
Configuring Actifio OnVault in Google Cloud

Copyright, Trademarks, and other Legal Matter

Copyright © 2021 Google LLC. All rights reserved.

Actifio™, OnVault™, and VDP™ are trademarks of Google LLC.

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

Contents

Chapter 1 - Introduction	1
Types of Incremental Forever Data Capture to OnVault Pools	2
Preface	3
The ActifioNOW Customer Portal	3
Actifio Support Centers	3
Chapter 3 - Creating an OnVault Pool	5
Before You Begin	5
Creating an OnVault Pool.....	8
Add an OnVault pool	8
Update an OnVault Pool.....	10
Delete an OnVault Pool.....	10
Chapter 4 - Creating Resource Profiles	11
Chapter 5 - Creating OnVault Policies	13
AGM Snapshot to OnVault Policy	13
AGM Direct to OnVault Policy.....	15
Chapter 6 - Accessing and Importing Images	17
Accessing Data in OnVault.....	17
Importing OnVault Images.....	17
Importing Images From the AGM Domain Manager Storage Pool Page	18
Importing Images From the AGM App Manager Applications Page.....	19

1 Introduction

OnVault policies support Actifio's incremental forever data capture model, where the first time a policy runs, it captures an entire image, then subsequent data captures are only the changes to the image. This allows you to perform more frequent uploads (typically daily) to an object storage target.

Actifio OnVault with incremental forever data capture is a cost-effective solution that allows you to replace your off site vault infrastructure with on-demand object storage to store your daily, weekly, monthly, and yearly backup images. To review the types of data capture and storage, see [Types of Incremental Forever Data Capture to OnVault Pools](#) on page 2.

Storage Pools

Actifio Appliances retain data in:

- **Snapshot Pools** provide, local, short-term data retention i.e. a few days. Snapshot data ensures instant access to the latest production data. Snapshot pools also serve as a source for OnVault policies.
- **OnVault Pools** define access to object stores. Data can be accessed directly from the object store without first copying it back to a local storage device.

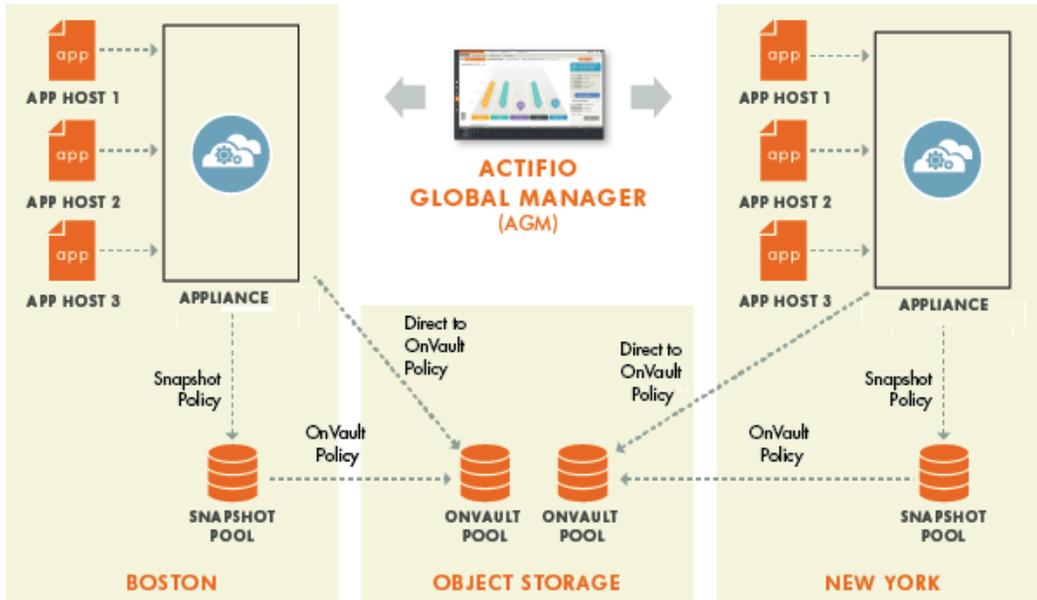
Import OnVault Images

AGM users can import OnVault images from one managed Actifio Appliance to another. An image that has been imported to another Actifio Appliance can be mounted to that appliance's application hosts. This is especially useful in a disaster scenario where the source Actifio Appliance is no longer available.

Ownership of an application's OnVault images can be taken by the Actifio Appliance to which it was imported. Actifio Appliances can only expire the OnVault images it owns. If a image is mistakenly imported, the AGM Forget option undoes the import operation. Importing OnVault images is detailed in [Chapter 6, Accessing and Importing Images](#).

Types of Incremental Forever Data Capture to OnVault Pools

Any data type captured in an Actifio Snapshot Pool can be written to an Actifio OnVault pool. In addition, VMware VMs can be captured directly from your production environment to an OnVault pool. For details on how to create the policies associated with these capture operations, see [Creating OnVault Policies](#) on page 13.



OnVault in a Multi-Appliance Environment - Managed by AGM

Note: Direct to OnVault supported for VMware VMs only.

Preface

Your Actifio Appliance's Documentation Library and AGM Online help contain detailed, step-by-step, application-specific instructions on how to protect and access your data.

Audience

The intended audience for this document has experience using object storage. Object storage vendors provide detailed conceptual information and step-by-step instructions on the use of their object storage product.

Actifio provides conceptual information and detailed step-by-step instructions that can be found in:

- The AGM Online Help
- The ActifioNOW customer portal

For an overview of basic concepts and procedures see ***Getting Started with Actifio Copy Data Management***.

The ActifioNOW Customer Portal

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

From the customer portal you can obtain detailed reports about your Actifio Appliance as well as search the portal's knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:

From anywhere: +1.315.261.7501

US Toll-Free: +1.855.392.6810

Australia: 0011 800-16165656

Germany: 00 800-16165656

New Zealand: 00 800-16165656

UK: 0 800-0155019

3 Creating an OnVault Pool

OnVault Pools are created from an Actifio Appliance. The AGM that manages that appliance can use the pool as the destination for a Resource Profile.

Use the same object storage for all OnVault Pools, with the same access credentials. This makes the import operation and disaster recovery operations seamless.

This chapter consists of two sections:

- [Before You Begin](#) on page 5
- [Creating an OnVault Pool](#) on page 8

Before You Begin

Be sure to:

- [Open Port 443](#)
- [Create a Service Account](#)
- [Set Private Google Access if Sky is in Google Cloud](#)
- [Add Google Storage Access Information to AGM](#)

Open Port 443

Be sure port 443 is open between the Actifio appliance and Google Cloud Storage, and that the appliance can resolve `storage.googleapis.com` and connect to `https://storage.googleapis.com`.

Create a Service Account

Before creating the OnVault pool, be sure you have created or identified a service account to use for access. This account will need either the Storage Admin Role or a custom role using these permissions:

- `storage.buckets.get`
- `storage.objects.create`
- `storage.objects.delete`
- `storage.objects.get`
- `storage.objects.list`

You will need to download a JSON key for this service account.

The screenshot shows the IAM & Admin console interface. On the left is a navigation menu with items like IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federati..., and Labels. The main content area displays details for a role named 'OnVault'. At the top right of this area are '+ EDIT ROLE' and 'CREATE FROM ROLE' buttons. Below these are two rows of key-value pairs: 'ID' with value 'projects/salins-lab/roles/onvault' and 'Role launch stage' with value 'General Availability'. A 'Description' section follows, stating 'Created on: 2021-04-28'. Below that is a section titled '5 assigned permissions' which lists: 'storage.buckets.get', 'storage.objects.create', 'storage.objects.delete', 'storage.objects.get', and 'storage.objects.list'.

Set Private Google Access if Sky is in Google Cloud

In addition, if Sky is running in Google Cloud, then the subnet that Sky is using must have **Private Google access** enabled in the subnet details.

The screenshot shows the 'Subnet details' page for a subnet named 'default'. The left sidebar lists various VPC network components like VPC networks, External IP addresses, Bring your own IP, Firewall, Routes, VPC network peering, Shared VPC, Serverless VPC access, and Packet mirroring. The main content area shows the following details for the 'default' subnet:

- VPC Network:** default
- Region:** us-west1
- IP address range:** 10.138.0.0/20. A warning message states: 'Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: 10.128.0.0/20, 25 MORE'. Below this is a text input field containing '10.138.0.0/20'.
- Secondary IP ranges:** A '+ ADD IP RANGE' button is visible.
- Gateway:** 10.138.0.1
- Private Google access:** This section is highlighted with a red box. It contains two radio buttons: 'On' (which is selected) and 'Off'.
- Flow logs:** Two radio buttons: 'On' and 'Off' (which is selected).

 At the bottom of the page are 'SAVE' and 'CANCEL' buttons.

Add Google Storage Access Information to AGM

OnVault Pools require access to your object storage. Before you can create an OnVault pool, you need basic access related information from your Google Nearline or Google Coldline Storage account.

Attribute	Required?	Description	Information Source
Pool Name	Required	A descriptive name for the OnVault pool	AGM
Pool Type	Required	Select: Cloud - Google Nearline Storage or Cloud - Google Coldline Storage	Actifio
Service Account ID	Required	The access ID for Object Store access	Google Cloud Console
Path to private key file in JSON format	Required	Upload a valid private key file.	AGM - File Upload OnVault Configuration Form
Bucket	Required	A name for the Object Store bucket	Customer
Compression	Optional	Specify if data in the OnVault pool should be stored compressed or uncompressed. Compressing reduces storage costs but requires additional compute capacity for Sky to compress the data before transmitting.	AGM
Proxy server (address:port)	Required if access to the Object Store needs a proxy server.	Enter both the address and port number.	Customer
Member of Organizations	Optional	Organizations and roles work together to enforce rules set up by AGM administrators for user access to AGM features.	AGM
Advanced Settings: Object size	Required	Values can be from 64 KB to 8 MB. The default value of 1MB is suitable in most cases. Changing object size can adversely affect the performance of the Sky appliance and the cost of object storage for OnVault.	AGM Note: Change this only under the guidance of Support.

Creating an OnVault Pool

Once you have gathered your object storage specific information, create an OnVault Pool.

OnVault pools are used to store backup data. They are referenced by Resource profiles. The Resource profile is used along with a production Snapshot to OnVault policy to send captured snapshot data to the assigned OnVault pool.

Before you begin

OnVault pools require access to the object storage. Before adding an OnVault pool, make sure you:

- Identify or create a storage bucket to hold the data:
 - All storage classes and locations are supported. Use an appropriate class for the data retention you will specify. Do not use archive tier without consulting with the sales or support organization first.
 - Versioning and retention must be disabled.
 - Access control should be set to "uniform" on any new bucket.
 - Google-managed encryption keys (GMEK) and customer-managed encryption keys (CMEK) are supported.
- Create or identify a service account with the required permissions (see below).
- Create a private key for the service account.
- Collect the service account id, private key, and bucket name to use during creation of the OnVault pool.

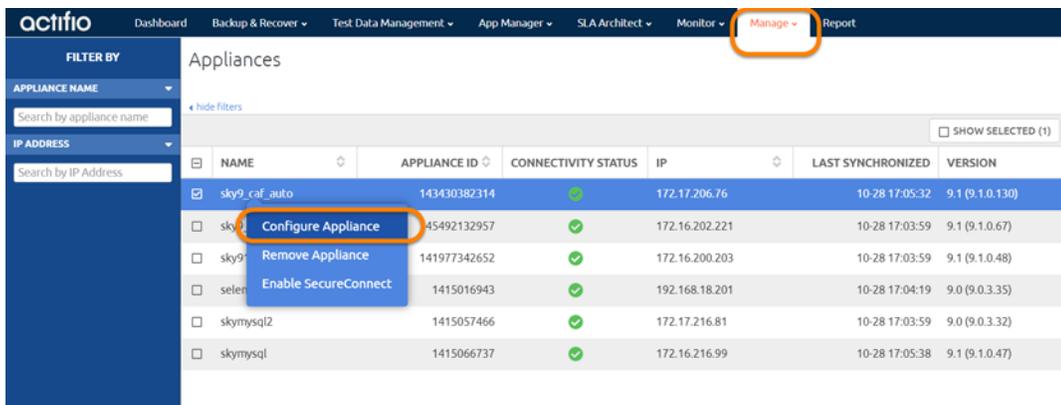
These are the permissions required on the service account used by an OnVault pool:

- storage.buckets.get
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list

Add an OnVault pool

To add an OnVault pool:

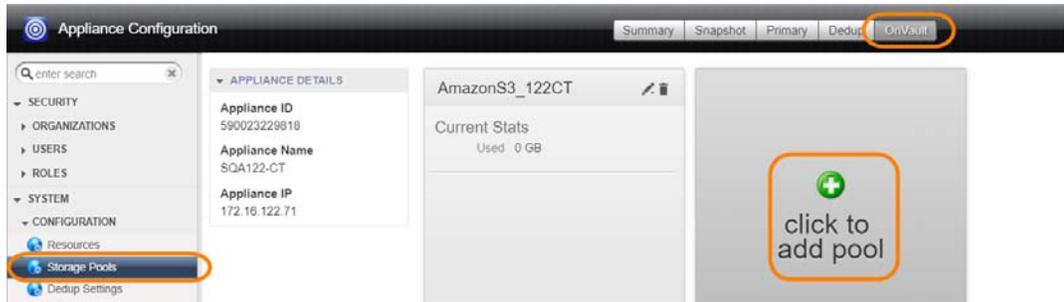
1. From the AGM Manage menu, select **Appliances**. Select the appliance that will have the OnVault Pool and click **Configure Appliance**.



The screenshot shows the Actifio AGM Manage interface. The top navigation bar includes 'Dashboard', 'Backup & Recover', 'Test Data Management', 'App Manager', 'SLA Architect', 'Monitor', 'Manage', and 'Report'. The 'Manage' menu item is highlighted with an orange box. Below the navigation bar, the 'Appliances' section is displayed. On the left, there are filter options for 'APPLIANCE NAME' and 'IP ADDRESS'. The main area shows a table of appliances with columns for NAME, APPLIANCE ID, CONNECTIVITY STATUS, IP, LAST SYNCHRONIZED, and VERSION. The second row is selected, and a context menu is open over it, showing 'Configure Appliance', 'Remove Appliance', and 'Enable SecureConnect'. The 'Configure Appliance' option is highlighted with an orange box.

	NAME	APPLIANCE ID	CONNECTIVITY STATUS	IP	LAST SYNCHRONIZED	VERSION
<input checked="" type="checkbox"/>	sky9_caf_auto	143430382314	●	172.17.206.76	10-28 17:05:32	9.1 (9.1.0.130)
<input checked="" type="checkbox"/>	sky9_caf	45492132957	●	172.16.202.221	10-28 17:03:59	9.1 (9.1.0.67)
<input type="checkbox"/>	sky9_caf_2	141977342652	●	172.16.200.203	10-28 17:03:59	9.1 (9.1.0.48)
<input type="checkbox"/>	selena	1415016943	●	192.168.18.201	10-28 17:04:19	9.0 (9.0.3.35)
<input type="checkbox"/>	skymysql2	1415057466	●	172.17.216.81	10-28 17:03:59	9.0 (9.0.3.32)
<input type="checkbox"/>	skymysql	1415066737	●	172.16.216.99	10-28 17:05:38	9.1 (9.1.0.47)

2. From Storage Pools, select the **OnVault** tab and then **click to add pool**. You may have to scroll down to see the Add Pool option.



3. Enter the **OnVault Pool Name**. Valid characters are letters, numbers, space, hyphen (-), and underscore(_).
4. Select the **Pool Type**. If you are specifying a bucket that was created to be used for this pool, but has no data in it yet, select the default (Google Cloud Storage). If connecting to a bucket that already has been used as an OnVault pool target, select the same type that was used by the first OnVault pool to use that bucket. This may be Google Coldline Storage or Google Nearline Storage, or the default Google Cloud Storage.

Note: The Google Cloud Storage pool type supports all storage tiers and should be used unless backward compatibility with a legacy OnVault pool is required.

5. Enter your **Service account**. It is the service account access ID, in email format, that will be used to access the object storage. For full details on service accounts, see <https://cloud.google.com/iam/docs/creating-managing-service-accounts>.
6. In the **Private Key File** field, paste the private key, or click **Choose file** to import a saved private key file.
7. In the **Bucket** field, enter the name of the object storage bucket that will hold your data. The bucket must already exist.
8. Specify if data in the OnVault pool should be stored in compressed or uncompressed format. Compressing data reduces storage costs but requires additional compute capacity for backup/recovery appliance to compress the data before transmitting. In most cases you will want to keep the compression checked. Compression also reduces network traffic.
9. Under Advanced Options:
 - a. Select the **Object size**. Values range from 64 KB to 8 MB. The default value of 1MB is suitable in most cases. Changing the object size can adversely affect the performance and the cost of object storage service used for OnVault.

Note: Do not change the object size from default unless advised to do so.

- b. If using a proxy, enter the proxy server's address and port number.
 - c. From appliance section, select one or more appliances where you want to add the pool.
 - d. Check the check boxes for the organizations that OnVault pool should be member of.
10. Click **Save**.

The OnVault Pool is created. Now it can be added to a Resource Profile as described in [Chapter 4, Creating Resource Profiles](#).

Update an OnVault Pool

You must upload the private key whenever you update the OnVault pool details.

To edit an OnVault pool:

1. Click the **Manage** tab and select **Storage Pools** from the drop-down menu.
2. Select the OnVault pool you wish to edit and click the **Edit** button on the bottom right corner of the page.
3. Edit the **OnVault Pool Name**, **Service Account**, and **Bucket** details as needed. Enable or disable **Compression** as needed.
4. Under Advanced Options, change the **Object size** and **Proxy Server**, as needed. Changing the object size can adversely affect the performance and the cost of object storage service used for OnVault.

Note: Do not change the object size from default unless advised to do so.

5. At the bottom of the page, edit **Organizations** as needed.
6. Paste or upload the **Private Key file** (required if changes have been made to any other field).
7. Click **Update**.

Note: If you change the Bucket Name, then the next backup jobs to this pool will be new full backups.

Delete an OnVault Pool

Deleting an OnVault pool from an appliance is only allowed if there are no backup images known to the appliance in the pool.

To delete an OnVault pool from a Sky appliance:

1. Click the **Manage** tab and select **Storage Pools** from the drop-down menu.
2. Right-click the desired OnVault pool and select **Delete**.
3. Click **Confirm**.

4 Creating Resource Profiles

Resource Profiles define which storage pools will be used to retain application data. Resource Profiles are created in the Service Level Architect (SLA) service. To create a Resource Profile:

1. From the SLA Architect select **Profiles** from the dropdown list.
2. Either select and edit existing an Resource Profile or click **Create Profile** to create a new profile. The Create New Profile page is displayed.

Note: If you select an existing Resource Profile, ALL applications on that appliance to which the profile is applied will be impacted by changes to the profile.

actifio Dashboard Backup & Recover Test Data Management App Manager SLA Architect Manage Report Monitor

Edit Profile

A resource profile defines the local and, optionally, remote appliances that manage data of an application, as well as the storage for snapshot and OnVault images. Select the primary (local) appliance for where the data images will reside and a remote appliance if applicable. Once saved, the primary appliance can not be changed within the current profile.

PROFILE* CDS139C2-to-CDS139C1 DESCRIPTION New Profile Description

Primary Appliance

APPLIANCE CDS139-C2

SNAPSHOT POOL* act_per_pool000

ONVAULT POOL 1 CDS81-Onvault

Remote Appliance

Cancel Save Profile

3. In the spaces provided, enter a name and description for the profile.
4. Select the Primary Appliance from the drop-down list. This is the appliance on which the profile was or will be created.
5. From the Snapshot Pool menu, select the Snapshot Pool that the OnVault Pool will use as source.
6. From the **OnVault Pool** drop down menu, select the OnVault Pool to which production data in the Snapshot Pool will be sent. You can select this option only if the selected Actifio Appliance has defined an OnVault Storage Pool.
7. If this Profile is in an SLA Template that contains policies to replicate data to another Actifio Appliance, then from the drop down list under Remote Appliance, select the Actifio Appliance to which data will be replicated. The remote Actifio Appliance selected is not used with OnVault.
8. Click **Save Profile**.

5 Creating OnVault Policies

An OnVault policy defines when data is captured, the frequency with which it will be captured, and how long it will be retained.

You can create two types of OnVault policies:

- Snapshot to OnVault policies capture data in a Snapshot Pool and further protect that data in an OnVault Pool. To create a Snapshot to OnVault policy, see [AGM Snapshot to OnVault Policy](#) on page 13.
- Direct to OnVault policies capture VMs in their production environment and protect them directly to an OnVault Pool. To create a Direct to OnVault policy, see [AGM Direct to OnVault Policy](#) on page 15.

An OnVault policy can be created in an existing SLA Template that has a Production to Snapshot policy, or created as part of a new SLA Template.

Note: If you add an OnVault Policy to an existing SLA Policy Template, **ALL applications** on this appliance to which the SLA Policy Template is applied will be impacted by the changes.

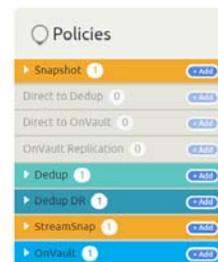
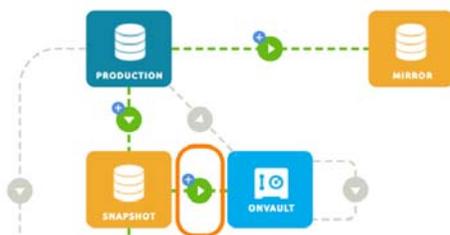
Note: Best practices for creating SLA Policy Templates and Policies can be found in the [AGM Online Help](#).

AGM Snapshot to OnVault Policy

SLA Policy Templates are defined in the SLA Architect service. Before you can create an OnVault policy, you must use an existing SLA Template that has a Production to Snapshot policy, or create a new SLA Template with a Production to Snapshot policy. Images captured by Production to Snapshot policies are used as the source for OnVault policies.

To create a Snapshot to OnVault Policy from AGM:

1. From an existing SLA Template or from a new SLA Template with a Production to Snapshot policy, click the plus sign + between Snapshot and OnVault.



The Snap to OnVault page is displayed:

The screenshot shows the Actifio web interface. At the top, there is a navigation bar with the Actifio logo and menu items: Dashboard, Backup & Recover, Test Data Management, App Manager, SLA Architect, Manage, Report, and Monitor. Below the navigation bar, the page title is 'Snapshot To OnVault'. On the left side, there is a 'Policies' sidebar with a search icon and a list of policy categories: Snapshot (1), Direct to Dedup (0), Direct to OnVault (0), OnVault Replication (0), Dedup (1), Dedup DR (1), StreamSnap (1), and OnVault (1). Each category has a '+ADD' button. The main content area is titled 'Create/Edit Policy' and contains the following fields and controls:

- POLICY NAME ***: A text input field.
- SCHEDULING**: A dropdown menu set to 'Windowed'.
- ON THESE DAYS**: A dropdown menu set to 'Everyday'.
- EXCEPT**: A dropdown menu set to 'Never' with a close icon (x).
- WITHIN THIS WINDOW**: Two time input fields set to '19:00' and '18:50'.
- RUN ONCE PER WINDOW**: A toggle switch that is turned on.
- EVERY**: A dropdown menu set to '24' with a 'Hour(s)' label.
- RETAIN FOR**: A numeric input field set to '14' with a 'Day(s)' label.
- SLA COMPLIANCE**: A dropdown menu set to 'Default'.
- PRIORITY**: A dropdown menu set to 'Medium'.
- TARGET POOL**: A dropdown menu set to 'OnVault Pool 1'.
- Advanced Policy Settings**: A button.
- Cancel** and **Update Policy**: Buttons at the bottom.

2. Set the policy according to your needs. For example, an OnVault policy could be defined as:
 - o Within a window
 - o Run **Everyday**, with **No Exceptions**
 - o Between **19:00 to 18:50**
 - o Once per window
 - o Retain for **3 Years**
3. Click **Update Policy** and the policy is created.

AGM Direct to OnVault Policy

Direct to OnVault policies are used to capture VMware VMs and can only be created in AGM. To create a Snapshot to OnVault Policy from AGM:

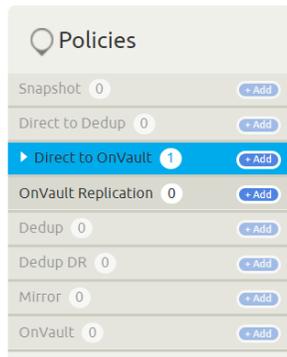
1. From an existing SLA Template or from a new SLA Template with NO Production to Snapshot policy and NO Production to Mirror policy, click the plus sign **+** between Production and OnVault.



2. The Direct to OnVault page is displayed.



Direct To OnVault

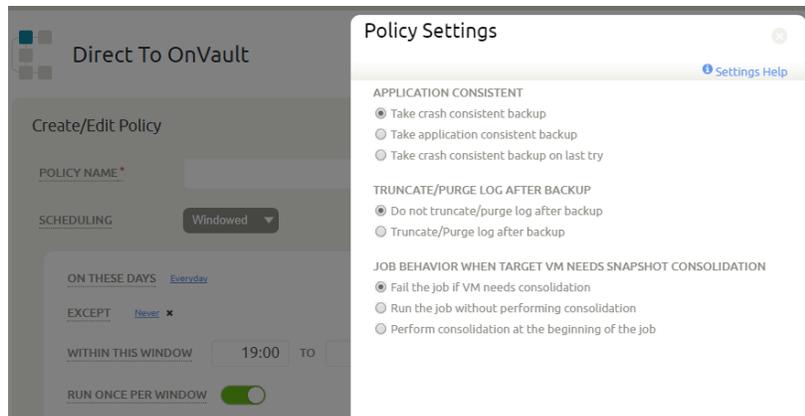


The 'Create/Edit Policy' configuration page includes the following fields and options:

- POLICY NAME***: A text input field.
- SCHEDULING**: A dropdown menu set to 'Windowed'.
- ON THESE DAYS**: A dropdown menu set to 'Everyday'.
- EXCEPT**: A dropdown menu set to 'Never'.
- WITHIN THIS WINDOW**: Two time input fields set to '19:00' and '18:50'.
- RUN ONCE PER WINDOW**: A toggle switch that is currently turned on.
- EVERY**: A numeric input field set to '24' with a 'Hour(s)' dropdown.
- RETAIN FOR**: A numeric input field set to '14' with a 'Day(s)' dropdown.
- SLA COMPLIANCE**: A dropdown menu set to 'Default'.
- PRIORITY**: A dropdown menu set to 'Medium'.
- TARGET POOL**: A dropdown menu set to 'OnVault Pool 1'.
- Advanced Policy Settings**: A button to expand more options.

Cancel Update Policy

3. Set the policy according to your needs. For example, an OnVault policy could be defined as:
 - o Within a window
 - o Run **Everyday**, with **No Exceptions**
 - o Between **19:00 to 18:50**
 - o Once per window
 - o Retain for **3 Years**
4. Click **Advanced Policy Settings** and the Policy Settings dialog box is displayed. This dialog box allows you to set VM specific advanced policy settings:



5. From the Policy settings dialog box select:

- **Application Consistent**

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

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

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

- **Truncate/Purge Log After Backup:** Select whether to truncate the logs after every backup. When this is selected, application-related logs are truncated up to the most recent backup.

- **Job Behavior When Target VM Needs Snapshot Consolidation**

Fail the job: Fails the job.

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

Perform consolidation at the beginning of the job: Backup jobs try to perform consolidation at the beginning of the job. If consolidation fails, the job fails.

6. Click **Save Changes** or **Cancel** and the dialog box closes.
7. Click **Update Policy** and the policy is created.

6 Accessing and Importing Images

Once you have a Resource Profile that uses an OnVault Pool and an SLA Policy Template that contains an OnVault Policy, you can, from the Application Manager, apply the Resource Profile and SLA Policy Template to applications and VMs. The OnVault policy will run according to its schedule and the captured image will be written to the OnVault Pool specified in the Resource Profile.

Accessing Data in OnVault

After the first capture operation has completed, data in an OnVault Pool's object storage location can be accessed, but:

Note: *Actifio VDP can create clones from OnVault data but it cannot create LiveClones from OnVault data.*

Note: *Data written to a mounted OnVault image is not persistent; it may be lost if the appliance is unexpectedly or 'uncleanly' shutdown. OnVault images should be mounted only for recoveries.*

For details on how to access data captured by AGM, see the AGM online help.

Importing OnVault Images

AGM supports the import of OnVault images between managed Actifio Appliances. Images cannot be imported from the Actifio Desktop.

When an image is imported to an Actifio Appliance, that Actifio Appliance can instantly mount the imported data to its managed hosts.

Ownership of imported data is maintained by the source appliance. The Import function allows ownership to be transferred to the appliance to which the data is imported. Ownership gives full control over the image, including the ability to expire the image.

In case an image is accidentally imported, AGM provides a Forget Imported Image function that will remove an imported image from an Actifio Appliance.

To import images see:

[Importing Images From the AGM Domain Manager Storage Pool Page](#) on page 18

[Importing Images From the AGM App Manager Applications Page](#) on page 19

When defining a OnVault Pool, use the same object store and object store credentials.

Importing Images From the AGM Domain Manager Storage Pool Page

Importing images from the Storage Pool page has the advantage of allowing you to select multiple application images. To import images from the Storage Pools page:

1. From Manage > Storage Pools, right click on an OnVault Storage Pool and from the drop down menu select **Import OnVault Images**. The Import OnVault Images page is displayed:

The screenshot shows a table of storage pools with columns: NAME, TYPE, APPLIANCE, STORAGE AR..., WARNING (%), and SAFE (%). The first row is selected, and a context menu is open over it. The menu options are: Edit Organizations, Import OnVault Images..., and Forget Imported Images... The 'Import OnVault Images...' option is circled in orange.

NAME	TYPE	APPLIANCE	STORAGE AR...	WARNING (%)	SAFE (%)
CDS81-Onvault	OnVault	CDS 39-C2		80	90
IBM	OnVault	CD		80	90
Minio	OnVault	CA		80	90
Minio	OnVault	SK		80	90

2. Select the Actifio Appliance to which the application(s) will be imported.

The screenshot shows the 'Import OnVault Images To SKY8.0-226 Appliance' page. It includes a 'TAKE OWNERSHIP' toggle, 'OnVault Pool Details' (Appliance: SKY8.0-226, Pool Name: Minio, Pool Type: vault, Bucket: qa-automation, Compression: true), 'SELECT SOURCE APPLIANCE (57)' (skyupg10), and 'APPLICATIONS (1)' (EmptyVM7 (emptyvm7)). The 'IMPORT' button is highlighted in blue.

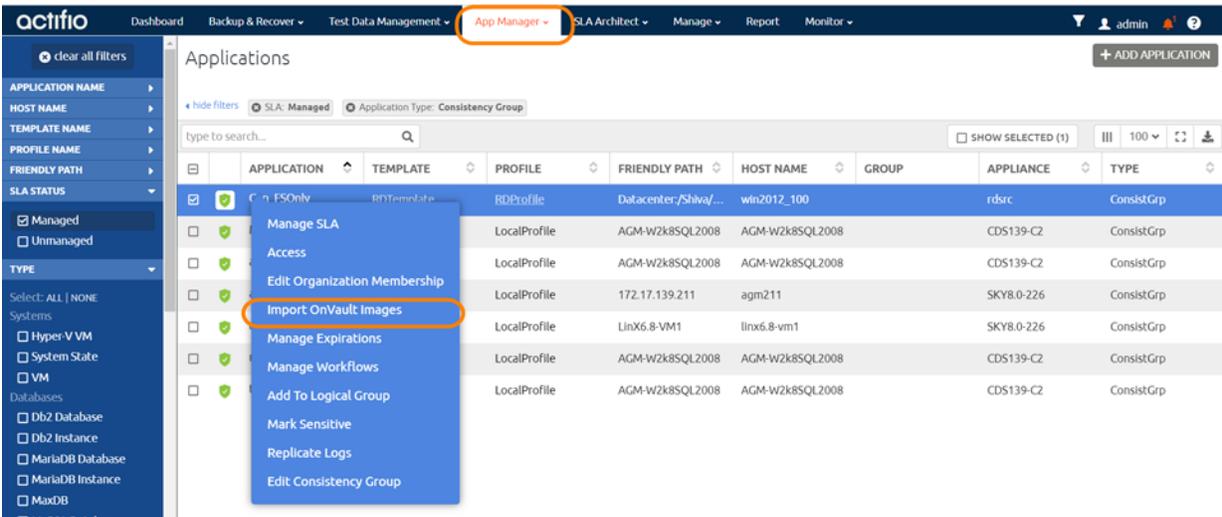
3. Select the application(s) to import.
4. Click **Import** and the import operation will begin. A message will be displayed when the operation completes.

Importing Images From the AGM App Manager Applications Page

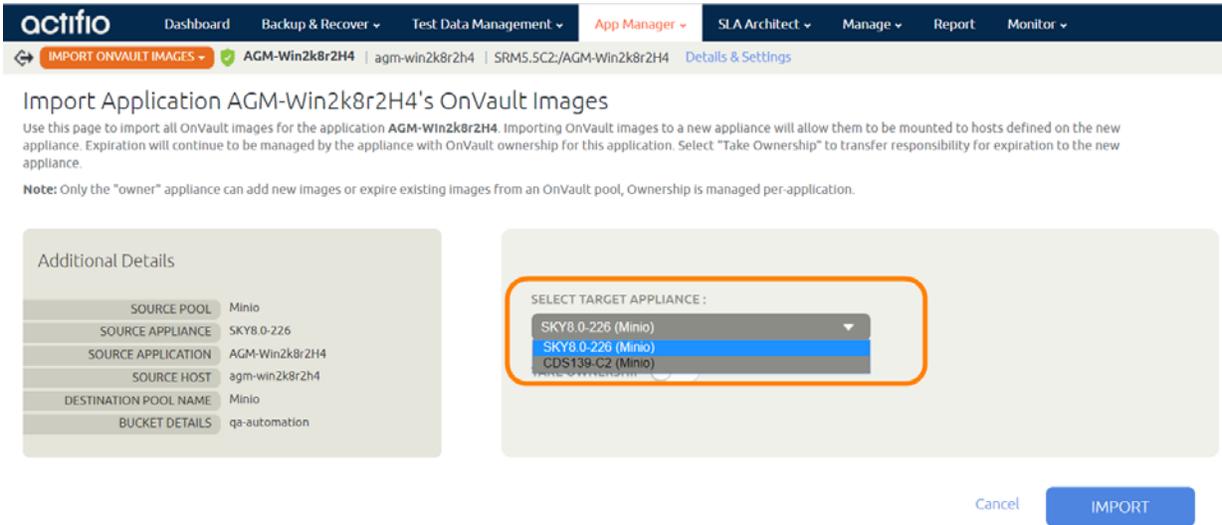
Importing images from the App Manager Applications page has the advantage of allowing you to quickly select a single, specific application image to be imported. To import multiple images, see [Importing Images From the AGM Domain Manager Storage Pool Page](#) on page 18.

To import an image from the App Manager Applications page:

1. Right click an application that is protected in an OnVault Pool.



2. From the drop down menu select **Import OnVault Images**. The Import OnVault Images page is displayed:



3. From the Select Target Appliance drop down menu, select the appliance to which the image will be imported.
4. Click **Import** and the import operation will begin. A message will be displayed when the operation is finished.

