
Replicating Data Using Actifio Appliances

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2019 Actifio, Inc. All rights reserved.

Actifio®, AnyIT®, Dedup Async®, OnVault®, Enterprise Data-as-a-Service®, FlashScan®, AppFlash DEVOPS Platform®, Copy Data Cloud®, and VDP® are registered trademarks of Actifio, Inc.

Actifio Sky™, Actifio One™, and Virtual Data Pipeline™ are trademarks of Actifio, Inc.

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

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

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

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

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

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

Contents

Preface	v
Actifio Appliances	v
The ActifioNOW Customer Portal	v
Actifio Support Centers	v
.....	v
Chapter 1 - Replication Overview	1
About Actifio Data Replication	1
Methods of Replication Between Actifio Appliances.....	2
Dedup Backup Replication.....	4
Dedup DR to Remote Replication (Multi-hop Replication)	5
Sending Snapshot Images to Storage Defined by an Actifio OnVault Pool	6
Production to Mirror Replication.....	7
Dedup Async Replication (DAR).....	7
StreamSnap Replication.....	8
Sync and Async Replication	10
Chapter 2 - Configuring Dedup Backup Replication for Long-Term Remote Storage	11
Configuring Dedup Backup Replication.....	11
Configuring Multi-hop Remote Dedup Backup Replication	15
Chapter 3 - Using Actifio OnVault Pools	19
Configuring Snapshot to OnVault Policy to Transfer Data	19
Chapter 4 - Performing Failover	23
Configuring Dedup-Async Replication for a VM to an ESX Datastore	24
Configuring Dedup-Async or StreamSnap Replication to Remote Storage.....	27
Testing Failover.....	30
Deleting Test-Failover Images	32
Failing Over a Protected Application	33
Failing Over a Protected VM	35
Chapter 5 - Restoring from a Failover Condition	41
Performing a Catch-Up Syncback.....	42
Stopping the Failed-Over Application.....	43

Performing the Final Syncback	43
Restoring a Syncback Image	44
Restoring an Application or VM Syncback Image	44
Mounting a VM Syncback Image	47
Failback to the Local Appliance	48
Deleting Failover and Syncback Images	49
Chapter 6 - Performing Synchronous and Asynchronous Replication	51
Initial Configuration Tasks Prior to Performing Sync and Async Replication	51
Configuring Synchronous Replication for In-Band Generic Applications	52
Configuring Asynchronous Replication for In-Band Generic Applications	54
Chapter 7 - StreamSnap Jobs and Error Handling	57
Index	61

Preface

This guide describes the different remote backup and disaster recovery methods supported by the Actifio CDS and Sky appliances along step-by-step instructions on their use. It assumes you have read **Getting Started with Actifio Copy Data Management**, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio appliance.

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

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

Actifio Appliances

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

The ActifioNOW Customer Portal

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

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

To log into the ActifioNOW customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:
 - From anywhere:** +1.315.261.7501
 - US Toll-Free:** +1.855.392.6810
 - Australia:** 0011 800-16165656
 - Germany:** 00 800-16165656
 - New Zealand:** 00 800-16165656
 - UK:** 0 800-0155019

1 Replication Overview

This chapter provides an overview on the different replication methods supported by Actifio CDS and Sky appliances along with general guidelines on their use. It covers the following topics:

[About Actifio Data Replication](#) on page 1

[Methods of Replication Between Actifio Appliances](#) on page 2

[Dedup Backup Replication](#) on page 4

[Sending Snapshot Images to Storage Defined by an Actifio OnVault Pool](#) on page 6

[Production to Mirror Replication](#) on page 7

About Actifio Data Replication

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.

Actifio data replication technology:

- Protects data in the event of potential loss or damage, across remote locations, data centers, and geographies. Should a disruption occur, Actifio data replication delivers rapid resumption of the access and use of that data.
- Makes the most effective use of network bandwidth by leveraging compression and deduplication technologies.
- Eliminates the need for a dedicated WAN accelerator/optimizer.
- Does not require storage array vendor licenses when data is sent from one Actifio appliance to another.
- Is heterogeneous from any supported array to any supported array: Tier 1 to Tier 2 and/or Vendor A to Vendor B.
- Preserves write-order, even across multiple LUNs in a consistency group.
- Is integrated with VMware Site Recovery Manager (SRM) and Actifio Resiliency Director.
- Encrypts data using the AES-256 encryption standard. Authentication between Actifio appliances is performed using 2048-bit RSA certificates.

Methods of Replication Between Actifio Appliances

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 defined in a resource profile. Resource profiles define where to store data. Data can be stored locally to a remote Actifio appliance to which data will be replicated, or to an Actifio OnVault Pool to which data will be sent. The method that works best for you is dependent on your environment, network, available bandwidth, and recovery requirements (RPO and RTO).

Data replication between a local and remote Actifio appliance can be implemented through a variety of different methods:

- **Data Mirroring** - 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. Data mirroring between a Production and Mirrored site is available in the following replication methods: Dedup Async, StreamSnap, Synchronous, and Asynchronous.

See [Production to Mirror Replication](#) on page 7.

- **Dedup Backup** - Dedup Backup policies use an Actifio proprietary replication engine to replicate data to a second Actifio appliance. Dedup Backup is efficient for medium to long-term storage (for example, 3 months to a year) of captured and deduplicated data to a remote Actifio appliance. In addition, a Second Hop Replication policy allows you to replicate dedup backup data to a third location operating as the second-leg in a multi-hop configuration of joined Actifio appliances. Remote dedup backup can be considered as storage optimized replication to a remote site.

See [Dedup Backup Replication](#) on page 4 and [Dedup DR to Remote Replication \(Multi-hop Replication\)](#) on page 5.

- **Snapshot to OnVault** - Snapshot to OnVault policies send data over the network to cloud object storage, typically for long-term retention with low frequency access. These policies allow you to send application and VM data to storage defined by an Actifio OnVault Pool. Typically data is retained for a year or longer.

See [Sending Snapshot Images to Storage Defined by an Actifio OnVault Pool](#) on page 6.

The following table summarizes the benefits of each method of replication supported by an Actifio appliance.

Replication Method	Recommended Use	Pros	Cons
Dedup Backup	Medium to long-term data retention offsite (for example, weeks to months)	<ul style="list-style-type: none">• Globally deduplicated• Compressed and encrypted• Most efficient bandwidth	<ul style="list-style-type: none">• Longer RTO• Data needs to be rehydrated
Snapshot to OnVault	Very long-term retention (for example, a year or longer); intended for periodic copies (for example, on a monthly basis)	<ul style="list-style-type: none">• Cost effective long-term retention• Compression reduces bandwidth consumption• Data is encrypted in-flight and, optionally, at rest	<ul style="list-style-type: none">• Long RTO• Higher bandwidth usage (as compared to Dedup Backup)• Applications can not be run in storage defined by an Actifio OnVault Pool

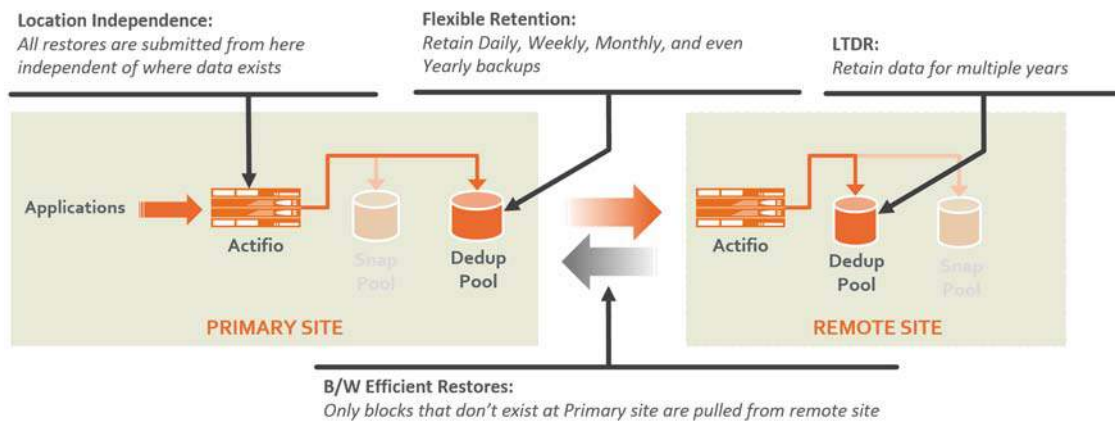
Replication Method	Recommended Use	Pros	Cons
Data Mirroring: Dedup Async	Disaster recovery for applications that do not require a short RPO	<ul style="list-style-type: none"> • Short RTO with near instant data access and failover • Globally deduplicated, compressed, and encrypted • Most efficient bandwidth 	<ul style="list-style-type: none"> • Longer RPO (24 hours typically with 8-12 hours possible)
Data Mirroring: StreamSnap	Disaster recovery for applications that require a shorter RPO	<ul style="list-style-type: none"> • RPO as short as an hour with near instant data access and failover • Compressed and encrypted • Replicates large amounts of data as well as data that is not conducive to deduplication (images, videos) • Retains snapshot images from multiple available points in time at the remote site • StreamSnap technology used for log replication between local and remote appliances 	<ul style="list-style-type: none"> • Higher bandwidth consumption
Data Mirroring: Synchronous/ Asynchronous	Storage transaction replication for near zero RPO	<ul style="list-style-type: none"> • Short RPO • Instantaneous failover of production data • Async replication has no distance limitation 	<ul style="list-style-type: none"> • Supports in-band generic apps on Actifio CDS appliance only • High bandwidth • Requires a dedicated Fibre Channel link • Distance limitation of 300KM maximum for Sync replication

Dedup Backup Replication

Dedup Backup replication is efficient for long-term storage of captured and deduplicated data to a remote Actifio appliance. Data replicated using a Dedup Backup policy is transmitted from the local Actifio appliance dedup pool to the dedup pool managed by another Actifio appliance. The need for and number of Dedup DR copies to retain on a second Actifio appliance for long-term data retention (LTDR) is driven by offsite retention requirements for the data.

Dedup Backup uses a Dedup Backup to Dedup DR policy. Dedup Backup replication is incremental, globally deduplicated, and compressed and encrypted in flight. The Dedup Backup replication process begins after the deduplication process completes. A proprietary deduplication-aware replication protocol enables the transmission of only the globally unique blocks, which minimizes the bandwidth required to move data between Actifio appliances.

Blocks are compressed and encrypted in flight for the most efficient bandwidth utilization. Deduplication and compression optimize the data set for transport between sites, eliminating the cost of WAN optimization.



Dedup Backup Replication to a Remote Site

Dedup Backup replication and Dedup Async mirroring replication (see [Dedup Async Replication \(DAR\)](#) on page 7) use the same dedup engine and dedup pool to transfer blocks of data between the local and remote sites. For example, if you are using Dedup Async replication to mirror VMs every 8 to 10 hours, and you are also running a daily dedup backup in the evenings, every 8 to 10 hours the incremental blocks will be sent across to the DR site in a globally deduplicated and compressed bit stream. When the dedup backup job starts, most of the blocks are already at the DR site so they are not sent again; only new blocks that are written between the last replication job and the backup job are sent.

To configure Dedup Backup replication for an application, see [Configuring Dedup Backup Replication](#) on page 11.

Dedup DR to Remote Replication (Multi-hop Replication)

If your long-term dedup protection needs require your data to be stored in two remote locations, a Dedup Backup and Dedup DR policy can be defined in a multi-hop replication scheme. Multi-hop replication enables you to store a deduplicated backup image from the primary Actifio appliance (site 1) to remote Actifio appliance 2 (site 2) and to remote appliance 3 (site 3).

You may require a multi-hop replication when you plan to:

- Replicate data from remote offices to a central or regional data center, and would like to replicate again to another data center for offsite retention (possibly at a service provider).
- Replicate data to a service provider data center, and the service provider wants to replicate again to another data center for extra protection.
- Replicate data for DR purposes bidirectionally between two local sites, and wish to replicate to a third, out-of-region, site.



Dedup Backup Replication Across Three Actifio Appliance Sites

To configure multi-hop replication for an application, see [Configuring Multi-hop Remote Dedup Backup Replication](#) on page 15.

Sending Snapshot Images to Storage Defined by an Actifio OnVault Pool

The Snapshot to OnVault policy defines when to send data to storage defined by an Actifio OnVault Pool, and how long the data will be retained. You can add a vaulting tier to SLA templates and the Actifio appliance will vault data to the selected cloud storage according to the defined OnVault policy. Actifio supports many popular cloud storage platforms and more are constantly being added; for more information see the OnVault section of the Actifio Documentation Library or in ActifioNOW.

The most recently completed snapshot taken by the snapshot policy is used by the Snapshot to OnVault policy. An HTTPS connection is used to ensure data security. The Actifio OnVault Pool uses a compression option to minimize network traffic.

Note: Data sent to storage defined by an Actifio OnVault Pool is not deduplicated.

An Actifio OnVault Pool defines the storage location and provides access credentials for the destination. The Actifio OnVault Pool is important in creating a Resource Profile. The combination of the Resource Profile and the Policy Template forms the SLA for the applications to which they are applied.

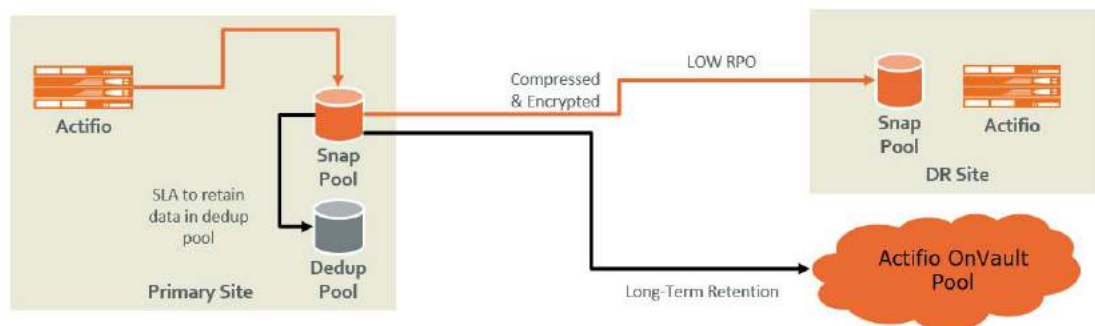
The storage location defined by an Actifio OnVault Pool is typically used for long-term retention (months to years). Applications can not be run in the storage location defined by an Actifio OnVault Pool.

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

- Actifio CDS and Sky appliances can create clones.
- Actifio Sky appliances can mount data.

Note: Mounted data can be accessed directly from a host, but it is not recommended to run workloads directly against this data.

- Actifio CDS appliances **cannot** mount data.
- LiveClones cannot be created.
- Actifio Application Aware mounts are not supported.



Actifio OnVault Pool Storage

To configure Snapshot to OnVault Policy to send application data to an Actifio OnVault Pool's defined storage location, see [Using Actifio OnVault Pools](#) on page 19.

Production to Mirror 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 failover to the remote site with an identical set of data that is mirrored between the local and remote Actifio appliances.

This section outlines the various methods of Production to Mirror replication supported by the Actifio appliance. You can select from one of the following methods to perform Production to Mirror replication.

- [Dedup Async Replication \(DAR\)](#) on page 7
- [StreamSnap Replication](#) on page 8
- [Sync and Async Replication](#) on page 10

Dedup Async Replication (DAR)

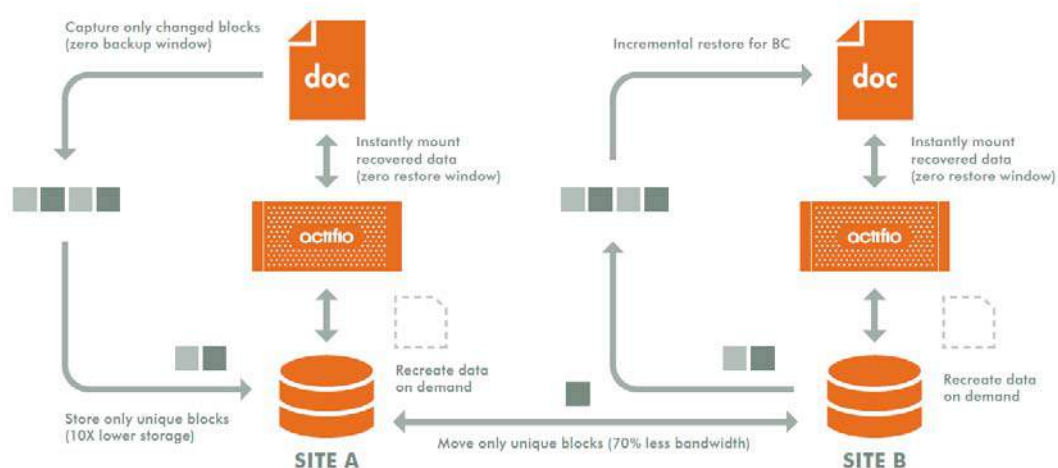
Dedup-Async Replication (DAR) allows you to keep a remote copy of an application's data up-to-date and ready to be used in a failover scenario, facilitating high-availability and redundancy. When a DAR-managed application fails for any reason, you can mount a failover image of the application at the remote site. When the problem has been resolved, then you can incrementally reverse replicate the changes made at the DR site to the primary site and then failback the application to the production site.

DAR is an Actifio-proprietary form of replication where initially a full copy of the application data is replicated to a target Snapshot pool on the second Actifio appliance or when a VM is replicated to the datastores of an ESX server. Dedup-Async replication sends deduplicated and compressed data over the network at a fraction of the bandwidth required for traditional replication technologies.

Once the Dedup-Async job takes a snapshot, it deduplicates the data, replicates the deduplicated data to another Actifio appliance, rehydrates that data on the second Actifio appliance, and updates the full copy of data on the second Actifio appliance to provide the flexibility of instant access at the remote location. This ensures that a full, up-to-date copy of data is ready and available on the second Actifio site.

Because the data is deduplicated before it is replicated, DAR requires less network bandwidth than StreamSnap replication but it does require additional Actifio system resources and a longer replication cycle.

Note: Production to Mirror policies that use DAR make snapshots of their own. They do not use a snapshot created by another snapshot policy.



Dedup-Async Replication Between a Local and Remote Actifio Appliance

Dedup-Async replication:

- Achieves typical Recovery Point Objectives (RPOs) of 24 hours with 12 and 8 hour RPOs possible.
- Achieves low Recovery Time Objectives (RTOs) at a remote location.
- Replicates data that can be efficiently deduplicated.
- Uses an existing IP network to replicate data.
- Replicates repeatedly at intervals determined by the Dedup-Async replication policy.
- Makes disk management transparent.
- Replicates VMware VMs to a datastore (optional).
- Makes fail-over to a host on the remote site simple.
- Makes syncback to the local Actifio appliance simple.

Note: For inband applications, the first DAR always communicates with the Actifio Connector. Subsequent application consistent jobs communicate with the Connector. Jobs that are not application consistent do not.

To configure Dedup-Async replication for an application or VM, see [Chapter 4, Performing Failover](#).

StreamSnap Replication

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 at the remote site. When the problem has been resolved, then you can use the syncback/restore/failback process (see [Chapter 4, Performing Failover](#)) to return the application to the production site..

StreamSnap replicates data snapshots to a remote Actifio appliance without deduplication, 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. The Actifio appliance allows you to maintain multiple local snapshots as well as store local images in the Dedup pool for long-term retention.

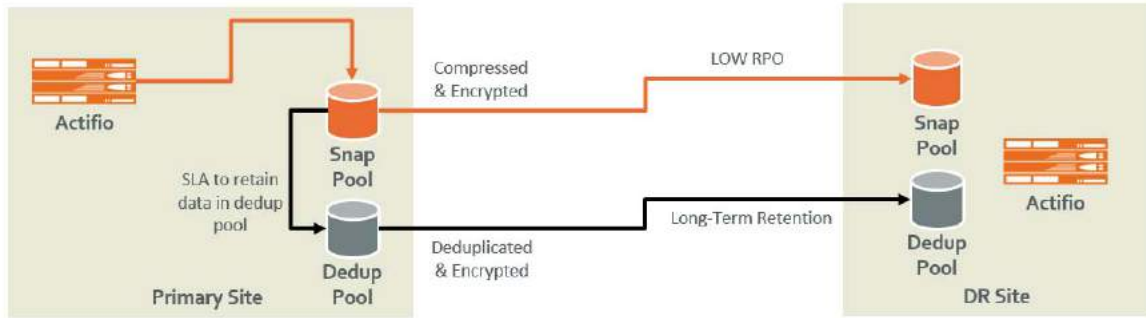
Production to Mirror policies that use StreamSnap replication are tied to a specific snapshot policy. They use the schedule and frequency settings of their associated snapshot policy.

You have the option to retain snapshot images from multiple available points in time at the remote site by applying retention in a StreamSnap policy. You can choose to:

- Retain only the latest remote StreamSnap image.
- Use the same retention as the local snapshot policy associated with this StreamSnap policy.
- Retain the remote snapshot image for a specific period of time (minutes, hours, days, weeks, months, or years).

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 Application Manager.

StreamSnap replication requires a reliable, high-quality 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).



StreamSnap Replication Between a Local and Remote Actifio Appliance

StreamSnap replication:

- Achieves Recovery Point Objectives (RPOs) as short as one hour. The StreamSnap replication policy relies on the associated snapshot policy for RPO and advanced settings.
- Uses an existing IP network to replicate data.
- Replicates data that is not conducive to deduplication. For example, data that is compressed or encrypted. Such data includes: images, videos, and encrypted databases.
- Replicates Oracle or Microsoft® SQL Server database log files to a remote Actifio appliance (Enable Database Log Backup and Enable Replication advanced settings active in snapshot policy).
- Replicates large amounts of data to remote users (for example, test and development environments).
- More efficient when replicating a large single dataset (such as a large database) than deduplication.
- 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.

Note: Compression is enabled by default for StreamSnap replication to the second Actifio appliance. From the Advanced Settings for a StreamSnap policy, you can disable compression if the data is already compressed (for example, for images and videos).

Note: StreamSnap jobs run for DB and DB+Log types. To perform on-demand log replication of the database logs to a remote Actifio appliance, select the database in Application Manager, then click the gear icon in the lower left corner of the Actifio Desktop and select **Replicate Logs**.

To configure StreamSnap replication for an application or VM, see [Chapter 4, Performing Failover](#).

For detailed information on StreamSnap jobs and error handling, see [Chapter 7, StreamSnap Jobs and Error Handling](#).

Sync and Async Replication

Sync and Async replication are forms of data mirroring that enable instantaneous failover/failback of production data for high availability. Both Sync and Async Replication are used only by Actifio CDS appliances to protect in-band generic applications; they are not intended for use by Actifio Sky appliances.

- **Sync (Synchronous) Replication** - Sync Replication is used for real-time data mirroring. It uses a fibre channel connection between locations, and supports connectivity to Actifio appliances located distances of 300KM apart. Sync replication can have a production data performance impact as every write operation must be replicated to the remote site before it is acknowledged to the host performing the write.
- **Async (Asynchronous) Replication** - Async Replication is also used for real-time data mirroring to a remote site, but it has no distance limitation. Async Replication will send data over the WAN as fast as network bandwidth allows. Async replication does not impact production data performance as it allows replication to fall behind and catch up using caching techniques.

Data that is replicated using either Sync and Async is not deduplicated. Both Sync and Async replication captures in-band data in real time; blocks are sent as they change.

Note: Both Sync and Async Replication require a Fibre Channel link between the source appliance and the target appliance. This can be accomplished through dark fiber or through an FCIP connection between the two sites, but the Fibre Channel ports at the target site must be zoned to the Fibre Channel ports at the source site.

To configure Sync or Async replication for an application, see [Chapter 6, Performing Synchronous and Asynchronous Replication](#).

2 Configuring Dedup Backup Replication for Long-Term Remote Storage

This section outlines procedures for:

[Configuring Dedup Backup Replication](#) on page 11

[Configuring Multi-hop Remote Dedup Backup Replication](#) on page 15

Note: For background on Dedup Backup replication see [Dedup Backup Replication](#) on page 4. Note that Dedup Backup replication is not a data-mirroring method such as [Dedup Async Replication \(DAR\)](#) on page 7, [StreamSnap Replication](#) on page 8, or [Sync and Async Replication](#) on page 10.

Configuring Dedup Backup Replication

To replicate your dedup backup data to a remote Actifio appliance for long-term storage:

1. Make sure both appliances are configured and joined (exchange security certificates), and are operating in either sharing or non-sharing mode so the image can be replicated to another Actifio appliance's Remote Dedup DR Pool for long-term storage. See **Configuring Resources and Settings with the Domain Manager** in the Actifio Documentation Library for background details.
2. In the **SLA Architect**, first create a template that includes either:
 - o **Production to Snap policy** and **Snapshot to Dedup Backup policy** to perform deduplication. A dedup policy will not run if there is not a snapshot to deduplicate. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for background details.
 - o **Production to Direct-to-Dedup policy**. Production Direct-to-Dedup policies are used for VMware VMs when you do not need the high availability of snapshots because Direct-to-Dedup policies require much less storage in the Snapshot Pool. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for background details.

Direct-to-Dedup protection is only recommended for non-critical VMware VMs. Mount, Clone, and Restore operations take longer with this type of protection, and backups of physical machines will be more resource intensive. If your storage environment requires the high availability of snapshots, consider using a **Production to Snap policy** and **Snapshot to Dedup Backup policy** in the template instead of a Production Direct-to-Dedup policy.

Note: If you enable the database log backup advanced settings as part of the snapshot policy associated with remote dedup storage, and you enable the **Replicate Logs (Using StreamSnap Technology)** setting, Oracle or Microsoft® SQL Server database transaction logs will be replicated to the remote Actifio appliance. Note that log replication does not occur until the Oracle or SQL Server database has been replicated to the remote appliance. At least one successful replication of the database must be completed first before a log will be visible on the remote appliance.

Once completed, add a Dedup Backup to Dedup DR policy to the template.

The Dedup Backup to Dedup DR schedule will not run unless there is a new deduplicated image to replicate to another Actifio appliance. Define the Dedup Backup to Dedup DR policy schedules in such a way that they start as soon as a Snapshot to Dedup completes. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for background details.

Note: To configure a multi-hop replication configuration between two remote Actifio appliances, see [Configuring Multi-hop Remote Dedup Backup Replication](#) on page 15.

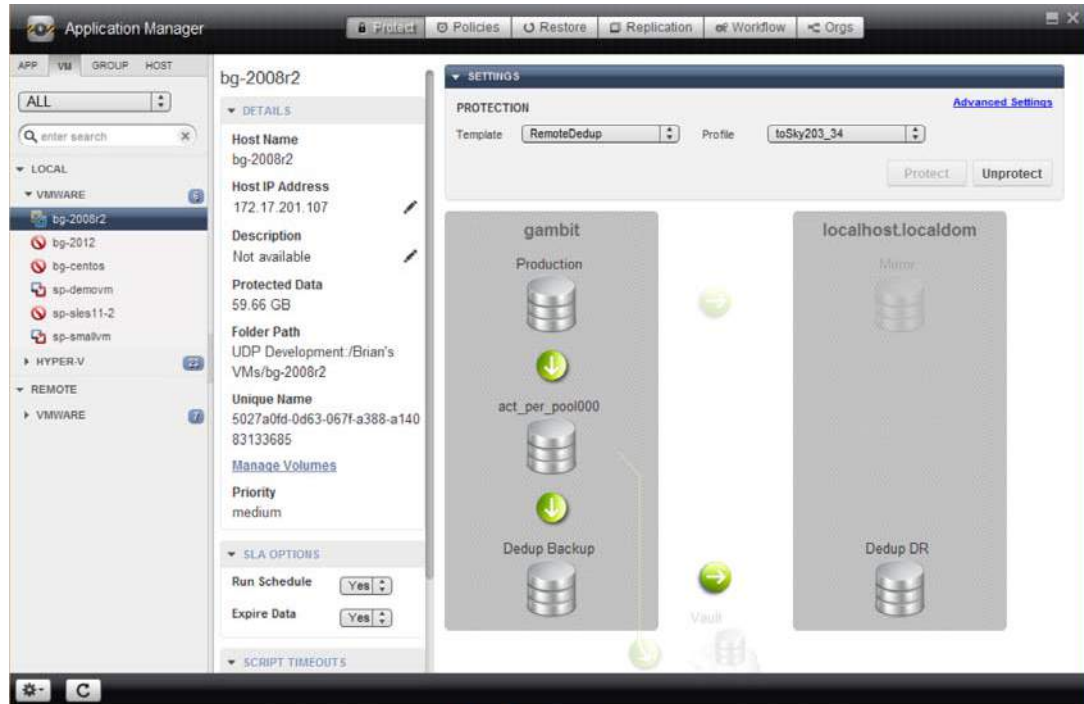


Creating a Policy for Replicating Deduplicated Images

3. In the **SLA Architect**, create a resource profile that specifies where to store data locally as well as where to replicate data. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.
4. Open the Actifio Desktop to the **Application Manager**.
5. In the navigation pane, select APP or VM.
6. Click the **Protect** tab in the Application Manager and:
 - o Select the Dedup Backup to Dedup DR policy template from the Template drop-down list.
 - o Select a resource profile from Profile drop-down list configured to include a remote Actifio appliance.
 - o Click **Protect**.

An application becomes protected when the first replication job completes successfully. When the local Actifio appliance copies the image from the snapshot pool to the dedup pool, the image is also sent to the remote Actifio appliance for long-term storage.

See **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library for details on protecting each type of application and VM supported by the Actifio appliance.

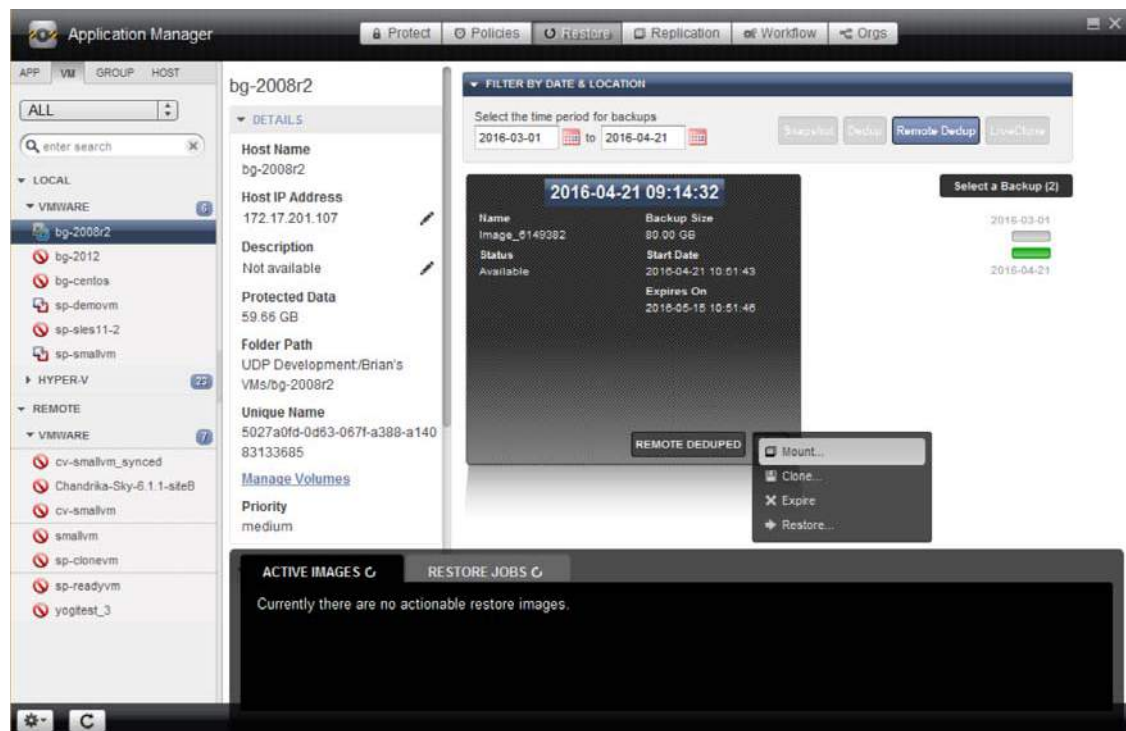


7. If you plan to replicate your dedup backup data to a remote Actifio appliance in the second leg of a multi-hop configuration, see [Configuring Multi-hop Remote Dedup Backup Replication](#) on page 15.

8. Based on your access and recovery requirements of the data stored at the remote site, you can perform a Mount, Clone, or Restore operation. Click **Remote Dedup** to see the dedup backup data at the remote Actifio appliance.

Note: If you specified replication of Oracle or Microsoft® SQL Server database transaction logs to a remote Actifio appliance as part of your SLA template, you can access the logs at the remote site for any database image within the retention range of the replicated logs.

For details on performing Mount, Clone, or Restore operations on your applications or VMs, see **Accessing and Recovering Copy Data with the Application Manager** and **Restoring Copy Data with the Application Manager** in the Actifio Documentation Library.



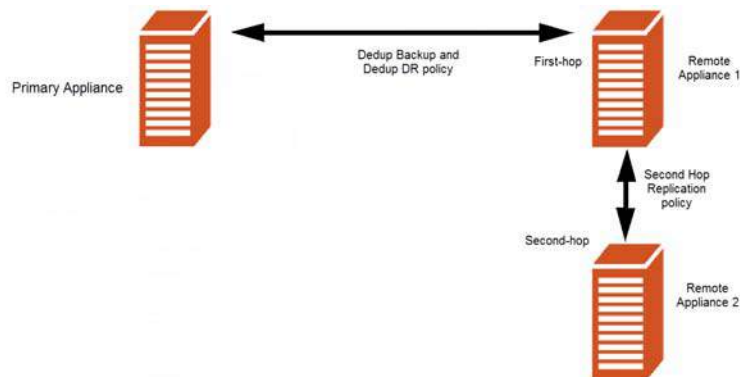
Configuring Multi-hop Remote Dedup Backup Replication

Multi-hop Backup Replication is an extension of Dedup Backup replication. If you are operating in a multi-Actifio configuration that includes a primary Actifio appliance and two remote Actifio appliances (1 and 2), you can specify a multi-hop replication configuration to define the replication of the dedup backup image between the two remote Actifio appliances.

Note: Multi-hop replication requires that the primary Actifio appliance and two remote Actifio appliances first be joined in sharing or non-sharing mode in the Domain Manager. See **Configuring Resources and Settings With the Domain Manager** included in the Actifio Documentation Library for background information.

To replicate your dedup backup data to a remote Actifio appliance in the second leg of a multi-hop configuration:

1. Make sure the primary Actifio appliance and the two remote Actifio appliances are configured, joined (exchange security certificates), and partnered in sharing or non-sharing mode.
2. In the **SLA Architect**, develop a set of policy templates as outlined below. For details, see **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.
 - o For the primary Actifio appliance, create a Dedup Backup and Dedup DR policy that forwards the dedup backup image to remote Actifio appliance 1. This policy operates as a single hop replication to Actifio appliance 1. See [Creating a Dedup Backup to Dedup DR Policy](#) on page 68.
 - o For remote Actifio appliance 1, create a second hop replication policy for the second leg of the multi-hop configuration. This policy defines the replication of the dedup backup image from remote Actifio appliance 1 to remote Actifio appliance 2.
 - o Remote Actifio appliance 2 does not require a specific policy definition for multi-hop replication; it acts as the recipient of the dedup backup in this multi-hop configuration.



Defining Policies for a Multi-hop Configuration



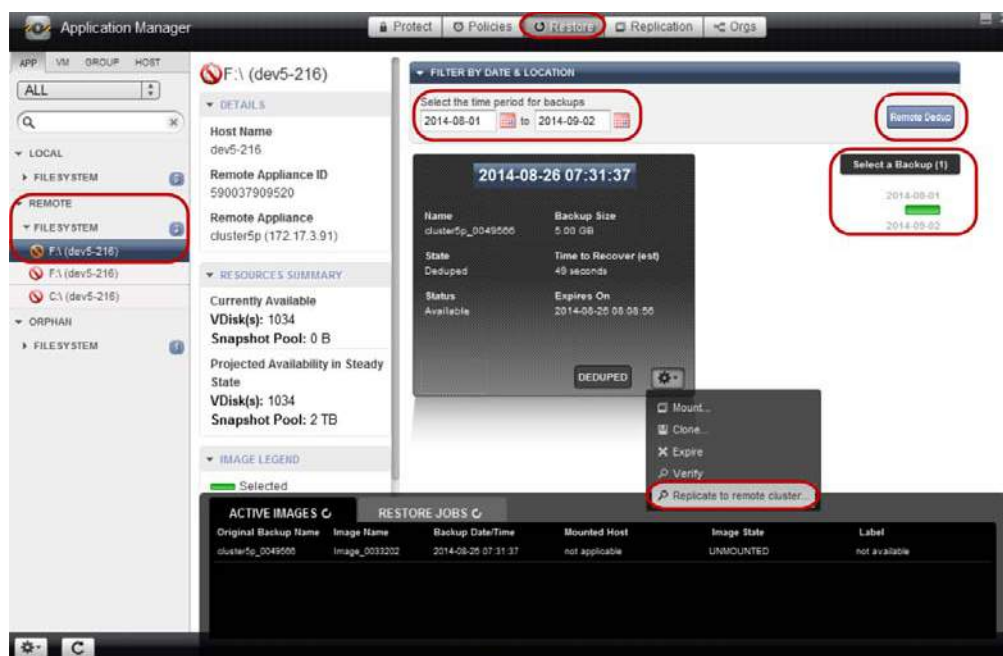
Creating a Policy for Second-Hop Replication

3. In the **SLA Architect**, create a resource profile for Actifio appliances operating in a multi-hop replication configuration (primary Actifio appliance and remote Actifio appliances 1 and 2). See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.
4. Open the Actifio Desktop to the **Application Manager**.
5. In the navigation pane, select APP or VM.
6. Click the **Protect** tab in the Application Manager and:
 - o Select the Second Hop Replication policy template from the Template drop-down list. When protecting remote applications, only Second Hop Replication policy templates will be listed in the Template drop-down list.
 - o Select a resource profile from Profile drop-down list configured to include the local and remote Actifio appliances involved in the second-hop of the multi-hop configuration.
 - o Click **Protect**.



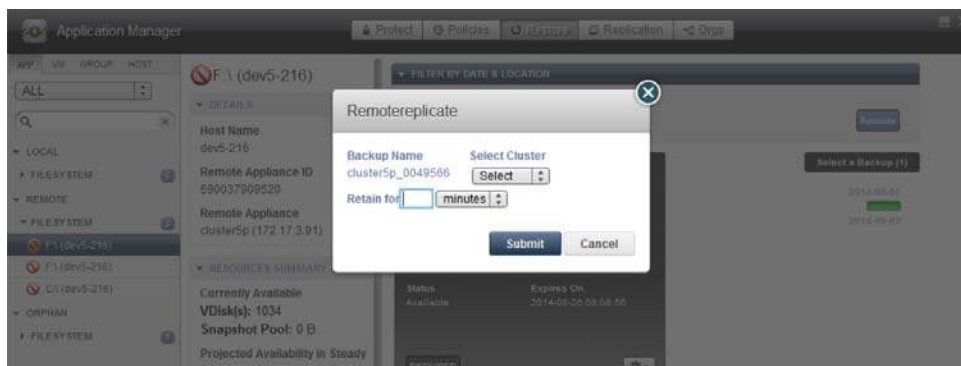
Applying a Second Hop Replication Policy Template

7. After the protection has completed, click the **Restore** tab and select the dedup image from the remote Actifio appliance.
8. Click **Replicate to remote appliance** from the drop-down menu.



Restoring a Backup Image from a Remote Appliance

9. From the Remote Replicate dialog box, make the following selections:
 - o **Select Appliance:** Choose from the list of joined Actifio appliances in the multi-hop configuration that you want to replicate the backup image.
 - o **Retain for:** Specify the expiration time period for retaining the selected image (from hours to years).
- Click **Submit** to initiate the on-demand replication to a remote Actifio appliance.



Identifying the Remote Appliance to Replicate

3 Using Actifio OnVault Pools

Snapshot to OnVault Policies control the transfer of data to storage defined by Actifio OnVault Pools by providing a schedule for when to send the data as well as a definition of how long to retain data. The combination of the Resource Profile and the Policy Template forms the SLA for the applications to which they are applied.

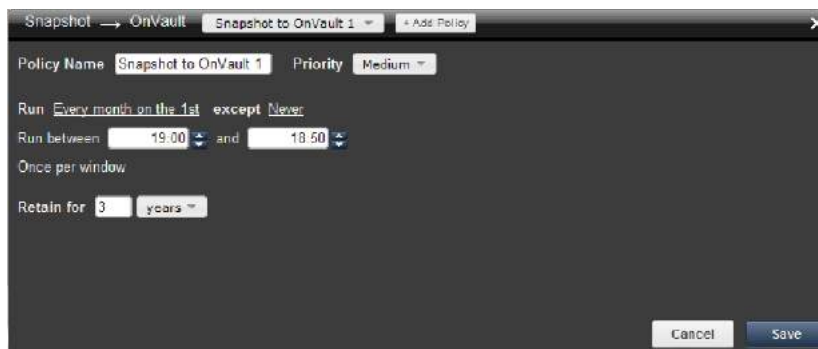
Note: For background information on storage defined by an Actifio OnVault Pool see [Sending Snapshot Images to Storage Defined by an Actifio OnVault Pool](#) on page 6.

Configuring Snapshot to OnVault Policy to Transfer Data

To transfer image data to the storage defined by an Actifio OnVault Storage Pool:

1. Make sure you have created an Actifio OnVault Pool. OnVault storage pools define storage and are specified in a Resource Profile for the long-term storage of data. Actifio OnVault Pools can use Amazon S3 Storage or Google Nearline Storage. See **Configuring Resources and Settings with the Domain Manager** in the Actifio Documentation Library for background details.
2. In the **SLA Architect**, create a template that includes:
 - o **Production to Snap policy** to use the most recently completed snapshot image.
 - o **Snapshot to OnVault policy** to schedule the movement of file system and application data to the storage defined by an Actifio OnVault Pool.

See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for background details.



Creating a Snapshot to OnVault Policy

3. In the **SLA Architect**, create a resource profile that specifies where to store data locally as well as an Actifio OnVault Pool to which data will be sent. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.

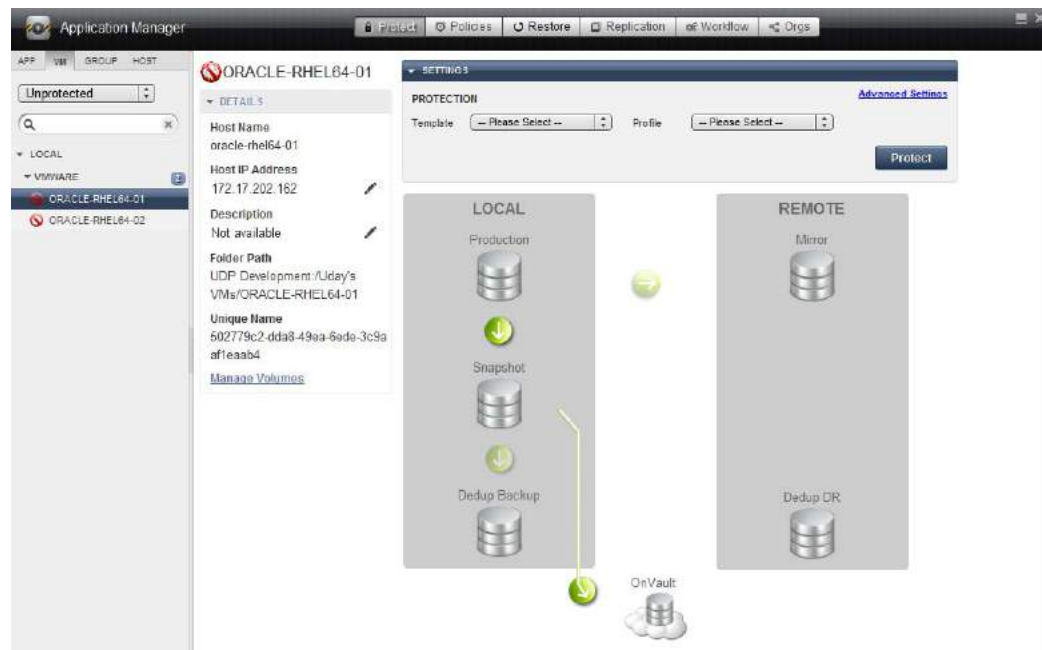


Creating an OnVault Resource Profile

4. Open the Actifio Desktop to the **Application Manager**.
5. In the navigation pane, select APP or VM.
6. Click the **Protect** tab in the Application Manager and:
 - o Select the Snapshot to OnVault policy template from the Template drop-down list.
 - o Select a resource profile from the Profile drop-down list configured to include the remote OnVault storage pool (Actifio OnVault Pool).
 - o Click **Protect**.

An application becomes protected when the first job completes successfully. When the local Actifio appliance copies the image from the snapshot pool to the dedup pool, the image is also sent to the Actifio OnVault Pool for long-term storage.

See **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library for details on protecting each type of application and VM supported by the Actifio appliance.



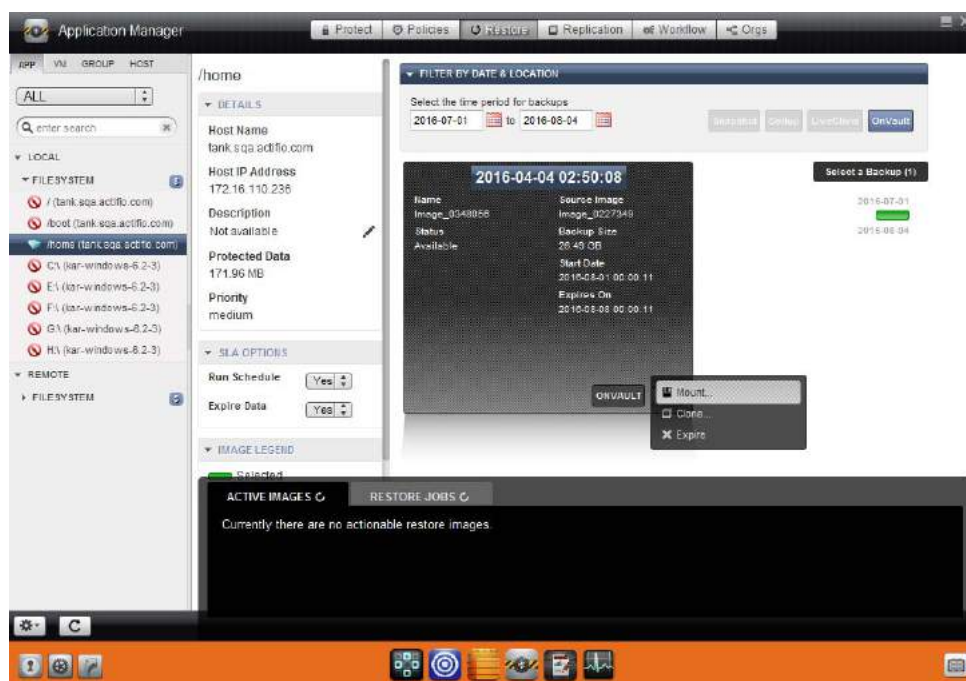
Protecting a VM Using a Snapshot to OnVault Template and Resource Profile

7. When accessing data in an Actifio OnVault Pool's storage:
 - o Actifio CDS and Sky appliances can create clones.
 - o Actifio Sky appliances can mount data.

Note: Mounted data can be accessed directly from a host, but it is not recommended to run workloads directly against this data.

- o Actifio CDS appliances **cannot** mount data.
- o LiveClones cannot be created.

For details on performing Mount, Clone, or Restore operations on your applications or VMs, see **Accessing and Recovering Copy Data with the Application Manager** and **Restoring Copy Data with the Application Manager** in the Actifio Documentation Library.



Restore Window with a OnVault Image (Shown for an Actifio Sky Appliance)

4 Performing Failover

Based on your Production to Mirror requirements for replicating a copy of your data to a second Actifio appliance, you can execute the failover of a Dedup-Async replication (DAR) image or a StreamSnap replication image to a mirrored data production site at a second Actifio appliance. Subsequently, changes made at the DR site can be replicated back (failback) to your production environment at the local Actifio appliance.

- Multiple syncback images can be used to replicate cumulative changes made at the DR site back to production.
- Syncback images can be mounted, cloned, or restored at the production site to restore access.

Note: For background on Production to Mirroring replication see [Dedup Async Replication \(DAR\)](#) on page 7 and [StreamSnap Replication](#) on page 8.

This chapter details:

[Configuring Dedup-Async or StreamSnap Replication to Remote Storage](#) on page 27

[Testing Failover](#) on page 30

[Failing Over a Protected Application](#) on page 33

[Failing Over a Protected VM](#) on page 35

Refer to [Chapter 5, Restoring from a Failover Condition](#) for the detailed procedure to fail back from the remote Actifio appliance to your production environment.

Configuring Dedup-Async Replication for a VM to an ESX Datastore

Note: This option is not available when performing StreamSnap replication.

Note: The CLI uses the shorthand term ReadyVM for the VM override feature.

To manage VM using a Dedup-Async replication policy:

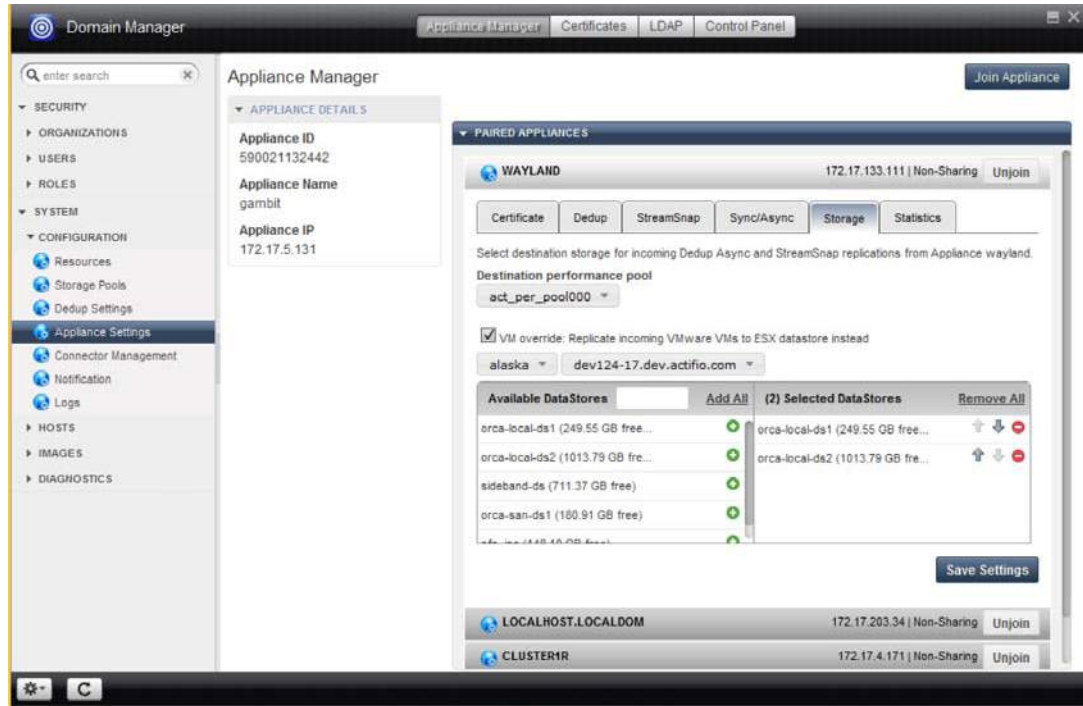
1. Make sure both Actifio appliances are configured and joined (exchange security certificates), and are operating in Sharing Mode. See **Configuring Resources and Settings With the Domain Manager** in the Actifio Documentation Library.
2. A VMware VM can be replicated to a datastore instead of a destination performance pool. Note the following considerations:
 - o The datastore must be part of an ESX server/vCenter added/discovered by the remote Actifio appliance to which the local Actifio appliance is joined. See **Configuring Resources and Settings With the Domain Manager** in the Actifio Documentation Library for details.
 - o Data must be replicated via a Production to Mirror policy that uses Dedup-Async replication. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for details.

To use this option:

- a. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
- b. Click the **Storage** subtab and the storage options are displayed:
- c. If the local Actifio appliance is joined with multiple remote Actifio appliances, select the remote Actifio appliance needed.
- d. Click the **VM override** check box.
- e. From the drop-down menus, select a vCenter host/ESX host.
- f. Click the green plus sign next to the required datastore name. When selecting datastores:
 - o Select as many datastores as needed. When multiple datastores are selected, VMDKs will be written to the datastores in round robin fashion.
 - o Ensure the datastore(s) free space equals the amount of data that will be replicated plus enough extra space to accommodate future growth
- g. Click **Save Settings** and Resource Profiles on this Actifio appliance that include the remote Actifio appliance set up with the VM override, will replicate VMware data to the selected datastore.

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

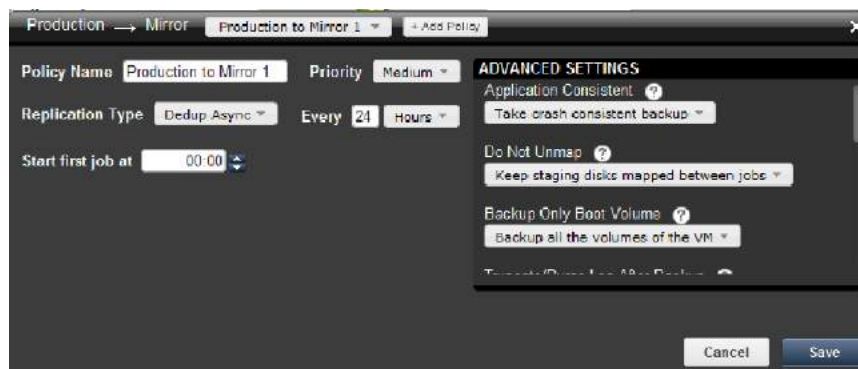
Note: When you configure VMware override it affects the incoming Dedup-Async replication to the Actifio appliance you are currently logged onto. If you require the DR appliance to create its DR copy in a VMware datastore rather than the DR appliance's Snapshot pool, be sure to set the VMware override at the DR appliance site.



Configuring VM Override for Dedup-Async or StreamSnap Replication

8. In the **SLA Architect** create a template that includes both a:
 - o **Production to Snap policy** as a good practice to include a snapshot policy as part of the Dedup-Async replication template to ensure recoverability at the local Actifio appliance side for local application management. The Snapshot and Dedup-Async policies share staging disks. In this case, the snapshot policy is run before the Dedup-Async policy takes effect.
 - o **Production to Mirror policy** that specifies Dedup-Async replication.

Note: If you enable the database log backup advanced settings as part of the snapshot policy in the same template as the Dedup Async policy, and you enable the **Replicate Logs (Using StreamSnap Technology)** setting, Oracle or Microsoft® SQL Server database logs will be replicated to the remote Actifio appliance. Note that log replication does not occur until the Oracle or SQL Server database has been replicated to the remote appliance. At least one successful replication of the database must be completed first before a log will be visible on the remote appliance.

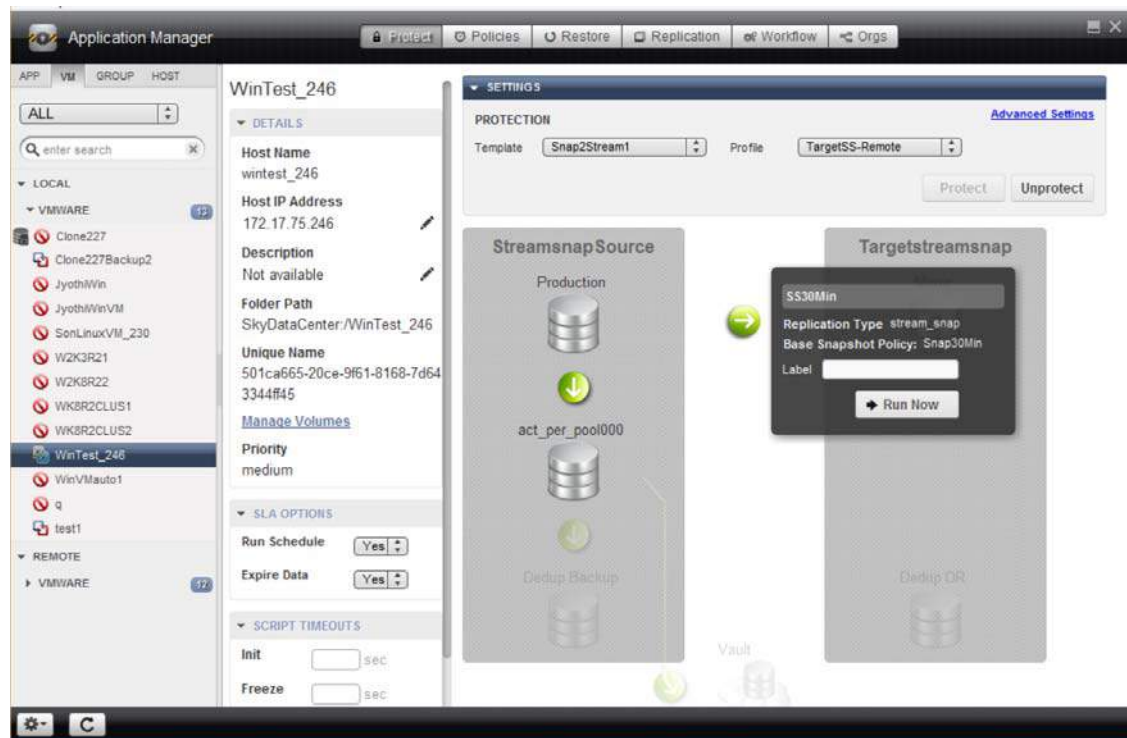


Creating a Dedup-Async Production to Mirror Replication Policy

Note: For background details on creating a template with a Dedup-Async replication policy, see **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.

9. In the **SLA Architect**, create a resource profile that specifies where to store data locally as well as where to replicate data. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.
10. Open the Actifio Desktop to the **Application Manager**.
11. In the navigation pane, select VM.
12. Click the **Protect** tab in the Application Manager and:
 - o Select the appropriate policy template from the Template drop-down list (a template that includes Dedup-Async replication or StreamSnap replication).
 - o Select a resource profile from Profile drop-down list configured to include a remote Actifio appliance.
 - o Click **Protect**. See **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library for details on protecting each type of application and VM supported by the Actifio appliance.

For Dedup-Async replication, once the Production to Mirror policy takes a snapshot, it deduplicates the data and then replicates the deduplicated data to the remote Actifio appliance. At the remote appliance, the full copy of the data is rehydrated and updated to provide the flexibility of instant access. Images appear on the remote system when you click the **Remote Snap** button in the Restore window in Application Manager.



Applying an SLA Template to Protect an Application or VM (Shown for StreamSnap Replication)

13. Test failover to the remote Actifio appliance as described in [Testing Failover](#) on page 30.

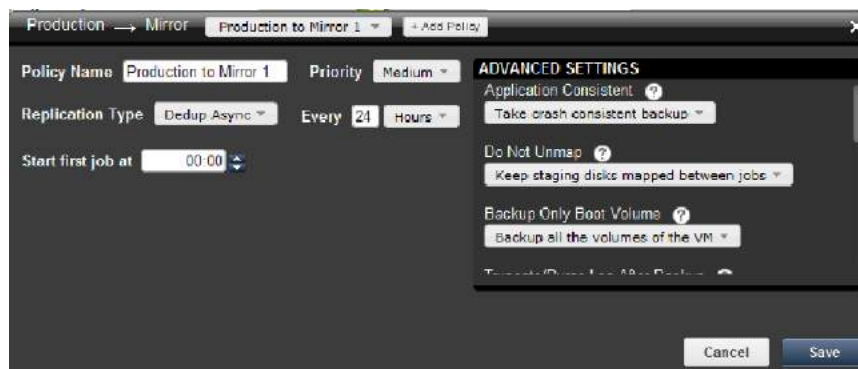
Configuring Dedup-Async or StreamSnap Replication to Remote Storage

You can replicate a VMware VM directly to an ESX datastore. This is detailed in [Configuring Dedup-Async Replication for a VM to an ESX Datastore](#) on page 24.

To manage an application or VM using a Dedup-Async or StreamSnap replication policy:

1. Make sure both Actifio appliances are configured and joined (exchange security certificates), and are operating in Sharing Mode. See **Configuring Resources and Settings With the Domain Manager** in the Actifio Documentation Library.
2. If performing Dedup-Async replication, in the **SLA Architect** create a template that includes both a:
 - o **Production to Snap policy** as a good practice to include a snapshot policy as part of the Dedup-Async replication template to ensure recoverability at the local Actifio appliance side for local application management. The Snapshot and Dedup-Async policies share staging disks. In this case, the snapshot policy is run before the Dedup-Async policy takes effect.
 - o **Production to Mirror policy** that specifies Dedup-Async replication.

Note: If you enable the database log backup advanced settings as part of the snapshot policy in the same template as the Dedup Async policy, and you enable the **Replicate Logs (Using StreamSnap Technology)** setting, Oracle or Microsoft® SQL Server database logs will be replicated to the remote Actifio appliance. Note that log replication does not occur until the Oracle or SQL Server database has been replicated to the remote appliance. At least one successful replication of the database must be completed first before a log will be visible on the remote appliance.



Creating a Dedup-Async Production to Mirror Replication Policy

Note: For background details on creating a template with a Dedup-Async replication policy, see **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.

3. If performing StreamSnap replication, in the **SLA Architect** create a template that includes both a:
 - o **Production to Snap policy.** Production to Mirror policies that use the StreamSnap replication option are tied to a specific snapshot policy. The StreamSnap policy requires the schedule and frequency settings of the associated snapshot policy in the template. You will be prevented from saving the StreamSnap replication policy without an associated base snapshot policy in the template.

- o **Production to Mirror policy** that uses StreamSnap replication. Actifio appliances can retain multiple point-in-time images at the remote site, with retention being specified in the policy. When retaining snapshot images at the remote Actifio appliance, each new snapshot image will be created at the remote appliance with a specific retention expiration date. Remote snapshot images support all operations available with a local snapshot image when accessed in the Application Manager.

Note: If you enable the database log backup advanced settings as part of the snapshot policy associated with StreamSnap replication, and you enable the **Replicate Logs (Using StreamSnap Technology)** setting, Oracle or Microsoft® SQL Server database logs will be replicated to the remote Actifio appliance. Note that log replication does not occur until the Oracle or SQL Server database has been replicated to the remote appliance. At least one successful replication of the database must be completed first before a log will be visible on the remote appliance.



Creating a StreamSnap Production to Mirror Replication Policy

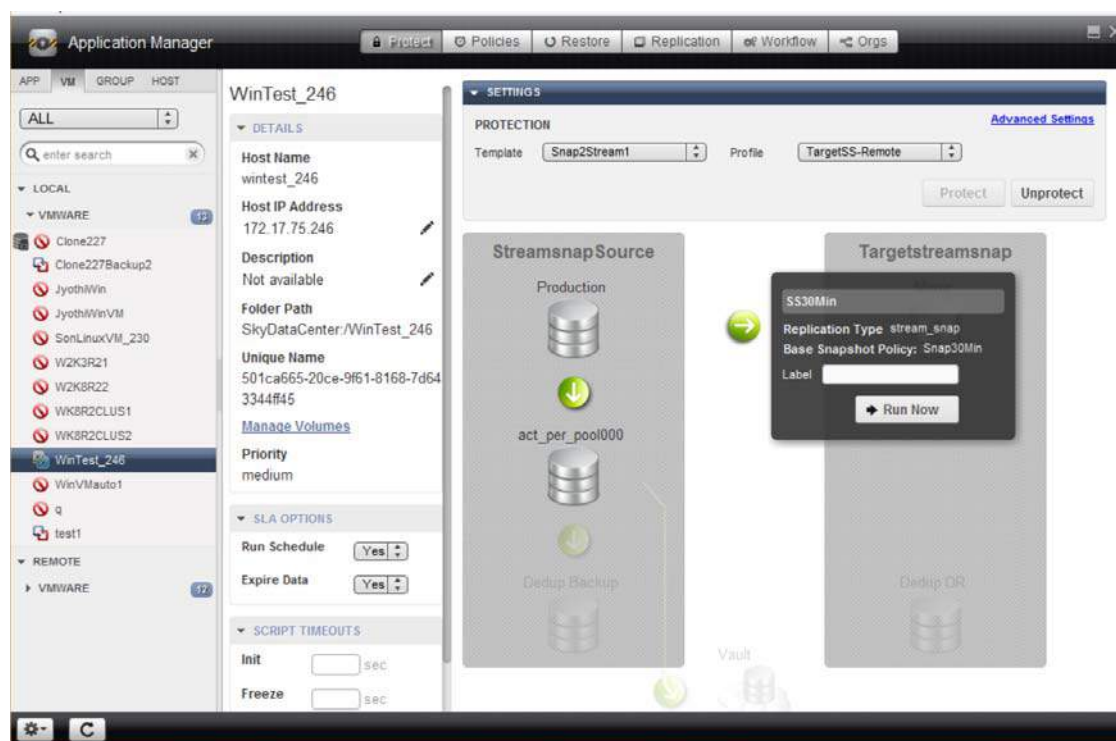
Note: For background details on creating a template with a StreamSnap replication policy, see **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.

4. In the **SLA Architect**, create a resource profile that specifies where to store data locally as well as where to replicate data. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.
5. Open the Actifio Desktop to the **Application Manager**.
6. In the navigation pane, select APP or VM.
7. Click the **Protect** tab in the Application Manager and:
 - o Select the appropriate policy template from the Template drop-down list (a template that includes Dedup-Async replication or StreamSnap replication).
 - o Select a resource profile from Profile drop-down list configured to include a remote Actifio appliance.
 - o Click **Protect**. See **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library for details on protecting each type of application and VM supported by the Actifio appliance.

For Dedup-Async replication, once the Production to Mirror policy takes a snapshot, it deduplicates the data and then replicates the deduplicated data to the remote Actifio appliance. At the remote appliance, the full copy of the data is rehydrated and updated to provide the flexibility of instant access. Images appear on the remote system when you click the **Remote Snap** button in the Restore window in Application Manager.

For StreamSnap replication, snapshots are replicated to a remote Actifio appliance without the use of deduplication. The data is then available locally and on the remote appliance to provide the flexibility of instant access. Images appear on the remote system when you click the **Remote Snap** button in the Restore window in Application Manager.

Note: If you specified replication of Oracle or Microsoft® SQL Server database transaction logs to a remote Actifio appliance as part of your SLA template, you can access the logs at the remote site for any database image within the retention range of the replicated logs.



Applying an SLA Template to Protect an Application or VM (Shown for StreamSnap Replication)

8. Test failover to the remote Actifio appliance as described in [Testing Failover](#) on page 30.

Testing Failover

After you configure an SLA Production to Mirror replication policy to perform Dedup-Async or StreamSnap replication, and then you protect an application or VM, you can test the failover to determine the readiness of the remote Actifio appliance. When you test a failover operation a virtual copy of the most recently replicated image of the application is created and presented to the host that you select. You can log on to the host and verify that the image is consistent. Test failover mounts to the target without stopping replication.

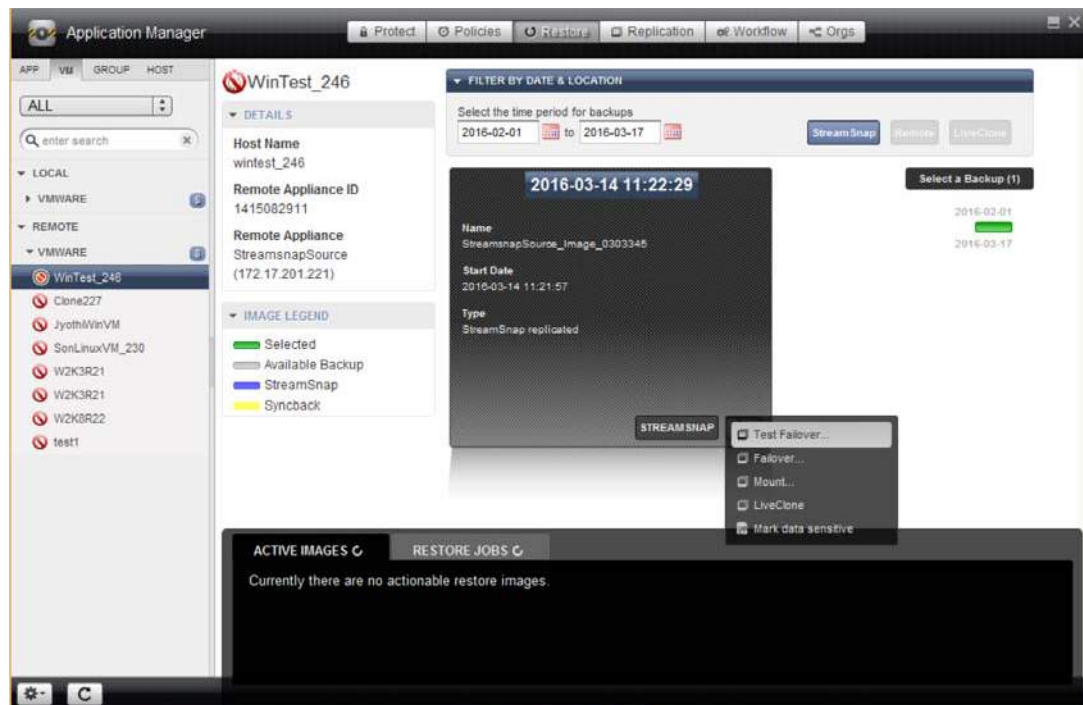
Note: When a test failover occurs on the remote Actifio appliance, a staging VDisk is created to quickly mount up the latest snapshot. This staging VDisk can be mounted to a new VM on the remote site or to an existing VM.

Before performing a test failover note the following usage considerations:

- Ensure that the WWPNI/SCSI port of the target host where the backup image is to be mounted is accessible by the remote Actifio appliance.
- You can have only one image test-failed-over to one host at one time. For example, when a failover image is available on the remote Actifio appliance and the local Actifio appliance is managing hosts A and B, you can host the image on either A or B but not both.
- You cannot failover a virtual machine application to the same virtual machine.
- For VMware VM failover, you must have an ESX server and vCenter server up and running at the remote site to test failover.

To test failover on the remote Actifio appliance from the Actifio Desktop:

1. Open the Application Manager to the **Restore** tab.
2. From the Remote list, select the application or VM from the navigation pane. The last successful backup job is displayed.
3. From the image information action pull-down menu, click **Test Failover**.



Specifying the Test Failover Operation (Shown for a StreamSnap Image)

4. From the Test Failover dialog:
 - o When failing over to an existing host, select the target host from the Select Host drop-down list to fail over the image.

The screenshot shows the 'Test Failover' dialog box. At the top, it displays 'Image Name' as 'StreamsnapSource_image_0303345', 'Backup Date' as '2016-03-14 11:22:29', and 'Host Name' as 'wintest_246'. Below this is a 'Label' text field. The 'Mount To' section has two radio buttons: 'Existing Host' (selected) and 'New VM'. Under 'Existing Host', there is a 'Select Host' dropdown menu currently showing 'aman_linux'. There is also a checkbox for 'Map to all ESX hosts'. The 'Mount Mode' section has two radio buttons: 'vRDM' (selected) and 'pRDM'. At the bottom, there are 'Mount Drive' and 'Mount Point' text fields. 'Submit' and 'Cancel' buttons are at the bottom right.

Performing a Test Failover to an Existing Host

- o When failing over to a new VMware VM select **New VM**:

The screenshot shows the 'Test Failover' dialog box with the 'New VM' radio button selected under 'Mount To'. The 'VM Name*' field is empty. The 'ESX Host*' dropdown menu is open, showing a list of hosts: 'None', '172.17.75.8', 'enterprise.dev.actifio.com' (highlighted), '172.17.124.138', and '172.16.11.8'. The 'Datastore*' dropdown menu shows 'None' and 'sys (4.64 GB free)'. The 'Select vCenter Server*' dropdown menu shows '172.17.75.100'. There are checkboxes for 'Map to all ESX hosts' and 'Power on VM after Test Failover ?'. The 'Mount Mode' section has 'vRDM' and 'pRDM' radio buttons. 'Submit' and 'Cancel' buttons are at the bottom right.

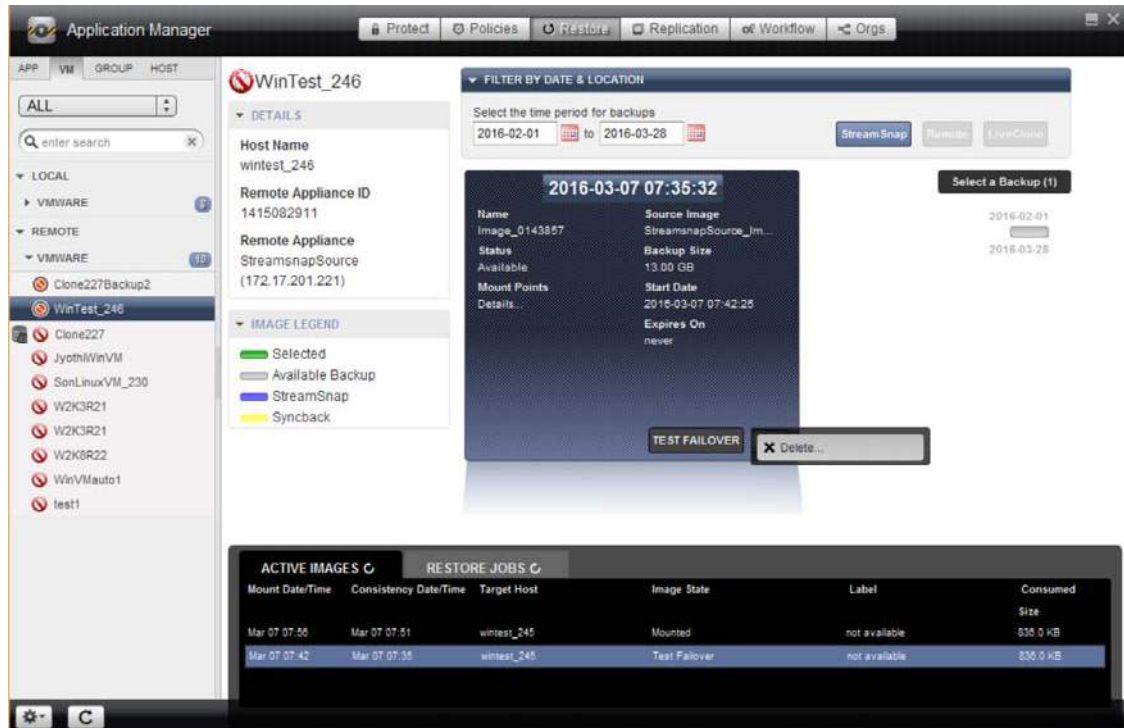
Performing a Test Failover to a New VM

5. Click **Submit**. The latest Dedup-Async or StreamSnap image of the application is used to create a virtual copy and presents it to the host you have selected. Since it is a virtual copy of the image, the host can use it without affecting the actual Dedup-Async or StreamSnap image.
6. When the job completes with the job status **Successful**, you can then mount, log on to the host, and view the failover image to ensure the consistency of data and your complete DR procedure.
7. When you are satisfied with the failover test results, delete the test failover image as described in [Deleting Test-Failover Images](#) on page 32.

Deleting Test-Failover Images

To delete a test failover image from the remote Actifio appliance:

1. Open the **Application Manager** to the **Restore** tab.
2. Select the application from the navigation pane, from the APP or VM tab Remote list.
3. Select the test failover image from the Active Images pane at the bottom.
4. From the image information action pull-down menu, click **Delete**.



Deleting a Test Failover Image

Failing Over a Protected Application

At the time of application failover, Dedup-Async or StreamSnap replication of the application data from the local Actifio appliance is stopped to make use of the most recent copy of the application image at the remote appliance. The most recent image of the application data is made available as a snapshot to any available host. The Actifio appliance internally maintains another reference copy, so the mounted snapshot can be used to write data as applications continue to run at the remote appliance.

While in the failed over state, the application accesses the remote image directly, so replication to the remote Actifio appliance is paused. When the application is ready to operate from the local appliance, you can syncback the data back to the local appliance, and then perform a failback operation.

Note: Before performing a failover task, ensure that the WWPN/iSCSI port of the host where the backup image is to be mounted is accessible to the remote Actifio appliance.

To failover a Dedup-Async or StreamSnap-protected application:

1. Click **Desktop > New Desktop** to launch another session of the Actifio Desktop on the *remote* Actifio appliance.
2. Open the Actifio Desktop on the remote Actifio appliance to the **Application Manager**.
3. Select the shadow application from **Remote** in the navigation pane:
4. Depending on the replication image:
 - o Click **Dedup Async** if it is a Dedup-Async replication image.
 - o Click **StreamSnap** if it is a StreamSnap replication image.

By default, the latest image is selected for failover.

5. From the image information action pull-down menu, click **Failover**. The Failover dialog appears.



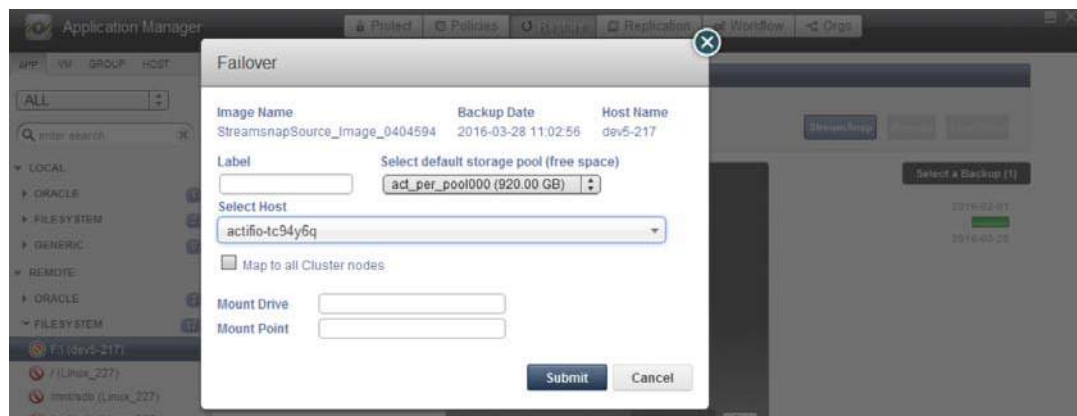
Mounting a Failover Image from the Remote Appliance (Shown for StreamSnap)

6. From the Failover dialog:
 - o If required, enter a label for the failover operation.
 - o If necessary, change the default storage pool from the drop-down list. The default storage pool is `act_per_pool` (the performance pool).
 - o Select a physical host from Host drop-down list. The selected host must be a SAN host or a Virtual Machine on ESX Server that is connected to the Actifio appliance.
 - o For Mount Mode, vRDM mode is selected by default. For file-level restore operations, select pRDM (physical raw device mapping) mode.

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

Then specify the following additional mount information:

- o **Mount Drive:** Specifies a drive letter to be assigned to the volume. If the drive letter is not available, the job fails. If multiple volumes are found, then it assigns subsequent drive letters. If no Mount Drive is specified, the Actifio Connector chooses a drive letter itself, if available.
- o **Mount Point:** The full path at which you want to mount the volume. If the path exists as an empty folder, the Actifio Connector will use it. If it does not exist, the Actifio Connector will create it. If it exist as a file or as a folder that is not empty, then the job will fail. If there are multiple volumes to be mounted, the Actifio Connector chooses the user specified for one of the volumes and for the remaining it appends an underscore (_) followed by a number (for example, <user_specified>_#).



7. Click **Submit**. A warning message is displayed instructing you that this action will stop replication.
8. Type **FAILOVER** in the text box to confirm the operation.



9. Click **Start Failover** to initiate a failover job. The failover job stops any Dedup-Async or StreamSnap replication jobs in progress for this application and presents the latest replicated image to the selected host.
10. Log on to the host, bring up the application, and direct all the external clients to use this application copy.

When you are ready to bring back the data generated at the remote Actifio appliance to the local Actifio appliance, start the failback operation described in on page 39.

Failing Over a Protected VM

At the time of VM failover, Dedup-Async or StreamSnap replication of the VM data from the local Actifio appliance is stopped to make use of the most recent copy of the image at the remote appliance. The most recent image of the VM data is made available as a snapshot to any available host. The Actifio appliance internally maintains another reference copy, so the mounted snapshot can be used to write data as applications continue to run at the remote appliance.

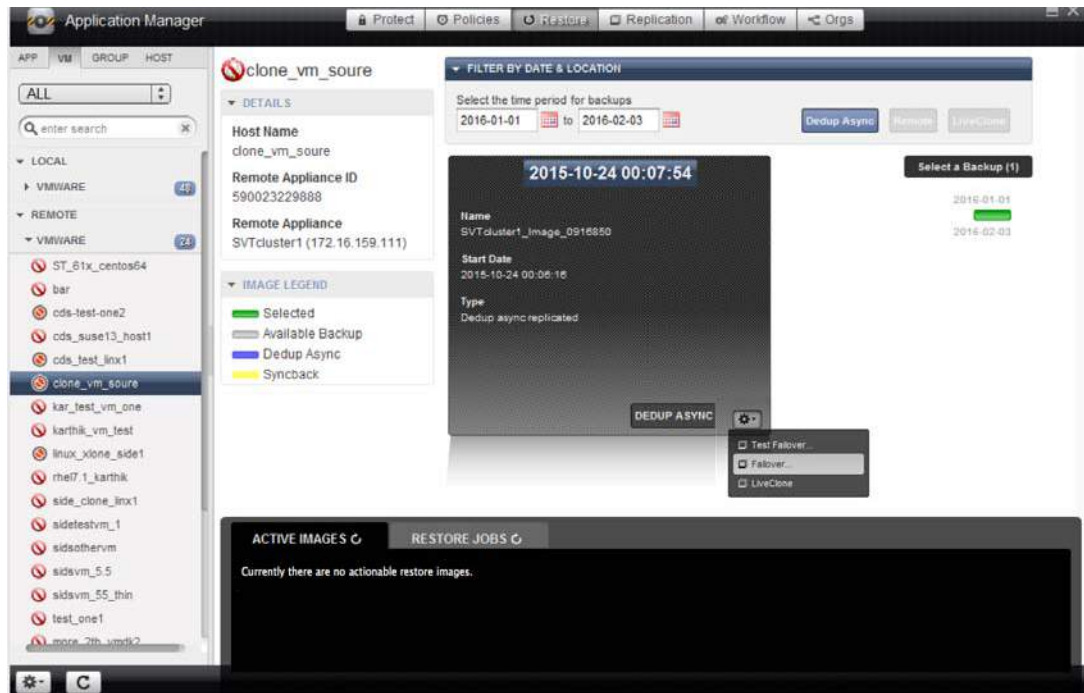
While in the failed over state, the VM accesses the remote image directly, so replication to the remote Actifio appliance is paused. When the VM is ready to operate from the local appliance, you can syncback the data back to the local appliance, and then perform a failback operation.

Note: Before performing a failover task, ensure that the WWPN/iSCSI port of the host where the backup image is to be mounted is accessible to the remote Actifio appliance.

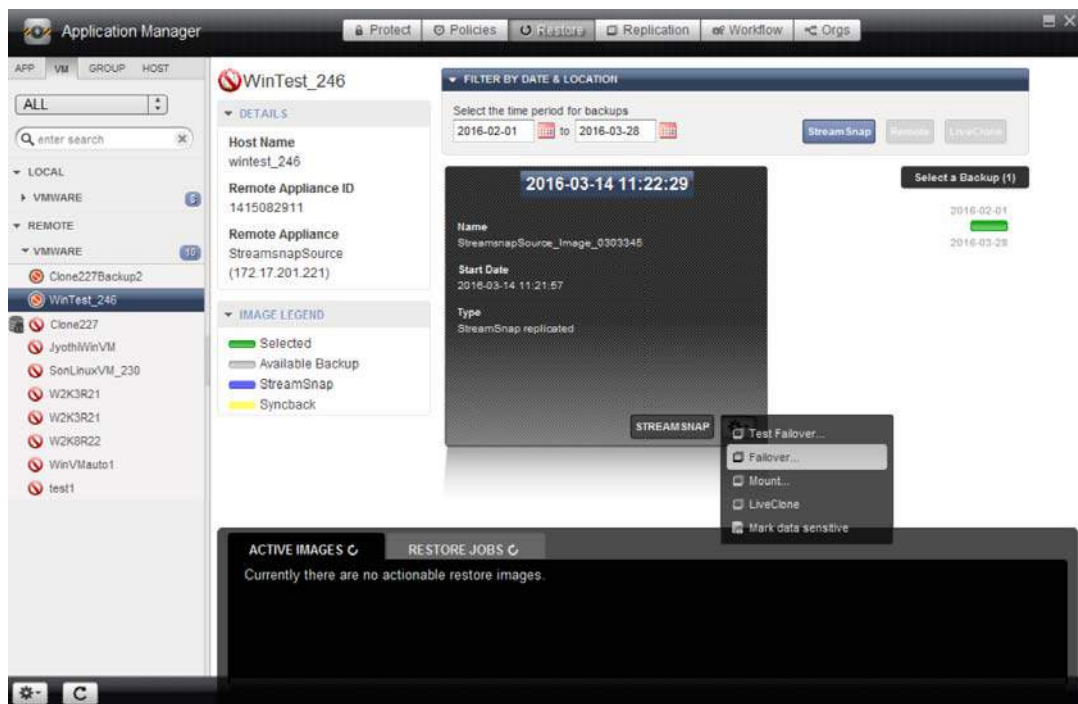
To failover a Dedup-Async or StreamSnap-protected VM:

1. Click **Desktop > New Desktop** to launch another session of the Actifio Desktop on the *remote* Actifio appliance.
2. Open the Actifio Desktop on the remote Actifio appliance to the **Application Manager**.
3. Select the shadow VM from **Remote** in the navigation pane:
4. Depending on the replication image:
 - o Click **Dedup Async** if it is a Dedup-Async replication image.
 - o Click **StreamSnap** if it is a StreamSnap replication image.

By default, the latest image is selected for failover.



Failing Over a Dedup-Async Failover Image from the Remote Appliance



Failing Over a StreamSnap Image from the Remote Appliance

5. From the image information action pull-down menu, select **Failover**. The Failover dialog appears.
6. If required, enter a label for the failover operation.

7. If necessary, change the default storage pool from the drop-down list. The default storage pool is act_per_pool (the performance pool).
8. For the Mount To option:
 - o To fail over to an existing host, select Existing Host and specify a physical host from the drop-down list.

The screenshot shows the 'Failover' configuration window. It includes the following fields and options:

- Image Name:** StreamsnapSource_Image_0303345
- Backup Date:** 2016-03-14 11:22:29
- Host Name:** wintest_245
- Label:** (empty text box)
- Select default storage pool (free space):** act_per_pool000 (920.00 GB)
- Mount To:** ☒ Existing Host ☐ New VM
- Select Host:** wintest_245 (dropdown menu)
- Map to all ESX hosts:** ☐
- Mount Mode:** ☒ vRDM ☐ pRDM
- Mount Drive:** (empty text box)
- Mount Point:** (empty text box)
- Buttons:** Submit, Cancel

Mounting a Failover Image to an Existing Host

- o To fail over to a new VMware VM select **New VM**. You can only failover a VM to a new VM.
 - Enter a name for the new VM that you want to mount,
 - Select a vCenter from the drop-down list for the new VM you want to mount.
 - Select an ESX Host from the drop-down list for the new VM you want to mount.
 - Select a datastore that has the required storage available from the drop-down list for the new VM you want to mount.
 - Click the check box if you want the new VM powered on after failover.

The screenshot shows the 'Failover' dialog box with the following fields and options:

- Image Name:** StreamsnapSource_Image_0303345
- Backup Date:** 2016-03-14 11:22:29
- Host Name:** wintest_246
- Label:** (empty text field)
- Select default storage pool (free space):** act_per_pool000 (920.00 GB)
- Mount To:** ☐ Existing Host ☒ New VM
- VM Name:** (empty text field)
- Select vCenter Server:** 172.17.75.100
- ESX Host:**
 - None
 - 172.17.75.8
 - enterprise.dev.actifio.com
 - 172.17.124.138
 - 172.16.11.8
- Datastore:** None (38.46 GB free)
- ☐ Map to all ESX hosts
- ☒ Power on VM after Failover
- Mount Mode:** ☒ vRDM ☐ pRDM
- Buttons:** Submit, Cancel

Mounting a Failover Image to a New VMware VM

- o When failing over to a new Hyper-V VM, select **New VM**. You can only failover a VM to a new VM.
 - Select whether to mount to **SCVMM** or a **Hyper-V** server.
 - Enter a VM name as needed.
 - Select an SCVMM server as needed.
 - Select a Hyper-V server as needed.
 - Enter a path to the VM as needed.

The screenshot shows the 'Failover' dialog box with the following fields and options:

- Select Diskpool:** act_per_pool000 (906.00GB)
- Label:** (empty text field)
- Mount To:** ☐ Existing Host ☒ New VM
- Mount To VM:** ☒ SCVMM ☐ Hyper-V
- VM Name:** (empty text field)
- Hyper-V Server:** (empty text field)
- Path:** (empty text field)
- Select SCVMM Server:** None
- Buttons:** Submit, Cancel

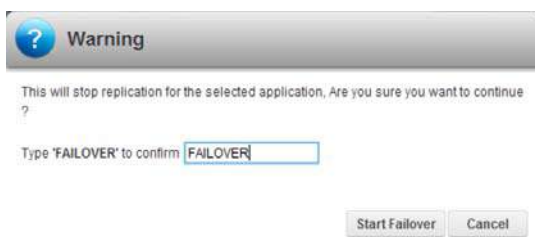
Mounting a Failover Image to a New Hyper-V VM

9. Select one of the following as the Mount Mode selection:
 - o vRDM (virtual raw device mapping). By default vRDM mode is selected.
 - o pRDM (physical raw device mapping). For file-level restore operations, select pRDM mode.

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

Then specify the following additional mount information:

- o **Mount Drive:** Specifies a drive letter to be assigned to the volume. If the drive letter is not available, the job fails. If multiple volumes are found, then it assigns subsequent drive letters. If no Mount Drive is specified, the Actifio Connector chooses a drive letter itself, if available.
 - o **Mount Point:** The full path at which you want to mount the volume. If the path exists as an empty folder, the Actifio Connector will use it. If it does not exist, the Actifio Connector will create it. If it exist as a file or as a folder that is not empty, then the job will fail. If there are multiple volumes to be mounted, the Actifio Connector chooses the user specified for one of the volumes and for the remaining it appends an underscore (_) followed by a number (for example, <user_specified>_#).
10. Click **Submit**. A warning message is displayed instructing you that this action will stop replication.
 11. Type **FAILOVER** in the text box to confirm the operation.



12. Click **Start Failover** to initiate a failover job. The failover job stops any Dedup-Async or StreamSnap replication jobs in progress for this VM and presents the latest replicated image to the selected host or the new VM.
13. Open the System Monitor service from the Actifio Desktop to view the failover job status.
14. Log on to the host, bring up the VM, and direct all the external clients to use this copy of the application.

When you are ready to bring back the data generated at the remote Actifio appliance to the local Actifio appliance, start the failback operation described in [Chapter 5, Restoring from a Failover Condition](#).

5 Restoring from a Failover Condition

Note: For the detailed procedure to failover a Dedup-Async or StreamSnap-protected application or VM to a remote Actifio appliance, see [Chapter 4, Performing Failover](#).

In a failover situation, users of an Actifio appliance may continue to use and generate data on the application, but the application is running from an image on the remote Actifio appliance. After an application fails over to a remote Actifio appliance, you can failback the application to the local Actifio appliance.

Failback involves restoring the latest data from the backup image to the production application, restoring the application from the latest data, and then cleaning up. After failback, the application state changes to Protected and the replication to the remote appliance is resumed.

To minimize application downtime, perform these procedures in the following order.

1. [Performing a Catch-Up Syncback](#) on page 42
2. [Stopping the Failed-Over Application](#) on page 43
3. [Performing the Final Syncback](#) on page 43
4. [Restoring a Syncback Image](#) on page 44
5. [Failback to the Local Appliance](#) on page 48
6. [Deleting Failover and Syncback Images](#) on page 49

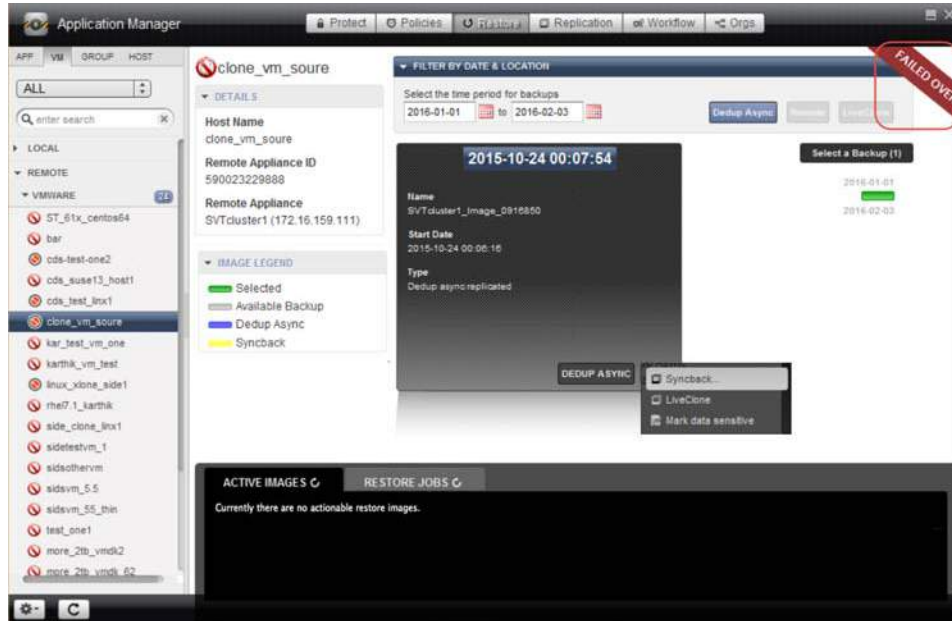
Note: If you do not require the remote data, you can skip directly to Step 5, [Failback to the Local Appliance](#) on page 48.

Performing a Catch-Up Syncback

At the time you begin the failback process, your users are accessing the application on the remote Actifio appliance. The first syncback copies all the data generated at the remote Actifio appliance since the failover to the local Actifio appliance. This can take some time depending upon how active the application is and how long it has been in a failover state.

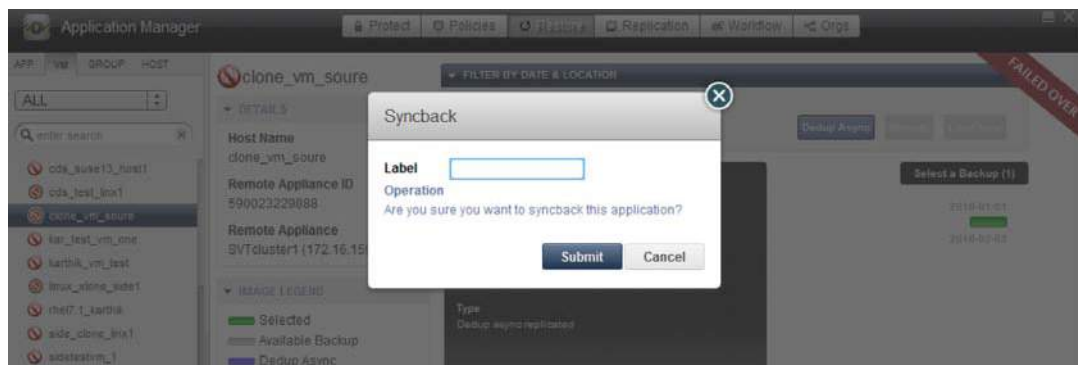
Execute the syncback task on the remote Actifio appliance as follows:

1. On the remote Actifio appliance, open the Actifio Desktop to the **Application Manager**.
2. Select the application from the navigation pane, and on the service menu, click **Syncback**. The Syncback dialog appears.



Performing a Syncback from the Remote Appliance (Shown for Dedup-Async)

3. From the Syncback dialog, you can optionally enter a label for the application syncback operation.



4. Click **Submit**. The newly generated data from the remote application is brought back to the local Actifio appliance, but it is not automatically applied to the original image of the application. Instead, it is made available on the local Actifio appliance as a Syncback image.

You can view the synchronized image on the local appliance at **Application Manager > Restore > Syncback**. The synchronized image is yellow in the Restore window; when you select the synchronized image it turns green. You can restore, mount, or clone a synchronized image.

5. Open the System Monitor service from the Actifio Desktop to view the syncback job status, including statistics associated with the job.



The next step requires [Stopping the Failed-Over Application](#) during the restore operation. If you are not yet ready to perform the restore operation, you can perform syncback operations until you are ready to failback. Each one creates a new syncback image on the local Actifio appliance. There is no limit to the number of times syncback can be executed.

Stopping the Failed-Over Application

This step marks the start of the time that the application is out of service. Stop the application on the remote Actifio appliance to prevent new data from coming in after the final syncback has begun. The application will be out of service for the final syncback step and through the restoration step, coming back online at the end of the restoration step.

Performing the Final Syncback

Because the application is still in service on the remote Actifio appliance, the data on the remote appliance may have changed during the catchup syncback. The final syncback will be faster because it includes less data.

1. On the remote Actifio appliance, open the Actifio Desktop to the **Application Manager**.
2. Shut down the application on the remote appliance.
3. Select the application from the navigation pane, and on the service menu click **Syncback**.
4. Click **Submit**. The final data from the remote application is brought back to the local Actifio appliance.
5. Restore the Syncback image as described in [Restoring a Syncback Image](#) on page 44.

Restoring a Syncback Image

After synchronizing back the failed-over application or VM image, you may either perform a restore operation to put the data back to its original location, or a mount operation to access the data more quickly. Note the following guidelines to assist in determining the ideal approach, based on data type and your needs:

- For a non-VM application, we recommend that you perform a restore of the application data from the synchronized image instead of performing a mount operation (see [Restoring an Application or VM Syncback Image](#) on page 44). With non-VM application types, the subsequent copy back to production disk is a manual operation and typically needs to be performed while users do not require access to this data. In this case, an image restore is often the best choice. The restoration replaces the application's image in use prior to failover with the latest image that includes changes from the remote Actifio appliance.
- For a VM, you have the following options:

You can perform a restore to bring the VM back to the original location (see [Restoring an Application or VM Syncback Image](#) on page 44). Note that a restore operation takes time for the data movement. During this time, the VM will be offline. In this case, the network settings and MAC address are preserved when performing a restore because the operation updates the disks, instead of recreating the VM. Protection will remain intact, but will perform a “low splash” job during the next snapshot job due to the loss of VMware CBT data that results from any restore operation. See .

You can mount the VM to either a new VM or to an existing VM (see [Mounting a VM Syncback Image](#) on page 47). This provides immediate access to the VM and/or its data without waiting for a traditional restore window. Note the following usage considerations if you intend to perform a mount operation for the VM:

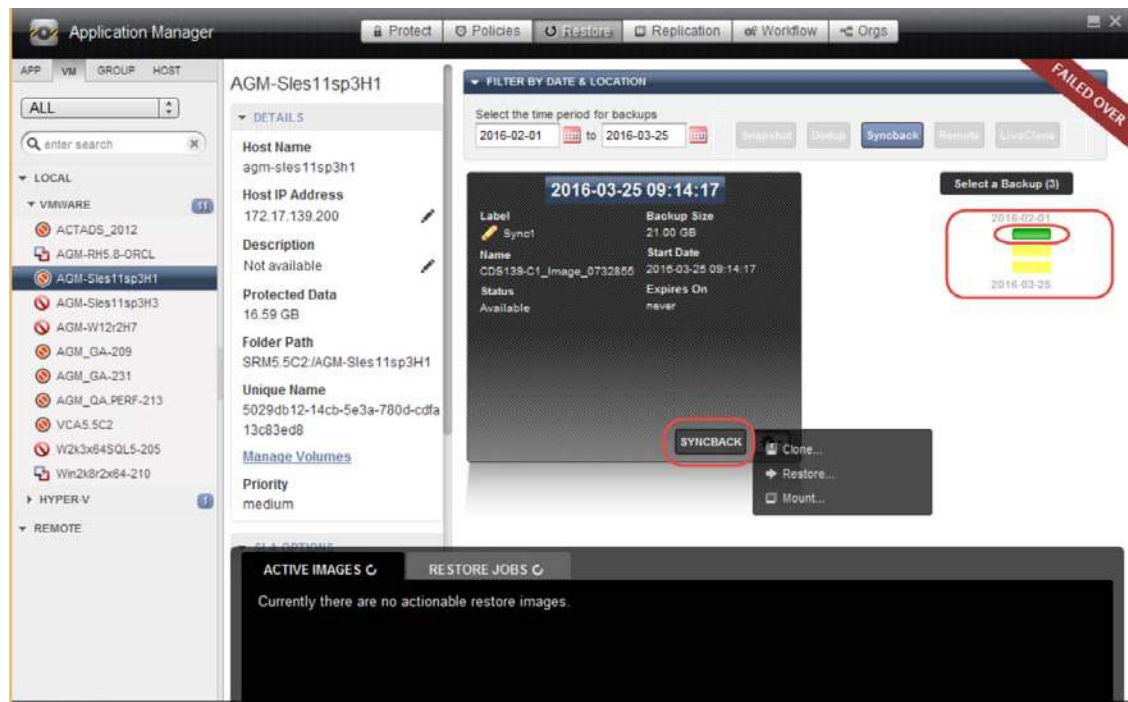
- o If you mount to an existing VM, note that you will get new disks in the existing VM, which may not be desirable for your environment. However, if you delete the original disks first you may be able to then boot from the VM and use Storage vMotion. In this case, the primary benefit is that the previous discovery and protection are retained.
- o If you mount to a new VM, you will have a recoverable VM. You may want to manually update the MAC addresses to match the original VM so the network settings are preserved. You can then use Storage vMotion to migrate the VM to a datastore. You will have to re-discover and re-protect using this method.

Restoring an Application or VM Syncback Image

To restore an application or VM syncback image:

1. On the local Actifio appliance, open the Application Manager to the **Restore** tab.
2. Select the application from the navigation pane.
3. Note the following considerations prior to restoring:
 - o If you are restoring a non-VM application, be sure to shut down the application and unmount the filesystem.
 - o If you are restoring a VM, the restore procedure will automatically power down the virtual machine.

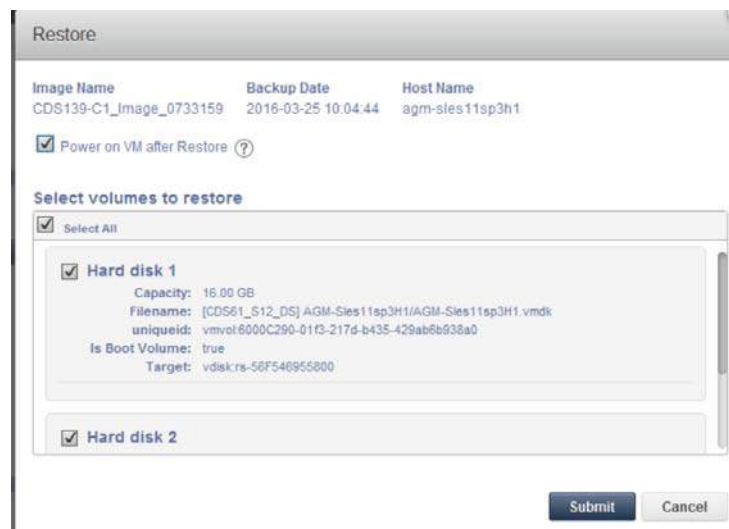
4. Locate the latest (or desired) syncback image in the Restore window; the syncback image appears in yellow. When you select a syncback image it will turn green as shown in the example below.



Selecting a Syncback Image in the Restore Window

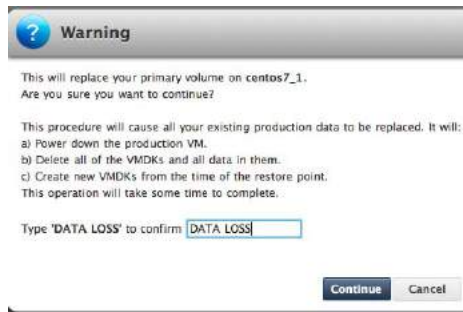
5. From the image information action pull-down menu, select **Restore**. The Restore dialog appears.
 - o Click the check box if you want the VM powered on after restore.
 - o Select the volume(s) to restore.

Click **Submit**.

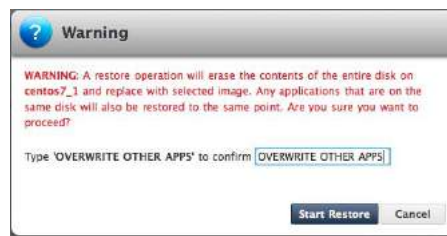


Example of the Restore Dialog for a Syncback Image

6. A warning message appears. Type **DATA LOSS**, then click **Continue**.



7. Depending on the syncback application image that you intend to restore, a second warning message may appear to warn you of overwriting other applications on the disk. Type **OVERWRITE OTHER APPS**, then click **Start Restore**. The restore job starts.



8. You can verify that the restore operation is successful by viewing the job status in System Monitor.
9. After the restore operation is completed successfully:
 - o For a non-VM application, mount the filesystem and restart the application.
 - o For a VM, if you chose not to power it after performing the restore, power on the VM.
10. The production application is back in service, but it is not yet protected again. Proceed to the failback operation, described in [Failback to the Local Appliance](#).

To mount a VM syncback image:

-
- The screenshot displays the Application Manager interface. The top navigation bar includes tabs for APP, VM, GROUP, and HOST. Below this, a search bar and a list of VMs are visible. The VMs are categorized under LOCAL and REMOTE. The main panel shows the details for AGM-Sles11sp3H1, including Host Name, Host IP Address, Description, Protected Data, Folder Path, Unique Name, and Priority. A 'SYNCBACK' button is highlighted in the bottom right corner. A red banner in the top right corner reads 'FAILED OVER'.

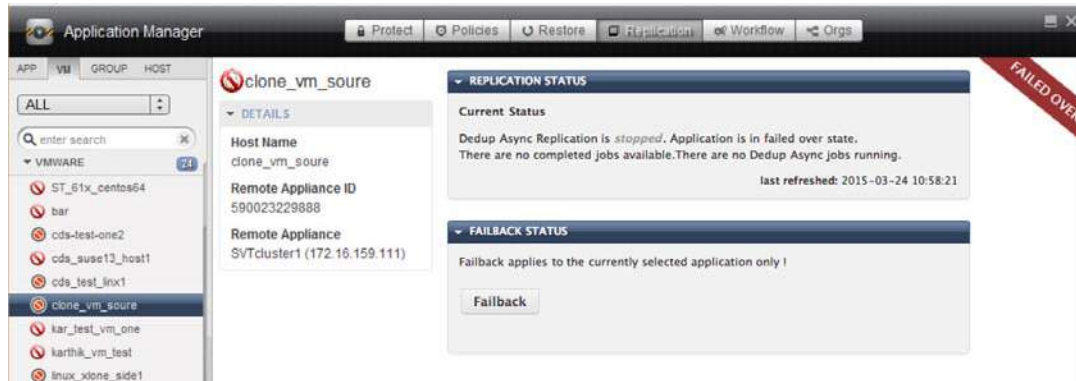
4. From the image information action pull-down menu, select **Mount**. The Mount Job window appears. For details on mounting a VM image, see ***Accessing and Recovering Copy Data with the Application Manager*** in the Actifio Documentation Library.
5. You can verify that the VM image mount operation is successful by viewing the job status in System Monitor.
6. After the VM image mount operation is completed successfully, power on the virtual machine (if necessary) and perform a Storage vMotion to move the mounted disks or VM to the desired datastore.
7. If you mounted to a new VM, this VM must be discovered before it may be protected again. Follow the VM discovery procedure in ***Virtualizing and Protecting Copy Data with the Application Manager*** in the Actifio Documentation Library.
8. The production VM is back in service, but it is not yet protected again. Proceed to the failback operation, described in [Failback to the Local Appliance](#).

Failback to the Local Appliance

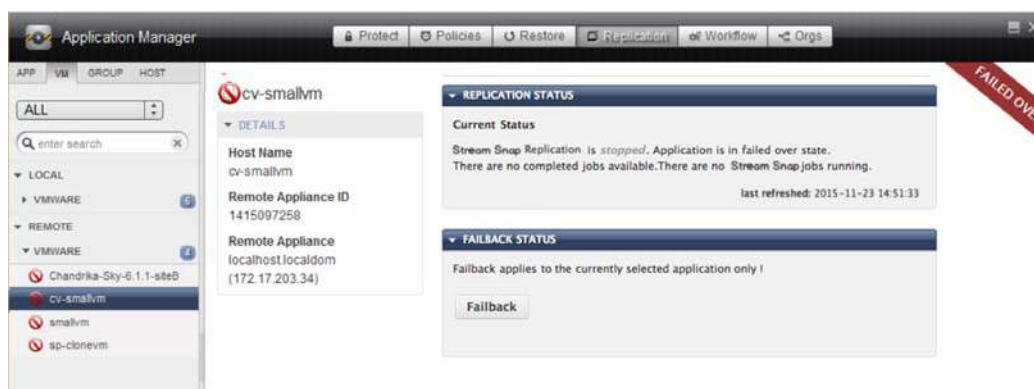
Failback deletes the syncback images brought back from the remote Actifio appliance and the failover image that may still be mounted on the remote Actifio appliance. Failback also deletes any test failover images that remain on the remote Actifio appliance. After these steps are complete, the application resumes the Dedup-Async or StreamSnap replication of the application data from the local appliance to the remote appliance.

To failback an application from the remote appliance to the local appliance:

1. Log into the Actifio Desktop on the **local** appliance and open the Application Manager.
2. Select the failed over application from the navigation pane.
3. Select the Replication tab and click **Failback**. A warning dialog appears.



Replication Tab (Shown for Dedup-Async Replication)



Replication Tab (Shown for StreamSnap Replication)

4. Type **FAILBACK** in the provided field. On successful failback, Dedup-Async or StreamSnap replication to the remote appliance is resumed.



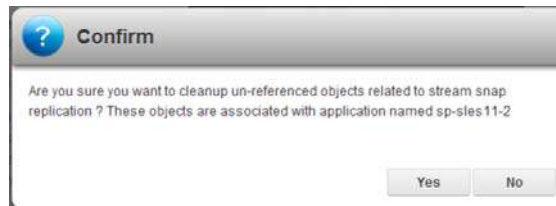
5. Open the System Monitor service from the Actifio Desktop to view the failback job status, including statistics associated with the job.

After failback, the application state changes to Protected and the replication to the remote appliance is resumed.

Deleting Failover and Syncback Images

Normally, all failover, test-failover, and syncback images of an application are deleted when the failback operation is executed. In rare cases, some images created as part of Dedup-Async or StreamSnap replication of an application may not be deleted. To delete the failover, test-failover, and syncback images of an application from the local and remote Actifio appliances:

1. Open the **Application Manager**.
2. Select the application from the navigation pane.
3. Right-click the application image.
4. Select **Cleanup Dedup Async** or **Cleanup StreamSnap**. The Confirm message box appears.
5. Click **Yes** to confirm removing Dedup-Async or StreamSnap protection and to cleanup any related objects.



Note: If any of the images remain, the Cleanup option appears on right-clicking the application. Use this option to delete the images.

6 Performing Synchronous and Asynchronous Replication

This chapter outlines the procedures to implement synchronous or asynchronous replication on your Actifio CDS appliance:

- [Initial Configuration Tasks Prior to Performing Sync and Async Replication](#) on page 51
- [Configuring Synchronous Replication for In-Band Generic Applications](#) on page 52
- [Configuring Asynchronous Replication for In-Band Generic Applications](#) on page 54

Note: *Synchronous and Asynchronous replication are not supported on an Actifio Sky appliance.*

Initial Configuration Tasks Prior to Performing Sync and Async Replication

Before you initiate a synchronous or asynchronous replication operation you must first ensure that the local and remote Actifio CDS appliances are properly configured as outlined below:

1. Unmap the disks from the back-end array to the production host.
2. Present storage (MDisk) using a Fibre Channel link from the back-end array (for example, v3700, EMC storage or NetApp storage) to the Actifio CDS appliance.
3. Create image-mode vDisks on the Actifio CDS appliance from each of the MDisk.
4. Map the vDisks to the production host. The host can now see the same data through the Actifio CDS appliance that it was originally seeing directly from the array.
5. Create a generic application on the Actifio CDS appliance using the disks mapped to the host. You create a generic application using the New Application function in the Application Manager service of the Actifio CDS appliance. Generic applications are defined by the LUNs they consist of (for example, a 1 GB LUN that is mapped to the host 'actifio-w2k3'). Assign the in-band LUN(s) that you want to replicate to it.

See the “Creating Generic Applications” procedure in ***Virtualizing and Protecting Copy Data with the Application Manager*** in the Actifio Documentation Library.

6. Make sure both the local and remote Actifio appliances are configured, joined (exchange security certificates), and partnered in Sharing Mode.

See ***Configuring Resources and Settings With the Domain Manager*** in the Actifio Documentation Library.

7. Zone together the appliances from the primary (local) Actifio appliance (A) and the remote Actifio CDS appliance (B) in order for the B side to be the target for replication.

Note: *The remote Actifio CDS appliance (B) side appliance must have matching vDisks of equal size. If the B side vDisk needs to be accessed by the same host, the host will need to be added to the B-side Actifio CDS appliance and is given the mapping to the destination vDisk through iSCSI or a Fibre Channel link.*

8. From the Actifio CDS appliance, configure the Sync or Async replication policy as outlined in the appropriate procedure:

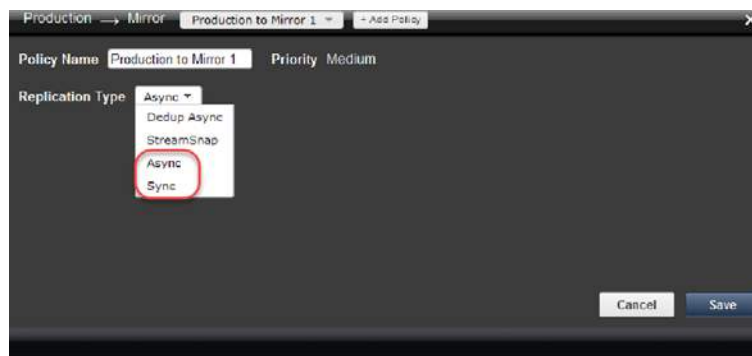
[Configuring Synchronous Replication for In-Band Generic Applications](#) on page 52

[Configuring Asynchronous Replication for In-Band Generic Applications](#) on page 54

Configuring Synchronous Replication for In-Band Generic Applications

To set up synchronous replication for an in-band generic application:

1. Make sure the Actifio appliances are configured as detailed in [Initial Configuration Tasks Prior to Performing Sync and Async Replication](#) on page 51.
2. In the **Domain Manager** open **System > Configuration > Appliance Settings > Appliance Manager** and select the Sync/Async tab. Enable the Fibre Channel partnership between appliances and assign a bandwidth throttle. Replication will not start until a bandwidth throttle is assigned.
3. In the **SLA Architect**, create a policy template that includes a **Production to Mirror - Sync** replication policy. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for details on creating an Async replication policy.



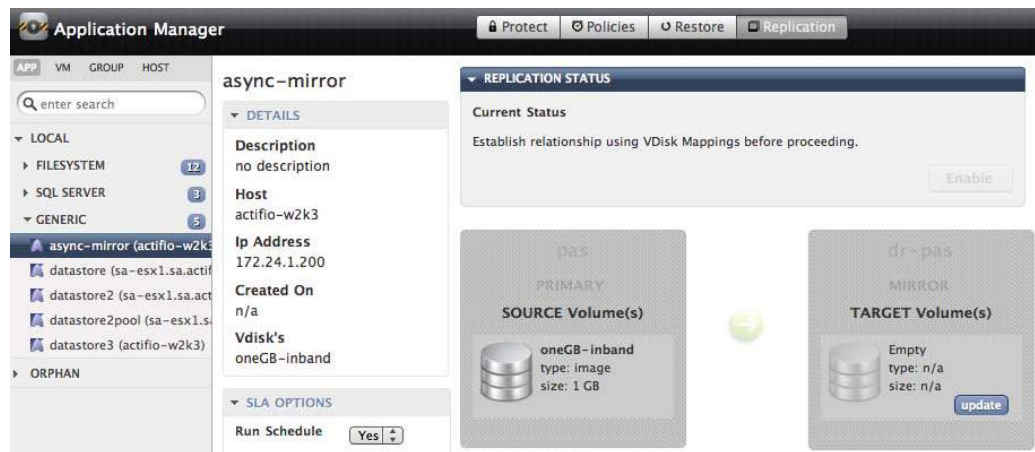
Creating a Sync Production to Mirror Replication Policy

4. In the **SLA Architect**, create a resource profile that specifies where to store data locally as well as where to replicate data.

Note: For background details on creating a resource profile, see **Planning and Developing Service Level Agreements** in the Actifio Documentation Library.

5. Open the Actifio Desktop to the **Application Manager**.
 - o If you have not yet created a generic application using the New Application function in the Application Manager, see the "Creating Generic Applications" procedure in **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library.
 - o Select the **Production to Mirror - Sync** policy template from the Template drop-down list.
 - o Select the resource profile from Profile drop-down list configured to include a remote Actifio appliance.
 - o Click **Protect** to apply the Production to Mirror policy template to the generic application (see [Initial Configuration Tasks Prior to Performing Sync and Async Replication](#) on page 51).

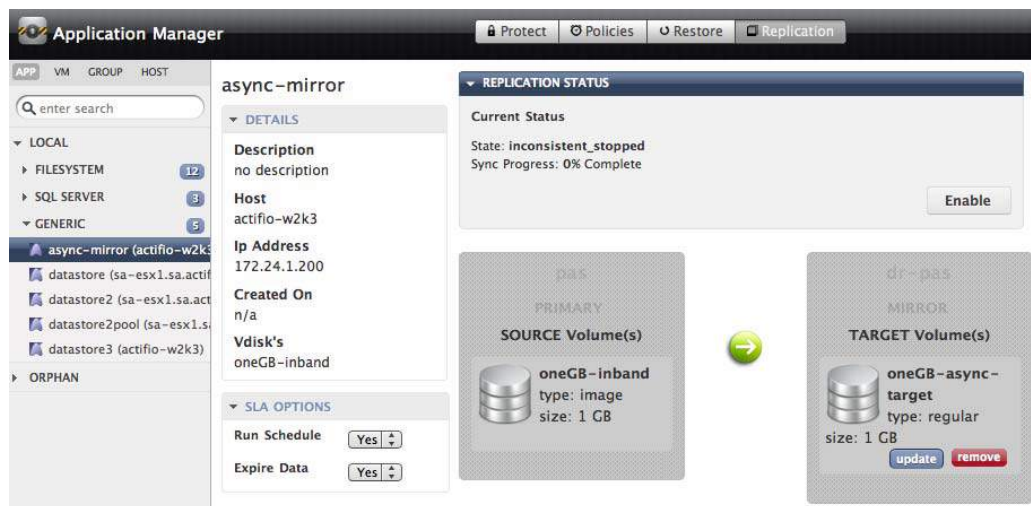
- On the Replication tab, click **update** to choose the replication target.



Choosing the Replication Target Volume

You are presented with a dialog to choose an MDisk, a VDisk, or an MDiskgroup to replicate to at the target site. You can get the MDisk number from Create VDisk in **Domain Manager > Host > Storage** at the target site.

- Select a target volume and give it a name.
- Enable the replication by clicking **Enable** in Replication Status.



Enabling Replication

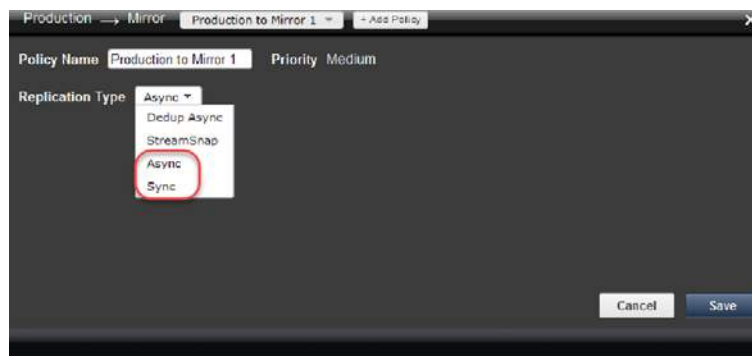
- The status changes from *inconsistent* to *inconsistent_copying*.
Once the initial synchronization is complete, the status changes to *consistent_synchronized* and sync replication is fully underway. The initial synchronization depends on the bandwidth available and the size of the volume(s).
- Based on your access and recovery requirements of the data replicated to the remote site, you can perform a Mount, Clone, or Restore operation.

For details on performing Mount, Clone, or Restore operations on your applications or VMs, see **Accessing and Recovering Copy Data with the Application Manager** and **Restoring Copy Data with the Application Manager** in the Actifio Documentation Library.

Configuring Asynchronous Replication for In-Band Generic Applications

To set up asynchronous replication for an in-band generic application:

1. Make sure the Actifio appliances are configured as detailed in [Initial Configuration Tasks Prior to Performing Sync and Async Replication](#) on page 51.
2. In the **Domain Manager** open **System > Configuration > Appliance Settings > Appliance Manager** and select the Sync/Async tab. Enable the Fibre Channel partnership between appliances and assign a bandwidth throttle. Replication will not start until a bandwidth throttle is assigned.
3. In the **SLA Architect**, create a policy template that includes a **Production to Mirror - Async** replication policy. See **Planning and Developing Service Level Agreements** in the Actifio Documentation Library for details on creating an Async replication policy.



Creating an Async Production to Mirror Replication Policy

4. Open the Actifio Desktop to the **Application Manager**.
 - o If you have not yet created a generic application using the New Application function in the Application Manager, see the "Creating Generic Applications" procedure in **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library.
 - o Select the **Production to Mirror - Async** policy template from the Template drop-down list.
 - o Select a resource profile from Profile drop-down list configured to include a remote Actifio appliance.
 - o Click **Protect** to apply the Production to Mirror policy template to the generic application (see [Initial Configuration Tasks Prior to Performing Sync and Async Replication](#) on page 51).

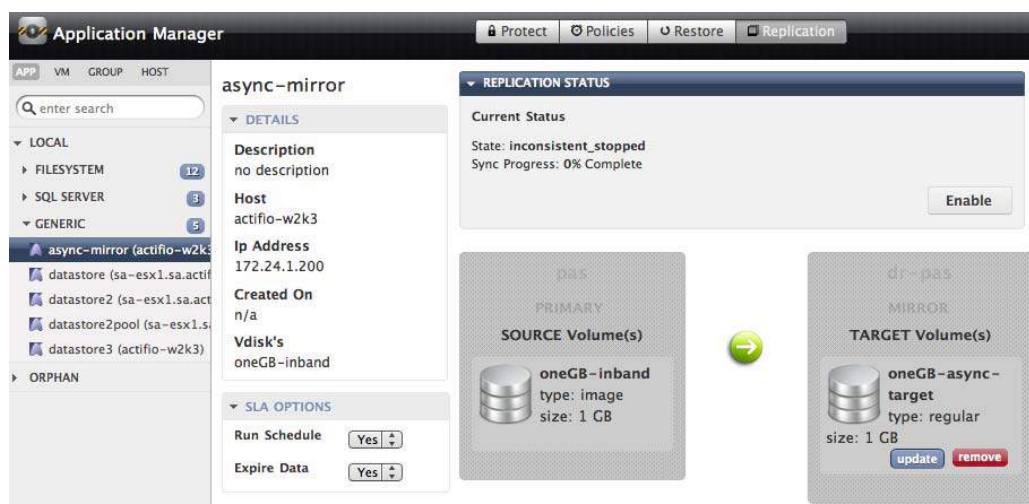
- On the Replication tab, click **update** to choose the replication target.



Choosing the Replication Target Volume

You are presented with a dialog to choose an MDisk, a VDisk, or an MDiskgroup to replicate to at the target site. You can get the MDisk number from Create VDisk in **Domain Manager > Host > Storage** at the target site.

- Select a target volume and give it a name.
- Enable the replication by clicking **Enable** in Replication Status.



Enabling Replication

- The status changes from *inconsistent_stopped* to *inconsistent_copying*.
Once the initial synchronization is complete, the status changes to *consistent_asynchronized* and async replication is fully underway. The initial synchronization depends on the bandwidth available and the size of the volume(s).
- Based on your access and recovery requirements of the data replicated to the remote site, you can perform a Mount, Clone, or Restore operation.

For details on performing Mount, Clone, or Restore operations on your applications or VMs, see **Accessing and Recovering Copy Data with the Application Manager** and **Restoring Copy Data with the Application Manager** in the Actifio Documentation Library.

7 StreamSnap Jobs and Error Handling

When an SLA template includes a StreamSnap replication policy and a Snapshot policy, and you apply that SLA template to an application or VM in the Application Manager, the System Monitor records the results of the StreamSnap job. While it is running, the StreamSnap job appears as a single job in System Monitor. Once replication is complete, two jobs appear in System Monitor; one for the Snapshot job and a second for the StreamSnap job.

Note the following ways an Actifio appliance tracks those jobs:

- If replication succeeds, two separate job entries appear in the list of jobs in the System Monitor with a **Succeeded** status. Both job entries have the same Job Name, except that the StreamSnap job also includes an "S" suffix in its Job Name.
- If there is a job failure, for either the StreamSnap job or the Snapshot job, two job entries appear in the list of jobs in the System Monitor to identify which job was successful and which job failed.

Note: Failover, test failover, and syncback jobs that have been triggered for a StreamSnap image will appear in the List of Jobs when you filter the type of job either by StreamSnap or Dedup Async. The Actifio Desktop System Monitor does not distinguish between the two images as they relate to failover, test failover, and syncback job types.

Data Movement during a StreamSnap Job

A StreamSnap replication job comprises two distinct tasks, with two different entries in the job history (jobs with the same job ID, with the "S" appended to the StreamSnap job). The tasks generate different metrics.

- **Data Capture from the source:** This is performed the same way as a standard snapshot job. A key metric for this task is "Data copied", which shows how much new data was copied from the source application to the Actifio snapshot pool.
- **Data Replication from appliance to appliance:** Two key metrics for the replication task are "Data sent over network" and "Data written at remote side".

It would seem that the values for the Data Capture metric "Data copied" and the Data Replication metric "Data written at remote side" would be the same. When you look at Snapshot and StreamSnap job pairs in the Job History, you may sometimes see that this is not so. This is because it is possible that some snapshots will be replicated while others will not be.

For example, snapshots may be set up to run hourly and daily with different retention periods. Consider a StreamSnap policy linked to the daily snapshot policy. In this situation, the data written at the remote site would be *close* to the sum of the values for data copied for all snapshot jobs since the previous StreamSnap job. The values will not *exactly* match as blocks of data that changed multiple times since the previous StreamSnap job may have been copied multiple times in multiple snapshots, but only written once at the remote site during the StreamSnap job.

System Monitor

Jobs Events

Filter by Date: LAST 24 HRS, LAST WEEK, LAST MONTH, LAST 3 MONTHS, CUSTOM DATES

Filter by Status: ALL, RUNNING, SUCCEEDED, CANCELED, RETRIED, FAILED, QUEUED

Filter by Type: ALL, SNAPSHOT, DEDUP, EXPIRATION, GARBAGE COLLECTION, MOUNT, UNMOUNT, CLONE, LIVECLONE, RESTORE, DELETE, VERIFICATION, DEDUP ASYNC, STREAMSNAP, REMOTE

Search: [Search] [Clear Search] [Change Priority] [View Details] [Cancel Job]

Job Name	Type	Priority	Status	Host	Application	Policy	Template	Consistency De	Start Time	End Time
Job_5511816	streamsnap	medium	running: 4%	sp-sles11	perfgn	ssonlystream	streamsnap_ssonly	Mar 16 15:43	Mar 16 15:43	
Job_5511813	dedup	medium	succeeded	agent008	/boot	Snapshot to	streamsnap03_ded	Mar 16 15:42	Mar 16 15:43	
Job_5511790	streamsnap	medium	succeeded	agent008	/boot	Production to	streamsnap03_ded	Mar 16 15:42	Mar 16 15:42	
Job_5511788	streamsnap	medium	running: 16%	sp-sles11-2	sp-sles11-2	Production to	streamsnap03_ded	Mar 16 15:42	Mar 16 15:42	
Job_5511770	snapshot	medium	succeeded	sp-smallvm	sp-smallvm	ssonlysnap	streamsnap_ssonly	Mar 16 15:41	Mar 16 15:41	Mar 16 15:42
Job_5511770S	streamsnap	medium	succeeded	sp-smallvm	sp-smallvm	ssonlystream	streamsnap_ssonly	Mar 16 15:41	Mar 16 15:41	Mar 16 15:42
Job_5511794	expiration		succeeded	sp-smallvm	sp-smallvm	ssonlystream	streamsnap_ssonly	Mar 16 15:42	Mar 16 15:42	Mar 16 15:42
Job_5511718	snapshot	medium	succeeded	sp-démovm	sp-démovm	ss01snap2	streamsnap01	Mar 16 15:40	Mar 16 15:40	Mar 16 15:42
Job_5511780	expiration		succeeded	sp-sles11	v2vgen7	Production to	streamsnap03_ded	Mar 16 15:41	Mar 16 15:41	Mar 16 15:42
Job_5511694	snapshot	medium	succeeded	sp-sles11-2	sp-sles11-2	Production to	streamsnap03_ded	Mar 16 15:39	Mar 16 15:39	Mar 16 15:41
Job_5511694S	streamsnap	medium	succeeded	sp-sles11-2	sp-sles11-2	Production to	streamsnap03_ded	Mar 16 15:39	Mar 16 15:39	Mar 16 15:41
Job_5511767	dedup	medium	succeeded	sp-sles11	v2vgen7	Snapshot to	streamsnap03_ded	Mar 16 15:41	Mar 16 15:41	Mar 16 15:41
Job_5511741	snapshot	medium	succeeded	sp-sles11	v2vgen7	Production to	streamsnap03_ded	Mar 16 15:41	Mar 16 15:40	Mar 16 15:41
Job_5511741S	streamsnap	medium	succeeded	sp-sles11	v2vgen7	Production to	streamsnap03_ded	Mar 16 15:41	Mar 16 15:40	Mar 16 15:41
Job_5511728	snapshot	medium	succeeded	agent008	/home	ss01snap2	streamsnap01	Mar 16 15:40	Mar 16 15:40	Mar 16 15:41
Job_5511742	expiration		succeeded	sp-sles11-2	sp-sles11-2	Production to	streamsnap03_ded	Mar 16 15:40	Mar 16 15:40	Mar 16 15:41
Job_5511740	expiration		succeeded	agent008	/boot	Production to	streamsnap03_ded	Mar 16 15:40	Mar 16 15:40	Mar 16 15:40
Job_5511719	dedup	medium	succeeded	agent008	/boot	Snapshot to	streamsnap03_ded	Mar 16 15:39	Mar 16 15:40	Mar 16 15:40
Job_5511695S	streamsnap	medium	succeeded	agent008	/boot	Production to	streamsnap03_ded	Mar 16 15:39	Mar 16 15:39	Mar 16 15:40

Updated: 2016-03-16 15:52:49 # Job(s): 6633 Page 1 of 350 Displaying jobs: 1-19

System Monitor with Successful StreamSnap and Snapshot Jobs

System Monitor

Jobs Events

Filter by Date: LAST WEEK, LAST MONTH, LAST 3 MONTHS, CUSTOM DATES

Filter by Status: ALL, RUNNING, SUCCEEDED, CANCELED, RETRIED, FAILED, QUEUED

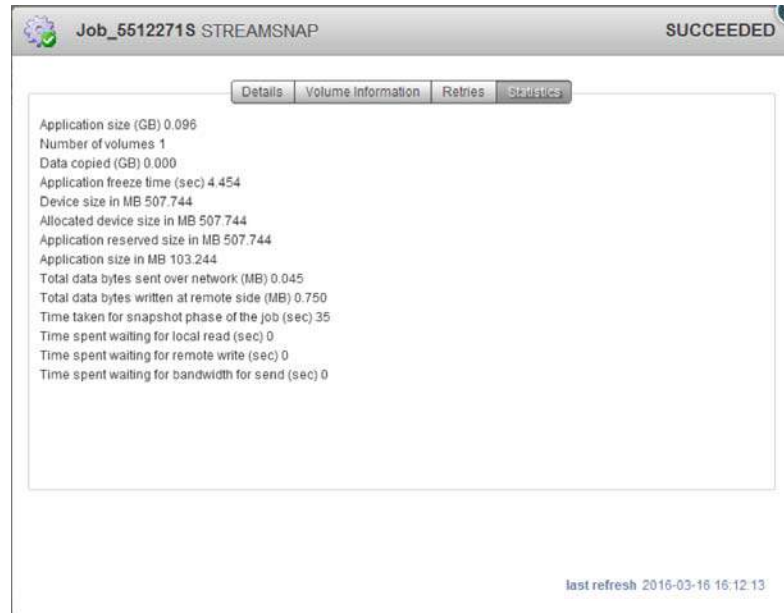
Filter by Type: ALL, SNAPSHOT, DEDUP, EXPIRATION, GARBAGE COLLECTION, MOUNT, UNMOUNT, CLONE

Search: [Search] [Clear Search] [Change Priority] [View Details] [Cancel Job]

Job Name	Type	Priority	Status	Host	Application	Policy	Template	Consistency	Start Time	End Time
Job_4939650	expiration		succeeded	smallvm	smallvm	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939649	expiration		succeeded	agent008	/mnt/ssmnt	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939641	streamsnap	medium	failed	accoraprod	accprddb	ss02_stream	streamsnap02	Feb 12 11:1	Feb 12 11:0	Feb 12 11:1
Job_4939641	snapshot (DE	medium	succeeded	accoraprod	accprddb	ss02_snap	streamsnap02	Feb 12 11:1	Feb 12 11:0	Feb 12 11:1
Job_4939620	expiration		succeeded	sp-sles11-2	sp-sles11-2	ss02_stream	streamsnap02	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939616	streamsnap	medium	failed	agent008	/mnt/ssmnt	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939616	snapshot	medium	succeeded	agent008	/mnt/ssmnt	ssonlysnap	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939608	streamsnap	medium	failed	smallvm	smallvm	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939608	snapshot	medium	succeeded	smallvm	smallvm	ssonlysnap	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939607	streamsnap	medium	failed	sp-démovm	sp-démovm	Production	streamsnap03	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939607	snapshot	medium	succeeded	sp-démovm	sp-démovm	Production	streamsnap03	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939593	expiration		succeeded	agent008	/mnt/ssmnt	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939586	snapshot	medium	succeeded	sp-sles11	v2vgen7	ss01snap2	streamsnap01	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939585	expiration		succeeded	smallvm	smallvm	ssonlystream	streamsnap_ss	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939573	streamsnap	medium	failed	sp-sles11-2	sp-sles11-2	ss02_stream	streamsnap02	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0
Job_4939573	snapshot	medium	succeeded	sp-sles11-2	sp-sles11-2	ss02_snap	streamsnap02	Feb 12 11:0	Feb 12 11:0	Feb 12 11:0

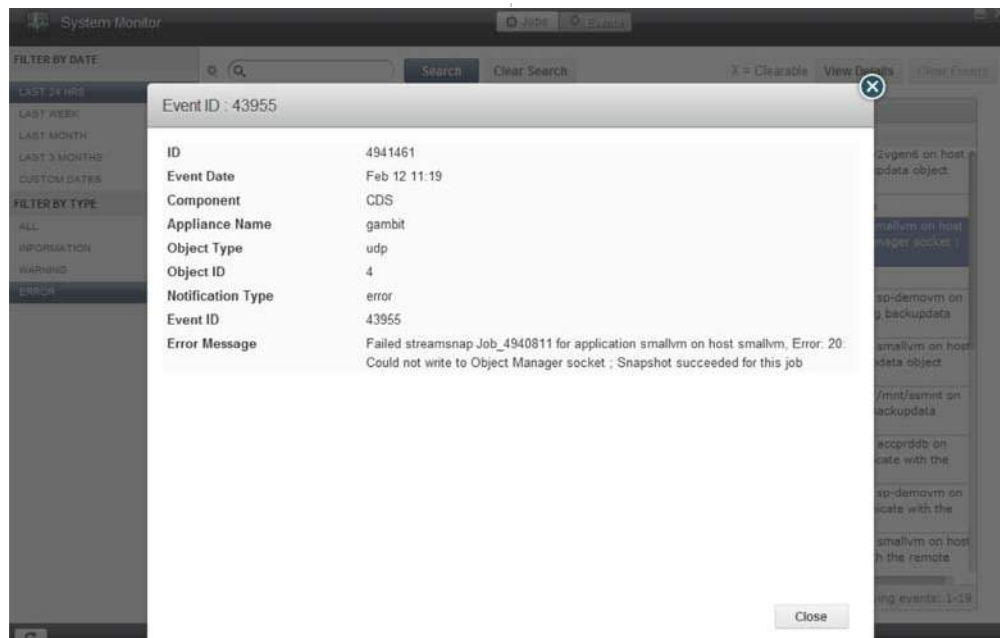
System Monitor with a Successful Snapshot Job But a Failed StreamSnap Job

The start and end times of the StreamSnap job entry and the Snapshot job entry will be identical in System Monitor. The actual amount of time taken for the Snapshot phase is listed in the Statistics page for the StreamSnap job.



StreamSnap Job Statistics

Here is an example of a typical event in System Monitor indicating that a StreamSnap job failed but that the associated Snapshot job succeeded.



Viewing an Event for a Failed StreamSnap Job

The following table outlines the job history and error handling behavior of an Actifio appliance based on the success or failure of the Snapshot policy and the StreamSnap replication policy when used to protect an application.

Protection Scenario	Job History Behavior
Both the Snapshot and StreamSnap jobs succeed	Two separate job entries appear in the list of jobs with Succeeded status when the job completes. Both job entries have the same Job Name, except that the StreamSnap job also includes an "S" suffix in its Job Name.
Snapshot job succeeds, StreamSnap job fails	For the Snapshot job - one job entry appears in the list of jobs with Succeeded status. For the StreamSnap job - one job entry appears with Failed status.
Both the Snapshot and StreamSnap jobs fail but then the Actifio appliance attempts a retry	One StreamSnap job entry appears in the list of jobs with Retried status. If the Snapshot job succeeds but the StreamSnap job still fails, this results in two job entries as outlined above and there will be no further retries for StreamSnap.
Both the individual Snapshot and StreamSnap jobs fail after maximum number of retries	One StreamSnap job entry appears in the list of jobs with Failed status.

Index

A

- Actifio data replication technology 1
- Actifio OnVault 6, 19, 20
- appliance zoning 51
- appliances in sharing mode 11, 24, 27, 51
- Application Manager
 - failback to local appliance 48
 - failing back from the remote appliance 41
 - failing over a protected application 33
 - failing over a protected VM 35
 - generic applications 51
 - protecting applications and VMs 12, 16, 20, 26, 28
 - protecting generic applications 52
 - Remote Replicate dialog box 17
 - replicate to remote appliance (multi-hop) 17
 - replication target, choosing 53, 55
 - restoring application data from a synchronized image 44
 - running catch-up syncback 42
 - running final syncback 43
 - testing failover 30
- Async replication 10, 51, 54

B

- benefits table for replication methods 2

C

- contact information, Actifio Support ii
- copyright ii

D

- data mirroring 2, 7
- Dedup Back policy template 2
- Dedup Backup replication
 - benefits 2
 - Dedup Backup to Dedup DR policy template 11, 15
 - overview 4
 - procedure 11
 - resource profile 12
- Dedup Backup to Dedup DR policy template 11, 15
- Dedup-Async replication

- benefits 3
- cleanup images 49
- failing over a protected application 33
- failing over a protected VM 35
- overview 7
- Production to Mirror Dedup-Async policy template 25, 27
- resource profile 26, 28
- testing failover 30
- VM override 24

E

- ESX datastore, failover to 24

F

- failback
 - catch-up syncback 42
 - failing back from the remote appliance 41
 - final syncback 43
 - restoring syncback image 44
 - stopping the failed-over application 43
 - to local appliance 48
- failover
 - deleting failover image manually 49
 - deleting test failover image 32
 - failing over a protected application 33
 - failing over a protected VM 35
 - Test Failover dialog 31
 - test failover usage considerations 30
 - testing 30
 - to an ESX datastore 24

G

- generic applications, creating 51

H

- high availability of applications 10

L

- legal matter ii
- long-term storage of deduplicated data 11

M

Multi-hop replication

- between primary appliance and two remote appliances 15
- configuring second leg of a multi-hop configuration 15
- overview 5
- Remote Replicate dialog box 17
- replicate to remote appliance 17
- resource profile 16
- Second Hop Replication policy template 15
- SLA policy templates 15
- use cases 5

O

Object storage 6, 19

OnVault storage pool 19

P

Production to Mirror Async policy template 2, 54

Production to Mirror Dedup-Async policy template 2, 25, 27

Production to Mirror policy template 11, 19, 25, 27

Production to Mirror replication

- Dedup-Async overview 7
- overview 7
- StreamSnap overview 8
- Sync/Async overview 10

Production to Mirror StreamSnap policy template 2, 27

Production to Mirror Sync policy template 2, 52

Production to Snap policy template 11, 19, 25, 27

R

ReadyVM 24

replication

- Actifio data replication overview 1
- benefits of each method 2
- between primary appliance and two remote appliances 15
- Dedup Backup overview 4
- methods 2
- Multi-hop replication overview 5
- Production to Mirror Dedup-Async overview 7
- Production to Mirror overview 7
- Production to Mirror Sync/Async overview 10
- replicate to remote appliance (multi-hop) 17
- Snapshot to OnVault overview 6
- StreamSnap overview 8

resource profile

- Async replication 54
- Dedup Backup replication 12
- Dedup-Async replication 26, 28
- multi-hop replication 16

Snapshot to OnVault replication 20

StreamSnap replication 26, 28

Sync replication 52

restoring application data from a synchronized image 44

S

Second Hop Replication policy template 15

Snapshot to OnVault policy template 2, 19

Snapshot to OnVault replication

- benefits 2
- configuring 19
- OnVault pools 20
- overview 6
- resource profile 20
- Snapshot to OnVault policy template 19

StreamSnap replication

- benefits 3
- cleanup images 49
- failing over a protected application 33
- failing over a protected VM 35
- job failure 57, 58, 59
- job protection scenarios 60
- job start and end times 59
- job success 57, 58
- jobs 57
- overview 8
- Production to Mirror StreamSnap policy template 27
- resource profile 26, 28
- testing failover 30

Sync replication 10, 51, 52

Sync/Async replication

- Async policy template 54
- benefits 3
- configuring 52
- enabling replication 53, 55
- Fibre Channel partnership 52, 54
- initial configuration tasks 51
- MDisk, VDisk, or MDiskgroup, choosing 53, 55
- overview 10
- replication target, choosing 53, 55
- resource profile 52, 54
- status 53, 55
- Sync policy template 52

syncback

- deleting image manually 49
- restoring image 44
- running catch-up syncback 42
- running final syncback 43

System Monitor

- StreamSnap job failure 58, 59
- StreamSnap job protection scenarios 60

StreamSnap job start and end times 59
StreamSnap job success 58
tracking StreamSnap jobs 57

T

test-failover images, deleting 32, 49
trademarks ii

W

warranty ii