

---

# Planning and Developing Service Level Agreements

## 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](mailto:docs@actifio.com).





# Contents

<b>Preface .....</b>	<b>v</b>
Actifio Appliances .....	v
The ActifioNOW Customer Portal .....	v
Actifio Support Centers .....	v
<b>Chapter 1 - Introduction to the Actifio SLA Architect .....</b>	<b>1</b>
Policy Templates .....	2
Policy Advanced Settings Override .....	4
Host-Side Script Timeouts .....	5
Appliance Specific Policy Templates .....	6
Resource Profiles .....	7
<b>Chapter 2 - Best Practices for Policy Templates .....</b>	<b>9</b>
Initial Data Capture .....	10
Resizing Volumes .....	10
System Resources .....	10
Concurrency .....	11
Policy Schedules .....	11
Calculating Frequency .....	13
Job Priority and Scheduling .....	14
Job Retries .....	14
Policy Compliance Settings .....	15
Windowed Policy Compliance Settings .....	16
Continuous Policy Compliance Settings .....	16
Policy Specific Best Practices .....	18
Production to Snapshot Policies .....	19
Database Log File Snapshot Policies .....	22
Snapshot to Dedup Backup Policies .....	23
Production to Direct to Dedup Policies .....	24
Dedup Backup to Dedup DR Policy Policies .....	25
Dedup DR to Remote Replication Policies (Multi-hop Replication) .....	26
Snapshot to OnVault Policies .....	28
Production to Mirror Policies .....	29
Scheduling Policy Best Practices at a Glance .....	33
Application Specific Best Practices .....	35

<b>Chapter 3 - Policy and System Resource Considerations .....</b>	<b>37</b>
Impact of Policy Settings on System Performance .....	38
Validating Projected Resources for a Policy .....	39
Resolving Warnings.....	41
Viewing the Top 10 policy templates in the Domain Manager .....	42
<b>Chapter 4 - Creating and Managing Policy Templates .....</b>	<b>43</b>
Creating and Modifying a Policy Template .....	44
Configuring Host-Side Script Timeouts .....	46
Cloning a Policy Template .....	47
Exporting a Policy Template .....	47
Importing a Policy Template .....	47
Viewing Policy Templates .....	48
Deleting a Policy Template .....	48
Viewing Policy Schedules .....	49
Viewing the Applications Protected by a Policy Template .....	50
Viewing and Modifying Organizations and Policy Relationship .....	50
<b>Chapter 5 - Creating Policies .....</b>	<b>51</b>
Creating a Production to Snapshot Policy .....	52
Creating a Snapshot to OnVault Policy .....	58
Creating a Snapshot to Dedup Backup Policy .....	60
Creating a Production Direct-to-Dedup Policy .....	63
Creating a Dedup Backup to Dedup DR Policy .....	68
Creating a Multi-hop Remote Dedup Backup Replication Policy .....	71
Creating a Production to Mirror Policy .....	74
Creating a Dedup-Async Replication (DAR) Production to Mirror Policy .....	75
Creating a StreamSnap Production to Mirror Replication Policy .....	79
Creating a Synchronous or Asynchronous Production to Mirror Replication Policy .....	80
<b>Chapter 6 - Creating and Managing Resource Profiles .....</b>	<b>83</b>
Creating a Resource Profile .....	84
Creating a Resource Profile for a Multi-hop Configuration .....	85
Cloning a Resource Profile .....	86
Viewing Resource Profiles .....	87
Deleting a Resource Profile .....	88
<b>Index .....</b>	<b>89</b>

---

# Preface

---

This guide provides step-by-step instructions on how to use the Actifio SLA Architect. 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 online, downloaded, or 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***
- ***Connecting Hosts to Actifio Appliances***
- ***Virtualizing and Protecting Copy Data with the Application Manager***
- ***Accessing and Recovering Copy Data with the Application Manager***
- ***Performing Replication Using Actifio Appliances***

## 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](mailto:support@actifio.com)
- Call:
  - From anywhere:** +1.315.261.7501
  - US Toll-Free:** +1.855.392.6810
  - Australia:** 0011 800-16165656
  - Germany:** 00 800-16165656
  - New Zealand:** 00 800-16165656
  - UK:** 0 800-0155019





# 1 Introduction to the Actifio SLA Architect

**Note:** If you are new to managing data with an Actifio appliance, Actifio recommends you first familiarize yourself with the concepts presented in **Getting Started with Actifio Copy Data Management**. This guide can be found in the Actifio Documentation Library and the Actifio Now customer portal.

From the SLA Architect you can create policy templates and resource profiles. Policy templates and resource profiles are applied to applications and VMs in the Application Manager. The SLA for an application or VM is defined by the combination of the policy template and the resource profile applied to that application or VM.



**SLA Architect**

This chapter provides an overview of the basic concepts associated with policy templates and resource profiles.

[Policy Templates](#) on page 2

[Policy Advanced Settings Override](#) on page 4

[Host-Side Script Timeouts](#) on page 5

[Appliance Specific Policy Templates](#) on page 6

[Resource Profiles](#) on page 7

## Policy Templates

A policy template is a collection of policies. A policy defines:

- How often data will be protected
- Whether data will be protected as a snapshot or sent directly to deduplication
- Whether data will be deduplicated
- How long data will be retained
- Whether or not data will be replicated to another Actifio appliance

Policies reside in policy templates. The green arrows displayed in the graphical SLA policy map represent the individual policies in the template. Dark green arrows indicate that a policy has been defined. Light green arrows indicate that a policy is not or cannot be defined for the policy template.

A policy template can be made up of one or more of the following policies:

- **Production to Snapshot** policy defines when and how often production data will be captured and how many snapshots are retained. Data recovery from the Snapshot Pool is fast because images have not been deduplicated; they are still stored in the local Snapshot Pool. Snapshots are meant for short term retention. See [Creating a Production to Snapshot Policy](#) on page 52 for details.
- **Snapshot to Dedup Backup** policy defines when to deduplicate snapshot data and how long to retain the deduplicated data. Data in the Dedup Backup Pool is meant for longer term retention. If you take many snapshots in a short time, you can dedup the snapshots sometime later. This prevents the dedup jobs from competing with the more time-critical snapshot jobs for system resources. See [Creating a Snapshot to Dedup Backup Policy](#) on page 60 for details.
- **Production Direct-to-Dedup** policy defines when to deduplicate VMware VMs directly from production data and how long to retain the deduplicated data. Capturing VMware VMs directly to a Dedup Backup Pool is meant for long term retention when instant access from a Snapshot Pool is not required. See [Creating a Production to Mirror Policy](#) on page 74 for details.
- **Dedup Backup to Dedup DR** policy defines when to replicate deduplicated data to a remote Actifio appliance's Local Dedup Pool and how long to retain the data in that pool. Data in the Dedup DR Pool is meant for retention of data in case of a disaster at the local appliance's site. See [Creating a Production Direct-to-Dedup Policy](#) on page 63 for details.
- **Dedup DR to Remote Replication** policy defines the second leg in a multi-hop replication scheme. Multi-hop replication enables you to store a deduplicated backup image from the primary Actifio appliance to two remote Actifio appliances. See [Creating a Multi-hop Remote Dedup Backup Replication Policy](#) on page 71.
- **Snapshot to OnVault** policy allows you to replicate data to an Actifio OnVault Storage Pool. An Actifio OnVault storage pool is typically used for long-term retention and consists of file system and application data. See [Creating a Snapshot to OnVault Policy](#) on page 58.

- **Production to Mirror** policy defines how data will be replicated to a Mirror Pool (a Snapshot Pool on a remote Actifio appliance). Data in the Mirror Pool is meant for instant recovery in a disaster recovery scenario. When creating a Production to Mirror policy you can choose from the following types of replication:
  - o **Dedup-Async Replication (DAR)** - Uses dedup processing for bandwidth efficient replication. See [Creating a Dedup-Async Replication \(DAR\) Production to Mirror Policy](#) on page 75 for details.
  - o **StreamSnap Replication** - Replicates a point-in-time snapshot of the original application without performing deduplication. See [Creating a StreamSnap Production to Mirror Replication Policy](#) on page 79 for details.
  - o **Synchronous (Sync) and Asynchronous (Async) Replication** - For use only with generic applications on an Actifio CDS appliance. See [Creating a Synchronous or Asynchronous Production to Mirror Replication Policy](#) on page 80 for details.

---

**Note:** For details on replicating data, see **Replicating Data Using Actifio Appliances** in your Actifio Documentation Library and available on the Actifio Now customer portal.

---

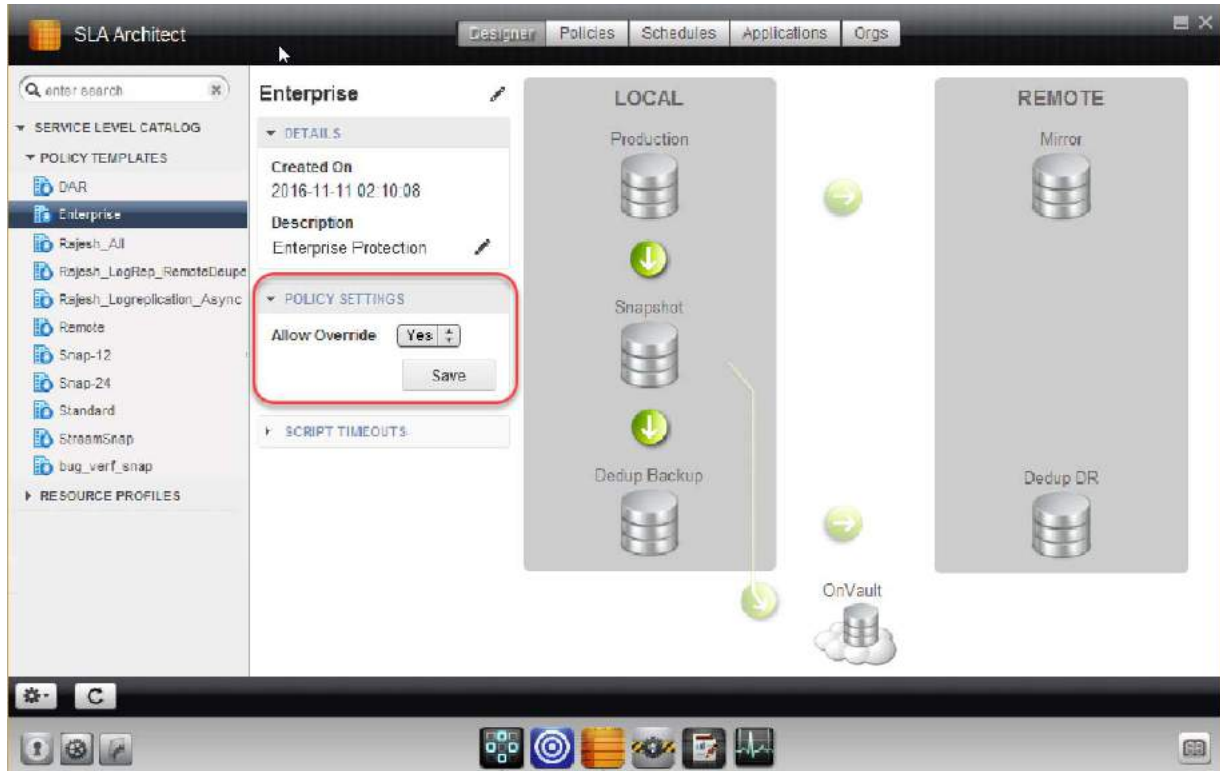
The SLA Architect enforces a specific policy development sequence when you define the policies associated with a policy template. Certain policies will be unavailable based on the type of policy template you develop. In addition, the types of policy templates and the minimum and maximum settings of policies are specific to the Actifio appliance on which they reside. policy templates are applied to applications in the Application Manager.

## Policy Advanced Settings Override

Policies contain a series of advanced settings for all applications supported by an Actifio appliance. When creating a policy you can define the policy advanced settings that are most appropriate for the application to which the policy's template will be applied. See [Creating Policies](#) on page 51 for detailed descriptions of various advanced settings that can be configured on a per-policy basis.

Advanced settings specified in a policy are then applied in the Application Manager to all applications to which the policy's template is applied.

Advanced Settings defined in a policy can be overridden by application-specific Advanced Settings in the Application Manager, provided that the template has been set to allow policy overrides. You can override policy settings in the Application Manager only if the policy template Allow Override parameter has been set to **Yes**.



**Policy Settings Allow Override Selection**

## Host-Side Script Timeouts

**Note:** For details on host-side scripting, see **Connecting Hosts to Actifio Appliances** in your Actifio Documentation Library and available on the Actifio Now customer portal.

The Actifio Connector allows you to create host-side scripts that run on an application's host before and/or after a policy is run. The four timeouts provided in a policy template map directly into the four stages of a host-side script:

**Init:** Defines how long a policy should wait before assuming host-side scripts on a protected host have been initialized.

**Freeze:** Defines how long a policy should wait before assuming the application is frozen and ready for protection.

**Unfreeze:** Defines how long a policy should wait before assuming the application is unfrozen.

**Finish:** Defines how long a policy should wait before protection is complete.



**Script Timeouts Selections**

## Appliance Specific Policy Templates

The SLA Architect comes with predefined policy templates specific to the Actifio appliance on which they reside. The rules governing the modification of predefined templates and policies and the creation of new templates and policies are also specific to each Actifio appliance type.

The following sections describe the predefined templates that come with each Actifio appliance type and the rules governing modification and creation of templates and policies.

Predefined templates can be used as is or you can modify their policies to meet application requirements. You can also create new templates and policies.

### Actifio CDS Appliance Templates

Actifio CDS appliances come with two predefined templates:

**Enterprise template** contains policies that capture data, deduplicate the data and then retain the data at the local site: The Enterprise template employs two policies:

- o Production to Snapshot - Retains three daily snapshots.
- o Snapshot to Dedup Backup - Retains daily, weekly and monthly deduplicated snapshots.

**Standard template** contains a single policy that captures production VMware data and sends it directly to deduplication without keeping a local snapshot copy. The Direct to Deduplication template employs one policy: Direct to Dedup - Retains daily, weekly, and monthly deduplicated snapshots of VMware VMs.

### Actifio Sky Appliance Templates

Actifio Sky appliances come with five predefined policy templates:

**Tier-0, Tier-1, Tier-2** templates provide either a 4, 12, or 24 hour RPO respectively. These templates contain the following policies to capture, deduplicate, and then retain data at the local site or at a remote site:

- o Production to Snapshot
- o Snapshot to Dedup Backup
- o Production to Mirror
- o Dedup Backup to Dedup DR

The frequency at which data is captured and replicated determines whether it is a Tier-0, Tier-1, or Tier-2.

**Tier-3** template provides an RPO of greater than twenty four hours. The Tier-3 template uses the following policies to capture, deduplicate, and then retain data at the local site, or at a remote site:

- o Production to Snapshot
- o Snapshot to Dedup Backup
- o Dedup Backup to Dedup DR

**Tier-4** template allows you to capture and deduplicate data locally; it does not replicate data. The Tier-4 template uses the following policies:

- o Production to Snapshot
- o Snapshot to Dedup Backup

## Resource Profiles

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

- Locally
- On another Actifio appliance
- In an Actifio OnVault storage pool

---

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

---

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

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

For details on creating a resource profile see [Chapter 6, Creating and Managing Resource Profiles](#).





## 2 Best Practices for Policy Templates

---

When your Actifio appliance was installed, your Actifio representative configured policy templates according to your Actifio Managed Data License (MDL), Recovery Point Objectives (RPOs), and Recovery Time Objectives (RTOs).

Over time you may find it necessary to make changes to the existing policy templates or create new policy templates of your own. Making changes to existing policy templates and adding new policy templates could impact the consumption of system resources as well as the performance of your Actifio appliance.

---

**Note:** The Actifio appliance can check the validity of a policy within a policy template as well as the impact a new policy or changes to an existing policy will have. For details see [Policy and System Resource Considerations](#) on page 37.

---

Following the best practices in this chapter will help you avoid some of the more common mistakes users make when creating and modifying policy templates.

This chapter contains best practice information on:

- [Initial Data Capture](#) on page 10
- [Resizing Volumes](#) on page 10
- [System Resources](#) on page 10
- [Concurrency](#) on page 11
- [Policy Schedules](#) on page 11
- [Calculating Frequency](#) on page 13
- [Job Priority and Scheduling](#) on page 14
- [Job Retries](#) on page 14
- [Policy Compliance Settings](#) on page 15
- [Policy Specific Best Practices](#) on page 18
- [Application Specific Best Practices](#) on page 35

---

**Note:** The term *application* is used in this document as a convenience. Unless otherwise specified, it applies to: databases, consistency groups, filesystems, VMs, and NAS datasets.

---

## Initial Data Capture

The first time a policy in a policy template captures an application's data it captures the data in its entirety. Subsequent data captures will be incremental data captures.

When adding new applications to an Actifio appliance, stagger the initial data captures so as not to overwhelm your application servers, network, or Actifio appliance.

For example, to protect multiple applications with one policy template, apply the policy template to just a few of the applications. Once the initial full data capture is complete, apply the policy template to more applications. Repeat the process until the policy template has been applied to all applications.

## Resizing Volumes

If you resize a volume that contains protected data, the next time the Snapshot policy or Direct to Dedup policy for that volume runs, it will perform a full capture operation; regardless of how many times that volume's data has been captured.

If you must resize a volume, consider the impact capturing all of the data will have on the applications server(s), network, and the Actifio appliance.

---

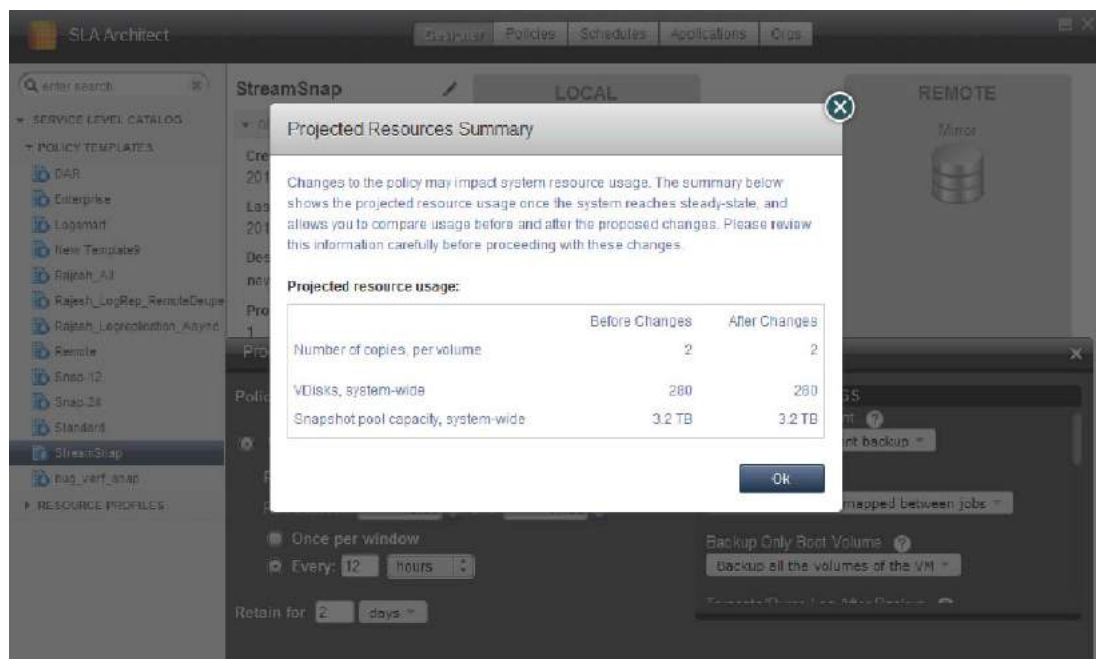
**Note:** Resizing an Oracle database larger than 1 TB on Linux and UNIX systems will create an additional staging disk but will not trigger a full capture.

---

## System Resources

Each Actifio appliance has a finite amount of system resources. The amount of resources used is driven by the configuration of the Actifio appliance's policy templates and the type and size of the applications captured. If you create a policy that consumes too many resources, the Actifio appliance will generate an SLA Violation warning. [Chapter 3, Policy and System Resource Considerations](#) has a detailed description of these warnings.

When modifying a policy, click **Project Changes** to display a summary of how your modifications will impact system resources. Use the before-and-after information displayed in the Projected Resources Summary dialog box to ensure your modifications will have the expected impact on system resources.



**Policy Impact on System Resources**

## Concurrency

An Actifio appliance, by default, can run six snapshot jobs at a time. If you have more than the allowed number of jobs scheduled for the same time period, the policy scheduler will start as many jobs as allowed and queue the other jobs.

Because each user's network, data, and storage environments differ, experiment with concurrency until the optimal number of concurrent jobs is reached.

## Policy Schedules

An Actifio appliance supports two methods of specifying a policy schedule when configuring a policy:

- **Windowed** - Defines a discrete image capture schedule adhering to a specific frequency and time window. A windowed schedule ignores the start or queued time of any previous job. You can instruct an Actifio appliance to run multiple capture jobs at a specified frequency interval or to run once during a specified time window.  
Example: perform a capture every 30 minutes, daily from 9:00 AM to 5:00 PM.
- **Continuous** - Defines a continuous image capture schedule. A continuous schedule uses the start or queued time of previous jobs to determine when the next job will run. In this type of policy schedule, jobs run continuously (24/7) at the specified time interval.  
Example: perform a capture job every 8 hours, starting the first job at 1:00 AM.

The following table compares two policies that take a snapshot every five hours. One policy is set to windowed and the other to continuous.

**Window vs Continuous Policy Schedule**

Policy's Job is Run	Window Start Time	Continuous Start Time
First time	Sunday 00:00	Sunday 00:00
Second time	Sunday 05:00	Sunday 05:00
Third time	Sunday 10:00	Sunday 10:00
Fourth time	Sunday 15:00	Sunday 15:00
Fifth time	Sunday 20:00	Sunday 20:00
Sixth time	Monday 00:00 (New window starts)	Monday 01:00 (5 hours after 20:00 Sunday)
Seventh time	Monday 05:00	Monday 06:00

A downstream policy such as Dedup Backup, Dedup DR, OnVault, or StreamSnap performs an action on data processed by another policy. If there is no new data for a downstream job to process, it will not run. Downstream policies can retry continually until they have source data to process. Provided the source data is eventually provided in time to meet the downstream policy's SLA compliance settings, the downstream data will remain in compliance.

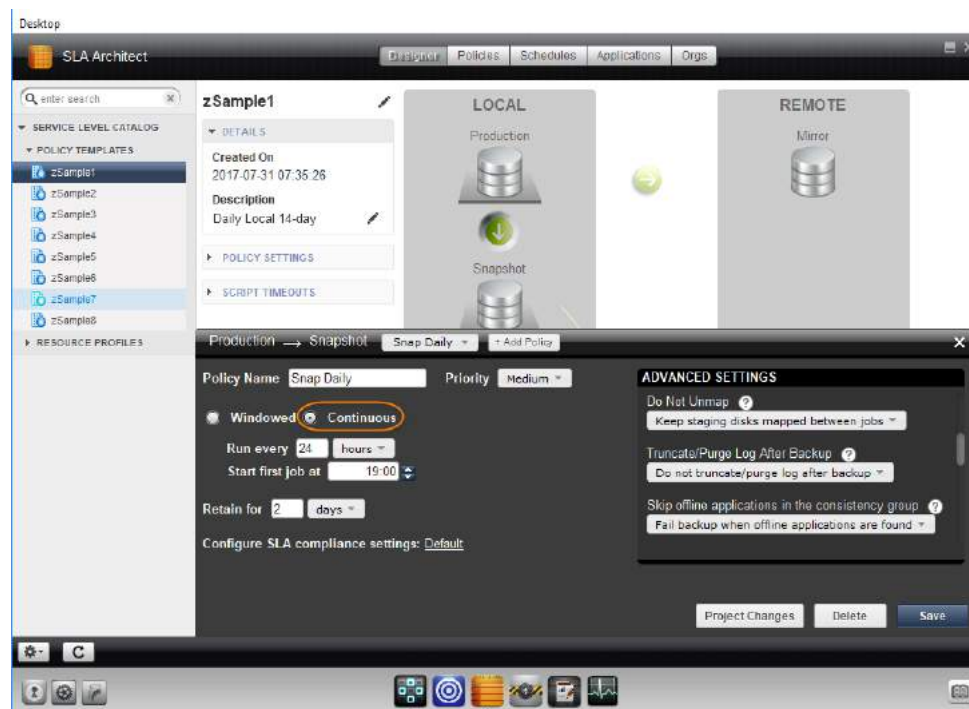
In addition:

- Production to Mirror policies that use Dedup Async replication are always set to continuous and cannot be set to windowed.
- Production to Mirror policies that use StreamSnap replication will use the continuous or windowed setting of the policy that captures its source images.
- Snapshot to OnVault policies are always set as windowed and can not be set to continuous.

For a set of best practices on configuring windowed and continuous policy schedules for the various policy types, see [Policy Specific Best Practices](#) on page 18.



**Windowed Policy Schedule**



**Continuous Policy Schedule**

## Calculating Frequency

The period is the time between scheduled runs and frequency is the number of jobs run per unit time. For example, if a schedule calls for jobs to run every 4 hours, the period is 4 hours and the expected frequency is 6 times per day. If a job takes one hour to complete and the policy has a 12 hour frequency, then the policy's job will run again 11 hours after the previous job completes.

Be sure to select a frequency that achieves your required Recovery Point Objectives (RPOs) and allows sufficient time for a job to finish.

- Minimum recommended frequency for a Snapshot policy is 1 hour (local RPO).
- Minimum recommended frequency for a Dedup Async policy is 4 hours (remote RPO).
- A StreamSnap policy can point to any Snapshot policy with frequency of 1 hour or longer (remote RPO).
- Minimum recommended frequency for a Dedup Backup to Dedup DR policy is 4 hours, with a recommended best practice of 24 hours (remote RPO)

## Job Priority and Scheduling

All activities run as jobs. Jobs are executed according to the schedules configured when the policies were created.

Some jobs take much longer than others. Expiration jobs are fast. Snapshot jobs depend upon variables like the size of the application or VM and how much data has changed since its last snapshot; the initial snapshot of any application or VM is all-new data, so those can take a long time. Deduplication jobs take a varying amount of time depending on how full the Dedup Pool is and if Garbage Collection is running.

The policy scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority.

---

**Note:** For detailed information on jobs, job types, and managing jobs, see **Virtualizing and Protecting Copy Data with the Application Manager** in the Actifio Documentation Library and on the Actifio Now customer portal.

---

## Job Retries

If a job fails, the scheduler will automatically retry running the job. The first time the job fails the scheduler will wait 4 minutes before making it available for retry. After 3 failed job attempts the job is marked as Failed and is no longer retried. The next job will be attempted according to the policy's schedule.

The scheduler will treat a job retry like any other available job. If there are more jobs available than slots to accommodate them, then jobs are queued. This may result in a retry failing to start within the window and the job being marked as failed.

Job retries are reported in the System Monitor. To identify job retries, the System Monitor appends a, b, or c to a job's name. For example:

Job Name	Type	Priority	Status	Host	Application	Policy	Template	Consistency D	Start Time	End Time
Job_3828633a	dedupasync	medium	retry	vc1-r4_esxi5.1	vc1-r4_esxi5.1	12hr-DAR	Enterprise-DAR	Dec 16 10:40	Dec 16 10:40	Dec 16 11:07
Job_3828633b	dedupasync	medium	retry	vc1-r4_esxi5.1	vc1-r4_esxi5.1	12hr-DAR	Enterprise-DAR	Dec 16 11:07	Dec 16 11:07	Dec 16 11:31
Job_3828633c	dedupasync	medium	failed	vc1-r4_esxi5.1	vc1-r4_esxi5.1	12hr-DAR	Enterprise-DAR	Dec 16 12:11	Dec 16 12:11	Dec 16 12:34
Job_3828979	remote-dedup	medium	failed	vm004-59	vm004-59	DR-Daily	Enterprise	Dec 01 17:49	Dec 16 10:31	Dec 16 10:47
Job_3829296	remote-dedup	medium	failed	vm004-59	vm004-59	DR-Daily	Enterprise	Dec 01 17:49	Dec 16 10:47	Dec 16 11:03
Job_3829430	snapshot (DB)	medium	failed	SERSQLAG	db1	Snapshot	LogSmart-SQL	Dec 16 10:54	Dec 16 10:54	Dec 16 10:55
Job_3829530	snapshot	medium	retry	w2k12r2	w2k12r2	S-4hrs	Enterprise	Dec 16 10:59	Dec 16 10:59	Dec 16 11:03
Job_3829530a	snapshot	medium	retry	w2k12r2	w2k12r2	S-4hrs	Enterprise	Dec 16 11:04	Dec 16 11:04	Dec 16 11:06
Job_3829530b	snapshot	medium	retry	w2k12r2	w2k12r2	S-4hrs	Enterprise	Dec 16 11:20	Dec 16 11:20	Dec 16 11:23
Job_3829530c	snapshot	medium	succeeded	w2k12r2	w2k12r2	S-4hrs	Enterprise	Dec 16 12:27	Dec 16 12:24	Dec 16 12:27
Job_3829567	snapshot	medium	retry	vm004-59	vm004-59	S-4hrs	Enterprise	Dec 16 11:01	Dec 16 11:01	Dec 16 11:02
Job_3829567a	snapshot	medium	retry	vm004-59	vm004-59	S-4hrs	Enterprise	Dec 16 11:05	Dec 16 11:05	Dec 16 11:06
Job_3829567b	snapshot	medium	retry	vm004-59	vm004-59	S-4hrs	Enterprise	Dec 16 11:21	Dec 16 11:21	Dec 16 11:22
Job_3829567c	snapshot	medium	succeeded	vm004-59	vm004-59	S-4hrs	Enterprise	Dec 16 12:27	Dec 16 12:25	Dec 16 12:27
Job_38295620	remote-dedup	medium	failed	vm004-59	vm004-59	DR-Daily	Enterprise	Dec 01 17:49	Dec 16 11:03	Dec 16 11:19
Job_3829757	snapshot (DB)	medium	failed	SERSQLAG	db1	Snapshot	LogSmart-SQL	Dec 16 11:09	Dec 16 11:09	Dec 16 11:10
Job_3829945	expiration		succeeded	mpnode0	mprotectlog1	S-2hrs	Db2Log	Dec 16 11:14	Dec 16 11:14	Dec 16 11:14
Job_3829944	snapshot	medium	succeeded	mpnode0	mprotectlog1	S-2hrs	Db2Log	Dec 16 11:16	Dec 16 11:16	Dec 16 11:17
Job_3829964	remote-dedup	medium	failed	vm004-59	vm004-59	DR-Daily	Enterprise	Dec 01 17:49	Dec 16 11:19	Dec 16 11:35

**Job Retries Listed in System Monitor**

## Policy Compliance Settings

Actifio policies define schedules for when and how often an Actifio job will run, and how long to retain data. A Policy also allows you define whether its schedule will run within a window or continuously.

Where applicable, SLA Template Policies allow you to define the rules for determining whether or not a data protected by a policy meets your requirements. If data is being protected according to your needs, then it is considered to be in compliance.

### Definitions

To understand how an Actifio appliance calculates and reports on SLA Compliance, you must first understand the following terms:

- **Windowed** - A policy setting that defines a period of time in which jobs are allowed to start.
- **Continuous** - A policy setting that defines when its first job can start but as the name implies, allows subsequent jobs to run at a frequency without regard to any time boundary.
- **Compliance threshold** - Used to fine tune the acceptable time frame for successfully captured data.
- **Consistency time** - The point in time that data is recoverable. Consistency time is established when an application has been captured. If the snapped image is protected successfully, then the consistency time for that image is used in determining compliance. If the image is not protected successfully, then the consistency time for the last successfully protected image is used.

---

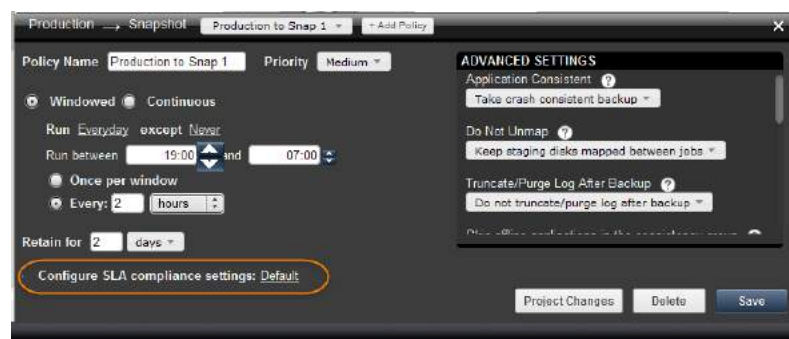
**Note:** The first time a continuous policy runs, an Actifio appliance does not have a consistency time to use to determine compliance. In that case, the policy's **Start first job at:** setting is used in lieu of consistency time.

---

The Actifio appliance automatically calculates and sets default SLA Compliance settings. Default settings are based on whether the policy is set to windowed or continuous, the policy type, and Actifio-recommended best practices. The default settings calculated will meet the needs of most users.

SLA Compliance settings can be set manually to meet specific requirements. In addition, a threshold can be set to alert you if your data is approaching a point where it will be out of compliance.

To view or modify SLA Compliance settings, click **Configure SLA policy compliance settings** at the bottom of a policy's page. The default link name is Default, however, the link name is dynamic and changes according to the SLA Compliance settings used.



### SLA Compliance Settings Link

If data exceeds the SLA Compliance settings, a violation is raised and it remains in effect until you have successfully captured data with a consistency time that falls within the specified threshold. Because compliance is time based, a job can fail and restart multiple times but the data will remain in compliance as long as the job eventually captures data with a consistency time that falls within the boundary of a specified threshold.

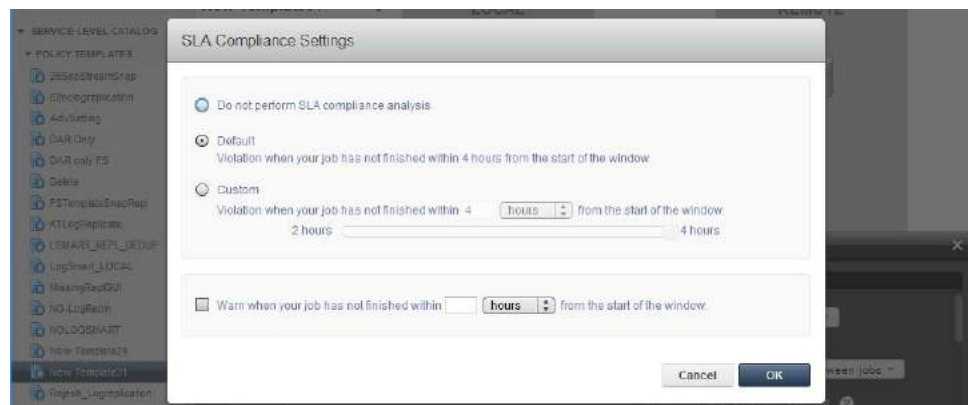


## Windowed Policy Compliance Settings

Policies set to **Windowed** provide a link to SLA Compliance Settings that have settings for:

- Turning off SLA compliance analysis
- Using the default SLA compliance settings
- Defining a custom compliance setting. When defining a custom setting for a windowed policy, consider the time at which the data will be snapped (consistency time), how long the window will be open, and the amount of time required to capture the data.
- Setting a warning that will send you a notification if a job is still running after a specified period of time. Set this to less than the wait time for raising a violation and you can address issues before a job is in violation.

To determine whether the data captured is in compliance, an Actifio appliance uses the start of the window, the consistency time of the captured image, and the violation threshold specified in the SLA compliance settings dialog box. If successfully captured data has a consistency time that falls within the window's defined threshold, the data is in compliance.



**SLA Compliance Settings for a Windowed Policy**

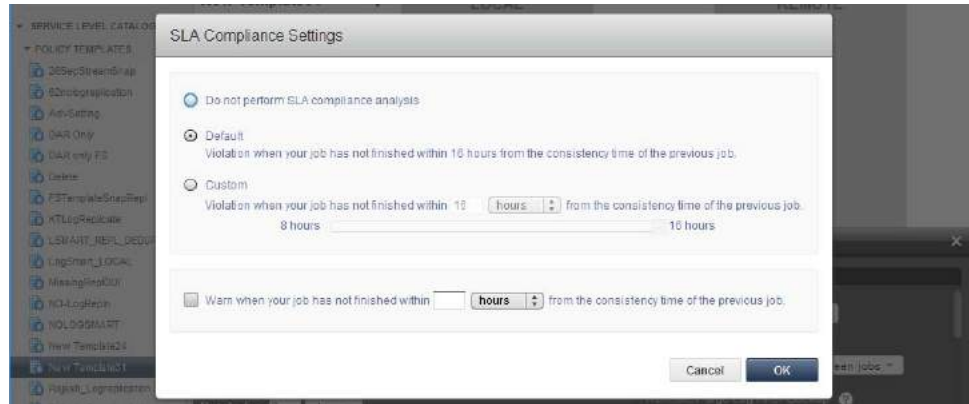
## Continuous Policy Compliance Settings

Policies set to **Continuous** provide a link to SLA Compliance Settings that have settings for:

- Turning off SLA compliance analysis.
- Using the default SLA compliance settings
- Defining a custom SLA compliance setting. When defining a custom setting you must consider the time at which the data will be snapped (consistency time) and the amount of time required to physically capture the data.
- Setting a warning that will send you a notification if a job is still running after a specified period of time. Set this to less than the wait time for raising a violation and you can address issues before a job is in violation.

To determine whether captured data is in compliance, Actifio uses the consistency time of the last captured image and the violation threshold specified in the SLA compliance settings dialog box. If the consistency time for the most recently captured image does not fall outside of the violation threshold, then the captured data is in compliance.





### SLA Compliance Settings for a Continuous Policy

## Policy Specific Best Practices

You define policy schedules that meet your data capture window requirements, RPOs, and RTOs. For example if a daily capture must be performed some time between 7:00PM and 7:00AM, then you would specify a policy with a windowed schedule that has a capture window of 19:00 to 7:00. Giving the policy the widest window possible will give the maximum flexibility for the Actifio scheduler to schedule all needed jobs.

The time window specified will define the allowed start time for the data capture job. Jobs started at the end of the window will be allowed to run through completion.



**Caution:** The Control Panel tab in the Appliance Settings section of the Domain Manager allows you to enable and disable ALL schedules. Disabling all schedules will result in a generating numerous SLA violation notifications.

However, note that if the **ignore.schedule.off.violation** system-level parameter is set to 1, this specifies that the Actifio appliance is to ignore SLA violations when the scheduler is off. See the **Actifio CLI Reference** in the Actifio Documentation Library.

---

---

**Note:** Windows that use Daylight Savings Time (DST) may end up being one hour shorter or longer on the day of the DST transition.

---

The following sections detail the best practices for the different policy template policies.

- [Production to Snapshot Policies](#) on page 19
- [Snapshot to Dedup Backup Policies](#) on page 23
- [Production to Direct to Dedup Policies](#) on page 24
- [Dedup Backup to Dedup DR Policy Policies](#) on page 25
- [Dedup DR to Remote Replication Policies \(Multi-hop Replication\)](#) on page 26
- [Snapshot to OnVault Policies](#) on page 28
- [Production to Mirror Policies](#) on page 29
- [Scheduling Policy Best Practices at a Glance](#) on page 33

## Production to Snapshot Policies

Recent data is accessed the most frequently. Because of this, you only need to retain two or three snapshots of data. Older, less frequently accessed data can be rehydrated and accessed from the dedup pool. You can choose to schedule a Snapshot policy schedule that occurs during a specific frequency and time window or on a continuous basis. The minimum recommended frequency for a Snapshot policy is 1 hour (local RPO).

---

**Note:** Snapshot to Dedup and Dedup to Dedup DR policies associated with a Production to Snapshot policy should be configured with the same window start time as the Production to Snapshot policy.

---

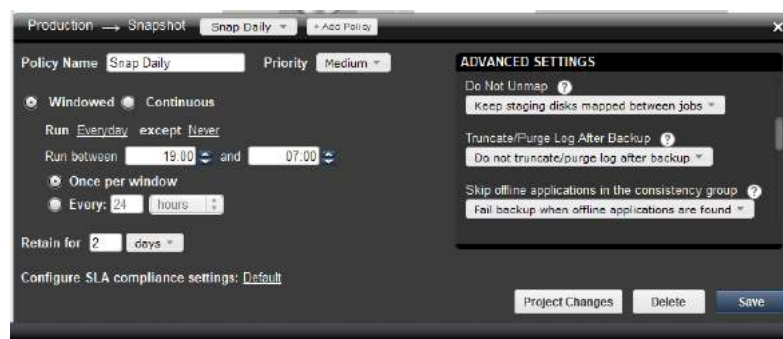
### Windowed Schedule -- One Snapshot per Window

Most Production to Snapshot policies are designed to take a single snapshot of data in a 24 hour window. Single snapshots can be scheduled to take place within a window that may or may not respect day boundaries (for example, 7 pm to 7 am).

For example, to create a Snapshot policy schedule that crosses a day boundary and takes a single snapshot during a specific time window, set:

- Schedule type of **Windowed** (default)
- Snap on these days: **Everyday except Never**
- The window to open and close as needed, typically set from 19:00 to 07:00
- The frequency to **Once Per Window**
- The desired retention time (for example, retain for **2 days**)

With this windowed schedule, the day boundary (midnight) is ignored.

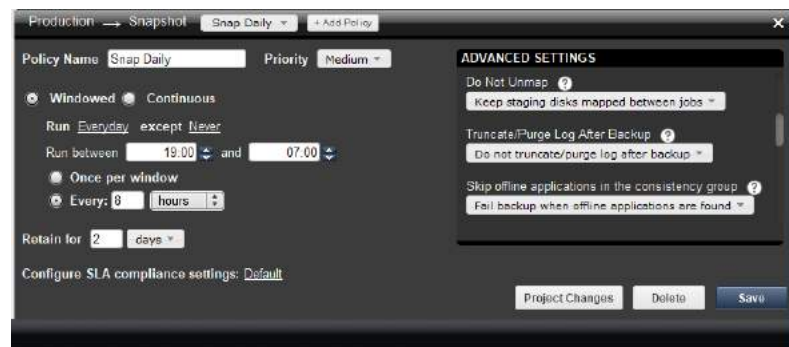


## Windowed Schedule -- Multiple Snapshots in a Window

In some cases you may want to capture multiple snapshots within a time window. This approach requires careful planning since it may result in the consumption of system resources and could lead to a situation where snapshots are constantly being taken.

For example, to create a Snapshot policy schedule that takes multiple snapshots during a specific time window, set:

- Schedule type of **Windowed** (default)
- Snap on these days: **Everyday except Never**
- The window to open as needed, and may or may not span the day boundary.
- The frequency so as not to overlap the time required to take a snapshot. The minimum recommended frequency for a Snapshot policy is to run every **1 hour (local RPO)**.
- The desired retention time (for example, retain for **2 days**)



With this approach, the job will run according to its frequency within the specified window. Any job already running at the close of the window will continue to run until it completes.

## Continuous Schedule -- Run Daily at Regular Intervals

You can configure a Snapshot policy schedule that continuously runs on a daily basis (24/7) at a time interval of every x minutes or hours. For example, you can create a Snapshot policy where jobs run daily every 4 hours, with the first job starting at 1:00 am.

To create a Snapshot policy that is scheduled to run continuously at a regularly set interval, set:

- Schedule type of **Continuous**
- The frequency so as not to overlap the time required to take a snapshot. The minimum recommended frequency for a Snapshot policy is to run every **1 hour (local RPO)**.
- Time to initiate the first snapshot job.
- The desired retention time (for example, retain for **2 days**)

The screenshot shows the 'Snap Daily' configuration window. The 'Policy Name' is 'Snap Daily' and the 'Priority' is 'Medium'. The 'Schedule' is set to 'Continuous'. The 'Run every' interval is '8 hours'. The 'Start first job at' time is '19:00'. The 'Retain for' duration is '2 days'. The 'Configure SLA compliance settings' is set to 'Default'. The 'ADVANCED SETTINGS' section includes options for 'Do Not Unmap' (Keep staging disks mapped between jobs), 'Truncate/Purge Log After Backup' (Do not truncate/purge log after backup), and 'Skip offline applications in the consistency group' (Fail backup when offline applications are found). Buttons for 'Project Changes', 'Delete', and 'Save' are at the bottom.

You also have the option of scheduling a continuous job to run once per day (the longest continuous policy schedule period without defining a windowed policy schedule). In this case you would specify to **Run Every 24 hours**, which equals a continuous daily schedule.

The screenshot shows the 'Snap Daily' configuration window with the 'Run every' interval set to '24 hours'. All other settings, including 'Policy Name', 'Priority', 'Schedule', 'Start first job at', 'Retain for', 'Configure SLA compliance settings', and 'ADVANCED SETTINGS', are identical to the previous screenshot.

## Database Log File Snapshot Policies

When creating a Snapshot policy for a database you have the option of also capturing its log files at a specified frequency. The frequency at which database logs are captured is defined separately from that of the database. For example, a database can be captured every day and its logs captured every hour.

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

Frequency and retention are defined in the advanced settings of the database's Snapshot policy. The capture of logs is done without regard to day boundaries, window, or frequency at which its associated database is captured.



The physical space required to accommodate a database's logs is automatically managed by the Actifio appliance. At a minimum, the Actifio appliance will evaluate typical log sizes and their retention period and add space as needed.

To more efficiently and effectively manage the storage requirements for a database's logs, Snapshot policies provide the following advanced settings:

- **Log Backup Retention Period** - Log retention is defined separately from the retention of the Snapshot policy. Having a separate retention period allows you to use logs in conjunction with copies of the database stored in both the Snapshot and Dedup pools. The log retention period is a mandatory setting.
- **Log Staging Disk Size Growth** - Defines the percent at which to automatically grow the staging VDisk on which the logs reside. This setting is from 5 to 100 percent.
- **Estimated Change Rate** - Defines the daily change (in percent), which allows the Actifio appliance to better calculate the size of the staging disk needed to hold logs. This setting is from 0 to 100.
- **Compress Database Log Backup** - Instructs the source database to compress its logs before capture by the Actifio appliance. The database server performs log compression during log backup.

If required, you can replicate Oracle or Microsoft® SQL Server database logs to a remote Actifio appliance. You can use the logs at the remote site for any database image within the retention range of the replicated logs. Log replication uses StreamSnap technology to perform the replication between the local and remote Actifio appliances; log replication goes directly from the local snapshot pool to the snapshot pool on the remote appliance. For a log replication job to run, there must be a replication policy (StreamSnap, Dedup-Async, or Remote Dedup) included in the template, and at least one successful replication of the database must first be completed.

## Snapshot to Dedup Backup Policies

A Snapshot to Dedup policy schedule must be coordinated with its associated Production to Snapshot policy schedule. A dedup policy will not run if there is not a snapshot to deduplicate. For example, a policy template with a Snapshot policy that runs once a week and a dedup policy that runs three times a day would have twenty deduplication jobs per week with nothing to deduplicate.

The best practice for a Snapshot to Dedup Backup policy recommends deduplicating one snapshot per day. If you are taking multiple snapshots per day, when the Snapshot to Dedup Backup policy runs it will deduplicate the most recently completed snapshot. The other snapshots will expire before they are deduplicated.

In addition, if you set the window for a dedup policy too narrow, a snapshot could complete outside of the dedup policy's window. In most cases it is advisable to set a dedup policy's window from 19:00 to 18:59. This ensures that the dedup policy will run, even for those rare occasions when the snapshot finishes later than usual.

---

**Note:** *Snapshot to Dedup and Dedup to Dedup DR policies associated with a Production to Snapshot policy should be configured with the same window start time as the Production to Snapshot policy.*

---

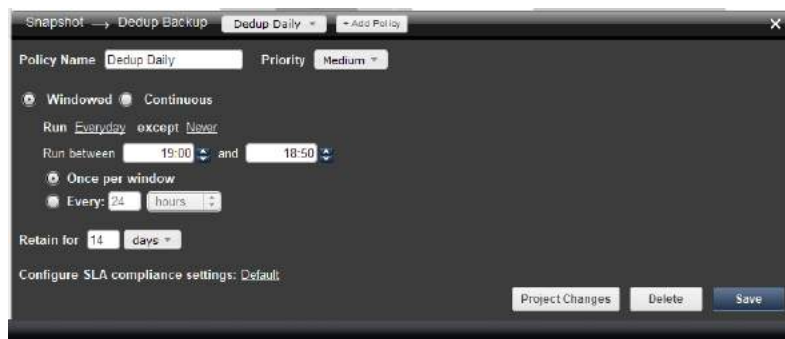
For example, to create a Production to Dedup Backup policy schedule that runs as soon as there is something to deduplicate, set:

- Schedule type of **Windowed** (default)
- Dedup on these days: **Everyday except Never**
- The window to open and close as needed. Typically set to 19:00 to 18:59
- The frequency to **Once Per Window**
- The desired retention time (for example, retain for **14 days**)

---

**Note:** *With this configuration, when multiple Production to Snapshot images are available, only the most recently completed snapshot will be deduplicated.*

---



This ensures that regardless of what time a Production to Snapshot job finishes, the Snapshot to Deduplication job will start in the next available scheduler slot.



**Caution:** *Snapshot to Dedup Backup policies allow you to set the policy type to Image Verification. This setting has a dramatic impact on system performance and should only be used when recommended by your Actifio representative.*

---

## Production to Direct to Dedup Policies

Production to Direct to Dedup policies can only be applied to VMware VMs. Direct to dedup takes advantage of VMware's change block tracking capabilities and writes deduplicated captured data directly to the Actifio dedup pool. Data protected with Direct to Dedup policies do not consume Actifio VDisks.

For example to create a Direct to Dedup policy schedule that will capture a single image in a day, set:

- Schedule type of **Windowed** (default)
- Dedup on these days: **Everyday except Never**
- The window to open and close as needed. Typically set to 19:00 to 07:00
- The frequency to **Once per Window**
- The desired retention time (for example, retain for **14 days**)

The screenshot shows the 'Direct to Dedup' policy configuration window. The 'Policy Name' is 'Direct to Dedup 1' and the 'Priority' is 'Medium'. The 'Windowed' radio button is selected, and the 'Run' schedule is set to 'Everyday except Never'. The 'Run between' time is set to '19:00' and '07:00'. The 'Once per window' radio button is selected, and the 'Every' frequency is set to '8 hours'. The 'Retain for' time is set to '14 days'. The 'ADVANCED SETTINGS' section on the right includes 'Application Consistent' (set to 'Take crash consistent backup'), 'Enable Catalog' (set to 'Disable catalog'), and 'Catalog Username' (empty). The 'Configure SLA compliance settings' is set to 'Default'. The 'Project Changes', 'Cancel', and 'Save' buttons are at the bottom right.



## Dedup Backup to Dedup DR Policy Policies

---

**Note:** Details about the Dedup Backup method supported by Actifio appliances, along step-by-step instructions on performing failover and restoring from a failover condition, can be found in **Replicating Data Using Actifio Appliances** in your Actifio Documentation Library and on the Actifio Now customer portal.

---

Dedup Backup uses a Dedup Backup to Dedup DR policy. 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 minimum recommended frequency for a Dedup Backup to Dedup DR policy is 4 hours, with a recommended best practice of 24 hours (remote RPO).

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.

To create a Dedup Backup to Dedup DR policy schedule that will replicate a single deduplicated image in a day, and will run as soon as there is something to replicate, set:

- Schedule type of **Windowed** (default)
- Replicate on these days: **Everyday except Never**
- The window to open and close as needed. Typically set to 19:00 to 18:50
- The frequency to **Once per Window**
- The desired retention time (for example, retain for **14 days**)



This ensures that regardless of what time the Snapshot to Dedup Backup policy finishes, the Dedup Backup to Dedup to DR policy will start in the next available scheduler slot.

## Dedup DR to Remote Replication Policies (Multi-hop Replication)

If your long-term Dedup Backup remote storage protection needs require your data to be stored in two remote locations, you can specify the Dedup DR to Remote Replication policy to define the second leg 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 DR purposes (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.

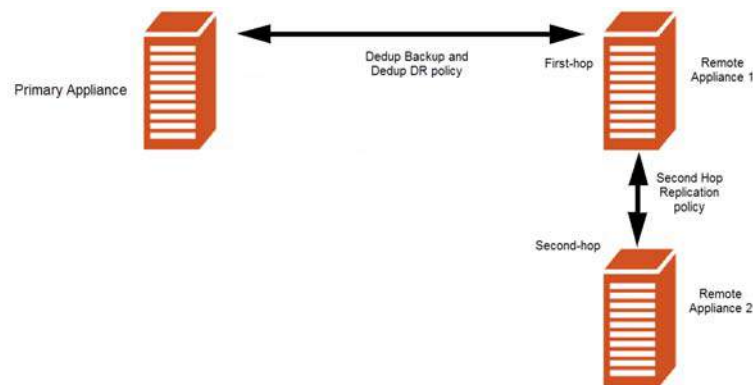
To perform multi-hop replication, configure the policy templates for the primary Actifio appliance and the two remote Actifio appliances (1 and 2) as follows:

- 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.
- For remote Actifio appliance 1, create a Dedup DR to Remote 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. See [Creating a Multi-hop Remote Dedup Backup Replication Policy](#) on page 71.
- 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.

---

**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.

---



### Defining Template Policies for a Multi-hop Configuration

To create a Dedup DR to Remote Replication policy schedule that will replicate a single deduplicated image in a day, and will run as soon as there is something to replicate, set:

- Schedule type of **Windowed** (default)
- Replicate on these days: **Everyday except Never**
- The window to open and close as needed. Typically set to 19:00 to 18:59
- The frequency to **Once Per Window**
- The desired retention time (for example, retain for **24 days**)

---

**Note:** The Dedup DR to Remote Replication policy can use a set of policy settings that are different from the first hop replication policy (the Dedup Backup and Dedup DR policy).

---



## Snapshot to OnVault Policies

The Snapshot to OnVault policy allows you to send snapshot data to storage defined by an Actifio OnVault Pool. A schedule within the policy is used to send the most recent snapshot taken by the policy template's Production to Snapshot policy to the storage defined by the Actifio OnVault Pool. After the initial ingest of data, an OnVault capture operation follows Actifio's incremental forever data capture process.

Actifio OnVault Pool storage is typically used for long-term retention.

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

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

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

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

To create a Snapshot to OnVault policy schedule that will, once a month send the most recent Production to Snapshot data to storage defined by an Actifio OnVault Pool, set:

- Vault on these days: **Every month on the 1st**
- The window to open and close as needed. Typically set to 19:00 to 18:50
- The frequency to **Every 24 Hours**
- The desired retention time (for example, retain for **3 years**)

The screenshot shows a configuration window titled "Snapshot -> OnVault" with a sub-header "Snapshot to OnVault 1" and an "Add Policy" button. The window contains the following settings:

- Policy Name:** Snapshot to OnVault 1
- Priority:** Medium
- Windowed/Continuous:** Windowed (selected)
- Run:** Everyday except Never
- Run between:** 19:00 and 18:59
- Frequency:** Once per window (selected), Every: 24 hours
- Retain for:** 14 days

At the bottom right, there are "Cancel" and "Save" buttons.

## Production to Mirror Policies

---

**Note:** Details about the different Production to Mirror methods supported by the Actifio appliances along with step-by-step instructions on their use can be found in **Replicating Data Using Actifio Appliances** in your Actifio Documentation Library and on the ActifioNOW customer portal.

---

A Production to Mirror policy defines how data will be replicated to a Mirror Pool (a Snapshot Pool on a remote Actifio appliance). Data in the Mirror Pool is meant for instant recovery in a disaster recovery scenario. When creating a Production to Mirror policy you can choose from the following types of replication:

- **Dedup-Async Replication (DAR)** - 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. This replication method uses dedup processing for bandwidth efficient replication. See [Creating a Dedup-Async Replication \(DAR\) Production to Mirror Policy](#) on page 75 for details.
- **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. This replication method uses a point-in-time snapshot of the original application without performing deduplication. See [Creating a StreamSnap Production to Mirror Replication Policy](#) on page 79 for details.
- **Synchronous (Sync) and Asynchronous (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. See [Creating a Synchronous or Asynchronous Production to Mirror Replication Policy](#) on page 80 for details.

Best practices for Production to Mirror policies depend on which replication option you plan to use. This section outlines the policy best practices for the Dedup Async, StreamSnap, Synchronous, and Asynchronous replication methods offered by the Actifio appliance.

### Production to Mirror: Dedup-Async Replication (DAR) Policies

Production to Mirror policies that use Dedup Async replication (DAR) take snapshots of their own. They do not use snapshots created by other policies.

Once the Production to Mirror policy 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. 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, Dedup Async replication is optimized to require less network bandwidth than the other replication options (such as StreamSnap replication), but it does require additional Actifio system resources to deduplicate data.

Dedup-Async replication:

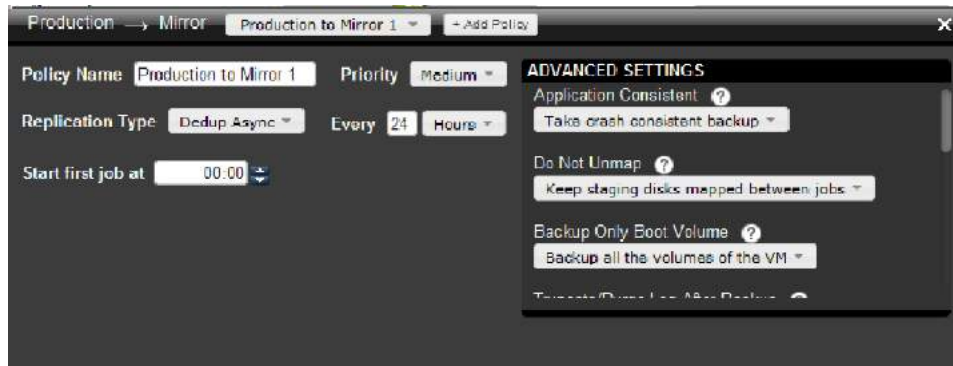
- Achieves Recovery Point Objectives (RPOs) of 24 hours with 12 and 8 hour RPOs possible. The minimum recommended frequency for a Dedup Async policy is 4 hours (remote RPO).
- Replicates data that is can be efficiently deduplicated.
- Uses an existing IP network to replicate data.
- Minimizes bandwidth requirements for replication.
- Replicates repeatedly at intervals determined by the Dedup-Async Production to Mirror 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.

Dedup Async replication allows you to define a frequency (Every) for the Production to Mirror policy. Actifio's best practice is to set a frequency of (Every) 24 hours.

---

**Note:** A Production to Mirror policy job will be queued as soon as it is saved. Before saving a Production to Mirror policy consider its impact on other data operations; especially for the initial ingest of data.

---



### Production to Mirror: StreamSnap Replication Policies

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

---

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

---

StreamSnap replicates data snapshots to a remote Actifio appliance 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.

---

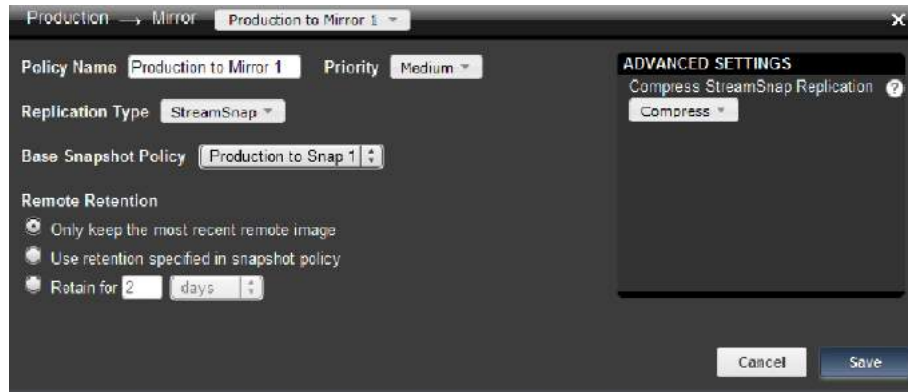
**Note:** StreamSnap replication and local snapshots are integrated to avoid the creation of double snapshots. The Actifio appliance allows you to maintain multiple local snapshots and store local images in the Dedup pool for long-term retention.

---

StreamSnap replication:

- Achieves Recovery Point Objectives (RPOs) as short as one hour. The StreamSnap replication policy relies on the associated Production to Snapshot policy for RPO and the other advanced snapshot settings. A StreamSnap policy can point to any Snapshot policy with frequency of 1 hour or longer (remote RPO).
- Uses an existing IP network to replicate data.
- Replicates data that is not conducive to deduplication (for example, data that is compressed or encrypted). Such data includes: images, videos, and encrypted databases.
- Replicates large amounts of data to remote users (for example, test and development environments).
- Retains multiple point-in-time snapshot images at the remote site, with retention behavior being driven by the settings in the StreamSnap policy.
- 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. You can disable compression if the data is already compressed (for example, for images and videos).

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



When you apply the policy template to an application or VM in the Application Manager, System Monitor will record the results of the StreamSnap job and it will appear as a single job while it is running. Once replication is complete, two jobs appear in System Monitor with a Succeeded status; one for the Snapshot job and one for the StreamSnap job. If there is a job failure, either for the StreamSnap job or the Snapshot job, two job entries appear to identify which job was successful.

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

**Listing of a Successful StreamSnap Job and Snapshot Job in System Monitor (Two Entries)**

## Production to Mirror: Sync and Async Replication Policies

Sync and Async replication is used by a local and remote Actifio CDS appliance to protect in-band generic applications. Sync and Async replication require a Fibre Channel connection; they are not intended for use by a Actifio Sky appliance. Data that is replicated via Sync and Async is not deduplicated.

- **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 up to 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.





## Scheduling Policy Best Practices at a Glance

The previous sections provided definitions, detailed descriptions, and best practices of how to set a schedule in a policy. The following table summarizes the best practices and most often used schedules for policies.

Production to Snapshot Policy	Snapshot to Dedup Policy	Dedup Backup to Dedup DR Policy	Dedup DR to Remote Replication Policy (Multi-hop)
<p>Defines when and how often production data will be captured and how many snapshots are retained.</p> <p><b>Windowed Schedule -- One Snapshot per Window</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 07:00. Frequency: Once per window. Retain for 2 days.</p> <p><b>Windowed Schedule -- Multiple Snapshots in a Window</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 07:00. Frequency: As needed, not to overlap with time to take a snapshot. Default is every 8 hours. Retain for 2 days.</p> <p><b>Continuous Schedule -- Run Daily at Regular Intervals</b> Continuous schedule spans a single 24 hour boundary. Frequency: As needed, not to overlap with time to take a snapshot. Default is every 8 hours. Retain for 2 days.</p>	<p>Deduplicate a snapshot as soon as possible.</p> <p><b>Windowed (Default)</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 18:59. Frequency: Once per window. Retain for 14 days.</p> <p><b>Continuous</b> Continuous schedule spans a 24 hour boundary. Frequency: Default is to start first job at 19:00 and to run every 24 hours. Retain for 14 days.</p>	<p>Replicate a deduplicated snapshot as soon as possible.</p> <p><b>Windowed (Default)</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 18:50. Frequency: Once per window. Retain for 14 days.</p> <p><b>Continuous</b> Continuous schedule spans a 24 hour boundary. Frequency: Default is to start first job at 00:00 (midnight) and to run every 24 hours. Retain for 14 days.</p>	<p>Replicate 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).</p> <p><b>Windowed (Default)</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 18:59. Frequency: Once per window. Retain for 24 days.</p> <p><b>Continuous</b> Continuous schedule spans a 24 hour boundary. Frequency: Default is to start first job at 00:00 (midnight) and to run every 24 hours. Retain for 24 days.</p>

Production to Direct to Dedup Policy	Snapshot to OnVault Policy	Dedup-Async Replication Policy	StreamSnap Replication Policy
<p>Write deduplicated captured data directly to the Actifio dedup pool. Applies only to VMware VMs.</p> <p><b>Windowed (Default)</b> Window to open as needed, and may or may not span day boundary. Default is 19:00 to 07:00. Frequency: Once per window. Retain for 14 days.</p> <p><b>Continuous</b> Continuous schedule spans a 24 hour boundary. Frequency: Default is to start first job at start first job at 00:00 (midnight) and to run every 8 hours. Retain for 14 days.</p>	<p>Send snapshot data to storage defined by an Actifio OnVault Pool for long-term storage (for example, 3 years).</p> <p>Window to open as needed, and may or may not span day boundary. Default is 19:00 to 18:59. Frequency: Once per window. Retain for 3 Years</p>	<p>Deduplicate snapshot data, replicate the deduplicated data to a remote Actifio appliance, rehydrate this data on the remote appliance, and update the full copy of data on the remote appliance. This policy supports only a continuous schedule. Frequency: Default is to start first job at 00:00 (midnight) and to run every 24 hours.</p>	<p>Replicate snapshot data to a remote Actifio appliance without deduplication, over a high quality network, to provide RPOs as low as one hour.</p> <p>A StreamSnap policy is always tied to a specific Snapshot policy, and uses the schedule and frequency settings of that Snapshot policy.</p> <p>Can retain multiple point-in-time snapshot images at the remote site.</p>

## Application Specific Best Practices

The following sections detail policy template best practices for specific application types.

### Consistency Groups

A consistency group is a group of applications that are quiesced and captured together using a single policy. As the name implies, consistency groups ensure consistent point-in-time capture and recovery across multiple applications.

Capturing application data with a consistency group will consume fewer system resources than capturing applications individually. For this reason, it is common to see groups of SQL Server databases placed into consistency groups.

All applications in a consistency group must exist on the same application server. You cannot place applications from different servers into the same consistency group.

A consistency group cannot contain multiple Oracle databases. However, a single Oracle database can be included in a consistency group with other applications.

---

**Note:** *Generic applications and VMs are not allowed in consistency groups.*

---

### Multiple Applications on a Host

The number of concurrent data capture jobs that are allowed to run for a single application host is configurable, but by default is limited to one at a time. Running one job at a time minimizes the impact on the application servers hosting the data. If some or all of the applications on a host must be captured with separate policy templates, then ensure there are enough system resources (VDisks) to accommodate the individual protection jobs.

### Capture a VM and its Applications

In some cases you may be required to capture an entire VM, then capture one or more applications on that VM. In such situations, create two policy templates; one to capture the VM's boot volume and another to capture the application(s) on the VM. Keep in mind that the two capture operations cannot run at the same time.

### Actifio Sky Appliances on Licensed/Unlicensed ESXi Servers

If an Actifio Sky appliance is installed on an unlicensed (free) ESXi server, the policy templates for that Actifio Sky appliance CANNOT capture other VMs and applications installed on that ESXi server.

If an Actifio Sky appliance is installed on an unlicensed (free) ESXi server, the policy templates for that Actifio Sky appliance CAN capture and access VMs and applications on licensed ESXi servers and applications on physical servers.

If an Actifio Sky appliance is installed on a licensed ESX server, the policy templates for that Actifio Sky appliance CAN capture VMs and applications on the ESX server on which the Actifio Sky appliance is installed. policy templates for that Actifio Sky appliance can also capture VMs and applications on other licensed ESX servers and applications on physical servers.

### Microsoft® SQL Server Databases

For Microsoft® SQL Server databases that use the Full Recovery Model take advantage of the Actifio appliance's ability to capture both the database and its logs with a single policy. When both the database and its logs are captured, the Actifio appliance can recover the database to a point in time by rolling its logs forward via the Actifio Desktop. Capturing both the database and its logs is enabled via the policy template's advanced settings.

## **Microsoft® Exchange**

Actifio appliances capture Microsoft® Exchange by taking snapshots of individual databases.

For Exchange Database Availability Groups (DAG) an Actifio appliance will, by default, capture data from one of the passive nodes. Capturing from the passive node minimizes impact on your production environment. If the passive node should fail, the Actifio appliance can select another node based on a user defined prioritized list of nodes.

Snapshots of Exchange VMs are not supported by Microsoft. VM snapshots can cause performance issues or DAG failovers. Restoring an entire Exchange VM over an existing Exchange VM is not supported by Microsoft. For best results, protect each Exchange database as an application. To do this, install the Actifio Connector on the Exchange VM.

# 3 Policy and System Resource Considerations

---

This section provides guidance on how you can proactively develop a policy template that takes into consideration how the frequency and retention settings for the various policies (Production to Snapshot, Snapshot to Dedup Backup, Production Direct-to-Dedup, and Dedup Backup to Dedup DR) can result in excessive system resource usage which impacts Actifio appliance performance.

This chapter includes the following topics:

[Impact of Policy Settings on System Performance](#) on page 38

[Validating Projected Resources for a Policy](#) on page 39

[Resolving Warnings](#) on page 41

[Viewing the Top 10 policy templates in the Domain Manager](#) on page 42

For an overview of the basic concepts associated with policy templates and resource profiles, see [Chapter 1, Introduction to the Actifio SLA Architect](#).

For a set of best practices to help you avoid common mistakes when creating and modifying policy templates, see [Chapter 2, Best Practices for Policy Templates](#).

## Impact of Policy Settings on System Performance

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

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

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

Critical resources configured as part of a policy template include:

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

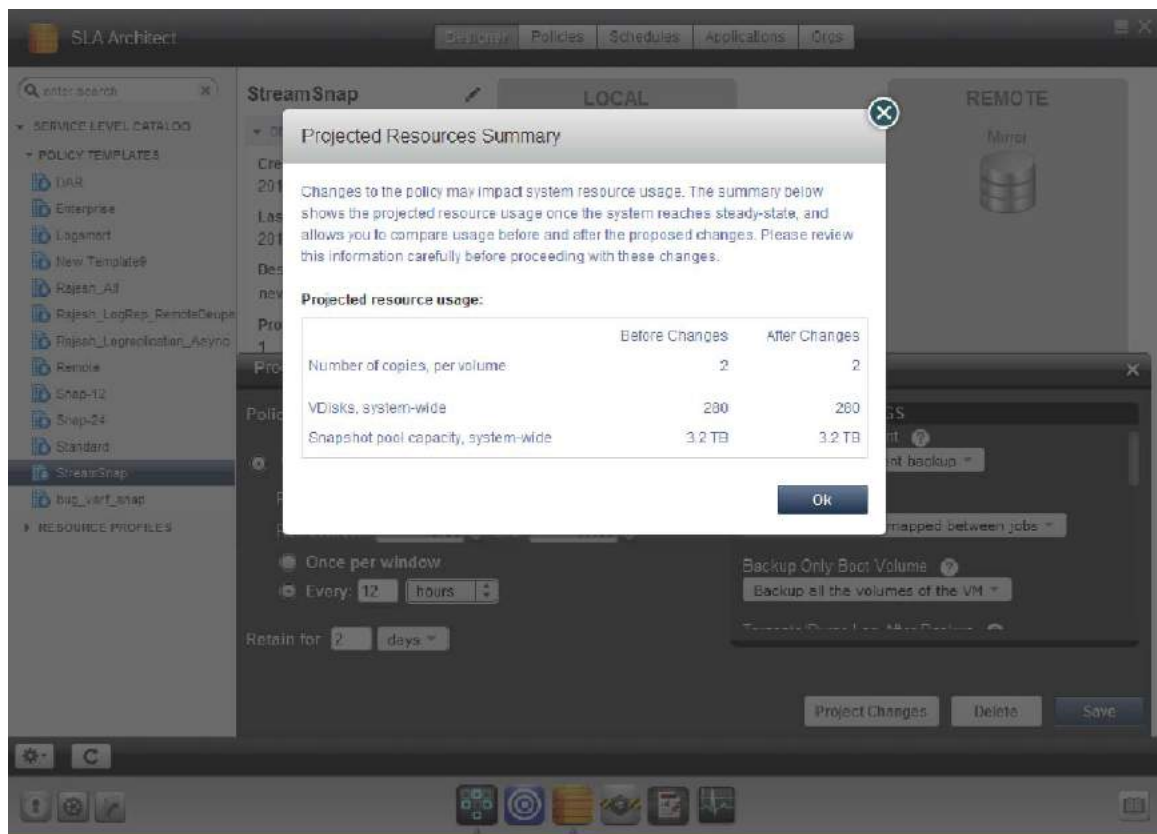
---

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

---

## Validating Projected Resources for a Policy

During policy development in a policy window you can confirm the impact of your policy on system resources by pressing the **Project Changes** button. This action opens the Projected Resources Summary screen for the policy.



### Verifying Project Resources for a Policy

The Projected Resources Summary screen displays Projected Resources Usage information on the configured policy, the number of copies created based on the SLA, and its potential impact on VDisk usage and performance pool usage:

#### Before Changes

- **Number of copies per volume** - The expected number of snapshot copies per volume **before** applying the changes to the current SLA policy.
- **VDisks, system-wide** - The expected VDisks usage by the Actifio appliance to protect applications and VMs **before** applying the changes to the current SLA policy. A VDisk (or volume) is a virtual disk on an Actifio appliance presented to a host as a unit of usable storage capacity. This system resource number is the number of VDisks consumed per volume, including the staging disks.
- **Snapshot pool capacity, system-wide** - The expected usage by all performance pools (staging disks and snapshot disks) as applied to the existing applications and VMs protected by the Actifio appliance **before** applying the changes to the current SLA policy. The Snapshot pool holds "golden copies" of application data at the points in time specified by Service Level Agreement (SLA). The Snapshot pool often contains hundreds of VDisks. This system resource usage is specified as capacity per 1TB based on retention and average change rates.

## After Changes

- **Number of copies per volume** - The expected number of snapshot copies per volume **after** applying the changes to the current SLA policy.
- **VDisks, system-wide** - The expected VDisks usage by the Actifio appliance **after** applying the changes to the current SLA policy.
- **Snapshot pool capacity, system-wide** - The expected performance pool usage by the Actifio appliance **after** applying the changes to the current SLA policy.

Included below is an example of a Projected Resources Summary screen that identifies a potential system resource issue for the defined template policy. At this point you can return to the policy and make the necessary adjustments to reduce VDisk and/or performance pool usage. Evaluate the frequency of the backup operation and lifetime of the backed up data to see where adjustments can be made in the policy.

### Projected Resources Summary

Changes to the policy may impact system resource usage. The summary below shows the projected resource usage once the system reaches steady-state, and allows you to compare usage before and after the proposed changes. Please review this information carefully before proceeding with these changes.

**Projected resource usage:**

	Before Changes	After Changes
Number of copies, per volume	1	15
VDisks, system-wide	439	523
Snapshot pool capacity, system-wide	18 TB	20 TB

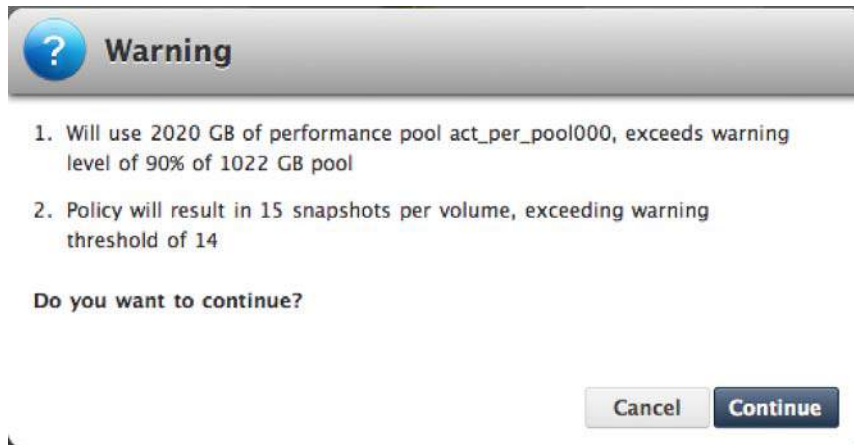
Ok

## Verifying Project Resources for a Policy -- Exceeded System Resources



## Resolving Warnings

When you perform a **Save** from a policy window, if there are issues with the policy settings a warning message appears.



### Policy Exceeding Performance Pool and Snapshot Limits

Warnings display when:

- The SLA policy has more than 14 snapshots.
- VDisk usage with the SLA policy (new or modified) will result in VDisks usage exceeding the warning level (default of 90%) during steady state.
- Performance pool (staging disks and snapshot disks) usage with the SLA policy (new or modified) results in a performance pool to exceed its warning level (default of 90% for the snapshot and primary pools).
- Adding a new dedup SLA policy when dedup utilization is already at the warning level (75% by default) and there are additional dedup jobs in the queue. This action has the potential of adding more dedup jobs to an already overloaded dedup system.

You can choose to:

- Click **Cancel** to adjust the policy template.
- Click **Continue** to accept the policy.

If you choose to make changes to the policy in the SLA Architect, evaluate the frequency of the backup operation and lifetime of the backed up data to see where adjustments can be made to resolve the warning.

## Viewing the Top 10 policy templates in the Domain Manager

For each Service Level Agreement (SLA), the top resources consumed by applications and VMs protected by policy templates appear in the **System > Configuration > Resources** section of the Domain Manager, in the Top 10 Templates tab.

Resource consumption information includes:

- Top 10 VDisk-consuming applications (with total number of VDIs used)
- Top 10 snapshot pool space usage applications (including total amount of storage used)

If you double-click a row in either the VDisk Usage or Snapshot Pool Usage table, this action brings you to the associated policy template in the SLA Architect.

For details on viewing the top 10 policy templates in the Domain Manager, see **Configuring Resources and Settings With the Domain Manager** in the Actifio Documentation Library and on the Actifio Now customer portal.

**Domain Manager** | Summary | VDIs | Snaps | Replication | **Top 10 Templates** | Mirror

Search: enter search

**Top 10 Templates**

**APPLIANCE DETAILS**

Appliance ID: 590021132436  
Appliance Name: amazon  
Appliance IP: 172.16.9.111

**VDisks Usage**

Policy Template	VDIs
Remote	182
Snap-12	122
Logsmart	47
bug_verif_snap	37
DAR	29
Rajesh_All	21
Snap-24	14
Rajesh_Logreplication_Async	5
StreamSnap	4

\*Double click on selected row to see the policy template details.

**Snapshot Pool Usage**

Policy Template	Snapshot Pool
Rajesh_All	53.2 GB
Logsmart	59.2 GB
Snap-24	18.3 GB
Snap-12	15.5 GB
Remote	14.2 GB
Rajesh_Logreplication_Async	1.9 GB
DAR	867.5 MB
bug_verif_snap	692.8 MB
StreamSnap	145.3 MB

### Verifying Resources for All Policy Templates in the Domain Manager

# 4 Creating and Managing Policy Templates

---

**Note:** Before attempting the procedures in this chapter you should understand the concepts presented in **Getting Started with Actifio Copy Data Management** included in the Actifio Documentation Library and also available on the Actifio Now customer portal.

---

This chapter includes:

- [Creating and Modifying a Policy Template](#) on page 44
- [Cloning a Policy Template](#) on page 47
- [Exporting a Policy Template](#) on page 47
- [Importing a Policy Template](#) on page 47
- [Viewing Policy Templates](#) on page 48
- [Deleting a Policy Template](#) on page 48
- [Viewing Policy Schedules](#) on page 49
- [Viewing the Applications Protected by a Policy Template](#) on page 50
- [Viewing and Modifying Organizations and Policy Relationship](#) on page 50

---

**Note:** The SLA Architect enforces a specific policy development sequence when you define the policies associated with a policy template. Certain policies will be unavailable based on the type of policy template you develop.

*In addition, the types and number of policy templates and the minimum and maximum settings of policies are specific to the Actifio appliance on which they reside. Your policy templates can look slightly different from those used in the following examples.*

---

For an overview of the basic concepts associated with policy templates and resource profiles, see [Chapter 1, Introduction to the Actifio SLA Architect](#). This chapter also includes guidance on defining SLA Template Policy Compliance.

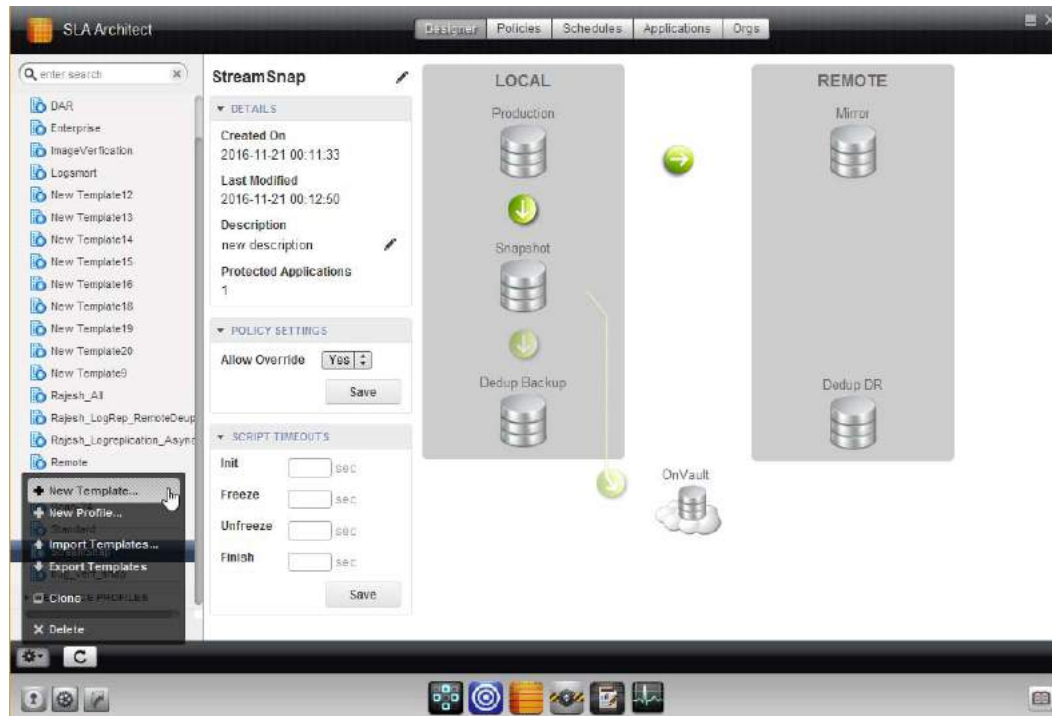
The best practices for creating and modifying specific policies in an SLA Template, can be found in [Chapter 2, Best Practices for Policy Templates](#).

For guidance on how you can proactively develop a policy template that takes into consideration the frequency and retention settings for various policies, see [Chapter 3, Policy and System Resource Considerations](#).

## Creating and Modifying a Policy Template

To create a new template or modify an existing template:

1. Open the **SLA Architect**.
2. Select a predefined template or select **New Template** from the Services menu.
3. Select the **Designer** tab.



### Creating a New Template

4. To modify the Allow Overrides Policy Settings, click **POLICY SETTINGS**.
  - o Select **Yes** to allow selected Application Manager advanced settings to override the settings specified in an SLA policy's advanced settings.
  - o Click **No** if you do not want to allow SLA policy setting override in the Application Manager.

See [Policy Advanced Settings Override](#) on page 4 for details.

5. To create host-side scripts that run on an application's host before and/or after a policy is run, click **SCRIPT TIMEOUTS** and define host-side script timeout selections as needed. See [Configuring Host-Side Script Timeouts](#) on page 46 for details.

6. Depending on your template requirements, click one of the policy arrows in the graphical SLA policy map. The green arrows displayed in graphical SLA policy map represent the individual policies in the template. Policy types include: Snapshots, Snapshot to OnVault, Dedup Images, Direct-to-Dedup, Remote, and Production-to-Mirror replication (Dedup Async, StreamSnap, Sync, or Async).

Dark green arrows indicate that a policy has been defined. Light green arrows indicate that a policy is not available or cannot be defined for the specific policy template.

---

**Note:** For a set of best practices to help you avoid common mistakes when creating and modifying a template with one or more policies, see [Chapter 2, Best Practices for Policy Templates](#).

---

7. From the policy window, develop or edit the policy as needed. For new templates, click **Click to Add Policy** in the policy window. See [Chapter 5, Creating Policies](#) for details on creating or modifying a policy.



### Creating or Modifying a Policy

8. Click **Save** to add the policy to the template. If there are issues with the policy settings, a warning message appears. You can adjust the policy (click **Cancel**) or click **Continue** to accept the policy. See [Resolving Warnings](#) on page 41 for details.
9. If appropriate for your templates, click Add Policy to create another policy. For example, if you create a Production to Snapshot policy and you also want to perform deduplication on those images, you can then create and save a Snapshot to Dedup policy from the policy window.

---

**Note:** Multiple deduplication policies cannot run simultaneously on an application, they run one at a time.

---

10. When you are done creating or modifying policies close the policy window to return to the Template Designer window.

## Configuring Host-Side Script Timeouts

**Note:** For details on host-side scripting, see **Connecting Hosts to Actifio Appliances** in your Actifio Documentation Library.

The Actifio Connector allows you to create host-side scripts that run on an application's host before and/or after a policy is run. The four timeouts provided in a policy template map directly into the four stages of a host-side script:

**Init:** Defines how long a policy should wait before assuming host-side scripts on a protected host have been initialized.

**Freeze:** Defines how long a policy should wait before assuming the application is frozen and ready for protection.

**Unfreeze:** Defines how long a policy should wait before assuming the application is unfrozen.

**Finish:** Defines how long a policy should wait before protection is complete.

By default, script timeout values are displayed empty but set to their default values:

**Init:** Default value is 120 seconds, range is from 1 - 86400 seconds (24 hours).

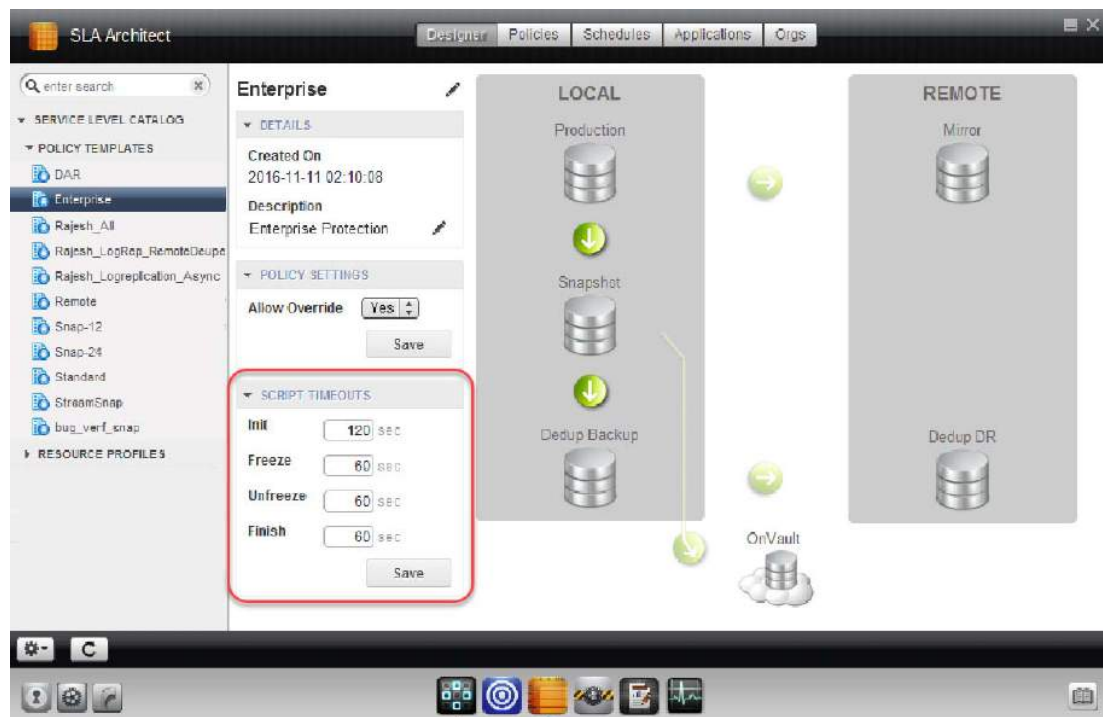
**Freeze:** Default value is 60 seconds, range is from 1 - 86400 seconds.

**Unfreeze:** Default value is 60 seconds, range is from 1 - 86400 seconds.

**Finish:** Default value is 60 seconds, range is from 1 - 86400 seconds.

To set host-side script timeouts:

1. Within a policy template, click **SCRIPTTIMEOUT**.
2. Enter the script timeout values for Init, Freeze, Unfreeze, and/or Finish.
3. Click **Save**.



**Configuring ScriptTimeouts in a Template**

## Cloning a Policy Template

You can clone a template to create a custom template.

1. Open the SLA Architect.
2. Select a template from the policy templates navigation pane.
3. From the service menu, select **Clone**. A copy of the selected template is created. You can modify the details of the policy as required.

## Exporting a Policy Template

You can export all policy templates of an Actifio appliance together:

1. Open the SLA Architect.
2. From the service menu, select **Export Templates....** A single file with a copy of each template is created at the specified location.

## Importing a Policy Template

You can import a policy template from other Actifio appliances to use the existing policy configurations.

To import a policy template:

1. Open the SLA Architect.
2. From the service menu, select **Import Templates....** The Import Template dialog appears.

IMPORT TEMPLATE

Template Path:  **Browse**

**Ignore** **Add** **Replace**

These buttons determine how Actifio Desktop manages the local templates when a template with the same name is imported.  
When you click Ignore, Actifio Desktop does not import the template.  
Click Replace to replace the existing template.  
Click Add to retain the existing template and also download the new template with a modified name

**Save** **Cancel**

3. Select the template file using the **Browse** button. If you import a template with the same name as an existing template, you can overwrite the existing template or save the template with a different name.
4. Click **Ignore**, **Add**, or **Replace**. These buttons determine how Actifio Desktop manages the local templates when a template with the same name is imported:
  - o Use **Replace** to replace an existing template.
  - o Use **Add** to retain the existing template and also download the new template with a different name.
  - o Use **Ignore** to not import the selected template.
5. Click **Save**.

## Viewing Policy Templates

To view the configured policy templates on an Actifio appliance, open the SLA Architect to the **Policies** tab. A list of all the policies configured on the Actifio appliance appears.



### Viewing Two Policy Templates

## Deleting a Policy Template

You can delete a template.

1. Open the SLA Architect.
2. Select the template you would like to delete.
3. From the service menu, select **Delete**.
4. Click **Yes** in the confirmation dialog.

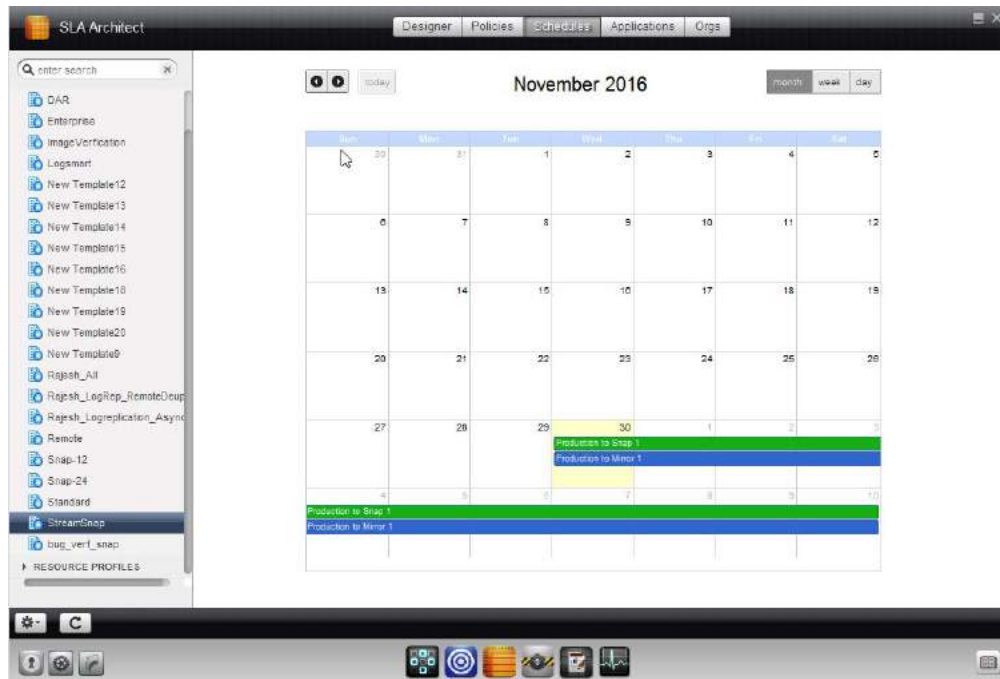


## Viewing Policy Schedules

To view the schedules of the policies of a policy template:

1. Open the SLA Architect to the **Schedules** tab.
2. Select the template you would like to view the schedules of the policies from the navigation name.

The schedules are displayed in a calendar view.



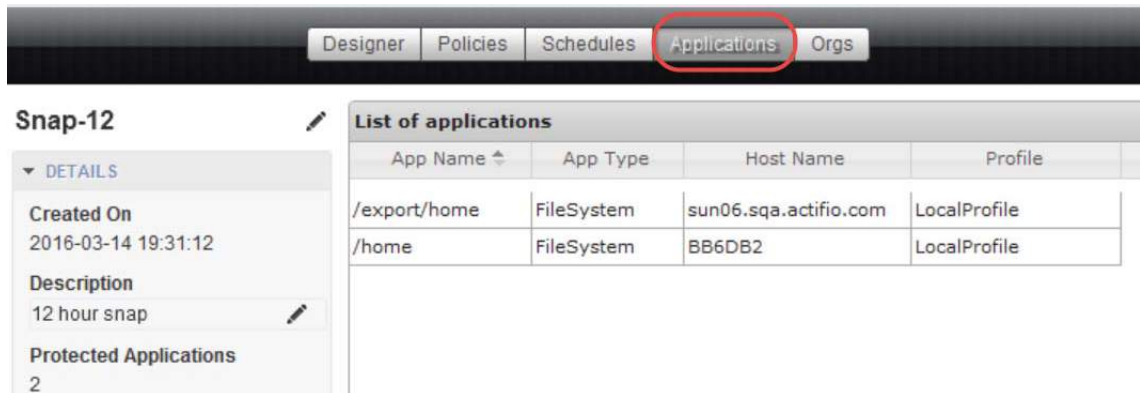
**Viewing Policy Schedules**

## Viewing the Applications Protected by a Policy Template

To view the applications protected by a policy template:

1. Open the SLA Architect to the **Applications** tab.
2. Select the template from the navigation pane.

A list of protected applications appears.

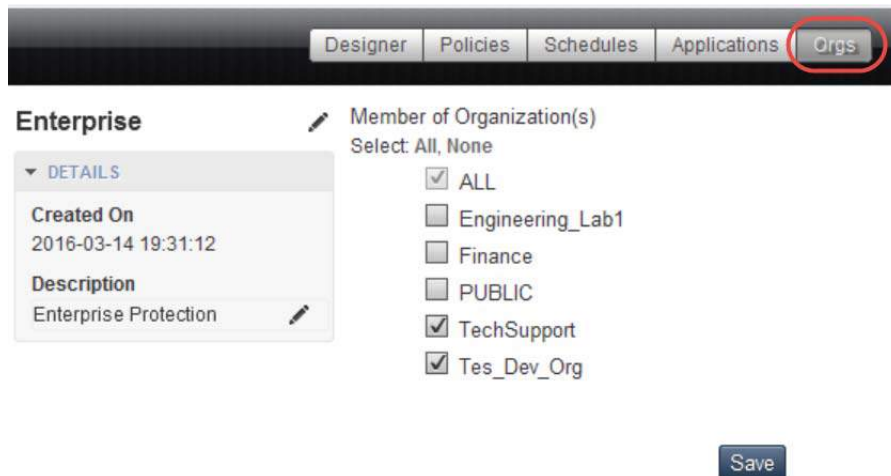


### Viewing Applications Protected by a Policy Template

## Viewing and Modifying Organizations and Policy Relationship

To view or modify the organization and policy template relationship:

1. Open the SLA Architect.
2. Select the template from the navigation pane.
3. Click **Orgs** from the menu bar. A list of member organizations is displayed.



### Viewing and Modifying Organizations and Policy Relationship

**Note:** In this page, you can make changes to the existing policy template. Add or remove a policy template as an organization member from the available organizations list using the appropriate check boxes and click **Save** to update the changes.

# 5 Creating Policies

---

**Note:** Before attempting the procedures in this chapter you should understand the concepts presented in **Getting Started with Actifio Copy Data Management** included in the Actifio Documentation Library and also available on the Actifio Now customer portal.

---

This chapter describes:

[Creating a Production to Snapshot Policy](#) on page 52

[Creating a Snapshot to Dedup Backup Policy](#) on page 60

[Creating a Production Direct-to-Dedup Policy](#) on page 63

[Creating a Dedup Backup to Dedup DR Policy](#) on page 68

[Creating a Multi-hop Remote Dedup Backup Replication Policy](#) on page 71

[Creating a Snapshot to OnVault Policy](#) on page 58

[Creating a Production to Mirror Policy](#) on page 74

The best practices for creating and modifying specific policies in an SLA Template, can be found in [Chapter 2, Best Practices for Policy Templates](#). This chapter also includes guidance on defining SLA Template Policy Compliance.

For guidance on how you can proactively develop a policy template that takes into consideration the frequency and retention settings for various policies, see [Chapter 3, Policy and System Resource Considerations](#).

For the step-by-step procedure on how to develop a policy template, see [Chapter 4, Creating and Managing Policy Templates](#).

## Creating a Production to Snapshot Policy

Production to Snapshot policies define how to capture application production data as a snapshot. Snapshots are the fast virtualization step that protects your data at a specific moment. For a set of best practices when developing a Production to Snapshot policy, see [Production to Snapshot Policies](#) on page 19.

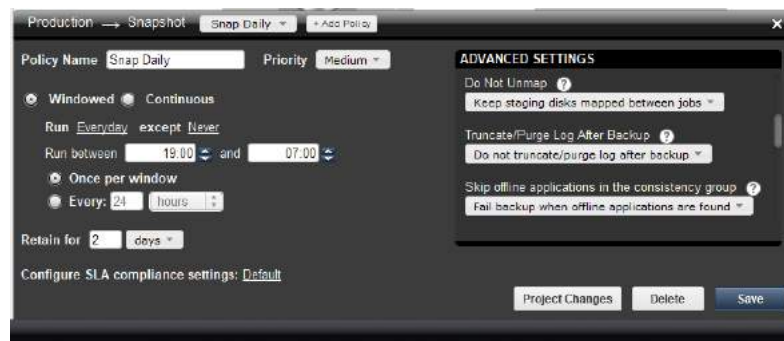
---

**Note:** A Production to Snapshot policy is a requirement if you are developing a template that includes a Snapshot to Dedup Backup policy (see [Creating a Snapshot to Dedup Backup Policy](#) on page 60) or a Production to Mirror StreamSnap replication policy (see [Creating a StreamSnap Production to Mirror Replication Policy](#) on page 79).

---

To create a new Production to Snapshot policy:

1. Open the SLA Architect.
2. Click **New Template...** from the service menu.
3. Click the arrow between **Production** and **Snapshot**. The policy window appears.
4. Click the **+**(plus) icon. The policy settings are displayed.



### Creating a Policy for Snapshots (Windowed)

5. Enter a policy name in **Policy Name**.
6. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

7. Specify the schedule type for the Production to Snapshot policy: Windowed or Continuous. The default is Windowed.
  - o **Windowed** - Defines a discrete snapshot image capture schedule adhering to a specific frequency and time window (for example, perform a capture every 30 minutes, daily from 9 am to 5 pm). You can instruct the Actifio appliance to run multiple capture jobs at a specified frequency interval or once during a specified time window.
  - o **Continuous** - Defines a continuous snapshot image capture schedule (for example, perform a capture job every 8 hours, starting the first job at 1 am). In this policy schedule, jobs run continuously (24/7) at the specified time interval.
8. Configure the policy frequency settings per the selected schedule type as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency of the policy by defining an interval at which snapshot images are captured. Based on this interval setting, the snapshot job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Defines an exception to the Run schedule. You can specify an Except value of daily, weekly, monthly, or yearly. For example, to skip the daily snapshot schedule every Friday, select weekly and select Friday.  Click the link to the right of this parameter and modify the exception. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing snapshot images.
Once Per Window	Specifies that the frequency duration for capturing snapshot images is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing snapshot images during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the snapshot image capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of snapshot image captures.
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the snapshot image. Example: retain the image for 2 days.

9. Configure the **Advanced Settings** for the Production to Snapshot policy.

**Note:** Advanced Settings defined in a policy can be overridden by the Application Advanced Settings in the Application Manager, provided the policy's template has been set to allow overrides (see [Creating and Modifying a Policy Template](#) on page 44).

Advanced Setting	Description
<b>Application Consistent</b> (Oracle and SQL databases, Hyper-V VMs with Microsoft Hyper-V Integration Services enabled, and Microsoft Exchange, SharePoint, and file systems protected out-of-band are always application consistent.)	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Take crash consistent backup:</b> Crash-consistent backup is a fast backup of application data in storage as if power were lost at that moment. It does not pause application data I/O. All data on disk are saved, and data in memory is lost. Incomplete transactions may be saved. The recovery of a crash consistent backup may take longer time and introduce exceptions. Typically recovery from crash has to be made manually. Crash consistent backups are easy and fast for virtual machines.</li> <li>• <b>Take application consistent backup:</b> Application-consistent backup notifies the application to prepare for a backup. This option loses no data. It pauses application data I/O, completes in-flight transactions, and flushes memory to disk. On recovery, data is easily accessible. For virtual clients, usually an agent is needed to get notification of a backup at host, and then notify applications, and may need to wait for an approval from applications. Not all applications support application-consistent backups.</li> <li>• <b>Take crash consistent backup on last try:</b> This protection option initially takes application consistent backups, but if an application consistent backup fails for any reason, it will then take a crash consistent backup.</li> </ul>
<b>Do Not Unmap</b>	<p>Select either:</p> <ul style="list-style-type: none"> <li>• <b>Keep staging disks mapped between jobs:</b> Select this option if you want the temporary staging disks mapped to the host and used during data movement to remain mapped to the host. LUNs are mapped during the first job and subsequent jobs reuse the same mapped LUN. By default, this is selected.</li> </ul> <p><b>Note:</b> For applications protected using the Actifio Connector where the application is on an OS running inside a VMware VM, this option is ignored. The staging disk will be unmapped from the VM after every job.</p> <ul style="list-style-type: none"> <li>• <b>Unmap staging disks after each job:</b> This option both unmounts the staging disk from the operating system at the conclusion of every job (removing mount points or drive letters), and also unmaps it from the host altogether. This option will require the host to perform a scan for SCSI LUNs at the start of the next job, as the re-mapped staging disks must be rediscovered before they can be remounted.</li> </ul>
<b>Backup Only Boot Volume</b> (VMs only)	<p>Specify whether to back up only the boot volume of the VM or all volumes of the VM:</p> <ul style="list-style-type: none"> <li>• <b>Back up all the volumes of VM</b></li> <li>• <b>Backup only boot volume of the VM</b></li> </ul> <p><b>Note:</b> When protecting VMware and Hyper-V VMs, if the boot volume is not the first drive on the bus, or if application binaries are spread over multiple VMware VMDKs, then the entire boot volume may not be captured.</p>

Advanced Setting	Description
<b>Truncate/ Purge Log After Backup</b>	<p>Specify whether to truncate the logs after every backup. When <b>Truncate/Purge Log After Backup</b> is enabled, application-related logs are truncated until the recent or current backup. If you truncate logs, you must also back up the transaction log to enable a roll forward recovery. (SQL Server, Exchange, SharePoint). Options are:</p> <ul style="list-style-type: none"> <li>• <b>Do not truncate/purge log after backup</b></li> <li>• <b>Truncate/purge log after backup</b></li> </ul>
<b>Skip offline applications in consistency group</b> (Not Oracle)	<p>Select how to handle offline applications in a consistency group:</p> <ul style="list-style-type: none"> <li>• <b>Skip offline applications during backup:</b> Offline applications in a consistency group will be skipped and the backup will not fail.</li> <li>• <b>Fail backup when offline applications are found</b></li> </ul>
<b>Map staging disks to all nodes in an application cluster</b>	<p>If your nodes are in an application cluster, you can use this to ensure that the nodes of an application cluster are protected in case of failover during backup.</p> <ul style="list-style-type: none"> <li>• <b>Do not map staging disk to all nodes of application cluster</b></li> <li>• <b>Map staging disk to all nodes of application cluster:</b> In the event of an application cluster failure, this option will protect failover copies.</li> </ul>
<b>Map staging disk to all ESX hosts in a cluster</b> (VMware VMs only)	<p>If your ESX servers are in a cluster, you can use this setting to ensure that the VMs are protected in case of failover during backup. (Oracle, local filesystems, CIFS, NFS, SharePoint, SQL Server, Exchange):</p> <ul style="list-style-type: none"> <li>• <b>Do not map staging disk to all ESX hosts</b></li> <li>• <b>Map staging disk to all ESX hosts:</b> In the event of an ESX host failure, this option will protect failover copies of VMware VMs.</li> </ul>
<b>Force Out of Band Backup</b>	<p>Specify if you want to force In-Band backups to an Out-of-Band mode. Options are <b>Yes</b> or <b>No</b>.</p>
<b>Enable Database Log Backup</b>	<p>The Enable Database Log Backup option allows the SLA policy to backup an Oracle or Microsoft® SQL Server database and all associated transaction log files. The logs are backed up when the log snapshot job runs. Options are Yes or No. When set to <b>Yes</b>, the related options are enabled.</p> <p>See <a href="#">Database Log File Snapshot Policies</a> on page 22 for background details on the frequency and log retention settings when creating a Production to Snapshot policy for an Oracle or Microsoft SQL Server database.</p>
<b>RPO</b>	<p>When Enable Database Log Backup is set to <b>Yes</b>, RPO defines the frequency for database log backup. Frequency is set in minutes and must not exceed the database backup interval.</p>
<b>Log Backup Retention Period (in days)</b>	<p>When Enable Database Log Backup is set to <b>Yes</b>, log retention is defined separately from the retention of the Snapshot policy. Having a separate retention period allows you to use logs in conjunction with copies of the database stored in both the Snapshot and Dedup pools. The log retention period is a mandatory setting.</p>

Advanced Setting	Description
<b>Replicate Logs (Using StreamSnap Technology)</b>	<p>When Enable Database Log Backup is set to <b>Enable</b>, the Replicate Logs advanced setting allows Oracle archive logs or Microsoft® SQL Server database transaction logs to be replicated to a remote Actifio appliance. For a log replication job to run, there must be a replication policy (StreamSnap, Dedup-Async, or Remote Dedup) included in the template along with a resource profile that specifies a remote Actifio appliance, and at least one successful replication of the database must first be completed. You can then use the logs at the remote site for any database image within the retention range of the replicated logs. This function is enabled by default.</p> <p>Log replication uses StreamSnap technology to perform the replication between the local and remote Actifio appliances; log replication goes directly from the local snapshot pool to the snapshot pool on the remote appliance.</p> <hr/> <p><b>Note:</b> Log replication does not occur until an Oracle or SQL Server database has been protected and the database replicated to the remote Actifio appliance.</p> <hr/>
<b>Log Staging Disk Size Growth (in Percent)</b>	<p>When Enable Database Log Backup is set to <b>Yes</b>, Log Staging Disk Growth Size defines the growth to use when automatically growing the staging disk on which the logs reside. This setting is from 5 to 100 percent.</p>
<b>Estimated Change Rate</b>	<p>When Enable Database Log Backup is set to <b>Yes</b>, this setting defines the daily change (in percent), which allows the Actifio appliance to better calculate the size of the staging disk needed to hold logs. This setting is from 0 to 100.</p>
<b>Compress Database Log Backup</b>	<p>When Enable Database Log Backup is set to <b>Yes</b>, this setting instructs the source database to compress its logs before capture by the Actifio appliance. The database server performs log compression during log backup.</p>
<b>Job Behavior When Target VM Needs Snapshot Consolidation</b>	<p>Select an action if the VM requires consolidation:</p> <ul style="list-style-type: none"> <li>• <b>Fail the job:</b> backup/DAR/direct-dedup jobs fail.</li> <li>• <b>Run the job without performing consolidation:</b> All jobs run normally even if consolidation is pending.</li> <li>• <b>Perform consolidation at the beginning of the job:</b> Backup/direct-dedup/DAR jobs try to perform consolidation at the beginning of the job. If consolidation fails, the job fails with an error message.</li> </ul>
<b>Fail On Missing Start Path</b>	<p>If one or more start paths are specified, and any of these start paths does not exist, the job will fail with the message <b>UDSAgent: Specified start path does not exist</b>. If no start paths are specified, this option has no effect. Options are <b>Yes</b> or <b>No</b>. The default is <b>No</b>.</p>
<b>Enable Degraded Capture Mode</b>	<p>Degraded capture mode captures incremental data when Change Block Tracking (CBT) service is unavailable. Data capture may take longer. Options are Yes or No.</p>



10. Prior to saving your policy, if you would like to first confirm if the policy settings will consume system resources and possibly result in system performance issues, click **Project Changes**. The Projected Resources Summary screen appears. See [Validating Projected Resources for a Policy](#) on page 39 for details.
11. Click **Save**. If there are issues with the policy settings a warning message appears. You can adjust the policy (click **Cancel**) or click **Continue** to accept the policy. See [Resolving Warnings](#) on page 41 for details.
12. Proceed to [Creating a Snapshot to Dedup Backup Policy](#) on page 60 to create a policy that will deduplicate the snapshot.

## Creating a Snapshot to OnVault Policy

The Snapshot to OnVault policy allows you to send snapshot data to storage defined by the Actifio OnVault Pool. A schedule within the policy is used to send the most recent snapshot taken by the policy template's Production to Snapshot policy to the storage defined by the Actifio OnVault Pool. The Actifio OnVault Pool storage is typically used for long-term retention (for example for 3 years). For a set of best practices when developing a Snapshot to OnVault policy, see [Snapshot to OnVault Policies](#) on page 28.

---

**Note:** Before you can define a Snapshot to OnVault Policy you must first define a corresponding Snapshot policy as described in [Creating a Production to Snapshot Policy](#) on page 52.

---

To create a Production Snapshot to OnVault policy:

1. Open the SLA Architect.
2. Click **New Template...** from the service menu. A new policy template is displayed.
3. Click the arrow between **Production** and **Snapshot** and define a Production to Snapshot policy as described in [Creating a Production to Snapshot Policy](#) on page 52.
4. Click the arrow between **Snapshot** and **OnVault**. The arrow is activated when a Production to Snapshot Policy is defined.
5. Click the **+**(plus) icon. The policy settings are displayed.

The screenshot shows a configuration window titled 'Snapshot to OnVault 1'. At the top, there's a breadcrumb 'Snapshot -> OnVault' and a '+ Add Policy' button. Below this, the 'Policy Name' is 'Snapshot to OnVault 1' and the 'Priority' is 'Medium'. There are two radio buttons for 'Windowed' (selected) and 'Continuous'. Under 'Windowed', there's a 'Run' section with 'Everyday' selected and 'except Never' as an option. Below that, 'Run between' is set to '19:00' and '18:59'. There are also radio buttons for 'Once per window' (selected) and 'Every: 24 hours'. At the bottom, 'Retain for' is set to '14 days'. 'Cancel' and 'Save' buttons are at the bottom right.

### Creating an OnVault Policy

6. Enter a policy name in **Policy Name**.
7. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority.

8. Configure the policy frequency schedule as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency at which data will be captured by defining an interval at which the OnVault policy is run.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Defines an exception to the Run schedule. You can specify an Except value of daily, weekly, monthly, or yearly. For example, to skip every Friday, select weekly and select Friday.  Click the link to the right of this parameter and modify the exception. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing data.
Once Per Window	Specifies that the frequency duration for capturing data is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing data during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the data capture.
Start First Job At	Specifies the time of day at which to run the first job in the continuous cycle of data.
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the captured data. Example: retain the image for 14 days.

9. Click **Save** to save the policy changes.

## Creating a Snapshot to Dedup Backup Policy

Snapshot to Dedup Backup policies define how often to deduplicate production data captured from a Production to Snapshot policy. Deduplication is not as time-sensitive as the snapshot; you can schedule dedup jobs for times that snapshot jobs are not running such as overnight. For a set of best practices when developing a Snapshot to Dedup Backup policy, see [Snapshot to Dedup Backup Policies](#) on page 23.

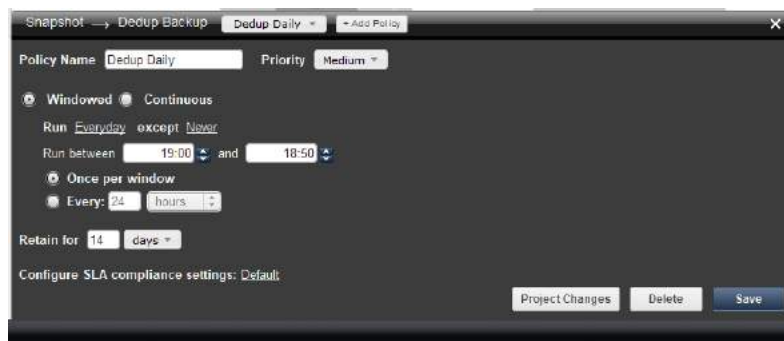
---

**Note:** Before creating a policy for deduplication, you must first create a Snapshot policy as described in [Creating a Production to Snapshot Policy](#) on page 52.

---

To create a Snapshot to Dedup Backup policy:

1. Open the SLA Architect and select a template that includes a Snapshot policy.
2. Click the arrow between **Snapshot** and **Dedup**. The policy window appears.
3. Click the **+**(plus) icon. The policy settings are displayed.



### Creating a Policy for Deduplication (Windowed)

4. Enter a name in **Policy Name**.
5. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

6. Specify the schedule type for the Snapshot to Dedup Backup policy: Windowed or Continuous. The default is Windowed.
  - o **Windowed** - Defines a discrete dedup image capture schedule adhering to a specific frequency and time window (for example, perform a capture every 30 minutes, daily from 9 am to 5 pm). You can instruct the Actifio appliance to run multiple capture jobs at a specified frequency interval or once during a specified time window.
  - o **Continuous** - Defines a continuous dedup image capture schedule (for example, perform a capture job every 8 hours, starting the first job at 1 am). In this policy schedule, jobs run continuously (24/7) at the specified time interval.
7. Configure the policy frequency settings per the selected schedule type as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency of the policy by defining an interval at which dedup backup images are captured. Based on this interval setting, the dedup backup job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Defines an exception to the Run schedule. You can specify an Except value of daily, weekly, monthly, or yearly. For example, to skip the daily dedup backup schedule every Friday, select weekly and select Friday.  Click the link to the right of this parameter and modify the exception. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing dedup backup images.
Once Per Window	Specifies that the frequency duration for capturing dedup backup images is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing dedup backup images during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the dedup backup image capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of dedup backup image captures.
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the dedup backup image. Example: retain the image for 14 days.

8. Prior to saving your policy, if you would like to first confirm if the policy settings will consume system resources and possibly result in system performance issues, click **Project Changes**. The Projected Resources Summary screen appears. See [Validating Projected Resources for a Policy](#) on page 39 for details.
9. Click **Save**. If there are issues with the policy settings a warning message appears. You can adjust the policy (click **Cancel**) or click **Continue** to accept the policy. See [Resolving Warnings](#) on page 41 for details.

## Creating a Production 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. For a set of best practices when developing a Production Direct-to-Dedup policy, see [Production to Direct to Dedup Policies](#) on page 24.

VMware VMs that are protected direct-to-dedup do not go through a staging disk because the Actifio appliance can get changed-block information directly from the VMware layer.

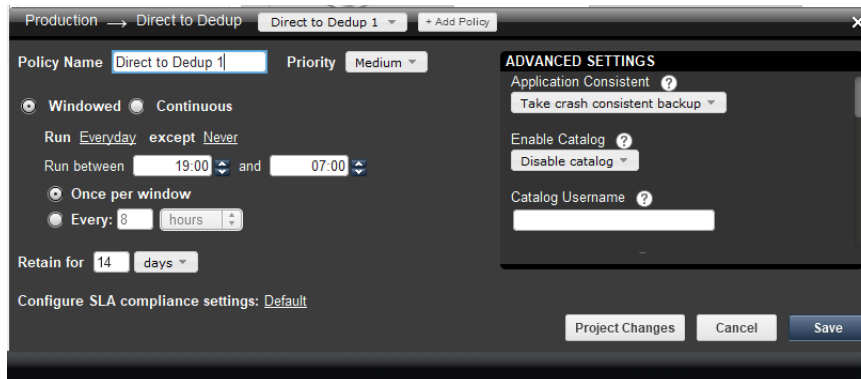
---

**Note:** 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 Snapshot policy as described in [Creating a Production to Snapshot Policy](#) on page 52.

---

To create a policy for Direct-to-Dedup:

1. Open the SLA Architect.
2. Click **New Template** from the service menu.
3. Click the long arrow (indicates Direct to Dedup) between **Production** and **Dedup**. A warning message is displayed; click **OK**. The policy window appears.
4. Click the **+**(plus) icon. The policy settings are displayed.



### Creating a Policy for Direct-to-Dedup (Windowed)

5. Enter a name in **Policy Name**.
6. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

7. Specify the schedule type for the Direct-to-Dedup policy: Windowed or Continuous. The default is Windowed.
  - o **Windowed** - Defines a discrete Direct-to-Dedup image capture schedule adhering to a specific frequency and time window (for example, perform a capture every 30 minutes, daily from 9 am to 5 pm). You can instruct the Actifio appliance to run multiple capture jobs at a specified frequency interval or once during a specified time window.
  - o **Continuous** - Defines a continuous Direct-to-Dedup image capture schedule (for example, perform a capture job every 8 hours, starting the first job at 1 am). In this policy schedule, jobs run continuously (24/7) at the specified time interval.
8. Configure the policy frequency settings per the selected schedule type as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency of the policy by defining an interval at which Direct-to-Dedup images are captured. Based on this interval setting, the Direct-to-Dedup job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Defines an exception to the Run schedule. You can specify an Except value of daily, weekly, monthly, or yearly. For example, to skip the daily Direct-to-Dedup schedule every Friday, select weekly and select Friday.  Click the link to the right of this parameter and modify the exception. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing Direct-to-Dedup images.
Once Per Window	Specifies that the frequency duration for capturing Direct-to-Dedup images is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing Direct-to-Dedup images during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the Direct-to-Dedup capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of Direct-to-Dedup image captures.
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the Direct-to-Dedup image. Example: retain the image for 14 days.



9. Configure the **Advanced Settings** for the Production Direct-to-Dedup policy:

---

**Note:** Advanced Settings defined in a policy can be overridden by the Application Advanced Settings in the Application Manager, provided the policy's template has been set to allow overrides (see [Creating and Modifying a Policy Template](#) on page 44).

---

Advanced Setting	Description
<b>Application Consistent</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Take crash consistent backup:</b> Crash-consistent backup is a fast backup of application data in storage as if power were lost at that moment. It does not pause application data I/O. All data on disk are saved, and data in memory is lost. Incomplete transactions may be saved. The recovery of a crash consistent backup may take longer time and introduce exceptions. Typically recovery from crash has to be made manually. Crash consistent backups are easy and fast for virtual machines.</li> <li>• <b>Take application consistent backup:</b> Application-consistent backup notifies the application to prepare for a backup. This option loses no data. It pauses application data I/O, completes in-flight transactions, and flushes memory to disk. On recovery, data is easily accessible. For virtual clients, usually an agent is needed to get notification of a backup at host, and then notify applications, and may need to wait for an approval from applications. Not all applications support application-consistent backups.</li> <li>• <b>Take crash consistent backup on last try:</b> This protection option initially takes application consistent backups, but if an application consistent backup fails for any reason, it will then take a crash consistent backup.</li> </ul> <hr/> <p><b>Note:</b> Oracle and SQL databases, Hyper-V VMs with Microsoft Hyper-V Integration Services enabled, and Microsoft Exchange, SharePoint, and file systems protected out-of-band are always application consistent.</p> <hr/>
<b>Do Not Unmap</b>	<p>Select either:</p> <ul style="list-style-type: none"> <li>• <b>Keep staging disks mapped between jobs:</b> Select this if you want the temporary staging disks mapped to the host and used during data movement to remain mapped to the host. LUNs are mapped during the first job and subsequent jobs reuse the same mapped LUN. By default, this is selected.</li> </ul> <p><b>Note:</b> For applications protected using the Actifio Connector (such as SQL or Exchange databases) where the application is on an OS running inside a VMware VM, this option is ignored. The staging disk will always be unmapped from the VM after every job.</p> <ul style="list-style-type: none"> <li>• <b>Unmap staging disks after each job:</b> This option both unmounts the staging disk from the operating system at the conclusion of every job (removing mount points or drive letters), and also unmaps it from the host altogether. This option will require the host to perform a scan for SCSI LUNs at the start of the next job, as the re-mapped staging disks must be rediscovered before they can be remounted.</li> </ul>

Advanced Setting	Description
<b>Backup Only Boot Volume</b>	<p>Specify whether to back up only the boot volume of the VM or all the volumes of the VM:</p> <ul style="list-style-type: none"> <li>• <b>Back up all the volumes of VM</b></li> <li>• <b>Backup only boot volume of the VM</b></li> </ul> <p><b>Note:</b> If the boot volume is not the first drive on the bus, or if application binaries are spread over multiple VMware VMDKs, the entire boot volume may not be captured.</p>
<b>Truncate/Purge Log After Backup</b>	<p>Specify whether to truncate the logs after every backup. When <b>Truncate/Purge Log After Backup</b> is enabled, application-related logs are truncated until the recent or current backup. If you truncate logs, you must also back up the transaction log to enable a roll forward recovery. (SQL Server, Exchange, SharePoint). Options are:</p> <ul style="list-style-type: none"> <li>• <b>Do not truncate/purge log after backup</b></li> <li>• <b>Truncate/purge log after backup</b></li> </ul>
<b>Skip offline applications in consistency group</b> (not Oracle)	<p>Select how to handle offline applications in a consistency group:</p> <ul style="list-style-type: none"> <li>• <b>Skip offline applications during backup:</b> Offline applications in a consistency group will be skipped and the backup will not fail.</li> <li>• <b>Fail backup when offline applications are found</b></li> </ul>
<b>Map staging disks to all nodes in an application cluster</b>	<p>If your nodes are in an application cluster, you can use this to ensure that the nodes of an application cluster are protected in case of failover during backup.</p> <ul style="list-style-type: none"> <li>• <b>Do not map staging disk to all nodes of application cluster</b></li> <li>• <b>Map staging disk to all nodes of application cluster:</b> In the event of an application cluster failure, this option will protect failover copies.</li> </ul>
<b>Map staging disk to all ESX hosts in a cluster</b> (VMware VMs only)	<p>If your ESX servers are in a cluster, you can use this to ensure that the VMs are protected in case of failover during backup. (Oracle, local filesystems, CIFS, NFS, SharePoint, SQL Server, Exchange):</p> <ul style="list-style-type: none"> <li>• <b>Do not map staging disk to all ESX hosts</b></li> <li>• <b>Map staging disk to all ESX hosts:</b> In the event of an ESX host failure, this option will protect failover copies of VMware VMs.</li> </ul>
<b>Force Out of Band Backup</b>	<p>Specify if you want to force In-Band backups to an Out-of-Band mode. Options are <b>Yes</b> or <b>No</b>.</p>
<b>Job Behavior When Target VM Needs Snapshot Consolidation</b>	<p>Select an action if the VM requires consolidation:</p> <ul style="list-style-type: none"> <li>• <b>Fail the job:</b> backup/DAR/direct-dedup jobs fail.</li> <li>• <b>Run the job without performing consolidation:</b> All jobs run normally even if consolidation is pending.</li> <li>• <b>Perform consolidation at the beginning of the job:</b> Backup/direct-dedup/DAR jobs try to perform consolidation at the beginning of the job. If consolidation fails, the job fails with an error message.</li> </ul>

Advanced Setting	Description
<b>Fail On Missing Start Path</b>	If one or more start paths are specified, and any of these start paths does not exist, the job will fail with the message <b>UDSAgent: Specified start path does not exist</b> . If no start paths are specified, this option has no effect. Options are <b>Yes</b> or <b>No</b> . The default is <b>No</b> .

10. Prior to saving your policy, if you would like to first confirm if the policy settings will consume system resources and possibly result in system performance issues, click **Project Changes**. The Projected Resources Summary screen appears. See [Validating Projected Resources for a Policy](#) on page 39 for details.
11. Click **Save**. If there are issues with the policy settings a warning message appears. You can adjust the policy (click **Cancel**) or click **Continue** to accept the policy. See [Resolving Warnings](#) on page 41 for details.

## Creating a Dedup Backup to Dedup DR Policy

**Note:** Before creating a policy to store a deduplicated image at a remote site, you must first either create a dedup policy (see [Creating a Snapshot to Dedup Backup Policy](#) on page 60) or a Production to Direct-to-Dedup policy (see [Creating a Production Direct-to-Dedup Policy](#) on page 63).

Dedup Backup to Dedup DR policies are used to replicate deduplicated data to another Actifio appliance. This type of policy is efficient for the long-term storage of captured and deduplicated data to a remote Actifio appliance. Remote dedup is intended to retain data for a medium to long-term retention period (for example, 3 years or longer).

A Dedup Backup to Dedup DR Policy is used in tandem with a resource profile that defines the replication destination as another Actifio appliance. You apply both the policy and the resource profile to applications in the Application Manager. For a set of best practices when developing a Dedup Backup to Dedup DR policy, see [Dedup Backup to Dedup DR Policy Policies](#) on page 25.

To create a Dedup Backup to Dedup DR policy:

1. Open the SLA Architect and select a template that includes a Snapshot policy and dedup policy.
2. Click the arrow between **Dedup Backup** and **Dedup DR**. The policy window appears.
3. Click the **+**(plus) icon. The policy settings are displayed.



### Creating a Policy for Replicating Deduplicated Images (Windowed)

4. Enter a policy name in **Policy Name**.
5. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

6. Specify the schedule type for the Dedup Backup to Dedup DR policy: Windowed or Continuous. The default is Windowed.
  - o **Windowed** - Defines a discrete remote dedup image capture schedule adhering to a specific frequency and time window (for example, perform a capture every 30 minutes, daily from 9 am to 5 pm). You can instruct the Actifio appliance to run multiple capture jobs at a specified frequency interval or once during a specified time window.
  - o **Continuous** - Defines a continuous remote dedup image capture schedule (for example, perform a capture job every 8 hours, starting the first job at 1 am). In this policy schedule, jobs run continuously (24/7) at the specified time interval.
7. Configure the policy frequency settings per the selected schedule type as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency of the policy by defining an interval at which remote dedup images are captured. Based on this interval setting, the job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Defines an exception to the Run schedule. You can specify an Except value of daily, weekly, monthly, or yearly. For example, to skip the daily remote dedup schedule every Friday, select weekly and select Friday.  Click the link to the right of this parameter and modify the exception. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing remote dedup images.
Once Per Window	Specifies that the frequency duration for capturing remote dedup images is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing remote dedup images during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the remote dedup image capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of remote dedup image captures.
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the remote dedup image. Example: retain the image for 14 days.

8. Prior to saving your policy, if you would like to first confirm if the policy settings will consume system resources and possibly result in system performance issues, click **Project Changes**. The Projected Resources Summary screen appears. See [Validating Projected Resources for a Policy](#) on page 39 for details.
9. Click **Save**. If there are issues with the policy settings a warning message appears. You can adjust the policy (click **Cancel**) or click **Continue** to accept the policy. See [Resolving Warnings](#) on page 41 for details.

## Creating a Multi-hop Remote Dedup Backup Replication Policy

To create a policy for the second hop of a multi-hop configuration (remote Actifio appliance 1):

---

**Note:** For the primary Actifio appliance, be sure to create a Dedup Backup policy that forwards the dedup backup image to remote Actifio appliance 1. This policy operates as a single hop replication to remote Actifio appliance 1. See [Creating a Dedup Backup to Dedup DR Policy](#) on page 68.

For background details on developing a multi-hop policy, see [Dedup DR to Remote Replication Policies \(Multi-hop Replication\)](#) on page 26.

---

1. Open the SLA Architect.
2. Click **New Template...** from the service menu.
3. For remote Actifio appliance 1, click the arrow between **Dedup Backup** and **Dedup DR** from the template to define the Second Hop Replication policy between remote appliance 1 and remote appliance 2.

---

**Note:** When you select a Second Hop Replication policy, the other arrows in the SLA Architect are disabled.

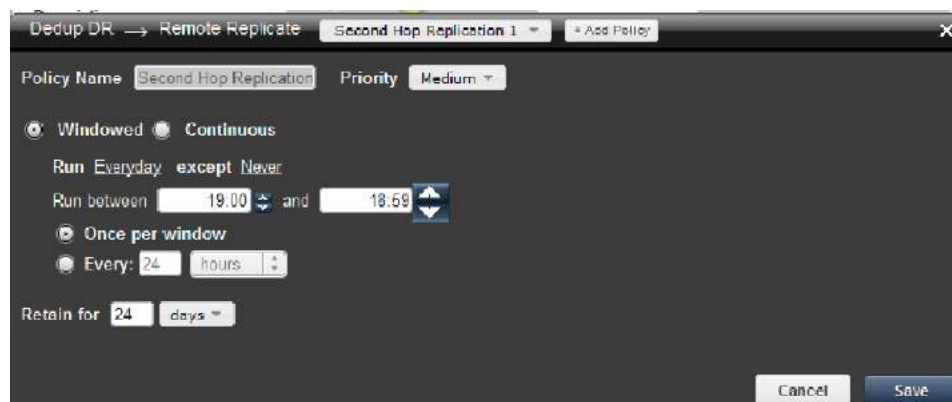
---

4. A Confirm warning message instructs you that this template is intended only for the second hop of the multi-hop configuration. Click **Continue** to confirm that you want to use this template as the Second Hop Replication policy. The policy window appears.
5. Click the **+**(plus) icon. The policy settings are displayed.

---

**Note:** The Second Hop Replication policy can use a set of policy settings that are different from the first hop replication policy (the Dedup Backup and Dedup DR policy).

---



### Creating a Policy for Multi-hop Replication (Windowed)

6. Enter a policy name in **Policy Name**.
7. If desired, change the application priority from the Priority drop-down list. The default job priority is Medium, but you can change the priority to High or Low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will only run when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

8. Specify the schedule type for the Second Hop Replication policy: Windowed or Continuous. The default is Windowed.
  - o **Windowed** - Defines a discrete image capture schedule adhering to a specific frequency and time window (for example, perform a capture every 30 minutes, daily from 9 am to 5 pm). You can instruct the Actifio appliance to run multiple capture jobs at a specified frequency interval or once during a specified time window.
  - o **Continuous** - Defines a continuous image capture schedule (for example, perform a capture job every 8 hours, starting the first job at 1 am). In this policy schedule, jobs run continuously (24/7) at the specified time interval.
9. Configure the policy frequency settings per the selected schedule type as outlined in the table below.

Policy Setting	Description
<b>Windowed</b>	
Run	Configures the frequency of the policy by defining an interval at which Second Hop Replication images are captured. Based on this interval setting, the job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Except	Configures the frequency of the policy by defining an interval at which Second Hop Replication images are captured. Based on this interval setting, the job runs once every specified number of days, weeks, months, or years.  Click the link to the right of this parameter and modify the Run interval. The schedule is displayed in a calendar view (see <a href="#">Viewing Policy Schedules</a> on page 49).
Run Between	Defines a start and end time window for capturing Second Hop Replication images.
Once Per Window	Specifies that the frequency duration for capturing Second Hop Replication images is once during the specified Run Between time window.
Every	Specifies a repeat frequency duration (minutes or hours) for capturing Second Hop Replication images during the specified Run Between time window. Example: every 2 hours.
<b>Continuous</b>	
Run Every	Specifies the time period in which to repeat the Second Hop Replication image capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of Second Hop Replication image captures.



Policy Setting	Description
<b>Both Windowed and Continuous</b>	
Retain For	Specifies the length of time that you intend to retain the Second Hop Replication image. Example: retain the image for 24 days.

10. Click **Save** to save the policy changes.

---

**Note:** You can use the **Add Policy** button to create another policy for second-hop replication.

---

## Creating a Production to Mirror Policy

Production to Mirror policies are used to replicate snapshots of your production data to the Mirror (Snapshot Pool) of a second Actifio appliance. These policy types 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 the remote site by accessing data from the remote DR copy.

A Production to Mirror Policy is used in tandem with a resource profile that defines the replication destination as another Actifio appliance. Both the Production to Mirror Policy and the resource profile are applied to applications in the Application Manager.

When creating a Production to Mirror Policy you have the following choices for replicating data:

- **Dedup-Async Replication (DAR)** - Uses dedup processing for bandwidth efficient replication. See [Creating a Dedup-Async Replication \(DAR\) Production to Mirror Policy](#) on page 75.
- **StreamSnap Replication** - Replicates a point-in-time snapshot of the original application without deduplication. See [Creating a StreamSnap Production to Mirror Replication Policy](#) on page 79.
- **Synchronous (Sync) and Asynchronous (Async) Replication** - For use only with generic applications on Actifio CDS appliances only. See [Creating a Synchronous or Asynchronous Production to Mirror Replication Policy](#) on page 80.

---

**Note:** Policies are applied to applications and VMs in the Application Manager. When applying a policy that uses either Sync or Async replication, you must, in the Application Manager's Replication tab, select an MDisk, VDisk, or an MDiskgroup to replicate to at the target replication site.

---

Details about the different types of replication methods can be found in ***Replicating Data Using Actifio Appliances*** in your Actifio Documentation Library and on the Actifio Now customer portal.

For a set of best practices when developing a Production to Mirror policy, see [Production to Mirror Policies](#) on page 29.

## Creating a Dedup-Async Replication (DAR) Production to Mirror Policy

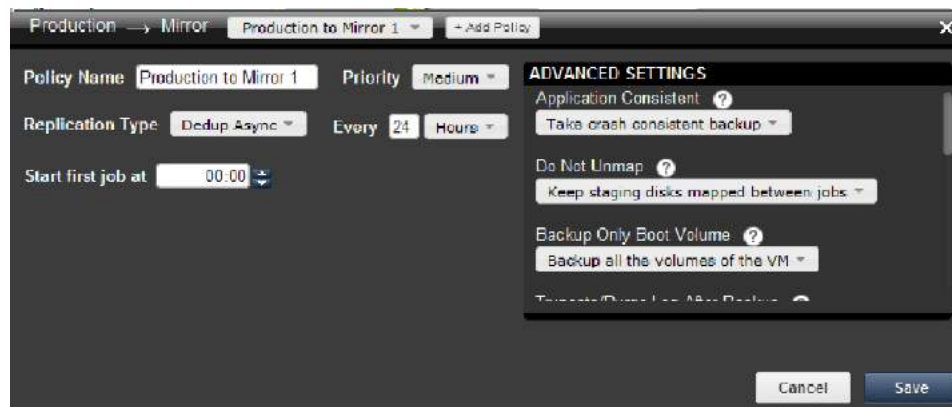
To create a Dedup-Async Production to Mirror replication policy:

---

**Note:** It is a good practice to include a Snapshot policy as part of the DAR template to ensure recoverability at the local Actifio appliance side for local data management (see [Creating a Production to Snapshot Policy](#) on page 52). Snapshot and dedup-async replication share staging disks. In this case, the Snapshot policy is run before the DAR policy takes effect.

---

1. Open the SLA Architect.
2. Click **New Template...** from the service menu. A new template is displayed.
3. Click the arrow between **Production** and **Remote Mirror**.
4. Click the **+**(plus) icon. The policy settings are displayed.
5. Select **Dedup Async** from the Replication Type drop-down list.



### Creating a Dedup-Async Production to Mirror Replication Policy

6. Enter a policy name in **Policy Name**.
7. If desired, change the application priority from the Priority drop-down list. The default job priority is medium, but you can change the priority to high or low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

**Note:** You can modify the priority of a Dedup-Async replication when a job based on the policy template is running.

8. Configure the policy frequency schedule as outlined in the table below.

---

**Note:** A Dedup-Async Production to Mirror replication policy supports only a windowed schedule.

---

Policy Setting	Description
Every	Specifies the time period in which to repeat the Dedup-Async image capture.
Start First Job At	Specific the time of day at which to run the first job in the continuous cycle of Dedup-Async image captures.

9. Configure the following **Advanced Settings** for the Dedup-Async Production to Mirror replication policy:

---

**Note:** Advanced Settings defined in a policy can be overridden by the Application Advanced Settings in the Application Manager, provided the policy's template has been set to allow overrides (see [Creating and Modifying a Policy Template](#) on page 44).

---

Advanced Setting	Description
<b>Application Consistent</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Take crash consistent backup:</b> Crash-consistent backup is a fast backup of application data in storage as if power were lost at that moment. It does not pause application data I/O. All data on disk are saved, and data in memory is lost. Incomplete transactions may be saved. The recovery of a crash consistent backup may take longer time and introduce exceptions. Typically recovery from crash must be made manually. Crash consistent backups are easy and fast for virtual machines.</li><li>• <b>Take application consistent backup:</b> Application-consistent backup notifies the application to prepare for a backup. This option loses no data. It pauses application data I/O, completes in-flight transactions, and flushes memory to disk. On recovery, data is easily accessible. For virtual clients, usually an agent is needed to get notification of a backup at host, and then notify applications, and may need to wait for an approval from applications. Not all applications support application-consistent backups.</li><li>• <b>Take crash consistent backup on last try:</b> This protection option initially takes application consistent backups, but if an application consistent backup fails for any reason, it will then take a crash consistent backup.</li></ul> <hr/> <p><b>Note:</b> Oracle and SQL databases, Hyper-V VMs with Microsoft Hyper-V Integration Services enabled, and Microsoft Exchange, SharePoint, and file systems protected out-of-band are always application consistent.</p> <hr/>

Advanced Setting	Description
<b>Do Not Unmap</b>	<p>Select either:</p> <ul style="list-style-type: none"> <li> <b>Keep staging disks mapped between jobs:</b> Select this if you want the temporary staging disks mapped to the host and used during data movement to remain mapped to the host. LUNs are mapped during the first job and subsequent jobs reuse the same mapped LUN. By default, this is selected.  <i><b>Note:</b> For applications protected using the Actifio Connector (such as SQL or Exchange databases) where the application is on an OS running inside a VMware VM, this option is ignored. The staging disk will always be unmapped from the VM after every job.</i> </li> <li> <b>Unmap staging disks after each job:</b> This option both unmounts the staging disk from the operating system at the conclusion of every job (removing mount points or drive letters), and also unmaps it from the host altogether. This option will require the host to perform a scan for SCSI LUNs at the start of the next job, as the re-mapped staging disks must be rediscovered before they can be remounted. </li> </ul>
<b>Backup Only Boot Volume</b> (VMs only)	<p>Specify whether to back up only the boot volume of the VM or all volumes of the VM:</p> <ul style="list-style-type: none"> <li><b>Back up all the volumes of VM</b></li> <li><b>Backup only boot volumes of the VM</b></li> </ul> <p><i><b>Note:</b> If the boot volume is not the first drive on the bus or if application binaries are spread over multiple VMware VMDKs, the entire boot volume may not be captured.</i></p>
<b>Truncate/ Purge Log After Backup</b>	<p>Specify whether to truncate the logs after every backup. When <b>Truncate/Purge Log After Backup</b> is enabled, application-related logs are truncated until the recent or current backup. If you truncate logs, you must also back up the transaction log to enable a roll forward recovery. (SQL Server, Exchange, SharePoint).</p> <p>Options are:</p> <ul style="list-style-type: none"> <li><b>Do not truncate/purge log after backup</b></li> <li><b>Truncate/purge log after backup</b></li> </ul>
<b>Skip offline applications in consistency group</b> (Not Oracle)	<p>Select how to handle offline applications in a consistency group:</p> <ul style="list-style-type: none"> <li><b>Skip offline applications during backup:</b> Offline applications in a consistency group will be skipped and the backup will not fail.</li> <li><b>Fail backup when offline applications are found</b></li> </ul>
<b>Map staging disks to all nodes in an application cluster</b>	<p>If your nodes are in an application cluster, you can use this to ensure that the nodes of an application cluster are protected in case of failover during backup.</p> <ul style="list-style-type: none"> <li><b>Do not map staging disk to all nodes of application cluster</b></li> <li><b>Map staging disk to all nodes of application cluster:</b> In the event of an application cluster failure, this option will protect failover copies.</li> </ul>

Advanced Setting	Description
<b>Map staging disk to all ESX hosts in a cluster</b> (VMware VMs only)	<p>If your ESX servers are in a cluster, you can use this setting to ensure that the VMs are protected in case of failover during backup. (Oracle, local filesystems, CIFS, NFS, SharePoint, SQL Server, Exchange):</p> <ul style="list-style-type: none"> <li>• <b>Do not map staging disk to all ESX hosts</b></li> <li>• <b>Map staging disk to all ESX hosts:</b> In the event of an ESX host failure, this option will protect failover copies of VMware VMs.</li> </ul>
<b>Force Out of Band Backup</b>	Specify if you want to force In-Band backups to an Out-of-Band mode. Options are <b>Yes</b> or <b>No</b> .
<b>Job Behavior When Target VM Needs Snapshot Consolidation</b>	<p>Select an action if the VM requires consolidation:</p> <ul style="list-style-type: none"> <li>• <b>Fail the job if VM needs consolidation:</b> Backup/DAR/direct-dedup jobs fail.</li> <li>• <b>Run the job without performing consolidation:</b> All jobs run normally even if consolidation is pending.</li> <li>• <b>Perform consolidation at the beginning of the job:</b> Backup/direct-dedup/DAR jobs try to perform consolidation at the beginning of the job. If consolidation fails, the job fails with an error message.</li> </ul>
<b>Fail On Missing Start Path</b>	If one or more start paths are specified, and any of these start paths does not exist, the job will fail with the message UDSAgent: Specified start path does not exist. If no start paths are specified, this option has no effect. Options are <b>Yes</b> or <b>No</b> . The default is <b>No</b> .

10. Click **Save** to save the policy changes.

## Creating a StreamSnap Production to Mirror Replication Policy

To create a StreamSnap Production to Mirror replication policy:

---

**Note:** Before creating a StreamSnap replication policy, you **must** first create a Snapshot policy as described in [Creating a Production to Snapshot Policy](#) on page 52. Production to Mirror policies that use the StreamSnap replication option are tied to a specific Production to Snapshot policy. They inherit the schedule and frequency settings, as well as the advanced settings, of the associated Production to Snapshot policy. You will be prevented from saving the StreamSnap replication policy without an associated base Snapshot policy.

---

1. Open the SLA Architect and select a template that includes a Snapshot policy.
2. Click the arrow between **Production** and **Remote Mirror**.
3. Click the **+**(plus) icon. The policy settings are displayed.
4. Select **StreamSnap** from the Replication Type drop-down list.



### Creating a StreamSnap Production to Mirror Replication Policy

5. Enter a policy name in **Policy Name**.
6. If desired, change the application priority from the Priority drop-down list. The default job priority for StreamSnap replication is medium, but you can change the priority to high or low.

The SLA scheduler identifies when one or more policies applied to applications are to run, and then initiates a job that places the policy into a queue when the scheduled start time occurs. For each policy type there is a pacing mechanism to ensure that the system is not overwhelmed with running jobs. This pacing mechanism uses job slots to achieve this steady state, which means that even if a job is supposed to start at a particular time it will execute only occur when a job slot is available.

If multiple applications are scheduled to run at the same time with the same job priority, the selection of the application to run is randomized to ensure fairness across all of the applications of the same priority. Job priority is explained in [Job Priority and Scheduling](#) on page 14.

**Note:** You can modify the priority of a StreamSnap replication when a job based on the policy template is running.

7. **Base Snapshot Type** identifies a previously created Snapshot policy in the template for use as the base Snapshot policy for StreamSnap replication. StreamSnap replication policy is always tied to a specific Snapshot policy, and uses the schedule and frequency settings of this Snapshot policy. If more than one Snapshot policy exists in the template, select the Snapshot policy to use with the StreamSnap policy.

8. Under **Remote Retention** select the desired remote snapshot retention for the StreamSnap policy by choosing:
  - o **Only Keep the Most Recent Remote Image**—Instructs the Actifio appliance to retain only the latest remote StreamSnap image (default setting).
  - o **Use Retention Specified in Snapshot Policy**—Instructs the Actifio appliance to use the same retention as the local (base) Snapshot policy associated with this StreamSnap policy.
  - o **Retain For**—Instructs the Actifio appliance to retain the remote snapshot image for a specific period of time (minutes, hours, days, weeks, months, or years). You define the time period to retain the image by making a choice from the drop-down list and then entering a specific value.

Actifio appliances will retain multiple point-in-time images at the remote site, with retention behavior being driven by this setting. 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 of the same operations available with a local snapshot image.

9. By default, compression for StreamSnap replication is enabled in the **Advanced Settings** section. Compression increases efficiency of the StreamSnap replication to the remote Actifio appliance when transferring data over the network. When compression is enabled, all packets are compressed. The target Actifio appliance decompresses the packets before writing to the staging disk.

If compression is not desired for StreamSnap replication to the second Actifio appliance (for example, when replicating images and videos), change the Compress StreamSnap Replication advanced setting to **Do not compress**.

---

**Note:** Enabling compression may not always provide the best results. Compression uses additional CPU cycles but reduces network bandwidth consumption. If the available network bandwidth is better than the system resources such as CPUs, it is advised to disable compression.

---

10. Click **Save** to save the policy changes.

## Creating a Synchronous or Asynchronous Production to Mirror Replication Policy

To create a Synchronous (Sync) or Asynchronous (Async) Production to Mirror replication policy:

1. Open the SLA Architect.
2. Click **New Template...** from the service menu. A new template is displayed.
3. Click the arrow between **Production** and **Remote Mirror**.
4. Click the **+**(plus) icon. The policy settings are displayed.



**Creating a Sync or Async Production to Mirror Replication Policy**



5. Enter a policy name in **Policy Name**.
6. From the drop down list select the replication type: Sync (Synchronous) or Async (Asynchronous).
7. Configure the policy frequency settings in the **Every** selection (for example: every 2 hours).
8. For Priority, the priority is Medium and cannot be changed for synchronous and asynchronous replication.

---

**Note:** Job priority is explained in [Job Priority and Scheduling](#) on page 14.

---

9. Click **Save** to save the policy changes.



# 6 Creating and Managing Resource Profiles

---

Resource profiles are created in the SLA Architect and applied to applications in the Application Manager.

A resource profile is applied to an application along with a policy template. The policy template specifies how data is captured. The resource profile specifies where to store captured data.

A policy template that specifies data replication must be used with a resource profile that specifies where to store data locally as well as where to replicate data. A policy template that does not specify data replication must be used with a resource profile that specifies where to store data locally.

---

**Note:** Details about the different types of replication methods can be found in **Replicating Data Using Actifio Appliances** in your Actifio Documentation Library and on the Actifio Now customer portal.

---

This chapter details:

[Creating a Resource Profile](#) on page 84

[Creating a Resource Profile for a Multi-hop Configuration](#) on page 85

[Cloning a Resource Profile](#) on page 86

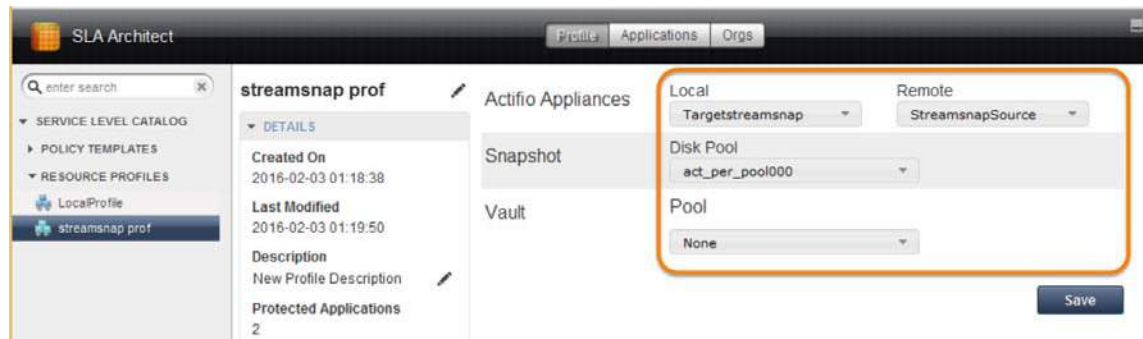
[Viewing Resource Profiles](#) on page 87

[Deleting a Resource Profile](#) on page 88

## Creating a Resource Profile

To create a resource profile:

1. Open the SLA Architect.
2. Click **New Profile...** from the Service menu.
3. Click the profile name to give it a new, descriptive name, and click **OK**.
4. Select the local Actifio appliance from **Local** drop-down list. This is the Actifio appliance that the profile is created on.
5. From the Remote drop down menu select either:
  - o A remote Actifio appliance to which data will be replicated. You can select this option only if the Actifio appliance is joined with another Actifio appliance.
  - o An Actifio OnVault Pool to which data will be sent (such as Amazon S3 Storage, Amazon S3 Compatible Storage, Google Nearline Storage, IBM Cloud Object Storage, or Microsoft Azure Storage). You can select this option only if this Actifio appliance has defined a OnVault Storage Pool. See **Configuring Resources and Settings With the Domain Manager** for details.
  - o **None** if data will not be replicated.
6. Select the disk pool (where you want to preserve the local snapshots) from **Disk Pool**. Click **Save**.



### Creating a Resource Profile (Shown for Replication to a Remote Actifio Appliance)



### Creating a Resource Profile (Shown for Storage to an Actifio OnVault Pool)

## Creating a Resource Profile for a Multi-hop Configuration

To create a resource profile for Actifio appliances operating in a multi-hop replication configuration (primary Actifio appliance and remote Actifio appliances 1 and 2):

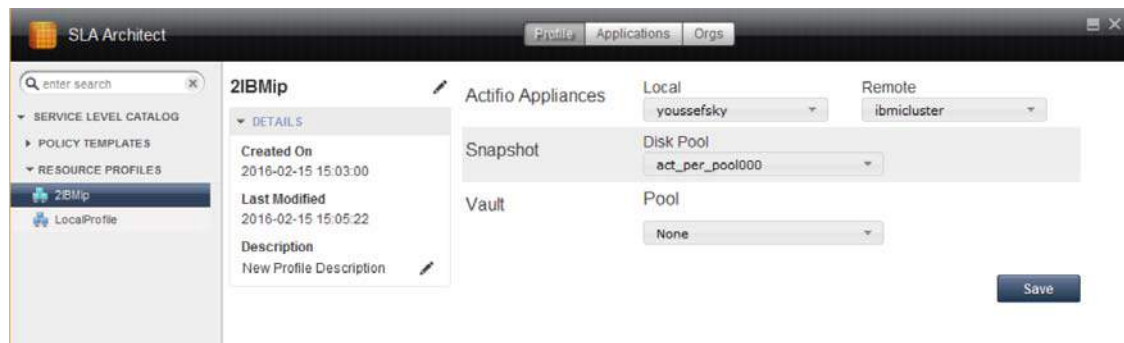
---

**Note:** See [Creating a Multi-hop Remote Dedup Backup Replication Policy](#) on page 71 for details on defining a *Second Hop Replication policy*.

---

1. Open the SLA Architect.
2. Click **New Profile...** from the Service menu.
3. Click the profile name to give it a new, descriptive name, and click **OK**.
4. Select the local Actifio appliance from **Local** drop-down list. This is the Actifio appliance that the profile is created on.
5. Select a remote Actifio appliance from **Remote** drop-down list. This appliance is used for remote deduplication/ replication. You can configure this field only when one or more remote Actifio appliances are configured. Makes the following selections as follows:

For	To Go	Specify as destination
Primary Actifio appliance	The first-hop	Remote Actifio appliance 1
Remote Actifio appliance 1	The second-hop	Remote Actifio appliance 2



### Creating a Multi-Hop Resource Profile

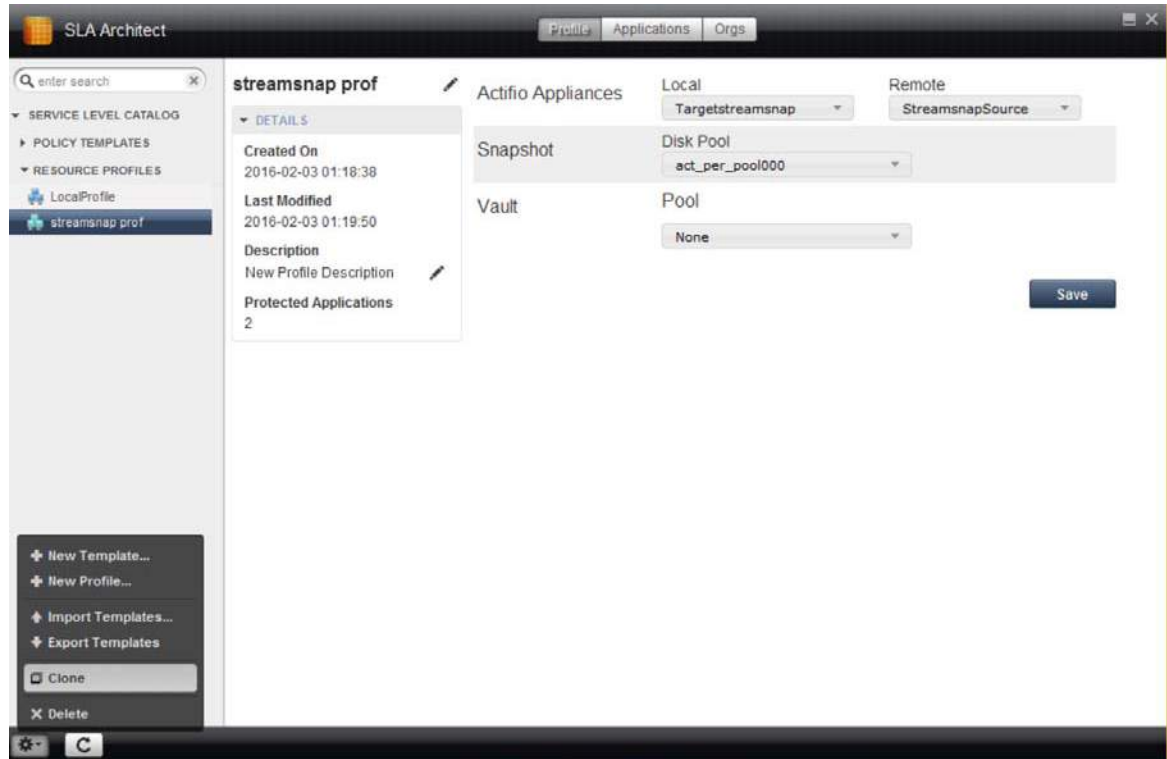
6. Select the disk pool (where you want to preserve the snapshots) from **Disk Pool**. The disk-pool drop-down displays all performance pools created during and after the Actifio appliance installation. Optionally, you can select **None** to configure a profile without a snapshot pool for the second-hop in the multi-hop replication configuration (remote Actifio appliance 1).
7. Click **Save**.

## Cloning a Resource Profile

Cloning lets you configure new resource profiles from the existing resource profiles.

To clone a resource profile:

1. Open the SLA Architect.
2. Select the resource profile you would like to clone from the navigation pane.
3. Either right-click the profile name or go to the service menu and select **Clone**.



### Cloning a Resource Profile

## Viewing Resource Profiles

To view the resource profiles:

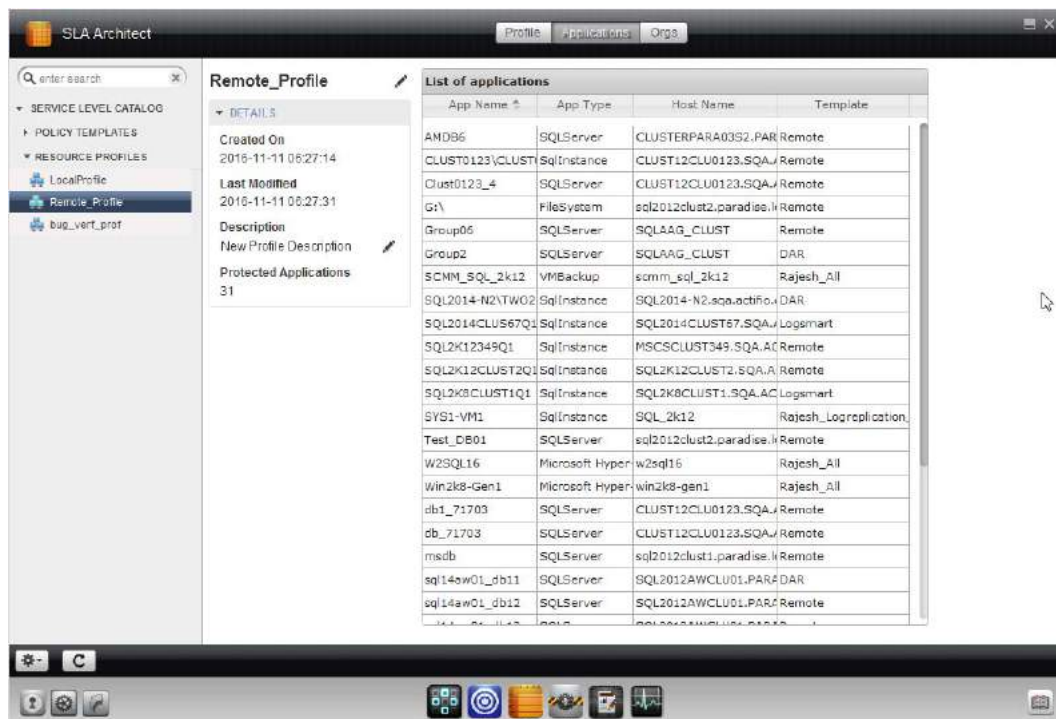
1. Open the SLA Architect.
2. Click **Resource Profiles** from the navigation pane. A list of resource profiles is displayed.

## Viewing Protected Applications on a Resource Profile

To view a list of protected applications:

1. Open the **SLA Architect**.
2. Select **Resource Profiles** from the navigation pane.
3. Select a resource profile from the navigation pane.
4. From the service menu, select **Applications**. A list of applications to be protected using the resource profile is displayed.

The cloned resource profile appears in the navigation pane with a modified name.



## Viewing Protected Applications

## Deleting a Resource Profile

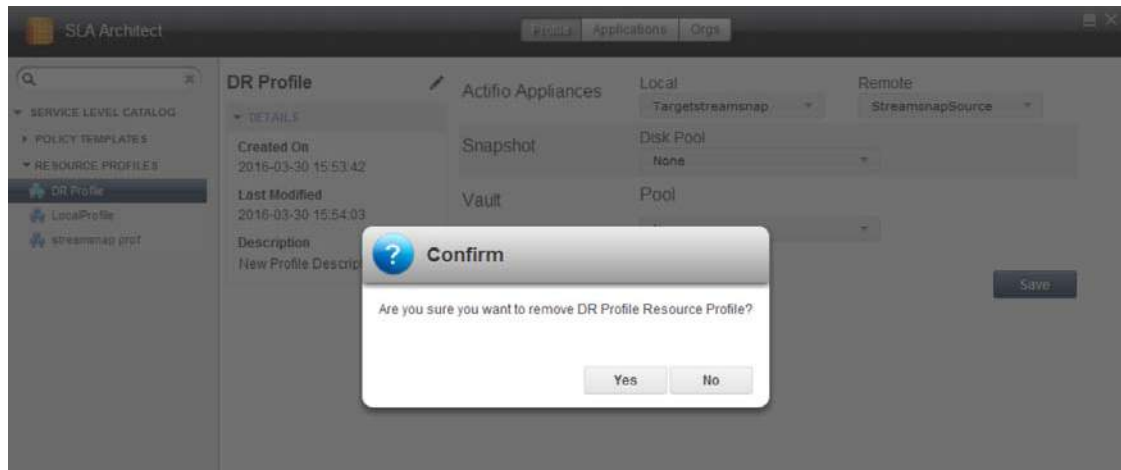
---

**Note:** Before deleting a profile, ensure that none of the protected applications are using the profile.

---

To delete a resource profile:

1. Open the SLA Architect to the Profile tab.
2. Click **Resource Profiles**.
3. Select the resource profile you would like to delete from the navigation pane.
4. Either right-click on the profile or from the service menu, select **Delete**. A confirmation dialog appears.
5. Click **Yes** in the confirmation dialog. The resource profile is deleted.



**Deleting a Resource Profile**



# Index

## A

Actifio OnVault 28

## B

best practices

- policy templates 9

- system resource considerations 37

## C

clone

- policy template 47

- resource profile 86

contact information, Actifio Support ii

copyright ii

## D

database log file snapshot policies 22

deduplication policy, creating 60

delete

- resource profile 88

- template 48

direct-to-dedup policy, creating 63

## E

export all policy templates 47

## I

import a policy template 47

## J

jobs

- priority 14

- retries 14

- StreamSnap jobs and error handling 31

## L

legal matter ii

## M

multi-hop remote dedup backup replication

- creating policy 71

- overview 26

- resource profile guidelines 85

- use cases 26

## P

policies

- database log file snapshot policies 22

- deduplication, creating 60

- development workflow 3, 43

- direct-to-dedup, creating 63

- impact on system performance 38

- multi-hop remote dedup backup replication, creating 71

- overview 2, 43, 51

- policy-specific best practices 18

- resolving warnings 41

- snapshot to OnVault, creating 58

- snapshots, creating 52

- steps to avoid consuming system resources 37

- storing de-duplicated images 68

- StreamSnap, creating 79

- validating projected resources for a policy 39

policy best practices

- dedup backup to dedup DR 25

- dedup DR to remote replication 26

- production to direct to dedup 24

- production to mirror - dedup-async replication (DAR) 29

- production to mirror - StreamSnap replication 30

- production to mirror - sync/async replication 32

- production to snapshot 19

- snapshot to dedup backup 23

- snapshot to OnVault 28

policy schedule

- continuous 11, 21

- windowed 11, 19, 20

policy template

- best practices 9

- cloning 47

- creating 44

- deleting 48

- exporting 47

- importing from other Actifio appliances 47

- modifying 44

- policy-specific best practices 18

- viewing 48
- projected resources, validating for a policy 39

## **R**

- resource profile
  - cloning 86
  - creating 84
  - creating for multi-hop configuration 85
  - deleting 88
  - viewing 87

## **S**

- Scheduler 14
- snapshot policy, creating 52
- snapshot to OnVault policy, creating 58
- storing deduped backup images remotely 68
- StreamSnap policy, creating 79
- system performance, impact of policy settings 38
- system resources, how to avoid consuming during policy development 37

## **T**

- Top 10 Templates (Domain Manager) 42
- trademarks ii

## **V**

- view
  - applications protected by a policy template 50
  - configured policy 48
  - organizations and policy relationships 50
  - policy schedules 49
  - resource profiles 87
  - Top 10 Templates in Domain Manager 42

## **W**

- warnings, resolving for a policy 41
- warranty ii