SAP MaxDB DBA's Guide to Actifio GO

Updated on August 31, 2022

Actifio GO

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

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 GO*** and who are qualified to administer SAP MaxDB 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:

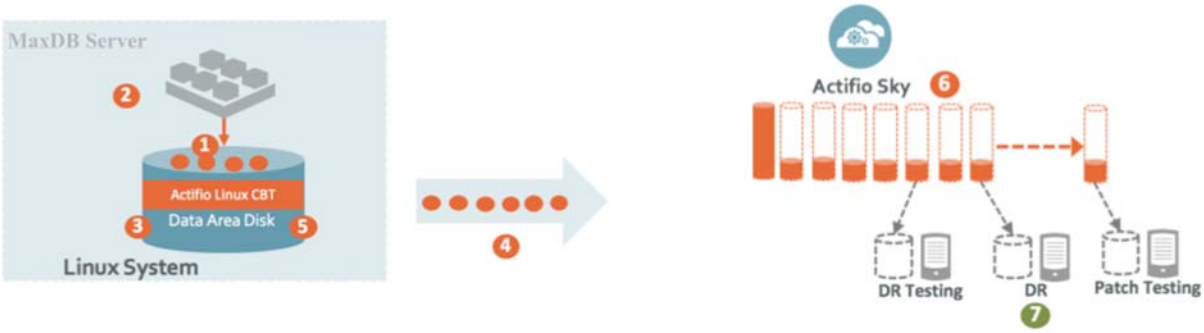
1. Go to: **https://now.actifio.com**
2. When prompted, enter the user name and password provided by your Actifio representative.

1 SAP MaxDB DBA's Introduction to Actifio Copy Data Management

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.

SAP MaxDB is the database management system developed and supported by SAP SE. SAP MaxDB is available on Microsoft Windows, Linux, and Unix, and for the most prominent hardware platforms.

Actifio VDP provides two ways to manage SAP MaxDB databases:



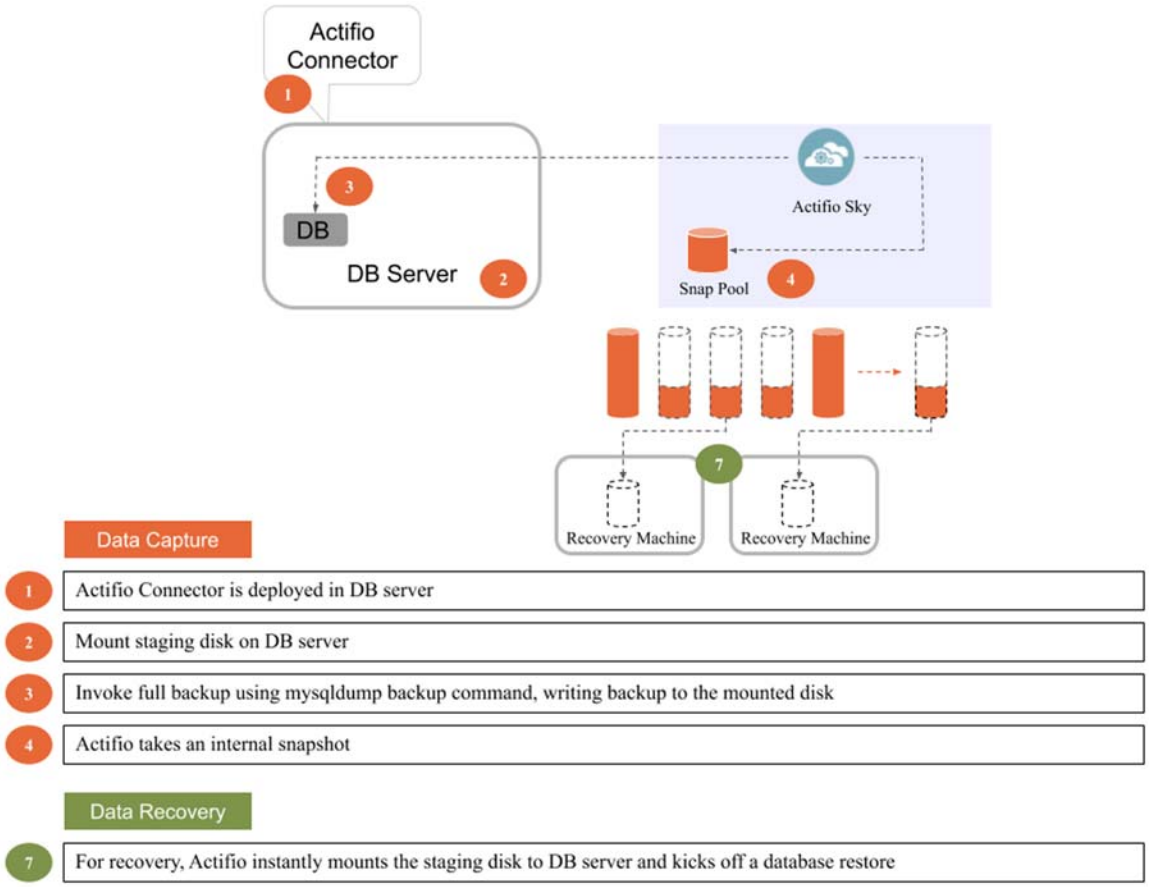
Data Capture

1. Actifio connector has CBT which keeps track of changed blocks in MaxDB database data area
2. Connector call MaxDB "*util_execute suspend logwriter*" command before LVM snapshot
3. Connector creates LVM snapshot of MaxDB database data area and synthesize a bitmap
4. Connector call MaxDB "*util_execute resume logwriter*" command and copies changed blocks
5. Connector deletes LVM snapshot and catalogs backup
6. Sky issues an internal snapshot and synthesize point-in-time virtual full

Data Recovery

7. For recovery, Actifio instantly mounts re-writable staging disk & brings DB online

SAP MaxDB with Linux CBT and LVM Snapshot



SAP MaxDB with Traditional File-Based Backup

SAP MaxDB APIs

Actifio VDP uses these SAP MaxDB backup APIs:

- **Linux CBT and LVM snapshot**: MaxDB "UTIL_EXECUTE SUSPEND LOGWRITER" and "UTIL_EXECUTE RESUME LOGWRITER" API with Linux CBT and LVM snapshot
- **File-based backups**: MaxDB "dbmcli -d <dbsid> -u <dbm_username>,<dbm_password> backup_start " file-based backups API

  This provides the full backup of the database in backup format The prerequisite for data backup is we need to define the backup template first. Recovery API restore db will recover the database by physically overwriting the data area
- **MaxDB log backup**: MaxDB Autolog Backup should be enabled on the application side. Actifio will just copy the log backup files to staging disk with "cp" command. As Autolog Backup is enabled we use os command to purge the log backup.

2 Preparing an SAP MaxDB Database for Protection

This section details the steps involved in preparing an SAP MaxDB database for Actifio protection and management:

Before You Begin

Before you begin, on the SAP MaxDB server:

- If there are multiple MaxDB instances running on a server, then the DB username/password must be common for all MaxDB instance running on that server.
- Autolog backup must be enabled. Use the following command to enable auto log backup:

```
dbmcli -d <DBSID> -u <DBM_USERNAME>,<DBM_PASSWD> autolog_on <autolog_backup_template_name>
```

- For enabling the autolog backup, you need an autolog backup template.
  To create a backup template.

```
dbmcli -d <DBSID> -u <DBM_USERNAME>,<DBM_PASSWD> backup_template_create <BACKUP_TEMPLATE_NAME>
to file  <FULL_PATH_WITH_FILE_NAME>  content log
```

- Log Overwrite area must be deactivated to enable autolog backup enable.
  To deactivate log overwrite:

```
dbmcli -d <DBSID> -u <DBM_USERNAME>,<DBM_PASSWD> db_execute SET LOG AUTO OVERWRITE OFF.
```

- Install the Actifio Connector on the SAP MaxDB server host (see ***A Network Administrator's Guide to Actifio VDP***.)

Adding an SAP MaxDB Database Host and Discovering the Database

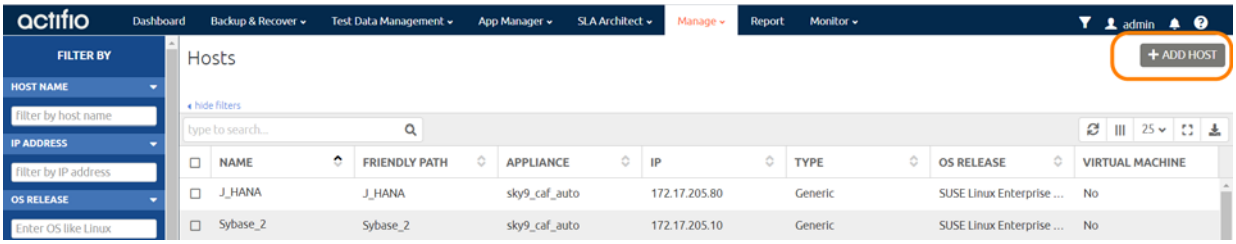
Before you can protect an SAP MaxDB database, you must add the host and discover the database:

1. Adding the Host from the AGM on page 4
2. Discovering the SAP MaxDB Database Application from the App Manager on page 5
3. Finding the Discovered SAP MaxDB Database in the App Manager on page 6

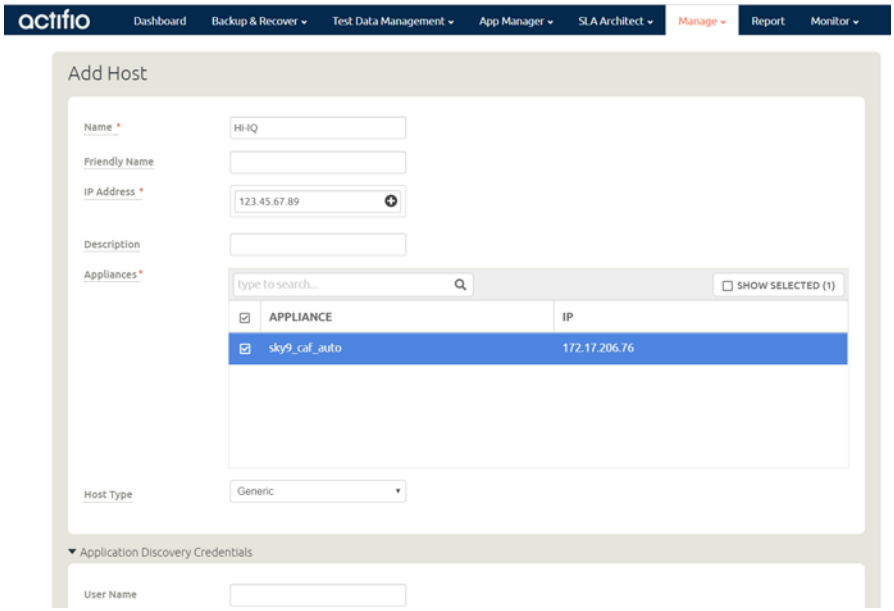
Adding the Host from the AGM

To add the host:

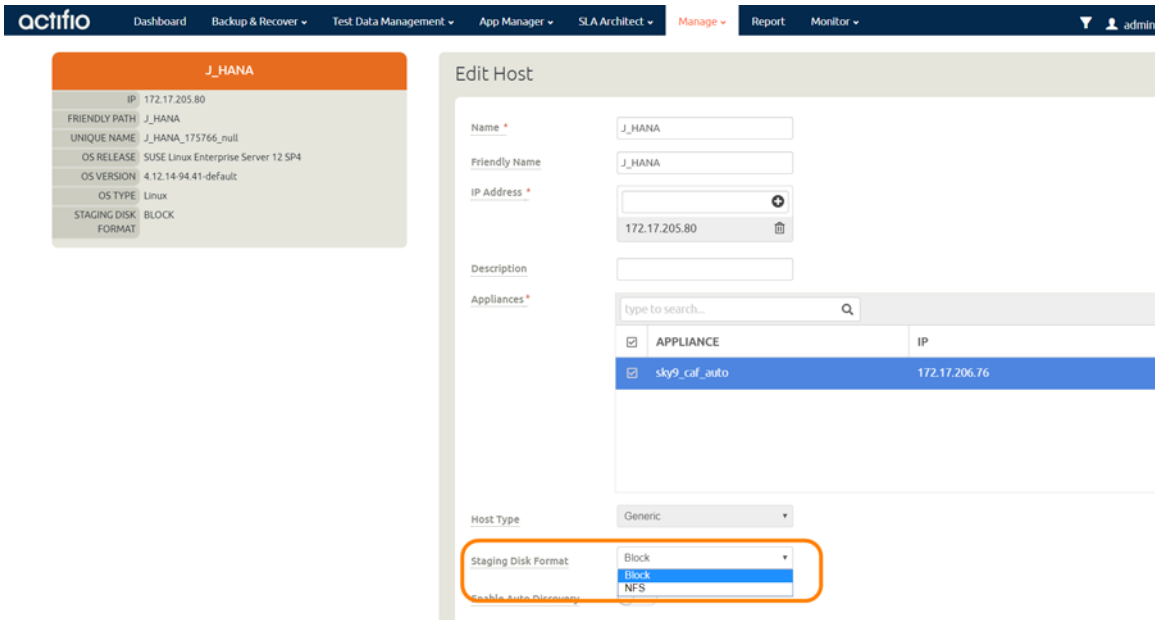
1. From the AGM Manage > Hosts list, in the upper right corner, click **+Add Host**.



2. On the Add Host page:
   - **Name**: Provide the SAP MaxDB database server name.
   - **IP Address**: Provide the SAP MaxDB database server IP and click the **+** sign on the right corner.
   - **Appliances**: Select the check box for the Actifio Appliance.
   - **Host Type**: Make sure this is **Generic**.
   - Provide **Application Discovery Credentials** to discover SAP MaxDB databases.



3. Click **Add** at bottom right to add the host. The Host will be added.
4. Right-click the host and select **Edit**.
5. On the Edit Host page: Set the staging disk format:
   - For block-based backup with CBT, select **Block**.
   - For file-based backup with Full+Incremental file system backup: select either **Block** or **NFS**.



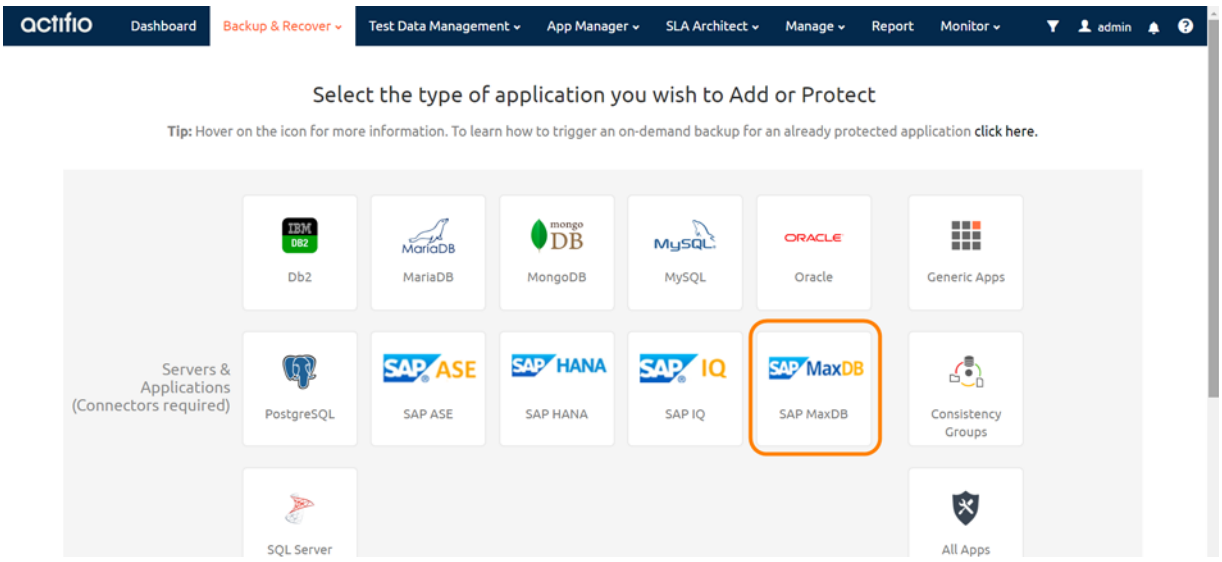
6. Select **Save** at the bottom of Edit Host page.

Discovering the SAP MaxDB Database Application from the App Manager

To discover the SAP MaxDB database:

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

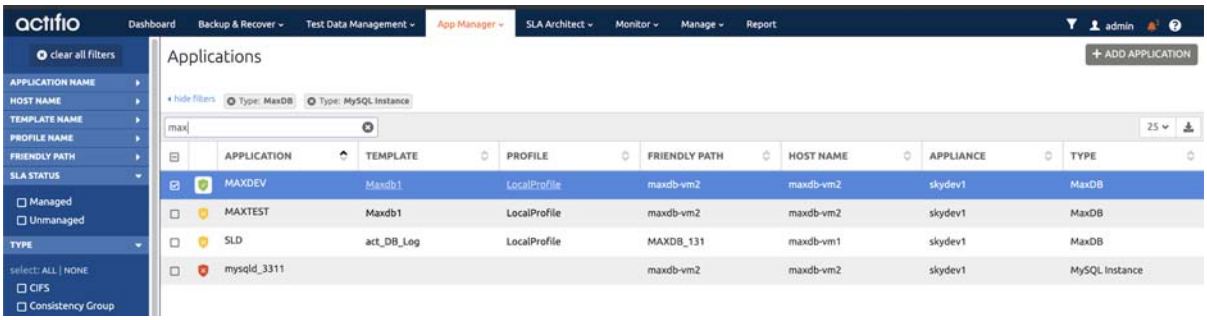
2. The Onboarding Wizard opens. Select **SAP MaxDB**.



3. Select the host and click **Next** in the bottom right corner. Discovery may take a while. Then follow the Onboarding Wizard to completion.

Finding the Discovered SAP MaxDB Database 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 left pane to show only SAP MaxDB databases.



3 Configuring the Backup Method

After the database is prepared and discovered as explained in Chapter 2, Preparing an SAP MaxDB Database for Protection, you can configure an Actifio backup method for the database.

- Using block-based volume level LVM snapshots with CBT on Linux. This option enables you to create application-aware virtual databases from the snapshot images.
- Using file-based traditional backup and recovery. This "file dump" method does not support the creation of virtual databases, and it requires Setting the Schedule for Dumps on page 12.

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

Whichever method you select involves these steps:

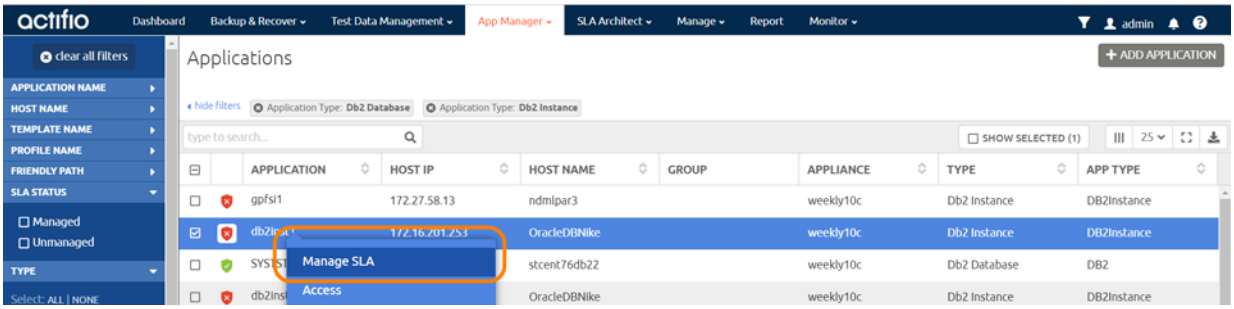
Table 1: SAP MaxDB Application Details & Settings

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	Needed for LVM snapshot temporary space. Recommended value is 20%	Not applicable
Backup Capture Method	Use volume level backup	Use full+incremental filesystem backup
Force Full Filesystem Backup	Not applicable	Use for an on demand full backup
Database Filesystem Staging Disk Size in GB	Not applicable	Use the default calculation: (database size * 1.5)+ 10%. The 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.	

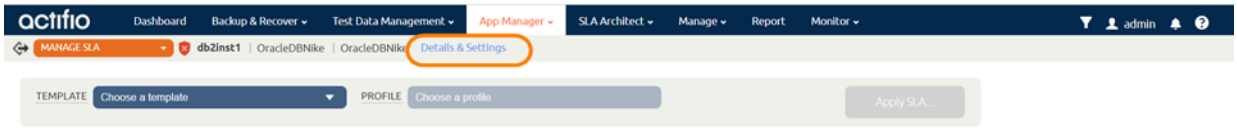
Ensuring that the Backup Capture Method is Set Correctly

Backup capture settings depend upon the backup capture method that you need. 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**.



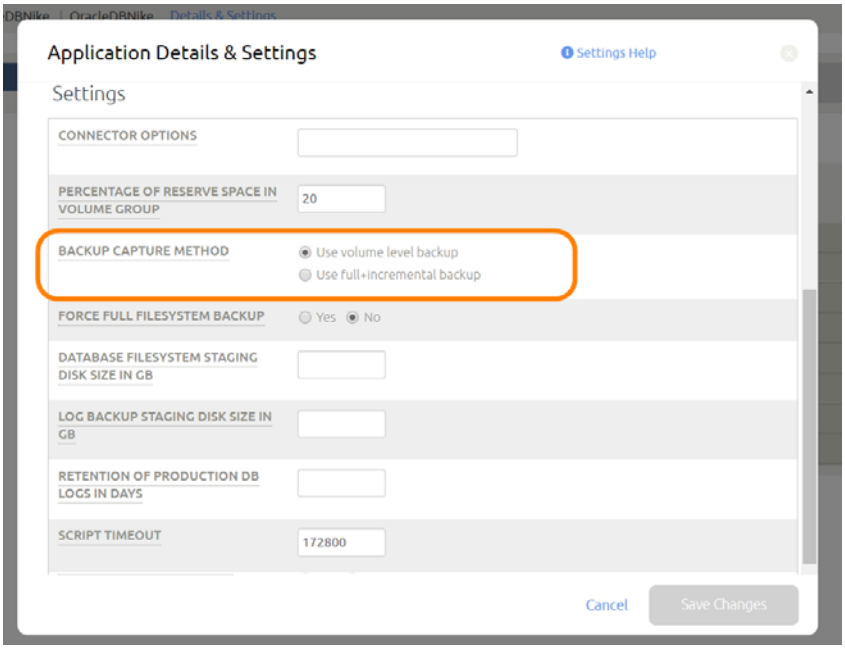
2. At the top of the Manage SLA page, select the **Details & Settings** link:



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

- LVM Snapshot with Change Block Tracking: **Use volume level backup**.
- Traditional Backup and Recovery API "file-based" backups: **Use full+incremental 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 Changes** at the bottom of the page if you had to change anything.

Ensuring that the Staging Disk Format on the Host is Set Correctly

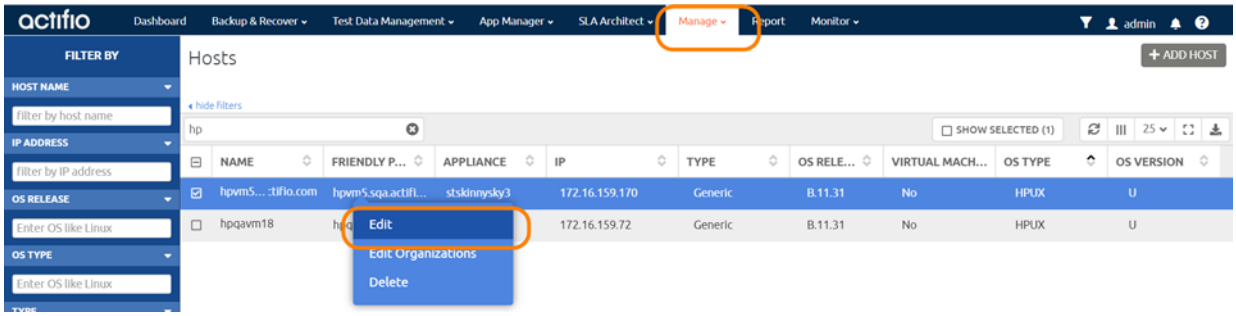
Choose between:

- Staging Disk Format: File-Based Traditional Backup and Recovery in NFS/Block on page 10
- Staging Disk Format: LVM Snapshot with Change Block Tracking on Linux on page 11

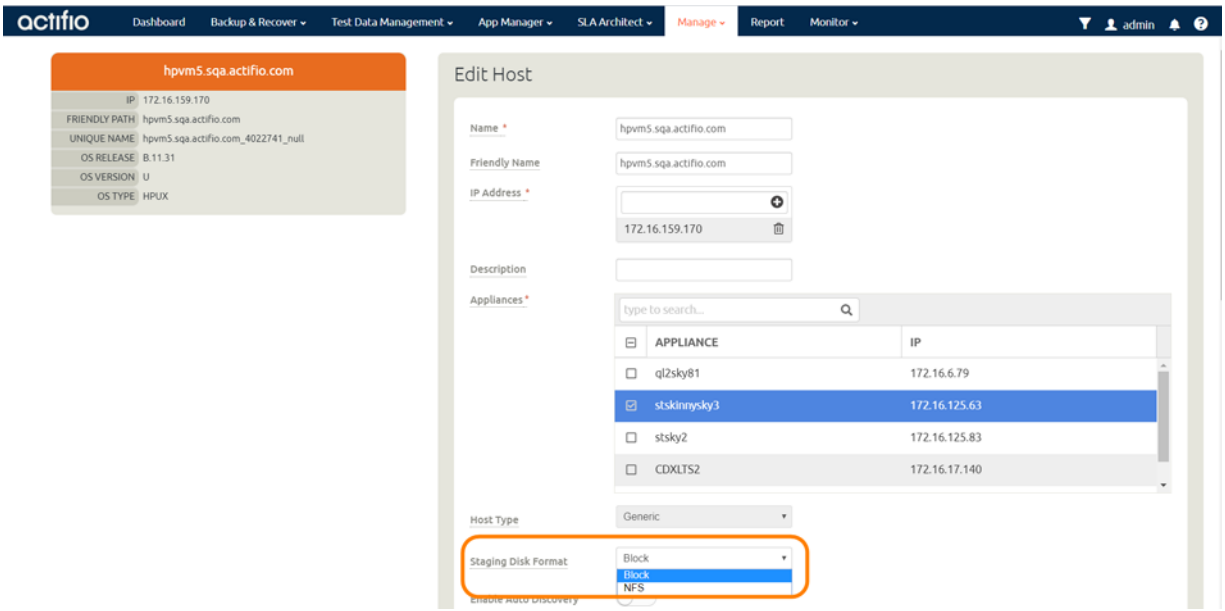
Staging Disk Format: File-Based Traditional Backup and Recovery in NFS/Block

To set the 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 either **NFS** or to **Block**.



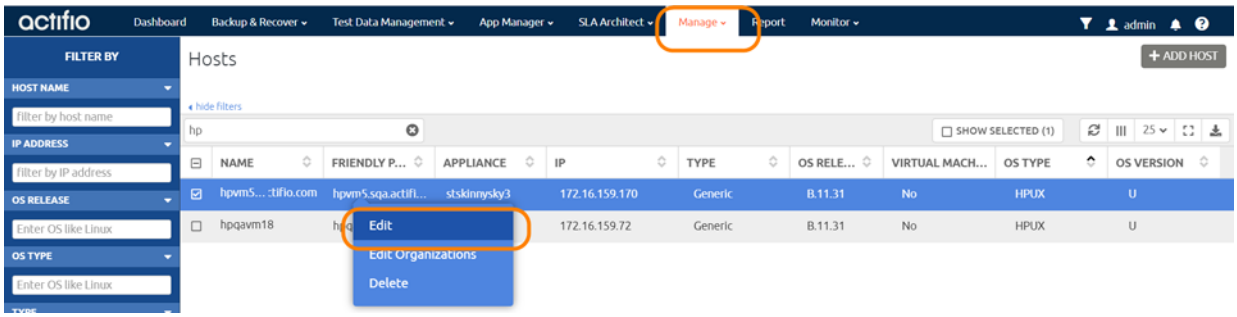
3. Then click **Save** at the bottom of the page.

Note: *File-based backup also requires the DB dump schedule be configured. See* Setting the Schedule for Dumps *on page 12.*

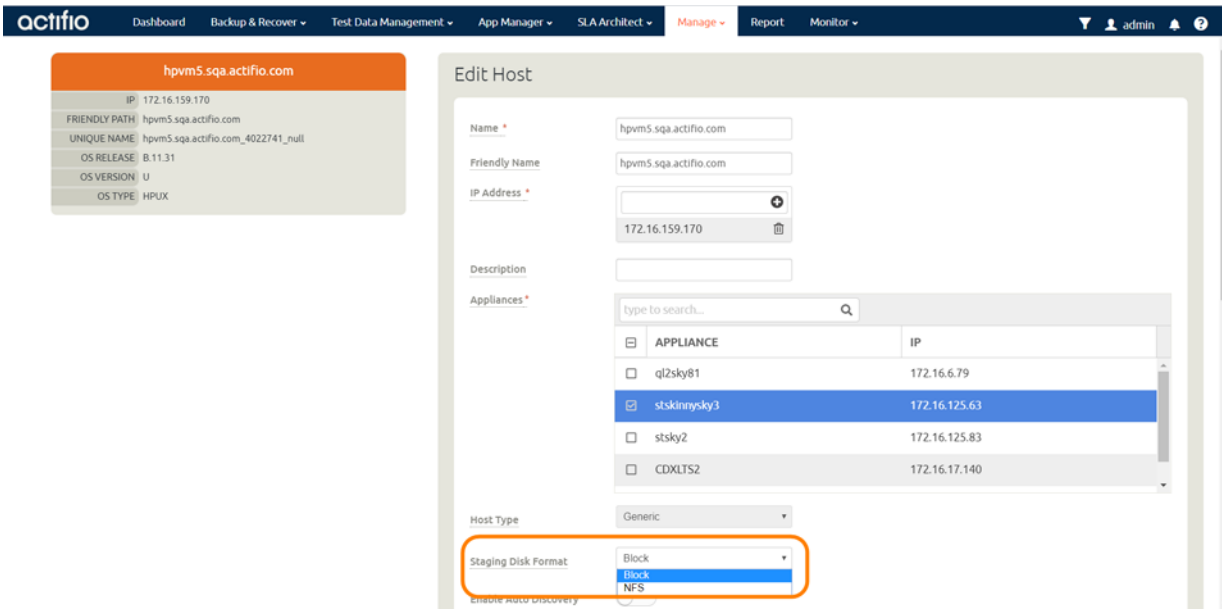
Staging Disk Format: LVM Snapshot with Change Block Tracking on Linux

To set the 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.

Setting the Schedule for Dumps

The database dump schedule is set by the Actifio CLI policy parameter dumpschedule. The default value of dumpschedule="FIIIIII":

- The string must be seven characters - either an 'F' or an 'I'
- Each position within the string represents a weekday, starting with Sunday.
- **F** represents a full db dump
- **I** represents an incremental db dump

For example, "FIIIIII" results in:

- Sunday: Full backup
- Monday through Saturday: Incremental backups
- The following Sunday: Full backup again

To check the dump schedule, run this CLI command from the Actifio Appliance:

```
udsinfo lspolicyoption -filtervalue appid=<appid> | grep dumpschedule
```

If this does not return any value, then the dumpschedule is set to default.

To modify the dump schedule run this CLI command from the Actifio Appliance:

```
udstask mkpolicyoption -appid <appid> -name "dumpschedule" -value "FIIIIII"
```

Replace <appid> with the application id of the MaxDB application.

Replace "FIIIIII" as needed.

Example

To run full backup on Saturday and Tuesday, set `dumpschedule="IIFIIIF"`

For more information, refer to the ***Actifio CLI Reference***.

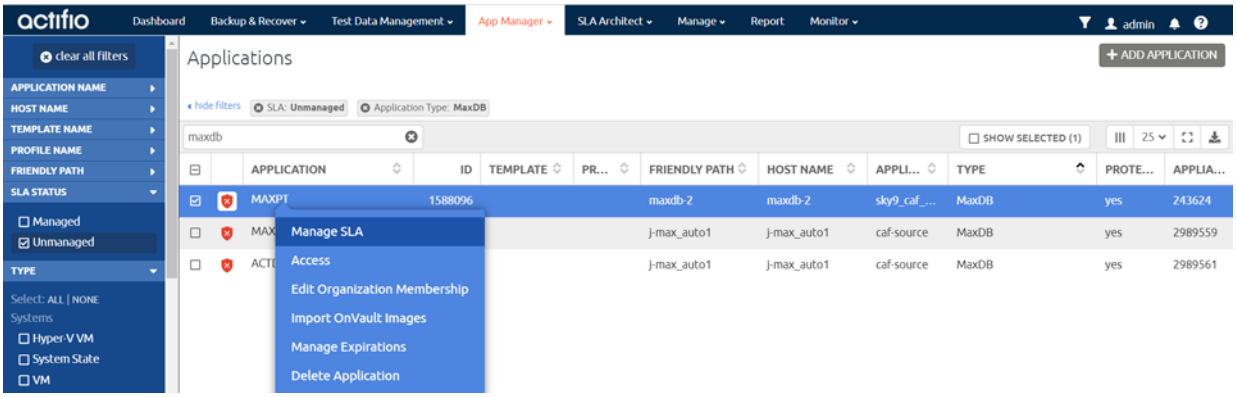
4 Protecting an SAP MaxDB Database and its Logs

Protecting an SAP MaxDB database includes both:

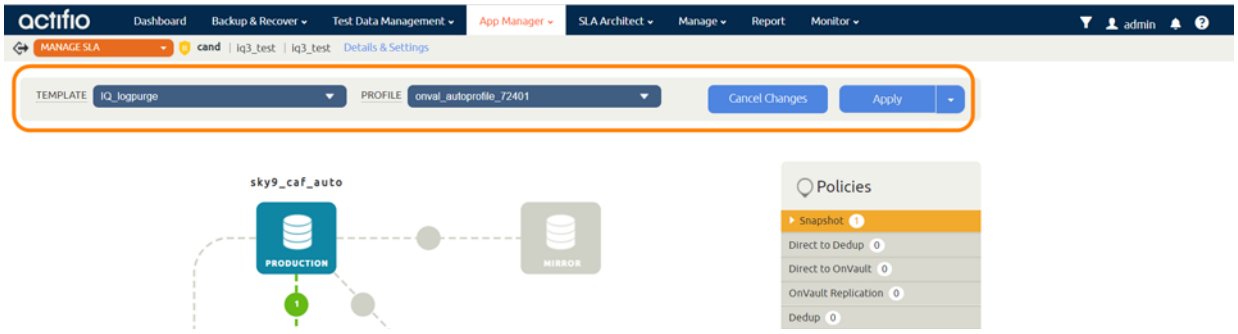
Protecting an SAP MaxDB Database

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**.

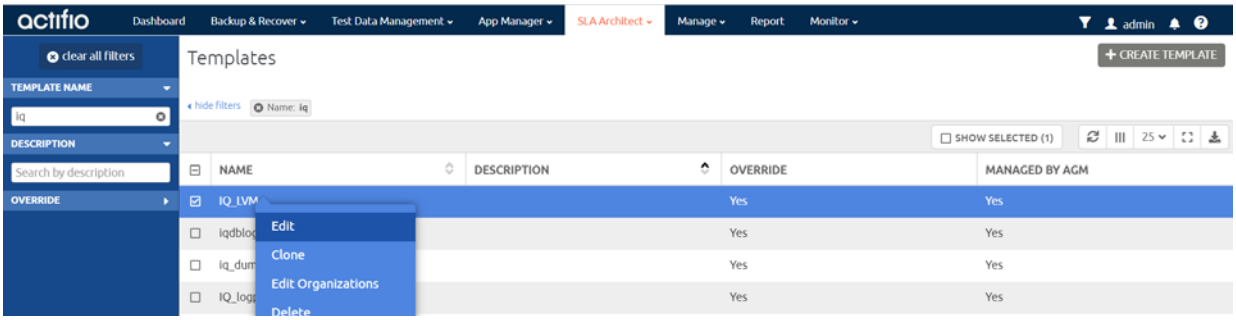


3. On the Apply SLA page, fill in the required field based on type of backup as detailed in Ensuring that the Backup Capture Method is Set Correctly on page 9.
4. Click **Save Changes**. The database appears in the App Manager Applications list with a green shield icon, and the database will be protected when the job runs according to the schedule in the template.

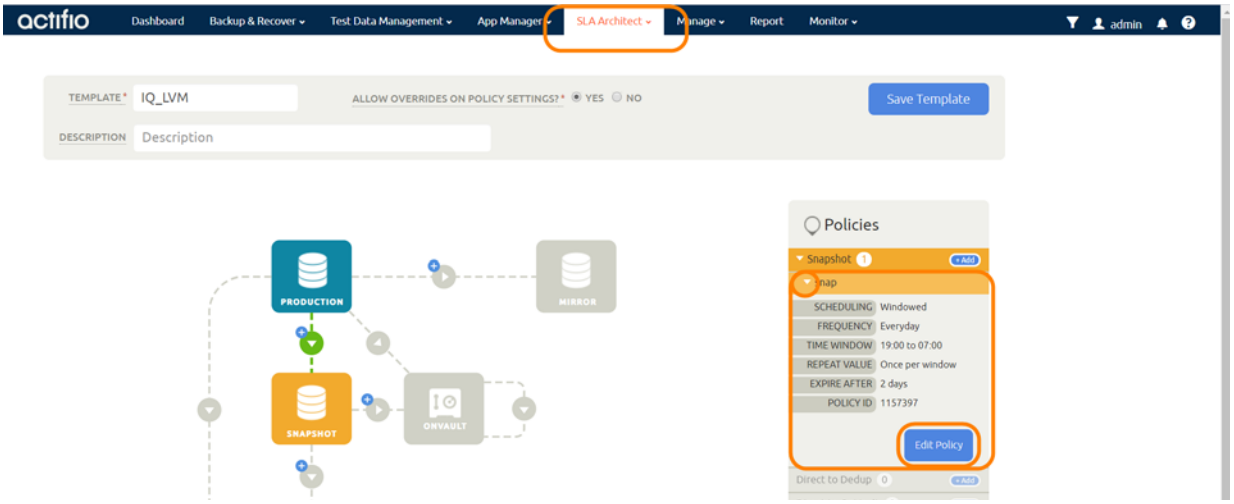
Protecting SAP MaxDB Database Logs

To enable and set up the SAP MaxDB database log backup:

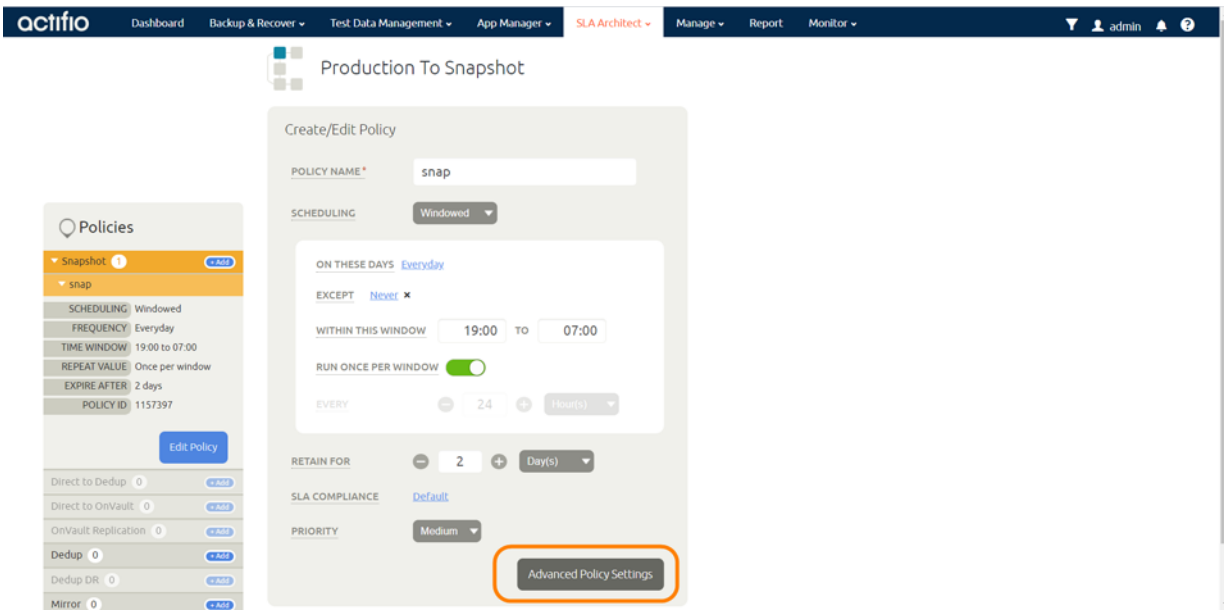
1. From the SLA Architect, Templates list, right-click the template for SAP MaxDB database protection and click **Edit**.



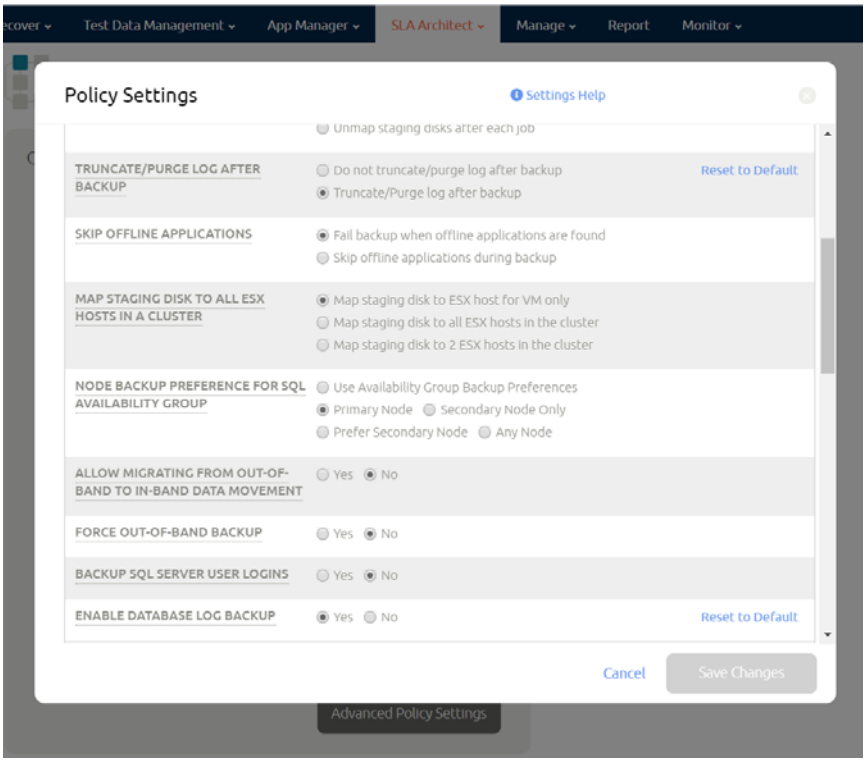
2. Click the arrow beside the Snapshot policy to open up the details, then click **Edit Policy**.



3. Near the bottom, select **Advanced Policy Settings**.



4. Set the log policy options (you will have to scroll to see them all):
    - Enable **Truncate/Purge log after backup**.
    - Set **Enable Database Log Backup** to **Yes**.
    - For **RPO (Minutes)**, enter the desired frequency of log backup.
    - Set **Log Backup Retention Period (in Days)** for point in time recovery.
    - Set **Replicate Logs (Uses StreamSnap Technology)** to **Yes** if you want to enable StreamSnap replication of log backup to a DR site.
    - Set **Send Logs to OnVault Pool** to **Yes** if you want the database logs to be sent to an OnVault Pool, enabling for point-in-time recoveries from OnVault on another site.



5. Click **Save Changes**.

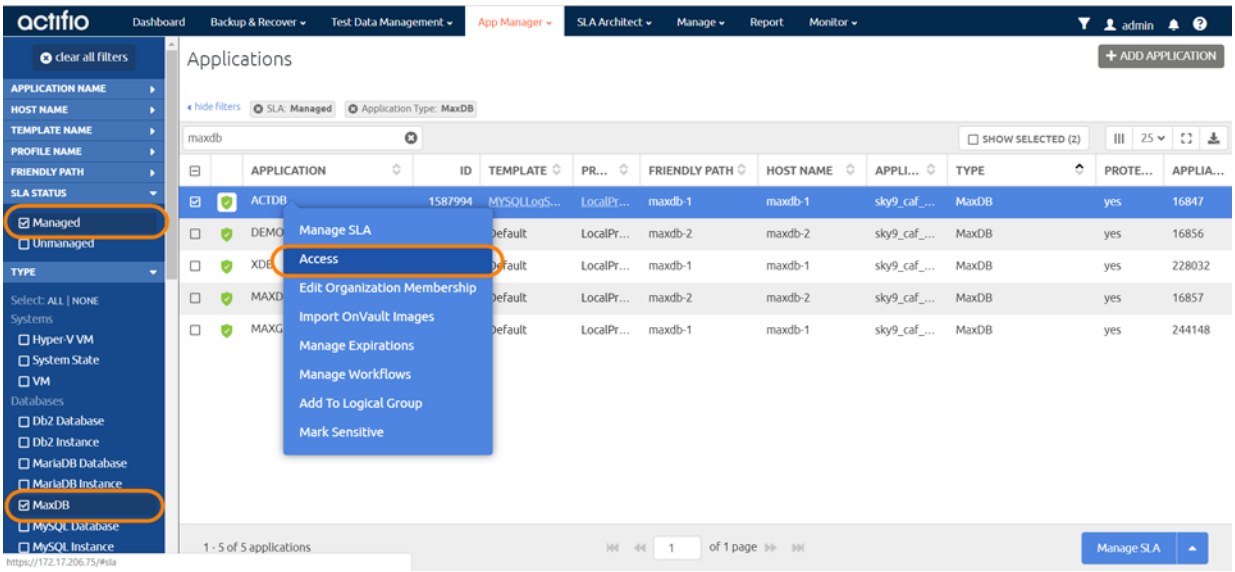
5 Restoring, Accessing, or Recovering an SAP MaxDB Database

This section describes:

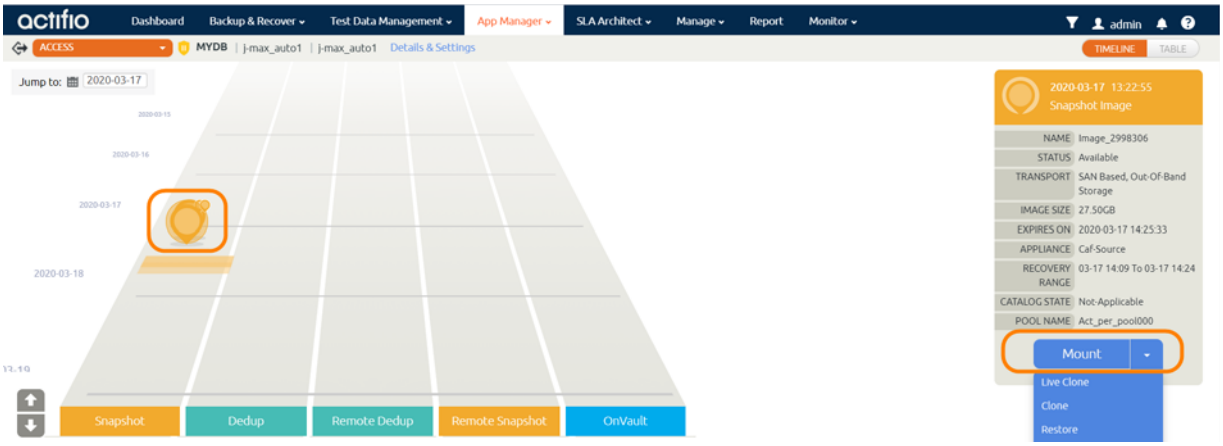
Mount and Refresh from Block-Based Volume Snapshot to a Target MaxDB Server as a Virtual Database

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

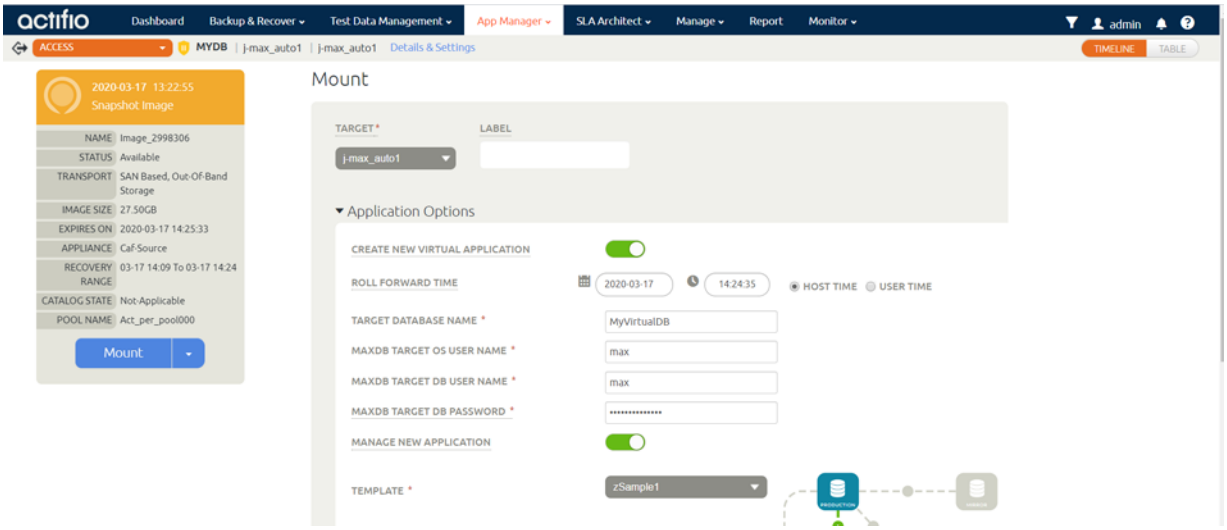
1. From the App Manager Applications list, right-click the protected database and select **Access**. You can use the Managed SLA Status filter to show only protected databases.



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



3. On the Mount page, from Target, choose the desired target MaxDB server from the dropdown.
4. Under Application Options, enable **Create New Virtual Application**.



5. For a database protected with log roll-forward, choose a target point in time.
6. Fill in:

   TARGET DATABASE NAME: The name of the target MaxDB database

   MAXDB TARGET OS USER NAME: OS user for target MaxDB instance

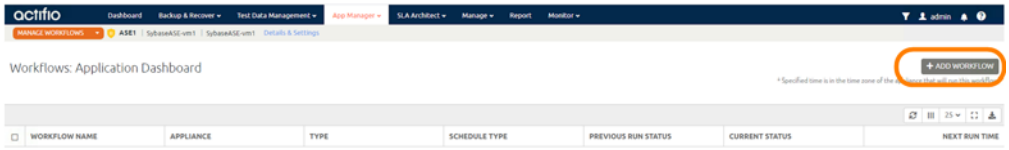
   MAXDB TARGET DB USER NAME: dbm user for target MaxDB

   MAXDB TARGET DB PASSWORD: dbm user password for target MaxDB
7. To protect the new virtual database, enable **Manage New Application**. Then choose a template and a resource profile to protect the database.
8. In Advanced Options, you can enter the **Home Directory** of the MaxDB database, and for **Overwrite Existing Database**, indicate when to overwrite a database on the target server that has the same name as the new database(s) being mounted: Yes, No, or Only if it's Stale.
9. Under Mapping Options:
   - Storage Pool: The image will be mounted in the Snapshot Pool unless you select a different one.
   - Mount Location: specify a target mount point to mount the new virtual database to.
10. Click **Submit**.

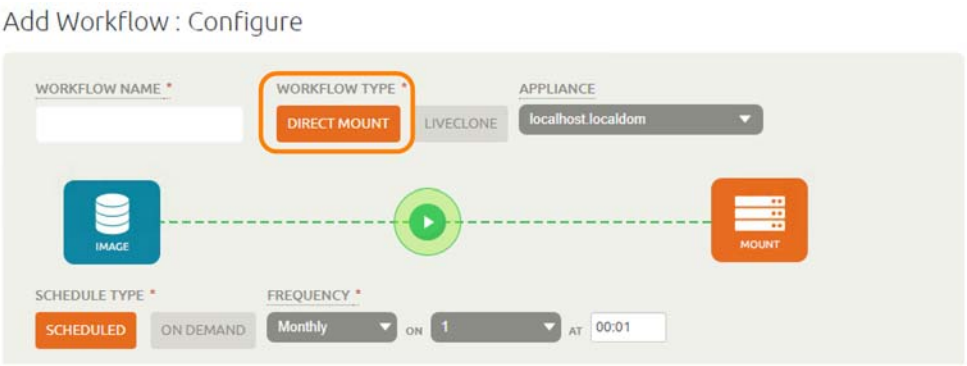
Refreshing a Virtual Database Using an Actifio Workflow

You can use a workflow to automate the process of mounting and refreshing a Db2 instance's databases from a snapshot.

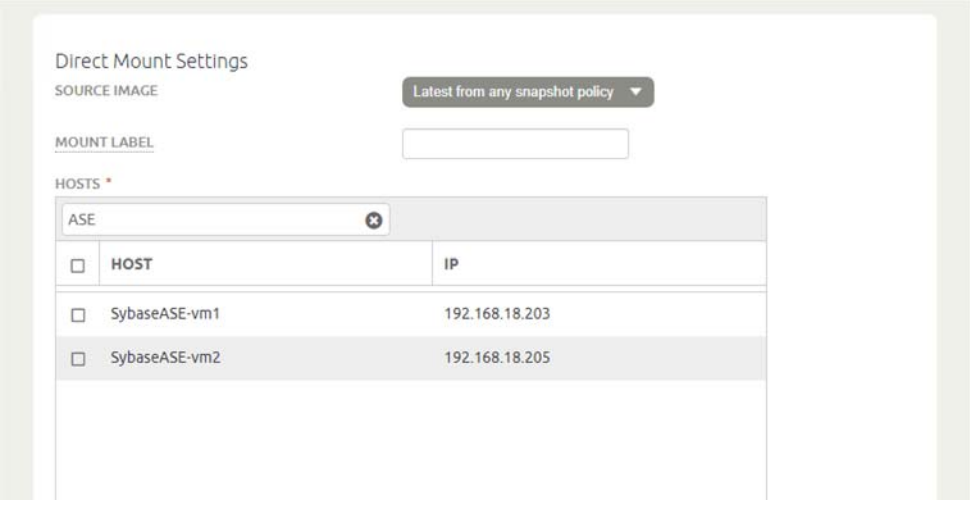
1. From the AGM App Manager, right-click the Db2 Instance and select **Manage Workflows**.
2. In the upper right corner of the Workflows: Application Dashboard page, click **+ Add Workflow**.



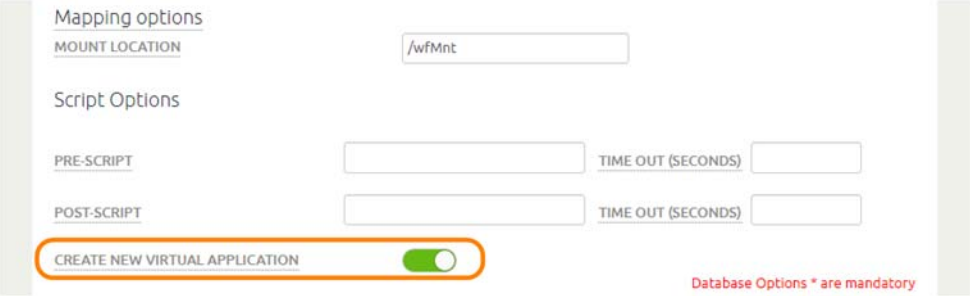
3. Specify:
   - Workflow Name: Enter a name for this workflow.
   - Workflow Type: Select **Direct Mount**.
   - Schedule Type: Choose Scheduled or On Demand based on your requirement. For a scheduled workflow, specify the frequency as well.



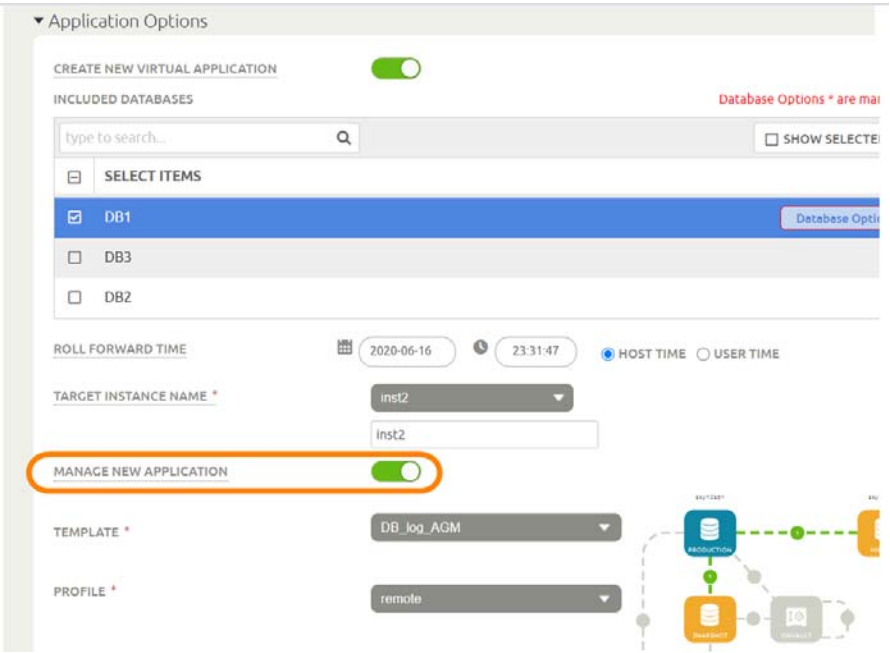
   - Source Image: Select based on requirements.
   - Mount Label: (Optional) Specify a mount label for the mounted image.
   - Hosts: Select the target host or hosts where the virtual Db2 instance database copy will be created.



- Mount Location: Specify a mount point to mount the data volumes and log volumes of the target.
- Pre-Script (optional): Specify a prescript name to be run before refresh. Pre scripts are detailed in ***Network Administrator's Guide to Actifio VDP***.
- Post-Script (optional): Specify a postscript name to be run at the end of refresh. Post scripts are detailed in ***Network Administrator's Guide to Actifio VDP***.
- Create New Virtual Application: Enable **Create New Virtual Application**.



- Select Items: Select the databases to refresh on target and specify the target dbname from 'Database Options' for each database.
- Target Instance Name: If the target instance is visible, select it. Otherwise specify the target instance name.



- Manage New Application: Enable **Manage New Application**.
- Template and Profile: Choose a template and a profile to protect the database.

4. Click **Add**. This will create an on-demand or scheduled workflow to create or refresh the Db2 Instance's database virtual copy.

Restoring and Recovering a MaxDB Database to the Source

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

Recovering from a Block-Based Volume Snapshot to the Source on page 21
Recovering from a File-Based Full+Incremental Backup to the Source on page 23

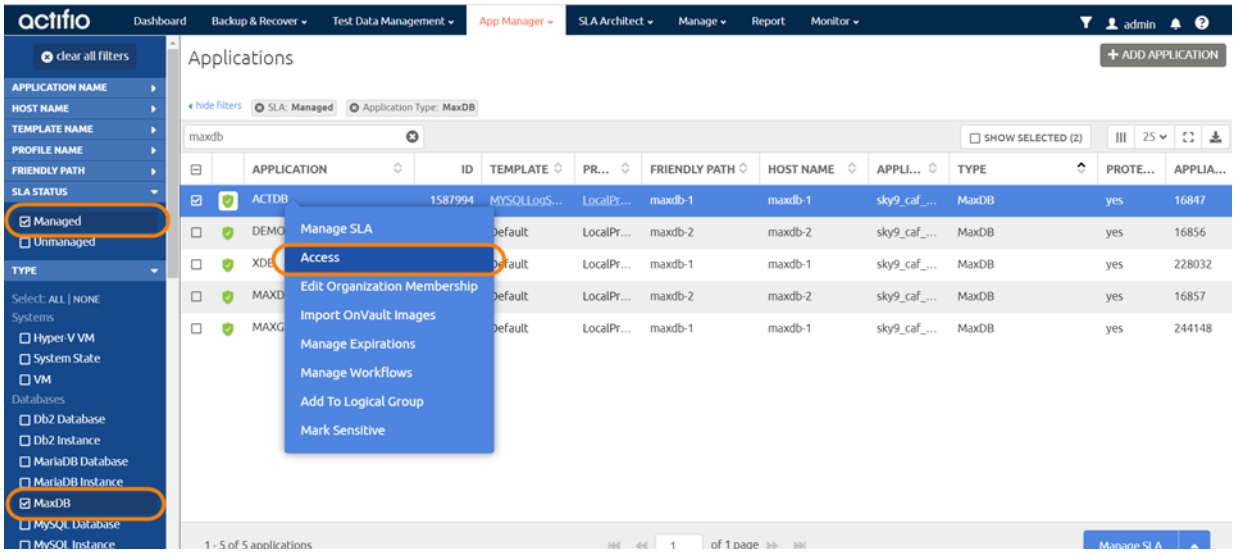
Recovering from a Block-Based Volume Snapshot to the Source

Use this procedure to restore and recover the source MaxDB database from a volume-based LVM snapshot image. This procedure uses physical recovery of the source data area.

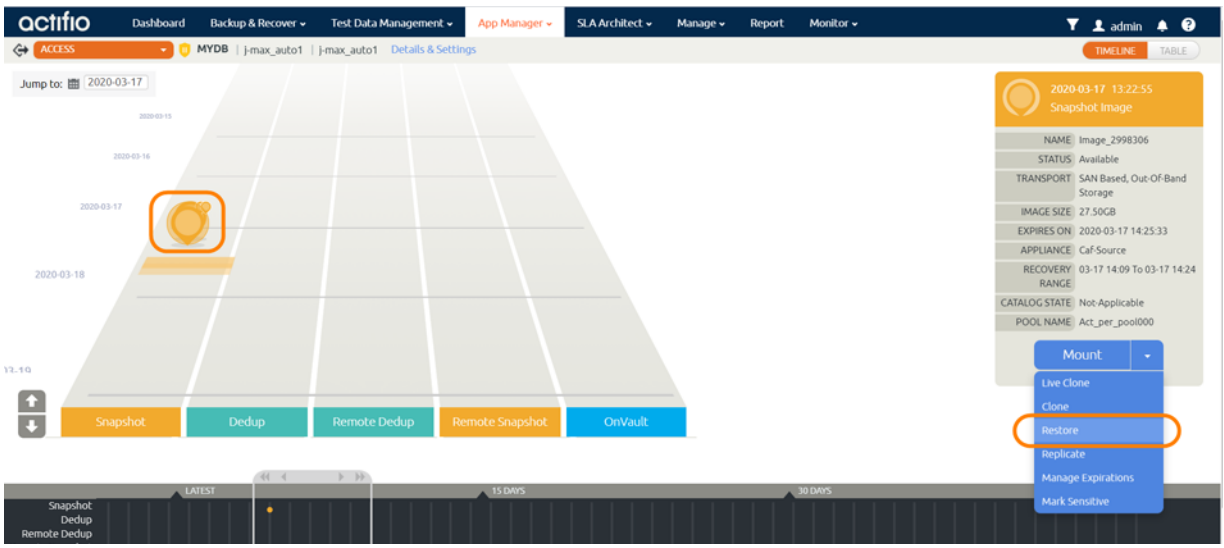
Note: *System databases on a root partition backed up as LVM Snapshots can be mounted as virtual databases, but they cannot be used in a traditional Restore operation as the root partition cannot be unmounted. This will need manual restore and recovery from a simple mount back to the same host.*

To recover a block-based image back to the source:

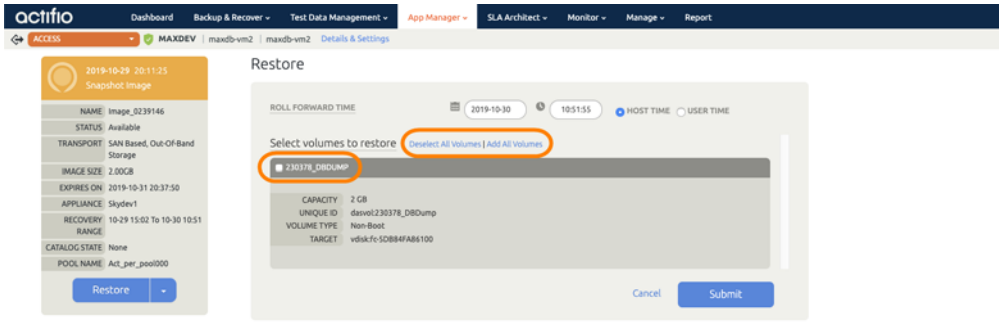
1. From the App Manager Applications list, right-click the protected database and select **Access**. You can use the Managed SLA Status filter to show only protected databases.



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.



4. Select one or more volumes to restore and click **Submit**.

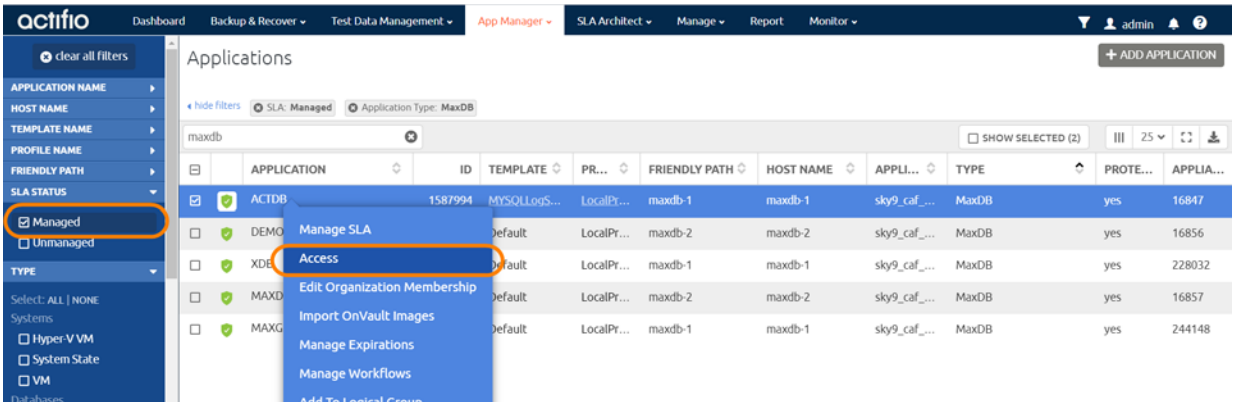
Recovering from a File-Based Full+Incremental Backup to the Source

Use this procedure to restore and recover the source MaxDB database from a traditional file-based full+incremental backup image. This procedure overwrites the source data. To recover a volume-base backup with CBT, see Recovering from a Block-Based Volume Snapshot to the Source on page 21.

Using this method, we can restore databases on a MaxDB Instance.

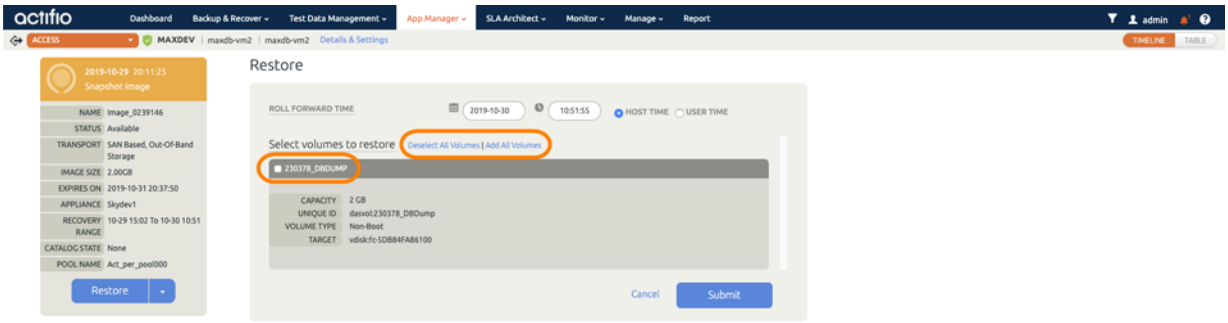
To recover back to the source, overwriting the source data:

1. From the App Manager Applications list, right-click the protected database and select **Access**. You can use the Managed SLA Status filter to show only protected databases.



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

3. For a database with multiple volumes, select some or all volumes to restore.



4. Click **Submit**. This will start the source database physical recovery using MaxDB recover commands.

Restoring a MaxDB Database to a New Target

Both of these procedures require you to customize and run a config file.

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

Restoring from a Block-Based Volume Snapshot to a New Target on page 24
Restoring from a File-Based Full+Incremental Backup to a New Target on page 27

Restoring from a Block-Based Volume Snapshot to a New Target

Before You Begin

This procedure requires you to customize and run `/var/act/scripts/ACT_MAXDB_lvmRestore_newTarget.conf`.

After the file has been edited, save it to `/act/custom_apps/maxdb/restore`.

These are the arguments in the config file, and where to get the values:

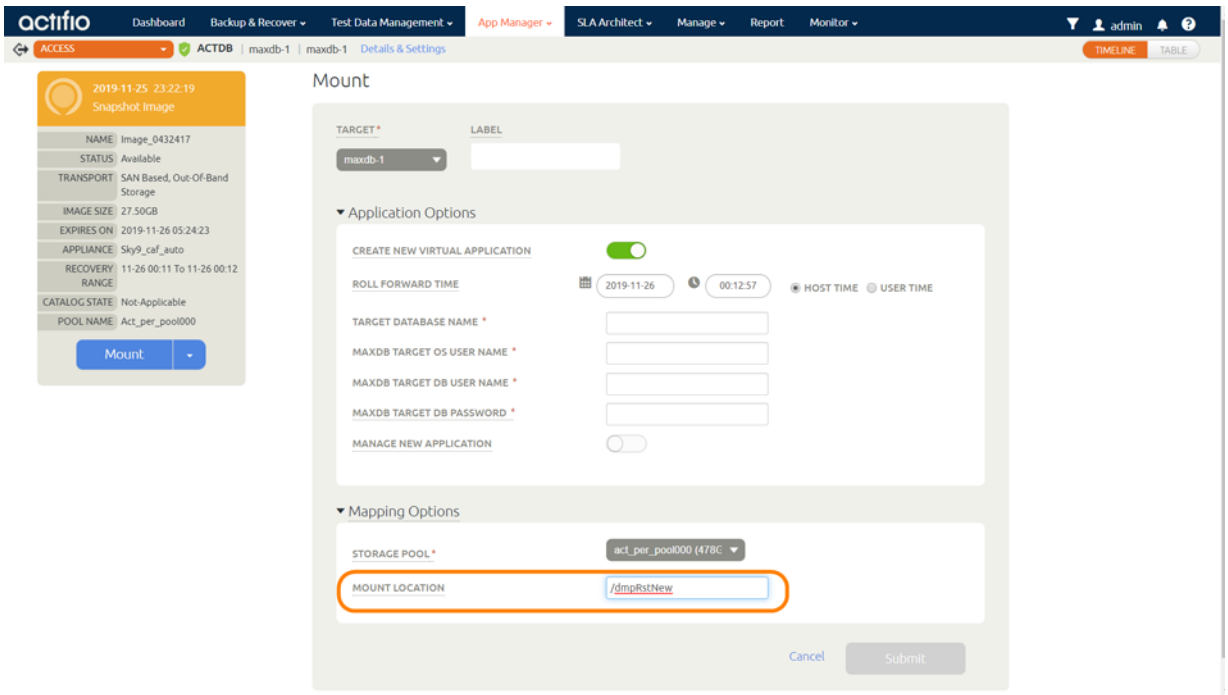
Argument	Description, or Code to Get the Value (run on the target server)
OSUSER	Target MAXDB OS User
SRC_DBSID	Source MAXDB SID of the source database to restore from
TARGET_DB_USER	Target MAXDB Instance DBM username and password. *These must be the same as source DBM username and password or restore and recovery will fail. You can change the password after restore is finished.*
TARGET_DBUSER_PASSWD	
TARGET_SERVER_NAME	Target MAXDB SID to restore
TARGET_MNT_PNT	This is the value that you will use in Step 3
UNTIL_TIME	Recovery Time in the format: YYYY-MM-DD HH24:MI:SS
MANIFEST_FILE_LOC	`cat /var/act/log/UDSAgent.log | grep <JOBID> | grep -i "Manifest_File_" | grep "/act/tmpdata/" | awk -F"disk at " '{print $2}'`
JobID	`cat /var/act/log/UDSAgent.log | grep -w <TARGET_MNT_PNT> | grep "GEN-INFO" | tail -1 | cut -d']' -f2 | cut -d' ' -f2`
LOG_BKP_MNTPT	`df -h | grep <TARGET_MNT_PNT> | grep "_archivelog" | awk '{print $NF}'`
BEGIN_TIME	`cat /var/act/log/UDSAgent.log | grep "BEGIN_TIME" | grep -w <TARGET_MNT_PNT> | awk -F"BEGIN_TIME=" '{ print $2 }' | cut -d' ' -f1-2 | cut -d'"' -f2`
SRC_DB_VERSION	`#dbmcli -d <SRC_DBSID> dbm_version | grep "VERSION" | awk -F"= " '{print $2}'`

Procedure

To restore a block-based Volume Level backup image to a new target:

1. From the App Manager Applications list, right-click the protected database and select **Access**. You can use the Managed SLA Status filter to show only protected databases.
2. Select the latest snapshot to recover, and choose **Mount**.

3. Provide a target mount point under mount location, for example: /dmpRstNew. This will be used as the variable TARGET_MNT_PNT.



The database backup will be mounted under /dmpRstNew (TARGET_MNT_PNT) and the log backup will be mounted under /dmpRstNew_archivelog (LOG_BKP_MNTPT).

4. Log into the database server as root. Change directory to /act/custom_apps/maxdb/restore:

```
#cd /act/custom_apps/maxdb/restore
```

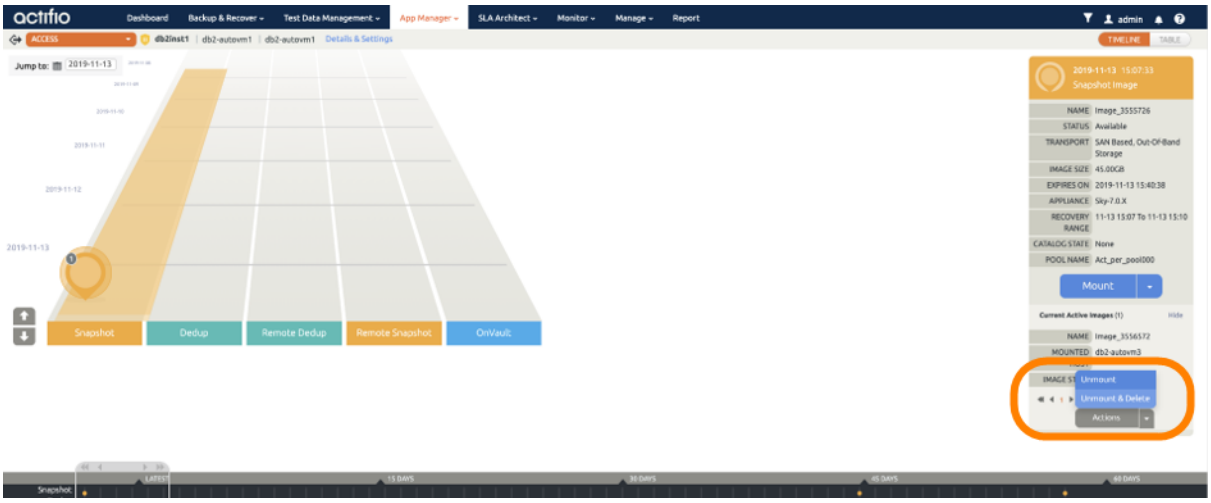
5. Run the ACT_MAXDB_lvmRestore_newTarget.sh config file as root user.

```
#sh ACT_MAXDB_lvmRestore_newTarget.sh
```

6. Connect to the MaxDB instance and confirm that the databases are recovered and online:

```
#dbmcli -d <TARGET_SERVER_NAME> -u <TARGET_DB_USER>,<TARGET_DBUSER_PASSWD> db_state
```

7. Unmount the mounted snapshot image.



To change the password

1. To change the password, login to the target db as DBM user:

```
#dbmcli -d TARGET_SERVER_NAME -u TARGET_DB_USER,TARGET_DBUSER_PASSWD
#user_changepwd dbm <new_password>
```

For example: for DBM user changing the password from welcome123 to welcome456

```
[root@maxdbtrg dump]# dbmcli -d glxn -u dbm,welcome123
dbmcli on glxn>
dbmcli on glxn>user_changepwd dbm welcome456
OK
---
dbmcli on glxn>
```

2. Login again with the new password.

```
[root@maxdbtrg dump]# dbmcli -d glxn -u dbm,welcome456
dbmcli on glxn>
```

Restoring from a File-Based Full+Incremental Backup to a New Target

Before You Begin

This procedure requires you to customize and run `/var/act/scripts/ACT_Maxdb_dumpRestore_newTarget.conf`.

After the file has been edited, save it to `/act/custom_apps/maxdb/dump`.

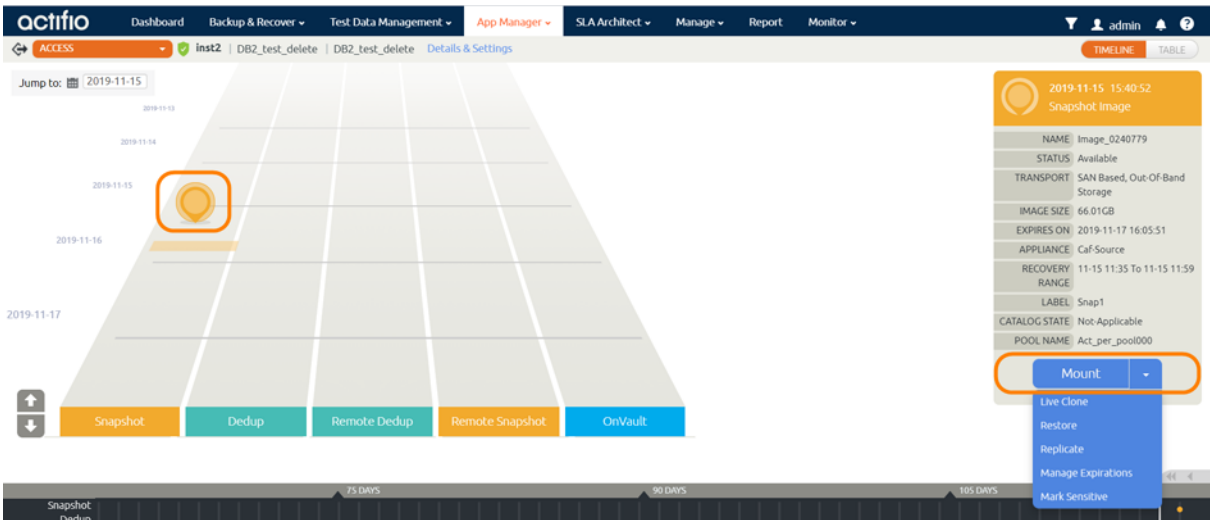
These are the arguments in the config file, and where to get the values:

Argument	Description, or Code to Get the Value (run on the target server)
OSUSER	Target MAXDB OS User
SRC_DBSID	Source MAXDB SID of the source database to restore from
TARGET_DB_USER	Target MAXDB Instance DBM username and password. *These must be the same as source DBM username and password or restore and recovery will fail. You can change the password after restore is finished.*
TARGET_DBUSER_PASSWD	
TARGET_SERVER_NAME	Target MAXDB SID to restore
DUMPBKPLOC	This is the value that you will use in Step 3
DBADMIN_PWD	DBADMIN Password for the target database
UNTIL_TIME	Recovery Time in the format: YYYY-MM-DD HH24:MI:SS
LOG_MNT_PNT	TargetDB log file mount point If target server directory structure is different from source
DATA_MNT_PNT	TargetDB data file mount point If target server directory structure is different from source
MANIFEST_FILE_LOC	`cat /var/act/log/UDSAgent.log | grep <JOBID> | grep -i "Manifest_File_" | grep "/act/tmpdata/" | awk -F"disk at " '{print $2}'`
JobID	`cat /var/act/log/UDSAgent.log | grep -w <DUMPBKPLOC> | grep "GEN-INFO" | tail -1 | cut -d']' -f2 | cut -d' ' -f2`
DUMPBKPLOC	`df -h | grep <DUMPBKPLOC> | grep "_archivelog" | awk '{print $NF}'`
LOG_BKP_MNTPT	`df -h | grep -w <DUMPBKPLOC> | grep "_archivelog" | awk '{print $NF}'`
BEGIN_TIME	`cat /var/act/log/UDSAgent.log | grep "BEGIN_TIME" | grep -w <DUMPBKPLOC> | awk -F"BEGIN_TIME=" '{ print $2 }' | cut -d' ' -f1-2 | cut -d'"' -f2`
SRC_DB_VERSION	`#dbmcli -d <SRC_DBSID> dbm_version | grep "VERSION" | awk -F"= " '{print $2}'`

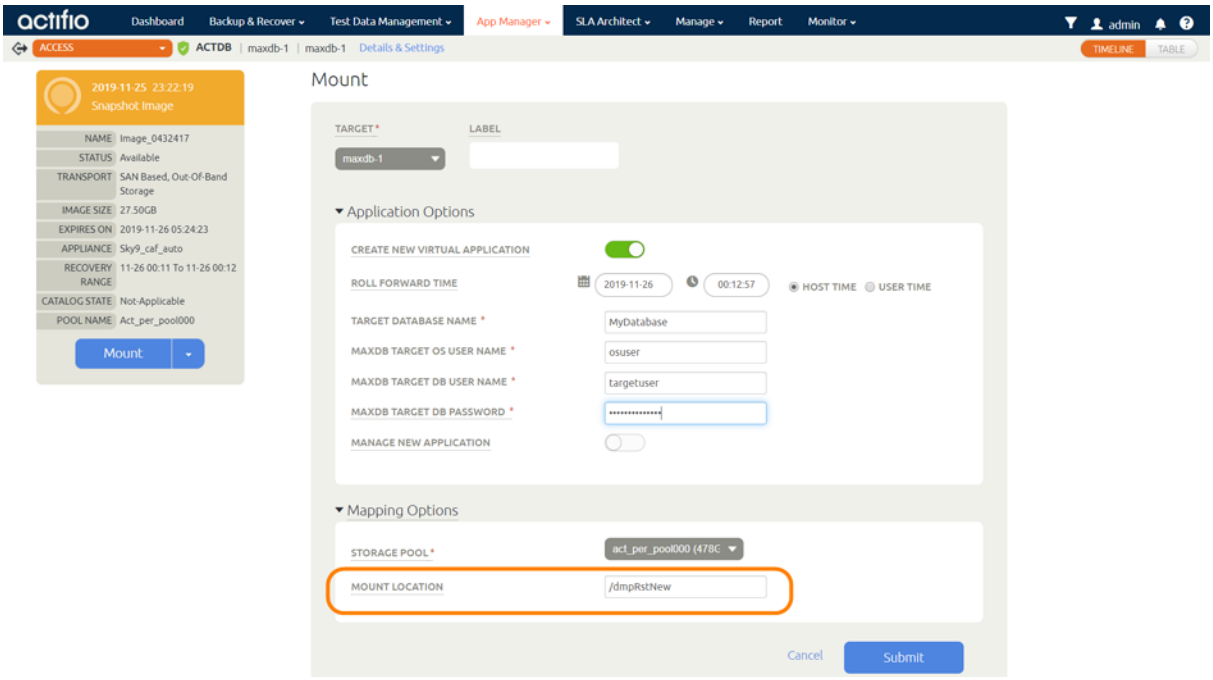
Procedure

To restore a traditional File-Based full+incremental backup image to a new target:

1. From the App Manager Applications list, right-click the protected database and select **Access**. You can use the Managed SLA Status filter to show only protected databases.
2. Select the latest snapshot to recover, and choose **Mount**.



3. Provide a target mount point under mount location, for example: /dmpRstNew. This will be used as the variable DUMPBKPLOC. The database backup will be mounted under /dmpRstNew (DUMPBKPLOC) and the log backup will be mounted under /dmpRstNew_archivelog (LOG_BKP_MNTPT).



4. Log into the database server as root and change directory to /act/custom_apps/maxdb/dump:

```
#cd /act/custom_apps/maxdb/dump
```

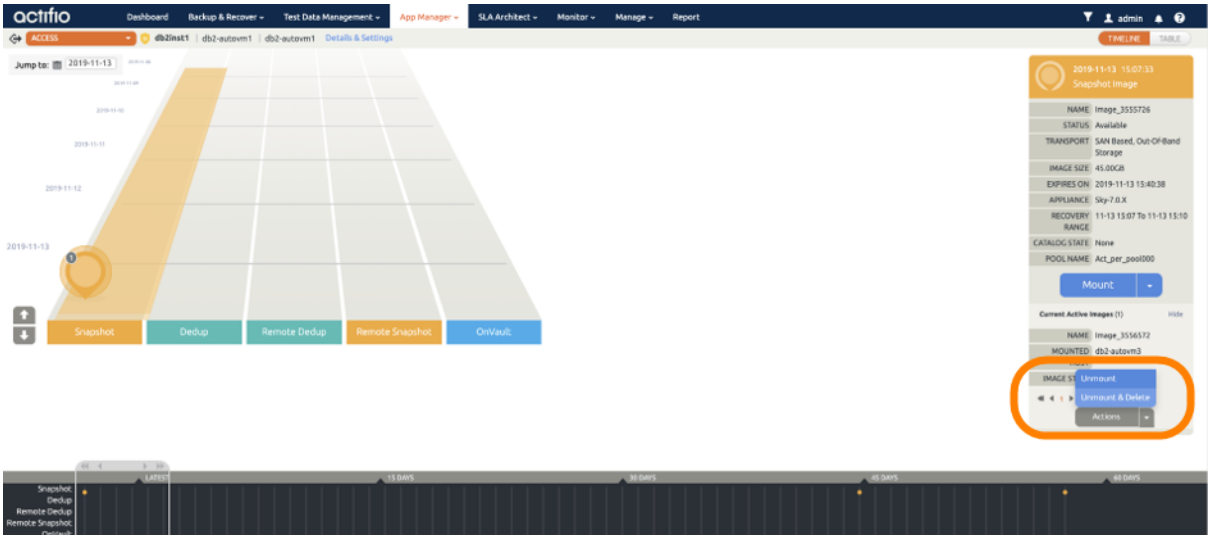
5. Run the ACT_MAXDB_dumpRestore_newTarget.sh config file as root user.

```
#sh ACT_MAXDB_dumpRestore_newTarget.sh
```

6. Connect to the MaxDB instance and confirm that the databases are recovered and online:

```
#dbmcli -d <TARGET_SERVER_NAME> -u <TARGET_DB_USER>,<TARGET_DBUSER_PASSWD> db_state
```

7. Unmount the mounted dump snapshot image.



To change the password

1. To change the password, login to the target db as DBM user:

```
#dbmcli -d TARGET_SERVER_NAME -u TARGET_DB_USER,TARGET_DBUSER_PASSWD
#user_changepwd dbm <new_password>
```

For example: for DBM user changing the password from welcome123 to welcome456

```
[root@maxdbtrg dump]# dbmcli -d glxn -u dbm,welcome123
dbmcli on glxn>
dbmcli on glxn>user_changepwd dbm welcome456
OK
---
dbmcli on glxn>
```

2. Login again with the new password.

```
[root@maxdbtrg dump]# dbmcli -d glxn -u dbm,welcome456
dbmcli on glxn>
```