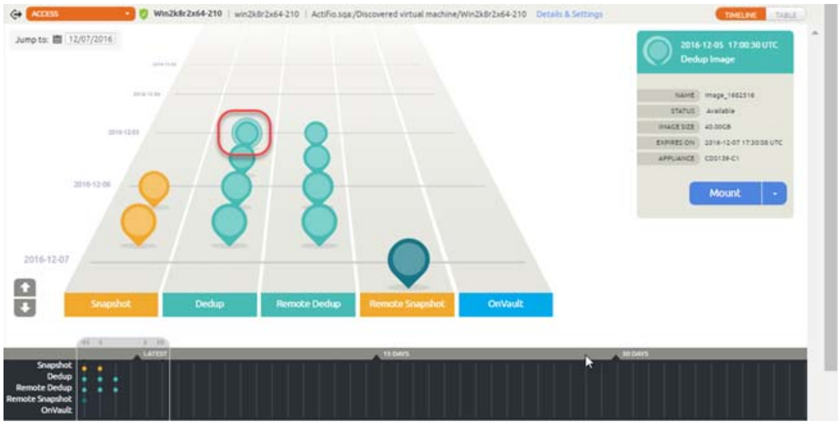
To mount an active image to a VMware VM:

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.



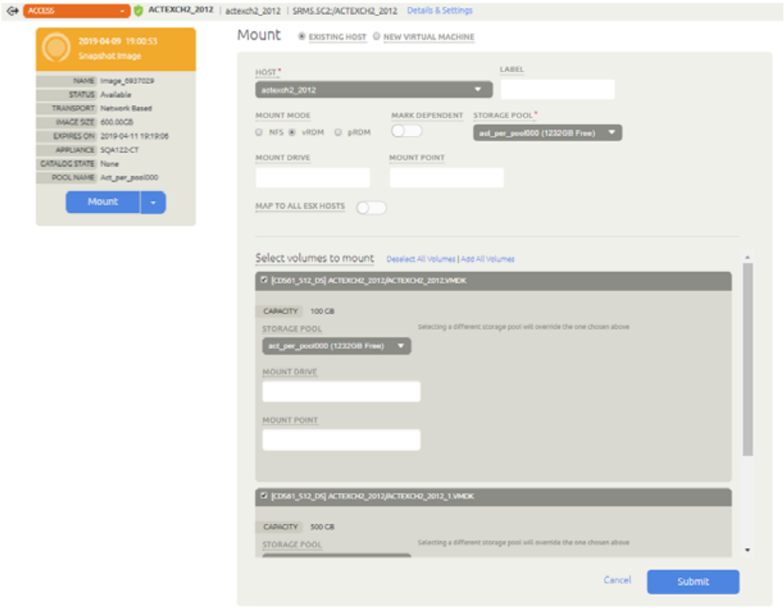
APPLICATION	TEMPLATE	PROFILE	FRIENDLY PATH	HOST NAME	GROUP	APPLIANCE	TYPE
WinVmAuto_Sky	StreamSnap-SnapDe...	SKY226-To_SQACT	Arun:/WinVmAuto_Sky	winvmauto_sky		SKY8.0-226	VMBackup
Win2012... 0_Multi		ile	Datacenter:/Shiva/Wi...	win2012_300_multinic		rdsrc	VMBackup
model			Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SQL Server Database
mahesh			Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SQL Server Database
winvvm		ile	Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SystemState
WINVVM			Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SQL Server Instance
msdb			Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SQL Server Database
master			Datacenter:/Shiva/Wi...	win2012_200		rdsrc	SQL Server Database
rddbtest1			Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
rddb2	zSample2	vinaytest	Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
model			Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
rddbtest2			Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
winvvm	RDTemplate	RDProfile	Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SystemState
rddbtest3	zSample2	vinaytest	Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
master			Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
rddbtest4			Datacenter:/Shiva/Wi...	win2012_100		rdsrc	SQL Server Database
msdb			Datacenter:/Shiva/Wi	win2012_100		rdsrc	SQL Server Database

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.



NAME image_1682516
STATUS Available
IMAGE SIZE 40.00GB
EXPIRES ON 2016-12-07 17:30:08 UTC
APPLIANCE CDS139-C1

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



NAME Image_6937029
STATUS Available
TRANSPORT Network Based
IMAGE SIZE 600.00GB
EXPIRES ON 2019-04-11 19:19:06
APPLIANCE SQA122-CT
CATALOG STATE None
POOL NAME Act_per_pool000

● EXISTING HOST ○ NEW VIRTUAL MACHINE

HOST * actexch2_2012
LABEL
MOUNT MODE ○ NFS ● vRDM ○ pRDM
MARK DEPENDENT
STORAGE POOL * act_per_pool000 (1232GB Free)
MOUNT DRIVE
MOUNT POINT
MAP TO ALL ESX HOSTS

☑ [CDS61_S12_DS] ACTEXCH2_2012/ACTEXCH2_2012.VMDK
CAPACITY 100 GB
STORAGE POOL act_per_pool000 (1232GB Free)
Selecting a different storage pool will override the one chosen above
MOUNT DRIVE
MOUNT POINT

☑ [CDS61_S12_DS] ACTEXCH2_2012/ACTEXCH2_2012_1.VMDK
CAPACITY 500 GB
STORAGE POOL
Selecting a different storage pool will override the one chosen above

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:

   - **VM Name**: Enter a name for the new VM that you want to mount,
   - **VCENTER**: Select a vCenter from the drop-down list for the new VM you want to mount.
   - **ESX HOST**: Select an ESX Host from the drop-down list for the new VM you want to mount.
   - **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:
   - **NFS** if you are in an NFS network environment.
   - **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.
   - **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:
   - **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.
   - **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:
    - 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.

- 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:
    - Change the datastore. The new datastore cannot be the same as the source datastore.
    - 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.

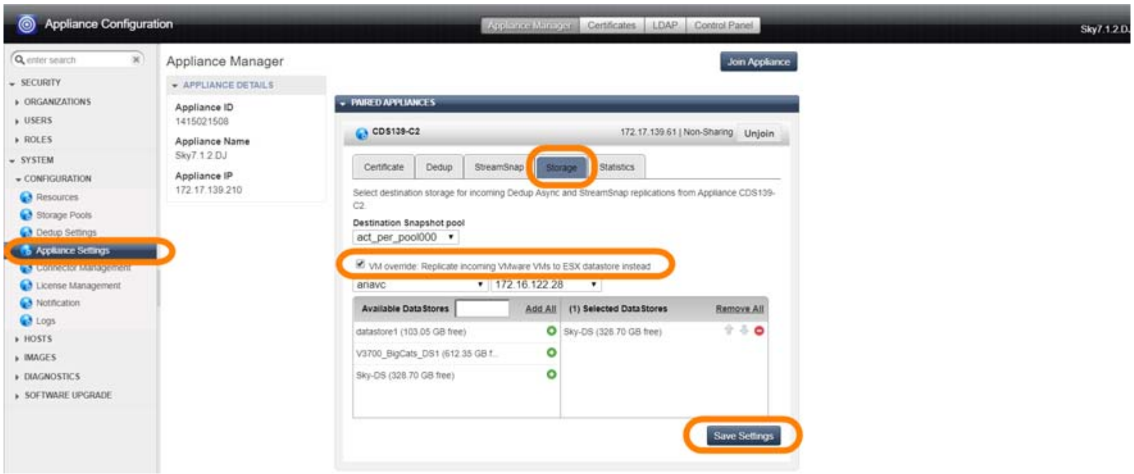
Resource Profiles define where to replicate data. By default, Resource Profiles replicate data to either a Snapshot Pool or a Dedup Backup Pool on a remote site. When coupled with a Production to Mirror Policy, a Resource Profile can replicate VMware data directly to a datastore. To use this option:

- 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:



Appliance ID
1415021508

Appliance Name
Sky7.1.2.DJ

Appliance IP
172.17.139.210

CDS139-C2 172.17.139.61 | Non-Sharing

Select destination storage for incoming Dedup Async and StreamSnap replications from Appliance CDS139-C2.

Destination Snapshot pool
act_per_pool000

☑ VM override: Replicate incoming VMware VMs to ESX datastore instead

anavc 172.16.122.28

Available DataStores	(1) Selected DataStores
datastore1 (103.05 GB free)	Sky-DS (328.70 GB free)
V3700_BigCats_DS1 (612.35 GB f...	
Sky-DS (328.70 GB free)	

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:
    - Select as many datastores as needed. When multiple datastores are selected, VMDKs will be written to the datastores in round robin fashion.
    - 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.

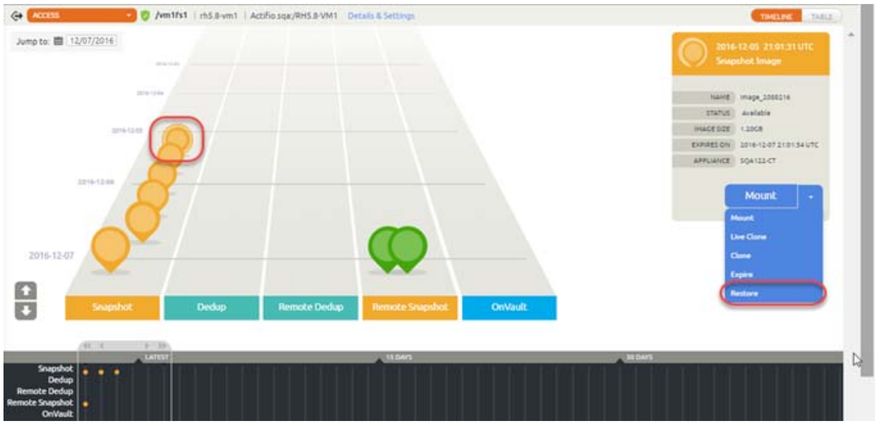
Restoring VMware VMs

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.



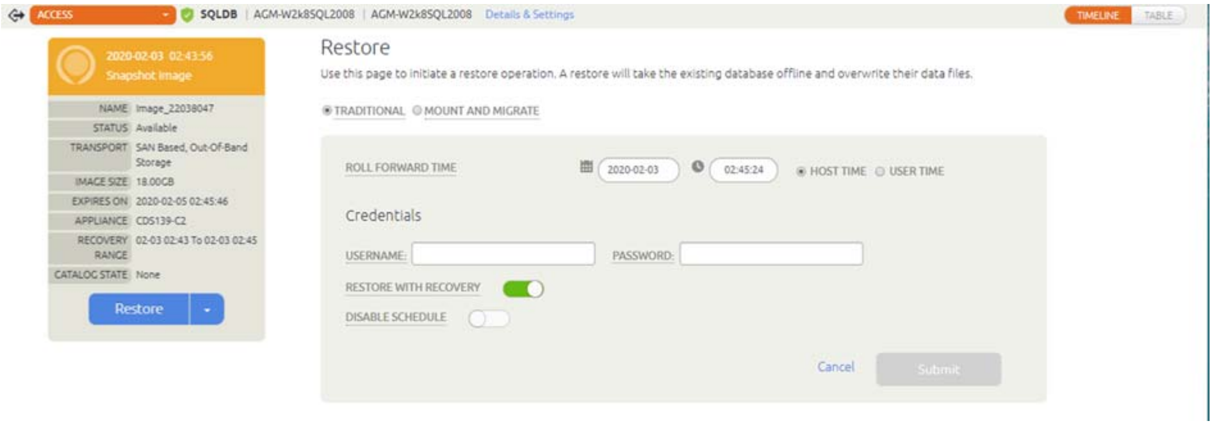
2016-12-05 21:01:31 UTC
Snapshot Image

NAME Image_2068216
STATUS Available
IMAGE SIZE 1.20GB
EXPIRES ON 2016-12-07 21:01:34 UTC
APPLIANCE SQA122-CT

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.


ACCESS
SQLDB | AGM-W2k8SQL2008 | AGM-W2k8SQL2008 Details & Settings
TIMELINE
TABLE
Restore
Cancel
Submit

2020-02-03 02:43:56
Snapshot Image

NAME Image_22038047
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 18.00GB
EXPIRES ON 2020-02-05 02:45:46
APPLIANCE CDS139-C2
RECOVERY RANGE 02-03 02:43 To 02-03 02:45
CATALOG STATE None

Restore

Use this page to initiate a restore operation. A restore will take the existing database offline and overwrite their data files.

● TRADITIONAL ○ MOUNT AND MIGRATE

ROLL FORWARD TIME 2020-02-03 02:45:24 ● HOST TIME ○ USER TIME

Credentials

USERNAME:
PASSWORD:

RESTORE WITH RECOVERY ●
DISABLE SCHEDULE ○

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 32
- VMotion for Host Migration of an Actifio-protected VM on page 33
- VMware FT (Fault Tolerance) Configurations on page 33
- Use of Resource Pools with Actifio Sky Appliance Instances on page 34
- Licensing Considerations on page 34
- Networking Considerations on page 35
- Best Practices for Actifio Sky Appliance in an HA Failover Configuration on page 35
- System Recovery Steps After an HA failover on page 35
- Migrating Actifio Sky Appliances on page 36

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.

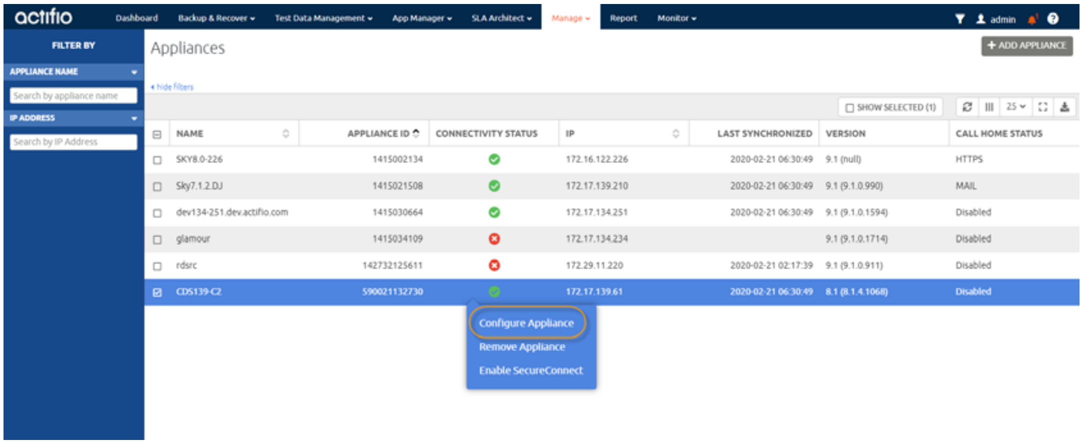
So while VMware HA failover can be used to restart a Sky Appliance VM instance in the event of a ESX host failure, it is best to configure the ESX environment and Actifio Sky Appliance instance to minimize the need for HA failover that requires the Sky Appliance VM to shut down without the proper quiesce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

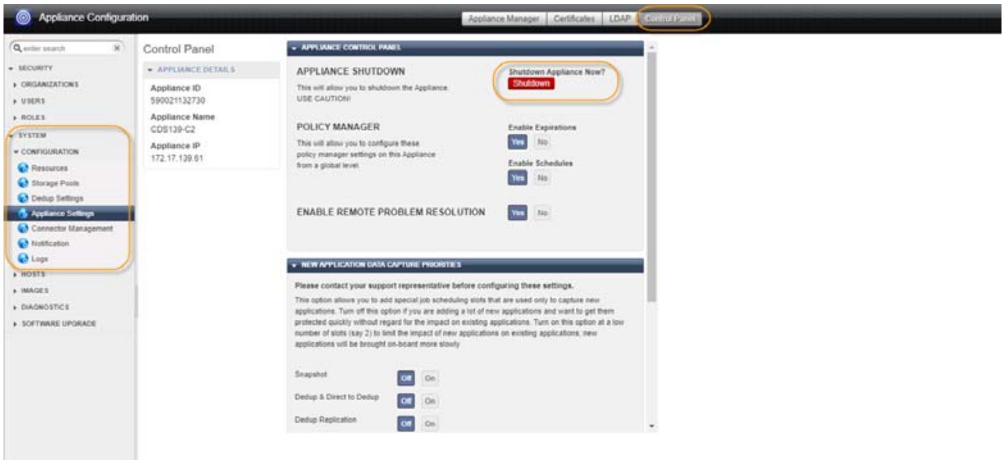
It is critical that you always shut down the Actifio Sky Appliance instance from within the Actifio Sky Appliance itself:

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.



☐	NAME	APPLIANCE ID	CONNECTIVITY STATUS	IP	LAST SYNCHRONIZED	VERSION	CALL HOME STATUS
☐	SKY8.0-226	1415002134	✓	172.16.122.226	2020-02-21 06:30:49	9.1 (null)	HTTPS
☐	Sky7.1.2.DJ	1415021508	✓	172.17.139.210	2020-02-21 06:30:49	9.1 (9.1.0.990)	MAIL
☐	dev134-251.dev.actifio.com	1415030664	✓	172.17.134.251	2020-02-21 06:30:49	9.1 (9.1.0.1594)	Disabled
☐	glamour	1415034109	✗	172.17.134.234		9.1 (9.1.0.1714)	Disabled
☐	rdsrc	142732125611	✗	172.29.11.220	2020-02-21 02:17:39	9.1 (9.1.0.911)	Disabled
☑	CDS139-C2	590021132730	✓	172.17.139.61	2020-02-21 06:30:49	8.1 (8.1.4.1068)	Disabled

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.



Appliance ID
590021132730

Appliance Name
CDS139-C2

Appliance IP
172.17.139.61

APPLIANCE SHUTDOWN

This will allow you to shutdown the Appliance.
USE CAUTION!

Shutdown Appliance Now?

POLICY MANAGER

This will allow you to configure these policy manager settings on this Appliance from a global level

Enable Expirations: [✓ Yes] No

Enable Schedules: [✓ Yes] No

ENABLE REMOTE PROBLEM RESOLUTION: [✓ Yes] No

Please contact your support representative before configuring these settings.

This option allows you to add special job scheduling slots that are used only to capture new applications. Turn off this option if you are adding a lot of new applications and want to get them protected quickly without regard for the impact on existing applications. Turn on this option at a low number of slots (say 2) to limit the impact of new applications on existing applications; new applications will be brought on-board more slowly

Snapshot: [✓ Off] On

Dedup & Direct to Dedup: [✓ Off] On

Dedup Replication: [✓ Off] On

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 defined in ***Installing and Upgrading Actifio Global Manager on a VMware Server*** 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***.

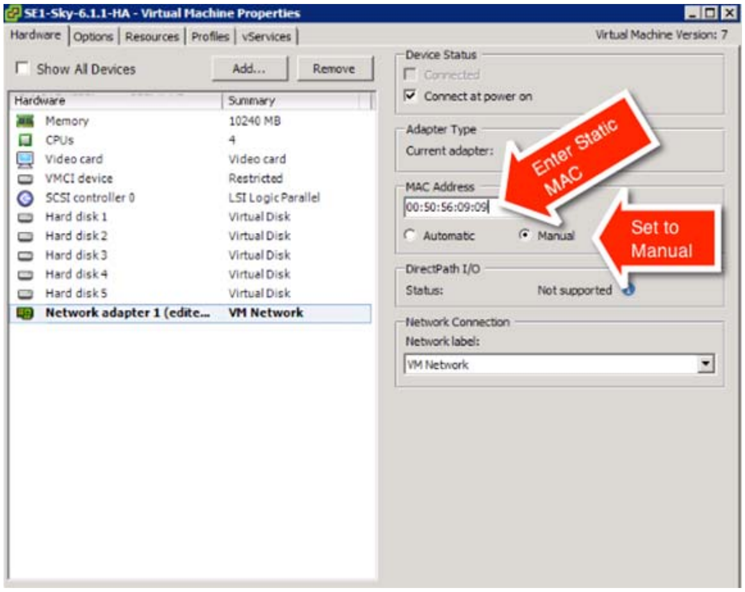
Licensing Considerations

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.



□ Show All Devices

Hardware	Summary
Memory	10240 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Hard disk 4	Virtual Disk
Hard disk 5	Virtual Disk
Network adapter 1 (edite...	**VM Network**

□ Connected
☑ Connect at power on

Current adapter:

MAC Address: 00:50:56:09:09

○ Automatic ● Manual

Status: Not supported

Network label: VM Network

Enter Static MAC

Set to Manual

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.

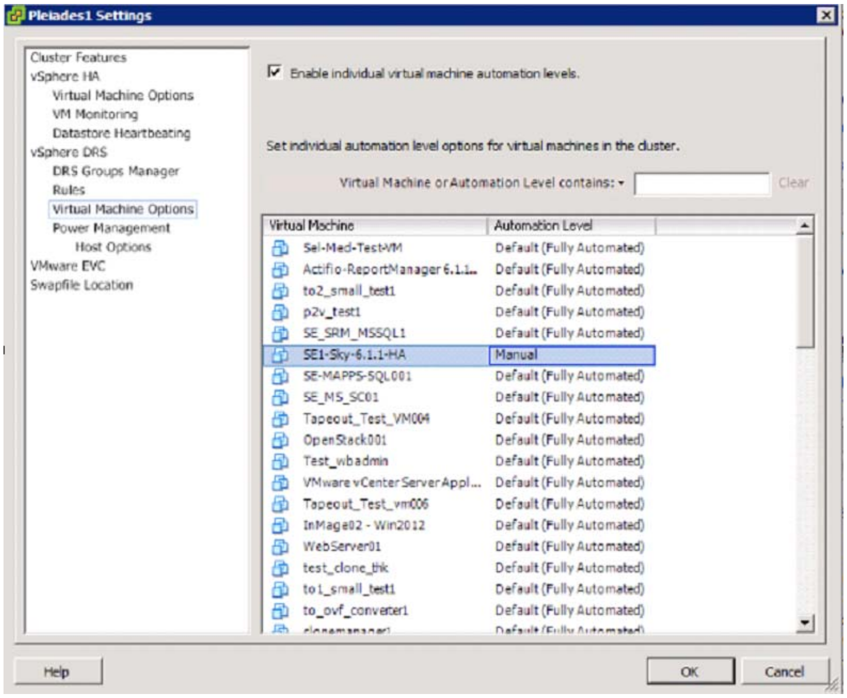
ESX Host failure: This assumes that the host Sky Appliance VM's ESX has failed and the Sky Appliance instance was not shut down cleanly. VMware HA can restart the Sky Appliance instance on another host in the HA cluster.

- 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.



☑ Enable individual virtual machine automation levels.

Set individual automation level options for virtual machines in the cluster.

Virtual Machine or Automation Level contains: ▾

Virtual Machine	Automation Level
Sel-Med-Test-VM	Default (Fully Automated)
Actifio-ReportManager 6.1.1...	Default (Fully Automated)
to2_small_test1	Default (Fully Automated)
p2v_test1	Default (Fully Automated)
SE_SRM_MSSQL1	Default (Fully Automated)
SE1-Sky-6.1.1-HA	Manual
SE-MAPPS-SQL001	Default (Fully Automated)
SE_MS_SC01	Default (Fully Automated)
Tapeout_Test_VM004	Default (Fully Automated)
OpenStack001	Default (Fully Automated)
Test_wbadmin	Default (Fully Automated)
VMware vCenter Server Appl...	Default (Fully Automated)
Tapeout_Test_vm006	Default (Fully Automated)
InMage02 - Win2012	Default (Fully Automated)
WebServer01	Default (Fully Automated)
test_clone_thk	Default (Fully Automated)
to1_small_test1	Default (Fully Automated)
to_ovf_converter1	Default (Fully Automated)
clonemanager1	Default (Fully Automated)

8 VMware Permissions

VMware sometimes combines, separates, renames, and adds permissions with new releases of vCenter Server.

This section includes:

Permissions Required for Catalog Indexing the Contents of a Windows Server in a VM on page 37

Creating the VDPReadOnly vCenter Role on page 39

Creating the VDPOperations vCenter Role on page 40

The vCenter Permissions List, vCenter 6.0 on page 41

The vCenter Permissions List, vCenter 6.5 on page 42

The vCenter Permissions List, vCenter 6.7 on page 43

The vCenter Permissions List, vCenter 7.0 on page 44

Assigning Minimum Permissions on page 45

Permissions Required for Catalog Indexing the Contents of a Windows Server in a VM

To scan VMs during backup and index the contents in the Actifio Catalog feature:

- The VM must have a Actifio Connector v8.0+ installed and running.
- The appliance must know the IP address for the VM (this normally happens during VM discovery).

If *both* of those are not true, then *one* of these must be true:

- The selected Catalog User (configured on the template or overridden on the application) in Actifio is the Administrator account.
- The selected Catalog User in Actifio is a member of the Administrators group and you have disabled Admin Approval Mode for "all administrators". Admin Approval Mode is disabled by default for Administrator and enabled by default for all other users in the Administrators group:
  a. In the Windows Group Policy Editor (gpedit.msc) on the protected server, go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
  b. Find "User Account Control: Run all administrators in Admin Approval Mode"
  c. Change the setting from the default of Enabled to Disabled.
  d. Reboot Windows for this change to take effect.

Note: *In some circumstances, interactively logging into the Windows VM using the selected Catalog user may resolve issues due to missing profiles. Do this by RDP into the Windows VM as the catalog user and then log out. This is only necessary once.*

Before You Begin

In order for Actifio to back up and recover VMware virtual machines, the Actifio Appliance must authenticate to the VMware vCenter Server with a user id that has sufficient privileges to perform the required operations. Create a custom Actifio user account assigned a custom VDPReadOnly role and a custom VDPOperations role with a reduced set of privileges. A custom user also enables traceability within VMware logs to find commands used by the Actifio Appliance. In this document, the custom user is referred to as **ActifioUser**.

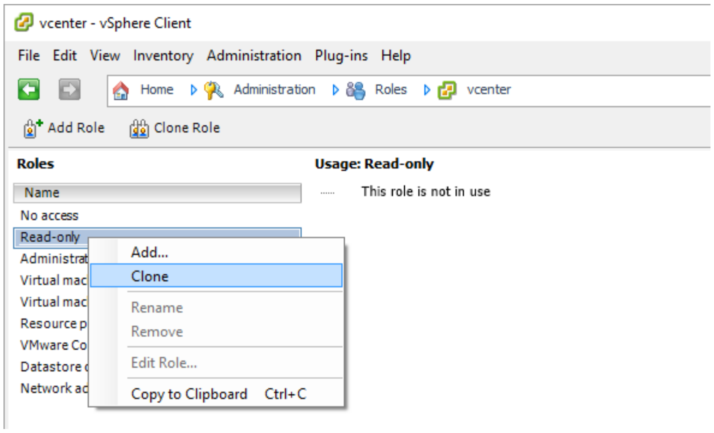
This document provides the minimum set of privileges needed to have the Actifio Appliance perform all backup and recovery operations.

Note: *Consider setting the password for this user to never expire. If the password expires then your Actifio Appliances will be unable to work with vCenter until the password is updated, which would be a manual process.*

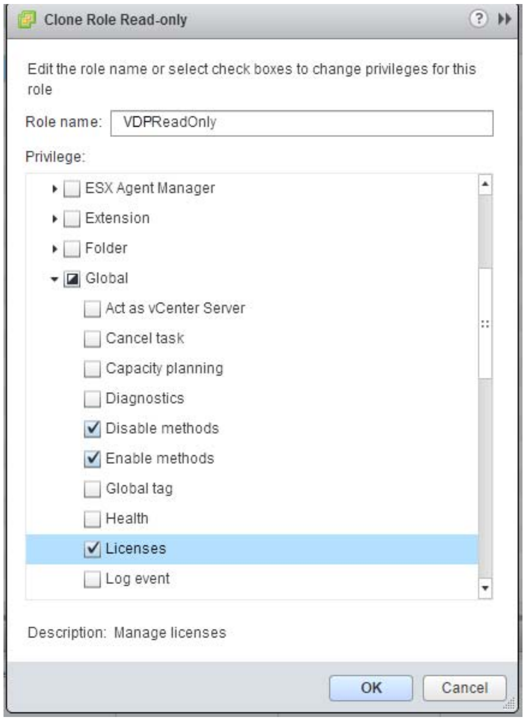
Creating the VDPReadOnly vCenter Role

You will create two vCenter roles. The first one is an VDPReadOnly role to assign the licenses permission and no other permissions:

1. Log into vSphere as a user with Administrator privileges.
2. On the vSphere Client Home page, under Administration, click **Roles**.
3. Right-click the **Read-Only** role and click **Clone**. A new *Clone of Read-Only* role appears in the list of roles.



4. Right-click **Clone of Read-Only** and click **Edit**.
5. Rename the new role **VDPReadOnly**.
6. Under **Global**, check:
   - **Disable methods**
   - **Enable methods**
   - **Licenses**
7. Assign no other privileges; you will add privileges as needed for the VM, cluster, etc. Click **OK**.


Clone Role Read-only

Edit the role name or select check boxes to change privileges for this role

Role name: VDPReadOnly

Privilege:

- □ ESX Agent Manager
- □ Extension
- □ Folder
- ▣ Global
  - □ Act as vCenter Server
  - □ Cancel task
  - □ Capacity planning
  - □ Diagnostics
  - ☑ Disable methods
  - ☑ Enable methods
  - □ Global tag
  - □ Health
  - ☑ Licenses
  - □ Log event

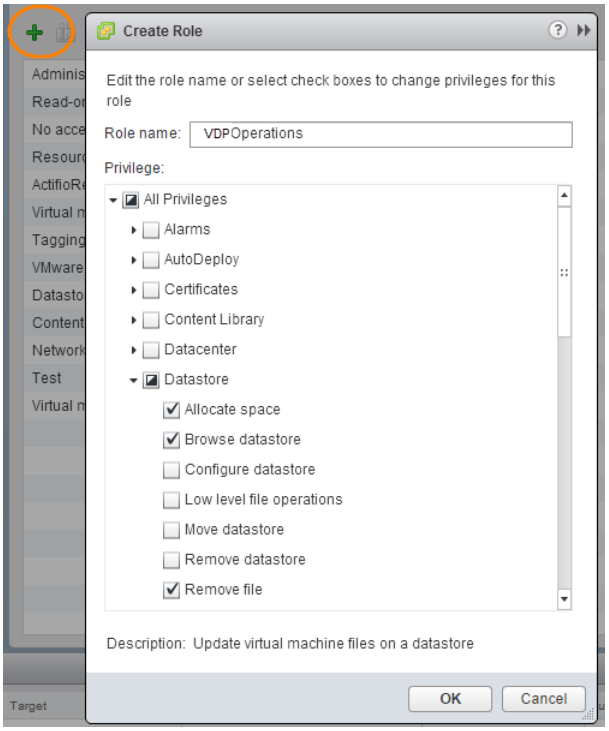
Description: Manage licenses

Note: *These examples show the vSphere client application running on a Windows host. Your screens will look a little different if you use the VMware web interface.*

Creating the VDPOperations vCenter Role

After the VDPReadOnly role exists, create a new vCenter role for Actifio operations:

1. Log into vSphere as a user with Administrator privileges.
2. On the vSphere Client Home page, under Administration, click **Roles**.
3. Create a new role called **VDPOperations**.
4. Check the checkboxes for each of the privileges listed in:
   - The vCenter Permissions List, vCenter 6.0 on page 41
   - The vCenter Permissions List, vCenter 6.5 on page 42
   - The vCenter Permissions List, vCenter 6.7 on page 43
5. Click **OK** to save the role.



Edit the role name or select check boxes to change privileges for this role

Role name: VDPOperations

Privilege:

- ▪ All Privileges
  - □ Alarms
  - □ AutoDeploy
  - □ Certificates
  - □ Content Library
  - □ Datacenter
  - ▪ Datastore
    - ☑ Allocate space
    - ☑ Browse datastore
    - □ Configure datastore
    - □ Low level file operations
    - □ Move datastore
    - □ Remove datastore
    - ☑ Remove file

Description: Update virtual machine files on a datastore

Set the Permissions by Checking their Checkboxes

Note: *An Actifio VM capture operation does not require capturing of .vmx files. To capture .vmx metadata files, the role must include the* ***All Privileges > Datastore > Update Virtual Machine Metadata*** *option.*

The vCenter Permissions List, vCenter 6.0

The Actifio vCenter Server user must have the following permissions:

- Datastore: Allocate Space
- Datastore: Browse Datastore
- Datastore: Low Level File Operations
- Datastore: Remove file
- Datastore: Update virtual machine files
- Global: Cancel task
- Global: Disable methods
- Global: Enable methods
- Global: Licenses
- Global: Log Event
- Host: Configuration: Storage partition configuration
- Host: Local Operations: Create virtual machine
- Host: Local Operations: Delete virtual machine
- Host: Local Operations: Reconfigure virtual machine
- Network: Assign network
- Resource: Assign virtual machine to resource pool
- Tasks: Create task
- Tasks: Update task
- vApp: Export
- vApp: View OVF Environment
- vApp: vApp application configuration
- Virtual machine: Configuration: Add existing disk
- Virtual machine: Configuration: Add new disk
- Virtual machine: Configuration: Add or remove device
- Virtual machine: Configuration: Advanced
- Virtual machine: Configuration: Change resource
- Virtual machine: Configuration: Settings
- Virtual machine: Configuration: Disk change tracking
- Virtual machine: Configuration: Disk lease
- Virtual machine: Configuration: Modify device settings
- Virtual machine: Configuration: Query unowned files
- Virtual machine: Configuration: Raw device
- Virtual machine: Configuration: Remove disk
- Virtual machine: Guest Operations: Execute
- Virtual machine: Guest Operations: Modify
- Virtual machine: Guest Operations: Query
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Interaction: Suspend
- Virtual machine: Inventory: Create from existing
- Virtual machine: Inventory: Create new
- Virtual machine: Inventory: Remove
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Clone virtual machine
- Virtual machine: Snapshot management: Create snapshot
- Virtual machine: Snapshot management: Remove snapshot
- Virtual machine: Snapshot management: Rename snapshot
- Virtual machine: Snapshot management: Revert to snapshot (*In vCenter 5.0 was Virtual machine: State.*)

The vCenter Permissions List, vCenter 6.5

The Actifio vCenter Server user must have the following permissions:

- Datastore: Allocate Space
- Datastore: Browse Datastore
- Datastore: Low Level File Operations
- Datastore: Remove file
- Datastore: Update virtual machine files
- Global: Cancel task
- Global: Disable methods
- Global: Enable methods
- Global: Licenses
- Global: Log Event
- Host: Configuration: Storage partition configuration
- Host: Local Operations: Create virtual machine
- Host: Local Operations: Delete virtual machine
- Host: Local Operations: Reconfigure virtual machine
- Network: Assign network
- Resource: Assign virtual machine to resource pool
- Tasks: Create task
- Tasks: Update task
- vApp: Export
- vApp: View OVF Environment
- vApp: vApp application configuration
- Virtual machine: Configuration: Add existing disk
- Virtual machine: Configuration: Add new disk
- Virtual machine: Configuration: Add or remove device
- Virtual machine: Configuration: Advanced
- Virtual machine: Configuration: Change resource
- Virtual machine: Configuration: Disk change tracking
- Virtual machine: Configuration: Disk lease
- Virtual machine: Configuration: Modify device settings
- Virtual machine: Configuration: Query unowned files
- Virtual machine: Configuration: Raw device
- Virtual machine: Configuration: Remove disk
- Virtual machine: Configuration: Settings
- Virtual machine: Guest Operations: Guest Operation Modifications
- Virtual machine: Guest Operations: Guest Operation Program Execution
- Virtual machine: Guest Operations: Guest Operation Queries
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Interaction: Suspend
- Virtual machine: Inventory: Create from existing
- Virtual machine: Inventory: Create new
- Virtual machine: Inventory: Remove
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Clone virtual machine
- Virtual machine: Snapshot management: Create snapshot
- Virtual machine: Snapshot management: Remove snapshot
- Virtual machine: Snapshot management: Rename snapshot
- Virtual machine: Snapshot management: Revert to snapshot (*In vCenter 5.0 was Virtual machine: State.*)

The vCenter Permissions List, vCenter 6.7

The Actifio vCenter Server user must have the following permissions:

- Datastore: Allocate space
- Datastore: Browse datastore
- Datastore: Low level file operations
- Datastore: Remove file
- Datastore: Update virtual machine files
- Global: Cancel task
- Global: Disable methods
- Global: Enable methods
- Global: Licenses
- Global: Log Event
- Host: Configuration: Storage partition configuration
- Host: Local Operations: Create virtual machine
- Host: Local Operations: Delete virtual machine
- Host: Local Operations: Reconfigure virtual machine
- Network: Assign network
- Network: Configure
- Resource: Assign virtual machine to resource pool
- Tasks: Create task
- Tasks: Update task
- Virtual machine: Configuration: Acquire disk lease
- Virtual machine: Configuration: Add existing disk
- Virtual machine: Configuration: Add new disk
- Virtual machine: Configuration: Add or remove device
- Virtual machine: Configuration: Advanced configuration
- Virtual machine: Configuration: Change settings
- Virtual machine: Configuration: Change resource
- Virtual machine: Configuration: Configure raw device
- Virtual machine: Configuration: Modify device settings
- Virtual machine: Configuration: Query unowned files
- Virtual machine: Configuration: Remove disk
- Virtual machine: Configuration: Toggle disk change tracking
- Virtual machine: Edit Inventory: Create from existing
- Virtual machine: Edit Inventory: Create new
- Virtual machine: Edit Inventory: Remove
- Virtual machine: Guest Operations: Guest Operation Modifications
- Virtual machine: Guest Operations: Guest Operation Program Execution
- Virtual machine: Guest Operations: Guest Operation Queries
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Interaction: Suspend
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Clone virtual machine
- Virtual machine: Snapshot management: Create snapshot
- Virtual machine: Snapshot management: Remove snapshot
- Virtual machine: Snapshot management: Rename snapshot
- Virtual machine: Snapshot management: Revert to snapshot (*In vCenter 5.0 was Virtual machine: State.*)
- vApp: Export
- vApp: View OVF environment
- vApp: vApp application configuration

The vCenter Permissions List, vCenter 7.0

The Actifio vCenter Server user must have the following permissions:

- Cryptographic operations: Direct Access
- Datastore: Allocate space
- Datastore: Browse datastore
- Datastore: Low level file operations
- Datastore: Remove file
- Datastore: Update virtual machine files
- Global: Cancel task
- Global: Disable methods
- Global: Enable methods
- Global: Licenses
- Global: Log Event
- Host: Configuration: Storage partition configuration
- Host: Local Operations: Create virtual machine
- Host: Local Operations: Delete virtual machine
- Host: Local Operations: Reconfigure virtual machine
- Network: Assign network
- Network: Configure
- Resource: Assign virtual machine to resource pool
- Tasks: Create task
- Tasks: Update task
- Virtual machine: Configuration: Acquire disk lease
- Virtual machine: Configuration: Add existing disk
- Virtual machine: Configuration: Add new disk
- Virtual machine: Configuration: Add or remove device
- Virtual machine: Configuration: Advanced configuration
- Virtual machine: Configuration: Change settings
- Virtual machine: Configuration: Change resource
- Virtual machine: Configuration: Configure raw device
- Virtual machine: Configuration: Modify device settings
- Virtual machine: Configuration: Query unowned files
- Virtual machine: Configuration: Remove disk
- Virtual machine: Configuration: Toggle disk change tracking
- Virtual machine: Edit Inventory: Create from existing
- Virtual machine: Edit Inventory: Create new
- Virtual machine: Edit Inventory: Remove
- Virtual machine: Guest Operations: Guest Operation Modifications
- Virtual machine: Guest Operations: Guest Operation Program Execution
- Virtual machine: Guest Operations: Guest Operation Queries
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Interaction: Suspend
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Clone virtual machine
- Virtual machine: Snapshot management: Create snapshot
- Virtual machine: Snapshot management: Remove snapshot
- Virtual machine: Snapshot management: Rename snapshot
- Virtual machine: Snapshot management: Revert to snapshot (*In vCenter 5.0 was Virtual machine: State.*)
- vApp: Export
- vApp: View OVF environment
- vApp: vApp application configuration

Assigning Minimum Permissions

To limit access of ActifioUser, assign the VDPReadOnly role to ActifioUser at the vCenter level and the VDPOperations role to ActifioUser at the Datacenter level, then set NoAccess at the highest level necessary to restrict ActifioUser from all VMs and ESXi servers that will never be mounted to or backed up by the Actifio Appliance.

To assign to ActifioUser the minimum permissions necessary to perform all required functions:

1. Log into vSphere as a user with Administrator privileges. On the vSphere Client Home page, click **Hosts and Clusters**.
2. Select the vCenter to ensure that permissions are propagated correctly. On the **Permissions** tab or under the Actions dropdown, select **Add Permission**.
3. Select **VDPReadOnly** from the Assigned Role drop-down menu.
4. Check the **Propagate to Children** check box at the bottom of the window.
5. Click **Add** to open the Select Users or Groups dialog box.
6. Select the domain where **ActifioUser** is located from the Domain drop-down menu and type **ActifioUser** in the Search box. Click **Add**. ActifioUser is added to the Users list. Click **OK**.
7. Select the Datacenter to ensure that permissions are propagated correctly.
8. On the **Permissions** tab or under the Actions dropdown, select **Add Permission**.
9. Select **VDPOperations** from the Assigned Role drop-down menu.
10. Check the **Propagate to Children** check box at the bottom of the window.
11. Click **Add** to open the Select Users or Groups dialog box.
12. Select the domain where **ActifioUser** is located from the Domain drop-down menu and type **ActifioUser** in the Search box. Click **Add**. ActifioUser is added to the Users list. Click **OK** and then click **OK** again.
13. Go back to Inventory > Hosts and Clusters. Right-click each branch that will have no Actifio jobs, select ActifioUser, and assign the **No Access** role to ActifioUser. Click **OK** to finish.

In this example vCenter hierarchy, if you want to:

(Assume ActifioOperations role was assigned at Datacenter 2).

Protect a Single VM

If you want Actifio to back up VM2111, then assign the No Access role to ActifioUser at VM2111 and at ESXi Cluster 22 in Step 13 above.

Protect Multiple VMs, Access within Cluster

If you want Actifio to back up some or all VMs in ESXi Cluster 21, and if you expect to mount or restore the images within the same cluster, then select ESXi Cluster 22 in Step 13 above.

Protect Multiple VMs, Access to Different DataCenter

If you want Actifio to back up some or all VMs in ESXi Server 211, and if you expect to mount or restore the images to an ESXi server in DataCenter 1, then select vCenter in Step 13 above.

- vCenter
  - Datacenter 1
  - Datacenter 2
    - ESXi Cluster 21
      - ESXi Server 211
        - VM2111
        - VM2112
    - ESXi Cluster 22
      - ESXi Server 221
      - ESXi Server 222
        - VM2221
        - VM2222