A VMware vCenter Administrator's Guide to Actifio Copy Data Management

actifio

Actifio 9.0

Copyright, Trademarks, and other Legal Matter

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

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ACTIFIO, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This software and the associated documentation are proprietary and confidential to Actifio. Use, copying, and distribution of any Actifio software described in this publication requires an applicable software license. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

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

Table of Contents

Preface ..... **v**

Actifio Appliances v

The ActifioNOW Customer Portal v

Actifio Support Centers v

Chapter 1 - Introduction **1**

Actifio Data Virtualization 1

Capture Mechanisms 2

Capture Methods 3

Capturing Virtual Server Data 4

Replicating Captured VMware Data 7

Datastore Space Monitoring 7

Accessing Data 8

Workflows to Automate Access to SQL Server Data 9

Chapter 2 - Discovering and Deleting VMware VMs **11**

Discovering VMs 11

Deleting VMs 13

Discovering Applications on a Host that Has Been Added to the Actifio System 14

Chapter 3 - Protecting VMware VMs **15**

The Application Manager Navigation Pane VM List 16

Protecting a VMware VM 17

Specifying Individual VMware Volumes to Protect 18

Application Advanced Settings for VMware VMs 20

Chapter 4 - Capturing VMware VMs Direct to Dedup **21**

Chapter 5 - Mounting a VMware VM Image **23**

Mounting a VMware VM Image to an Existing Host 23

Mounting a VMware VM Image to a New VM 25

Recovering a Mounted VMware VM to Production Storage 26

Chapter 6 - Replicating VMware Data to a Datastore 27

Chapter 7 - Restoring Virtual Machines 29

Chapter 8 - VMware Permissions 31

Creating the ActifioReadOnly vCenter Role 32

Creating the ActifioOperations vCenter Role 33

The vCenter Permissions List, vCenter 6.0 34

The vCenter Permissions List, vCenter 6.5 35

The vCenter Permissions List, vCenter 6.7 36

Assigning Minimum Permissions 37

Preface

This guide provides detailed instructions on how to capture and access VMware data with an Actifio appliance. This guide assumes you have read ***Introducing Actifio Copy Data Management***, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio appliance.

Your Actifio appliance's Documentation Library contains detailed, step-by-step, general instructions on how to use your Actifio appliance. Each guide is in PDF format and may be viewed, downloaded, and printed on demand. The following guides will be of particular interest:

- ***Setting Up Users and Roles With the Domain Manager***
- ***Planning and Developing Service Level Agreements***
- ***Virtualizing and Protecting Copy Data with the Application Manager***
- ***Accessing and Recovering Copy Data with the Application Manager***

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

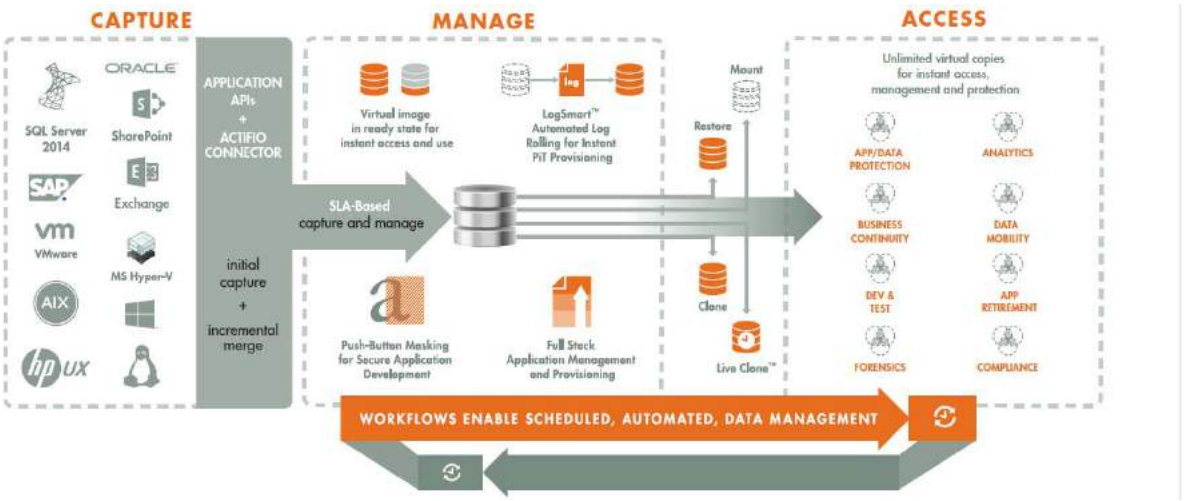
This chapter provides a high-level overview of basic Actifio concepts and procedures used to capture, manage, and access virtual machines (VMs). Specifically, this chapter describes:

- Actifio Data Virtualization on page 1
- Capture Mechanisms on page 2
- Capture Methods on page 3
- Capturing Virtual Server Data on page 4
- Accessing Data on page 8
- Workflows to Automate Access to SQL Server Data on page 9

Actifio Data Virtualization

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

Actifio CDS and Sky enable you to capture data from production systems, manage it in the most efficient way possible, and access virtual or physical copies of the data whenever and wherever they are needed.



Capture, Manage and Use Application Data

Application data is captured at the block level, in application native format, according to a specified SLA. A Golden copy of that data is created and stored once, and is then updated incrementally with only the changed blocks of data in an "incremental forever" model. Unlimited virtual copies of the data can then 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 changes to the application data or VM is captured. To track changes, the Actifio appliance uses either VMware API calls or the Actifio Connector.

VMware API Calls

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, if needed, 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

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. It allows you to capture applications that cannot be snapped by VMware. In addition, it also allows you to capture Microsoft® SQL Server clusters and offers options for handling individual database transaction logs.

Specifically, the Actifio Connector:

- Discovers applications
- Quiesces applications
- Where applicable, takes advantage of Microsoft® SQL Server and Exchange 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 on page 2.

Actifio supports three capture methods:

Out-of-Band on page 3

In-Band (CDS only) on page 4

LAN Free (CDS 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.

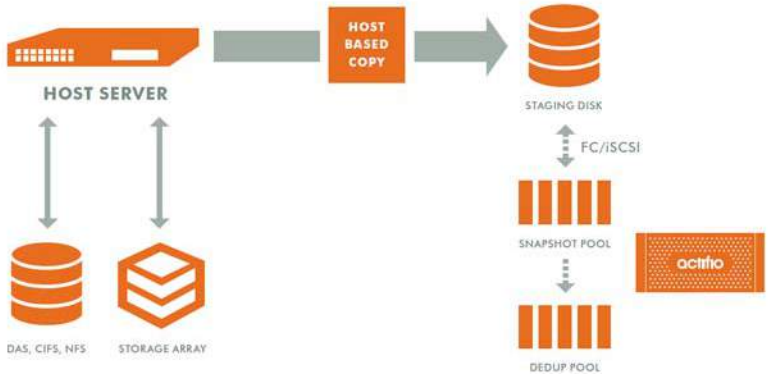
The Out-of-Band method will meet the needs of most users who want to capture:

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 via Fibre Channel (CDS only) or iSCSI.
- 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 only)

With the In-Band method, production data storage is controlled by an Actifio appliance. Snapshots and changed-block tracking are native to the Actifio appliance. The Actifio 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 only)

To capture VMware VMs, an Actifio 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 Actifio appliance access to the storage controller that manages the ESXi datastores.
2. Ensure that the storage controller is supported by the Actifio appliance.
3. Define the Actifio appliance as a host
4. LUN Mask all datastore LUNs to the Actifio appliance host.

The Actifio 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 Actifio appliance, then the Actifio appliance will switch to LAN based data capture.*

Capturing Virtual Server Data

Capturing virtual server copy data consists of five simple steps:

1. Add hypervisors via the Domain Manager Service.
2. Discover VMs via the Application Manager Service.
3. Discover applications on discovered VMs via the Application Manager Service.
4. Define Actifio Policy Templates and Resource Profiles according to your RPOs and RTOs via the SLA Architect Service.

Note: *You can create Production Direct-to-Dedup policies VMware VMs without keeping maintaining 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* ***Planning and Developing Service Level Agreements*** *guide for details.*

5. Apply Actifio Policy Templates and Resource Profiles to VMs and/or applications on a VM via the Application Manager Service.

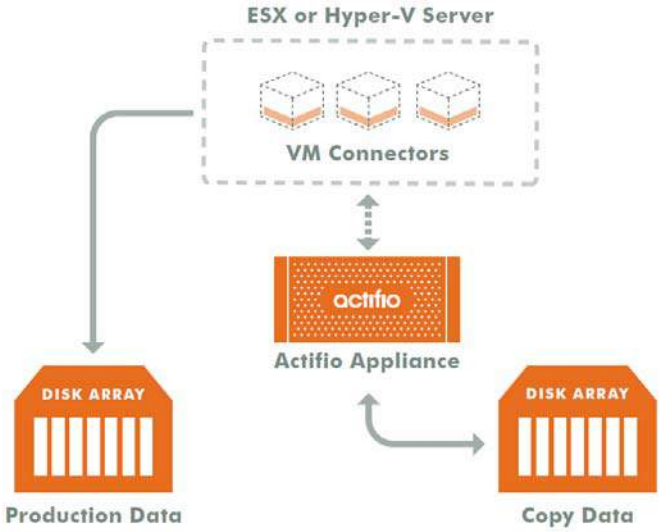
Note: *If you capture an entire VM with one policy and also capture individual applications on that VM with another policy, ensure that one capture operation completes before the other capture operation completes.*

When capturing virtual machine data, you can capture:

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

Capturing Applications on a VM

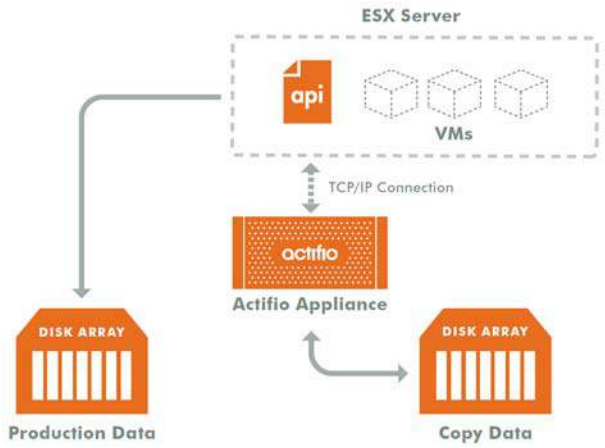
Installing the Actifio Connector on a VM allows you to capture applications on that VM. Multiple applications can be captured with a single policy template, or multiple policies can be used to capture individual applications.



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:*** *An Actifio Sky appliance is a VMware VM and 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 fast and without issues. Because the image presented is a fully functional virtual server, if needed, 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 (Microsoft SQL Server and Oracle only), 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 ***Configuring Resources and Settings With the Domain Manager*** in the Actifio Documentation Library.

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

Actifio Resource Policies 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

Resource Profiles that replicate captured VMware VM data have an additional option of replicating VMware data from a local Snapshot Pool to a remote VMware datastore. See Replicating VMware Data to a Datastore on page 27 for details.

By default, data is replicated to a Snapshot Pool on a remote Actifio appliance to which the local Actifio appliance is joined.

If you prefer, a VMware VM can be replicated to an 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 ***Configuring Resources and Settings With the Domain Manager*** for details.
- Data must be replicated via a Production to Mirror Policy that uses either Dedup-Async or StreamSnap replication. See ***Planning and Developing Service Level Agreements*** and ***Replicating Data Using Actifio Appliances*** for details. For details see, Replicating VMware Data to a Datastore on page 27.

Datastore Space Monitoring

Datastore space utilization is checked before creating the snapshot and also monitored through out 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 critical a 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: **Domain Manager > System > Configuration > Storage Pools**

Accessing Data

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

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.

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 (Microsoft SQL Server or Oracle) 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 an application or VM that can be refreshed when the source data changes. The advantage of a LiveClone is that they are independent copies 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 and not access or interfere with the production environment.

Restores

The restore function reverts the 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 through the Actifio user interface without specifying Restore with no Recovery, the database will be restored and brought on line without applying logs.

Workflows to Automate Access to SQL Server Data

While SLA Policy Templates govern the automated capture of production data. Workflows automate access to the captured data.

Workflows are built with captured data. Workflows can present data as either a direct mount or 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 on automatically on a schedule. Direct mounts allow you to instantly access captured Microsoft SQL Server data without actually moving the data.
- A LiveClone is a copy of your production Microsoft SQL Server data that can be updated manually or on a scheduled basis. You can mask sensitive Microsoft SQL Server data in a LiveClone prior to making it available to users.

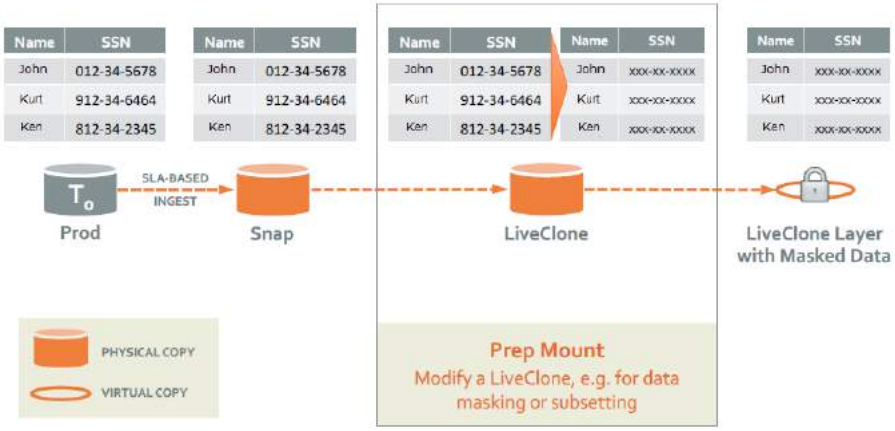
Combining Actifio's automated data capture, access control, with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait weeks for DBAs to update test and development environments, users can provision their own environments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



Workflow With Masked Social Security Data

2 Discovering and Deleting VMware VMs

This chapter details:

Discovering Applications on a Host that Has Been Added to the Actifio System on page 14

Discovering VMs on page 11

Deleting VMs on page 13

Discovering VMs

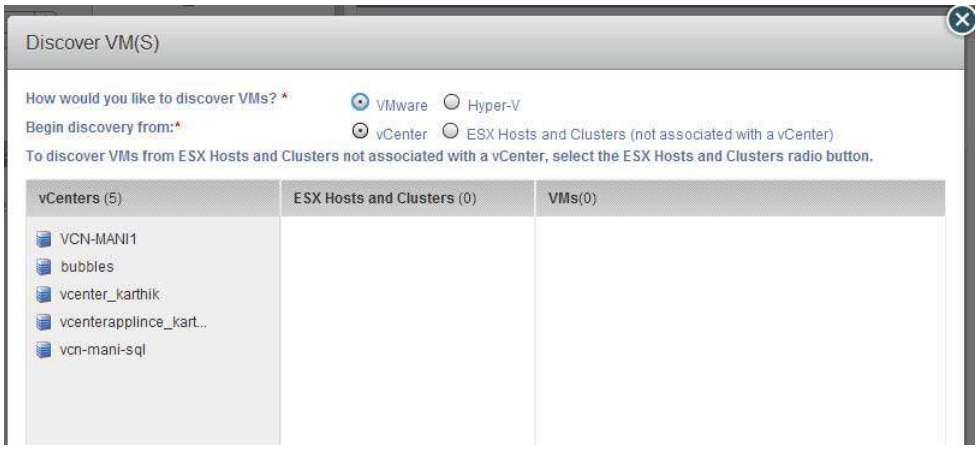
Virtual machines associated with a hypervisor host are discovered through the Application Manager. To discover VMs, you must first add the VM's hypervisor as a host. See ***Connecting Hosts to Actifio Appliances*** in the Actifio Documentation Library for details on how to add a new host.

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.*

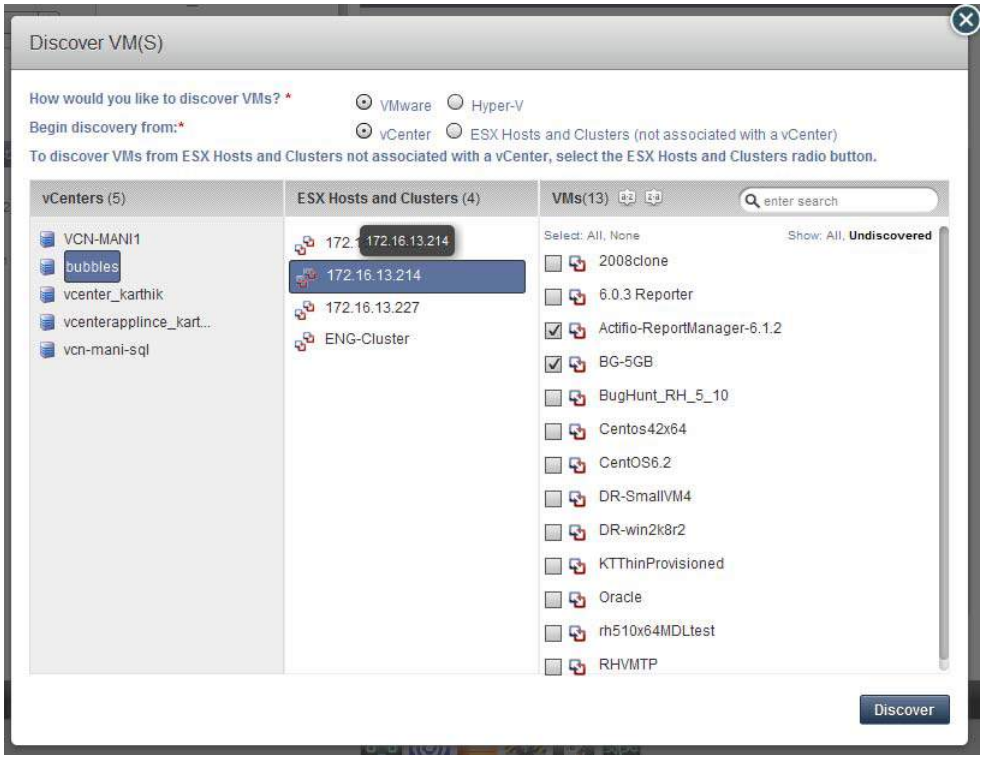
To discover a VM:

1. Open the **Application Manager**.
2. Click **Discover VM(s)**...from the service menu. The Discover VM(s) window appears.



Discovering vCenters on a Host

3. In the Discover VM(s) window, select either **VMware** or **Hyper-V**.
4. Depending on your previous choice select either a vCenter/ESX Host or SCVMM/Hyper-V Server. The Discover VMs window discovers and displays the host/appliances managed by the selected hypervisor.



Discovering VMs on an ESX Host in a vCenter

5. Select the virtual machines to protect.
6. Click **Discover**. The Virtual Machines are added to the list of virtual machines at **Application Manager** > **Applications by Type** > **VM**.
7. After discovery, the virtual machines and hypervisors are added as hosts in the Domain Manager.

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.*

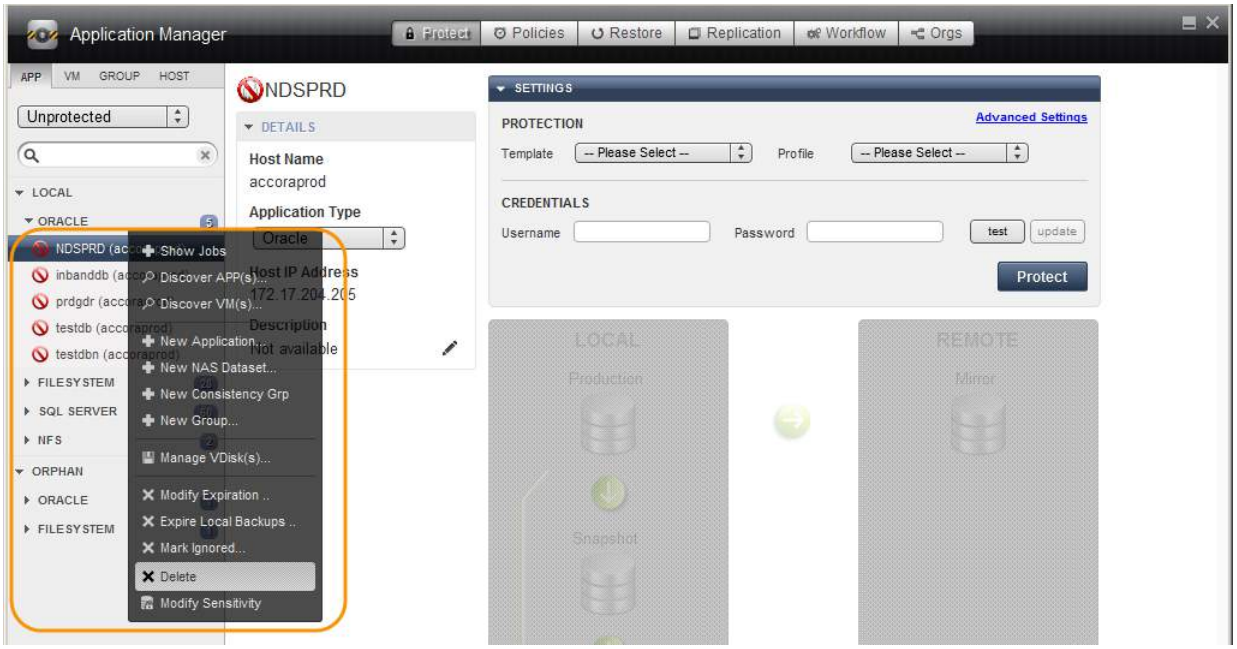
Deleting VMs

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

Note: *Remote VMs that appear in the Application Manager under the Remote category should be deleted from the remote Actifio appliance.*

To delete a VM:

1. Open the Application Manager.
2. Click the VM filter tab from the top of the navigation pane.



The Application Manager Navigation Pane List Filter

3. Select the VM to delete.
4. Right-click it to open the service menu, and click **Delete**.
5. Click **Yes** in the confirmation dialog.

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

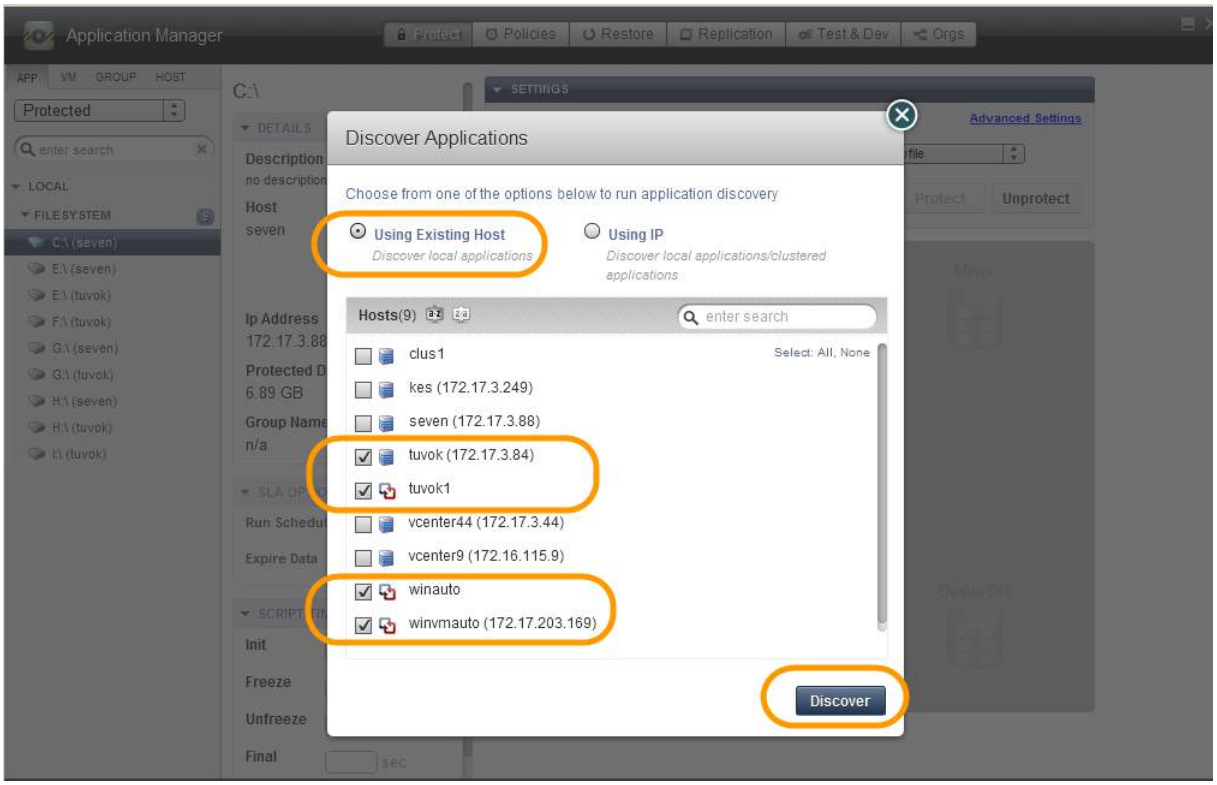
Note: *Deleting a VM or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that VM). If any stale images are left on an Actifio appliance (usually due to a remote appliance unavailability), in the left bottom menu list you will see an operation called* ***Cleanup Dedup Async*** *or* ***Cleanup StreamSnap****. For more information, see* ***Replicating Data Using Actifio Appliances****.*

Discovering Applications on a Host that Has Been Added to the Actifio System

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 Actifio Desktop to the **Application Manager**.
2. From the service menu, select **Discover App(s).** The Discover Applications dialog appears.
3. Select **Using Existing Host**.
4. Select the host that includes the application you would like to protect.
5. Click **Discover**. The navigation pane lists all the applications attached to the selected host, including applications residing on out-of-band storage, as soon as they are discovered.



Discovering Applications on a Host

Note: *Instructions for installing and configuring the Actifio Connectors are in* ***Connecting Hosts to Actifio Appliances*** *in the Actifio Documentation Library.*

3 Protecting VMware VMs

When an Actifio appliance protects an entire VMware VM, it is not aware of VM content so no application-specific actions are performed during either backup or restore. VMware VMs are captured in their entirety via VMware API calls.

Note: *As designed by VMware, disks set to Independent Mode cannot be snapped and therefore cannot be protected by an Actifio appliance.*

Note: *Before protecting VMs, be sure that your network configuration meets the requirements in the* ***Network Administrator's Guide to Actifio Copy Data Management****.*

You can also instruct the Actifio appliance to capture and protect only selected volumes (VMDK files) from VMware VMs during the backup process as detailed in Specifying Individual VMware Volumes to Protect on page 18.

A snapshot image of a VMware virtual machine includes the following information:

VM configuration details: VM Name, VM UUID, Inventory Path, OS Name, HostName, IPaddress, Number of CPUs, Memory, Version, GuestId, Resource Pool, Folder

Hardware details: Video card, Network interface details, CD-Rom, Floppy drive, Storage controllers such as LSI Logic Controller, Bus Logic Controller, LSI Logic SAS controller and Para virtual SCSI Controller

Volume details: Disk type, disk name, controller type, capacity and busid/lunid.

This chapter describes:

The Application Manager Navigation Pane VM List on page 16

Protecting a VMware VM on page 17

Specifying Individual VMware Volumes to Protect on page 18

Application Advanced Settings for VMware VMs on page 20

The Application Manager Navigation Pane VM List

VMs may be local or remote virtual machines. Applications hosted on VMs but discovered independently are listed under the APP tab.

VMs are listed under local or remote and as VMware or Hyper-V.

Click the pointer next to **Local**, **Remote**, **VMware** to expand the list of VMware VMs. The number of VMs listed is displayed to the right of the pointer. When a VM is selected details about the VM, and the SLA options currently applied are displayed.

The VM List, Showing Detail Pane for a VM

Note: *For VMware VMs from a vCenter, the Unique Name shown is the vc.uuid value, also called instanceUuid, which is guaranteed to be unique. The UUID displayed in vCenter is a different number, because vCenter displays the uuid.bios value, which is usually but not always unique.*

Protected Data is a measure of Actifio-managed copy data using the Managed Data License (MDL) metric. How this is calculated depends upon the type of VM being protected:

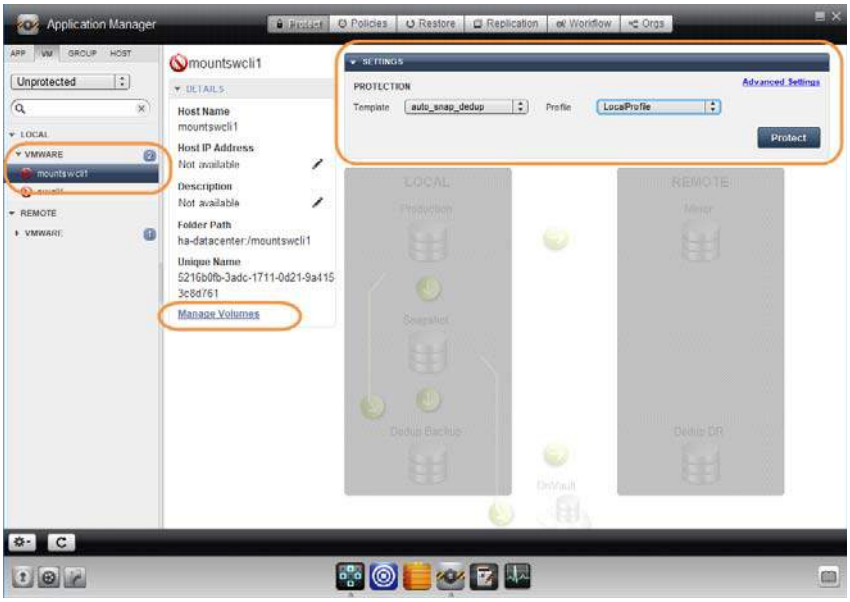
- **Only OS volume is protected**: The allocated size of that volume. If the volume is thinly provisioned, only the thinly allocated size is included. Any discovered applications with data on other volumes within that VM are counted separately towards consumed MDLs, as described in application-specific rules above.
- **All volumes are protected**: The total allocated size of all protected volumes. If volumes are thinly provisioned, only the thinly allocated size is included. Discovered applications with data on these protected volumes that are assigned separate SLAs (and thus are protected both as VMs and as applications) are double-counted. pRDMs and independent vRDMs, unless purposely marked as **Dependent**, are not included (since they are not protected).

Protecting a VMware VM

To protect an entire VMware VM:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **VM**. From the filter, select **Unprotected**.
3. On the navigation pane, select the VM that you want to protect.
4. To selectively choose which volumes (VMDK files) to backup from a VMware VM, click **Manage Volumes** (see Specifying Individual VMware Volumes to Protect on page 18).
5. Click the blue Advanced Settings link in the upper right corner of the Settings section to open the Application Advanced Settings page. Set the Application Advanced Settings as needed. Application Advanced settings are detailed in Application Advanced Settings for VMware VMs on page 20.
6. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
7. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
8. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs and according to the hours of operations defined in the template. For example, if at 10:00 AM today you assign a template that has hours of operation from 2:00 AM to 5:00 AM, then the first job will not start until the Actifio appliance has an available job slot after 2:00 AM tomorrow.

Note: *A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings.*



Protecting a VM

Specifying Individual VMware Volumes to Protect

You can choose which volumes to back up from a VMware VM prior to protecting it. This gives you the granularity to choose from a list of volumes mounted to a VMware VM to back up as part of the protection sequence. You can explicitly include the volumes to be captured or explicitly exclude volumes that should not be part of the capture process. You can then mount an individual captured VM volume to a host.

To select individual volumes to protect:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **VM**. From the filter, select **Unprotected**.
3. On the navigation pane, select the VM that you want to protect.
4. Click **Manage Volumes**. The Manage Volumes dialog appears.
5. From the Manage Volumes dialog, select from the following options to define how the Actifio appliance should protect the volumes in the selected VM:

   Capture all volumes: Captures the boot volume and all volumes in the VM. Any newly added volumes to the original VM will be captured when they are detected. This is the default selection.

   Capture boot volume: Captures only the boot volume and excludes all other volumes in the VM. When protecting VMs, if the application binaries are spread over multiple VMware volumes or if the boot volume is not the first drive on the bus, then the entire boot volume may not be captured.

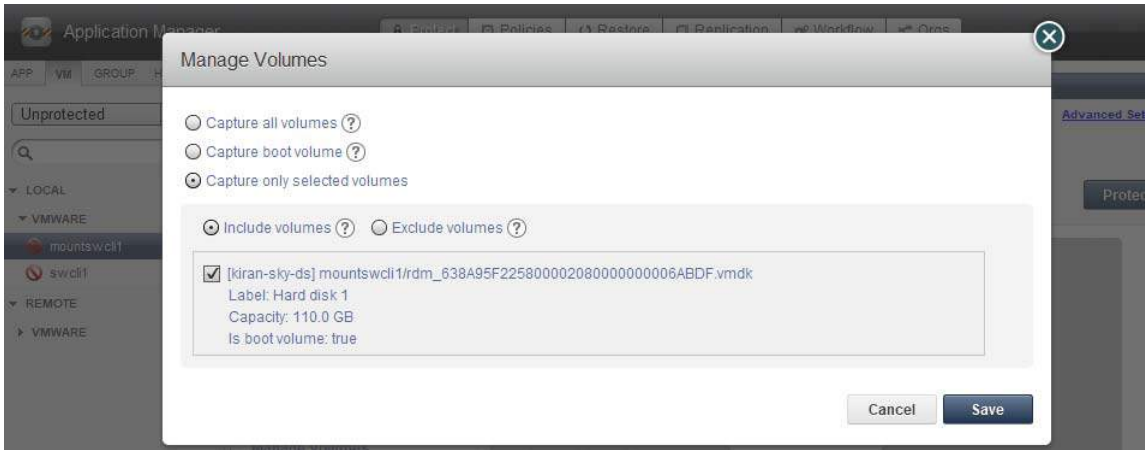
   Capture only selected volumes: Displays the **Include volumes** and **Exclude volumes** options along with a listing of all volumes in the specified VM. Make your selection based on the following:

   Include volumes: Captures the selected volumes in the VM, but any newly added volumes will be excluded from the capture process.

   If a selected volume is no longer available on the source VM, the capture job will succeed and then warn you the first time that the volume is detected as missing. If a previously selected volume re-appears after it has been identified as missing, future capture jobs will capture the VM.

   Exclude volumes: Excludes the selected volumes in the VM from being included in the capture process, but any newly detected volumes will automatically be captured.

   If a previously discovered volume is no longer available on the source VM, the capture job will succeed and then warn you the first time that the volume is detected as missing. If a previously discovered volume re-appears after it has been identified as missing, future capture jobs will capture the VM.

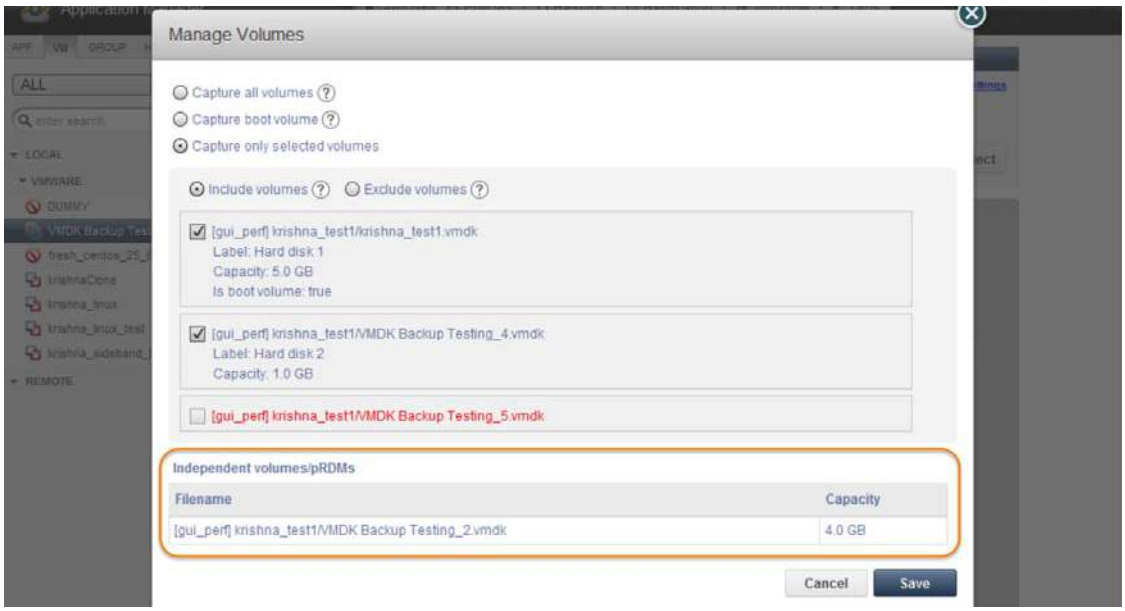


Choosing Volumes in the Manage Volume Dialog

6. Click **Save** to update the changes. The `Volumes have configured successfully` message is displayed.

7. After you explicitly include or exclude one or more individual volumes for capture, if you then delete one or more volumes from the VM and return to the Manage Volumes window you will see that the deleted volumes appear in red and the associated check boxes are disabled. This indicates that these volumes are unavailable for capture.

   In addition, the Independent Volumes/pRDMs section at the bottom of the Managed Volumes dialog shows a listing of the independent volumes and pRDM volumes that reside on the VM and that are not part of the capture process.



Summary of Deleted Volumes and Independent Volumes and pRDMs

Application Advanced Settings for VMware VMs

To configure application advanced settings for protecting a VMware VM:

1. Open the Application Manager to the **Protect** tab.
2. Select **VM** and select a VM from the navigation pane.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.
    - From the **Application Consistent** drop-down list, you can select from the following options:

      Take crash consistent backup: Crash-consistent backup is a fast backup of application data in storage as if power were lost at that moment. It does not pause application data I/O. All data on disk are saved, and data in memory is lost. Incomplete transactions may be saved. The recovery of a crash consistent backup may take longer time and introduce exceptions. Typically recovery from crash has to be made manually. Crash consistent backups are easy and fast for virtual machines.

      Take application consistent backup: Application-consistent backup notifies the application to prepare for a backup. This option loses no data. It pauses application data I/O, completes in-flight transactions, and flushes memory to disk. On recovery, data is easily accessible. For virtual clients, usually an agent is needed to get notification of a backup at host, and then notify applications, and may need to wait for an approval from applications. Not all applications support application-consistent backups.

      Take crash consistent backup on last try: This option initially takes application consistent backups, but if an application consistent backup fails for any reason, it will then take a crash consistent backup.

    - **Username/Password**: User credentials for truncating an SQL transaction log. This is required only if log truncation is required.
    - Select whether to truncate the logs after every backup from the **Truncate Log After Backup** drop-down list. When this is selected, application-related logs are truncated until the recent or current backup.
    - If the VM includes an SQL database, then enter an **SQL Database Backup Path** to define a location for a temporary SQL backup. If the Actifio Connector takes a full, native backup of the SQL Server database, the backup will be saved in this directory. Ensure that there is enough free space n the volume hosting this directory to hold a full database backup.
    - **Job Behavior When Target VM Needs Snapshot Consolidation**: If the VM requires consolidation:

      Fail the job: backup/DAR/direct-dedup jobs fail.

      Run the job without performing consolidation: All jobs run normally even if consolidation is pending.

      Perform consolidation at the beginning of the job: Backup/direct-dedup/DAR jobs try to perform consolidation at the beginning of the job. If consolidation fails, the job fails with an error message.
4. Click **Save** to update the changes.

Failed VM Protection Jobs

Sometimes a protection job fails. The most common job failure error codes are:

Error 43: retrieving VM details failed

Error 933: Failed to find VM with matching BIOS UUID.

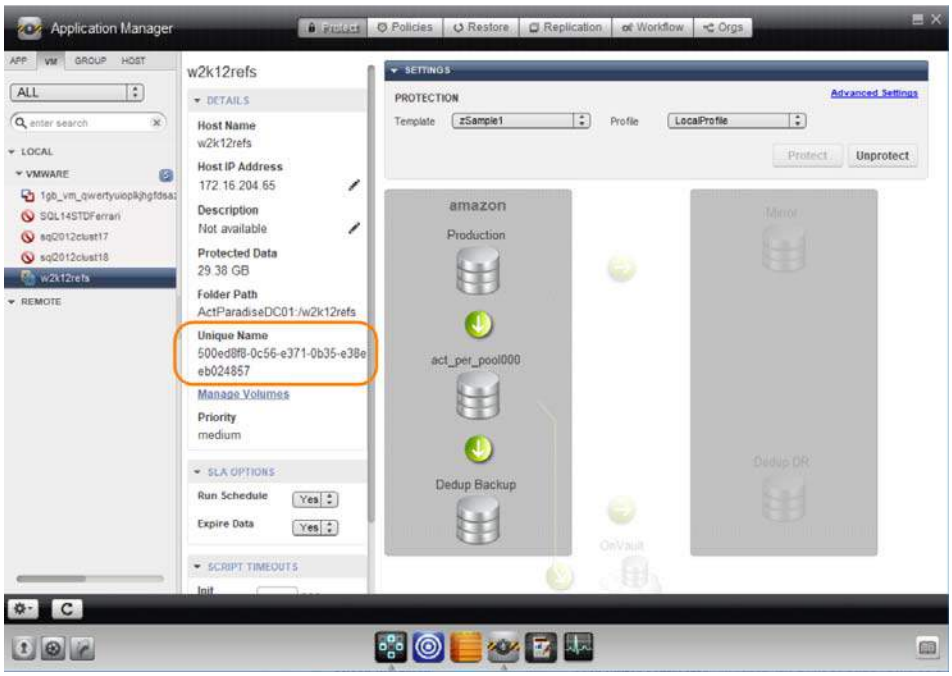
Error 833: Failed to login to vCenter Server

The most common causes for a VM backup failure are:

- Actifio Appliance has lost connection to the vCenter (possibly migrated)
- VM's UUID has been modified
- vCenter password has expired

Checking whether the VM has been moved or if UUID has been modified

Check whether the VM has been removed from the vCenter. If the VM still exists on this vCenter, then rediscover it. Check if it was discovered as a new UUID. Confirm this by looking at the UUID of the newly discovered VM and comparing it to the previously discovered Application. If the UUIDs do not match, the VM may have been cloned.



Checking connectivity and credentials

To test connectivity and credentials:

1. Log into the Actifio Desktop and select the vCenter in the Domain Manager under System > Configuration > Hosts.
2. Click **Test**. This will test if the known credentials have the proper permissions to access the vCenter. If this test fails, update the username and password.

4 Capturing VMware VMs Direct to Dedup

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

- Enable change block tracking for Actifio's incremental forever capture strategy.
- Quiesce applications for application consistency during capture.

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

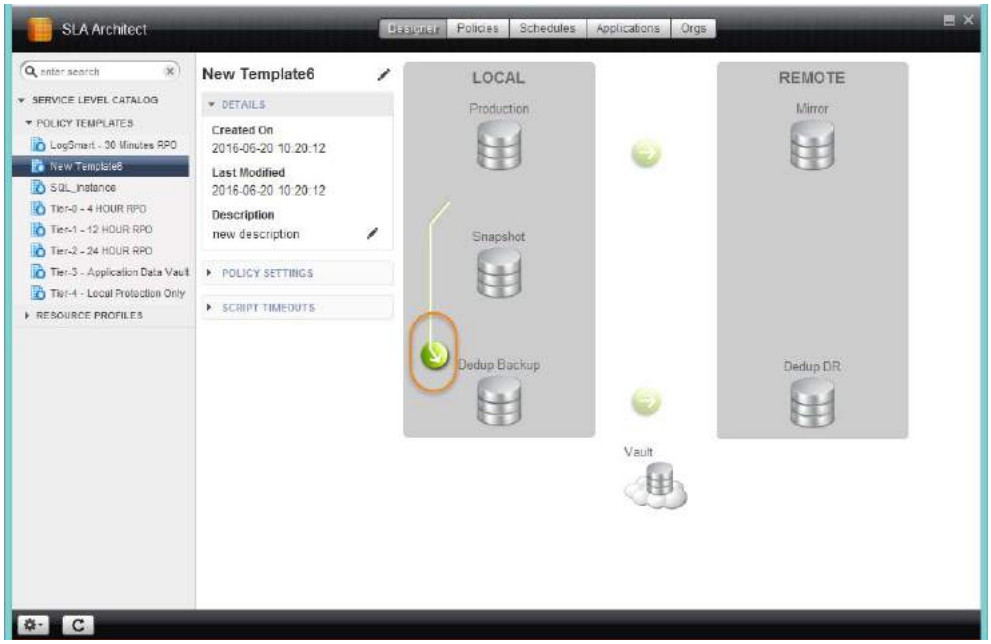
Capturing VMware VMs directly to a Dedup Backup Pool:

- Reduces the amount of storage space required for local Snapshot Pools because data is sent directly to the Dedup Pool.
- Is meant for long term retention when instant access from a Snapshot Pool is not required.
- Can be replicated to a second Actifio appliance for even longer term retention

Capturing VMware VMs Direct to Dedup

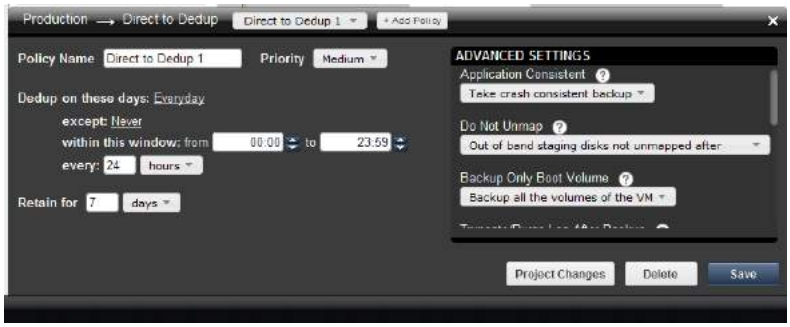
To capture a VMware VM directly to dedup you must:

1. Create a Policy Template in the Actifio SLA Architect as described in ***Planning and Developing Service Level Agreements***.



Direct to Dedup

2. Define the Policy Template's Production to Direct to Dedup policy as described in ***Planning and Developing Service Level Agreements***.



Direct to Dedup Policy

3. When defining a Production to Direct to Dedup policy, you will be prompted to confirm your actions:

Confirmation Message

4. Once the Policy Template with its Production to Direct to Dedup policy is defined, go to the Actifio Application Manager and apply the Policy Template to the required VM(s) as described in Managing Copy Data with the Application Manager.

5 Mounting a VMware VM Image

This chapter provides instruction for mounting VMware VMs:

- Mounting a VMware VM Image to an Existing Host on page 23
- Mounting a VMware VM Image to a New VM on page 25
- Recovering a Mounted VMware VM to Production Storage on page 26

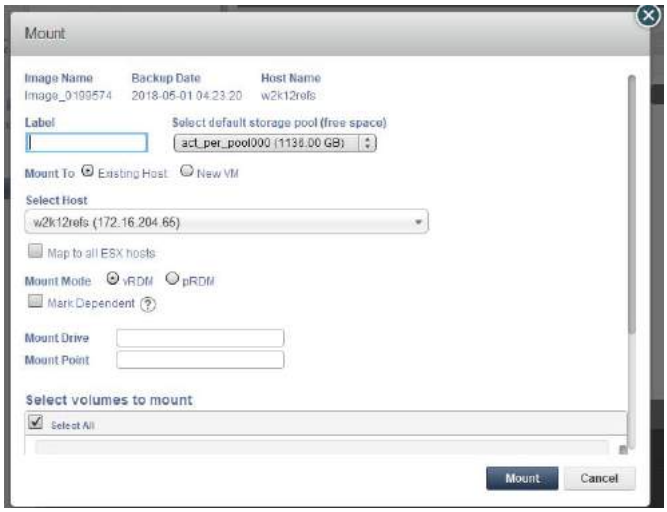
Mounting a VMware VM Image to an Existing Host

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).

To mount a VMware VM to an existing host:

1. Open the **Application Manager** to the **Restore** tab.
2. Select the VM from the navigation pane.
3. Select the time period for images using the calendar tool to filter the list of images as needed.
4. Select the image type by clicking on the corresponding Snapshot, Dedup, Remote, LiveClone, or Vault buttons. You can use the Shift key to select multiple types.
5. Select the image to mount from the list on the right. The selected image icon turns green and detailed information about it is displayed in the image box at the center of the display. The most recent image is selected by default.
6. Click the pull-down menu from the bottom right of the image information display and select **Mount**. The Mount Job window appears.



Mounting a VM

7. Image Name, Backup Date, and Host Name are provided at the top of the screen. A **Label** is optional.
8. If necessary, change the default storage pool from the **Select default storage pool** drop-down list.
9. Select a host from **Select Host**(s) to mount the image to. You can select any known host from the dropdown list, grouped into Physical Machines and Virtual Machines. If you need a host that has not yet been added, add it from the Domain Manager service menu.
10. Select whether to **Map to all ESX hosts**, and then select a **Mount Mode**:
    - **vRDM**: 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 (2TB minus 512B). In ESXi 5.5, the size was increased to 62TB.
    - **pRDM**: Use pRDM (physical raw device mapping) 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.

> ***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.*

11. Select whether to mount it to an existing VM host or to a VM host that you create, as described in Mounting a VMware VM Image to a New VM on page 25.
12. **Mount Drive**: (Windows only). Specifies a drive letter to the volume. If the drive letter is not available, the job fails. If multiple volumes are found, it assigns subsequent drive letters. If no Mount Drive is specified, the Connector chooses a drive letter itself, if available. If you are concerned about running out of drive letters, see ***Accessing and Recovering Copy Data with the Application Manager***.
13. **Mount Point**: the full path at which to mount the volume. If the path is an empty folder, the Connector will use it. If it does not exist, the Connector will create it. *If it exists 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 Connector chooses the user specified for one volume, and for the remaining volumes it appends an underscore (_) followed by a number, i.e., <user_specified>_#.
14. Select a single or multiple volumes from **Select volumes to mount**. By default, all volumes are selected.

15. Click **Mount**. A job is submitted to mount the image to the selected host. After the image has been mounted, the Active Images pane lists it among the images mounted on the host. Select the mounted image from the list.

Mounting a VMware VM Image to a New VM

When mounting a VMware VM as detailed in Mounting a VMware VM Image on page 23, you can choose to create a **New VM**.

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

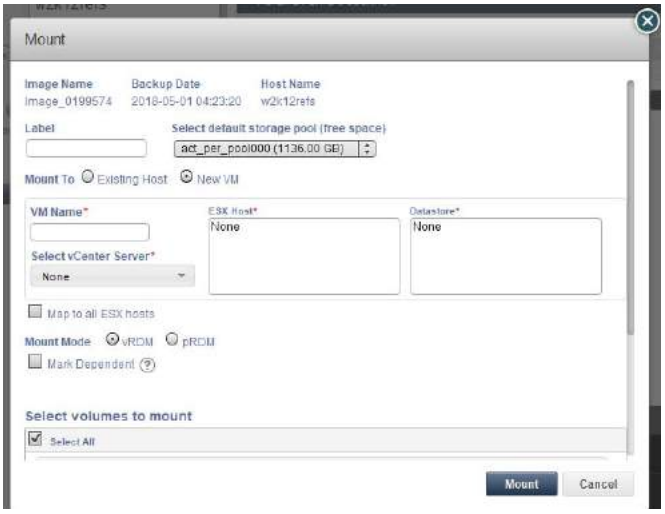
1. Enter a name for the new VM that you want to mount.
2. Specify a vCenter server, an ESX host, and a datastore in **Select vCenter Server**, **ESX Host**, and **Datastore** respectively.

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

   Select a single or multiple volumes to mount. By default all the volumes are selected. The first volume cannot be deselected.

   Note: *The Actifio Desktop 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.*

3. Return to Mounting a VMware VM Image on page 23.

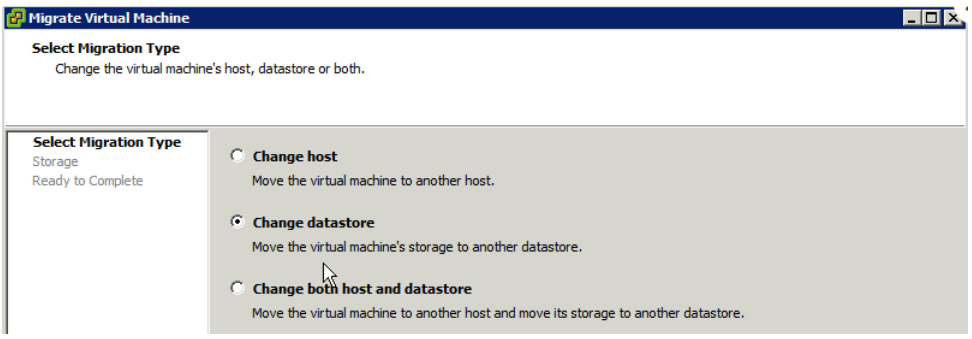


Mounting a VMware VM to a New VM

Recovering a Mounted VMware VM to Production Storage

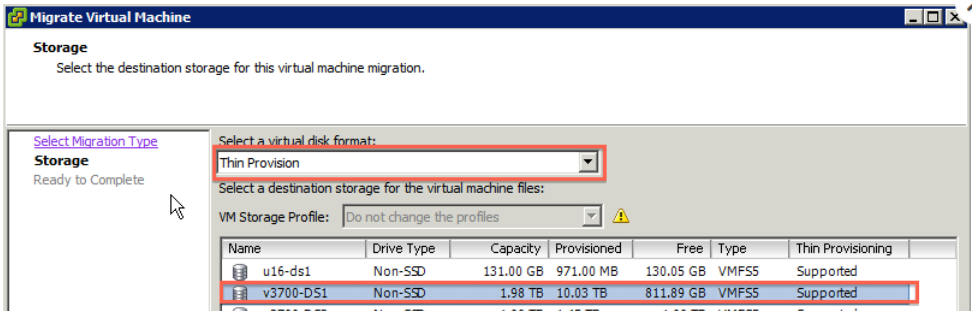
To mount a VMware VM and then migrate the VM data via VMware ESX vMotion:

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.



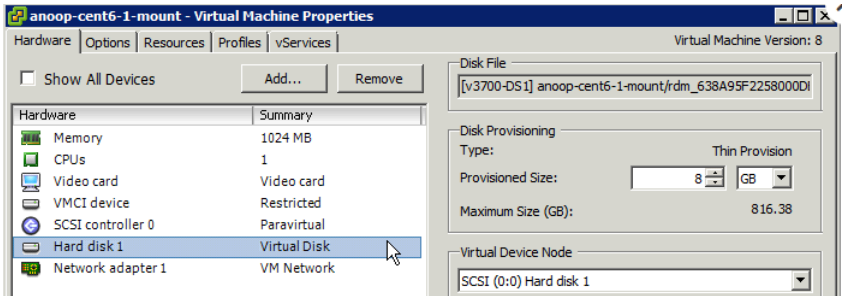
Change the Datastore

   - Change the format of the virtual disk. Leaving it as "Same format as source" will not work.



Change the Virtual Disk Format

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.*



After the vMotion Procedure, You Have VDisks Instead of a Mapped Raw LUN

3. Unmount & Delete the mount as described in ***Accessing and Recovering Copy Data with the Application Manager***.

6 Replicating VMware Data 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 ***Configuring Resources and Settings With the Domain Manager*** in the Actifio Documentation Library.

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.

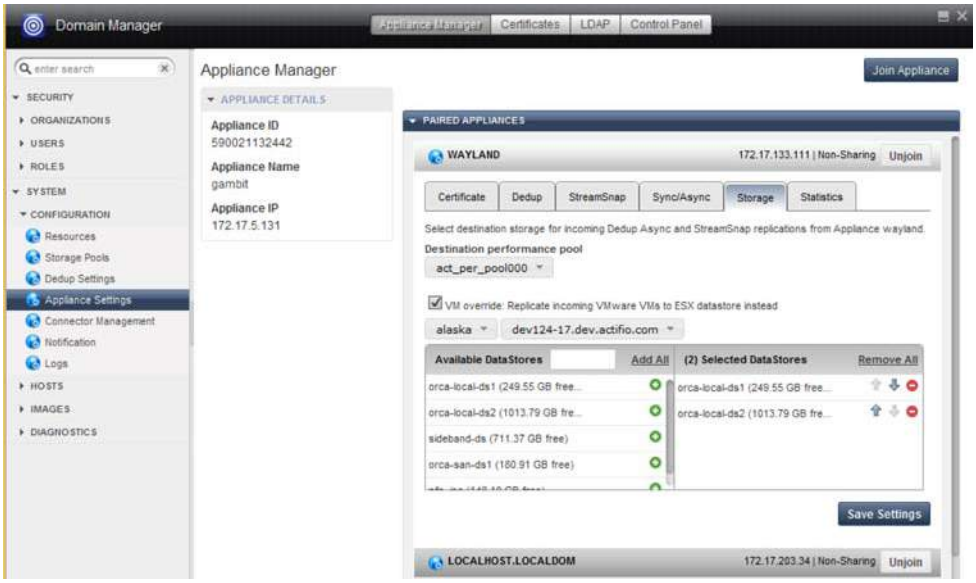
When coupled with a Production to Mirror Policy, a Resource Profile can replicate VMware data directly to a datastore. To use this option:

- 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 ***Configuring Resources and Settings With the Domain Manager*** for details.
- Data must be replicated via a Production to Mirror Policy that uses either Dedup-Async or StreamSnap replication. See ***Planning and Developing Service Level Agreements*** and ***Replicating Data Using Actifio Appliances*** for details.

To replicate VMware data directly to a datastore:

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

1. Open the **Domain Manager** to **System** > **Configuration** > **Appliance Settings**.
2. Click the **Storage** subtab and the storage options are displayed:



Storage Options

3. If the local Actifio appliance is joined with multiple remote Actifio appliances, select the remote Actifio appliance needed.
4. Click the **VM override** check box.
5. From the dropdown menus, select a vCenter host/ESX host
6. 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
7. Click **Save Settings** and 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) more can be added at a later date. Replicated VMDKs will be written to the new datastore(s). Data will not be balanced across datastores when new datastores are added.

7 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 risk of data loss. The Actifio appliance offers other options for recovering data. Before committing to a restore operation, please read ***Restoring Copy Data with the Application Manager***.

Applications on VMs that are protected through the Actifio Connector can be protected and restored as individual applications. See ***Accessing and Recovering Copy Data with the Application Manager*** 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 ***Accessing and Recovering Copy Data with the Application Manager***.

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 in the Actifio Desktop. If you need to add a new snapshot pool see Adding Snapshot Pools in ***Configuring Resources and Settings With the Domain Manager***.

To restore a VM:

1. Open the Application Manager to the **Restore** tab.
2. From the navigation pane, select the VM to restore.
3. In the application details under SLA Options, set **Run Schedule** to **No**. This is to prevent a new protection job from starting.
4. Select the image type by clicking on the corresponding Snapshot or Dedup button.
5. If the image that you need is not shown in the graphic list on the right (because it is from an earlier date), then use the calendar tool at the top of the screen to include the period that has the desired image.
6. Select the image to restore from the list on the right. The selected image icon turns green and detailed information about it is displayed in the image box at the center of the display.
7. From the pull-down menu, select **Restore**. The Restore Job window is displayed.
8. Check the **Power on VM after restore** checkbox if you want the restored VM to be powered on after the restore operation is complete.
9. Select a single volume or multiple volumes to restore. By default all the volumes are selected.
10. Click **Submit**. A warning dialog appears. Read the warning message carefully and then enter **DATA LOSS** in the provided field to confirm.
11. A second warning appears. Enter **OVERWRITE OTHER APPS** to confirm the restore operation.
12. Click **Start Restore** and the image is restored.

8 VMware Permissions

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

This section includes:

Creating the ActifioReadOnly vCenter Role on page 32

Creating the ActifioOperations vCenter Role on page 33

The vCenter Permissions List, vCenter 6.0 on page 34

The vCenter Permissions List, vCenter 6.5 on page 35

The vCenter Permissions List, vCenter 6.7 on page 36

Assigning Minimum Permissions on page 37

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 custom ActifioReadOnly role and ActifioOperations role with a lesser 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**.

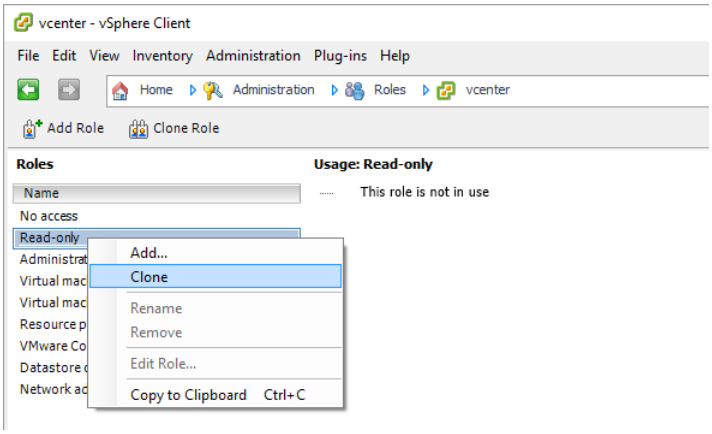
This document provides the minimum set of privileges needed to have the Actifio appliance perform all backup and recovery operations.

> ***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.*

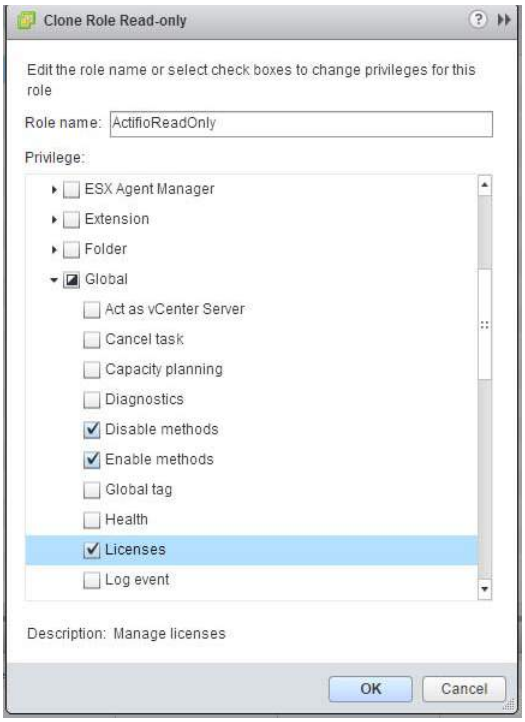
Creating the ActifioReadOnly vCenter Role

You will create two a vCenter roles. The first one is an ActifioReadOnly 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 **ActifioReadOnly**.
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**.

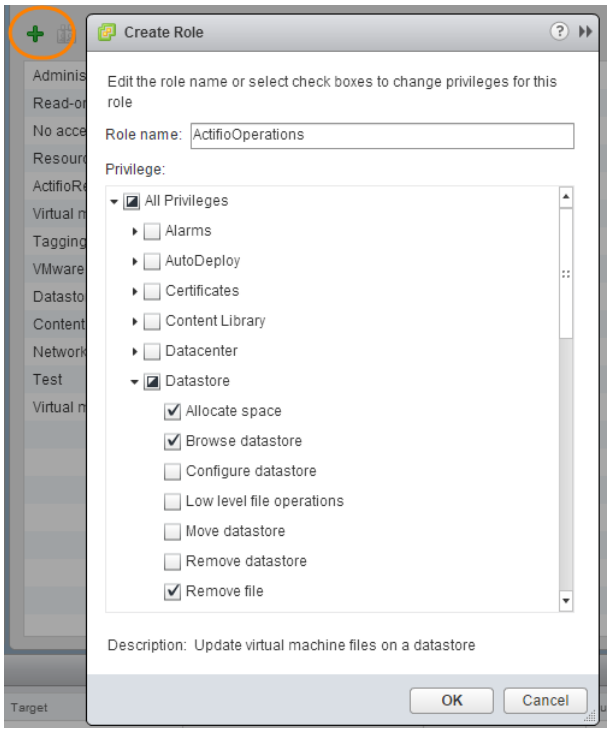


Note: *These examples show the vSphere client application running on a Windows host. Your screens will look a little different if you use the VMware web interface.*

Creating the ActifioOperations vCenter Role

After the ActifioReadOnly 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 **ActifioOperations**.
4. Check the checkboxes for each of the privileges listed in The vCenter Permissions List, vCenter 6.0 on page 34.
5. Click **OK** to save the role.



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

Assigning Minimum Permissions

To limit access of ActifioUser, assign the ActifioReadOnly role to ActifioUser at the vCenter level and the ActifioOperations 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 **ActifioReadOnly** 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 **ActifioOperations** 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).	vCenter
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 <Blue>Step 13 above.	Datacenter 1
	Datacenter 2
	ESXi Cluster 21
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 <Blue>Step 13 above.	ESXi Server 211
	VM2111
	VM2112
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 <Blue>Step 13 above.	ESXi Cluster 22
	ESXi Server 221
	ESXi Server 222
	VM2221
	VM2222