Getting Started with Actifio GO

Last updated on December 8, 2021

Actifio GO

Copyright, Trademarks, and other Legal Matter

Contents

Preface vii

The ActifioNOW Customer Portal vii

Actifio Support Centers vii

Chapter 1 - Introduction 1

Chapter 2 - Networks and Storage 3

Networks 3

Production Storage and Data 4

Protecting and Accessing Out-of-Band Data 4

Chapter 3 - Actifio Appliances and Storage Pools 7

Actifio Appliances 7

Storage Pools 8

Snapshot Pool for Instant Access to Images 8

Staging Disks 8

Understanding Snapshot Pool Consumption 9

VDisks 10

VDisk Consumption 10

OnVault Pool for Storing Images Long Term 11

Chapter 4 - Service Level Agreements (SLAs) 13

Policy Templates and Policies 13

Resource Profiles 14

Impact of Policy Settings on System Performance 14

Chapter 5 - Data Capture Overview 15

The Stages in Virtualizing an Application or a VM 15

Capture Mechanisms 16

Capture Options 17

Capture Applications 17

Capture Application Data in Actifio Consistency Groups 17

Capture a VM's Applications and Boot Volume 17

Capture Entire VMware VMs 18

Capture Generic Applications 18

Capture Database Logs 18

Capture System State 18

Chapter 6 - Capturing Applications 19

Discovering Applications and VMs 19

Policy Templates 20

Policies 20

Production to Snapshot Policies 20

OnVault Policies 20

Production to Mirror: StreamSnap Replication Policies 21

Resource Profiles 23

Scheduled Jobs 24

On-Demand Jobs 25

Maintaining Performance When Adding New Applications 26

Working with Preserved Snapshot Images 27

Viewing Preserved Images History 27

Viewing Discarded Images 27

Alerts and Warnings for Image Preservation in the Events Monitor 27

Chapter 7 - Data Replication 29

Sending Snapshots to One or More OnVault Pools 29

Production to Mirror Policy Replication 30

StreamSnap 30

Chapter 8 - Different Ways to Access Your Managed Data 31

Chapter 9 - Managed Data License (MDL) 33

How is MDL Measured? 33

Factors that Influence MDL Calculations 34

Frequently Asked Questions 34

Chapter 10 - Reporting & Monitoring Events 37

Reviewing Job Failures Displayed on the AGM Dashboard 37

Reviewing Errors and Warnings Displayed on the AGM Dashboard 38

Reviewing the Appliances Health Monitor in the AGM Dashboard 40

Reviewing Report Manager Reports 42

Reviewing SNMP Traps 45

Chapter 11 - Supporting Multitenancy using Actifio Organizations 47

Overview 47

Tenant logical resource isolation using organizations 48

Tenant resource access separation with role-based access control 48

Data storage tenant isolation 50
Isolating data traffic per tenant 50
Tenant specific reporting for chargeback 51
Writing multi-tenant cloud portals using Actifio Foresight APIs 52
Summary 52
Chapter 12 - Data Security 53
Secure Operating System Access to Actifio Appliances 53
Actifio VDP in a vSphere Environment 53
Internet Protocol (IP) Network Security 54
Access Control on Actifio Systems 55
Authentication and Authorization 56
Access Logging and Auditing 56
Actifio Secure Connectivity and Data Movement with iSCSI in the Public Cloud 56
Data Encryption 57
Command Line (CLI) Access to Actifio VDP 58
Vulnerabilities with Actifio VDP 58
The Actifio Connector 59
Chapter 13 - Support Resources 61
Actifio Product Documentation 61
Using the Actifio Knowledge Base to Review Event Information 62
Creating and Viewing Support Cases 64
Actifio Remote Support 66
Actifio Call Home Remote Event Notification 66
Actifio SecureConnect 67
Chapter 14 - Glossary 69

Preface

The information presented in this guide is intended for users who are new to managing and accessing data with an Actifio appliance. This document assumes that the Actifio appliance(s) have been installed and are ready to begin managing your data.

The AGM Online Help is comprehensive and easily searchable. You can reach it from the ? icon in the top right corner of AGM.

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 customer portal you can obtain detailed reports about your Actifio appliance as well as search the portal's 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

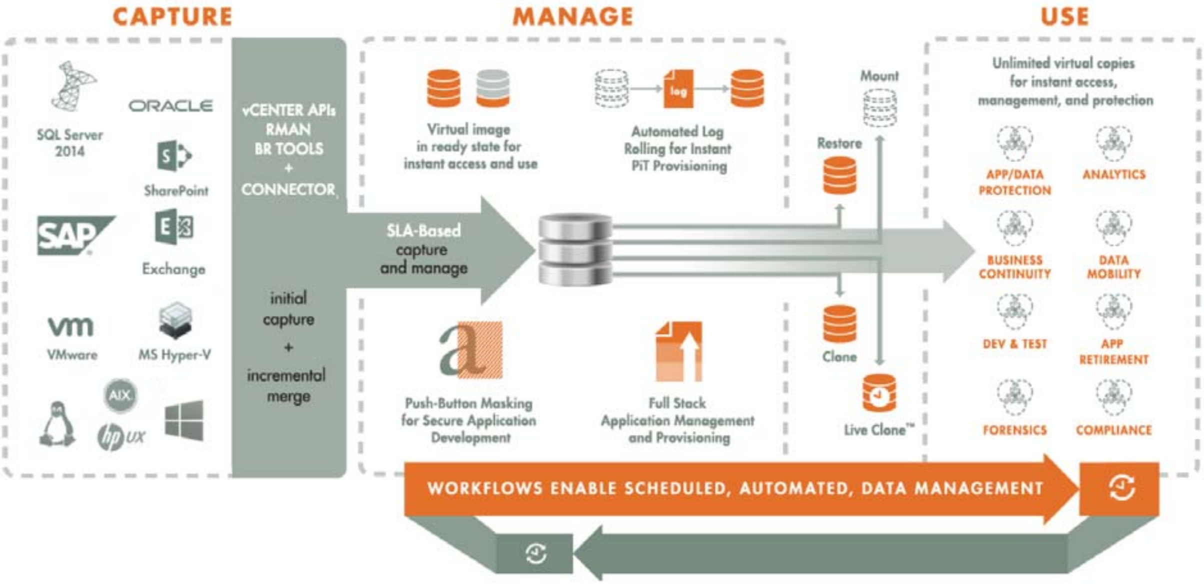
To contact an Actifio support representative, you can:

- 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

Actifio Virtual Data Pipeline (VDP) is a highly scalable copy data management platform that virtualizes application data to improve the resiliency, agility, and cloud mobility of your business. VDP virtualizes data in much the same way other technologies have virtualized servers and networks. Actifio VDP enables you to capture data from production systems, manage it in the most efficient way possible, and use virtual or physical copies of the data whenever and wherever they are needed.


CAPTURE
MANAGE
USE
SQL Server 2014
ORACLE
SharePoint
SAP
Exchange
vm
VMware
MS Hyper-V
AIX
hp UX
vCENTER APIs
RMAN
BR TOOLS
+
CONNECTOR
initial capture
+
incremental merge
SLA-Based capture and manage
log
Virtual image in ready state for instant access and use
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

The Actifio Virtual Data Pipeline (VDP)

In most cases, application data is captured at the block level, in native format, according to a specified SLA. A “golden copy” of that data is created, moved, 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 be accessed instantly for use, without proliferating physical copies and taking up additional storage infrastructure.

2 Networks and Storage

This chapter discusses connecting to and accessing your data. It includes:

Networks on page 3

Production Storage and Data on page 4

Networks

Actifio VDP supports networking over:

iSCSI: The Internet Small Computer System Interface works on top of the Transport Control Protocol (TCP) and allows the SCSI command to be sent end-to-end over local-area networks (LANs), wide-area networks (WANs) or the Internet.

Sky Appliances can support up to 100 iSCSI sessions.

NFS protocol: Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems allowing a user on a client computer to access files over a computer network much like local storage is accessed. Actifio supports NFS protocol in VMware and Linux environments.

Actifio supports NFS for capturing and presenting data in three deployment configurations:

- Using NFS to present a staging disk as a NFS share to a Linux host
- Presenting any backups to VMware hosts via a NFS datastore
- Presenting a staging disk for connector-based data capture within a VMware VM

In the first case, the staging disk is presented as a NFS file share directly to the production host.

In the other two cases, the mount disk/staging disk is presented as a VMDK to VMware virtual machine. Note that the data is not copied to the NFS datastore; a stub file is created that presents the underlying block disk from Sky Appliance to the VM as a VMDK via the NFS datastore.

External Snapshot Pools: You can exploit your production storage arrays' performance, connectivity, and availability by using the array native snapshots for Actifio's snapshot pool, providing:

- Better performance on mounted images. Activity on virtual clones does not go through the Sky Appliance but rather directly between the host and storage array. This is especially valuable in test/dev environments.
- Better performance and RTO for Disaster Recovery. When you use external snapshot pools on the DR side. Data is updated and available in its intended target storage so there is no need to copy it elsewhere.
- Better performance on backups (data moves directly from array to array, without going through the Sky Appliance).

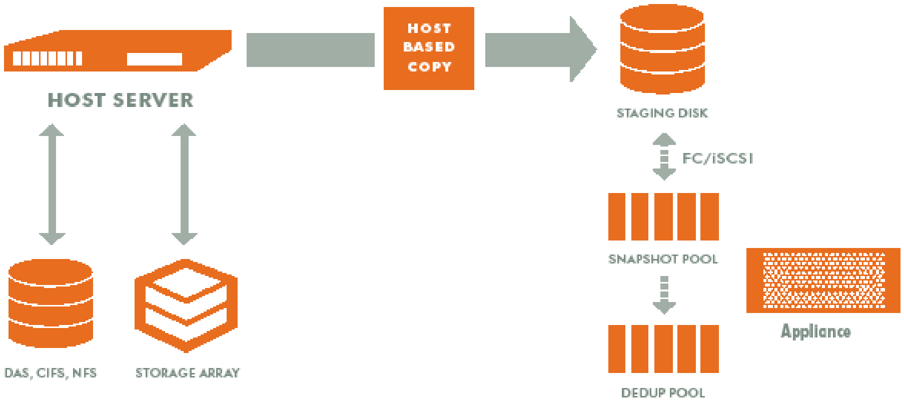
- o Incremental-only capture for applications that already reside on the array for near-instantaneous capture and reduced storage requirements (there is no need for a first full copy).
- o Highly available mounts from the storage array, coordinated by VDP.
- o FC host connectivity with Sky Appliance (Sky Appliance to array connection is iSCSI).

For full information on network matters, see ***A Network Administrator's Guide to Actifio VDP***.

Production Storage and Data

This is the method used when managing data. Production data is controlled by a non-Actifio storage controller on your existing storage arrays. The Actifio Appliance operates outside of the application's data path and uses the IP network. The Actifio Appliance moves and captures the application data separately from where the application writes its primary storage.

Actifio VDP captures copy data by presenting a staging disk that maintains a "golden copy" of the application data through time. Snapshots of application data are stored on the staging disk.



Typical Out-of-Band Capture Method

When capturing data Out-of-Band:

- A staging disk is mounted on a server via iSCSI or NFS.
- An initial capture of the entire image is made to the staging disk.
- Subsequent captures consist only of incremental changes. This is made possible by taking advantage of change block tracking via the Actifio Connector or by VMware APIs. See Capture Mechanisms on page 16 for details.
- The staging disk is unmounted on the server.
- A snapshot of the staging disk is made on the Actifio Appliance.

Protecting and Accessing Out-of-Band Data

When VDP is not in the data path, it protects copy data by presenting a staging disk to the host. This staging disk maintains a golden copy of the application data that is protected using VDP snapshots. On Windows, application-consistent backups are made via VSS. Oracle backups on all platforms are application consistent via RMAN interfaces. Whole VM backups are application-consistent if they are configured with vmtools.

Whenever possible, change block tracking is used to minimize backup data movement. Tracking is accomplished with VSS snapshots, Oracle RMAN, and the Actifio Connector.

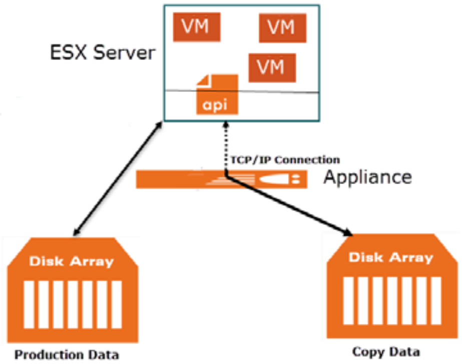
This section describes:

Protecting Entire VMware VMs Out-of-Band on page 5

Protecting Individual Applications on a VMware VM on page 5

Protecting Entire VMware VMs Out-of-Band

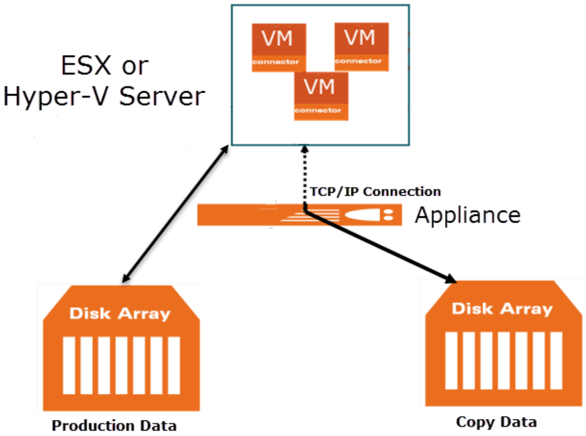
An Actifio Appliance can protect entire VMware VMs Out-of-Band. To protect entire VMware VMs, the Actifio Appliance takes advantage of VMware APIs.



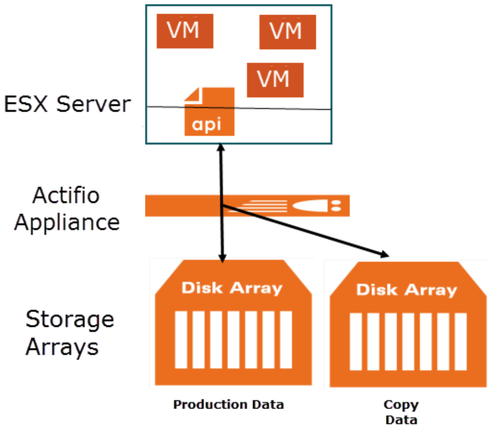
Protecting Entire VMs Out-of-Band

Protecting Individual Applications on a VMware VM

The Actifio Connector is used to protect individual applications on a VM. When the Actifio Connector is on a VM, you can create policies to protect individual applications and application groups on the VM.



Protecting Applications on a VM Out-of-Band



Protecting Entire VMware VMs

3 Actifio Appliances and Storage Pools

This chapter introduces how Actifio VDP captures, manages, and stores data.

Actifio Appliances on page 7
Storage Pools on page 8
VDisks on page 10

Actifio Appliances

Sky Appliance

A Sky Appliance is a virtual machine. A Sky Appliance captures and manages data locally and can replicate protected data to other Sky Appliances. A Sky Appliance resides in an ESXi environment, or it can be installed and operated from within Google Cloud.

Actifio GO

Actifio GO is a SaaS platform for VM, physical, and database backup and recovery to Google Cloud. Enterprises can use the ActifioGO SaaS platform to deliver cloud-based backup and recovery for cloud workloads.

Storage Pools

An Actifio Appliance uses pools of allocated storage to store data. The amount of space to be allocated is based on how data is managed, how much data is involved, the type of data, its change rate, how long it will be retained, and whether or not the data is replicated to another Actifio Appliance. For more information, review Production Storage and Data on page 4.

Snapshot Pool

The Snapshot Pool holds the most recent copies of your captured application data. Snapshot Pools retain protected data for short-term retention. Data is instantly accessible. Policies determine how long data is kept in this pool and when or if data is moved to another pool. The Snapshot Pool is also known as the Performance Pool.

Data that is replicated from a local Actifio Appliance to a remote Actifio Appliance via a Production to Mirror policy will land in the remote Actifio Appliance's Snapshot Pool. For more on the Snapshot Pool, see Snapshot Pool for Instant Access to Images on page 8.

OnVault Pool

An OnVault Pool defines the storage that can be used by a Snapshot to OnVault policy or a Direct to OnVault policy (VMware VMs only). Actifio OnVault Pools are used for long-term storage, not for primary data storage. For more on OnVault Pools, see OnVault Pool for Storing Images Long Term on page 11.

Primary Pool

The Primary Pool, act_pri_pool000, is for Actifio Appliance use. It is **not** a storage pool. Do not change the Primary pool or add a second pool unless instructed by Actifio Support.

Snapshot Pool for Instant Access to Images

The Snapshot pool (sometimes referred to as the Performance pool) holds "golden copies" of application data at the points in time specified by Service Level Agreement (SLA). The amount of data consumed is determined by whether an existing snapshot can be used.
This section includes:

Staging Disks on page 8

Understanding Snapshot Pool Consumption on page 9

VDisks on page 10

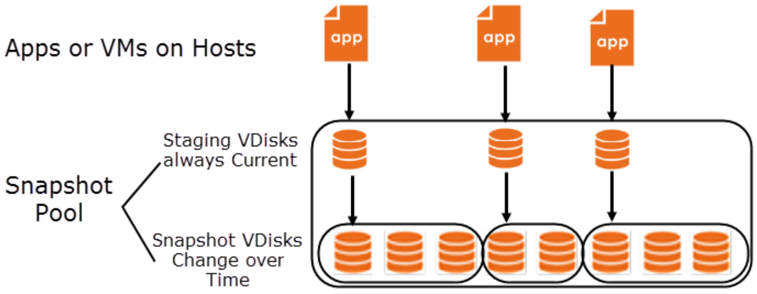
VDisk Consumption on page 10

OnVault Pool for Storing Images Long Term on page 11

Staging Disks

A staging disk is a VDisk created when an application is first protected. It is a copy of the production data as of the last backup invoked by the application's SLA. Each staging disk is associated with a number of snapshots on their own snapshot VDisks. The number of snapshots for each application or VM is determined by the SLA frequency of snapshot and retention period.

Because a staging disk is a complete copy of the production application or VM, each staging disk requires as much storage space in the Snapshot Pool as the protected application or VM requires in its production storage. Snapshots made from the staging disk reference the data in the staging disk, so they are much smaller. As subsequent backups change blocks in the staging disk, the original blocks are "pushed" into the snapshot VDisks, so the snapshot appears to have constant content but contains more and more blocks over time.


Apps or VMs on Hosts
app
app
app
Snapshot Pool
Staging VDisks always Current
Snapshot VDisks Change over Time

Virtualized Copy Data on Staging VDisks and Snapshot VDisks in the Snapshot Pool

Growth of Applications

If an application grows from 1TB to 2TB, a new 2TB staging disk is created. The original 1TB disk is preserved until all snapshots that depend on it are expired.

Note: *Windows staging disks up to 2 TB in size are MBR formatted. Those over 2TB are GPT formatted.*

Staging Disks for VMs and Out-of-Band Applications

When you protect a VM or an out-of-band application, copies of the selected image are put into a dedicated virtual staging disk in the Snapshot pool. VDP creates a snapshot from the image on the staging disk, and stores the snapshot in the snapshot pool for the time specified in the SLA.

Staging disks for out-of-band backups are allocated from the snapshot pool. The VDisk is thin-provisioned. Each snapshot created of that staging disk also consumes snapshot pool space, the amount depending on the application change rate.

An Exception for Direct-to-OnVault Protection for VMware VMs

VMware VMs protected direct-to-OnVault do not go through a staging disk because the Actifio Appliance can get changed-block information directly from the VMware layer. All other applications get changed-block information either via Oracle RMAN or the Actifio Connector (using an Actifio staging disk).

Understanding Snapshot Pool Consumption

The Snapshot Pool contains both the staging disks and the snapshot disks for every protected application or VM, plus any clones and mount images that you make.

The Snapshot Pool holds virtual disks, or VDisks. VDisks and VDisk consumption are explained in VDisks on page 10. Snapshot Pool space is consumed by four different kinds of VDisk:

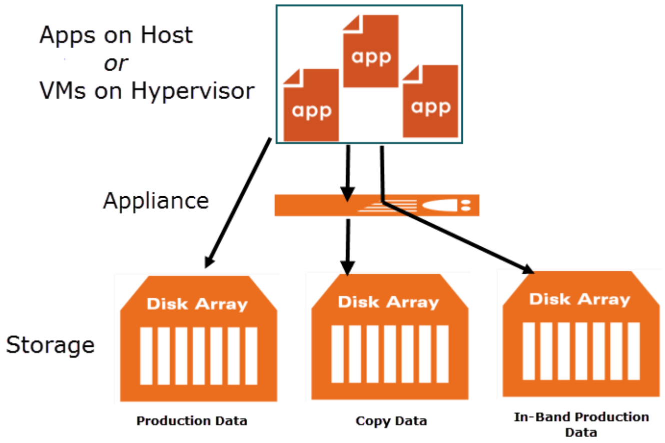
Staging VDisks: Staging VDisks, usually called staging disks, hold the VDP golden copy of the application. Staging disks are retained for as long as an application is protected and at least one snapshot exists. See Staging Disks on page 8.

Snapshot VDisks: These are used to preserve the state of staging disks at specific points in time. Snapshots are retained until their expiration time, but the last snapshot will never expire unless the application is unprotected or it is explicitly expired.

Mountable VDisk: Mountable VDisks are mountable images created at restore time from a snapshot on a snapshot disk.

Clone VDisks: Clone disks are full copies of an application’s production data. Clone disks are not automatically expired.

The storage space consumed in the Snapshot Pool is handled by a non-Actifio volume controller. Snapshots and changed-block tracking are handled by the Actifio Connector on physical hosts and through VMware APIs for VMware VMs. Out-of-Band storage uses your existing storage arrays.



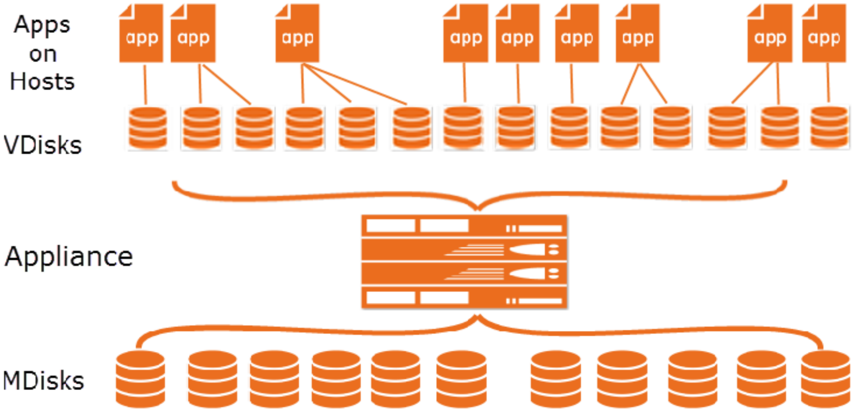
A Single Actifio Appliance Can Protect Data

VDisks

VDP uses logical VDisks (virtual disks or volumes) to virtualize data from hosts. VDisks are taken from a pool of managed disks (MDisks) presented to an Actifio Appliance from one or more internal and external arrays.

From the VDisks, the data can be cloned, mounted, and recovered, presented for test and development work, and manipulated in other tasks. VDisks are created as needed on physical disk arrays.

There is a fixed limit of VDisks per Actifio Appliance. As you create protection policies, your Actifio Appliance will warn you when a configuration may exceed VDisk limits. VDP employs VDisks in slightly different ways, but the information in this section applies to all types of Actifio Appliances.



Virtualized Applications on Managed Disks in Your Storage

VDisk Consumption

How Many VDisks Do I Have?

The VDisk limit for the Sky Appliance the VDisk limit varies with the installed capacity license (1000, 3000, or 5000 VDisks). If you have enough VDisks for your needs, but they are growing too large for your existing storage, then you must add storage. If you need more VDisks, then you need another Actifio Appliance.

How Many VDisks Do I Need?

In general, each protected application or VM requires one or more VDisks for the staging disk plus the same number more VDisks per snapshot. In addition, note these rules:

- VM-level backups with a snapshot SLA consume one VDisk for each virtual disk in the VM.

- File system backups in a Windows environment consume one VDisk for each protected file system.
- File system backups in a Unix environment consume a VDisk for every 833GB protected times 1+(number of retained snapshots). You can adjust the 833GB value by changing Staging Disk Granularity in Details & Settings, see the AGM Online Help.
- Mounts, LiveClones, and Clones of non-VM applications consume VDisks.
- On Linux systems, filesystems and Oracle databases consume one VDisk plus another for every additional 2TB data is being protected.
- SQL Server databases consume one VDisk for every volume that hosts the database.
- Each snapshot of a VDisk consumes one VDisk per snapshot per protected disk.
- Snapshots show peak usage, as new snapshots are created before old snapshots are expired.
- After failover and syncback, the failback operation cleans out all the syncback and failover VDisks.

VDisks are thin-provisioned, and can grow over time.

OnVault Pool for Storing Images Long Term

Actifio OnVault Pool storage is typically used for long-term retention of copy data. When sending data to a storage defined by an Actifio OnVault Pool, an HTTPS connection is used to ensure data security over the network. The OnVault Pool's compression option is on by default to minimize network traffic.

OnVault Pools can be created in Google Nearline, Coldline and Archive Class Storage. For full information on creating OnVault Pools, see the AGM online help or to ***Configuring Actifio OnVault***.

After the initial ingest of the full snapshot, only the changes to data are sent to the OnVault Pool. This is the same incremental forever model used by other Actifio policies.

When accessing data in an Actifio OnVault Pool's storage:

- All Actifio Appliances can create clones.
- All Actifio Appliances can mount data, but because data will first be copied to the snapshot pool then mounted, it is not recommended.
- LiveClones cannot be created.

4 Service Level Agreements (SLAs)

This chapter introduces the concepts of how Actifio VDP captures, manages, and accesses data. Understanding these concepts will help you to be successful with Actifio copy data management.

Policy Templates and Policies on page 13

Resource Profiles on page 14

Policy Templates and Policies

A Policy Template is a collection of policies. A policy defines:

- The source of the data managed by the policy
- Type of the protection operation
- Frequency of the protection operation
- How long to retain the data
- Whether data is replicated

Multiple policies within a template allow you to create a single template that defines short term and long term retention of data as well as whether data is replicated and how long replicated data is retained. Depending on Actifio Appliance type, Policy Templates can be made up of one or more of these policies:

Production to Snapshot defines when and how often production data will be captured and how many snapshots are retained. Snapshots are meant for short term retention. See Production to Snapshot Policies on page 20 for details.

Production to Mirror defines how data will be replicated to a Mirror Pool (a Snapshot Pool on a remote Actifio Appliance). Data in the Mirror Pool is meant for instant recovery in a disaster recovery scenario. For details on replicating data, see Chapter 7, Data Replication.

Production Direct-to-OnVault defines when to back up VMware VMs directly from production data and how long to retain the OnVault data. Capturing VMware VMs directly to a OnVault Pool is meant for long term retention.

Snapshot to OnVault defines when to send Production to Snapshot data to the storage defined by an Actifio OnVault Pool and how long to retain the data. Snapshot to OnVault Policies are meant for long-term retention of data. See OnVault Policies on page 20 for details.

Policy Templates are:

- Created in the SLA Architect
- Applied to applications in the App Manager

Resource Profiles

Resource profiles define where application data is retained. They define which pool to use: Snapshot or OnVault. Pools specified in Resource profiles are used along with policy templates to form an SLA for an application. Resource Profiles are:

- Created in the SLA Architect
- Applied to applications in the App Manager

This section outlines how to develop a policy template that takes into consideration how the frequency and retention settings for the various police templates can result in excessive system resource usage that impacts Actifio appliance performance.

Note: *The SLA Architect enforces a policy development sequence when you define the policies associated with a policy template. Certain policies will be unavailable based on the type of policy template you develop and the type of Actifio appliance involved.*
In addition, the types and number of policy templates and the minimum and maximum settings of policies are specific to the Actifio appliance on which they reside. Your policy templates can look slightly different from those in the following examples.

Impact of Policy Settings on System Performance

SLAs are the rules that you create for the Actifio appliance to determine what type of protection to apply to your data, when to apply it, and where to store it. Each template policy defines how your applications and VMs are managed by the Actifio appliance. SLA operations have the potential of impacting the performance of the Actifio appliance by running out of critical resources as a result of a template policy.

A few examples of the impact of policy settings can include:

- You create a new policy that results in the creation of a number of snapshot copies per volume that exceeds the threshold (a limit of 14 snapshot copies by default).
- You modify an existing policy with very frequent snapshots, which consumes an excessive number of VDisks and can impact system performance.
- You create a policy with long retention of snapshots, which consumes an excessive number of VDisks and a large Performance pool and can impact system performance

Critical resources configured as part of an SLA policy template include:

- VDisk usage statistics (total number, number used, and percent remaining)
- Performance pool usage statistics (total TB, TB used, and percent remaining)

Note: *The calculation of VDisk usage and performance pool usage is directly related to the number of snapshot copies during steady state. The number of snapshot copies during steady state is related to the Recovery Point Objective (RPO) and retention. For example, an RPO of 8 hours and a retention of 3 days means that there will be a total of 9 snapshot copies.*

5 Data Capture Overview

This includes:

The Stages in Virtualizing an Application or a VM on page 15

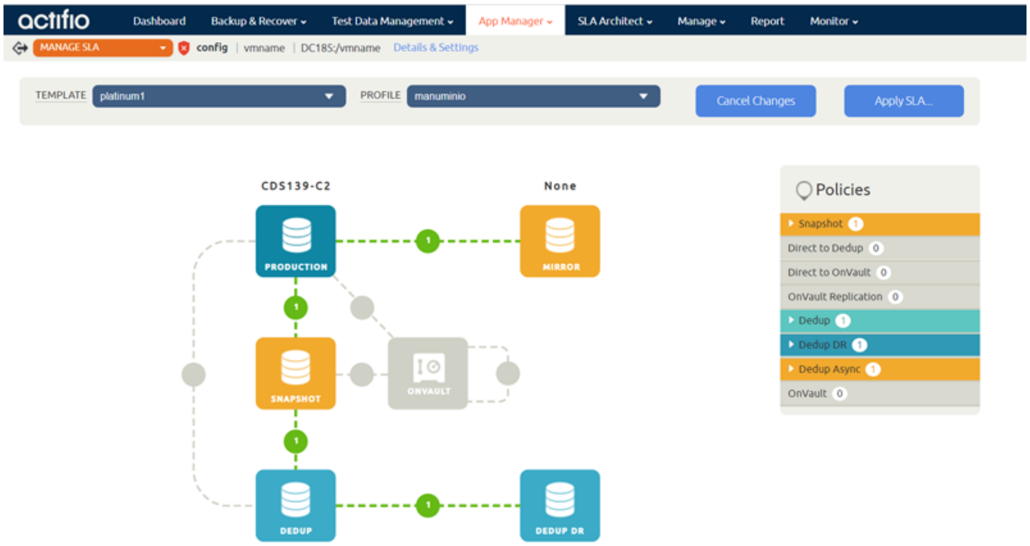
Capture Mechanisms on page 16

Capture Options on page 17

The Stages in Virtualizing an Application or a VM

When you first virtualize an application or a VM, you assign an SLA to run on a schedule. Then:

1. The application or VM is running on production storage.
2. According to the SLA settings, Actifio VDP takes a snapshot image of the production application and saves it in the Actifio Appliance Snapshot Pool.
3. Either immediately or at a later time according to the SLA, VDP copies the image from the Snapshot Pool or to a pool at a Mirror Location or to an OnVault pool.



TEMPLATE platinum1

PROFILE manuminio

Protecting an Application

When Application Protection Takes Effect

Applying an SLA does not immediately protect an application. Protection jobs run on a schedule, according to resource availability. You can also run the job immediately.

- The SLA includes a schedule of when to run the protection job for this application, such as daily between 6 PM and 6 AM, every four hours. If you apply protection to an application at 1 PM today, then the first protection operation will be scheduled for 6 PM today.
- At the scheduled time, the job is assigned a **job slot**, which may be available when the job is scheduled, but not always. Job slots are detailed in About Job Slots on page 25.

Changing Protection

You can change an application's protection at any time. Future backups will occur based on the new template. Existing backups will be retained according to the template in use when they were created.

The Change Tracking Driver

The Actifio Connector with its change tracking driver (sometimes called the filter driver) enables efficient incremental backups by tracking changes from the host side. After the first complete backup of a database, the Actifio Appliance performs incremental backups by default. If your backups are still always full backups, then check for:

- The change tracking driver is stopped. In this case, restart the change tracking driver service.
- The change tracking driver is incorrectly configured or not installed. In this case, uninstall and then make a full install of the Actifio Connector.

Capture Mechanisms

An Actifio Appliance captures data by making an initial full copy of the data, then making copies of incremental changes. This capability requires the ability to track and capture the changes that occur between capture operations. To track those changes the Actifio Appliance uses either The Actifio Connector or VMware API Calls.

The Actifio Connector

The Actifio Connector is used to capture selected applications and for capturing entire Hyper-V VMs. The Actifio Connector is a small-footprint, operating system specific, lightweight service that can be installed on either virtual or physical servers. The Actifio Connector provides a more granular data capture capability than what is provided by VMware API calls. It allows you to:

- Discover applications
- Quiesce applications, for application consistency during capture
- Enables change block tracking for VDP's incremental forever capture strategy
- A single policy template can be applied to multiple applications are resident on a server.
- Avoids VMware VMs "stun" issues

The Actifio Connector also enables host-side scripting for:

- On-demand jobs triggered from the Actifio CLI with the -scripts argument.
- Pre- and post- phases of a Workflow job.

Scripting is detailed in ***Network Administrator's Guide to Actifio VDP***.

VMware API Calls

Actifio VDP uses VMware APIs for data protection (VADP) calls to capture an entire virtual server. These enable change block tracking for Actifio's incremental forever capture strategy and 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. This guarantees that the data can be accessed fast and without issues. Because the image presented is a fully functional virtual server, it can be started and run from an Actifio Appliance directly and then optionally migrated to a new, permanent location on production storage.

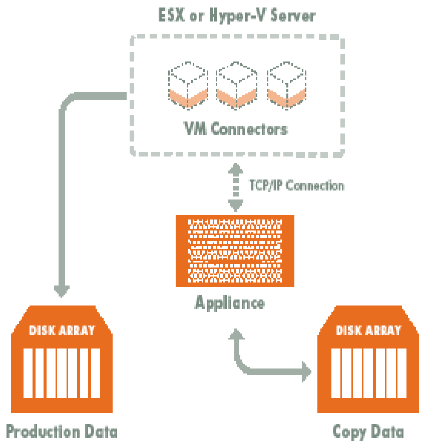
Capture Options

Actifio VDP allows you to:

- Capture Applications on page 17
- Capture Application Data in Actifio Consistency Groups on page 17
- Capture a VM's Applications and Boot Volume on page 17
- Capture Entire VMware VMs on page 18
- Capture Generic Applications on page 18
- Capture Database Logs on page 18
- Capture System State on page 18

Capture Applications

The Actifio Connector is used to capture individual applications and groups of applications on physical and virtual servers.



Managing Individual or Groups of Applications

Installing the Actifio Connector on a physical server or VM allows you to create a single Policy Template to capture all applications on the server or several Policy Templates to capture groups of applications.

Capture Application Data 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 Template.

If Actifio's Database Log Backup option is enabled in a Snapshot policy, then all databases captured by the Policy Template in which the Snapshot policy resides 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 AGM with a single action.

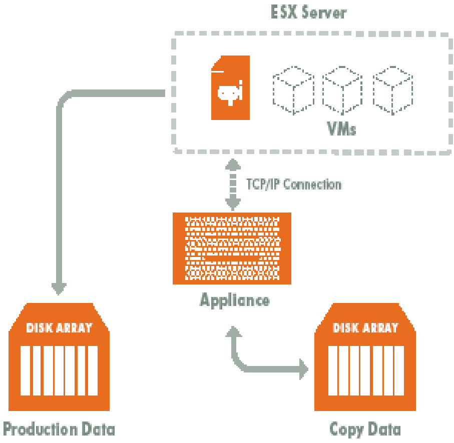
In addition to making capture and recovery operations easy and fast, consistency groups consume fewer system resources (VDisks).

Capture a VM's Applications and Boot Volume

When managing applications 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 applications, an image can be presented that is a fully functional VM. The image can then be migrated to a new, permanent location if needed.

Capture Entire VMware VMs

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



Managing Entire VMs

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, it can be migrated to a new, permanent location if needed. Capturing whole virtual servers allows groups of virtual servers and their applications to be protected with a single Policy Template.

Capture Generic Applications

Most applications are discovered through the Actifio Connector or through various APIs built into Actifio VDP. A generic application is an application that you define it by pointing to a group of volumes to be protected. AGM can protect LVM-based generic applications.

Capture Database Logs

Database log capture is enabled in a Snapshot policy's Advanced Options. It enables a single Snapshot policy to capture logs for Microsoft SQL Server databases, Oracle databases, and consistency groups that contain Microsoft SQL Server databases or Oracle databases. The frequency at which database logs are captured is defined separately from that of the database. For example, a database can be captured every day and its logs captured every hour.

The frequency of database log backup is set in minutes, and the frequency at which logs are captured must not exceed the frequency at which its associated database is captured. For example, if a database capture frequency is every 24 hours, the log file capture frequency must be less than every 24 hours.

Log retention is defined separately from the retention of the Snapshot policy. Having a separate retention period allows you to use logs in conjunction with copies of the database stored in the Snapshot pool.

Regardless of how many logs are captured during a specified log retention period, a database's captured logs are staged to a single VDisk in the Actifio Snapshot pool. To conserve space in the Snapshot pool, you can use an advanced setting to instruct the database to compress its logs.

Capture System State

Actifio by default will capture the system state when capturing data from Windows/Linux cloud-based virtual machines. For full details, see ***Actifio Cloud Mobility***.

6 Capturing Applications

This chapter presents high-level descriptions of the processes used to capture an application:

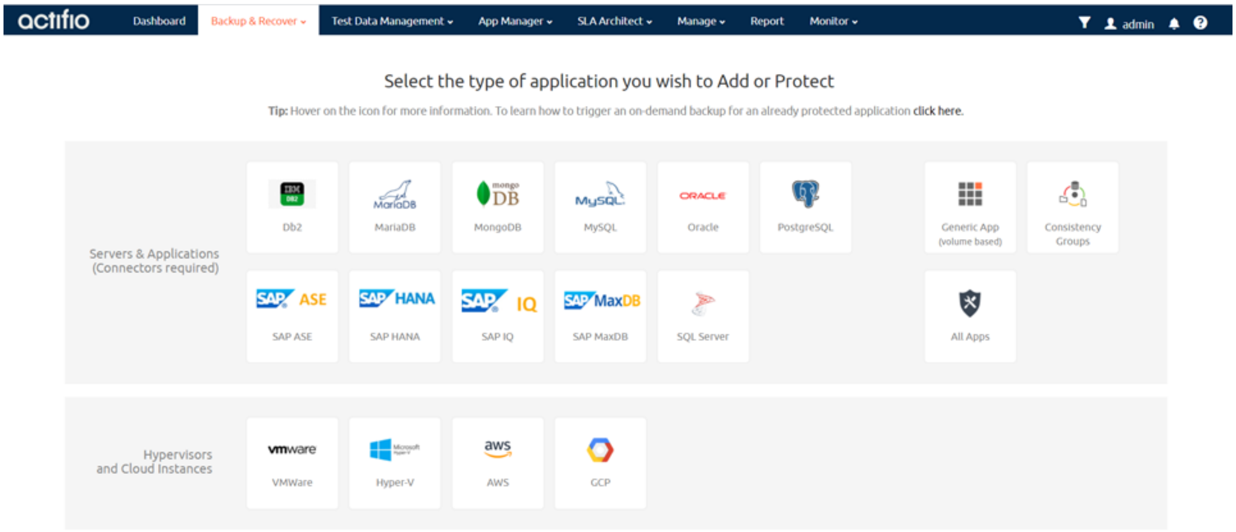
Discovering Applications and VMs on page 19
Policy Templates on page 20
Policies on page 20
Resource Profiles on page 23
Scheduled Jobs on page 24
On-Demand Jobs on page 25
Maintaining Performance When Adding New Applications on page 26
Working with Preserved Snapshot Images on page 27

Before You Begin

Add hosts that host applications using the Protection Wizard, introduced in Discovering Applications and VMs on page 19. For detailed, application-specific instructions see the ***Network Administrator's Guide to Actifio VDP*** in the ActifioNOW portal. Detailed, application-specific instructions on capturing applications and VMs are in the AGM online help.

Discovering Applications and VMs

Use the AGM Backup or Capture wizards to discover applications on physical servers, VMs on hypervisors, and applications on VMs. You will be prompted to select which of the discovered hosts or hypervisors you want to discover applications or VMs.



Select the type of application you wish to Add or Protect

Tip: Hover on the icon for more information. To learn how to trigger an on-demand backup for an already protected application **click here**.

Policy Templates

Policy templates are made up of one or more policies. Policy templates provide a high-level wrapper for an end-to-end definition of capturing application data. For example, if you need to capture an image as a local snapshot and replicate that image off to another Actifio Appliance, the policy template will contain both the local snapshot and remote off site policies. Once the policy template is created, create the individual policies that comprise the SLA template.

Policies

Policies define how often to capture an application, how long to retain the captured application and when applicable, where and how to replicate the captured application's data.

The green arrows in the SLA Architect represent the policies within a template that control data flow to the various pools.

A Policy allows you define whether its schedule will run:

- **Within a Window**: A period of time in which jobs are allowed to start.
- **Continuous**: Defines when its first job can start but as the name implies, allows subsequent jobs to run at a frequency without regard to any time boundary.

Where applicable, SLA Template Policies allow you to define the rules for determining whether or not a data protected by a policy meets your requirements. VDP automatically calculates and sets default SLA Compliance settings. Default settings are based on whether the policy is set to windowed or continuous, the policy type, and Actifio-recommended best practices. The default settings calculated will meet the needs of most users.

The SLA Templates are made up of the following types of policies:

Production to Snapshot Policies on page 20
OnVault Policies on page 20
Production to Mirror: StreamSnap Replication Policies on page 21

Production to Snapshot Policies

You can schedule a Snapshot policy schedule that occurs during a specific frequency and time window or on a continuous basis. The minimum recommended frequency for a Snapshot policy is 1 hour (local RPO).

Note: *When creating a snapshot policy for a database you have the option of also capturing its log files at a specified frequency.*

OnVault Policies

OnVault policies allow you to send data to cloud object storage (an Actifio OnVault Pool). A schedule within the policy is used to send the most recent data to object storage. After the initial ingest of data, an OnVault capture operation follows VDP's incremental forever data capture process.

When sending data to storage defined by the OnVault Pool, an HTTPS connection is used to ensure data security over the network. The OnVault Pool's compression option is on by default to minimize network traffic.

When accessing data in an OnVault Pool's defined storage location:

- All Actifio Appliances can create clones.
- All Actifio Appliances can mount data, but because data will first be copied to the snapshot pool then mounted, it is not recommended.
- LiveClones cannot be created.

You can create two types of OnVault policies:

- Snapshot To OnVault Policies allow you to capture data in a Snapshot Pool on any Actifio Appliance and then protect the data in the snapshot pool to object storage defined by an OnVault Pool.
- Direct To OnVault Policies allow you to capture VMs in their production environment and protect them directly to object storage defined by an OnVault Pool.

Snapshot To OnVault Policies

To create a Snapshot to OnVault policy schedule that will, once a day, within a defined window, send the most recent snapshot data to object storage defined by an OnVault Pool, set:

- Vault on these days: Everyday
- The window to open and close as needed. Typically set to 19:00 to 18:50
- The desired retention time (for example, retain for 3 years)

Direct To OnVault Policies

To create a Direct to OnVault policy schedule that will, once a day, within a defined window, send the most recent incremental updates directly to storage defined by an OnVault Pool, set:

- On these days: Everyday
- The window to open and close as needed. Typically set to 19:00 to 18:50
- The desired retention time (for example, retain for 3 years)

OnVault to Multiple Targets

Application data can be sent to multiple OnVault targets in the cloud. Each OnVault target is controlled by separate policies so frequency of update and retentions can be different (e.g., frequent local updates with short retention, together with less frequent updates to cloud with long-term retention).

Multi-target OnVault is supported with all application types, including Direct-to-OnVault with VMware VMs. In this case, the data is written directly to the first OnVault pool, bypassing the snapshot pool, and then read from the first OnVault pool and sent to the others.

This provides flexibility for multiple use cases. For example, you can protect data locally, and keep it for long retention remotely in one project, and send the same data to a different project for TDM purposes.

Production to Mirror: StreamSnap Replication Policies

Production to Mirror policies that use StreamSnap replication are tied to a specific snapshot policy. They use the schedule and frequency settings of the associated snapshot policy in the template.

Note: *Before creating a StreamSnap replication policy, you must first create a snapshot policy.*

StreamSnap replicates data snapshots to a remote Actifio Appliance over a high quality network, which can provide RPOs as low as one hour.

- For VMware VMs, snapshot replication is streamed to the second Actifio Appliance in parallel to the snapshot being copied. Streaming of a VMware VM is performed to avoid waiting until the local snapshot job completes before initiating replication.
- For non-VMware VM applications, snapshot replication occurs after the local snapshot job is completed.

Note: *StreamSnap replication and local snapshots are integrated to avoid the creation of double snapshots. Each Actifio Appliance allows you to maintain multiple local snapshots.*

StreamSnap Replication

- Achieves Recovery Point Objectives (RPOs) as short as one hour. The StreamSnap replication policy relies on the associated Production to Snapshot policy for RPO and the other advanced snapshot settings. A StreamSnap policy can point to any Snapshot policy with frequency of 1 hour or longer (remote RPO).
- Uses an existing IP network to replicate data.
- Replicates large amounts of data to remote users (for example, test and development environments).
- Retains multiple point-in-time snapshot images at the remote site, with retention behavior being driven by the settings in the StreamSnap policy.
- Makes fail-over to a host on the remote site simple.
- Enables incremental reverse replication (syncback) to the local Actifio Appliance.
- Compresses and encrypts replicated data to the second Actifio Appliance. You can disable compression if the data is already compressed (for example, for images and videos).

Note: *StreamSnap jobs run for non-DB, DB, and DB+Log types. To perform on-demand log replication of the database logs to a remote Actifio Appliance, select the database in App Manager, then select Replicate Logs.*

When you apply the SLA template to an application or VM in the App Manager, the Monitor will record the results of the StreamSnap job and it will appear as a single job. Once replication is complete, two jobs appear in the Monitor with a Succeeded status; one for the Snapshot job and one for the StreamSnap job (see StreamSnap Job Error Handling). If there is a job failure, either for the StreamSnap job or the Snapshot job, two job entries appear to identify which job was successful.

Resource Profiles

A resource profile specifies the storage media for captured application and VM data. The policy and the resource profile that make up the SLA dictate the type of application data capture to perform and where to store the captured application data (which pool of disks can be used). Resource Profiles define which Snapshot Pool (if needed) will be used and/or to which remote Actifio Appliance data will be replicated.

In addition to policy templates and policies, you also create resource profiles in the SLA Architect. Resource profiles define where to store data. Data can be stored:

- Local: The Actifio Appliance that the resource profile is created for.
- Remote: The Actifio Appliance used for replication. This remote appliance must be an appliance that is already paired to the selected local Actifio Appliance.

Note: *You can configure the Remote field only when one or more remote Actifio Appliances are configured on the selected local Actifio Appliance.*

- OnVault: Object storage defined by an Actifio OnVault storage pool.

Note: *You can use the OnVault Pool option only if the Actifio Appliance has a defined OnVault storage pool.*

Resource profiles are applied to applications in the App Manager and the resource profiles work in tandem with policy templates:

- A policy template that does not include a replication policy must be applied to an application along with a resource profile that only stores data locally.
- A policy template that includes a replication policy must be applied to an application along with a resource profile that stores data either on another Actifio Appliance or to object storage defined by an Actifio OnVault storage pool.

You define a resource profile for any Actifio Appliance that has been added to AGM.

Scheduled Jobs

Jobs run according to the schedule assigned in their SLA Template Policies. If you try to run many resource-intensive jobs simultaneously, then some will have to wait for the resources to come available. In a very bad situation, they may have to wait so long that an SLA Violation occurs.

It is better to stagger resource-intensive jobs like initial snapshot jobs over time rather than to have them all compete for resources at the same moment. For example, instead of snapping all VMs, file systems, and databases at 6:00pm on weekdays, consider snapping one type of application on the hour, another type at 10 minutes after the hour, another type at 20 minutes after the hour, and so on.

The initial snapshot of an application or a VM is the largest and most time-consuming snapshot it will ever get because every bit of data is new. When you add a new application or VM, perform an on-demand snapshot at an off-peak time for the first snapshot and then schedule an SLA Template Policy for all future snaps.

On-Demand Jobs

The great majority of jobs run on schedule according to their SLAs, but for upcoming maintenance windows, software upgrades, and for the first snapshot of a new application, you want to ensure that you have a successful copy of the data created before you start your scheduled maintenance task. These cases call for an on-demand job.

About Job Slots

VDP manages jobs by assigning *job slots*. The Actifio Appliance reserves a pool of slots for each category of jobs, plus an pool of unreserved slots.

Before starting a job, VDP checks whether a slot corresponding to the job's category is available to run the job. When a reserved slot is not available because all the slots of that category are running jobs, the Actifio Appliance checks whether an unreserved slot is available. If an unreserved slot is available, the job is started.

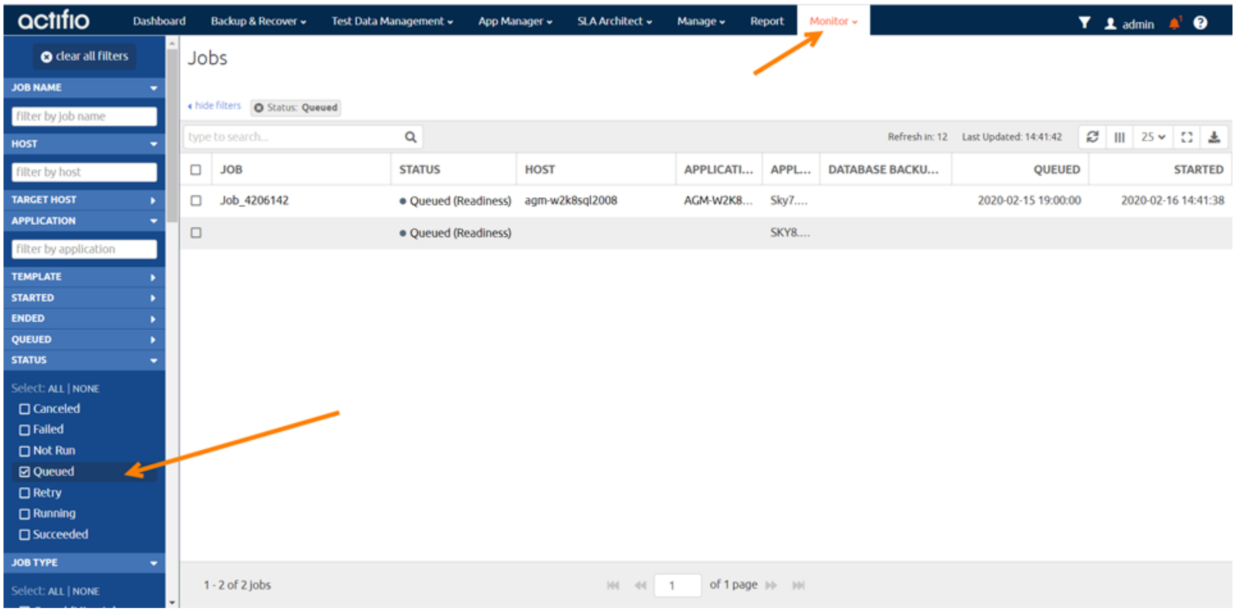
Queuing of On-Demand Backup Jobs

VDP supports queuing of on-demand jobs to provide you with the flexibility to create your images without concern for the number of on-demand job slots available to start the job. The queued on-demand job remains in the queued state until an on-demand job slot is available.

When an on-demand slot opens, the job progresses to the running state. This sequence occurs in the order that the job was submitted. If an on-demand job fails, the Actifio Appliance will attempt to run the next job in the queue. On-demand jobs use different job slots than scheduled jobs, so scheduled jobs may run before queued jobs.

While an on-demand job is in a queued state you can cancel the job or cancel protection for the application. The on-demand job will then appear in the job history table as a canceled job. The start time of the job and the end time of the job will be the time that the cancel request or the cancellation of application protection was acknowledged.

You can view the queued jobs from **Monitor > Jobs**.



☐	JOB	STATUS	HOST	APPLICATI...	APPL...	DATABASE BACKU...	QUEUED	STARTED
☐	Job_4206142	● Queued (Readiness)	agm-w2k8sql2008	AGM-W2K8...	Sky7....		2020-02-15 19:00:00	2020-02-16 14:41:38
☐		● Queued (Readiness)			SKY8....			

Queued Job List in the Jobs Monitor

Maintaining Performance When Adding New Applications

If your system has been performing acceptably and then you add new applications, performance may suffer for a short time. This is because VDP change block tracking recognizes new data and protects it even when it is only a small part of a large application. This means the system is optimized to process many changed blocks every day.

A new application requires a lot more resources for the initial capture, because it is all new data to the Actifio system.

For best results when adding new applications:

- When you add a new application, protect it for the first time using an on-demand job during a period of light load. This will prevent the resource-intensive initial ingest job from interfering with other jobs.
- When adding multiple new applications or VMs, try to stagger the initial protection jobs for each new application over time, to prevent all of the new data from being ingested simultaneously. Do this by assigning SLAs that run at different times. You can also use the on-ramp job slots feature to minimize disruption.
- Separate the initial protection job in time from the Mirror job. Once an application snapshot has been taken, the Mirror job can run some hours later when the system load is lighter.
- When you need to add additional applications, check your MDL. If your managed data is close to or over your licensed capacity, contact your Actifio representative to ensure continued high performance.
- Consistency Groups can be an efficient way to protect multiple applications with similar needs; see Capture Application Data in Actifio Consistency Groups on page 17
- Be aware of your existing SLAs and try not to schedule snapshot jobs simultaneously with the snapshot jobs for very large or dynamic applications.

Working with Preserved Snapshot Images

You can choose from the list of preserved snapshot images from the Manage tab, and:

- Select from the list of preserved images and navigate to that image in the App Manager.
- Expire one or more selected snapshot images.

Note: *When expiring snapshots, the amount of space reclaimed may be less than the amount of space consumed by that snapshot. This is due to the common block reference between snapshots. To ensure maximum space reclamation, expire the oldest snapshot first.*

This section includes the following topics:

- Viewing Preserved Images History on page 27
- Viewing Discarded Images on page 27
- Alerts and Warnings for Image Preservation in the Events Monitor on page 27

For details on how to modify or disable the application priority settings for preserved snapshots jobs, see the AGM online help.

Viewing Preserved Images History

You can view a graph that shows how many images were in a preserved state on each day over a selected time period (which can be an interval of either Last Week or Last Month). Data is logged in the Preserved Images History graph on an hourly basis.

Viewing Discarded Images

Preserved images will automatically be expired and discarded when pool space or VDisk count reaches the warning threshold levels. In this case, images are expired based on application priority and age. Images for applications with lower priority will be expired ahead of applications with higher priority. Within a priority level, older images will be expired before newer images.

From the Discarded Images window, you can see a summary of images that have been expired over the past day, week (7-day interval), or month (30-day interval) along with the reason for discarding the image. This window also includes images that have been manually expired prior to processing.

Note: *See AGM Online Help for additional details about the AGM Dashboard and the System Health widget.*

Alerts and Warnings for Image Preservation in the Events Monitor

This section outlines the various alerts and warnings related to image preservation.

Warning Level Alert: First Time the Snapshot Expiration Window is Reached

A Warning level alert is generated (and posted to the event log) the first time a snapshot that is eligible for expiration is held for pending processing.

This Warning level alert is generated for the first snapshot for each application that has its expiration deferred. When the count of deferred expirations for an application goes to zero, the Warning alert trigger is reset.

Warning Level Alert: Snapshot Image Expired Because Threshold Limit Exceeded

When an application has preserved snapshots to be sent to an OnVault pool, and a snapshot is expired because the Actifio Appliance has exceeded the threshold limits (such as VDisk count or pool capacity), a Warning level alert indicating this condition is posted. This warning will be logged only for the first snapshot expired due to this situation.

Below is a summary of the Warning thresholds for VDisk and storage pools:

- The Warning threshold for VDisks usage is 90%. The VDisk limit for the Sky Appliance varies with the installed capacity license (1000, 3000, or 5000 VDisks).
- The Warning level is 80% for the snapshot pool. The default value is 90% for the snapshot and primary pools.

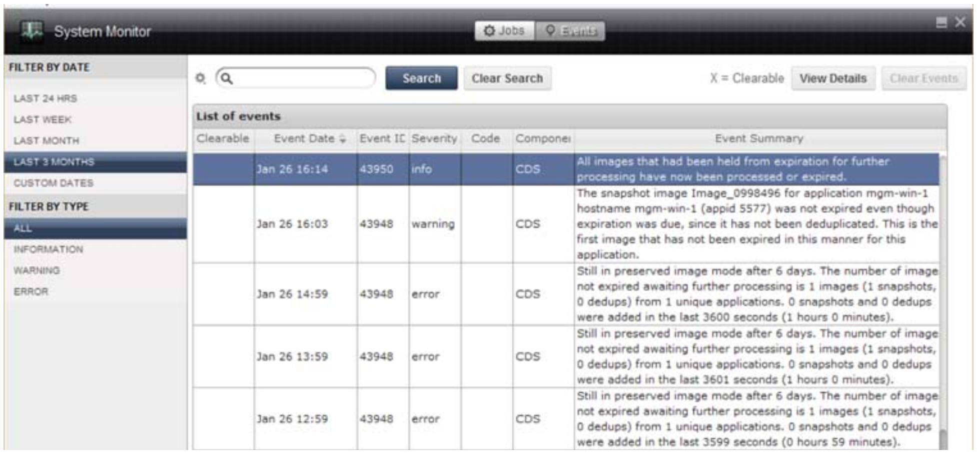
Daily Warning Level Event: Deferred Expirations Because Threshold Limit Exceeded

A daily warning level event is posted when a number of images that had deferred expirations were expired because the Actifio Appliance has exceeded the threshold limits (such as VDisk count or pool capacity). The message includes a count of images expired in this fashion. An example of such an event is shown below:

```
The number of images awaiting further processing that had to be discarded is 5 images (3
snapshots) from 3 unique applications in the last period of 24 hours.
```

Warning Level Alert: All Preserved Images Have Been Processed

When the number of preserved images drops to zero, this alert is posted in the appliance's System Monitor:



List of events

Clearable	Event Date	Event IC	Severity	Code	Componei	Event Summary
	Jan 26 16:14	43950	info		CDS	All images that had been held from expiration for further processing have now been processed or expired.
	Jan 26 16:03	43948	warning		CDS	The snapshot image Image_0998496 for application mgm-win-1 hostname mgm-win-1 (appid 5577) was not expired even though expiration was due, since it has not been deduplicated. This is the first image that has not been expired in this manner for this application.
	Jan 26 14:59	43948	error		CDS	Still in preserved image mode after 6 days. The number of image not expired awaiting further processing is 1 images (1 snapshots, 0 dedups) from 1 unique applications. 0 snapshots and 0 dedups were added in the last 3600 seconds (1 hours 0 minutes).
	Jan 26 13:59	43948	error		CDS	Still in preserved image mode after 6 days. The number of image not expired awaiting further processing is 1 images (1 snapshots, 0 dedups) from 1 unique applications. 0 snapshots and 0 dedups were added in the last 3601 seconds (1 hours 0 minutes).
	Jan 26 12:59	43948	error		CDS	Still in preserved image mode after 6 days. The number of image not expired awaiting further processing is 1 images (1 snapshots, 0 dedups) from 1 unique applications. 0 snapshots and 0 dedups were added in the last 3599 seconds (0 hours 59 minutes).

Event Monitor with All Preserved Images Have Been Processed Event

7 Data Replication

This includes:

Sending Snapshots to One or More OnVault Pools on page 29

Production to Mirror Policy Replication on page 30

Replication of copy data to remote storage protects the data in the event of disaster at the primary site and reduces the amount of storage required at the primary site. The goal of replication is to get your data back in situations of data loss and impact to your production systems due to issues such as a hardware failure, software issues, or a site event. Data replication also supports the creation of remote copies of Test/Dev, QA, and analytics data. Data can be replicated from one Actifio Appliance to a second (remote) appliance or to the cloud for recovery, disaster recovery, or test/development purposes.

Note: *Details about the different types of replication methods can be found in the AGM online help.*

Your SLA templates determine the method, schedule, and frequency of how data replication to a remote site is to be performed. The SLA template defines how to move and store data efficiently to the remote Actifio Appliance. Data replication is controlled by the individual template policies:

- Production to Mirror policies protect your application or VM data against a site failure by having a full copy of that data mirrored to a remote production site. Applications are kept up-to-date and can be re-started at a moment's notice at the remote site by accessing data from the remote DR copy. Data mirroring can be considered as access optimized replication to a remote site. For details see Production to Mirror Policy Replication on page 30.
- Snapshot to OnVault policies use an HTTPS connection to send data to storage defined by an Actifio OnVault Pool. The compress option is on by default in Actifio OnVault Pools. For details see Sending Snapshots to One or More OnVault Pools on page 29.

Sending Snapshots to One or More OnVault Pools

The Snapshot to OnVault policy allows you to send snapshot data to a location defined by an Actifio OnVault Pool. A schedule within the policy is used to send the most recent snapshot taken by the Policy Template's Production to Snapshot policy to the location defined by the OnVault Pool. OnVault Pool storage is typically used for long-term retention. For details on the OnVault Pool, see OnVault Pool for Storing Images Long Term on page 11.

When sending data to a storage defined by an OnVault Pool, an HTTPS connection is used to ensure data security over the network. The OnVault Pool's compression option is on by default to minimize network traffic.

After the initial ingest of the full snapshot, only the changes to data are sent to the OnVault Pool. This is the same incremental forever model used by other Actifio policies.

When accessing data in an OnVault Pool's storage:

- All Actifio Appliances can create clones.
- LiveClones cannot be created.

OnVault to Multiple OnVault Pools

Application data can be sent to multiple OnVault targets in the cloud. Each OnVault target is controlled by separate policies so frequency of update and retentions can be different (e.g., frequent local updates with short retention, together with less frequent updates to cloud with long-term retention).

Multi-target OnVault is supported with all application types, including Direct-to-OnVault with VMware VMs. In this case, the data is written directly to the first OnVault pool, bypassing the snapshot pool, and then read from the first OnVault pool and sent to the others.

Production to Mirror Policy Replication

Production to Mirror policies provide a means to replicate a copy of the application or VM data to a target Actifio Appliance and to have data access without a restore window, providing for very low RTO. As needed, you have the ability to perform a failback to the production site with an identical set of data that is mirrored between the local and remote Actifio Appliances.

StreamSnap

StreamSnap facilitates high-availability by allowing you to keep a remote copy of an application's storage and configuration up-to-date and ready for a failover scenario. When a StreamSnap-managed application fails, you mount a failover image of the application from the remote site. When the problem has been resolved, then you can restore the syncback image to the local site with the latest changes and then failback the application to the production site.

StreamSnap replicates data snapshots to a remote Actifio Appliance over a high quality bandwidth IP network, which can provide RPOs as low as one hour.

- For VMware VMs, snapshot replication is streamed to the second Actifio Appliance in parallel. Streaming of a VMware VM is performed to avoid waiting until the local snapshot job completes before initiating replication.
- For non-VMware VM applications, snapshot replication occurs after the local snapshot job is complete.

Note: *StreamSnap replication and local snapshots are integrated to avoid the creation of double snapshots. The Actifio Appliance allows you to maintain multiple local snapshots and store local images in an OnVault pool for long-term retention.*

Production to Mirror policies with StreamSnap replication are tied to a specific Production to Snapshot policy. They use the schedule and frequency settings of their associated Production to Snapshot policy.

You can retain snapshot images from multiple available points in time at the remote site by applying retention in a StreamSnap policy. When retaining snapshot images at the remote Actifio Appliance, a new snapshot image will be created at the remote appliance with an expiration date determined by the policy settings. Each remote snapshot image supports all operations available with a local snapshot image when accessed from the App Manager.

StreamSnap replication requires a reliable network connection to replicate data snapshots to the remote Actifio Appliance. The bandwidth required on the network connection is directly related to the application size (initial copy) and amount of change (for incremental updates).

For more on StreamSnap replication policies, see StreamSnap Replication on page 22.

8 Different Ways to Access Your Managed Data

This chapter describes the various ways in which you can access your captured data:

Mounts on page 31

Clones on page 32

LiveClones on page 32

Workflows on page 32

Restores on page 32

For detailed, application-specific instructions on how to access data, refer to the AGM online help.

Mounts

The Actifio mount function provides instant access to data without moving data. These are the options for mounting data:

- **The standard mount** presents and makes application data available to a target server as a file system, not as an application. This is useful if an application is corrupt, lost, or if an application server is being replaced. In such cases you can mount an image and copy the application files from the mounted image to their original location on the application server.
- **Application aware mounts** allow you to mount captured databases as virtual applications. This allows you to quickly bring a database on line without having to actually move the data and without having to manually configure a new instance of the database. Application aware mounts are particularly useful in test and development environments where multiple copies of a database must be quickly brought on line.

  Data presented as an application aware mount can be captured like any other application. Once the application aware mounted application data is captured, it too can be can be mounted as an application aware mount.

  The capture, application mount, capture sequence can be repeated to any depth. By default, the sequence is restricted to five generations of the original database.
- **Mount and Migrate** allows you to restore an application with near-zero downtime by first mounting it locally, and then migrating it to the original location or to a new location. Users have normal access to the application while it is mounted, and the migration step is very fast.

When performing a mount from OnVault you can control how much to optimize for performance vs. storage consumption, by selecting:

- **Storage-optimized**: only keep writes in the local snapshot pool (writes are always kept locally).
- **Balanced**: blocks that are read (from object storage) or written (to local snapshot pool) are kept in the snapshot pool, to serve as a "cache" for future reads.
- **Performance-optimized**: bring the entire image to the local snapshot pool, in the background. Reads will become faster as more of the image is available locally.

- **Max performance**: The entire image is rehydrated into the snapshot pool first, prior to the mount. This means that the host always works against local storage only.

Clones

Use the clone function to create an independent copy of a data set. The most common uses are: application development and testing, data audit for compliance, data warehousing, e-discovery, and user acceptance testing. Physical server or VM application-consistent data sets can be copied to a separate storage location anywhere in your environment. Like any other VM, a VM clone can be migrated to a new storage location.

LiveClones

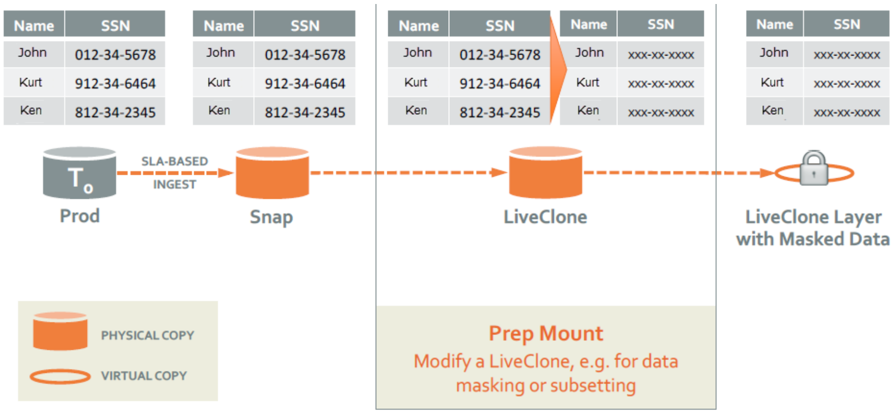
The LiveClone is similar to the Clone function, however, unlike a Clone, a LiveClone can be updated on demand or according to a schedule. When an updated copy of the data is available, a LiveClone allows an independent copy of a data to be mounted. This allows teams such as development and test to ensure they are working on the latest set of data without having to manually manage the data.

Workflows

A Workflow automates access to copy data. While SLA Policy Templates govern the automated capture of production data, Workflows automate the access to this data.

Steps are defined within a Workflow to perform a series of tasks on a schedule or on demand. This includes creating and refreshing LiveClones, data masking, persistent mounts, and non-persistent processing mounts for tasks such as tape-out, database integrity checks, and ETL loads. Workflows are also used by administrators to provide simplified and secured self-service data access to end users such as database administrators and application developers.

This is a high-level illustration of a Workflow that creates a LiveClone from production data, then scrubs the LiveClone of sensitive information, before mounting the LiveClone to a work environment.



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

Workflow With Scrubbed Data

Restores

The Restore function reverts the production data to a specified point in time. Restores and clones are the only data access operations that actually move data. Typically restore operations are performed to restore an 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.

9 Managed Data License (MDL)

Actifio Virtual Data Pipeline (VDP) licensing is based on source application data under management. This is referred to as Managed Data License (MDL).

How is MDL Measured?

Actifio measures MDL based on the actual application size at the front-end. If the application under management reports the volume size for data under management, Actifio takes into account the volume size reported (for example, the MDL calculation for VMware will be consistent with the reported size of the VM in vCenter). Actifio MDL can be independently verified from the application.

The unit of measurement is TB. Actifio measures usage based on the actual size of the applications it is managing. If you manage 10 TB of Oracle data spread across multiple databases, the Actifio MDL reports 10 TB of MDL use. For more information on calculations, see Frequently Asked Questions on page 34.

Actifio MDL measurement takes into consideration only the size of the data under management based on the last successful copy. It does *not* take into account:

- The frequency of data capture
- Where the copies are stored or how many copies are made
- The data change rate
- The retention period or how much storage is occupied by copies

Actifio Global Manager (AGM), Resiliency Director (RD), and Object Recovery for Exchange and SharePoint licensing are in addition to the base MDL licensing.

This section details how MDL is computed for various use cases.

- MDL Computation for VMware
- MDL Computation for Applications Managed with the Actifio Connector
- MDL Computation for Databases
- MDL Computation for OnVault Images of Unprotected Applications

Factors that Influence MDL Calculations and Frequently Asked Questions on page 34 address more scenarios.

MDL Computation for VMware

When the entire VMware VM is managed by Actifio Appliances (all volumes), the MDL count is the total allocated size of all managed volumes. If the volumes are thin-provisioned, then thin provision values are used. If the volumes are thick-provisioned, then the total allocated size is used.

Actifio takes into account the size of the managed volumes reported by VMware vCenter. If a VM has been configured with an 8 TB thin-provisioned volume, and it has been allocated 2 TB, then 2 TB is counted towards MDL use. When the allocated size increases, the MDL count will increase from the next successful copy after the increase in size.

This method of measurement applies all VMware backup scenarios. When an Actifio Actifio Connector is installed inside a VM and the application data within the VM is captured using the Actifio Connector, the MDL calculations are based on out-of-band connector based model described in MDL Computation for Applications Managed with the Actifio Connector.

MDL Computation for Applications Managed with the Actifio Connector

In out-of-band scenarios where the Actifio Connector is used, the actual size of the application is taken into account. If the managed application is 5TB on a 7TB volume, Actifio MDL count will be 5TB.

MDL Computation for Databases

For Oracle, Exchange, and SQL Server applications, only the databases protected are counted towards MDL. Log files are not taken into account:

- Oracle: The allocated size of the database files under protection are counted towards MDL. The allocated size includes data files and control files.
- Microsoft SQL Server: The total size of all the database files, including .MDF, .LDF and .NDF files under protection are counted towards MDL. Log files (.TRN) are not counted towards MDL.
- Microsoft Exchange: The total size of the EDB files and the log files under protection are counted towards MDL.

MDL Computation for OnVault Images of Unprotected Applications

OnVault images are only counted toward MDL while the source application is protected. If the source application becomes unprotected and if all snapshot images are expired, then the OnVault image is not counted for MDL.

Factors that Influence MDL Calculations

Here are some important factors that influence MDL calculations in Out-of-Band scenarios:

- **Compressed Volumes**: When volume is compression enabled, the MDL calculations count the post-compression values. For example, if a 2 TB volume has 2.5 TB of data that is compressed into 1.8 TB, MDL count will be 1.8 TB, not 2.5 TB.
- **Windows Optimized Volumes**: For Windows optimized volumes, VDP rehydrates the volume for backup, and the MDL count will be the rehydrated value. For example, if a 1TB Windows optimized volume contains 800GB data, which when rehydrated for backup ends up as 1.1 TB, the MDL will be 1.1 TB.
- **Block sizes**: The block size of the staging disk is taken into account for MDL measurement. If the source volume's block size and the staging disk block size match, then the MDL values will exactly match the source volume. If the block size used on the staging disk is different from the source volume, then there will be a minor difference because the MDL calculation is done on the staging disk.

> ***Note:*** *Note: Since ZFS volumes use EXT staging disks; ZFS Compression does not affect the MDL calculations, which will reflect the full data size.*

- **Consistency Groups**: The MDL count for a consistency group will be the sum of all application sizes in the consistency group. Applications are measured individually and summed.
- **Reparse points and Linked lists**: These have no impact on MDL.

Frequently Asked Questions

1. Q: What is the unit of measurement for an Actifio MDL?

   A: Actifio MDL unit of measurement is TB. The calculations are based on binary (base 2) and not decimal (base 10). In other words, Actifio counts 1024 GB as 1 TB, not 1000 GB as 1 TB.

2. Q: We just purchased a new Actifio Appliance to replicate from our primary appliance for DR purposes. Do I need additional MDL licenses to replicate between Actifio Appliances?

   A: Actifio MDL is based on front-end application size. It does not take into account how many copies are retained or where they are retained. Adding an appliance for DR purposes *only* will not change MDL consumption. Any applications managed locally on the DR site or VMware datastores replicated between Actifio Appliances will impact MDL consumption.

3. Q: If my file system application has 3 TB of data, and I use Prune Paths and Exclude lists to eliminate 1 TB of files from management, does Actifio count 3 TB as managed capacity or 2 TB as managed capacity?

   A: The MDL for file system applications is based on the actual amount of data managed, 2 TB in this example.

4. Q: How often does the Actifio MDL count get updated?

   A: Actifio MDL values are computed and updated once a day, at 3:00 AM (local time on the appliance). The capture operation should be successfully completed before 3:00 AM for it to be included in MDL measurement.

5. Q: My MDL count for my application seems to be lower than what it reported yesterday, why is that?

   A: Actifio MDL count is based on the most recent successful copy, not the largest recoverable copy. Applications shrink or expand over a period of time (irrespective of the change rates involved). When the application size shrinks, it is reflected on the MDL count the next day.

6. Q: I am managing a 4 TB Oracle database. The Oracle database has a 10% daily change rate, but the size of the database is always 4 TB. What will be my MDL on any given day?

   A: Actifio MDL measurement is based on the size of the last successful copy. In the above example, the managed application size will be 4 TB, so the MDL calculation will be 4 TB. Unless the size of the application changes, the change rate does not directly impact the MDL calculation.

7. Q: If I have an SQL Server application running on a VMware VM, and I manage the SQL Server application using Actifio Connector and the entire VM using VMware VADP, will my SQL database be counted on top of the VM?

   A: Actifio MDL counts VMware VM separately and the SQL database separately, which can lead to double counting. However, customers usually manage only the OS volume of the VM and not the entire VM, when managing the applications residing on the VMs separately. This effectively eliminates double counting.

8. Q: I manage Microsoft SQL and Oracle applications using VDP. Do you count only the database size or do you include the log files in MDL measurement?

   A: Actifio counts only the managed database files that are needed for a consistent database backup towards MDL measurement. Actifio does not count log files towards MDL measurement.

9. Q: I'm no longer actively managing an application that was backed up daily for over a year. When will Actifio MDL measurement stop including this application?

   A: Actifio MDL measurement is based on the last successful copy of the application available. Actifio MDL will consider the application for MDL measurement until all the copies under management have expired. In other words, as long as there's a recoverable image, Actifio will count it towards MDL. This includes orphan images as well (images that are retained per the SLA, whose source application has been deleted from VDP management).

10. Q: I use VDP for my Test/Dev. As part of the Test/Dev we use external tools for data masking and take new snapshots after data masking and present them to the test/dev teams, who also take snapshots periodically. How do changes in workflows like data masking affect my MDL count?

    A: Use of LiveClone and Snapshots manually or via workflow has no effect on MDL. If you rediscover these snapshots as new applications and apply an SLA to them, then they will be counted towards MDL use

11. Q: Will my operations be disrupted if I reach the limits of my purchased MDL?

    A: Actifio recognizes the critical nature of its products operation in customers' environments. There is a built-in grace operation to ensure that jobs are not stopped when MDL utilization extends beyond the purchased MDL. You should monitor your MDL usage regularly and contact Actifio when your usage approaches the purchased MDL.

12. Q: Do I need licenses to access/recover/restore my data?

    A: VDP does not check for the presence of MDL licenses during access/restore/recovery. Actifio licensing does not interfere with protecting or accessing data.

13. Q: I would like to chargeback my customers using a different scheme. Can I get the required information to generate my chargeback reports?

    A: The Report Manager provides a rich set of reports that you can leverage for chargeback. If you have needs that are not met with the Report Manager, contact your Actifio Representative.

14. Q: I have multiple Sky Appliances. Can I share my MDL licenses across these appliances?

    A: Actifio MDL can be shared across all Sky Appliances. However some Sky Appliances come with minimum MDL capacity that is purchased along with the appliance.

15. Q: I have an application with 3 months retention. I no longer need to protect this application, so I no longer actively protect it. When will the MDL consumed by this application be released?

    A: Any application that has a recoverable image, either under active protection or inactive, will be counted towards MDL use. There are two ways the MDL is released, at the end of 3 months when all recoverable images for the application have expired, or by manually expiring all images for the specific application.

16. Q: What happens if I accidentally delete an application and then re-discover it again?

    A: When an application is deleted and rediscovered, the newly discovered application is considered as a brand new application for MDL calculations. If recoverable images of the deleted application remain in the system, those images count towards MDL.

17. Q: How do I verify my VMware MDL usage?

    A: Actifio MDL calculations for VMware are consistent with the vCenter reported size for that VM. `du -h *.vmdk` output from the appropriate VM folder on the datastore matches the MDL count.

    Note: *When snapshots external to Actifio are found on the VM, the allocated size of the VM will be taken for MDL measurement until the snapshots are deleted, as the external snapshots can artificially inflate the MDL calculations.*

18. Q: How do I verify my Oracle MDL usage?

    A: Actifio MDL calculations for Oracle are based on the allocated size for the database. Here is a sample query to verify the Oracle database size.

    ```
    select (d.total + c.total) total from (select sum(bytes) total from v$datafile) d,
    (select sum(block_size*file_size_blks) total from v$controlfile) c;
    ```

    Then subtract the following; `select sum(bytes) free from dba_free_space;`

19. Q: How do I verify my MDL usage for File Systems?

    A: Actifio MDL calculations for file system based applications:

Windows	Used File System size reported by DiskManager
Linux	Used File System size reported by `df - k`

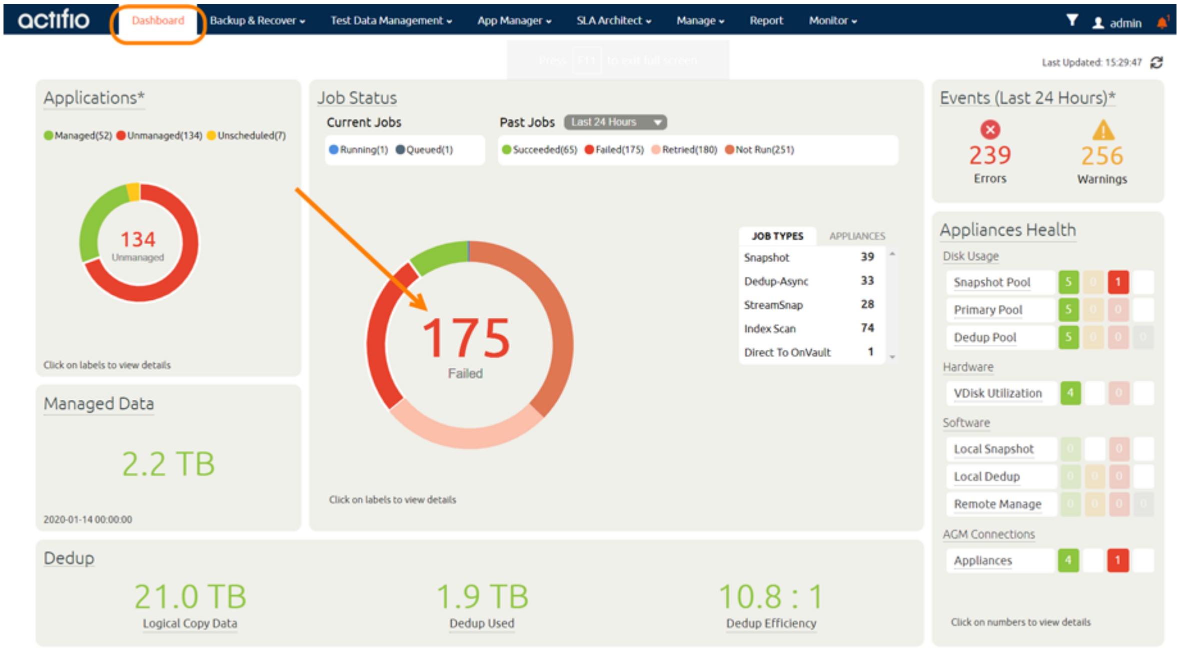
10 Reporting & Monitoring Events

This chapter includes:

Reviewing Job Failures Displayed on the AGM Dashboard on page 37
Reviewing Report Manager Reports on page 42
Reviewing SNMP Traps on page 45

Reviewing Job Failures Displayed on the AGM Dashboard

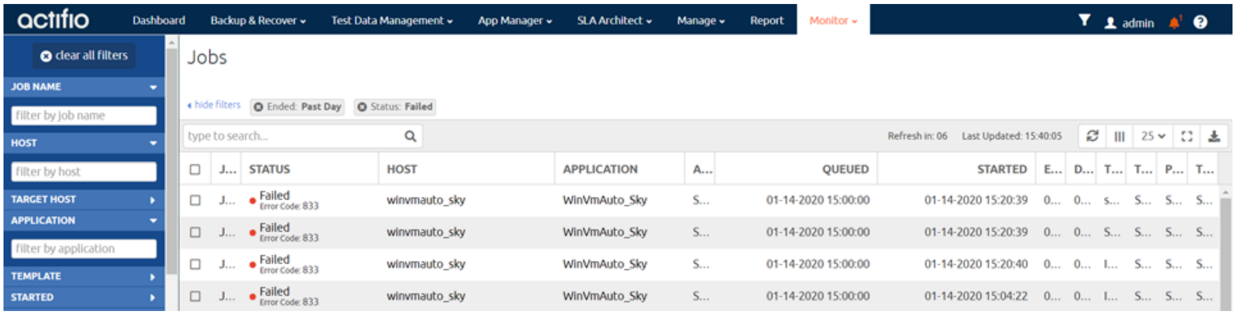
The number of and information about job failures is displayed in the center of the AGM Dashboard:



JOB TYPES	APPLIANCES
Snapshot	39
Dedup-Async	33
StreamSnap	28
Index Scan	74
Direct To OnVault	1

Number of Job Failures Displayed on Dashboard

Click on the number of job failures to display a list of failed jobs in the Jobs Monitor service. For example:



□	J...	STATUS	HOST	APPLICATION	A...	QUEUED	STARTED	E...	D...	T...	T...	P...	T...
□	J...	● Failed Error Code: 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 15:00:00	01-14-2020 15:20:39	0...	0...	s...	S...	S...	S...
□	J...	● Failed Error Code: 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 15:00:00	01-14-2020 15:20:39	0...	0...	S...	S...	S...	S...
□	J...	● Failed Error Code: 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 15:00:00	01-14-2020 15:20:40	0...	0...	I...	S...	S...	S...
□	J...	● Failed Error Code: 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 15:00:00	01-14-2020 15:04:22	0...	0...	I...	S...	S...	S...

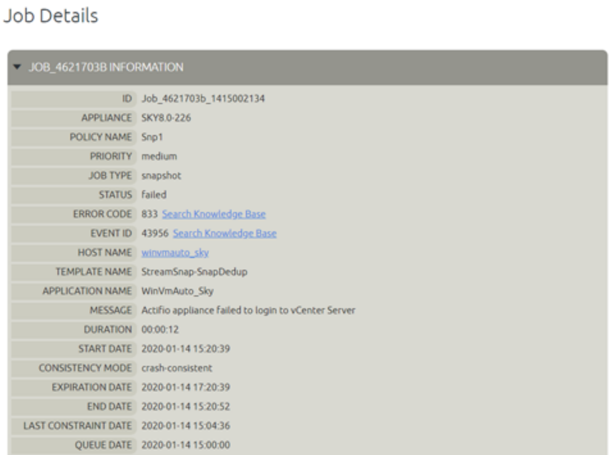
Job Failures Displayed in Jobs Monitor

Right-click on a job entry to display detailed information about the entry.

Review the details of the entry and:

- Use the Search Knowledge Base link to learn how to resolve the issue.
- Ensure the application's host is running.
- For virtual machines, verify the VM has not been migrated to another vCenter.
- If applicable, verify that the Actifio Connector service is running.

Learn more about common job failures in the Actifio Knowledge Base. To research the knowledge base, see Using the Actifio Knowledge Base to Review Event Information on page 62.



Job Details

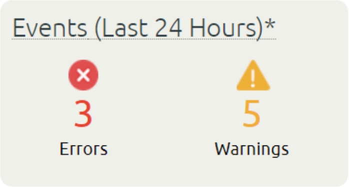
JOB_4621703B INFORMATION

ID	Job_4621703b_1415002134
APPLIANCE	SKY8.0-226
POLICY NAME	Snp1
PRIORITY	medium
JOB TYPE	snapshot
STATUS	failed
ERROR CODE	833 Search Knowledge Base
EVENT ID	43956 Search Knowledge Base
HOST NAME	winvmauto_sky
TEMPLATE NAME	StreamSnap-SnapDedup
APPLICATION NAME	WinVmAuto_Sky
MESSAGE	Actifio appliance failed to login to vCenter Server
DURATION	00:00:12
START DATE	2020-01-14 15:20:39
CONSISTENCY MODE	crash-consistent
EXPIRATION DATE	2020-01-14 17:20:39
END DATE	2020-01-14 15:20:52
LAST CONSTRAINT DATE	2020-01-14 15:04:36
QUEUE DATE	2020-01-14 15:00:00

If there are issues that you cannot resolve, you can contact Actifio Support or open a support case by following the procedure outlined in Creating and Viewing Support Cases on page 64.

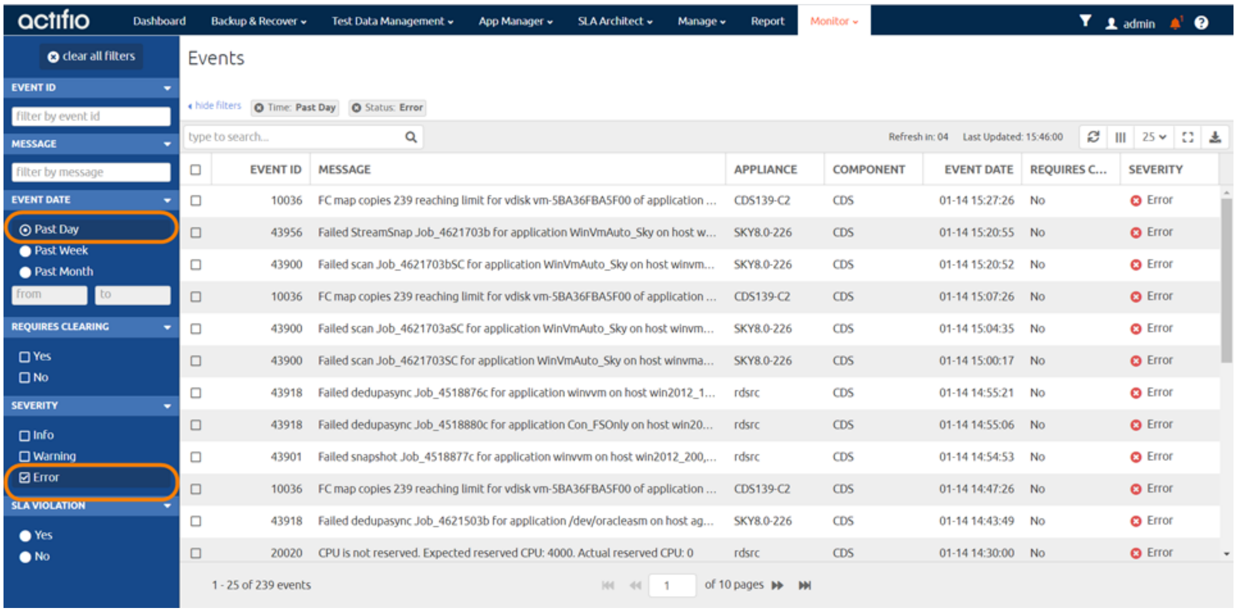
Reviewing Errors and Warnings Displayed on the AGM Dashboard

The number of errors and warnings encountered by an Actifio Appliance are displayed in the upper right-hand corner of the Dashboard:



Number of Errors and Warnings Displayed in AGM Dashboard

1. Click on the number of errors or warnings to display a list of the errors or warning in the Events Monitor service. For example:



□	EVENT ID	MESSAGE	APPLIANCE	COMPONENT	EVENT DATE	REQUIRES C...	SEVERITY
□	10036	FC map copies 239 reaching limit for vdisk vm-5BA36FBA5F00 of application ...	CDS139-C2	CDS	01-14 15:27:26	No	Error
□	43956	Failed StreamSnap Job_4621703b for application WinVmAuto_Sky on host w...	SKY8.0-226	CDS	01-14 15:20:55	No	Error
□	43900	Failed scan Job_4621703bSC for application WinVmAuto_Sky on host winvm...	SKY8.0-226	CDS	01-14 15:20:52	No	Error
□	10036	FC map copies 239 reaching limit for vdisk vm-5BA36FBA5F00 of application ...	CDS139-C2	CDS	01-14 15:07:26	No	Error
□	43900	Failed scan Job_4621703aSC for application WinVmAuto_Sky on host winvm...	SKY8.0-226	CDS	01-14 15:04:35	No	Error
□	43900	Failed scan Job_4621703SC for application WinVmAuto_Sky on host winvma...	SKY8.0-226	CDS	01-14 15:00:17	No	Error
□	43918	Failed dedupasync Job_4518876c for application winvvm on host win2012_1...	rdsrc	CDS	01-14 14:55:21	No	Error
□	43918	Failed dedupasync Job_4518880c for application Con_FSOnly on host win20...	rdsrc	CDS	01-14 14:55:06	No	Error
□	43901	Failed snapshot Job_4518877c for application winvvm on host win2012_200,...	rdsrc	CDS	01-14 14:54:53	No	Error
□	10036	FC map copies 239 reaching limit for vdisk vm-5BA36FBA5F00 of application ...	CDS139-C2	CDS	01-14 14:47:26	No	Error
□	43918	Failed dedupasync Job_4621503b for application /dev/oracleasm on host ag...	SKY8.0-226	CDS	01-14 14:43:49	No	Error
□	20020	CPU is not reserved. Expected reserved CPU: 4000. Actual reserved CPU: 0	rdsrc	CDS	01-14 14:30:00	No	Error

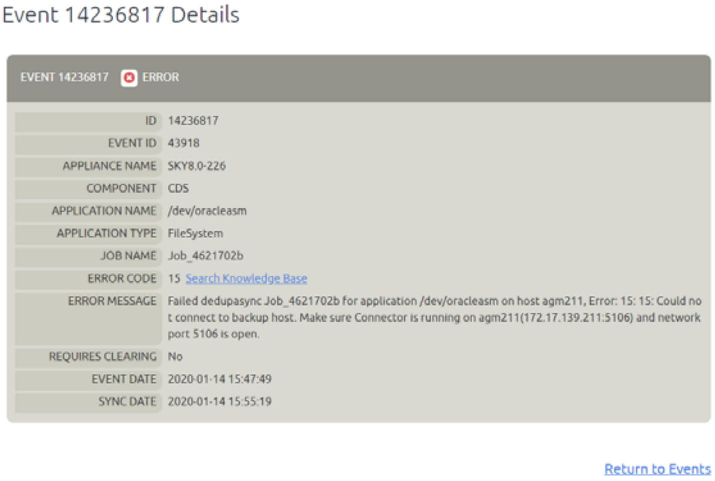
1 - 25 of 239 events

1 of 10 pages

Errors Displayed in Events Monitor

Right-click on an error entry to display detailed information about the error. You can learn more information about the most common errors in the Actifio Knowledge Base. To research the knowledge base, see Using the Actifio Knowledge Base to Review Event Information on page 62.

2. If there are issues that you cannot resolve, you can contact Actifio Support or open a support case by following the procedure outlined in Creating and Viewing Support Cases on page 64..



Event 14236817 Details

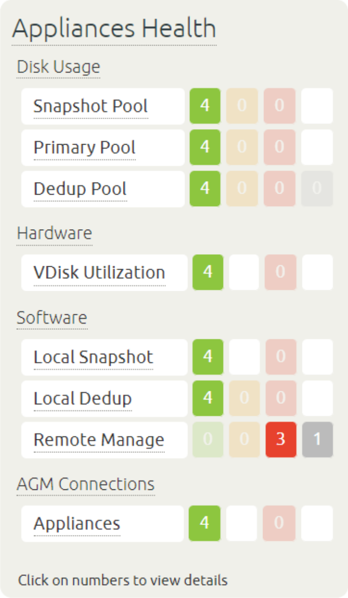
EVENT 14236817 ERROR

ID	14236817
EVENT ID	43918
APPLIANCE NAME	SKY8.0-226
COMPONENT	CDS
APPLICATION NAME	/dev/oracleasm
APPLICATION TYPE	FileSystem
JOB NAME	Job_4621702b
ERROR CODE	15 Search Knowledge Base
ERROR MESSAGE	Failed dedupasync Job_4621702b for application /dev/oracleasm on host agm211, Error: 15: 15: Could no t connect to backup host. Make sure Connector is running on agm211(172.17.139.211:5106) and network port 5106 is open.
REQUIRES CLEARING	No
EVENT DATE	2020-01-14 15:47:49
SYNC DATE	2020-01-14 15:55:19

Return to Events

Reviewing the Appliances Health Monitor in the AGM Dashboard

The high-level status of your managed Actifio Appliances is displayed in the Appliances Health Monitor on the right-hand side of the Dashboard:



Appliances Health

Disk Usage				
Snapshot Pool	4	0	0	
Primary Pool	4	0	0	
Dedup Pool	4	0	0	0
Hardware				
VDisk Utilization	4		0	
Software				
Local Snapshot	4		0	
Local Dedup	4	0	0	
Remote Manage	0	0	3	1
AGM Connections				
Appliances	4		0	

Click on numbers to view details

Appliances Health Monitor in the AGM Dashboard

The Appliances Health Monitor provides an overview of resource usage and system health.

- **Disk Usage**: Current percent utilization of the default pools (Snapshot and Primary pools). Clicking the Snapshot Pool or Primary Pool label displays the associated pool window. If you do not have access to Snapshot Pool or Primary Pool information, then you see no values in Disk Usage.
- **Hardware**: Status of storage resources and VDisk utilization.
- **Software**: Status of local snapshot and remote protection.
- **AGM Connections**: Status of connections to each managed Actifio Appliance.

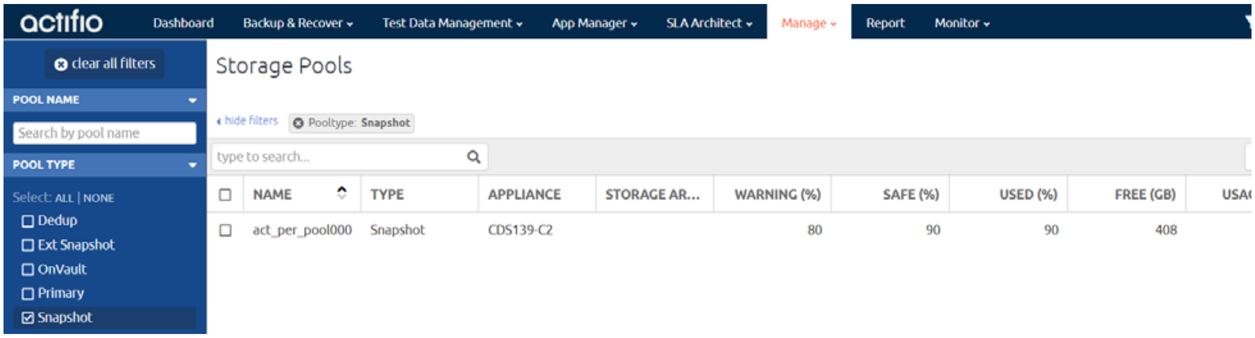
If you mouse over an entry in the Appliances Health Monitor, definitions for the various color coded status indicators are displayed:

Disk Usage
Hardware
Software
AGM Connections

Disk Usage

If the System Health Monitor shows a Disk Usage pool as YELLOW or RED:

1. Click on the pool and the Storage Pools page is displayed.
2. If possible, add more disks to the pool. See AGM Online Help for instructions.
3. Contact Actifio Support if more disks cannot be added.



□	NAME	TYPE	APPLIANCE	STORAGE AR...	WARNING (%)	SAFE (%)	USED (%)	FREE (GB)	USA
□	act_per_pool000	Snapshot	CDS139-C2		80	90	90	408	

Checking Disk Usage

Hardware

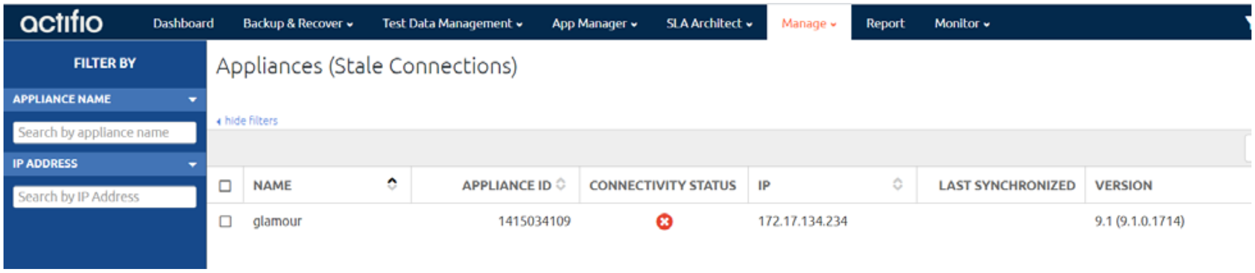
- If the System Health Monitor Hardware Storage section displays YELLOW or RED, ensure storage is online.
- If VDisk utilization is RED, the VDisk count has exceeded its limit and corrective action is necessary: unmount unneeded active images and expire old images from snapshot pool. The AGM online help has instructions.

Software

- If Local Snapshot is RED, contact Actifio Support.
- If Remote Manage is YELLOW or RED, determine if communication between Actifio Appliances has been disrupted or changed.
- If there are issues that you cannot resolve, you can contact Actifio Support or open a support case by following the procedure outlined in Creating and Viewing Support Cases on page 64.

AGM Connections

If any AGM connections are RED or YELLOW, then click on the red or yellow square to see in which managed appliances have issues.



□	NAME	APPLIANCE ID	CONNECTIVITY STATUS	IP	LAST SYNCHRONIZED	VERSION
□	glamour	1415034109	☒	172.17.134.234		9.1 (9.1.0.1714)

Checking AGM Stale Connections

Reviewing Report Manager Reports

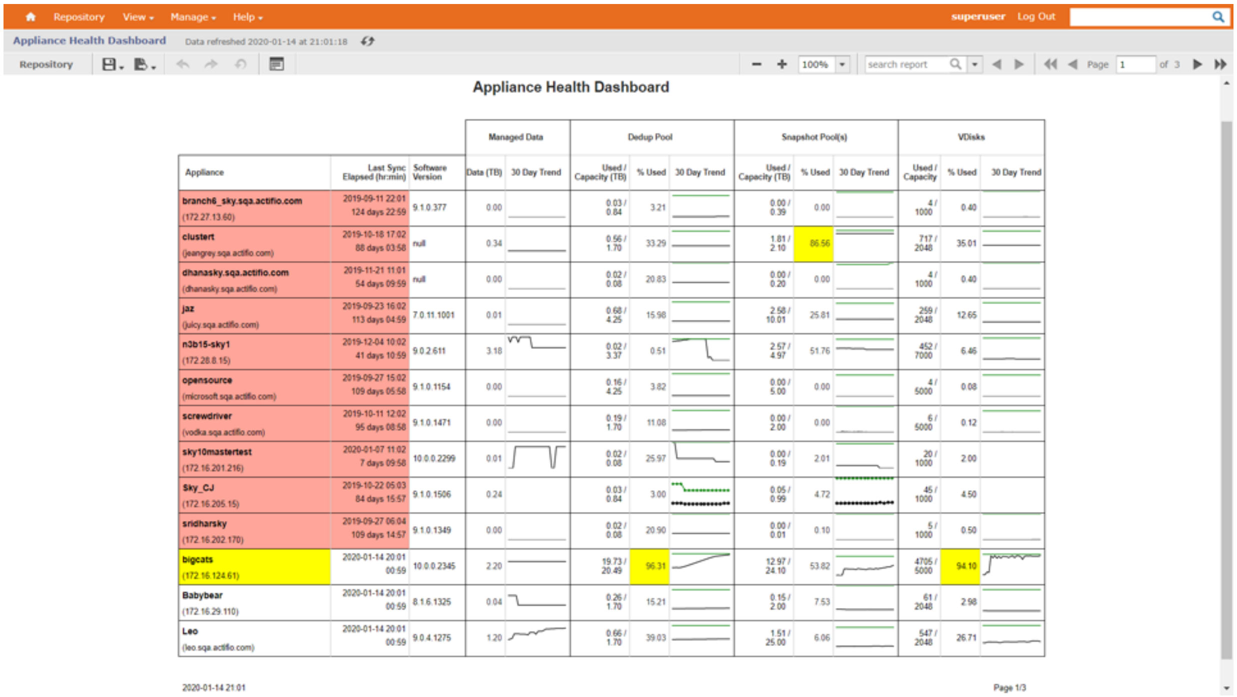
The optional Report Manager can generate detailed reports on your Actifio Appliance and the applications and data it manages. For details on how to configure the Report Manager to automatically generate and deliver daily email reports, see the Report Manager online help.

At a minimum, review the following reports either manually or included in your daily email reports:

Appliance Health Dashboard on page 42
Daily Protection Status on page 43
Database Backup Status on page 44
Storage Resource Trending on page 45

Appliance Health Dashboard

The Appliance Health Dashboard is the default home screen you see when you log on to the Report Manager. It shows you key attributes and resource consumption of your appliances at a glance, with colors to indicate snapshot pools and VDisks that are approaching their limits. Appliances that are in a critical or warning state appear at the top.



Appliance Health Dashboard

			Managed Data		Dedup Pool			Snapshot Pool(s)			VDisks		
Appliance	Last Sync Elapsed (hr:min)	Software Version	Data (TB)	30 Day Trend	Used / Capacity (TB)	% Used	30 Day Trend	Used / Capacity (TB)	% Used	30 Day Trend	Used / Capacity	% Used	30 Day Trend
branch6_sky.sqa.actifio.com (172.27.13.60)	2019-09-11 22:01 124 days 22:59	9.1.0.377	0.00		0.03 / 0.84	3.21		0.00 / 0.39	0.00		4 / 1000	0.40	
clustert (jeangrey.sqa.actifio.com)	2019-10-18 17:02 88 days 03:58	null	0.34		0.56 / 1.70	33.29		1.81 / 2.10	86.56		717 / 2048	35.01	
dhanasky.sqa.actifio.com (dhanasky.sqa.actifio.com)	2019-11-21 11:01 54 days 09:59	null	0.00		0.02 / 0.08	20.83		0.00 / 0.20	0.00		4 / 1000	0.40	
jaz (juicy.sqa.actifio.com)	2019-09-23 16:02 113 days 04:59	7.0.11.1001	0.01		0.68 / 4.25	15.98		2.58 / 10.01	25.81		259 / 2048	12.65	
n3b15-sky1 (172.28.8.15)	2019-12-04 10:02 41 days 10:59	9.0.2.611	3.18		0.02 / 3.37	0.51		2.57 / 4.97	51.76		452 / 7000	6.46	
opensource (microsoft.sqa.actifio.com)	2019-09-27 15:02 109 days 05:58	9.1.0.1154	0.00		0.16 / 4.25	3.82		0.00 / 5.00	0.00		4 / 5000	0.08	
screwdriver (vodka.sqa.actifio.com)	2019-10-11 12:02 95 days 08:58	9.1.0.1471	0.00		0.19 / 1.70	11.08		0.00 / 2.00	0.00		6 / 5000	0.12	
sky10mastertest (172.16.201.216)	2020-01-07 11:02 7 days 09:58	10.0.0.2299	0.01		0.02 / 0.08	25.97		0.00 / 0.19	2.01		20 / 1000	2.00	
Sky_CJ (172.16.205.15)	2019-10-22 05:03 84 days 15:57	9.1.0.1506	0.24		0.03 / 0.84	3.00		0.05 / 0.99	4.72		45 / 1000	4.50	
sridharsky (172.16.202.170)	2019-09-27 06:04 109 days 14:57	9.1.0.1349	0.00		0.02 / 0.08	20.90		0.00 / 0.01	0.10		5 / 1000	0.50	
bigcats (172.16.124.61)	2020-01-14 20:01 00:59	10.0.0.2345	2.20		19.73 / 20.49	96.31		12.97 / 24.10	53.82		4705 / 5000	94.10	
Babybear (172.16.29.110)	2020-01-14 20:01 00:59	8.1.6.1325	0.04		0.26 / 1.70	15.21		0.15 / 2.00	7.53		61 / 2048	2.98	
Leo (leo.sqa.actifio.com)	2020-01-14 20:01 00:59	9.0.4.1275	1.20		0.66 / 1.70	39.03		1.51 / 25.00	6.06		547 / 2048	26.71	

2020-01-14 21:01

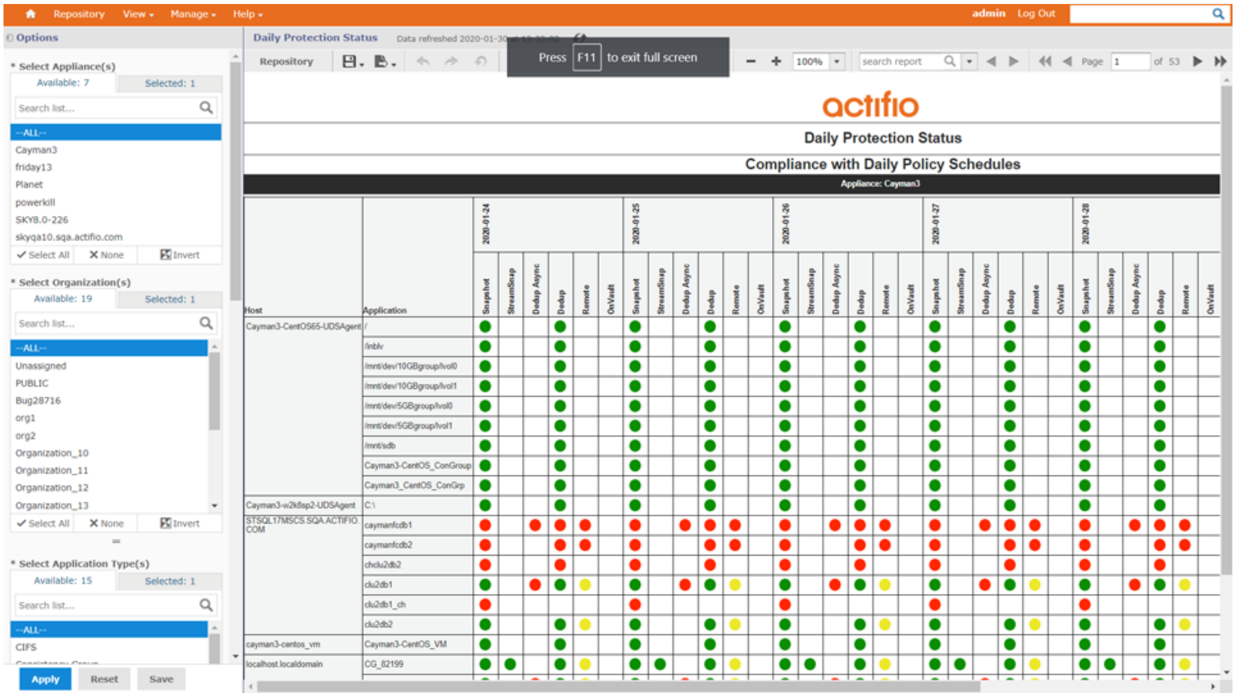
Page 1/3

Appliance Health Dashboard

Daily Protection Status

This reports shows whether any snapshot, StreamSnap, and OnVault jobs succeeded with consistency dates corresponding to the dates shown in the report. The number of color slots shown will depend on the policy types used for each appliance, representing snapshot, StreamSnap, and OnVault status. Direct to OnVault jobs are considered as OnVault. It only looks at policies with a daily schedule.

Details of the columns and parameters are in the Report Manager online help.



actifio

Daily Protection Status

Compliance with Daily Policy Schedules

Appliance: Cayman3

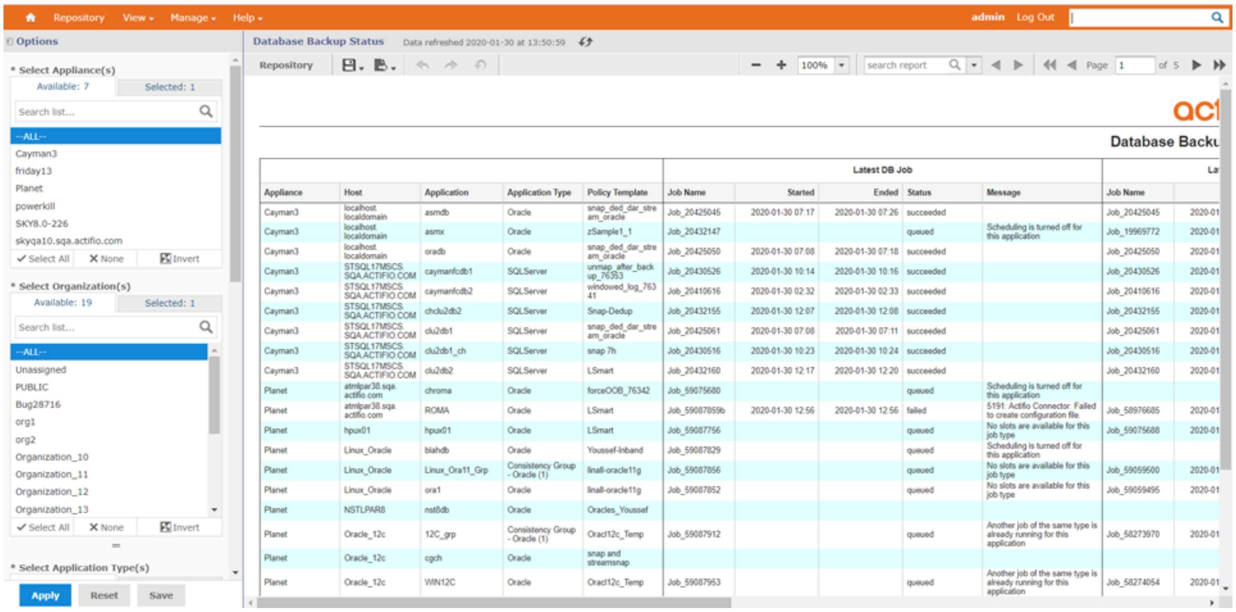
		2020-01-24						2020-01-25						2020-01-26						2020-01-27						2020-01-28					
Host	Application	Snapshot	StreamSnap	Dedup Async	Dedup	Remote	OnVault	Snapshot	StreamSnap	Dedup Async	Dedup	Remote	OnVault	Snapshot	StreamSnap	Dedup Async	Dedup	Remote	OnVault	Snapshot	StreamSnap	Dedup Async	Dedup	Remote	OnVault	Snapshot	StreamSnap	Dedup Async	Dedup	Remote	OnVault
Cayman3-CentOS65-UDSAgent	/	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/inblv	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/mnt/dev/10GBgroup/lvol0	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/mnt/dev/10GBgroup/lvol1	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/mnt/dev/5GBgroup/lvol0	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/mnt/dev/5GBgroup/lvol1	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	/mnt/sdb	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	Cayman3-CentOS_ConGroup	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
	Cayman3_CentOS_ConGrp	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
Cayman3-w2k8sp2-UDSAgent	C:\	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
STSQL17MSCS.SQA.ACTIFIO.COM	caymanfcdb1	🔴		🔴	🔴	🔴		🔴		🔴	🔴	🔴		🔴		🔴	🔴	🔴		🔴		🔴	🔴	🔴		🔴		🔴	🔴	🔴	
	caymanfcdb2	🔴			🔴	🔴		🔴			🔴	🔴		🔴			🔴	🔴		🔴			🔴	🔴		🔴			🔴	🔴	
	chclu2db2	🔴			🔴			🔴			🔴			🔴			🔴			🔴			🔴			🔴			🔴		
	clu2db1	🟢		🔴	🟢	🟡		🟢		🔴	🟢	🟡		🟢		🔴	🟢	🟡		🟢		🔴	🟢	🟡		🟢		🔴	🟢	🟡	
	clu2db1_ch	🔴						🔴						🔴						🔴						🔴					
	clu2db2	🟢			🟢	🟡		🟢			🟢	🟡		🟢			🟢	🟡		🟢			🟢	🟡		🟢			🟢	🟡	
cayman3-centos_vm	Cayman3-CentOS_VM	🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢			🟢		
localhost.localdomain	CG_82199	🟢	🟢		🟢	🟡		🟢	🟢		🟢	🟡		🟢	🟢		🟢	🟡		🟢	🟢		🟢	🟡		🟢	🟢		🟢	🟡	

Daily Protection Status Report

Database Backup Status

This report provides the database and log backup status for database applications such as Oracle, SQL Server, SAP HANA, or Consistency Groups with Oracle, SQL Server and SAP HANA applications as consistency group members. It also provides the most recent job status, along with the recent successful database and log jobs.

Details of the columns and parameters are in the Report Manager online help.



* Select Appliance(s)
Available: 7 | Selected: 1
Search list...
--ALL--
Cayman3
friday13
Planet
powerkill
SKY8.0-226
skyqa10.sqa.actifio.com
✓ Select All | ✕ None | Invert

* Select Organization(s)
Available: 19 | Selected: 1
Search list...
--ALL--
Unassigned
PUBLIC
Bug28716
org1
org2
Organization_10
Organization_11
Organization_12
Organization_13
✓ Select All | ✕ None | Invert

* Select Application Type(s)

Apply | Reset | Save

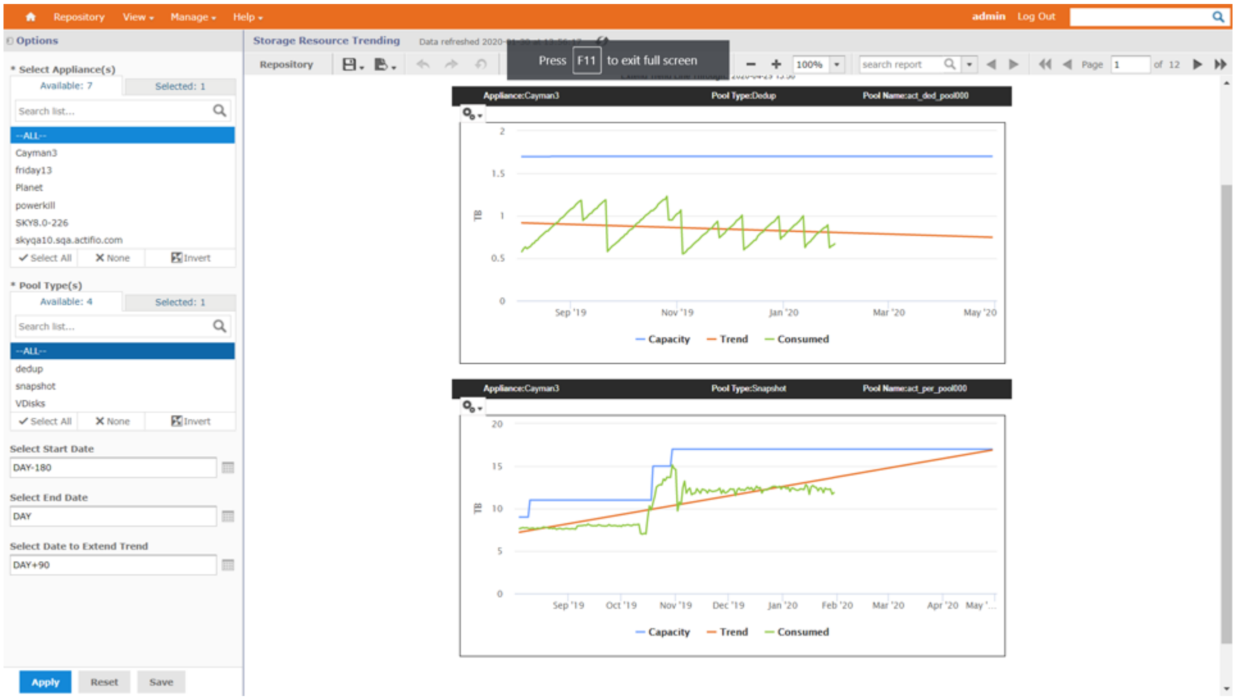
					Latest DB Job					La	
Appliance	Host	Application	Application Type	Policy Template	Job Name	Started	Ended	Status	Message	Job Name	
Cayman3	localhost. localdomain	asmdb	Oracle	snap_ded_dar_stre am_oracle	Job_20425045	2020-01-30 07:17	2020-01-30 07:26	succeeded		Job_20425045	2020-01
Cayman3	localhost. localdomain	asmx	Oracle	zSample1_1	Job_20432147			queued	Scheduling is turned off for this application	Job_19969772	2020-01
Cayman3	localhost. localdomain	oradb	Oracle	snap_ded_dar_stre am_oracle	Job_20425050	2020-01-30 07:08	2020-01-30 07:18	succeeded		Job_20425050	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	caymanfcdb1	SQLServer	unmap_after_back up_76353	Job_20430526	2020-01-30 10:14	2020-01-30 10:16	succeeded		Job_20430526	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	caymanfcdb2	SQLServer	windowed_log_763 41	Job_20410616	2020-01-30 02:32	2020-01-30 02:33	succeeded		Job_20410616	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	chclu2db2	SQLServer	Snap-Dedup	Job_20432155	2020-01-30 12:07	2020-01-30 12:08	succeeded		Job_20432155	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	clu2db1	SQLServer	snap_ded_dar_stre am_oracle	Job_20425061	2020-01-30 07:08	2020-01-30 07:11	succeeded		Job_20425061	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	clu2db1_ch	SQLServer	snap 7h	Job_20430516	2020-01-30 10:23	2020-01-30 10:24	succeeded		Job_20430516	2020-01
Cayman3	STSQL17MSCS. SQA.ACTIFIO.COM	clu2db2	SQLServer	LSmart	Job_20432160	2020-01-30 12:17	2020-01-30 12:20	succeeded		Job_20432160	2020-01
Planet	atmlpar38.sqa. actifio.com	chroma	Oracle	forceOOB_76342	Job_59075680			queued	Scheduling is turned off for this application		
Planet	atmlpar38.sqa. actifio.com	ROMA	Oracle	LSmart	Job_59087859b	2020-01-30 12:56	2020-01-30 12:56	failed	5191: Actifio Connector: Failed to create configuration file.	Job_58976685	2020-01
Planet	hpux01	hpux01	Oracle	LSmart	Job_59087756			queued	No slots are available for this job type	Job_59075688	2020-01
Planet	Linux_Oracle	blahdb	Oracle	Youssef-Inband	Job_59087829			queued	Scheduling is turned off for this application		
Planet	Linux_Oracle	Linux_Ora11_Grp	Consistency Group - Oracle (1)	linall-oracle11g	Job_59087856			queued	No slots are available for this job type	Job_59059500	2020-01
Planet	Linux_Oracle	ora1	Oracle	linall-oracle11g	Job_59087852			queued	No slots are available for this job type	Job_59059495	2020-01
Planet	NSTLPAR8	nst8db	Oracle	Oracles_Youssef							
Planet	Oracle_12c	12C_grp	Consistency Group - Oracle (1)	Oracl12c_Temp	Job_59087912			queued	Another job of the same type is already running for this application	Job_58273970	2020-01
Planet	Oracle_12c	cgch	Oracle	snap and streamsnap							
Planet	Oracle_12c	WIN12C	Oracle	Oracl12c_Temp	Job_59087953			queued	Another job of the same type is already running for this application	Job_58274054	2020-01

Database Backup Status Report

Storage Resource Trending

This report shows the resource consumption for snapshot pools and VDisks. It also forecasts the future consumption of the resources.

Details of the columns and parameters are in the Report Manager online help.



Storage Resource Trending

Data refreshed 2020-01-30 at 13:56:17

Press F11 to exit full screen

* Select Appliance(s): Available: 7, Selected: 1

--ALL--
Cayman3
friday13
Planet
powerkill
SKY8.0-226
skyqa10.sqa.actifio.com

* Pool Type(s): Available: 4, Selected: 1

--ALL--
dedup
snapshot
VDisks

Select Start Date: DAY-180

Select End Date: DAY

Select Date to Extend Trend: DAY+90

Appliance:Cayman3 | Pool Type:Dedup | Pool Name:act_ded_pool000

Appliance:Cayman3 | Pool Type:Snapshot | Pool Name:act_per_pool000

Storage Resource Trending Report

Reviewing SNMP Traps

If you have an SNMP trap receiver configured, your Actifio Appliance can send SNMP traps to the SNMP trap receiver in the appliance. Reviewing the SNMP trap receiver is the first place to look for critical issues.

For details on how to configure SNMP traps, including the location of the Actifio MIB file, see ***Network Administrator's Guide to Actifio VDP***. Pay particular attention to the 43900 and 43901 series events, as they indicate job failure. See Using the Actifio Knowledge Base to Review Event Information on page 62 for details.

11 Supporting Multitenancy using Actifio Organizations

This gives a detailed overview of how Actifio solutions should be deployed in a multi-tenant environment. Multi-tenancy is a reference to the mode of operation and a deployment model of software and hardware where multiple independent instances of one or multiple applications operate in a shared environment. In this deployment model, the tenants are logically isolated, but physically integrated. Multi-tenancy is a core deployment model for a cloud service provider or managed service provider to reduce resource cost by increasing infrastructure utilization and to make it easier to chargeback customers. Multi-tenancy in enterprise datacenters is also becoming a deployment model of choice as private and hybrid clouds take hold with internal business divisions identified as tenants that share the common IT infrastructure.

This provides details of how Actifio appliances and related management tools can be deployed in a multi-tenant model with the following characteristics:

- Logical separation of data traffic flow from customer datacenter to a CSP datacenter
- Logical and physical separation of data storage
- Tenant UI separation and access models
- Tenant specific resource usage reporting
- Developing portals and extensions using Foresight APIs in a multi-tenant deployment model

Overview

Multi-tenancy encompasses multiple aspects, from management and reporting through data separation at storage and networking. An Actifio environment is managed using Actifio Global Manager (AGM), and that where management separation is defined, using organizations that have users and resources associated with them. The data virtualization and handling is done on Actifio appliances, managed by AGM.

The simplest approach to multi-tenancy would be to use separate appliances for each tenant, managed by one AGM, thereby achieving data separation in combination with streamlined management. This enables a service provider, for example, to manage data across all customers, while providing the strictest and clearest operational separation. This is the most common model used today, especially leveraging the flexibility that the Actifio Sky Appliance provides to match appliance size with a customer's data capacity.

In some situations, especially with tenants that have small amounts of data, it is not economical to dedicate an appliance to each tenant. Actifio appliances can support multi-tenancy within an appliance, using organizations and separation of physical resource pools.

Tenant logical resource isolation using organizations

Actifio Organizations are the main means for logically separating multiple tenants within an Actifio environment. Organizations associate users with objects or physical resources to control who can view and act on what.

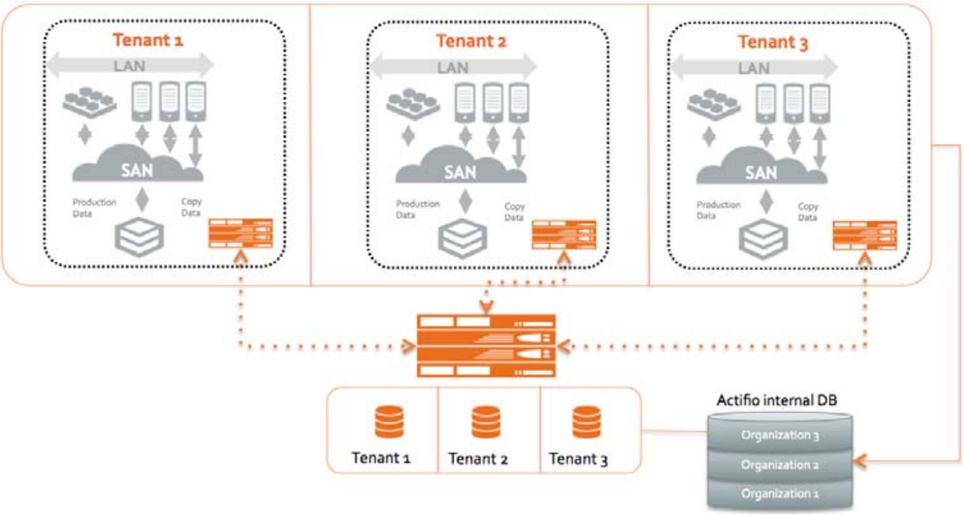
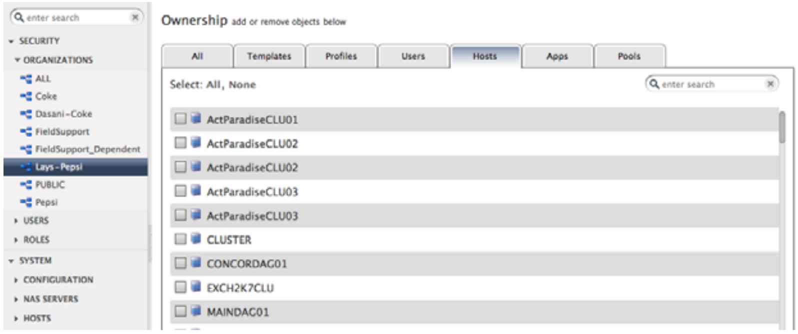


Figure 1 Resource Logical Separation in an Organization

Entities that can be logically separated includes storage pools, hosts and applications (with their images/ backups), SLA templates, and resource profiles.

Organizations can be created in a hierarchy, so that a tenant sub organization's resources can also be isolated. For instance, PepsiCo could have Frito-Lay hosts placed under a separate organization to simplify their chargeback model.



Ownership add or remove objects below

Select: All, None

- □ ActParadiseCLU01
- □ ActParadiseCLU02
- □ ActParadiseCLU02
- □ ActParadiseCLU03
- □ ActParadiseCLU03
- □ CLUSTER
- □ CONCORDAG01
- □ EXCH2K7CLU
- □ MAINDAG01

Figure 2 A Sub-organization within a Tenant

Tenant resource access separation with role-based access control

For a service provider, or a private enterprise operating in a service provider model, it is important to create separate users with clear separation of control responsibilities for different tenants. Actifio's Role-Based Access Control (RBAC) mechanism provides fine-grained access privileges for specific parts of the system using roles and their associated rights. There are a variety of predefined roles and it is easy to define new roles with appropriate rights. For example, a storage administrator can have access privilege for creating and maintaining a set of storage pools, and at the same time she might only have viewing privileges for hosts. Even within the context of one tenant, the administrator of all the tenant's resources can restrict who can access which service features in the product. For example, an administrator responsible for creating and maintaining SLA policies need not have access to storage and hosts. Figure 3 outlines how a tenant's user co-exists with other tenants in the same environment.

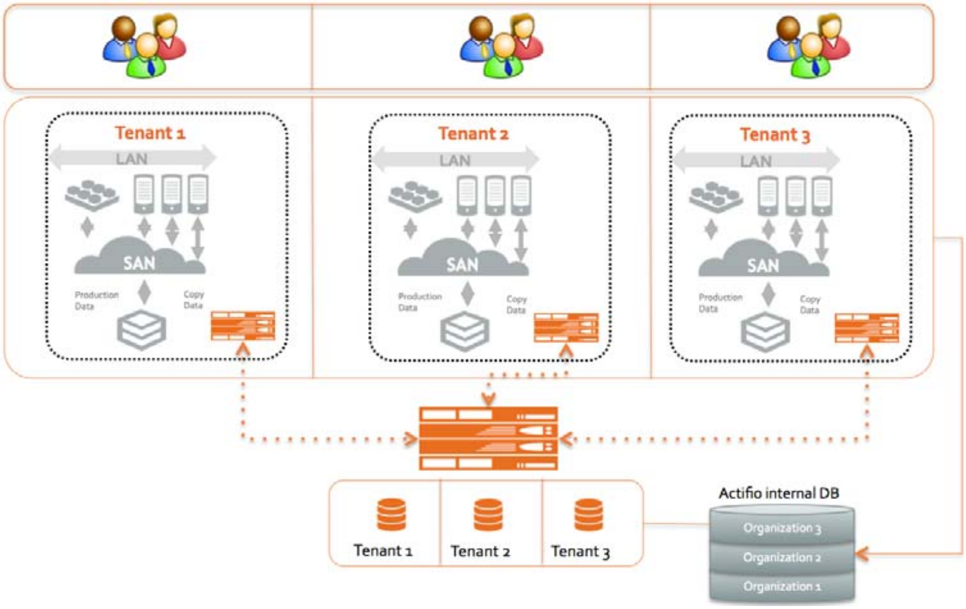
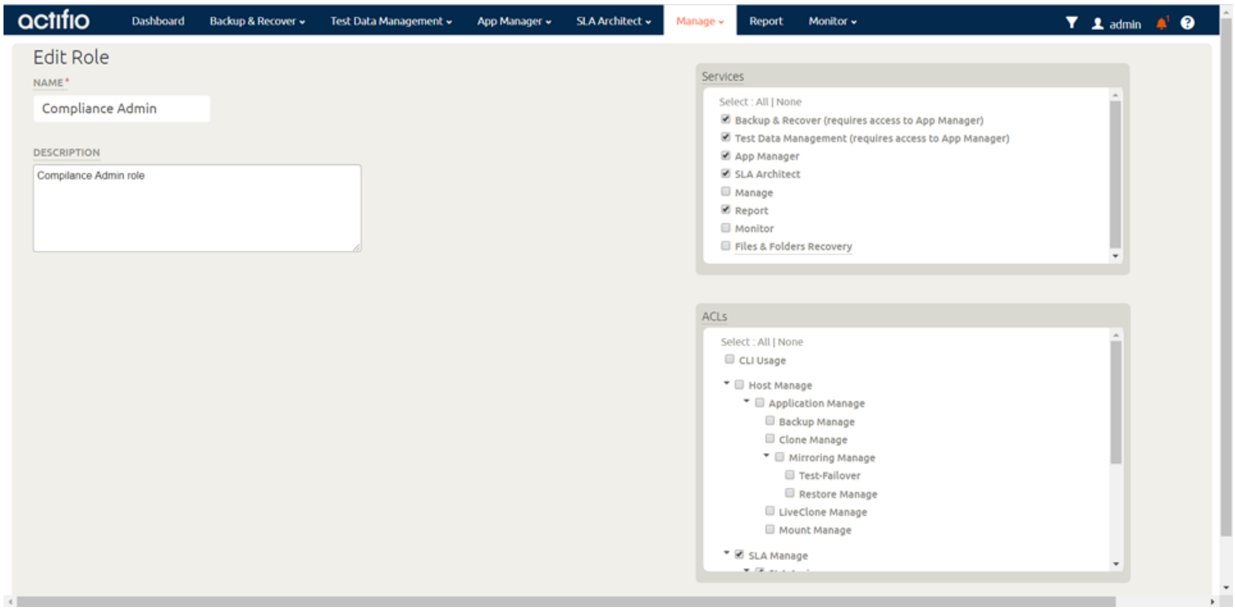


Figure 3 Role-Based Access Control per Tenant

Actifio provides several levels of rights for dealing with resources within the system. The most basic level is viewing a resource, whereas the most complete level is managing it (creating, modifying, deleting). Some resources have more levels in between - for example a user might be given a right to view SLA templates and assign them to applications, but not the right to manage the templates. Figure 4 provides an example of some of these access rights.

To summarize, a user is limited to performing specific actions (based on their role and associated rights) on specific resources (limited by the organizations to which they belong). A user cannot see resources that are not within their organizations.



Edit Role

NAME *

Compliance Admin

DESCRIPTION

Compliance Admin role

Services

Select : All | None

- ☑ Backup & Recover (requires access to App Manager)
- ☑ Test Data Management (requires access to App Manager)
- ☑ App Manager
- ☑ SLA Architect
- □ Manage
- ☑ Report
- □ Monitor
- □ Files & Folders Recovery

ACLs

Select : All | None

- □ CLI Usage
- □ Host Manage
  - □ Application Manage
    - □ Backup Manage
    - □ Clone Manage
    - □ Mirroring Manage
      - □ Test-Failover
      - □ Restore Manage
    - □ LiveClone Manage
    - □ Mount Manage
- ☑ SLA Manage

Figure 4 Roles and Rights within a Tenant Role

Data storage tenant isolation

In a multi-tenant environment, customers of Cloud Service Providers might require data storage isolation. An Actifio appliance can completely isolate tenant storage in different snapshot pools that use storage from separate RAID groups or even different storage arrays. These snapshot pools can have different performance characteristics with unrelated disk groups. They may even be from different vendors.

Similarly, multiple OnVault pools can be created, within one cloud account or object storage array or on different accounts and arrays. These pools provide data storage isolation among tenants for long-term retention on object storage. Note that OnVault can be configured with multiple appliances writing into the same object storage bucket, and when importing images from that bucket into a new Actifio appliance all images in that bucket will be available to the importing user. Different buckets should be used to ensure data separation. In addition, organization information is not written to OnVault so organizational separation must be re-established after importing images, if needed.

Figure 5 illustrates a deployment model of a Cloud Service Provider with a private cloud tenant co-located within the cloud provider facility and another tenant located outside of the CSP's facility.

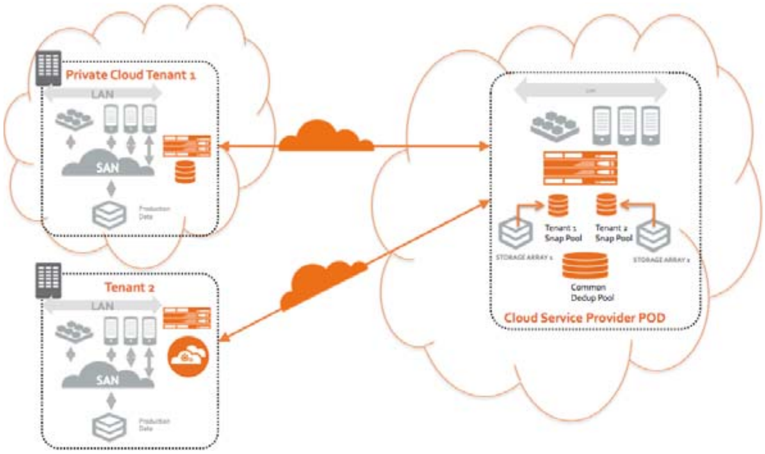


Figure 5 Data Storage Isolation with Actifio VDP

When replicating data from an on-prem (or colo) tenant appliance into a service provider appliance using StreamSnap replication, the service provider can control the target snapshot pool based on the source appliance, to ensure continued data storage separation.

Isolating data traffic per tenant

In addition to providing for data storage separation, service provider clouds require the ability to deal with data traffic isolation in the form of VLAN tags or the ability to deal with overlapping IP ranges when different customers replicate data over to CSP clouds. Actifio appliances provide basic support for network traffic separation with different network interfaces. From a Cloud Service Provider point of view, network separation is important between network edges up until where data touches the Actifio appliance replication interfaces. Data traffic between a customer datacenter and the CSP datacenter could be handled as mixed traffic or isolated using dedicated Virtual Private Networks. These VPN networks could also handle tagged VLAN traffic if customer networks are on a trusted domain. In a mixed data traffic environment such as over the Internet, IPSec VPNs can be configured to encrypt different tenants' data to avoid security problems. These mixed traffic environments can be terminated at the CSP using appropriate firewalls and routers. The following diagrams present different approaches on how Actifio appliances can be configured with various network isolation mechanisms.

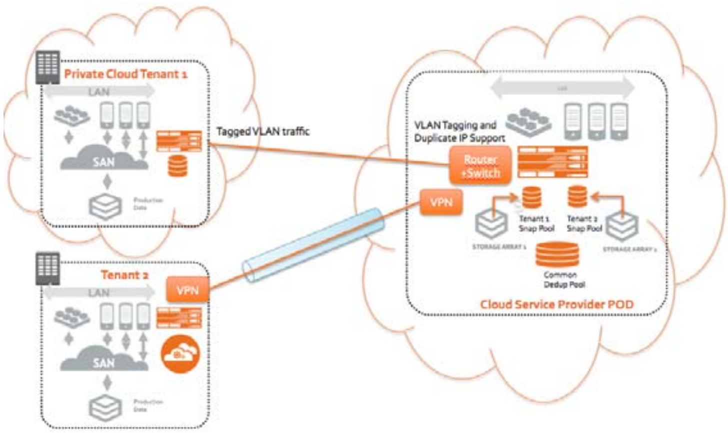


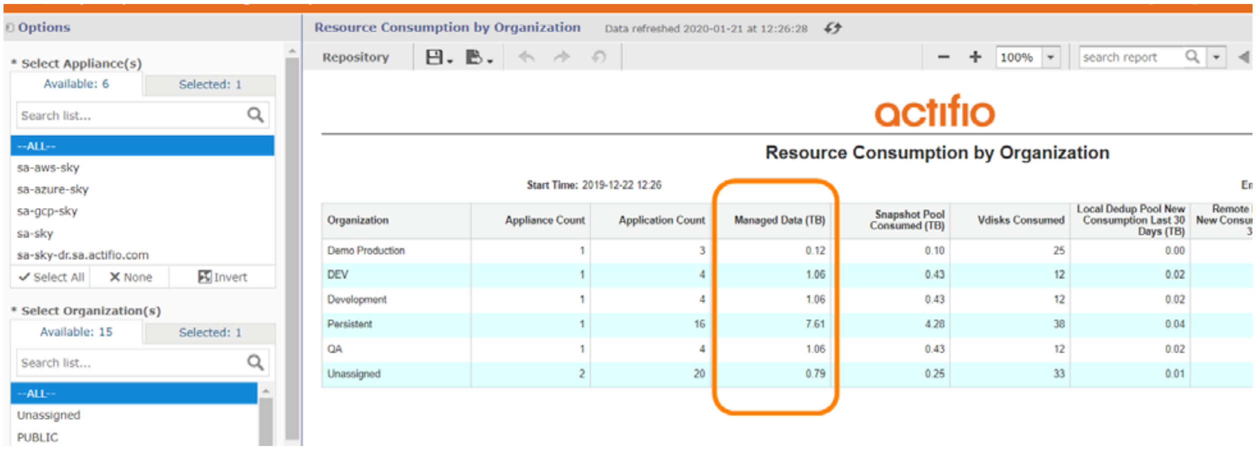
Figure 6 Data Traffic Isolation for Tenants

Tenant specific reporting for chargeback

A critical component of Cloud Service Provider business model relies on proper chargeback to customers. Actifio Report Manager provides the ability to measure resource utilization across multiple customer deployments and Actifio appliances, leveraging organization information. The following reports are typically used in such an environment for tenant chargeback and other reporting:

- SLA reports per tenant
- MDL consumption report that gives the total amount of Managed Data License consumed per tenant
- Storage Pool and other resource consumption details such as VDisks per tenant's application
- Job success and failures per tenant
- Historical data on storage pool consumption
- Replication reports, including bandwidth consumption per appliance/tenant

Note: *Not all organizational information is synchronized between AGM and the appliances for reporting purposes in the Standalone Report Manager. If Report Manager is a component of AGM (runs in the same VM), it will use the organization membership information from AGM instead of that provided by the appliances. In this case, the report will have correct data.*



Resource Consumption by Organization

Start Time: 2019-12-22 12:26

Organization	Appliance Count	Application Count	Managed Data (TB)	Snapshot Pool Consumed (TB)	Vdisks Consumed	Local Dedup Pool New Consumption Last 30 Days (TB)	Remote New Consu 3
Demo Production	1	3	0.12	0.10	25	0.00	
DEV	1	4	1.06	0.43	12	0.02	
Development	1	4	1.06	0.43	12	0.02	
Persistent	1	16	7.61	4.28	38	0.04	
QA	1	4	1.06	0.43	12	0.02	
Unassigned	2	20	0.79	0.25	33	0.01	

Figure 7 MDL Consumption by Organization/Tenant

Writing multi-tenant cloud portals using Actifio Foresight APIs

The Actifio Foresight platform allows third party portal development to customize and manage an Actifio environment at service providers. Capabilities to manage storage pools, resource profiles, SLA definition and management, data capture, manage and use lifecycle, replication pairing of appliances, users and their roles and rights are all exposed using a fine grained API which can be used from any RESTful capable portal development system at the service provider. Some service providers might want to even extend the Actifio organization capabilities in their portal system to better manage tenants as part of their IaaS infrastructure provisioning.

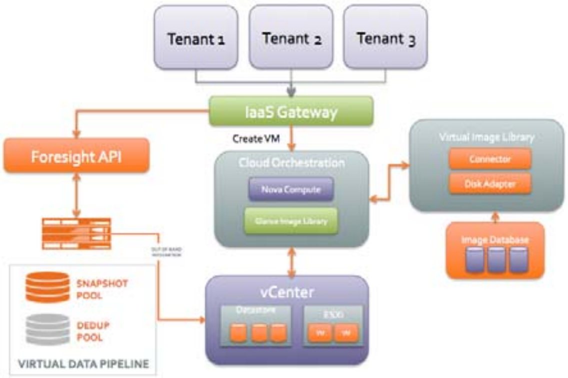


Figure 8 Integrating Foresight Into a Multi-tenant Portal

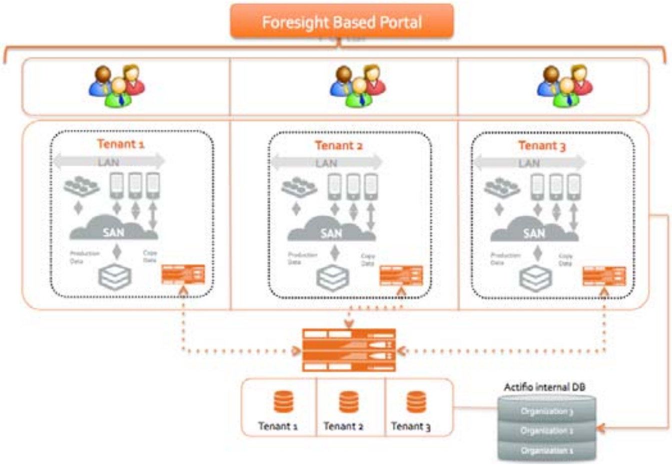


Figure 9 Managing Multiple Tenants using the Foresight Platform

Summary

Today's Cloud Service Provider (CSP) deployments are architecturally demanding. CSPs on the one hand want to deploy flexible solutions that satisfy many of their customers needs but on the other hand need an easier chargeback mechanism. Actifio offers a flexible architecture depending on the requirements of the CSPs as well as their end customers. Actifio enables multiple levels of tenant isolation and separation; isolation at the storage layer; separation of access per tenancy; filtering of reports per tenant for chargeback; and has the capabilities to adapt to different customer network demands.

CSPs need to go through a decision process to evaluate the best deployment architecture depending on their customer data size, their use cases, network capabilities as well as CSP datacenter and operations capabilities. Actifio Solution Architects can help in that process, sharing Actifio's experience and best practices.

12 Data Security

All components of the Actifio Virtual Data Pipeline have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

This chapter describes:

Secure Operating System Access to Actifio Appliances on page 53

Actifio VDP in a vSphere Environment on page 53

Internet Protocol (IP) Network Security on page 54

Access Control on Actifio Systems on page 55

Authentication and Authorization on page 56

Actifio Secure Connectivity and Data Movement with iSCSI in the Public Cloud on page 56

Access Logging and Auditing on page 56

Data Encryption on page 57

Command Line (CLI) Access to Actifio VDP on page 58

Vulnerabilities with Actifio VDP on page 58

The Actifio Connector on page 59

Secure Operating System Access to Actifio Appliances

Actifio systems run on a hardened Linux software stack. Linux user accounts and direct access to the operating system are not required nor employed for normal operations and support of the Actifio systems. Direct access to the operating system can only be obtained via the use of time and system-limited cryptographic credentials obtainable by select users within Actifio support and engineering who have been undergone extensive background checks. Certificates are stamped with the identity of the user to whom they are issued, the issuing is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. Actifio employs a locked-down operating system that minimizes the possibility of unauthorized access. Even privileged users with direct access to the appliance’s operating system can not access customer data unless they have access to a host on the storage fabric which can mount and understand the data.

Actifio VDP in a vSphere Environment

When Actifio VDP is deployed on a public cloud, the instance itself is protected by the cloud's security architecture. When deployed in an on-premises vSphere environment, the security of the instance is dependent on the configuration of the vSphere environment which hosts it. Insufficient security controls of the vSphere environment could allow an attacker to perform a side-channel or side-loading attack and gain unauthorized access to data or privileges on the Actifio Appliance(s).

While specific vSphere hardening is outside of the scope of this document, Actifio recommends customers follow VMware's best practices including, but not limited to, ensuring that the server BIOS and firmware be kept up-to-date along with the ESXi and vCenter versions to mitigate the "Meltdown/Spectre" class of side-channel vulnerabilities. Additionally, virtual machine encryption (available in vSphere 6.5+), can mitigate unauthorized tampering or side-loading of the Actifio Appliance(s) virtual disks. Customers should consult with their internal IT and/or security teams, VMware, or other resources with regard to security of a vSphere environment.

Internet Protocol (IP) Network Security

All components of Actifio VDP have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

Standard Network Services

The following services are deployed and listening on open network ports:

- HTTP (80): Actifio Appliance resource center, provides local downloads of the Connector software. No appliance control or data access is possible on this portal.
- HTTPS (443): Provides TLS-encrypted communication between AGM and the appliance, as well as some appliance-to-appliance communication. SSL certificates may be customer replaced.
- ssh (22): for user CLI
- ssh (26): for support CLI
- Actifio replication (5103): encrypted appliance-to-appliance data replication traffic. Both sides of this link utilize strong mutual authentication of the partner appliance.
- iSCSI, iSNS (3260, 3205): iSCSI target

Appliance Outbound Connections

The appliance may make outbound connections to the following services, but not does not listen on or run a service for these ports unless listed above:

- LDAP/LDAPS (389/tcp, 636/tcp) Authentication of users against a central directory if configured
- DNS (53/udp) Resolution of addresses for hosts, VMs, vCenters, and other infrastructure
- NTP (udp/123) Clock synchronization against a customer-provided or public source
- SMTP (25/tcp, 465/tcp) Optional transmission of events via a customer-provided SMTP email relay server, can optionally utilize SSL encryption.
- SNMP (162/udp) Optional delivery of events in the form of SNMP traps to a trap receiver
- vSphere API (443/tcp) Required to communicate with vCenter servers and ESX hosts for snapshot and image management during backup and mounts over an encrypted link.
- ESXi data connectivity (902/tcp) Encrypted connectivity to VMware ESXi hosts for data movement operations.
- Actifio Connectors (5106/tcp) Encrypted control channel between Actifio Appliance and hosts running the Actifio Connector.
- Appliance-to-appliance Replication (5103/tcp, 5107/tcp) Encrypted replication data and control between two Actifio Appliances.
- SecureConnect (optional feature) remote support (1194/udp, 443/tcp) Encrypted remote support access to Actifio Connector data centers. As the connection is mutually authenticated with strong cryptography, it is recommended that the destination not be limited by a firewall.

SNMP

Most SNMP code on Actifio Appliances is outgoing only, sending traps to a configured receiver to notify events and failures.

A list of allowlisted IPs can be viewed with the following commands. Currently SNMP v1 and v2 are supported.

```
udsinfo
lsmonitoreddevice
id
name
type
address
5847
Brocade--SAN
switch
X.X.X.X
5850
DS3512--A
storage
X.X.X.X
5852
DS3512--B
storage
X.X.X.X
```

No Actifio configuration will ever accept any SNMP walk or write (e.g. GetRequest, SetRequest, GetNextRequest, GetBulkRequest) and this configuration of community names is not required or supported.

Cross Cluster Communication and Replication

All Actifio Appliances utilize strong mutual authentication of the partner appliance with verification of 2048-bit RSA public keys.

Once authenticated, data in flight between appliances is encrypted using 256-bit AES encryption with session keys protected by Diffie-Hellman algorithms affording Perfect Forward Secrecy (PFS) over a TLS v1.2 channel.

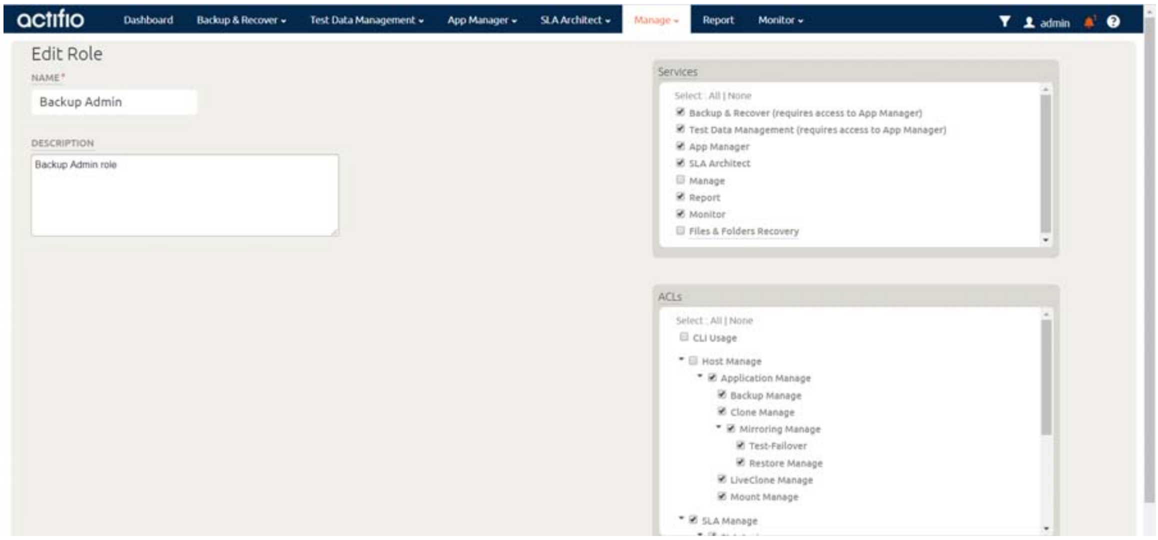
Access Control on Actifio Systems

Actifio Connector uses a very rich role-based access control mechanism that allows an administrator to assign rights to users to operate on objects. These users and rights are constrained to operating on objects owned by 'Organizations' of which they are members.

A role consists of a group of rights. Roles are assigned to users to use those rights on specific objects.

Users, Roles, Rights, and Organizations can all be modified and managed from either the CLI or the AGM.

Coupled together, roles and organizations allow the customer to define a specific group of servers/hosts/applications that a given user can perform specific actions on.



Edit Role

NAME*

Backup Admin

DESCRIPTION

Backup Admin role

Services

Select : All | None

- ☑ Backup & Recover (requires access to App Manager)
- ☑ Test Data Management (requires access to App Manager)
- ☑ App Manager
- ☑ SLA Architect
- □ Manage
- ☑ Report
- ☑ Monitor
- □ Files & Folders Recovery

ACLs

Select : All | None

- □ CLI Usage
- □ Host Manage
  - ☑ Application Manage
    - ☑ Backup Manage
    - ☑ Clone Manage
    - ☑ Mirroring Manage
      - ☑ Test-Failover
      - ☑ Restore Manage
    - ☑ LiveClone Manage
    - ☑ Mount Manage
- ☑ SLA Manage

A Role Called Backup Admin

Authentication and Authorization

Actifio Appliance can either utilize an internal user directory or integrate with an external LDAP source, including Active Directory. This allows users to leverage their existing usernames and passwords, ensuring compliance with corporate password standards such as complexity and expiration. SSL encryption may optionally be utilized between the Actifio Appliance and the external LDAP server. LDAP/ AD groups may be mapped to specific user-defined roles within the appliance.

Access Logging and Auditing

Actifio maintains a full audit log of every command that has been executed on the platform, including logging requester's IP address and method of access (CLI or AGM). The audit log can also be retrieved via the Actifio REST API for automatic ingestion into a central log or event correlation repository.
The audit log can be viewed from the CLI using the following command:

```
sa--hq1:~
$
udsinfo
lsaudit
id username stat status component issuedate proxy command ipaddress privileged
172675 admin 0 UI 13/12/2013 03:24:13.707 loginadmin 192.168.225.2 true
172675 admin 0 CLI 13/12/2013 03:24:25.707 loginadmin 192.168.225.2 true
172676 admin 0 UI 13/12/2013 03:24:14.124 lsprincipaldata1 192.168.225.2 false
172677 admin 0 CLI 13/12/2013 03:24:26.578 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2 false
172678 admin 0 CLI 13/12/2013 03:24:28.469 lsdiskpooldatamdiskgrpLIKE'act_pri% 192.168.225.2 false
172679 admin 0 UI 13/12/2013 03:24:18.737 lsdiskpooldatamdiskgrpLIKE'act_per% 192.168.225.2 false
172680 admin 0 UI 13/12/2013 03:24:19.037 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2 false
172681 admin 0 UI 13/12/2013 03:24:24.579 appgroupingregular 192.168.225.2 false
172682 admin 0 UI 13/12/2013 03:24:25.384 appgroupingremote 192.168.225.2 false
172683 admin 0 UI 13/12/2013 03:24:25.900 appgroupingorphan 192.168.225.2 false
```

Actifio Secure Connectivity and Data Movement with iSCSI in the Public Cloud

When Actifio Connector is deployed in the public cloud, iSCSI is utilized to transfer data between instances and the Actifio Appliance(s). Actifio establishes in-depth secure data transfer at multiple levels to ensure that no Connector-equipped Host or Appliance can access unauthorized data.

Both appliance(s) and instances should communicate over the provider's private network, using non-routable IP addresses, so the traffic is protected by the provider's software-defined network and subject to all the protections and external accreditations (e.g. SOC2 and ISO27001) public cloud providers offer.

Actifio also recommends:

- Firewall rules at the Public Cloud level that restrict iSCSI and/or control channel communication (5106/TCP) between the authorized appliance(s) to authorized instances only.
- Enable bi-directional iSCSI authentication (CHAP) utilizing pre-shared secrets known to both the appliance(s) and the authorized instances before any data can be accessed.
- Install the appliance certificate(s) in the Connector's trusted certificate directory on each instance.
- Some providers automatically encrypt all data at-rest (e.g. Google Cloud). On public clouds where such encryption is optional (e.g. EBS encryption on Amazon Web Services), it should be enabled to protect the appliance(s) virtual disks.

When properly configured, multiple levels of cryptographic authentication and security protect both the control and data movement channels. Additionally, only instances that have been pre-registered with the appliance(s) will be able to access data. All data operations are subject to the appliance(s) Role Based Access Control (RBAC) that validate that a user is authorized to perform a certain operation, with certain data, on a specific instance or host.

Data Encryption

Actifio Sky can be configured with optional storage pool encryption. This must be enabled at installation time. If configured, the appliance will encrypt the local storage pools (Primary and Snapshot) with AES-256 and requires an additional virtual CPU to offset the performance impact. The encryption keys are stored on the appliance's boot volume, which depending on the configuration may or may not be co-resident with the protected data. Customers are responsible for evaluating their own enterprise security requirements and policies.

Encryption In Flight

Data inflight traveling between Actifio Appliances and to OnVault, as well as SecureConnect remote support sessions, is encrypted in flight using AES-256 with session keys exchanged via Diffie-Hellman.

Management (GUI or CLI) sessions are protected utilizing the highest cipher negotiated between the client computer and the Actifio Appliance.

Data traveling between Actifio and VMware environments is protected using the strongest cipher negotiated between the Actifio Appliance and VMware ESXi/vCenter hosts up to and including AES-256.

For hosts protected using the Actifio Connector, the control channel between the appliance and the host is encrypted utilizing TLS and strongest cipher negotiated between the host and the appliance, however data movement occurs over iSCSI, which is not encrypted. If sensitive data is being transmitted via this mechanism it is recommended that this traffic be isolated to a given VLAN or subnet, or configured to use Fibre Channel, so that it cannot be intercepted. Traffic between an appliance and a host over iSCSI is not encrypted in flight.

Encryption At Rest

Administrative end-user credentials are hashed with a strong one-way salted SHA256 hash in the appliance database. Credentials used by the appliance to access other systems (vCenters, databases, etc) are stored in an AES256 encrypted form.

Sky Appliances encrypt customer data utilizing AES 256-bit encryption.

Command Line (CLI) Access to Actifio VDP

Following the security principle of separation of duties, Actifio uses two command line (CLI) interfaces for customer end-users and Actifio support personnel. These are described in detail below.

User CLI Access

One CLI interface is for general user access and is only accessible by users defined in the Actifio Appliance. This is accessible via an SSH based login via port 22 on either the primary cluster IP address or node IP addresses. All CLI access is via key based authentication only. This avoids the threat of brute force password attacks and social engineering of password theft.

A user must generate an SSH public key, and that public key must be installed on the user's account by an administrator before CLI access is granted.

The User CLI login allows authenticated users access to a heavily restricted shell where only Actifio-specific commands are available to be run. The full list of commands is documented in the Actifio Documentation Library available from the Actifio Resource Center on each Actifio Appliance (http://<cluster-IP>). Users (including admin) have no ability to upload and execute arbitrary binaries, nor can users escape the restricted shell to escalate their privileges.

Support CLI Access

The second CLI interface is for use by Actifio Support only. The time and system-limited login certificates required to use this service can only be acquired via a secure portal. The username of the user who generated the SSH certificate is embedded within the certificate and all actions are audited with this information allowing all activity to be positively tied to a specific individual.

Any employee granted authorization to generate these access certificates is subject to rigorous scrutiny including a background check for every individual.

The nature of this access mechanism means it's both very secure and fully traceable making it easy to identify which individuals have logged in using the support credentials and what actions they have performed.

Console CLI Access

Access to the Actifio CLI is also available the console on the Actifio Appliance. Use of this is restricted to Actifio staff who can leverage the key based login approach described above with the key loaded on a USB stick to gain a support login to the system.

Vulnerabilities with Actifio VDP

Actifio Engineering routinely monitors multiple sources for vulnerability information and makes available to all customers hotfixes to mitigate any discovered vulnerability in a component utilized by the appliance:

- Common Vulnerabilities and Exposures
- Security Focus - Vulnerabilities Search - http://www.securityfocus.com/bid
- National Vulnerabilities Database (NVD).

The Actifio Connector

The Actifio Connector is a highly optimized service that runs as root (or the system account on Windows) that accepts connections from Actifio Appliances and performs operations on the host to support backup, mount, and restore activities.

The Actifio Connector runs with elevated privileges as it performs a significant amount of low-level system functions including manipulating the SCSI bus, manipulating the LVM subsystem (where applicable), mounting/unmounting/formating volumes, loading and managing kernel modules (when change block tracking is enabled), copying any file on the host to the backup staging volume including protected OS files, accessing the MFT (on Windows NTFS), and more. As a C/C++ program, many of these operations are performed via native system calls and functions.

Because Actifio recognizes the risk of running any process as root, a significant amount of security architecture exists. The Connector utilizes statically linked libraries, it can validate with 2048-bit RSA certificates the identity of any Appliance that connects to it and reject any untrusted connections, and it has built-in "sudo"-like functionality to downgrade its privileges to other user accounts when it runs user-specified scripts or interacts with databases such as Oracle.

Classified as a backup agent by most companies, the Connector has been deployed across tens of thousands of customer systems in highly secure and regulated environments such as global financial institutions and banks, airlines, health care, and government agencies.

13 Support Resources

This includes:

Actifio Product Documentation on page 61
Using the Actifio Knowledge Base to Review Event Information on page 62
Creating and Viewing Support Cases on page 64
Actifio Remote Support on page 66

Actifio Product Documentation

Actifio GO is well documented. The AGM, Report Manager, and Resiliency Director each include comprehensive online help, and at https://docs.actifio.com you can find these helpful titles and more:

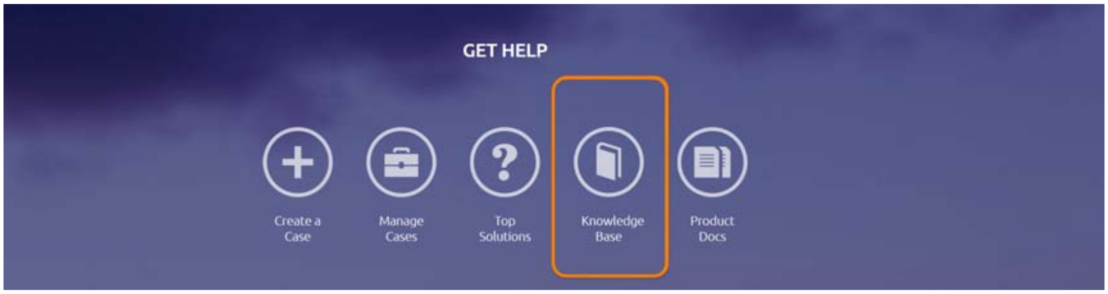
- ***Actifio Administrator's Survival Guide***
- ***Network Administrator's Guide to Actifio Copy Data Management***
- ***A VMware vCenter Administrator's Guide to Actifio VDP***
- ***Configuring Actifio OnVault***
- ***DBA Guides*** for Oracle, Microsoft SQL Server, SAP HANA, SAP ASE, SAP IQ, MaxDB, MongoDB, IBM Db2, MySQL, and MariaDB
- ***Troubleshooting Actifio Systems***
- ***Event IDs and Error Codes Reference***
- ***Release Notes***
- ***Support Matrix***

and more!

Using the Actifio Knowledge Base to Review Event Information

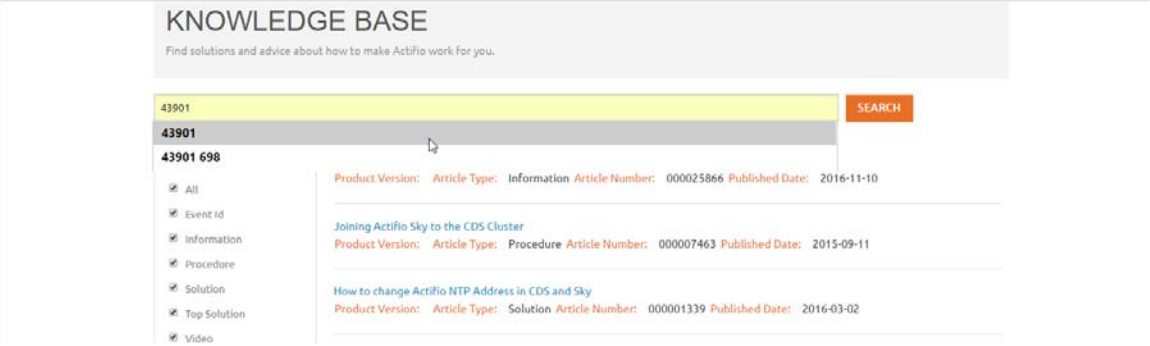
Search the Actifio Knowledge Base in the ActifioNOW customer portal for an event's meaning and resolution:

1. Go to: **https://now.actifio.com and** enter the user name and password provided by your Actifio representative, then click **Login**.
2. From the ActifioNOW portal, click **Get Help** in the banner at the top of the portal.
3. From the Get Help page, click **Knowledge Base**.



Get Help Page of the ActifioNOW Portal

4. From the Search Knowledge Base page, enter the event number and then press **Enter** on your keyboard.



KNOWLEDGE BASE

Find solutions and advice about how to make Actifio work for you.

43901 SEARCH

43901

43901 698

☑ All
☑ Event Id
☑ Information
☑ Procedure
☑ Solution
☑ Top Solution
☑ Video

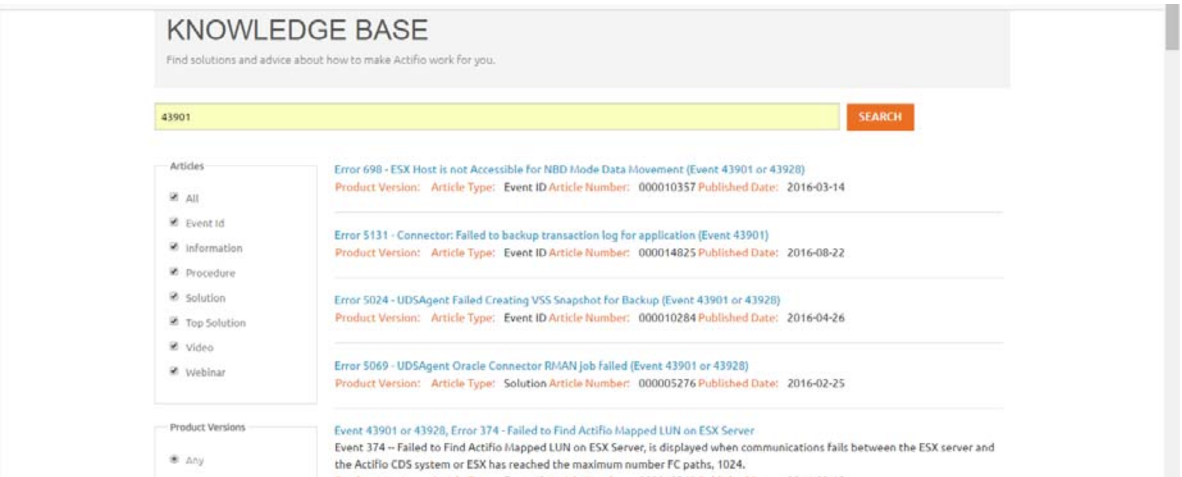
Product Version: Article Type: Information Article Number: 000025866 Published Date: 2016-11-10

Joining Actifio Sky to the CDS Cluster
Product Version: Article Type: Procedure Article Number: 000007463 Published Date: 2015-09-11

How to change Actifio NTP Address in CDS and Sky
Product Version: Article Type: Solution Article Number: 000001339 Published Date: 2016-03-02

Search Knowledge Base Page

Links to all relevant articles for the event number appear in the Search Knowledge Base page.



KNOWLEDGE BASE

Find solutions and advice about how to make Actifio work for you.

43901 SEARCH

Articles
☑ All
☑ Event Id
☑ Information
☑ Procedure
☑ Solution
☑ Top Solution
☑ Video
☑ Webinar

Product Versions
● Any

Error 698 - ESX Host is not Accessible for NBD Mode Data Movement (Event 43901 or 43928)
Product Version: Article Type: Event ID Article Number: 000010357 Published Date: 2016-03-14

Error 5131 - Connector: Failed to backup transaction log for application (Event 43901)
Product Version: Article Type: Event ID Article Number: 000014825 Published Date: 2016-08-22

Error 5024 - UDSAgent Failed Creating VSS Snapshot for Backup (Event 43901 or 43928)
Product Version: Article Type: Event ID Article Number: 000010284 Published Date: 2016-04-26

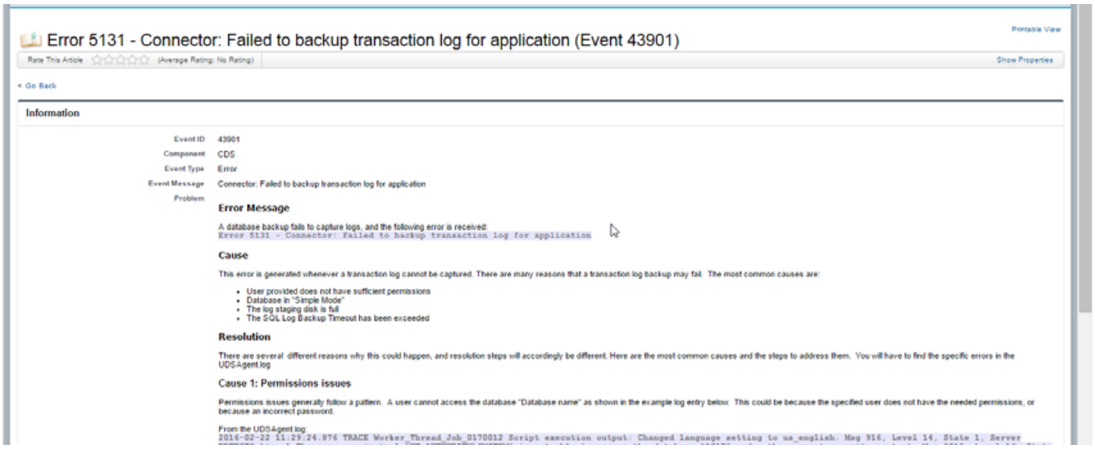
Error 5069 - UDSAgent Oracle Connector RMAN Job failed (Event 43901 or 43928)
Product Version: Article Type: Solution Article Number: 000005276 Published Date: 2016-02-25

Event 43901 or 43928, Error 374 - Failed to Find Actifio Mapped LUN on ESX Server
Event 374 -- Failed to Find Actifio Mapped LUN on ESX Server, is displayed when communications fails between the ESX server and the Actifio CDS system or ESX has reached the maximum number FC paths, 1024.

Summary of Search Results in the Search Knowledge Base Page

Note: *In the left sidebar there are filters that you can use to limit the search results. If you get many results, deselect Articles of all types except Event ID.*

5. Select a relevant Knowledge Base article and review the information for the specified event ID.



Error 5131 - Connector: Failed to backup transaction log for application (Event 43901)

Event ID	43901
Component	CDS
Event Type	Error
Event Message	Connector: Failed to backup transaction log for application
Problem	

Error Message

A database backup fails to capture logs, and the following error is received:

```
Error 5131 - Connector: Failed to backup transaction log for application
```

Cause

This error is generated whenever a transaction log cannot be captured. There are many reasons that a transaction log backup may fail. The most common causes are:

- User provided does not have sufficient permissions
- Database in "Simple Mode"
- The log staging disk is full
- The SQL Log Backup Timeout has been exceeded

Resolution

There are several different reasons why this could happen, and resolution steps will accordingly be different. Here are the most common causes and the steps to address them. You will have to find the specific errors in the UDSAgent.log

Cause 1: Permissions issues

Permissions issues generally follow a pattern. A user cannot access the database "Database name" as shown in the example log entry below. This could be because the specified user does not have the needed permissions, or because an incorrect password.

From the UDSAgent.log:

```
2016-02-22 11:29:24.876 TRACE Worker_Thread_Job_0170012 Script execution output: Changed language setting to us_english. Msg 916, Level 14, State 1, Server
```

A Sample Knowledge Base Entry for a Job Failure Event

Creating and Viewing Support Cases

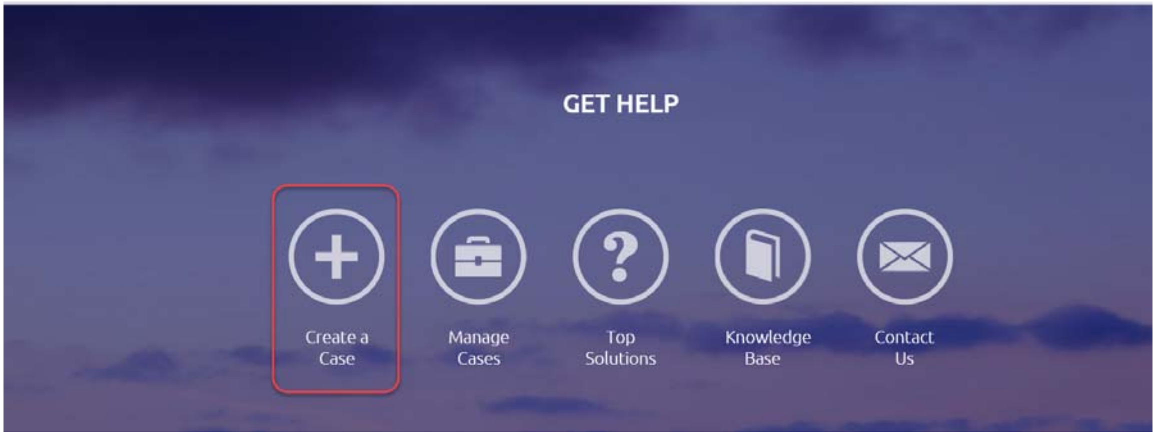
If there are issues that you cannot resolve, open a support case from the ActifioNOW customer portal, Depending the severity of the case, an Actifio support case may be auto-generated for you.

If you need to contact an Actifio support representative, you can call:

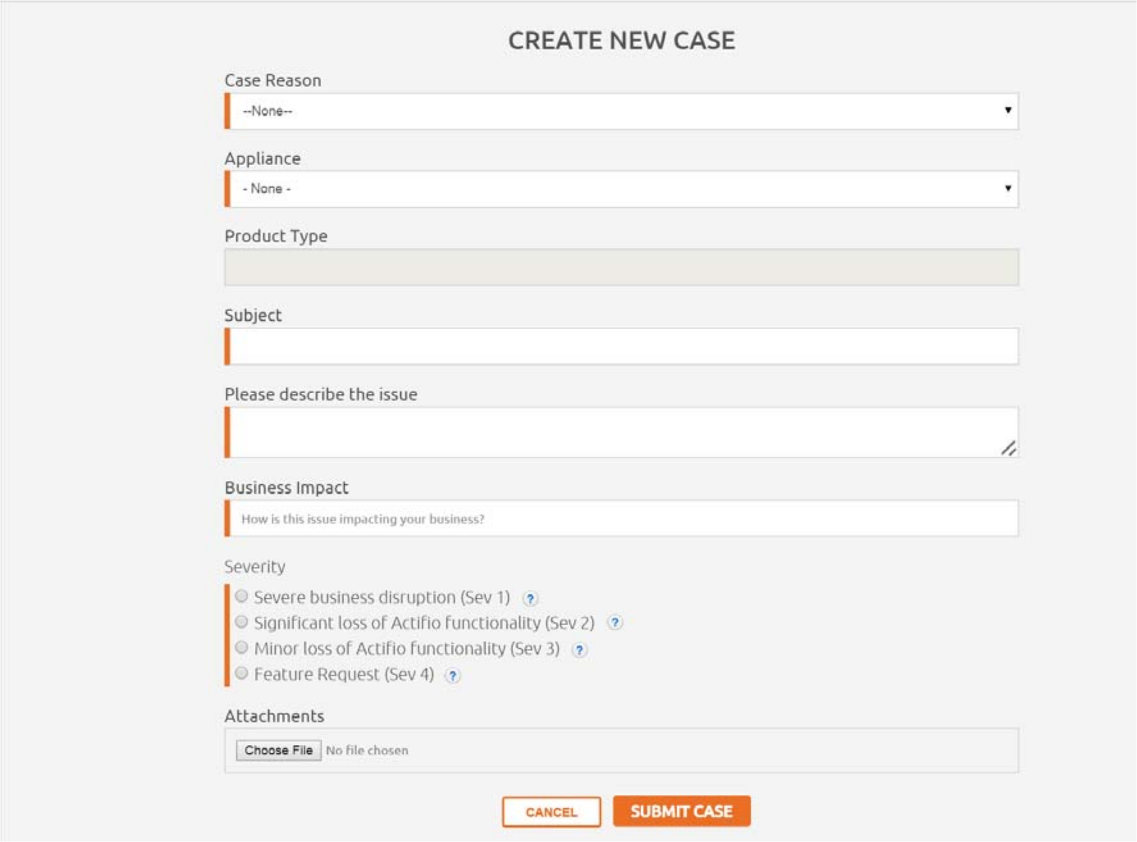
From anywhere: +1.315.261.7501
US Toll-Free: +1.855.392.6810
Australia: 0011 800-16165656
Germany: 00 800-16165656
New Zealand: 00 800-16165656
UK: 0 800-0155019

To log a case with Actifio Support and view case information related to an open case:

1. Log into the ActifioNOW customer portal at: https://now.actifio.com/.
2. From the ActifioNOW portal, click **Get Help** in the banner at the top of the portal.
3. From the Get Help page, click **Create a Case**.



4. From the Create New Case page, fill in the form as required for the issue you are experiencing. Click **Submit Case** when you are done. Your case is created and sent to Actifio Support, and you return to the Get Help page.



CREATE NEW CASE

Case Reason

--None--

Appliance

- None -

Product Type

Subject

Please describe the issue

Business Impact

How is this issue impacting your business?

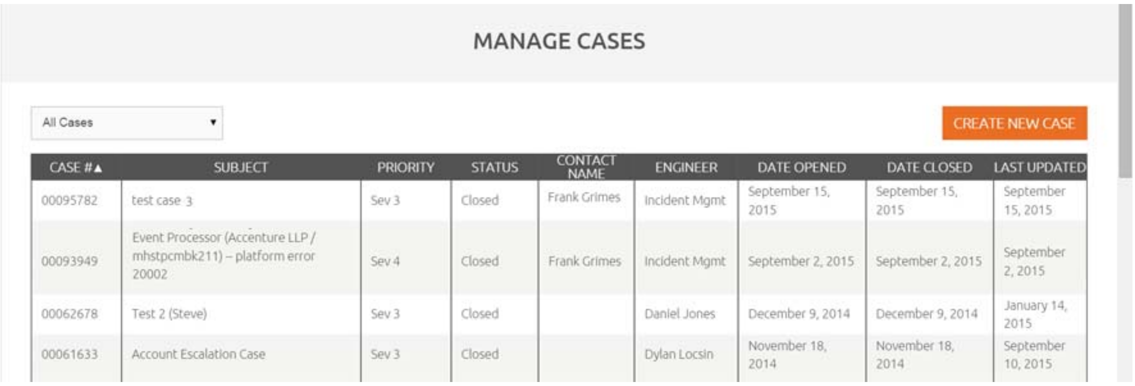
Severity

○ Severe business disruption (Sev 1) ?
○ Significant loss of Actifio functionality (Sev 2) ?
○ Minor loss of Actifio functionality (Sev 3) ?
○ Feature Request (Sev 4) ?

Attachments

Choose File No file chosen

5. To review information about your case, or other existing cases, from the Get Help page, click **Manage Cases**. The Manage Cases page appears. You can also create a new case from the Manage Cases page.



MANAGE CASES

All Cases

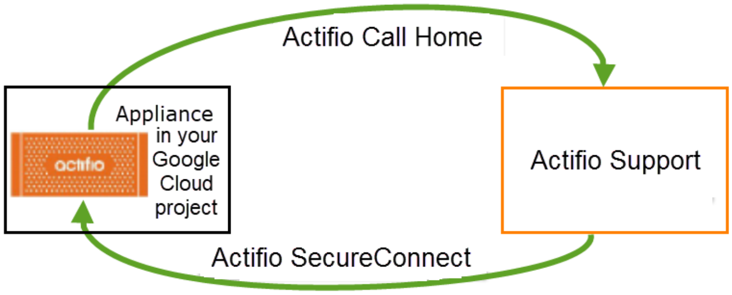
CASE #▲	SUBJECT	PRIORITY	STATUS	CONTACT NAME	ENGINEER	DATE OPENED	DATE CLOSED	LAST UPDATED
00095782	test case 3	Sev 3	Closed	Frank Grimes	Incident Mgmt	September 15, 2015	September 15, 2015	September 15, 2015
00093949	Event Processor (Accenture LLP / mhstpcmbk211) – platform error 20002	Sev 4	Closed	Frank Grimes	Incident Mgmt	September 2, 2015	September 2, 2015	September 2, 2015
00062678	Test 2 (Steve)	Sev 3	Closed		Daniel Jones	December 9, 2014	December 9, 2014	January 14, 2015
00061633	Account Escalation Case	Sev 3	Closed		Dylan Locsin	November 18, 2014	November 18, 2014	September 10, 2015

Actifio Remote Support

Actifio offers two optional remote support features:

Call Home remote event notification: When you enable the Actifio Call Home feature, your Actifio Appliance sends alerts and other diagnostic data to Actifio. Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you.
Actifio Call Home is detailed in Actifio Call Home Remote Event Notification.

SecureConnect remote service access: When you enable Actifio SecureConnect, Actifio Customer Support engineers can access your system remotely on an as-needed basis. Once you enable SecureConnect, Customer Success Engineering will have the ability to access your appliance until you disable it. As a situation requires, they can manage major upgrades and service pack updates and hotfixes, phase out failing hardware, collect log data on history of failures, restart data and I/O modules, change the configuration of ports, and more. All actions are documented in the Actifio Appliance audit log and in the Actifio installation/problem reporting databases for further review. Actifio SecureConnect is detailed in Actifio SecureConnect on page 67.



Actifio Call Home and Actifio SecureConnect

Actifio Call Home Remote Event Notification

Actifio Call Home sends an email to Actifio Customer Support every six hours. In the event of a problem, Actifio Support can refer to this information to minimize time to recovery. The email includes these statistics:

- Actifio Appliance version information
- Uptime of the Actifio Appliance
- Status check of services
- Process summary
- Logs of various processes
- Failed jobs and total jobs
- Storage pool statistics

Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you. Due to the redundant design of an Actifio Appliance, most alerts do not require immediate service attention.

Can I Enable Call Home Without Enabling SecureConnect?

Yes. Call Home provides data, and SecureConnect provides access. Enabling Call Home without enabling SecureConnect ensures that Actifio Customer Support has excellent monitoring, alerting, and analytics data, without the access that might be needed to perform further diagnostics or remediation. The data lets Actifio Customer Support know when a problem has occurred and prepare a response if needed, but investigation and troubleshooting has to be performed online or via conference call.

Most investigations require additional data to be gathered from the appliance, and without SecureConnect, the cycle of gather-analyze-followup-analyze can become cumbersome.

Call-Home Network Requirements

Actifio Call-Home requires a TCP connection on port 25.

Configuring Actifio Call Home

To send Actifio Appliance statistics to Actifio Support every 6 hours, refer to the AGM online help, reachable from the **?** icon in the top right corner of the AGM.

Actifio SecureConnect

Actifio SecureConnect is a secure method for remote support that employs dedicated ports and encrypted data. These built-in security features greatly reduce the risks associated with a connection to an external network. The SecureConnect protocol allows Actifio Customer Support engineers to access your system on an as-needed basis to manage cases and updates while meeting your SLA requirements.

Your Actifio account team is kept up to date on a repair status as the case progresses. If hardware replacement is required, parts & local support are shipped to the site and an Actifio Services engineer is dispatched to handle the installation. When the incident is resolved to your satisfaction, the Actifio Customer Support engineer logs out of your Actifio Appliance, disconnects from the remote access line, and creates a summary report of problem root cause and repair actions that is delivered to your account team and to you.

Advantages to using Actifio SecureConnect include:

- **Accelerated problem solving**: By leveraging Actifio follow-the-sun support, you can resolve problems without extending the wait time that invariably gets generated by relying on log files, dumps, and traces being transmitted across the globe.
- **Fine-grained monitoring and collaboration**: You can monitor remote support activities and join in conference calls with Actifio Customer Support engineers as the problem determination process proceeds.
- **Real-time learning**: Remote Actifio Customer Support engineers provide you with ongoing assistance in the setup, configuration, and management of your Actifio Appliances.

Without SecureConnect enabled, you can still contact Actifio Customer Support. Actifio support engineers can work with you via WebEx and other remote support tools for log file gathering and other forensics to help resolve the issue.

Can I Enable SecureConnect Without Enabling Call Home?

Yes. Call Home provides data, and SecureConnect provides access. Enabling SecureConnect without enabling Call Home allows Actifio Customer Support engineers to respond and investigate issues after you tell us a problem exists. Without Call Home, Actifio Customer Support has no way to know of problems with your system. There is no proactive data collection associated with activating SecureConnect.

How SecureConnect Works

SecureConnect uses client/server architecture. The SecureConnect client comes built into your Actifio Appliances, to be enabled and disabled by you.

After you enable the connection, your Actifio Appliance establishes a secure point-to-point connection to a secure server at the Actifio Global Support Center, enabling remote access from the Actifio Global Support Center to your Actifio Appliance. You must configure a firewall rule to allow the Actifio Appliance to connect to Actifio Support over UDP on port 1194.

As a client connection, SecureConnect does not bridge networks or perform any form of routing. Connections initiated at the Actifio Global Support Center communicate with your Actifio Appliance and no other systems on your network.

How Secure Is Actifio SecureConnect?

SecureConnect utilizes 2048-bit RSA cryptography for strong mutual authentication and encryption, 256-bit AES for encryption of data in flight, and Diffie-Hellman for Perfect Forward Secrecy (PFS) key exchange. Each connection is a point-to-point link and none of your equipment can access another endpoint. Intrusion detection software continually monitors the connection for any anomalous activity. Authentication records are replicated in real-time to off-site locations. The SecureConnect servers are routinely monitored for emerging threats and vulnerabilities.

Only select users within the support and engineering organizations are authorized with this level of access. Actifio employees who have a business need to access your systems must pass a third-party background check and sign a security, compliance, and confidentiality agreement. Access is reviewed annually and terminated immediately in the event of separation or role change. Authorized employees authenticate to SecureConnect with a 2048-bit X.509 certificate stamped with the identity of the user. A two-factor challenge is required after cryptographic authentication in the form of a smart phone push or code-generating token. The certificate must be renewed annually. Issuance is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. The VPN connection is protected using NIST-approved strong cryptography including AES-256 data encryption.

No Access to Your Business Data

Appliance service credentials are completely independent from SecureConnect and are generated on entirely separate systems. To gain access to a customer system, an Actifio Support staff member generates a time-limited, passphrase-protected authentication token which is locked specifically to the machine they have been granted access to log into. The system generating these tokens is on a secure network separate from the SecureConnect network and itself authenticates against a robust corporate directory. The ability to generate authentication tokens is limited to Actifio Support staff members who have been approved by a rigorous screening process.

Actifio SecureConnect Network Requirements

Actifio SecureConnect is a strong 2048-bit RSA mutually authenticated service not subject to redirection or man-in-the-middle attacks. SecureConnect requires a UDP connection over port 1194 **from** the Sky Appliance IP address **to** secureconnect2.actifio.com and a setting of “any” IP address. If you cannot use ‘any’, then contact Actifio Support.

Enabling Actifio SecureConnect

To enable SecureConnect mode, refer to the AGM online help, reachable from the **?** icon in the top right corner of the AGM.

14 Glossary

A | B | C | D | E | F | G | H | I-K | L | M-N | O | P-Q | R | S-T | U | V | W-Z

	Term	Definition
A	**Actifio Connector**	The Actifio Connector is a lightweight service that may be run on physical or virtual appliances. It discovers and captures individual applications, virtual and physical machines and servers so they can be replicated.
	Actifio Global Manager	The Actifio Global Manager (AGM) provides a web-based interface to manage multiple Actifio Appliances, including day-to-day copy data operations.
	ActifioGO	ActifioGO is a SaaS platform for VM, physical, and database backup and recovery to Google Cloud. Enterprises can use the ActifioGO SaaS platform to deliver cloud-based backup and recovery for on-premises and cloud workloads.
	ActifioNOW	The Actifio user portal, with product documentation, knowledge base, videos, training resources and more at http://now.actifio.com.
	Actifio Sky Appliance™	Actifio Sky Appliance is a robust virtual appliance built on Actifio's patented Virtual Data Pipeline™ (VDP). Actifio Sky Appliance offers deployment flexibility and range. As a virtual appliance, Actifio Sky Appliance can be deployed in minutes at any site across an organization's locations and environments.
	AGM	See Actifio Global Manager.
	App or Application	An app or application is a data resource that can be discovered and protected by an Actifio Appliance. Examples include Oracle or SQL databases, network or local file systems or parts of file systems, virtual machines, and so on.
	Application Aware mount	See Virtual Application.
	Appliance	An "appliance" is the generic term for the Actifio Sky Appliance.
	App Manager	The App Manager is used to discover applications, application data, and virtual machines, and to apply protection templates and resource profiles to them.
B	**Baseboard System Identification**	The base board system identifier (BBSID) is an arbitrary unique number that becomes part of a unique suffix for a node's World Wide Node Number and World Wide Port Number. These both must be unique within a fabric.
	BBSID	Baseboard System Identification
C	**CBT**	Changed Block Tracking.

	Term	Definition
	Changed Block Tracking	Changed block tracking is the process of comparing the golden snapshot to incremental point in time snapshots in order to identify changed data that must be preserved.
	CLI	Command line interface.
	Clone	The clone function creates an independent copy of a data set. A virtual server or physical server data set can be copied from any application-consistent point in the system to a separate storage location anywhere in the environment.
	Clone VDisks	Clone VDisks, are the part of a Snapshot pool that contains full copies of an application's production data.
	Connector	See Actifio Connector.
	Consistency Group	A group of storage resources protected as a single entity by an Actifio Appliance.
	Copy Data Virtualization	Copy Data Virtualization is the Actifio data management model — capture data and process it in a virtual data pipeline to create a single golden master copy that is incrementally updated according to a service level agreement (SLA) and is used to generate a virtual copy of any application data from any point in time for any authorized use.
D		
E	**External Snapshot Pool**	Actifio has extended its Virtual Data Pipeline to use and manage external snapshot pools using with IBM Storwize/SVC and Pure FlashStorage. You can use the array native snapshots for Actifio's snapshot pool, gaining the storage arrays' performance, connectivity, and availability.
F	**Failback**	Failback is the recovery process used when a primary system or data is restored to operation after a Failover. Also see Syncback.
	Failover	The process of using a secondary system, usually hardware, to replace a primary system that fails during operation. Also used to describe the data copied when a failover occurs. See Failback and Syncback.
	Filter Driver	The mechanism used by the Actifio Connector for Changed Block Tracking.
G	**Generic Application**	Most applications are discovered through the Actifio Connector or through various APIs built into Actifio VDP. A generic application is an application that you define it by pointing to a group of volumes to be protected. AGM can protect LVM-based generic applications.
H	**Host**	A server with managed or manageable applications.
I-K	**Immutability**	You can use policy settings to make a backup image immutable. An immutable image cannot be expired by any user until it reaches a date set in the policy.
	iSCSI	The Internet Small Computer System Interface works on top of the Transport Control Protocol (TCP) and allows the SCSI command to be sent end-to-end over local-area networks (LANs), wide-area networks (WANs) or the Internet.
L		

	Term	Definition
	LiveClone	An independent clone of a captured image that consumes full storage resources and can be mounted to a host. It can be refreshed incrementally from another captured image, allowing very fast and efficient data refreshes for ETL and test & development purposes. A LiveClone can also be mounted for direct modification to support operations such as data masking.
M-N		
	Managed Disk	A SCSI disk presented by a RAID controller and managed by the Actifio Appliance. The Managed Disk is not visible to host systems on the SAN.
	MDisk	These are disks presented to and managed by the Actifio solution.
	Monitor	A service within the Actifio Global Manager that monitors the progress of jobs.
	Mount	The mount function is the most frequently used data access method, as it directly leverages the virtual copies of data stored on an Actifio Appliance. By eliminating the data movement from the process, data sets of any size can be accessed instantly on any server.
	Multi-Hop replication	Replication is the process that replicates data from a "source" Actifio Appliance to a "remote" Actifio Appliance, and then from the remote appliance to a third Actifio Appliance.
O	**OnVault**	The Actifio Appliance vaults data to selected Google Cloud storage according to a defined OnVault policy. Users manage and pay for their own cloud storage directly with the provider.
	Out-of-Band	Out-of-Band is a network architecture describing protected applications that are housed on storage systems that are not connected directly to Actifio storage..
P-Q	**Performance pool**	The Snapshot pool.
	Policy	A policy defines when data will be captured, how long it will be retained, and where it will be replicated.
	Policy template	A collection of policies that, together, define when to perform a snapshot and how long to retain the image.
	PSRV	The platform service is a component of Actifio VDP software that coordinates other VDP services and functions.
R	**RD**	See Resiliency Director.
	ReadyVM	The CLI shorthand term for replicating a VMware VM to an ESX datastore. This is an asynchronous replication mechanism in which the data is directly replicated onto the datastore volumes that are configured for the remote VM. This lets you use an existing or a new virtual machine as the replication target.
	Report Manager	The Report Manager is an optional stand alone software package that reports on data protection and recovery operations.
	Resiliency Director	Resiliency Director is an optional product that works with Actifio Appliances to create and manage data that are part of disaster recovery services.
	Resource Profile	A resource profile specifies if, and which, Snapshot pool is used by Actifio and/or to which remote Actifio Appliance data will be replicated. A resource profile is paired with policy templates to protect a specific application by the App Manager.

	Term	Definition
	Restore	The restore function reverts the production data to look exactly as it did at the time of the data collection point. Typical use cases for restore would be to recover an entire server or application to a valid state after a massive data corruption or storage array failure.
	RM	Report Manager.
	RPO	A recovery point objective is the maximum period in which data might be lost from an IT service due to a major incident. See RTO.
	RTO	The recovery time objective is a period of time and a service level within which a business process must be restored after a disruption in order to avoid a break in business continuity. See RPO.
S-T	**SARG**	The Simple Actifio Report Generator, a command-line reporting tool documented in the ***SARG User Guide***. SARG is not the same as the Actifio Report Manager, which has a GUI.
	Service Level Agreement	An Actifio service level agreement is the linkage of a single policy template that defines when to perform actions, and a resource template that defines what storage resources are used by the actions.
	Sky Appliance	See Actifio Sky Appliance™
	SLA	See Service Level Agreement.
	Snapshot	A snapshot is the process that captures and stores the state of a Snapshot VDisk as a Snapshot VDisk.
	Snapshot pool	The snapshot pool holds "golden copies" of application data for short-term retention. Data is instantly accessible. Policies determine how long data is kept in the pool and when data is moved to another pool. The snapshot pool contains Staging VDisk, Snapshot VDisk, and Clone VDisks.
	Snapshot VDisk	A Snapshot VDisk is part of a Snapshot pool that preserves the state of Staging VDisk at specific points in time. Snapshots are retained according to a predefined protection policy.
	Staging VDisk	A Staging VDisk is part of a Snapshot pool that contains the Actifio golden copy of an application. It is retained for as long as an application is protected.
	StreamSnap	Direct replication of incremental snapshots from a local snapshot pool to a remote pool. StreamSnap keeps a full virtual copy of the application on the remote side, available for immediate failover, test failover, or mount operations.
	Syncback	Syncback is the process that verifies data that has failed over to be valid before a Failback. Also see Failover.
	System Monitor	See Monitor.
U	**UDS**	Universal data system
V	**VDisk**	Also referred to as a *volume*. See Virtual disk.
	VDP	See Virtual Data Pipeline™.
	Virtual Application	You can mount captured Microsoft SQL and Oracle databases as "Application Aware mounts", fully functional replicas of the original database. This allows you to quickly bring a database online without having to manually configure a new instance of the database and actually move the data into it.

	Term	Definition
	Virtual Data Pipeline™	Actifio's data virtualization delivers greater resilience and agility while enabling secure mobility of data to and from the cloud. By virtualizing data, creating a single "gold copy" available for instant access and use, Actifio frees application data from underlying infrastructure.
	Virtual disk	These are disks presented to applications by the Actifio solution that appear to host systems attached to the storage area network as a SCSI disk. Each VDisk is associated with one I/O group.
	VM	Virtual machine. Actifio supports VMware instances.
W-Z	**Workflow**	Actifio Workflows automate access to captured data. Workflows can run according to a schedule or on demand. Workflows present captured data as a LiveClone, a virtual application, or as just the application data.