
MariaDB DBA's Guide to Actifio Copy Data Management

Updated August 24, 2022



actifio

Actifio VDP 10.0

Copyright, Trademarks, and other Legal Matter

Copyright © 2022 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

Preface	vii
The ActifioNOW Customer Portal.....	vii
Chapter 1 - Introducing Actifio Copy Data Management for MariaDB Databases	1
Chapter 2 - Adding a MariaDB Database Host & Discovering the Database	3
Adding the Host.....	4
Discovering the MariaDB Instance from the App Manager.....	6
Finding the Discovered Instances and Databases in the App Manager.....	7
Chapter 3 - Configuring the MariaDB Backup Method	9
Ensuring that the Backup Capture Method is Set Correctly.....	11
Ensuring that the Disk Preference on the Host is Set Correctly	12
Staging Disk Format: File-Based Traditional Backup and Recovery in NFS/Block.....	12
Staging Disk Format: LVM Snapshot with Change Block Tracking on Linux.....	13
Chapter 4 - Protecting a MariaDB Instance and its Logs	15
Protecting a MariaDB Database.....	15
Protecting MariaDB Database Logs	17
Chapter 5 - Restoring, Accessing, or Recovering a MariaDB Database	19
Mount and Refresh from Block-Based Volume Snapshot to a Target MariaDB Instance as a Virtual Application.....	19
Restoring and Recovering a MariaDB Database	21
Recovering from Volume-Based Snapshot	21
Recovering from a Full+Incremental Backup.....	23

Preface

The information presented in this guide is intended for users who are familiar with basic Actifio processes and procedures as described in **Getting Started with Actifio Copy Data Management** and who are qualified to administer MariaDB databases.

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.

1 Introducing Actifio Copy Data Management for MariaDB Databases

An Actifio appliance is a highly scalable copy data management platform that virtualizes application data to improve the resiliency, agility, and cloud mobility of your business. It works by virtualizing data in much the same way other technologies have virtualized servers and networks. This enables you to capture data from production systems, manage it in the most efficient way possible, and use virtual copies of the data however they are needed.

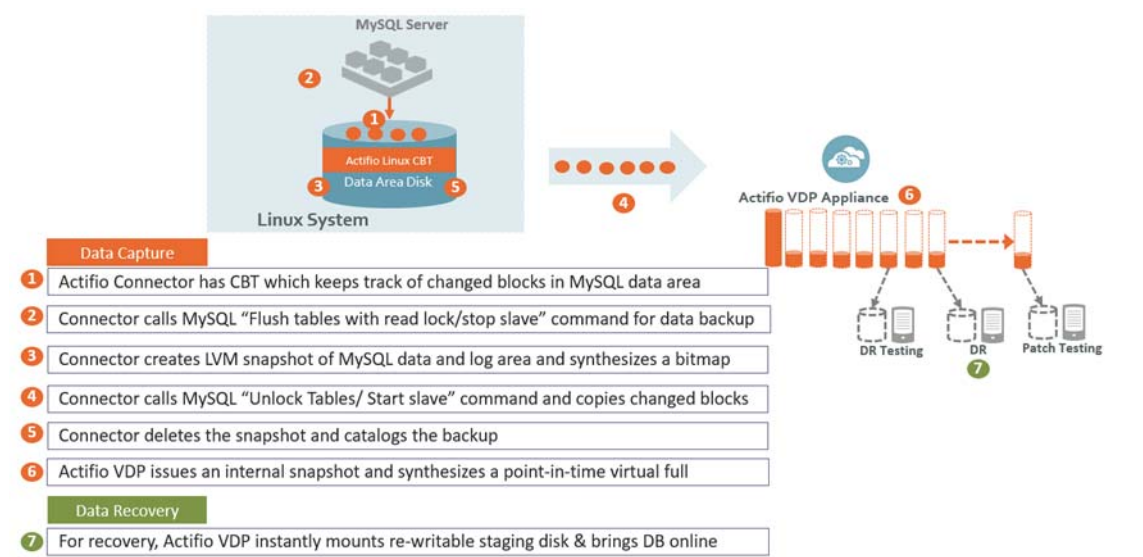
This DBA guide explains how to protect MariaDB application consistent database data with Actifio VDP in a Linux environment.

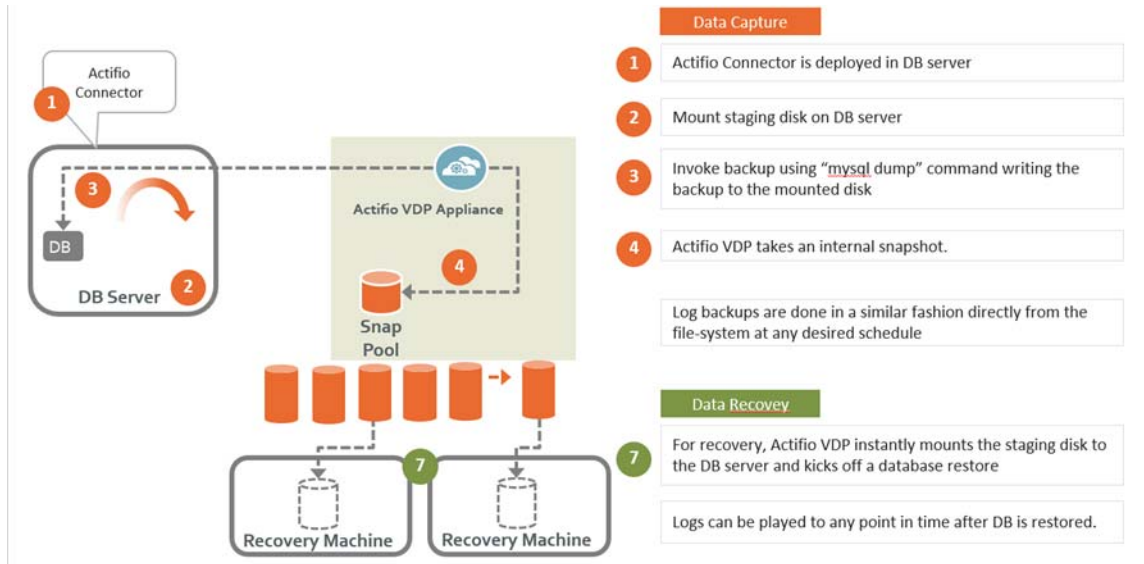
MariaDB Backup API used by Actifio VDP

Linux CBT and LVM snapshot: MariaDB "FLUSH TABLES WITH READ LOCK" and "UNLOCK TABLES" API

File-based backups: MariaDB "mysqldump" API. This provides the full backup of the database in backup format. On recovery, the restore db API recovers the database by physically overwriting the data area.

MariaDB log backup: During a log backup, VDP physically copies all the MariaDB binary logs. The MariaDB "purge binary logs BEFORE" API is used to purge the binary logs.





How It Works: MariaDB with File-Based Traditional Backup

2 Adding a MariaDB Database Host & Discovering the Database

Prerequisites

- The MariaDB database must be residing under LVM and it must not be the boot volume. Run `(mysql -e "select @@datadir")` to get the database data path.
- The LVM volume from which the MariaDB volumes are provisioned should have at least 20% free space.
- Install the Actifio Connector on the MariaDB server host (see **Network Administrator's Guide to Actifio VDP**.)
- Create a backup user with the privileges RELOAD, SELECT, LOCK TABLES, and SUPER (or) REPLICATION CLIENT. Backup username/password must be configured with host configuration.

To create the backup user:

```
create user actuser identified by 'actpasswd';
GRANT SELECT on *.* TO actuser;
GRANT RELOAD on *.* TO actuser;
GRANT LOCK TABLES on *.* TO actuser;
GRANT SUPER on *.* TO actuser;
GRANT REPLICATION CLIENT on *.* to actuser;
SHOW GRANTS FOR CURRENT_USER;
```

Note: If there are multiple MariaDB instances running on a server, then the backup username/password must be common for all MariaDB instance running on that server.

- MariaDB binary logging (`log_bin`) must be on to take log backup. To configure the binary log option, shut down the MariaDB server and edit the config file (`my.cnf` or `my.ini`). Within the `[mysqld]` section of the configuration file, add the `log-bin` option.

```
[mysqld]
log_bin = /log1/mysql13306/mysql13306-bin.0000
```

Adding a MariaDB Database Host and Discovering the Database

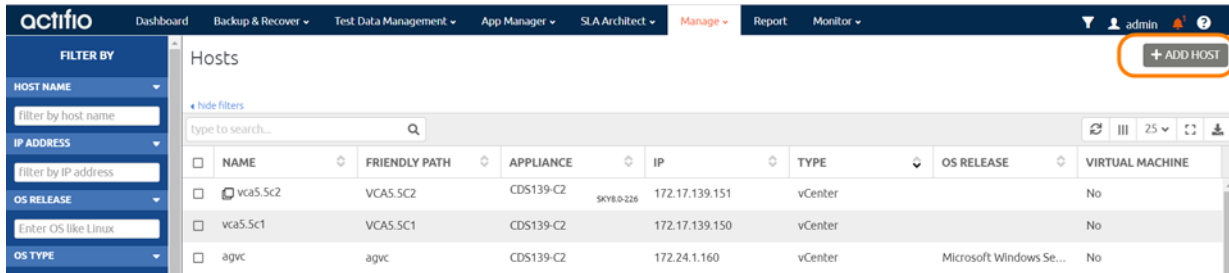
Before you can protect a MariaDB database, you must add the host and discover the database. This requires:

1. [Adding the Host](#) on page 4
2. [Discovering the MariaDB Instance from the App Manager](#) on page 6
3. [Finding the Discovered Instances and Databases in the App Manager](#) on page 7

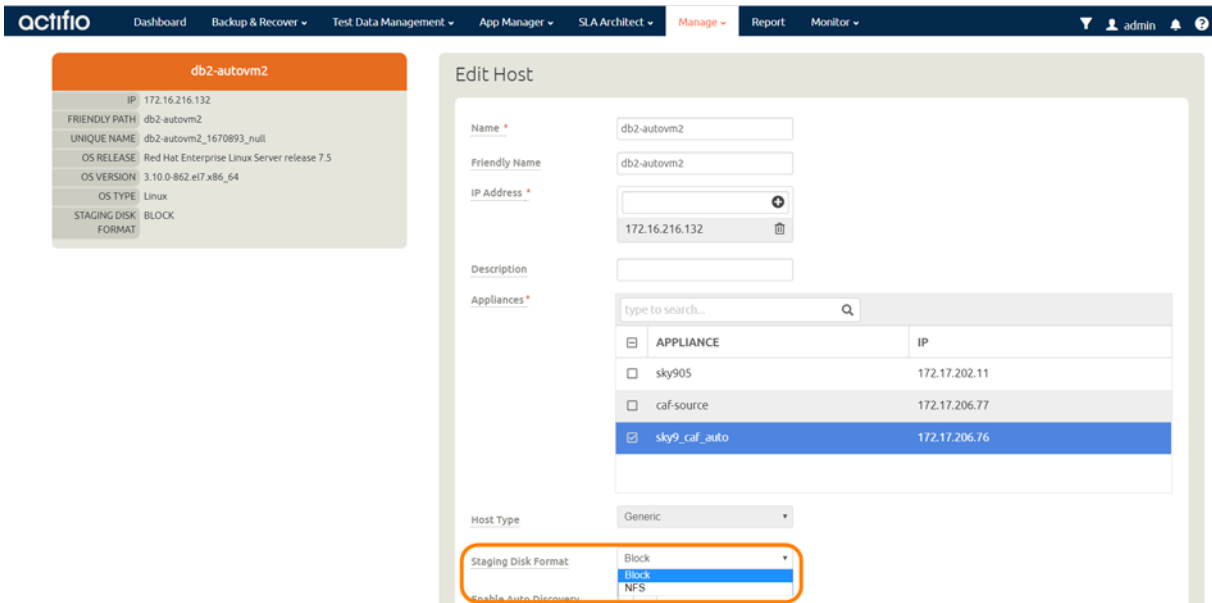
Adding the Host

Add the host to AGM. If the host is already added then edit the host and make sure to set all the configurations correctly.

1. From the Manage, Hosts list, click **+Add Host**.



2. On the Add Host page:
 - o **Name:** Provide the database server name.
 - o **IP Address:** Provide the database server IP and click the + sign on the right corner.
 - o **Appliances:** Select the check box for the appliance.
 - o **Host Type:** Make sure this is Generic.
3. Click **Add** at bottom right to add the host.
The Host is added.
4. Right-click the host and select **Edit**.
5. On the Edit Host page: Select the **Staging Disk Format:**
 - o For block-based backup with CBT or GPFS: select **Block**
 - o For file-based backup with Full+Incremental file system backup: select **Block or NFS**



- In Application Discovery Credentials, enter the username/password that you set up in [Prerequisites](#) on page 3.

Host Type
Generic

Staging Disk Format
Block

Enable Auto Discovery

Use Oracle Database Authentication

Must be enabled for hosts running Microsoft Windows.

Ports

Application Discovery Credentials

User Name
actuser

Password

Password Filepath

Connector Settings

Discovered Applications

Organizations

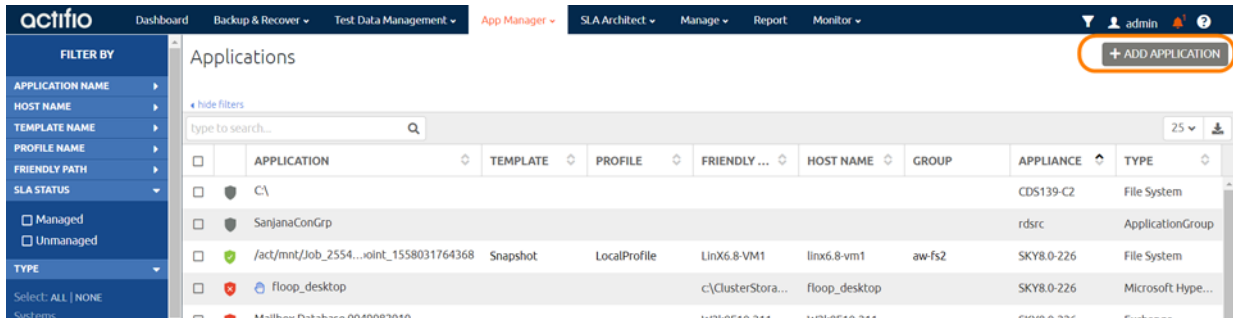
Cancel Save

- Select **Save** at the bottom of Edit Host page.

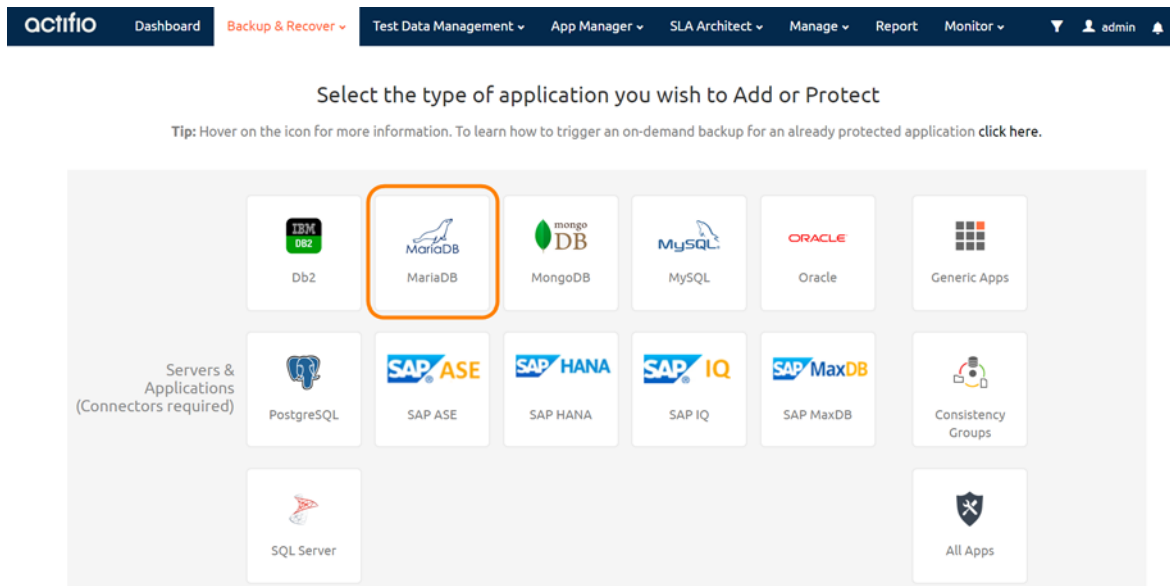
Discovering the MariaDB Instance from the App Manager

To discover the MariaDB instance:

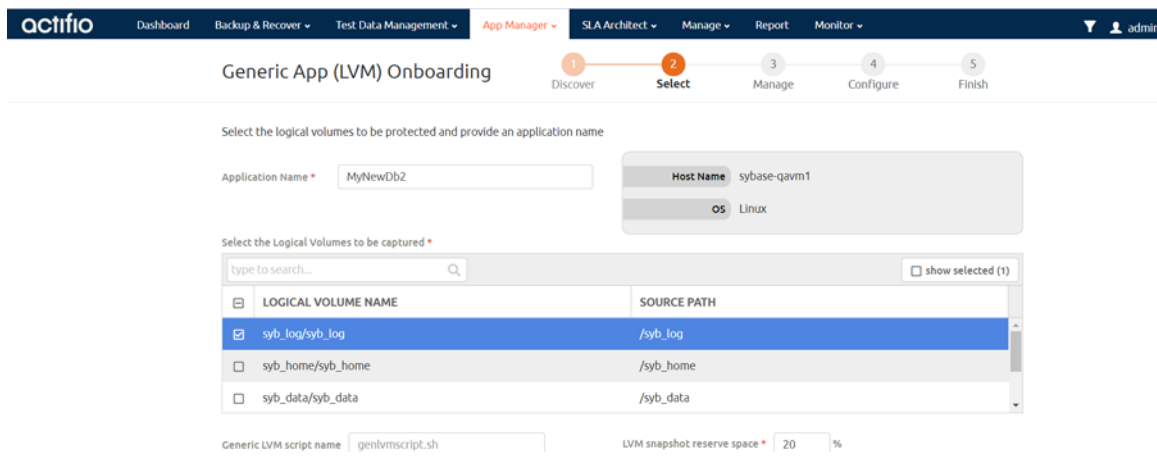
1. From the App Manager, Applications list, select **Add Application** in the upper right corner.



2. On the Add Application page, select **MariaDB**, then select the MariaDB database host. If you have many hosts, you can use the search feature or use the filter to see only hosts that are managed by a specific Actifio Appliance.



3. Select the host and click **Next** in the bottom right corner. This will run the discovery on the MariaDB host and will discover all MariaDB instances and databases running on it.



Finding the Discovered Instances and Databases in the App Manager

To find the newly-discovered database, go to the App Manager Applications list. All applications known to the AGM of all types are listed. Use the Type application filter on the left pane to show only MariaDB database instances. The new MariaDB instances and databases will appear in the list as unmanaged (the red shield icon).

The screenshot shows the Actifio App Manager interface. The left sidebar contains a filter menu with the following options:

- clear all filters
- APPLICATION NAME
- HOST NAME
- TEMPLATE NAME
- PROFILE NAME
- FRIENDLY PATH
- SLA STATUS
- Managed
- Unmanaged
- TYPE
- Select: ALL | NONE
- Systems
 - Hyper-V VM
 - System State
 - VM
- Databases
 - Db2 Database
 - Db2 Instance
 - MariaDB Database**
 - MariaDB Instance
 - MySQL Database
 - MySQL Instance

The main area displays a table of applications. The table has the following columns: APPLICATION, ID, TEMPLATE, PROFILE, FRIENDLY P..., HOST NAME, APPLIANCE, TYPE, and APPLIANCE A... The table contains 15 rows of data. The first 14 rows have a red shield icon in the first column, indicating they are unmanaged. The 15th row (AUTODB2) has a grey shield icon, indicating it is managed.

APPLICATION	ID	TEMPLATE	PROFILE	FRIENDLY P...	HOST NAME	APPLIANCE	TYPE	APPLIANCE A...
LVMNT2	1782897			maria_2	maria_2	sky9_caf_auto	MariaDB Datab...	1444878
BUG1	1772546			maria-1	maria-1	sky9_caf_auto	MariaDB Datab...	1417057
DIR333	1677033			maria_2	maria_2	sky9_caf_auto	MariaDB Datab...	1258410
DB99	1879781			j-maria-1	j-maria-1	caf-source	MariaDB Datab...	419465
CGDB32	1879757	onvault_slt_325...	onval_autoprofi...	j-maria-1	j-maria-1	caf-source	MariaDB Datab...	327947
CGDB12	1879755	onvault_slt_325...	onval_autoprofi...	j-maria-1	j-maria-1	caf-source	MariaDB Datab...	327945
FMO2	1682621			maria-1	maria-1	sky9_caf_auto	MariaDB Datab...	1262606
DIR222	1677168			maria_2	maria_2	sky9_caf_auto	MariaDB Datab...	1258508
DIR222	1664892	Maria_CBT	LocalProfile	maria-1	maria-1	sky9_caf_auto	MariaDB Datab...	1246958
AUTODB2	1880661					caf-source	MariaDB Datab...	211912
LVMNT1	1782855			maria_2	maria_2	sky9_caf_auto	MariaDB Datab...	1444641

3 Configuring the MariaDB Backup Method

After the database is prepared and discovered as explained in [Chapter 2, Adding a MariaDB Database Host & Discovering the Database](#), you can configure a VDP backup method SLA for the database.

The procedures for developing SLAs are detailed in the AGM online help. This chapter provides additional information of value to the MariaDB DBA.

Protection is set for the entire MariaDB Instance. You can include/exclude specific databases during the process using a Database Inclusion Rule from the Manage SLA page.

Whichever method you select involves these steps:

- [Application Details & Settings](#) on page 10

- [Ensuring that the Backup Capture Method is Set Correctly](#) on page 11

- [Ensuring that the Disk Preference on the Host is Set Correctly](#) on page 12

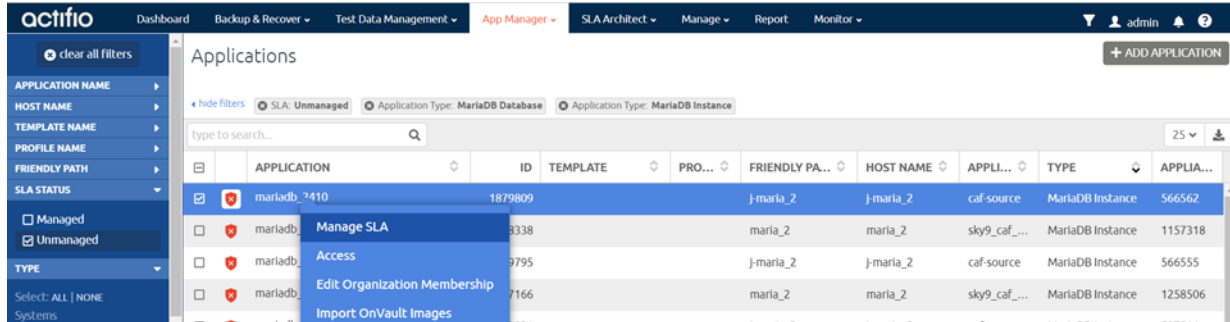
Table 1: Application Details & Settings

Setting	Block-Based LVM Snapshot with CBT on Linux	File-Based Backup and Recovery, Block or NFS
Use Staging Disk Granularity as Minimum Staging Disk Size	For applications that are under the size of granularity setting that tend to periodically grow this new option is useful to avoid frequent costly FULL backups. Because the staging disk is thin provisioned, there is no initial cost to use a staging disk that is larger than required for immediate use. The values are 0 for No and the Staging Disk Granularity setting for Yes.	
Staging Disk Granularity	Maximum size of each staging disk when multiple staging disks are used for an application. The default value is 1000GB.	
Last Staging Disk Minimum Size	Minimum size of the last staging disk created for an application with multiple staging disks. This value is also used for additional disks allocated to accommodate growth. The default value is 250GB.	
Connector Options	Use this only under the direction of Actifio Support.	
Percentage of Reserve Space in Volume Group	20% is recommended for LVM snapshot temporary space. Not applicable for protecting virtual databases.	Not applicable
Backup Capture Method	Use volume level backup	Use full+incremental filesystem backup
Database Filesystem Staging Disk Size in GB	Not applicable	Size of the database dump staging disk in GB. Use the default calculation: (database size * 1.5)+ 10%. Disks will grow dynamically.
Log Backup Staging Disk Size in GB	By default Actifio calculates this as daily log generation * retention of log backup SLA plus 20% buffer. Default is recommended. Providing a value will override the default calculation and the log disk will not grow dynamically. This will become a fixed size	
Retention of Production DB Logs in Days	This value is used to purge the log backup from basepath_logbackup destination. Based on this setting the last data backup id will be selected (CURRENT_TIMESTAMP, - the # days set) and the log will be purged older than the data backup id. Default value is 0 days. With default value all logs prior to last data backup will be purged.	
Script Timeout	The timeout value is applied to internal backup and recovery scripts called by connector. The default value is recommended.	

Ensuring that the Backup Capture Method is Set Correctly

Backup capture settings depend upon the backup capture method that you need. It is important to be certain that you have set the right backup method for your needs:

1. In the App Manager, Applications list, right-click the database and select **Manage SLA**.



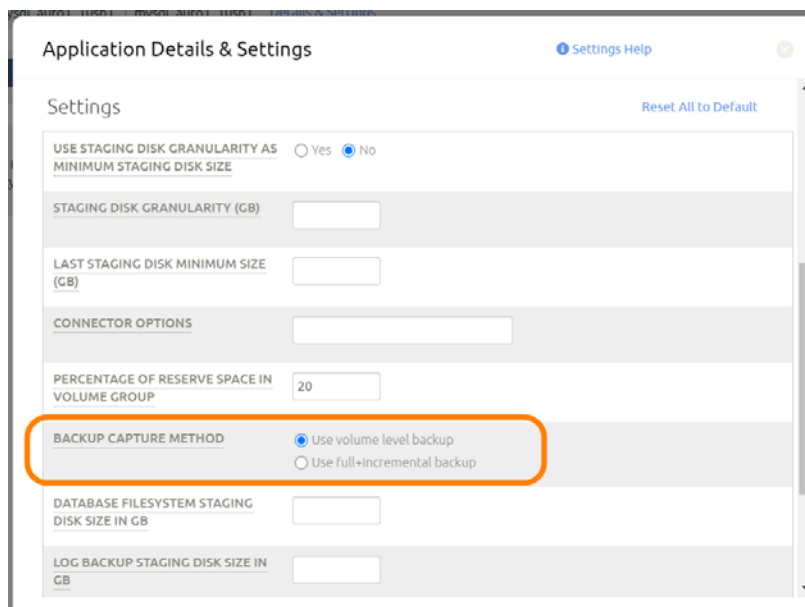
2. At the top of the Manage SLA page, select the **Details & Settings** link:



This opens the details and settings for this database. Check the Backup Capture Method:

- o Traditional Backup and Recovery API “file-based” backups: **Use full+incremental backup**
- o LVM Snapshot with Change Block Tracking: **Use volume level backup**

Note: System databases on a root partition can be backed up as LVM Snapshots and later mounted as virtual databases, but they cannot be used in a traditional Restore operation as the root partition cannot be unmounted. This will need manual restore and recovery from a simple mount back to the same host.



3. Click **Save** at the bottom of the page if you had to change anything.

Ensuring that the Disk Preference on the Host is Set Correctly

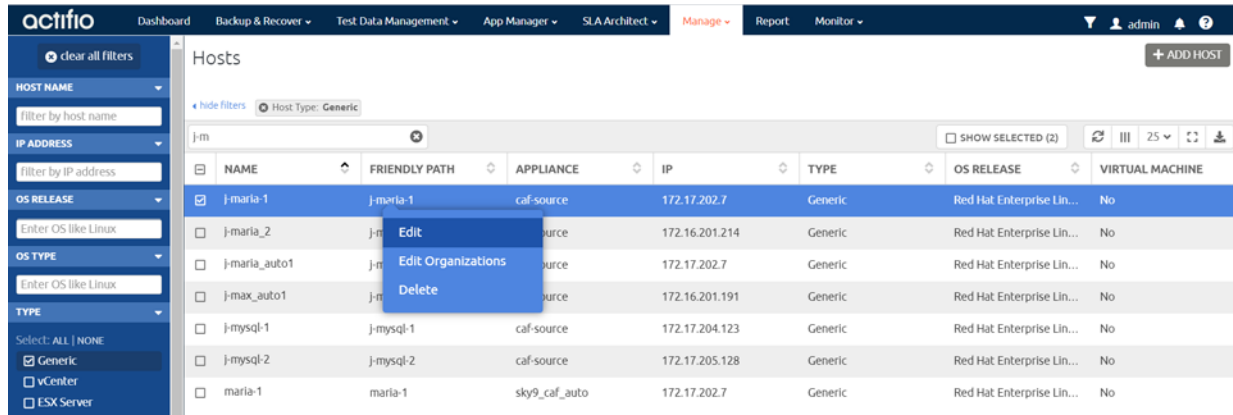
Choose between:

- [Staging Disk Format: File-Based Traditional Backup and Recovery in NFS/Block on page 12](#)
- [Staging Disk Format: LVM Snapshot with Change Block Tracking on Linux on page 13](#)

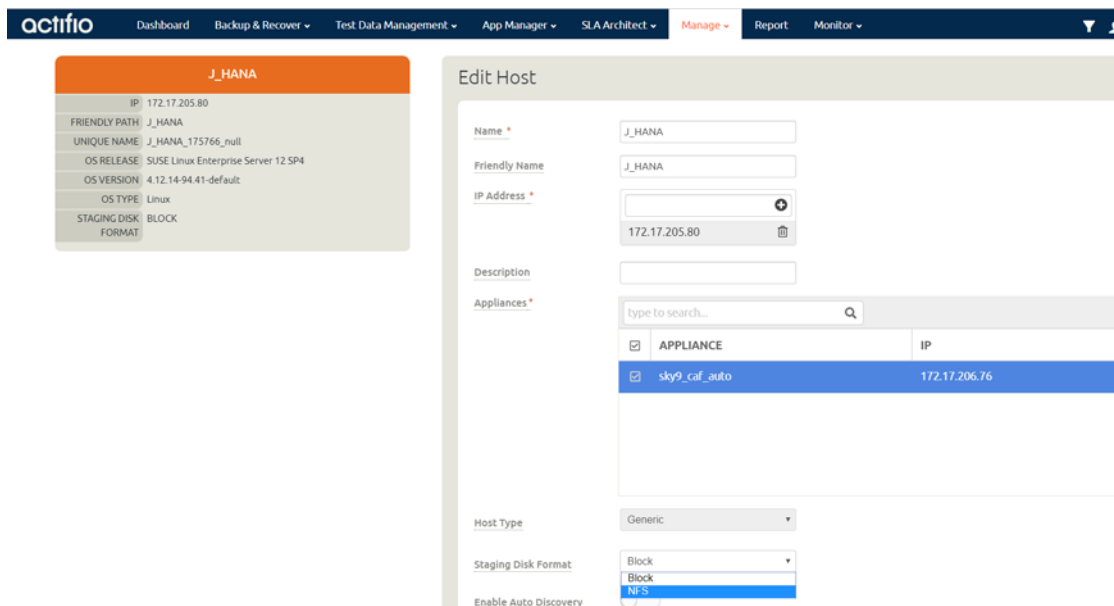
Staging Disk Format: File-Based Traditional Backup and Recovery in NFS/Block

To set staging disk format for storage snapshots:

1. From the Manage, Hosts list, right-click the host and select **Edit**.



2. Set Staging Disk Format to **NFS** or to **Block**.

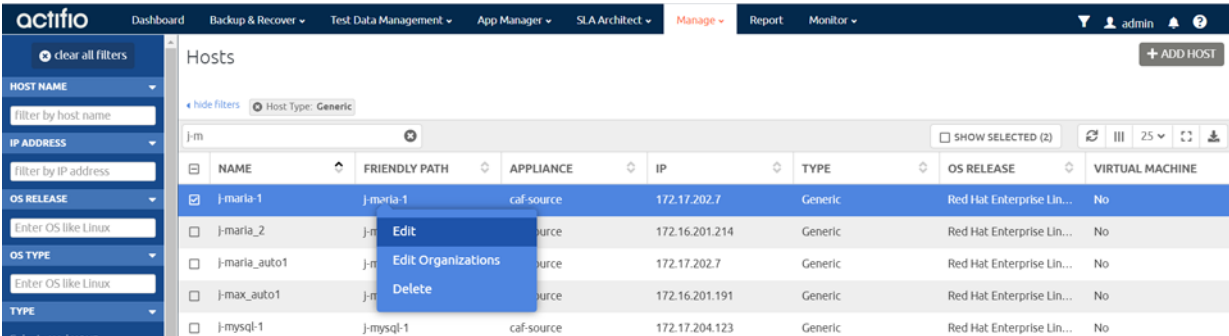


3. Then click **Save** at the bottom of the page.

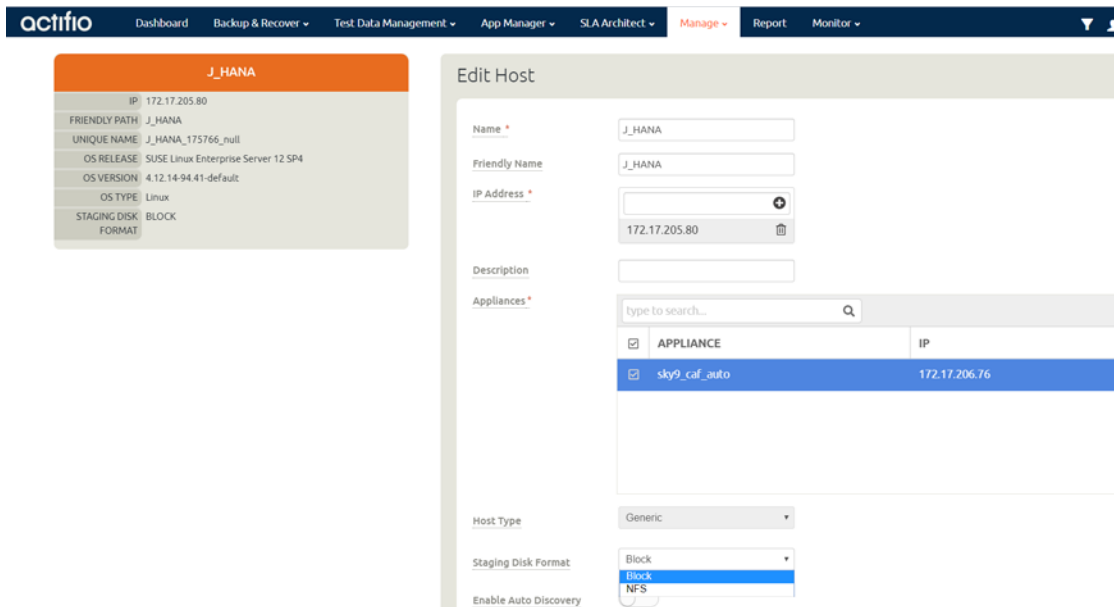
Staging Disk Format: LVM Snapshot with Change Block Tracking on Linux

To set staging disk format for storage snapshots:

1. From the Manage, Hosts list, right-click the host and select **Edit**.



2. Set Staging Disk Format to **Block**.



3. Then click **Save** at the bottom of the page.

4 Protecting a MariaDB Instance and its Logs

After the SLA is configured as detailed in [Chapter 3, Configuring the MariaDB Backup Method](#), you can configure a VDP backup method for the database.

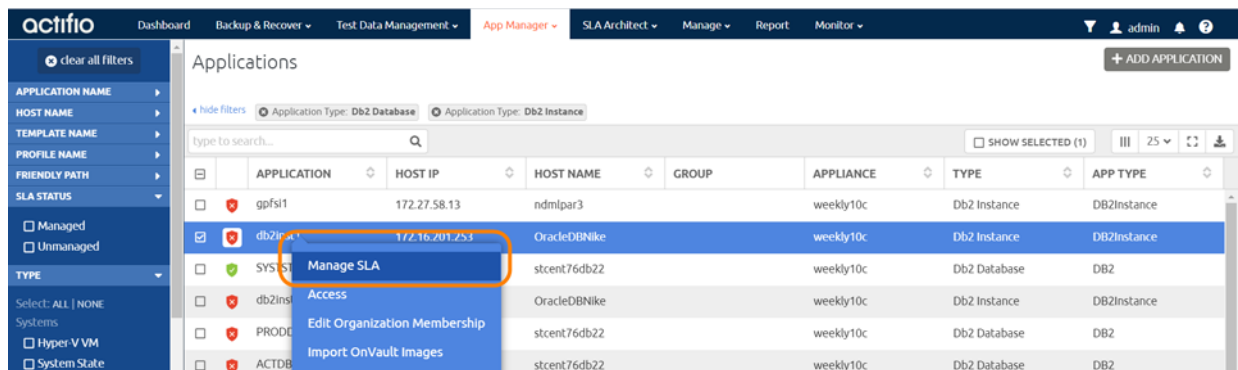
This chapter includes:

- [Protecting a MariaDB Database on page 15](#)
- [Protecting MariaDB Database Logs on page 17](#)

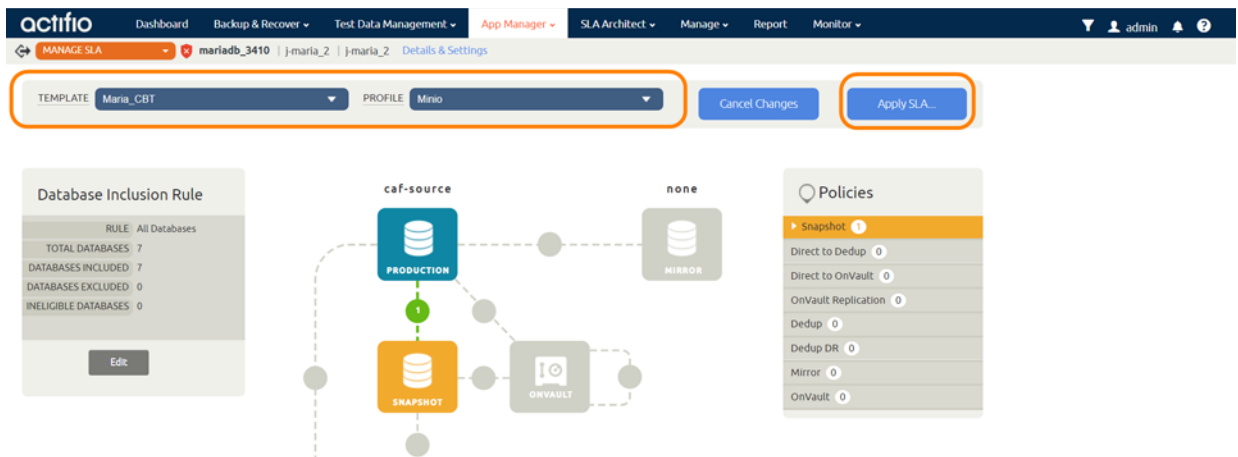
Protecting a MariaDB Database

To protect the database:

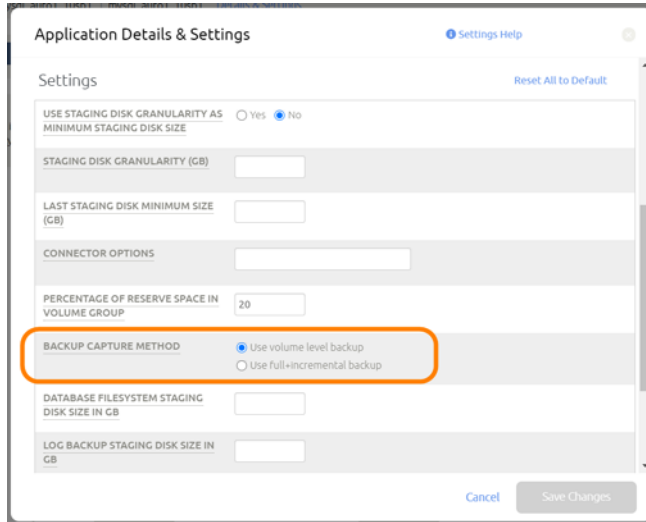
1. From the App Manager, Applications list, right-click the database and select **Manage SLA**.



2. On the Manage SLA page, select a template and a resource profile, then click **Apply SLA**.

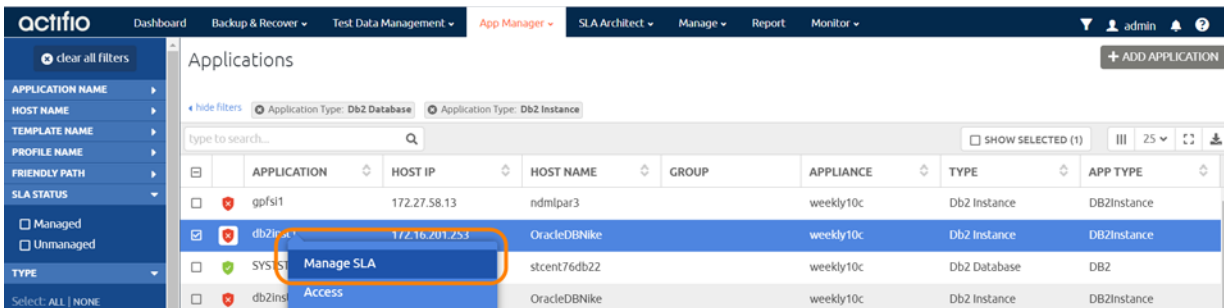


- On the Apply SLA page, make sure that the backup capture method matches the type of backup set in Chapter 3, Configuring the MariaDB Backup Method. Click **Apply SLA** or **Save Changes**.

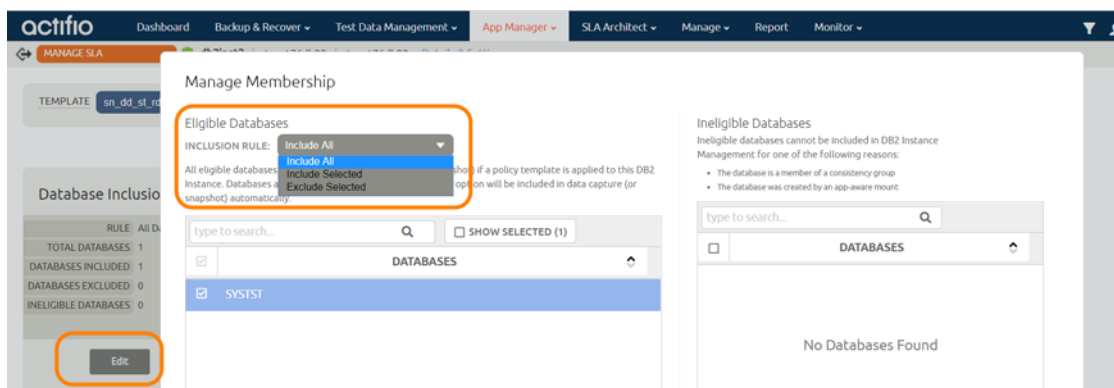


The database will be protected when the snapshot job runs according to the schedule in the template. After the first successful snapshot job the database appears in the App Manager with a green shield icon.

- You can include or exclude specific databases during backup. From the App Manager, Applications list, select the MariaDB Instance. You can use the Instance checkbox to filter the list. Select **Manage SLA**.



- Under Database Inclusion Rule, click **Edit**. If you do not see the Database Inclusion settings, you have a database, not an instance.

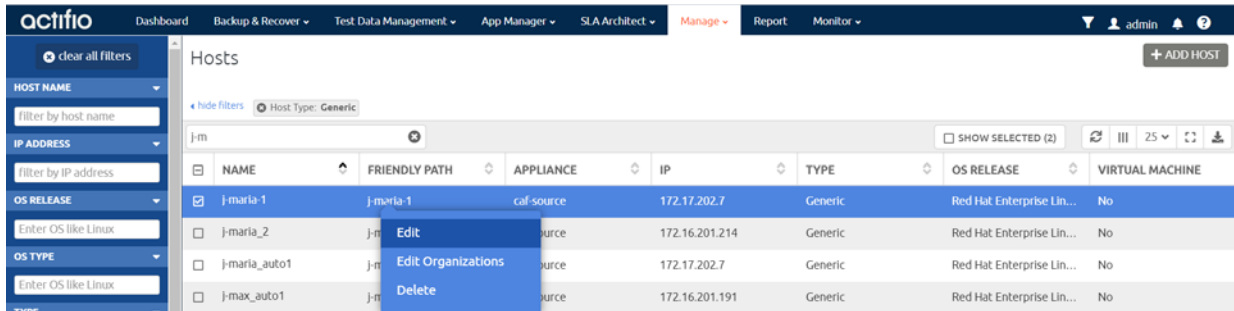


- Select an Inclusion Rule (Include All, Include Selected, or Exclude Selected) and then select the databases to include or exclude, then click **Save**.

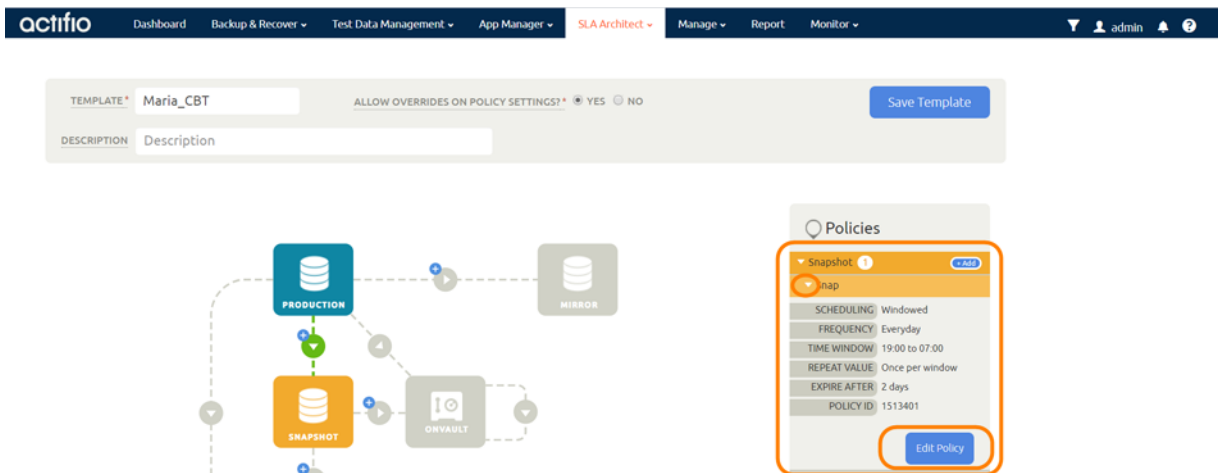
Protecting MariaDB Database Logs

To enable MariaDB database log backup:

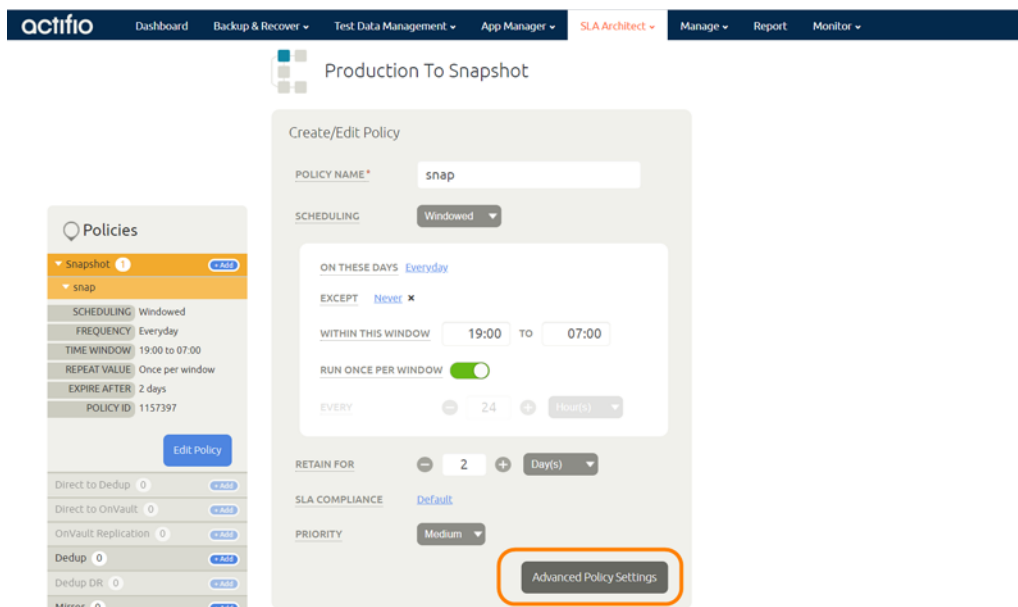
1. From the SLA Architect Templates list, right-click the template for MariaDB database protection and click **Edit**.



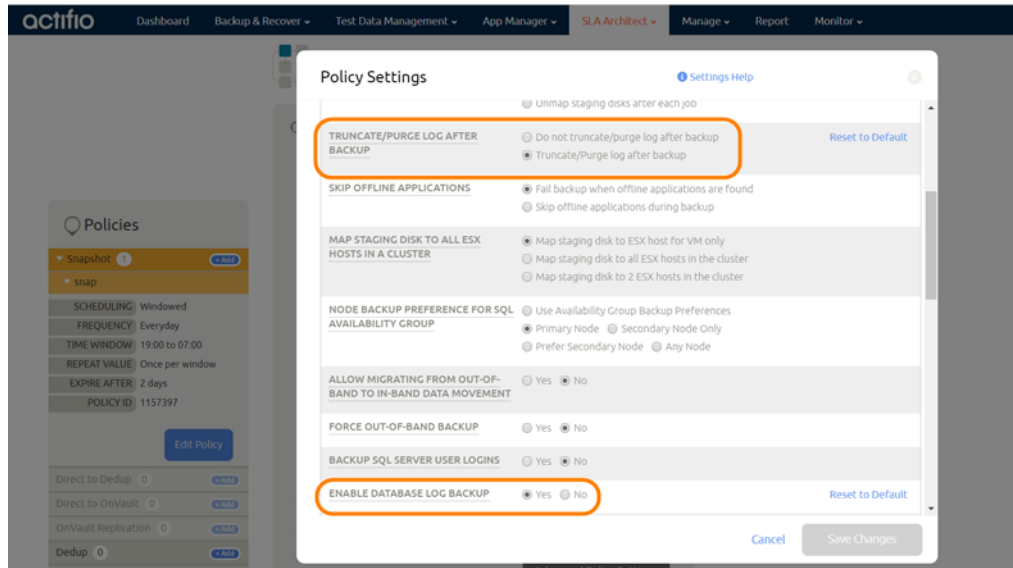
2. Click the arrow beside the Snapshot policy to open up the details, then select **Edit Policy**.



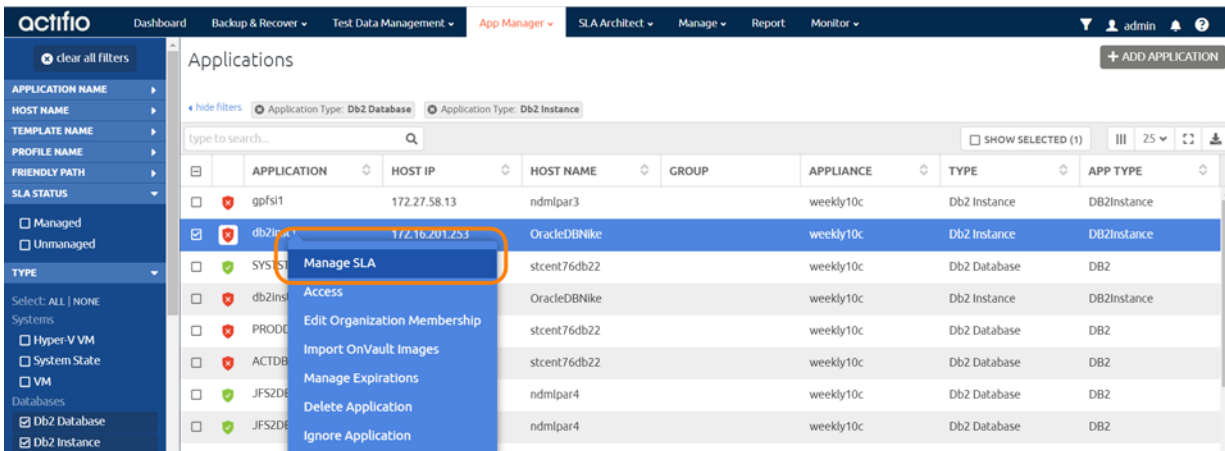
3. Near the bottom of the Create/Edit Policy page, select **Advanced Policy Settings**.



4. Set the log policy options (you will have to scroll to see them all):
 - o Enable **Truncate/Purge log after backup**.
 - o Set **Enable Database Log Backup** to **Yes**.
 - o For **RPO (Minutes)**, enter the desired frequency of log backup.
 - o Set **Log Backup Retention Period (in Days)** for point in time recovery.
 - o Set **Replicate Logs (Uses StreamSnap Technology)** to **Yes** if you want to enable StreamSnap replication of log backup to a DR site.
 - o Set **Log Staging Disk Growth Size** to a percent value that reflects your anticipated usage.



5. Click **Save Changes**.
6. From the App Manager, Applications list, right-click the MariaDB Instance and select **Manage SLA**.



7. At the top of the screen, select **Details & Settings**.
8. Set the **Retention of Production DB Logs** in days. This value is used to purge the logs from the production destination. Based on this setting the log will be purged older than the # of days specified. Default value is 0 days. With the default value, all logs prior to last log backups are purged.
9. Click **Save**.

5 Restoring, Accessing, or Recovering a MariaDB Database

This section describes:

Mount and Refresh from Block-Based Volume Snapshot to a Target MariaDB Instance as a Virtual Application on page 19

Restoring and Recovering a MariaDB Database on page 21

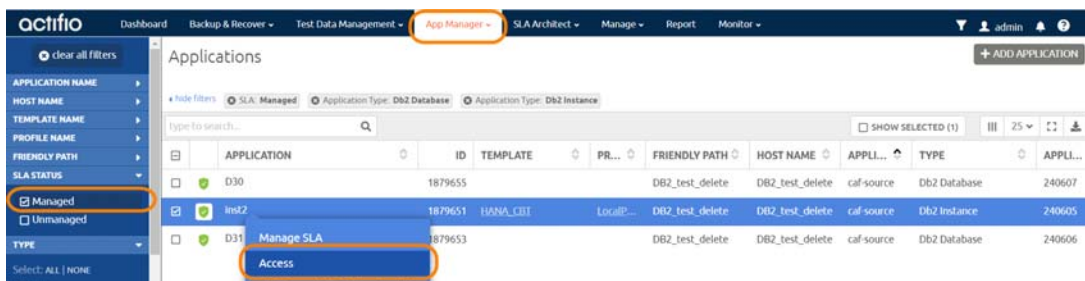
- o Recovering from Volume-Based Snapshot on page 21
- o Recovering from a Full+Incremental Backup on page 23

Mount and Refresh from Block-Based Volume Snapshot to a Target MariaDB Instance as a Virtual Application

To mount the database image as a virtual application (an application aware mount) to a new target:

1. From the App Manager, Applications list, right-click the database and select **Access**.

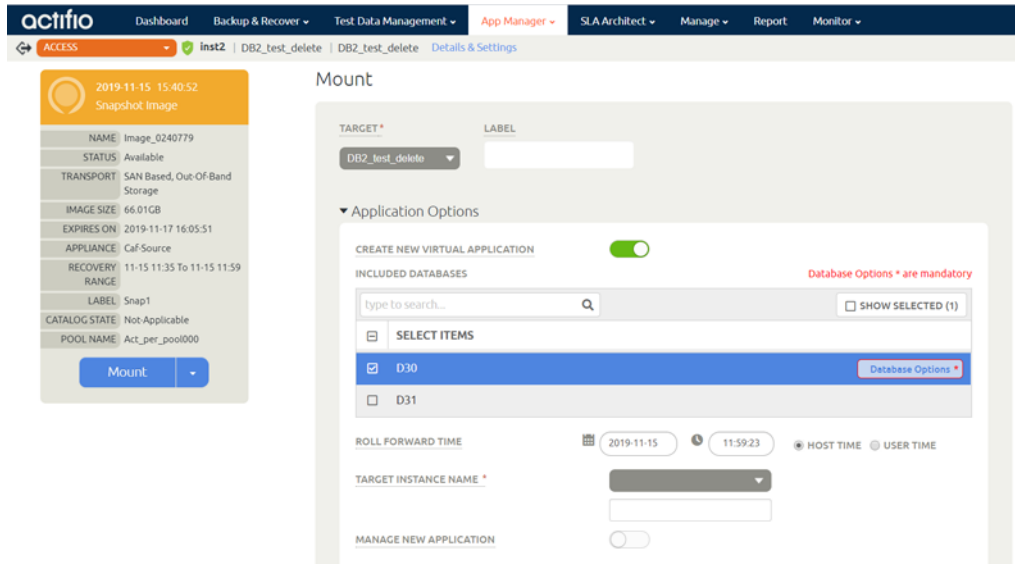
Note: You can use the Managed SLA Status filter to show only protected databases.



2. Select a snapshot image and choose **Mount**.



3. On the Mount page, from Target, choose the desired target server from the dropdown.
4. Under Application Options, enable **Create New Virtual Application**.
5. At Included Databases, Select Items, choose one or more databases to virtualize:
 - o A single database will be managed as standalone virtual copy
 - o Multiple databases will be managed as a consistency group



6. Click each selected database to specify the target database details for the new virtual copy.
7. Choose a target point in time for a database protected with log roll-forward.

NAME OF CONSISTENCY GROUP: This option will appear if more than one database is selected. Provide a unique name to manage the selected databases as a virtual copy.

TARGET MARIADB DATABASE NAME: From drop down select target instance to attach the selected database as virtual copy.

Manage New Application: To protect the new virtual database, click and enable Manage New Application. Choose a template and a resource profile to protect the database.
8. (Optional) Under Advanced Options, enter login credentials (username and password) for the target MySQL Instance that will be created. If you do not specify anything, empty database credentials will be used. For the directory path, enter the path to the messages directory for the MySQL Instance on the target server.
9. (Optional) Snatch Port by Stopping Existing Instance specifies whether to stop the existing instance and snatch the port if the target port is already in use by an existing instance.
10. Under Mapping Options:
 - o Storage Pool: Select a local or external storage pool for the mounted database.
 - o Mount Location: Specify a target mount point to mount the new virtual database to.
11. Click **Submit**.

Restoring and Recovering a MariaDB Database

Depending on how you protected the database, you need the procedure for:

[Recovering from Volume-Based Snapshot on page 21](#)

[Recovering from a Full+Incremental Backup on page 23](#)

Recovering from Volume-Based Snapshot

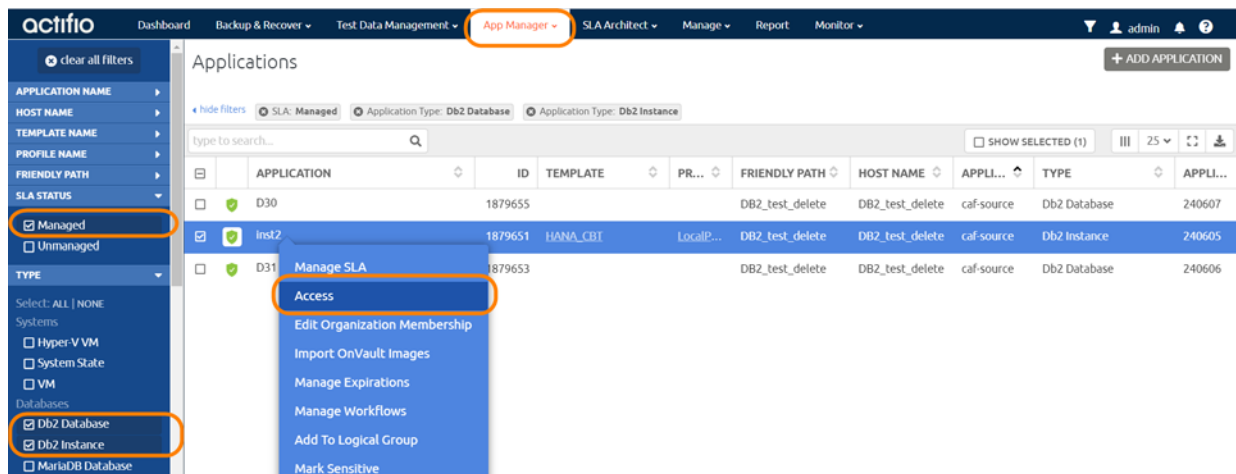
Use this procedure to restore and recover the source MariaDB database. This procedure uses physical recovery of the source data area.

Note: System databases on a root partition backed up as LVM Snapshots can be mounted as virtual databases, but they cannot be used in a traditional Restore operation as the root partition cannot be unmounted. This will need manual restore and recovery from a simple mount back to the same host.

To recover back to the source:

1. From the App Manager, Applications list right-click the protected database and select **Access**.

Note: You can use the Managed SLA Status filter to show only protected databases.



2. Select a snapshot image and choose **Restore**.



3. On the Restore page choose a point in time for the protected database to recover to.

The screenshot shows the Actifio interface for a restore operation. On the left, a sidebar displays details for a snapshot image: NAME: Image_0240779, STATUS: Available, TRANSPORT: SAN Based, Out-Of-Band Storage, IMAGE SIZE: 66.01GB, EXPIRES ON: 2019-11-17 16:05:51, APPLIANCE: Caf-Source, RECOVERY RANGE: 11-15 11:35 To 11-15 11:59, LABEL: Snap1, CATALOG STATE: Not-Applicable, POOL NAME: Act_per_pool000. A 'Restore' button is visible at the bottom of this sidebar.

The main area is titled 'Restore' and includes the instruction: 'Use this page to initiate a restore operation. A restore will take the existing database offline and overwrite their data files.' Below this, there are several configuration sections:

- ROLL FORWARD TIME:** Shows a date picker for '2019-11-15' and a time picker for '11:59:23'. Radio buttons for 'HOST TIME' (selected) and 'USER TIME' are present.
- INCLUDED DATABASES:** A search box with the text 'type to search...' and a 'SHOW SELECTED (2)' button.
- SELECT ITEMS:** A list of items, including 'D30' and 'D31', each with a checkbox. The 'D30' and 'D31' items are selected.
- RESTORE WITH RECOVERY:** A toggle switch that is currently turned on (green).
- Calendar:** A calendar for November 2019 with the 15th selected. A 'Close' button is at the bottom of the calendar.
- Buttons:** 'Cancel' and 'Submit' buttons are located at the bottom right of the main area.

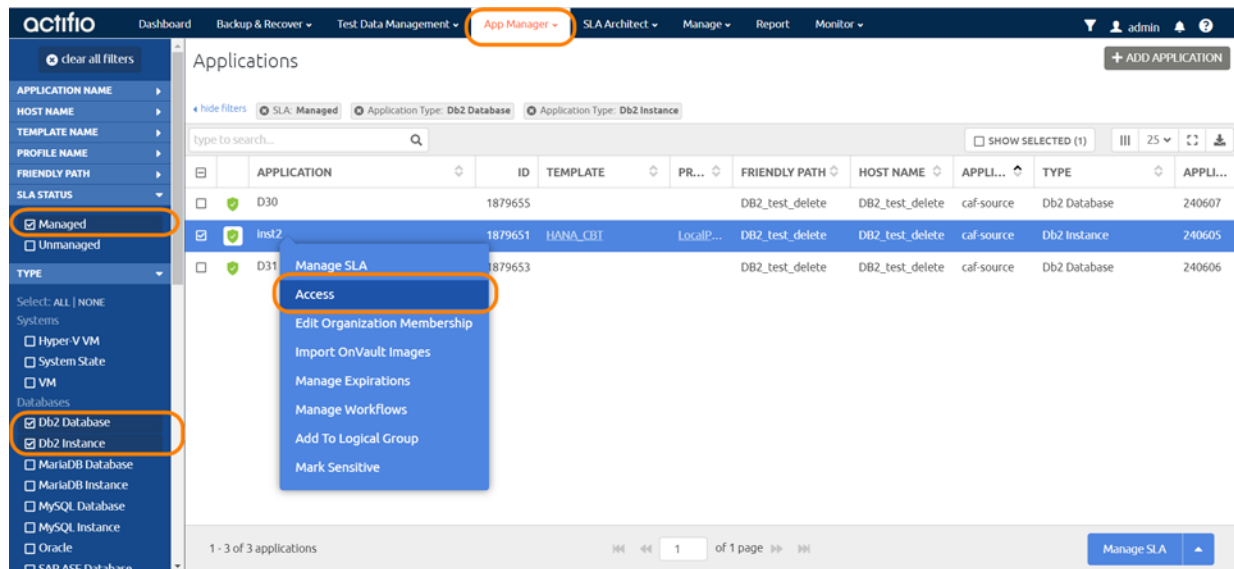
4. Enable **Restore With Recovery** to apply recovered logs.
5. Click **Submit**.

Recovering from a Full+Incremental Backup

Recovering Back to the Source: Use this procedure to restore and recover the source database. This procedure overwrites the source data.

1. From the App Manager, Applications list, right-click the protected database and select **Access**.

Note: You can use the Managed SLA Status filter to show only protected databases.



The screenshot shows the Actifio App Manager interface. The 'Applications' list is displayed with columns for APPLICATION, ID, TEMPLATE, FRIENDLY PATH, HOST NAME, APPLI..., TYPE, and APPLI... The 'inst2' application is selected, and a context menu is open with the 'Access' option highlighted. The left sidebar shows filters for SLA STATUS (Managed, Unmanaged) and TYPE (Db2 Database, Db2 Instance).

APPLICATION	ID	TEMPLATE	FRIENDLY PATH	HOST NAME	APPLI...	TYPE	APPLI...	
D30	1879655		DB2_test_delete	DB2_test_delete	caf-source	Db2 Database	240607	
inst2	1879651	HANA_CBI	LocalP...	DB2_test_delete	DB2_test_delete	caf-source	Db2 Instance	240605
D31	1879653		DB2_test_delete	DB2_test_delete	caf-source	Db2 Database	240606	

2. Select a snapshot image and choose **Restore**.



The screenshot shows the Actifio interface for a Snapshot Image. The timeline shows a snapshot taken on 2019-11-15 at 15:40:52. The 'Restore' option is highlighted in the context menu. The right sidebar shows details for the snapshot image, including NAME, STATUS, TRANSPORT, IMAGE SIZE, EXPIRES ON, APPLIANCE, RECOVERY RANGE, LABEL, CATALOG STATE, and POOL NAME.

NAME	STATUS	TRANSPORT	IMAGE SIZE	EXPIRES ON	APPLIANCE	RECOVERY RANGE	LABEL	CATALOG STATE	POOL NAME
Image_0240779	Available	SAN Based, Out-Of-Band Storage	66.01GB	2019-11-17 16:05:51	caf-Source	11-15 11:35 To 11-15 11:59	Snap1	Not-Applicable	Act_per_pool000

3. For a database protected with logs, on the Restore page, choose a date and a point in time.
4. Use **Select Items** to choose one or more databases to restore.
5. Click **Submit**. This will start the source database physical recovery.

