IBM Db2 DBA's Guide to Actifio GO

Updated August 24, 2022

Copyright, Trademarks, and other Legal Matter

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 Copy Data Management*** and who are qualified to administer IBM Db2 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 the Actifio Virtual Data Pipeline for IBM Db2 Databases

This chapter introduces Actifio concepts and the procedures used to capture and access databases. It includes:

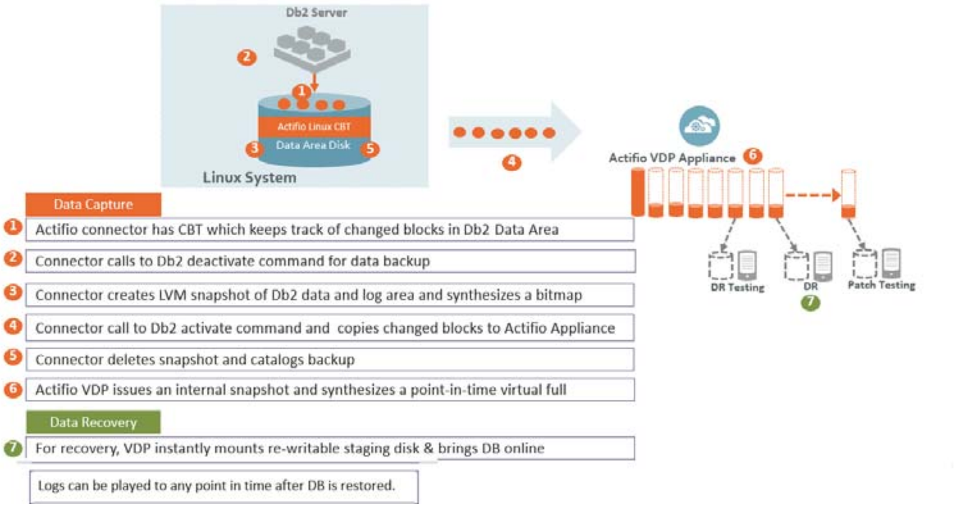
Actifio Data Virtualization

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.

Db2 is a is a family of relational database management systems within IBM's Information Management division that is centered on several relational database management system offerings. This section explains how to protect Db2 application consistent database data with Actifio VDP in Linux and AIX environments.

Db2 backup API used by Actifio:

- Linux CBT and LVM snapshot: Db2 database deactivate and activate API with Linux CBT and LVM snapshot
- IBM Spectrum Scale (GPFS) snapshot on AIX: Db2 database deactivate and activate API with GPFS snapshot on AIX.
- File-based backups: Db2 database API “Db2 backup db online” file-based backups provide full and incremental backups of the database in backup format. On recovery the restore db API recovers the database by physically overwriting the data area.
- Db2 log backup: Logs are flushed using “Db2 archive log for database”. During a log backup, the payload of the log segments is copied from the log area to the location specified by the parameter logarchmeth1.



Data Capture

1 Actifio connector has CBT which keeps track of changed blocks in Db2 Data Area

2 Connector calls to Db2 deactivate command for data backup

3 Connector creates LVM snapshot of Db2 data and log area and synthesizes a bitmap

4 Connector call to Db2 activate command and copies changed blocks to Actifio Appliance

5 Connector deletes snapshot and catalogs backup

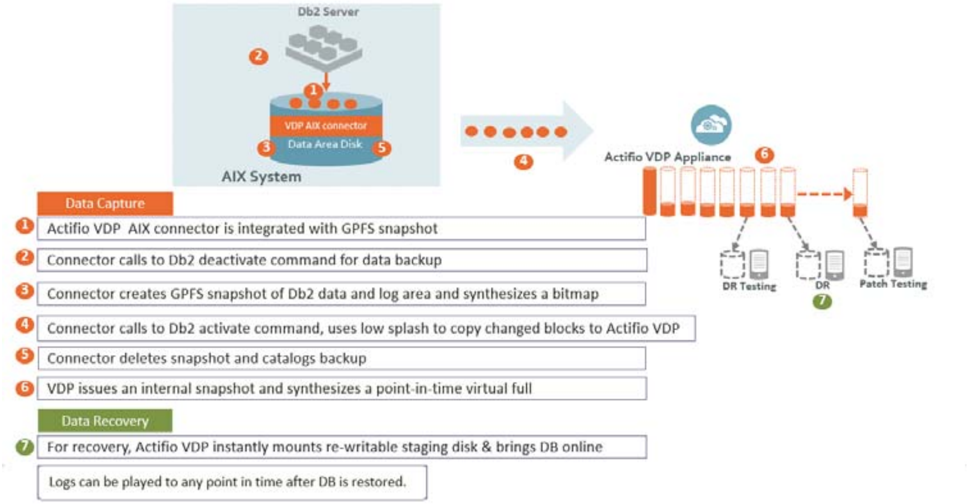
6 Actifio VDP issues an internal snapshot and synthesizes a point-in-time virtual full

Data Recovery

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

Logs can be played to any point in time after DB is restored.

Db2 with Actifio Volume-Based Backup with Linux CBT



Data Capture

1 Actifio VDP AIX connector is integrated with GPFS snapshot

2 Connector calls to Db2 deactivate command for data backup

3 Connector creates GPFS snapshot of Db2 data and log area and synthesizes a bitmap

4 Connector calls to Db2 activate command, uses low splash to copy changed blocks to Actifio VDP

5 Connector deletes snapshot and catalogs backup

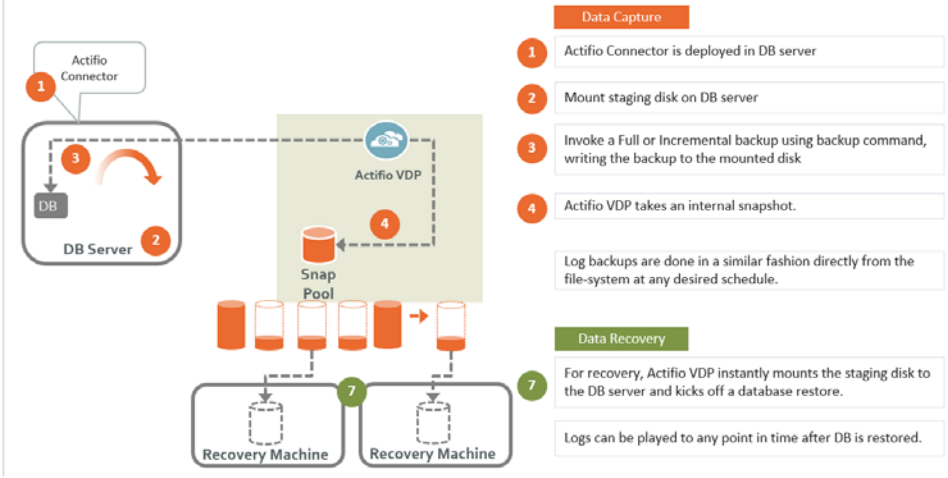
6 VDP issues an internal snapshot and synthesizes a point-in-time virtual full

Data Recovery

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

Logs can be played to any point in time after DB is restored.

Db2 with Actifio GPFS Snapshot on AIX



Data Capture

1 Actifio Connector is deployed in DB server

2 Mount staging disk on DB server

3 Invoke a Full or Incremental backup using backup command, writing the backup to the mounted disk

4 Actifio VDP takes an internal snapshot.

Log backups are done in a similar fashion directly from the file-system at any desired schedule.

Data Recovery

7 For recovery, Actifio VDP instantly mounts the staging disk to the DB server and kicks off a database restore.

Logs can be played to any point in time after DB is restored.

Db2 with Actifio File-Based Full+Incremental Backup

Capturing Data

Capturing data consists of four steps:

1. Add servers that host databases.
2. Discover the databases from AGM.
3. Define VDP Policy Templates and Resource Profiles according to your RPOs and RTOs.
4. Assign VDP Policy Templates and Resource Profiles to discovered databases.

The Actifio Connector

The Actifio Connector is used to capture selected databases. The Actifio Connector is a small-footprint, lightweight service that can be installed on either virtual or physical servers.

Specifically, the Actifio Connector:

- Creates an application to which data and log volumes will be added.
- Uses Linux changed block tracking to capture data at block level in incremental forever fashion.
- Identifies changes to database data for Actifio's incremental forever capture strategy.

Replicating Data

Data can be replicated to a second Actifio Appliance or to the cloud for recovery, disaster recovery, or test/development purposes.

Data replication has traditionally been an inhibitor to efficient data management in a geographically distributed environment. VDP replication:

- Drives down overall network usage.
- Eliminates the need for a dedicated WAN accelerator/optimizer.
- Does not require storage array vendor licenses as data is sent from one Actifio Appliance to another.
- Is heterogeneous from any supported array to any supported array: Tier 1 to Tier 2 and/or Vendor A to Vendor B.
- Preserves write-order, even across multiple LUNs.
- Is fully integrated with Actifio Resiliency Director.
- Encrypts data using the AES-256 encryption standard. Authentication between Actifio Appliances is performed using 1024-bit certificates.

Replication is controlled by Actifio Policy Template policies:

- Production to Mirror policies have several options to replicate data to a second Actifio Appliance.
- Production to Vault policies use a fixed, Actifio-proprietary replication engine to replicate data to the cloud.

Accessing Data

The Actifio Appliance can instantly present a copy of the database rolled forward to a specific point of time. The roll forward operation is performed from the Actifio Global Manager (AGM). Procedures for accessing databases images are described in Chapter 5, Accessing a Db2 Database as a Standard Mount or as a Refreshable Virtual Database.

Access options include:

Mounts
LiveClones
Restores
Workflows

Mounts

The Actifio VDP mount function provides instant access to data without moving data. Captured copies of databases can be rolled forward via the Actifio user interface and mounted on any database server.

LiveClones

The LiveClone is an independent copy of a snapshot image of data. LiveClones can be mounted and masked before being made available to users. A LiveClone can be refreshed incrementally from any snapshot when the source data changes (if the LiveClone data has been masked, the masking remains), allowing development and test teams to always work on the best set of data without having to manually manage the data and not access or interfere with the production data.

Restores

The restore function reverts the production data to a specified point in time. Restore operations actually move data. Typically restore operations are performed to restore a database to a valid state after a massive data corruption or storage array failure. The amount of time required to complete a restore operation depends on the amount of data involved.

Workflows

While SLAs govern the automated *capture* of a production database, Workflows automate *access* to the captured database.

Workflows are built with captured data. Workflows can present data as either a direct mount or as a LiveClone:

- Direct mounts (standard or application aware) work well for data that does not need to be masked prior to being presented. A mounted copy of data can be refreshed manually or on automatically on a schedule. Direct mounts allow you to instantly access captured data without actually moving the data.
- A LiveClone is a copy of your production data that can be updated manually or on a scheduled basis. You can mask sensitive data in a LiveClone prior to making it available to users.

Combining VDP's automated data capture and access control with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait for DBAs to update test and development environments, users can provision their own environments almost instantly.

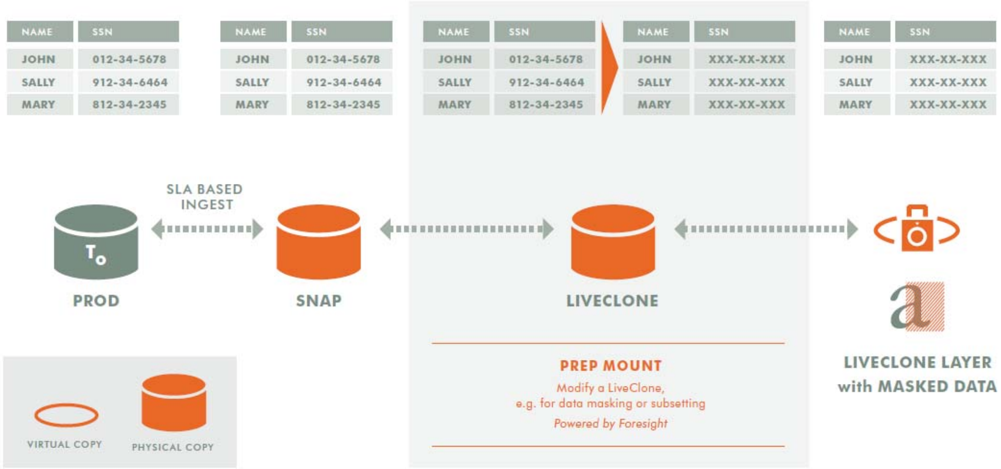
For example, an Actifio administrator can create an SLA Template Policy that captures data according to a specified schedule. Optionally, the administrator can mark the captured production data as sensitive and only accessible by users with the proper access rights.

After access rights have been defined and data has been captured, the administrator can create a Workflow that:

- Makes the captured data available as a LiveClone or as a direct mount
- Updates the LiveClone or mountable data on a scheduled or on-demand basis

- (Optional) Automatically applies scripts to the LiveClone's data after each update. This is useful for masking sensitive data.

Once the Workflow completes, users with proper access can provision their environments with the LiveClone or mountable data via the AGM.



NAME	SSN
JOHN	012-34-5678
SALLY	912-34-6464
MARY	812-34-2345

NAME	SSN
JOHN	012-34-5678
SALLY	912-34-6464
MARY	812-34-2345

NAME	SSN
JOHN	012-34-5678
SALLY	912-34-6464
MARY	812-34-2345

NAME	SSN
JOHN	XXX-XX-XXX
SALLY	XXX-XX-XXX
MARY	XXX-XX-XXX

NAME	SSN
JOHN	XXX-XX-XXX
SALLY	XXX-XX-XXX
MARY	XXX-XX-XXX

Workflow With Masked Social Security Data

2 Adding a Db2 Database Host and Discovering the Instance

Before You Begin

Each database must be using Automatic Storage Mode, or else only instances will be discovered.

Each database must be in Archive log mode. To learn if the database is in Circular mode or Archive log mode, run the command `#"db2 get db cfg for <database name>| grep LOGARCHMETH1"`

If the database is in Circular mode, then change the logging to Archive mode before continuing. To set the LOGARCHMETH1 parameter: `db2 update db cfg for <dbname> LOGARCHMETH1 using 'DISK:<location>'`

Overview

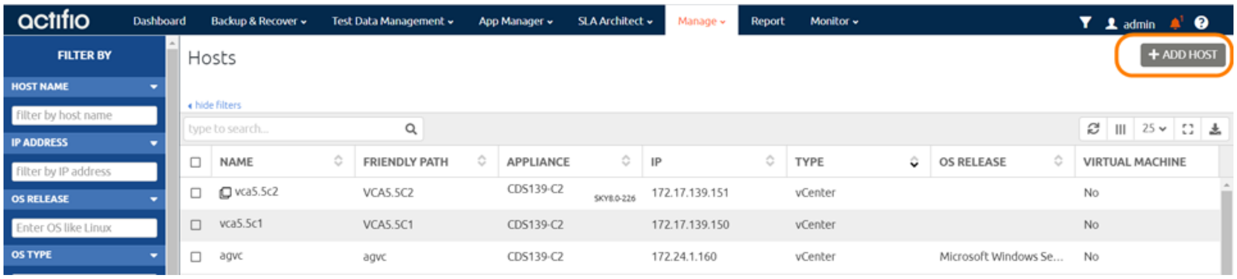
Before you can protect a Db2 database, you must add the host and discover the database. This requires:

1. Adding the Host to AGM on page 7
2. Discovering the Db2 Instance Application from the App Manager on page 9
3. Finding the Discovered Db2 Instance in the App Manager on page 9

Adding the Host to AGM

Add the host to AGM. If the host is already added then edit the host and make sure to set the Staging Disk Format correctly.

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



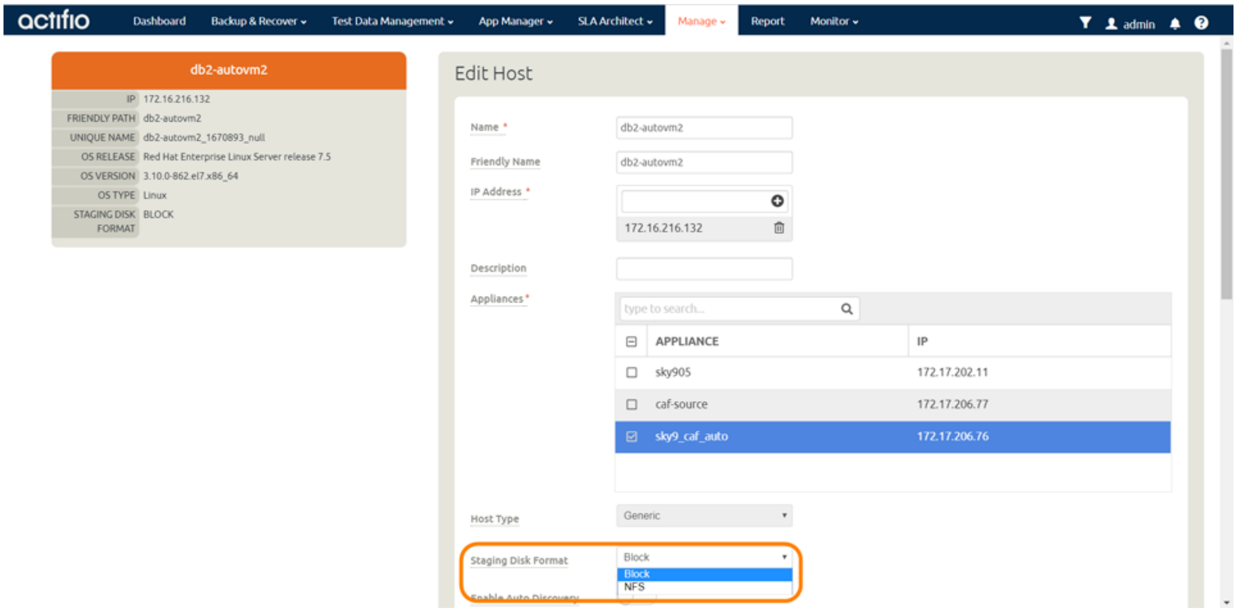
□	NAME	FRIENDLY PATH	APPLIANCE	IP	TYPE	OS RELEASE	VIRTUAL MACHINE
□	vca5.5c2	VCA5.5C2	CDS139-C2	172.17.139.151	vCenter		No
□	vca5.5c1	VCA5.5C1	CDS139-C2	172.17.139.150	vCenter		No
□	agvc	agvc	CDS139-C2	172.24.1.160	vCenter	Microsoft Windows Se...	No

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 Actifio Appliance that will manage the data.
   - 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:

   - **Block** -based staging disks are the most useful for both backup/recovery and TDM usage. Actifio changed-block tracking (CBT) is only available on block-based staging disks, and virtual databases can only be mounted to block-based staging disks.
   - **NFS** staging disks permit only traditional file-based backup with Full+Incremental file system backup. Select NFS only if Block is not an option in your network.



db2-autovm2

IP	172.16.216.132
FRIENDLY PATH	db2-autovm2
UNIQUE NAME	db2-autovm2_1670893_null
OS RELEASE	Red Hat Enterprise Linux Server release 7.5
OS VERSION	3.10.0-862.el7.x86_64
OS TYPE	Linux
STAGING DISK FORMAT	BLOCK

Edit Host

Name * db2-autovm2

Friendly Name db2-autovm2

IP Address * 172.16.216.132

Description

Appliances * type to search...

⊟	APPLIANCE	IP
□	sky905	172.17.202.11
□	caf-source	172.17.206.77
☑	sky9_caf_auto	172.17.206.76

Host Type Generic

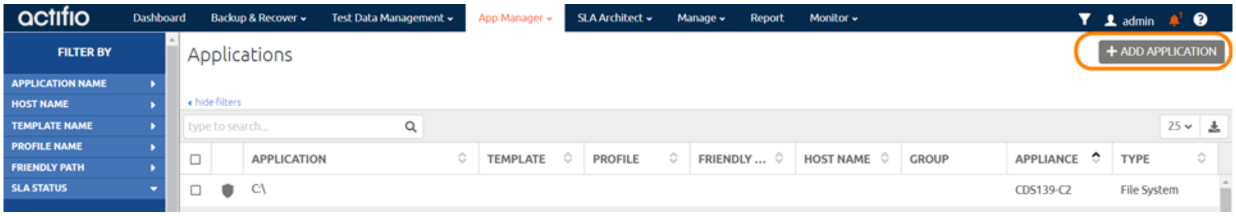
Staging Disk Format Block

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

Discovering the Db2 Instance Application from the App Manager

To discover and protect the Db2 database application:

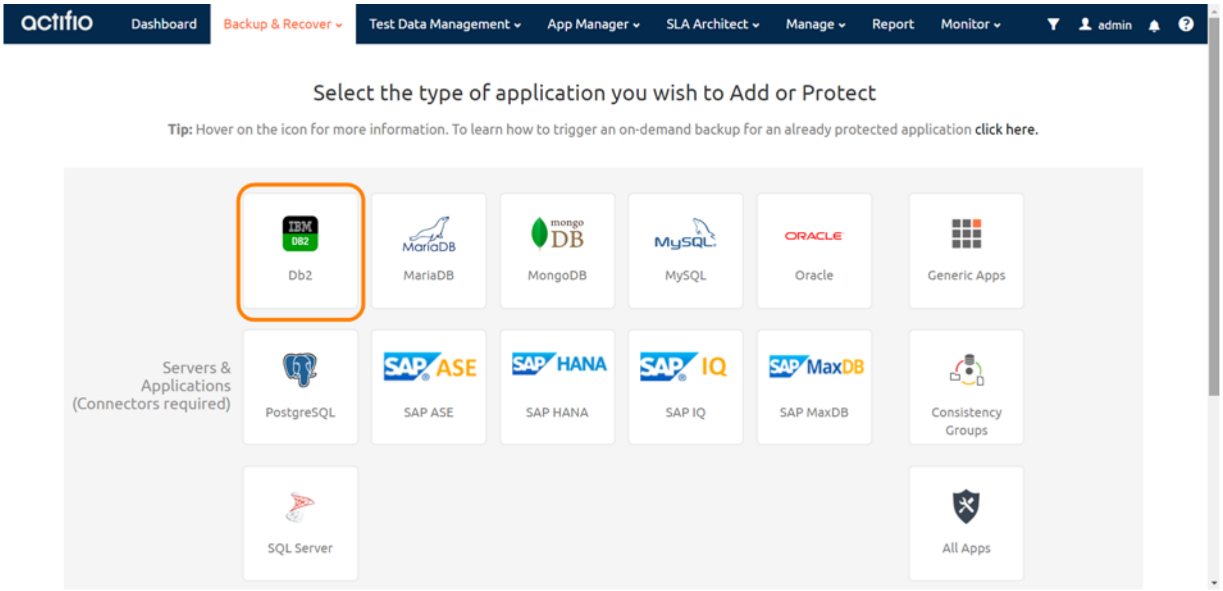
1. From the App Manager, Applications list, select **Add Application** in the upper right corner.



Applications

□		APPLICATION	TEMPLATE	PROFILE	FRIENDLY ...	HOST NAME	GROUP	APPLIANCE	TYPE
□		C:\						CDS139-C2	File System

2. In the Add Application wizard, select **Db2** and then follow the steps in the Wizard.

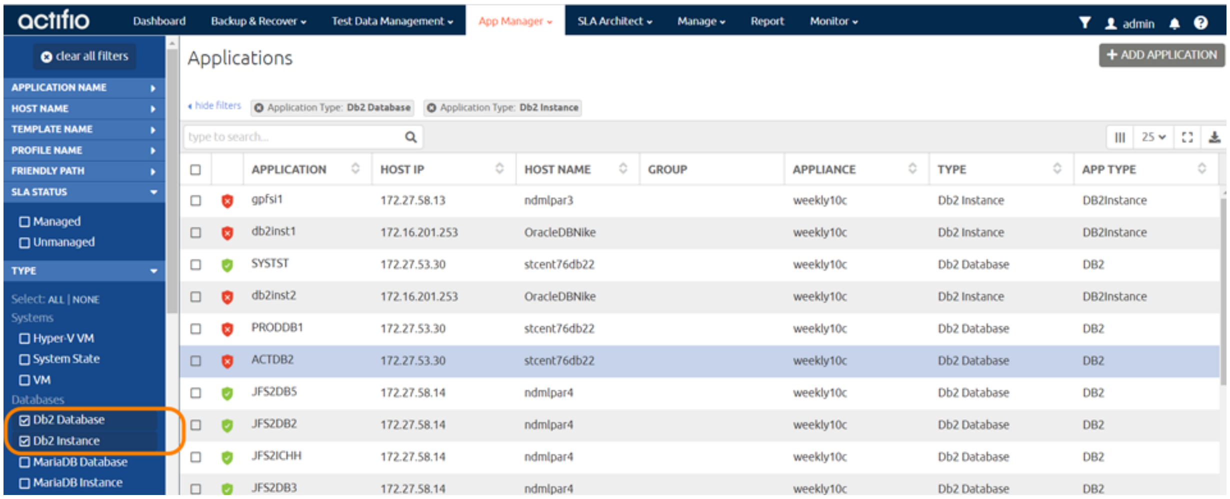


Select the type of application you wish to Add or Protect

Tip: Hover on the icon for more information. To learn how to trigger an on-demand backup for an already protected application **click here.**

Finding the Discovered Db2 Instance in the App Manager

To find the newly-discovered instance and its databases, go to the AGM App Manager Applications page. All applications known to the AGM of all types are listed. Use the Type application filter on left pane to show only Db2 instances and databases. The new Db2 instance will appear in the list as unmanaged (the red shield icon).



Applications

Application Type: **Db2 Database** Application Type: **Db2 Instance**

□ Managed
□ Unmanaged

□ Hyper-V VM
□ System State
□ VM

☑ Db2 Database
☑ Db2 Instance
□ MariaDB Database
□ MariaDB Instance

□		APPLICATION	HOST IP	HOST NAME	GROUP	APPLIANCE	TYPE	APP TYPE
□	🟥	gpfsi1	172.27.58.13	ndmlpar3		weekly10c	Db2 Instance	DB2Instance
□	🟥	db2inst1	172.16.201.253	OracleDBNike		weekly10c	Db2 Instance	DB2Instance
□	🟩	SYSTST	172.27.53.30	stcent76db22		weekly10c	Db2 Database	DB2
□	🟥	db2inst2	172.16.201.253	OracleDBNike		weekly10c	Db2 Instance	DB2Instance
□	🟥	PRODDB1	172.27.53.30	stcent76db22		weekly10c	Db2 Database	DB2
□	🟥	ACTDB2	172.27.53.30	stcent76db22		weekly10c	Db2 Database	DB2
□	🟩	JFS2DB5	172.27.58.14	ndmlpar4		weekly10c	Db2 Database	DB2
□	🟩	JFS2DB2	172.27.58.14	ndmlpar4		weekly10c	Db2 Database	DB2
□	🟩	JFS2ICHH	172.27.58.14	ndmlpar4		weekly10c	Db2 Database	DB2
□	🟩	JFS2DB3	172.27.58.14	ndmlpar4		weekly10c	Db2 Database	DB2

3 Configuring the SLA, Including the Backup Method

After the instance is prepared and discovered as explained in Chapter 2, Adding a Db2 Database Host and Discovering the Instance, you must configure the Actifio SLA for the instance, including the backup method.

The procedures for developing SLAs are detailed in the AGM online help. This chapter provides additional information of value to the Db2 DBA.

Protection is set for the entire Db2 Instance. You can include/exclude specific databases during the process using a Database Inclusion Rule from the Manage SLA page.

The backup method is limited by the staging disk format set in Adding the Host to AGM on page 7:

- **Block**-based staging disks are the most useful for both backup/recovery and TDM usage. Actifio changed-block tracking (CBT) is only available on block-based staging disks, and virtual databases can only be mounted to block-based staging disks. Block-based staging disks can be used for both volume-level and full+incremental file-based backups.
- **NFS** staging disks permit only traditional file-based backup with Full+Incremental file system backup. Select NFS only if Block is not an option in your network.

You choose between two very different backup methods in the Application Details & Settings:

- **Use volume level backup**: Use volume level LVM snapshots with CBT on Linux to a block-based staging disk. This option enables you to create application-aware virtual databases from the snapshot images. The production instance/database must be present on the LVM volume. GPFS on AIX will use volume-level GPFS snapshots with low-splash backups.
- **Use full+incremental backup**: This is the traditional file-based backup and recovery. This “file dump” method does not support the creation of virtual databases. You can select this for both Block and NFS staging disks, but if you can use block-based staging disks you probably should.

Note: *With one exception, protection is set for the entire Db2 instance. You can include/exclude specific databases during the process using a Database Inclusion Rule from the Manage SLA pages.*
The exception: A virtual database can be protected individually.

Whichever method you select involves these steps:

Ensuring that the Staging Disk Format is Set Correctly on page 12

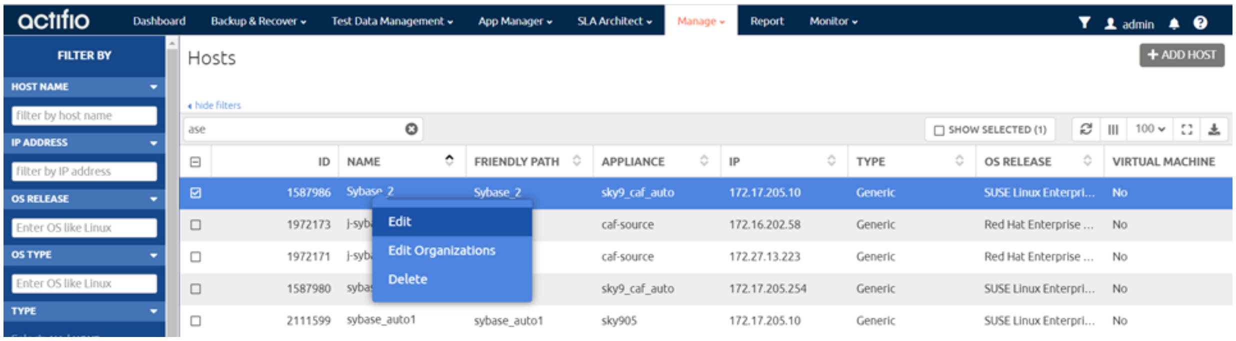
Configuring the Backup Capture Method and Other SLA Settings on page 13

Setting the Schedule for Dumps on page 15

Ensuring that the Staging Disk Format is Set Correctly

To check the staging disk format:

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



Hosts

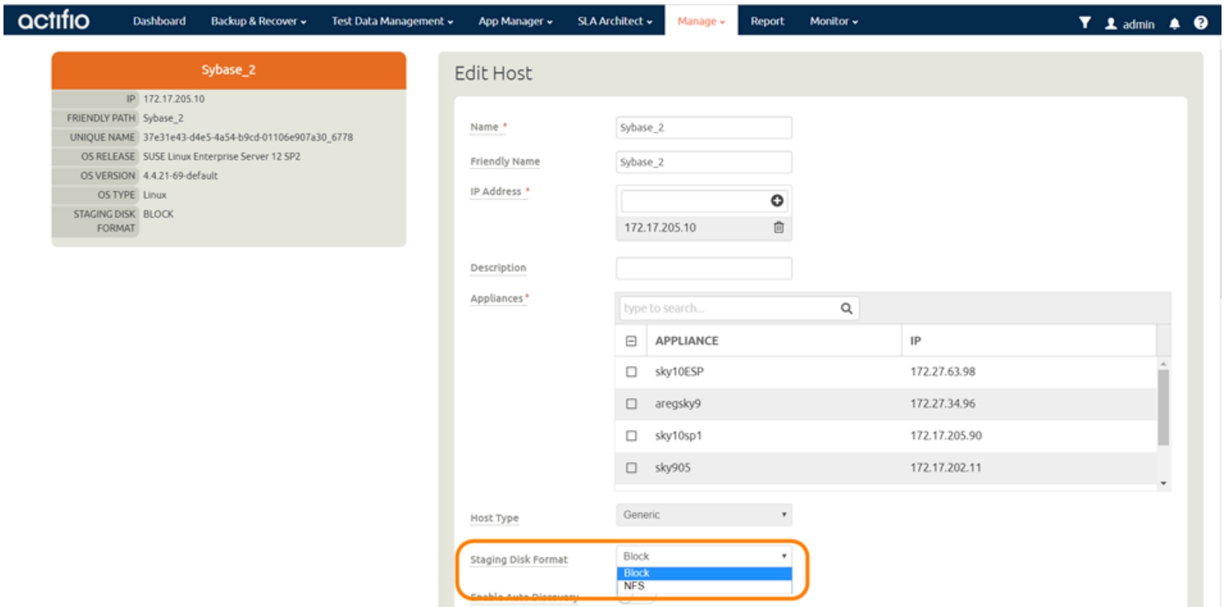
ase

	ID	NAME	FRIENDLY PATH	APPLIANCE	IP	TYPE	OS RELEASE	VIRTUAL MACHINE
☑	1587986	Sybase_2	Sybase_2	sky9_caf_auto	172.17.205.10	Generic	SUSE Linux Enterpri...	No
□	1972173	j-syb		caf-source	172.16.202.58	Generic	Red Hat Enterprise ...	No
□	1972171	j-syb		caf-source	172.27.13.223	Generic	Red Hat Enterprise ...	No
□	1587980	sybas		sky9_caf_auto	172.17.205.254	Generic	SUSE Linux Enterpri...	No
□	2111599	sybase_auto1	sybase_auto1	sky905	172.17.205.10	Generic	SUSE Linux Enterpri...	No

2. Halfway down the Edit Host page, the Staging Disk Format is either **NFS** or **Block**:

   - **Block**-based staging disks are the most useful for both backup/recovery and TDM usage. Actifio changed-block tracking (CBT) is only available on block-based staging disks, and virtual databases can only be mounted to block-based staging disks.

   - **NFS** staging disks permit only traditional file-based backup with Full+Incremental file system backup. Select NFS only if Block is not an option in your network.



Sybase_2

IP	172.17.205.10
FRIENDLY PATH	Sybase_2
UNIQUE NAME	37e31e43-d4e5-4a54-b9cd-01106e907a30_6778
OS RELEASE	SUSE Linux Enterprise Server 12 SP2
OS VERSION	4.4.21-69-default
OS TYPE	Linux
STAGING DISK FORMAT	BLOCK

Edit Host

Name * Sybase_2

Friendly Name Sybase_2

IP Address * 172.17.205.10

Description

Appliances* type to search...

	APPLIANCE	IP
□	sky10ESP	172.27.63.98
□	aregsky9	172.27.34.96
□	sky10sp1	172.17.205.90
□	sky905	172.17.202.11

Host Type Generic

Staging Disk Format Block

Enable Auto Discovery

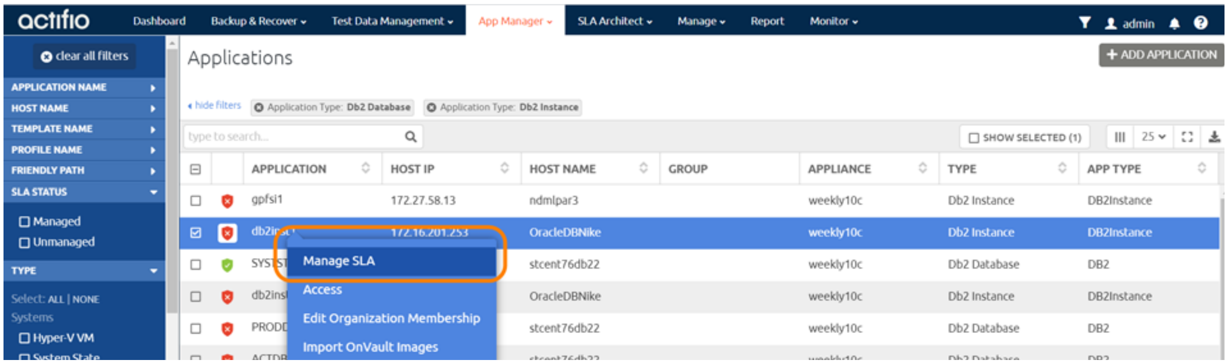
3. If the staging disk format is set incorrectly, change it now and click **Save** before continuing.

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 standard mount back to the same host.*

Configuring the Backup Capture Method and Other SLA Settings

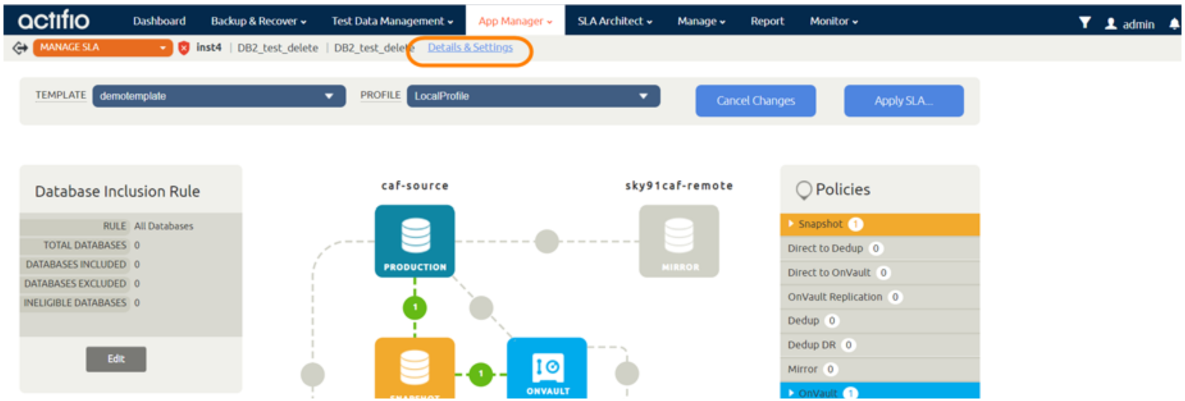
To configure the database SLA settings:

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



	APPLICATION	HOST IP	HOST NAME	GROUP	APPLIANCE	TYPE	APP TYPE
□	gpfsi1	172.27.58.13	ndmlpar3		weekly10c	Db2 Instance	DB2Instance
☑	db2inst	172.16.201.253	OracleDBNike		weekly10c	Db2 Instance	DB2Instance
□	SYSTST		stcent76db22		weekly10c	Db2 Database	DB2
□	db2ins		OracleDBNike		weekly10c	Db2 Instance	DB2Instance
□	PRODD		stcent76db22		weekly10c	Db2 Database	DB2

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



TEMPLATE demotemplate

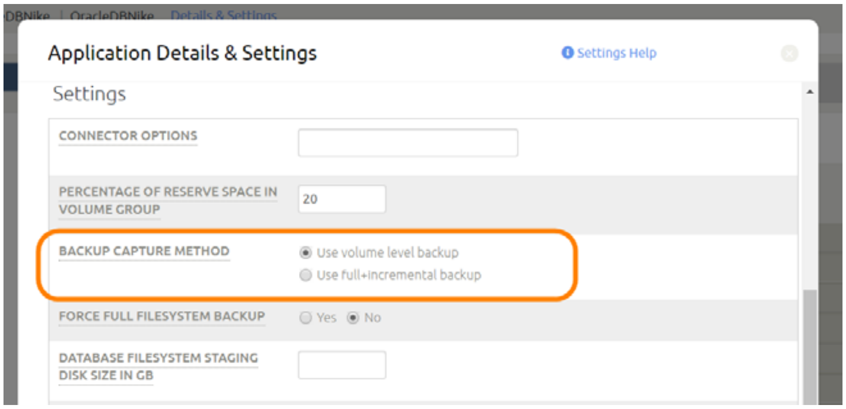
PROFILE LocalProfile

Database Inclusion Rule

RULE	All Databases
TOTAL DATABASES	0
DATABASES INCLUDED	0
DATABASES EXCLUDED	0
INELIGIBLE DATABASES	0

This opens the details and settings for this specific instance. Of particular importance is **Backup Capture Method**:

- **Use volume level backup**: Use volume level LVM snapshots with CBT on Linux to a block-based staging disk. This highly-efficient option enables you to create application-aware virtual databases from the snapshot images
- **Use full+incremental backup**: This is traditional file-based backup and recovery. This "file dump" method does not support creation of virtual databases. If you are required to use NFS staging disks, then you must use this backup method. You can select this method for use with Block staging disks, which also support the better volume-level backup method.


DBNike | OracleDBNike Details & Settings
Application Details & Settings
Settings Help
Settings

CONNECTOR OPTIONS	
PERCENTAGE OF RESERVE SPACE IN VOLUME GROUP	20
BACKUP CAPTURE METHOD	● Use volume level backup ○ Use full+incremental backup
FORCE FULL FILESYSTEM BACKUP	○ Yes ● No
DATABASE FILESYSTEM STAGING DISK SIZE IN GB	

3. Fill in the details and setting according to the backup method that you need:

Table 1: Db2 Details & Settings

Setting	**Block-Based LVM Snapshot with CBT on Linux**	**Block-Based GPFS Snapshot on AIX**	**File-Based Backup and Recovery, Block *or* NFS**
Use Staging Disk Granularity as Minimum Staging Disk Size	Use this for applications that are under the size of the granularity setting and that tend to periodically grow. This 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 default 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
Force Full Filesystem Backup	Not applicable		Set to Yes if you want an on-demand full backup
Database Filesystem Staging Disk Size in GB	Not applicable		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 logs older than <value> * 24 hours will be purged. For example, if this is set to 4 days, then 96 hours of logs are kept. The default value is 2 days.		
Script Timeout	The timeout value (in seconds) is applied to internal backup and recovery scripts called by connector. The default value is 172800 (48 hours).		

File-based backup requires the dump schedule to be configured. See Setting the Schedule for Dumps.

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 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 Db2 application.

Replace "FIIIIII" as needed. To run full backups on Tuesday, set `dumpschedule to "IIFIIII"`

4 Protecting the Db2 Instance and its Logs

After the SLA is configured as detailed in Chapter 3, Configuring the SLA, Including the Backup Method, you can configure a VDP backup method for the Db2 instance.

This chapter includes:

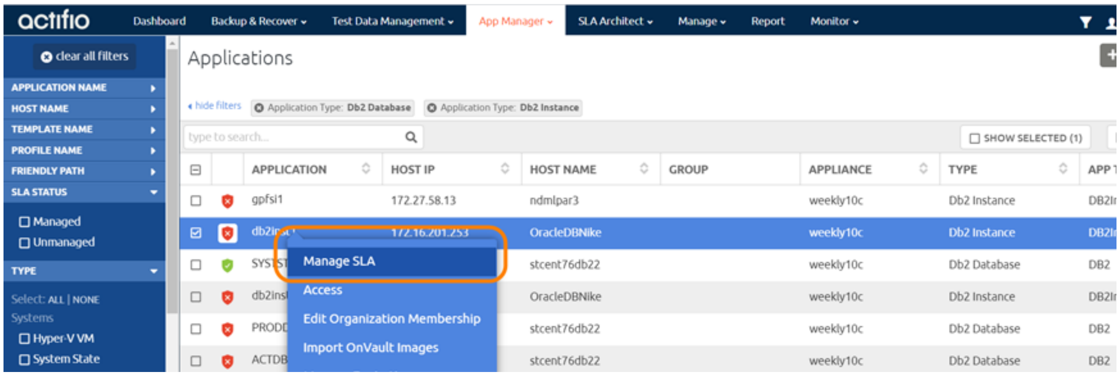
Note: *With one exception, protection is set for the entire Db2 instance. You can include/exclude specific databases during the process using a Database Inclusion Rule from the Manage SLA page.*
The exception is that virtual databases can be protected separately from the instance when created.

Protecting an IBM Db2 Instance

Database instance protection can be done from either the Primary node or from HADR nodes. To protect from the Db2 HADR node, the node must be read-enabled: ensure that the parameter `DB2_HADR_ROS=ON`.

To protect the Db2 instance:

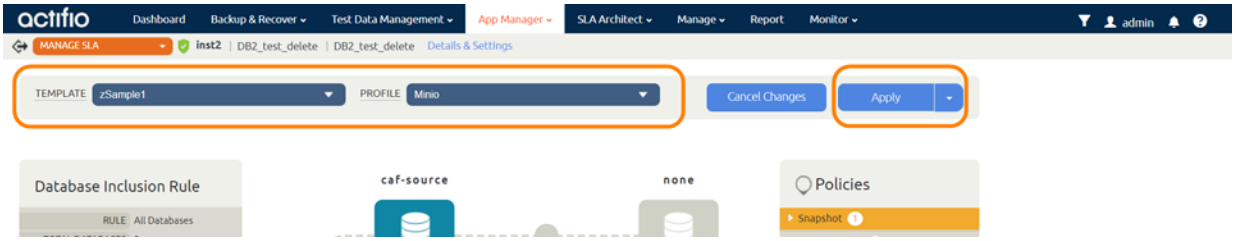
1. From the App Manager, Applications list, right-click the instance and select **Manage SLA**.



Application Type: Db2 Database
Application Type: Db2 Instance

	APPLICATION	HOST IP	HOST NAME	GROUP	APPLIANCE	TYPE	APP T
□	gpfsi1	172.27.58.13	ndmlpar3		weekly10c	Db2 Instance	DB2In
☑	db2in	172.16.201.253	OracleDBNike		weekly10c	Db2 Instance	DB2In
□	SYSTS		stcent76db22		weekly10c	Db2 Database	DB2
□	db2inst		OracleDBNike		weekly10c	Db2 Instance	DB2In
□	PRODD		stcent76db22		weekly10c	Db2 Database	DB2
□	ACTDB		stcent76db22		weekly10c	Db2 Database	DB2

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



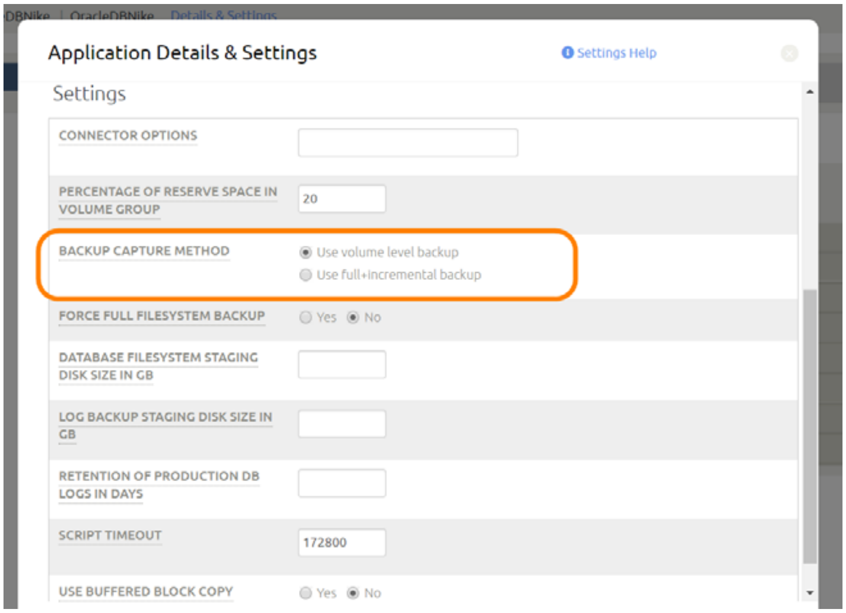
inst2 | DB2_test_delete | DB2_test_delete

TEMPLATE zSample1

PROFILE Minio

RULE All Databases

3. Above where you selected the template and the profile, click **Details & Settings**. On the Details & Settings page, make sure that the backup capture method matches the type of backup set in Chapter 3, Configuring the SLA, Including the Backup Method. Click **Apply SLA** or **Save Changes**. The instance appears in the App Manager with a green shield icon.



Application Details & Settings

Settings

CONNECTOR OPTIONS

PERCENTAGE OF RESERVE SPACE IN VOLUME GROUP: 20

BACKUP CAPTURE METHOD: ● Use volume level backup ○ Use full+incremental backup

FORCE FULL FILESYSTEM BACKUP: ○ Yes ● No

DATABASE FILESYSTEM STAGING DISK SIZE IN GB

LOG BACKUP STAGING DISK SIZE IN GB

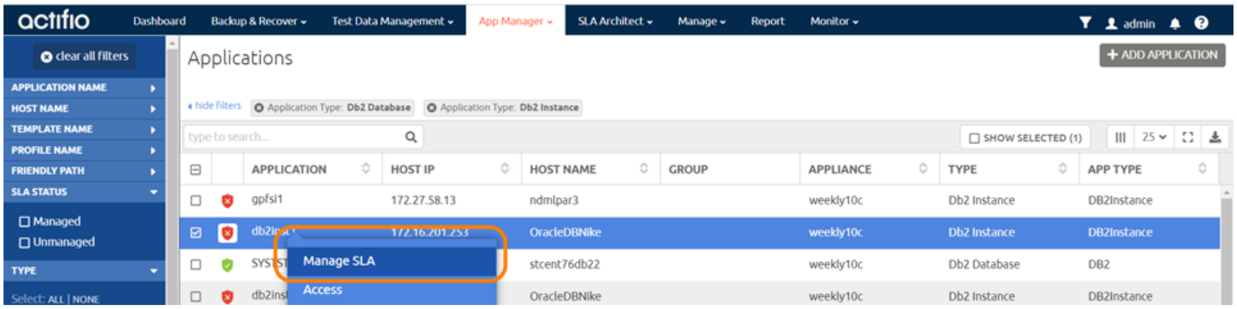
RETENTION OF PRODUCTION DB LOGS IN DAYS

SCRIPT TIMEOUT: 172800

USE BUFFERED BLOCK COPY: ○ Yes ● No

The instance will be protected when the snapshot job succeeds according to the schedule in the template.

4. You can include or exclude specific databases during backup. From the App Manager, select the Db2 instance. You can use the Db2 Instance checkbox to filter the list. Select **Manage SLA**.



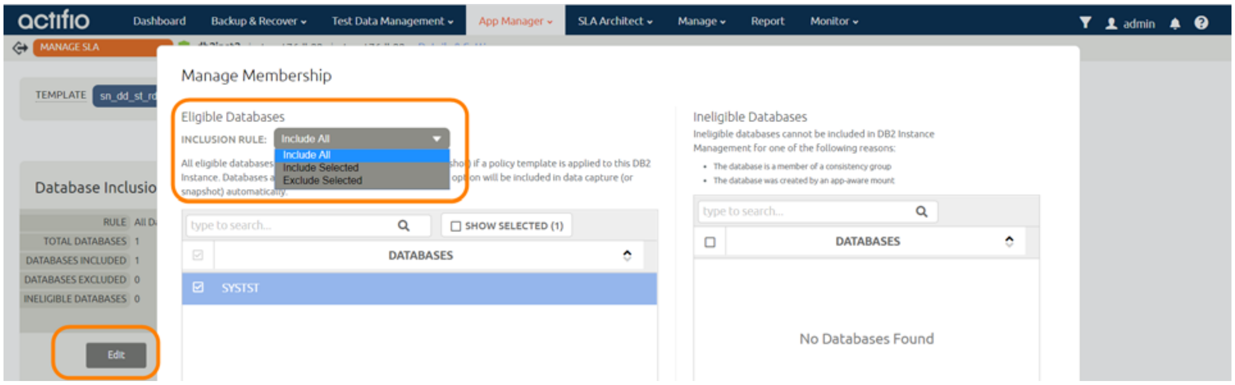
Applications

Application Type: Db2 Database | Application Type: Db2 Instance

SLA STATUS: □ Managed □ Unmanaged

	APPLICATION	HOST IP	HOST NAME	GROUP	APPLIANCE	TYPE	APP TYPE
□	gpfsi1	172.27.58.13	ndmlpar3		weekly10c	Db2 Instance	DB2Instance
☑	db2in	172.16.201.253	OracleDBNike		weekly10c	Db2 Instance	DB2Instance
□	SYSTST		stcent76db22		weekly10c	Db2 Database	DB2
□	db2ins		OracleDBNike		weekly10c	Db2 Instance	DB2Instance

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



TEMPLATE: sn_dd_st_r

Database Inclusio

RULE	All D
TOTAL DATABASES	1
DATABASES INCLUDED	1
DATABASES EXCLUDED	0
INELIGIBLE DATABASES	0

Manage Membership

Eligible Databases

INCLUSION RULE: Include All

All eligible databases sho if a policy template is applied to this DB2 Instance. Databases a op on will be included in data capture (or snapshot) automatically.

☑	DATABASES
☑	SYSTST

Ineligible Databases

Ineligible databases cannot be included in DB2 Instance Management for one of the following reasons:

- The database is a member of a consistency group
- The database was created by an app-aware mount

□	DATABASES

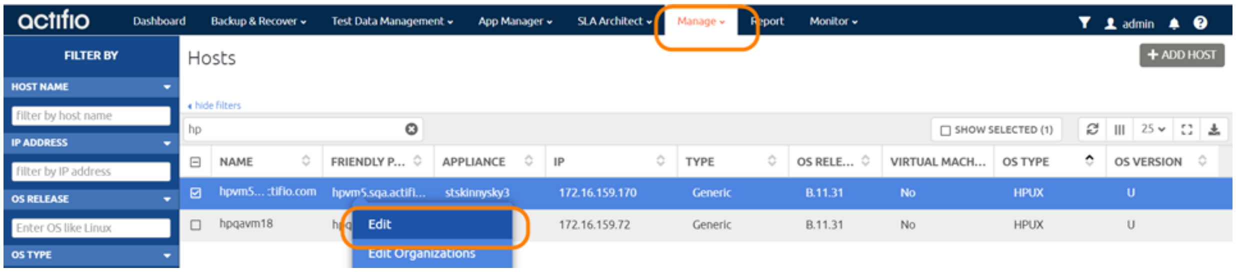
No Databases Found

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

Protecting IBM Db2 Database Logs

To enable and set up the Db2 database log backup:

1. From the SLA Architect Templates page, right-click the template for Db2 instance protection and click **Edit**.

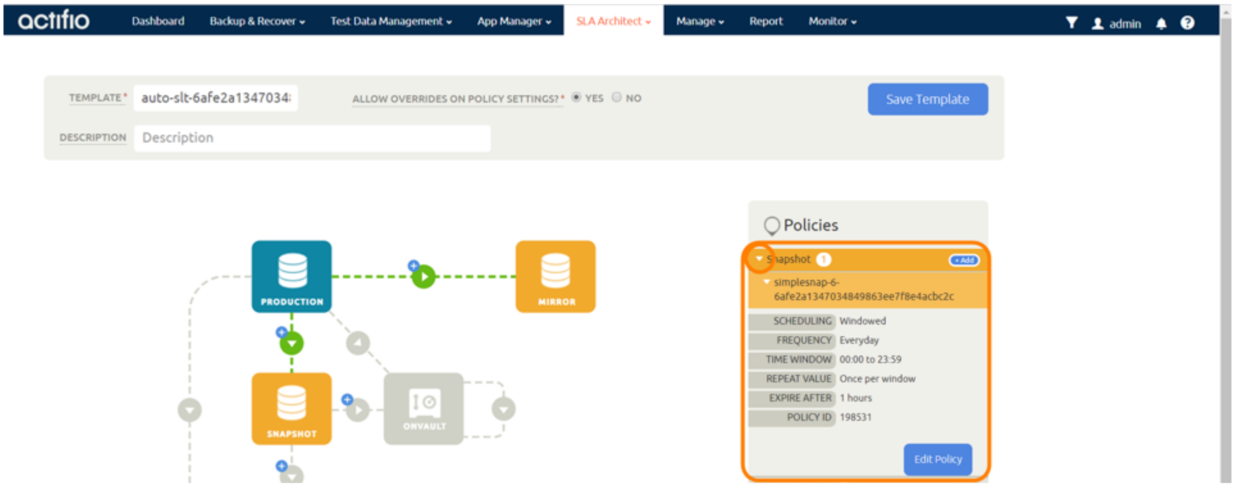


Hosts

hp

	NAME	FRIENDLY P...	APPLIANCE	IP	TYPE	OS RELE...	VIRTUAL MACH...	OS TYPE	OS VERSION
☑	hpvm5... :tifio.com	hpvm5.sqa.actifi...	stskinnysky3	172.16.159.170	Generic	B.11.31	No	HPUX	U
□	hpqavm18	hpq		172.16.159.72	Generic	B.11.31	No	HPUX	U

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



TEMPLATE* auto-slt-6afe2a1347034

ALLOW OVERRIDES ON POLICY SETTINGS?* ● YES ○ NO

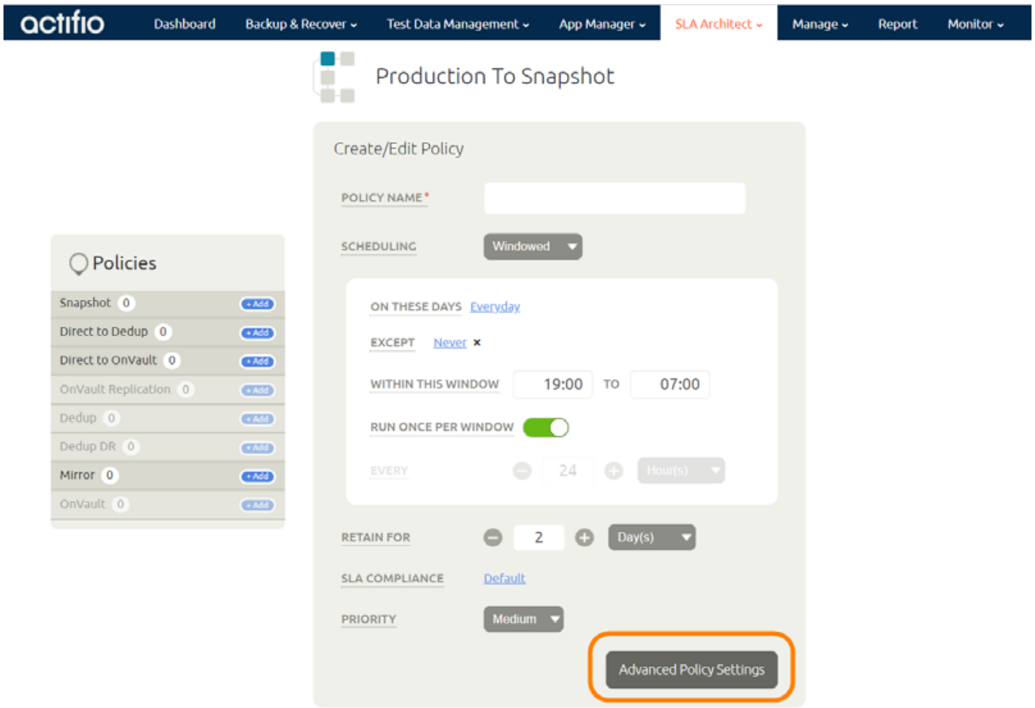
DESCRIPTION Description

Snapshot 1

simplesnap-6-6afe2a1347034849863ee7f8e4acbc2c

SCHEDULING	Windowed
FREQUENCY	Everyday
TIME WINDOW	00:00 to 23:59
REPEAT VALUE	Once per window
EXPIRE AFTER	1 hours
POLICY ID	198531

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



Production To Snapshot

Create/Edit Policy

Snapshot	0
Direct to Dedup	0
Direct to OnVault	0
OnVault Replication	0
Dedup	0
Dedup DR	0
Mirror	0
OnVault	0

POLICY NAME*

SCHEDULING Windowed

ON THESE DAYS Everyday

EXCEPT Never ×

WITHIN THIS WINDOW 19:00 TO 07:00

RUN ONCE PER WINDOW

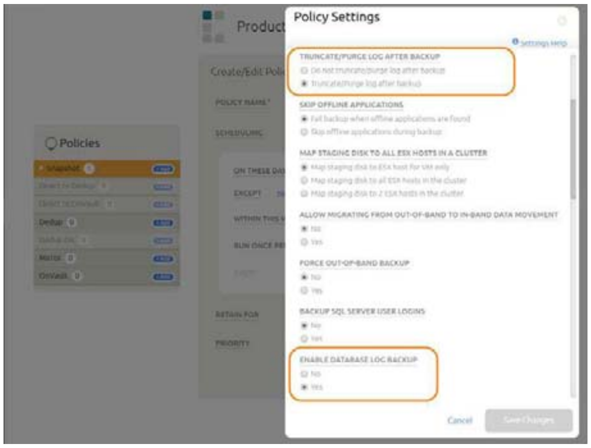
EVERY 24 Hour(s)

RETAIN FOR 2 Day(s)

SLA COMPLIANCE Default

PRIORITY Medium

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.



Policy Settings

TRUNCATE/PURGE LOG AFTER BACKUP
○ Do not truncate/purge log after backup
● Truncate/Purge log after backup

SKIP OFFLINE APPLICATIONS
● Fail backup when offline applications are found
○ Skip offline applications during backup

MAP STAGING DISK TO ALL ESX HOSTS IN A CLUSTER
● Map staging disk to ESX host for VM only
○ Map staging disk to all ESX hosts in the cluster
○ Map staging disk to 2 ESX hosts in the cluster

ALLOW MIGRATING FROM OUT-OF-BAND TO IN-BAND DATA MOVEMENT
● No
○ Yes

FORCE OUT-OF-BAND BACKUP
● No
○ Yes

BACKUP SQL SERVER USER LOGINS
● No
○ Yes

ENABLE DATABASE LOG BACKUP
○ No
● Yes

5. Click **Save Changes**.
6. From the App Manager Applications list, select the Db2 instance. You can use the Db2 Instance checkbox to filter the list. Right-click it 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 Db2 logs from the production destination. Based on this setting the log will be purged older then 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 Accessing a Db2 Database as a Standard Mount or as a Refreshable Virtual Database

This section describes:

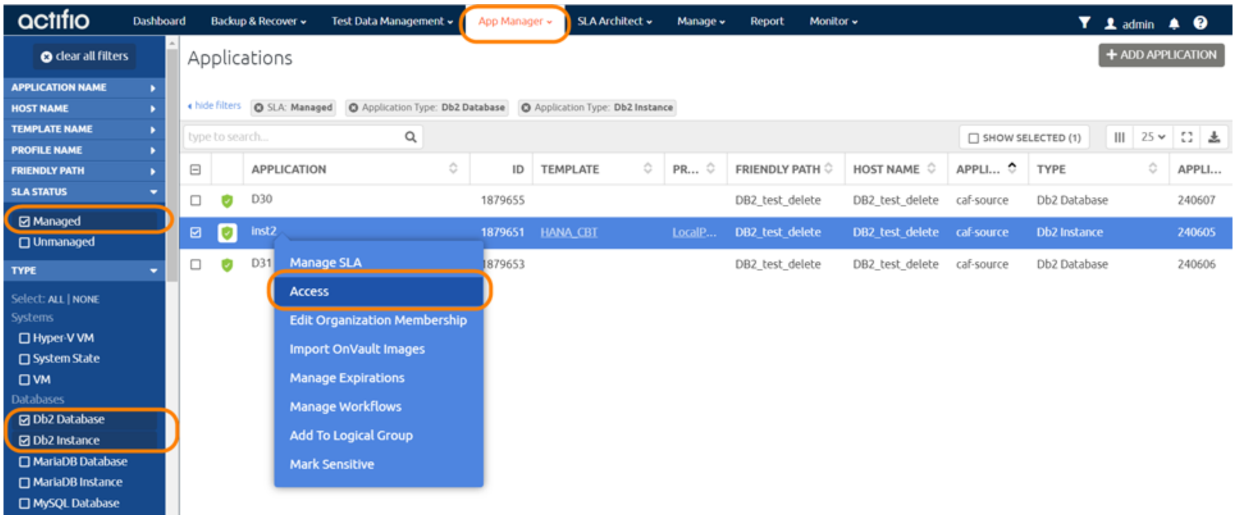
Mounting a Db2 Database as a Standard Mount

This is the procedure for a standard mount. To make a virtual database (application aware mount), see the procedure in Mount a Virtual Database from a Block-Based Volume Snapshot Image to the Source or to an Existing Db2 Instance on page 23.

To mount the database image as a standard mount:

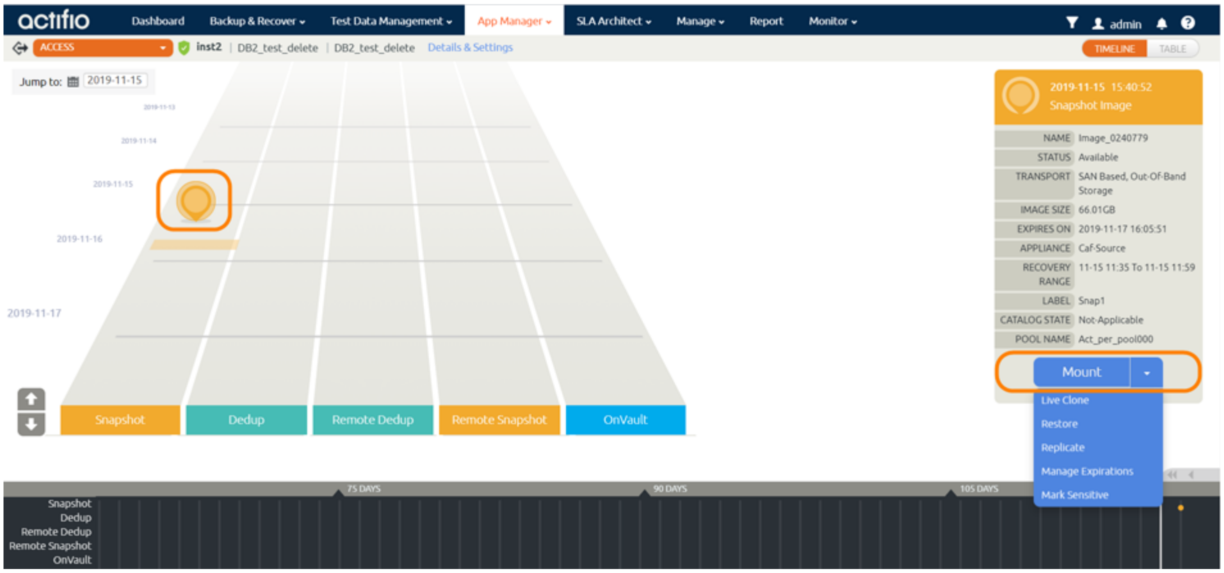
1. From the App Manager Applications list, right-click the protected database and select **Access**.

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



		APPLICATION	ID	TEMPLATE	PR...	FRIENDLY PATH	HOST NAME	APPLI...	TYPE	APPLI...
☐		D30	1879655			DB2_test_delete	DB2_test_delete	caf-source	Db2 Database	240607
☑		inst2	1879651	HANA_CBT	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 **Mount**.



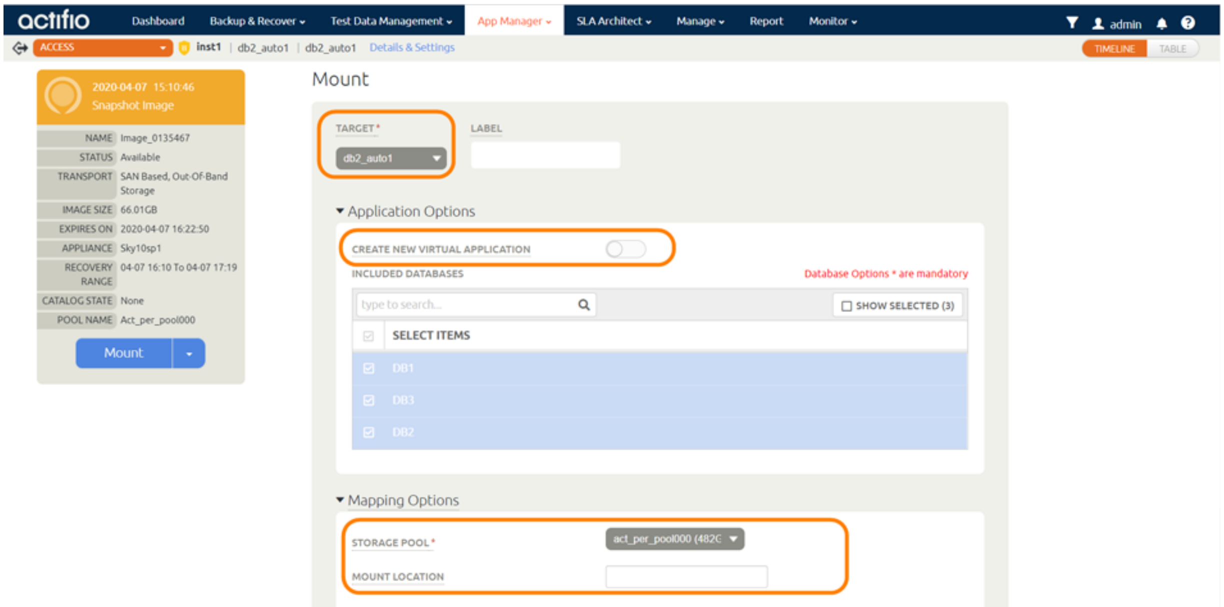
2019-11-15 15:40:52
Snapshot Image

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

3. On the Mount page, from **Target**, choose the desired target Db2 server from the dropdown.

4. Under Application Options, **disable** Create New Virtual Application.

5. Under Mapping Options, select a local or external **Storage Pool** and enter a **Mount Location**.



2020-04-07 15:10:46
Snapshot Image

NAME	Image_0135467
STATUS	Available
TRANSPORT	SAN Based, Out-Of-Band Storage
IMAGE SIZE	66.01GB
EXPIRES ON	2020-04-07 16:22:50
APPLIANCE	Sky10sp1
RECOVERY RANGE	04-07 16:10 To 04-07 17:19
CATALOG STATE	None
POOL NAME	Act_per_pool000

TARGET * db2_auto1

LABEL

CREATE NEW VIRTUAL APPLICATION ○

INCLUDED DATABASES

Database Options * are mandatory

☑ DB1
☑ DB3
☑ DB2

STORAGE POOL * act_per_pool000 (482C

MOUNT LOCATION

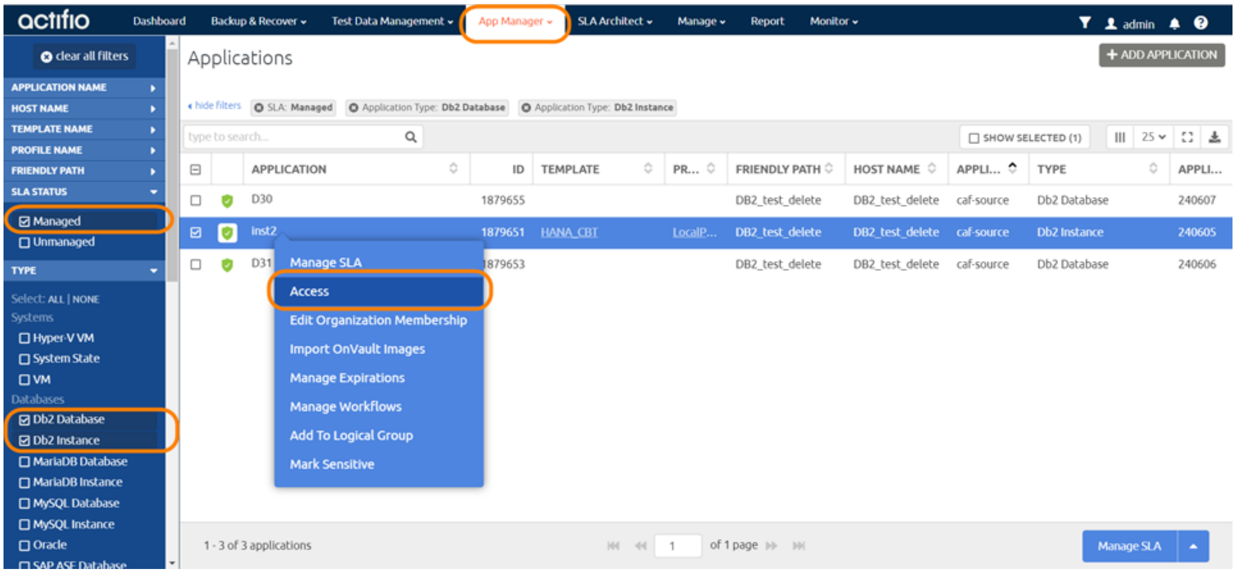
6. Click **Submit**. You can monitor the job progress from the Monitor, Jobs page.

Mount a Virtual Database from a Block-Based Volume Snapshot Image to the Source or to an Existing Db2 Instance

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

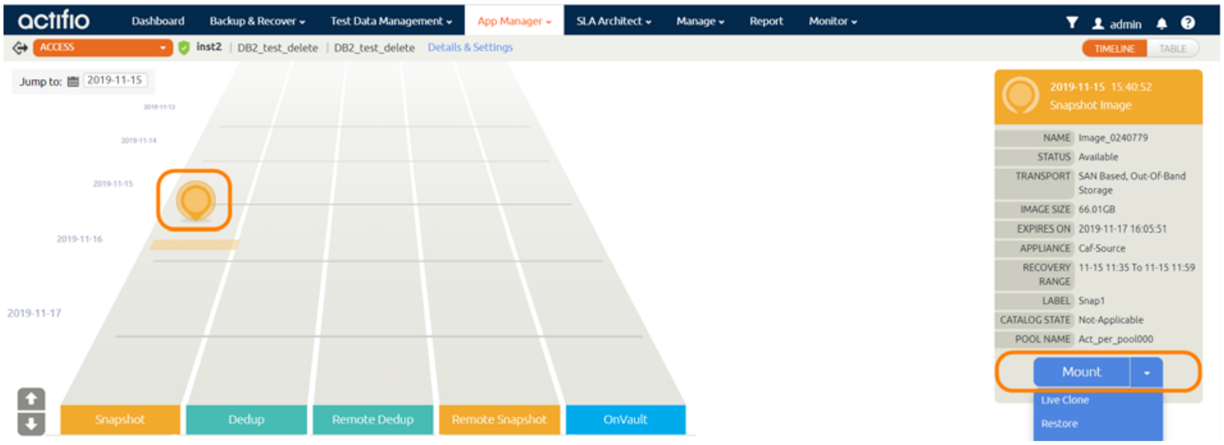
1. From the App Manager Applications list, right-click the protected database and select **Access**.

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



		APPLICATION	ID	TEMPLATE	PR...	FRIENDLY PATH	HOST NAME	APPLI...	TYPE	APPLI...
□	✓	D30	1879655			DB2_test_delete	DB2_test_delete	caf-source	Db2 Database	240607
☑	✓	inst2	1879651	HANA_CBT	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 **Mount**.



2019-11-15 15:40:52
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

3. On the Mount page, from Target, choose the desired target Db2 server from the dropdown.

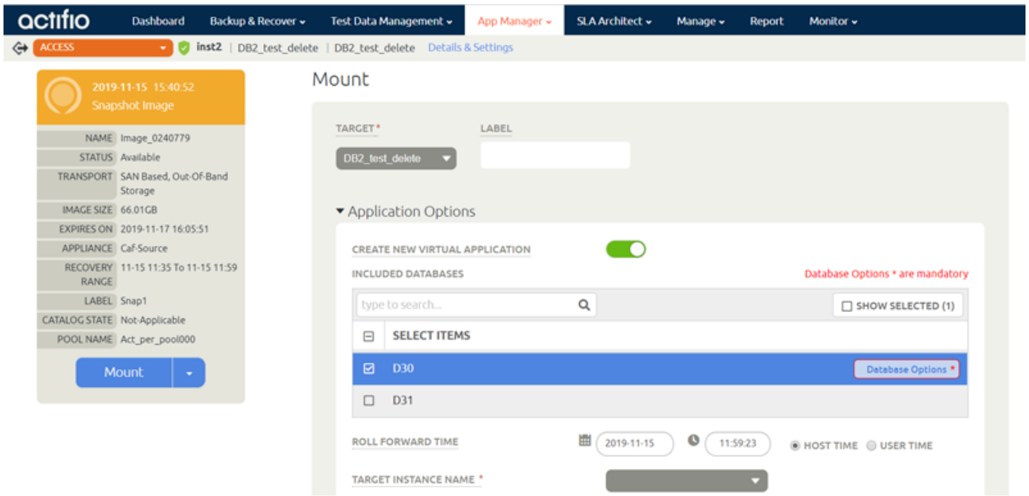
> ***Note:*** *Be sure that the target instance does not have any databases with the same name as any of the source databases or the new target database name selected for the source database(s) during mount.*

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.



2019-11-15 15:40:52
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

Mount

TARGET * DB2_test_delete

LABEL

Application Options

CREATE NEW VIRTUAL APPLICATION

INCLUDED DATABASES

Database Options * are mandatory

type to search...

□ SHOW SELECTED (1)

⊟ SELECT ITEMS

☑ D30 Database Options *

□ D31

ROLL FORWARD TIME 2019-11-15 11:59:23 ● HOST TIME ○ USER TIME

TARGET INSTANCE NAME *

6. Click each selected database to specify the target database details for the new virtual copy.

7. For a database protected with log roll-forward, choose a target point in time.

8. 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.

9. TARGET Db2 INSTANCE NAME: From the dropdown, select a target Db2 instance to attach the selected database as a virtual copy.

10. Manage New Application:
    - To protect the new virtual database, enable **Manage New Application**.
    - Choose a template and a resource profile to protect the database.

11. In Advanced Options:
    - Enter the **Home Directory** of the database (optional).
    - **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.

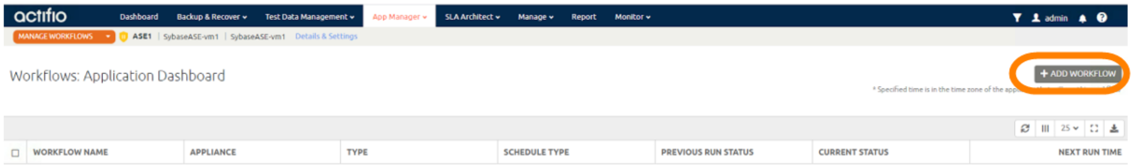
12. Under Mapping Options:
    - Storage Pool: The image will be mounted in the Snapshot Pool unless you select a different one.
    - Mount Location: specify a target mount point to mount the new virtual database to.

13. Click **Submit**.

Refreshing a Virtual Db2 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**.

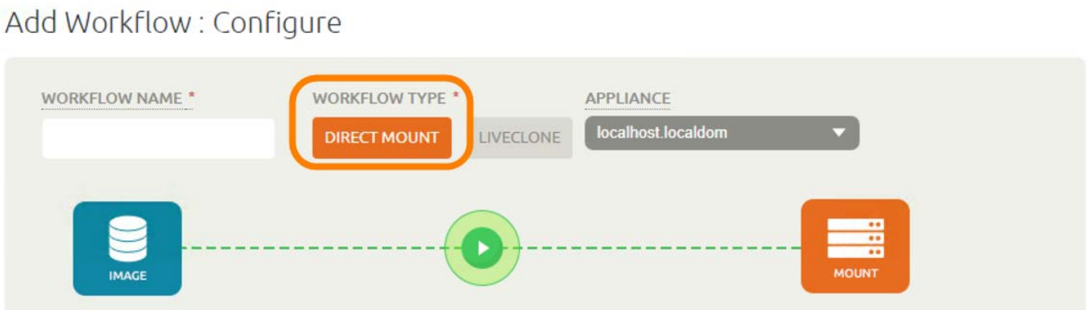


Workflows: Application Dashboard

* Specified time is in the time zone of the app

□	WORKFLOW NAME	APPLIANCE	TYPE	SCHEDULE TYPE	PREVIOUS RUN STATUS	CURRENT STATUS	NEXT RUN TIME

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.



Add Workflow : Configure

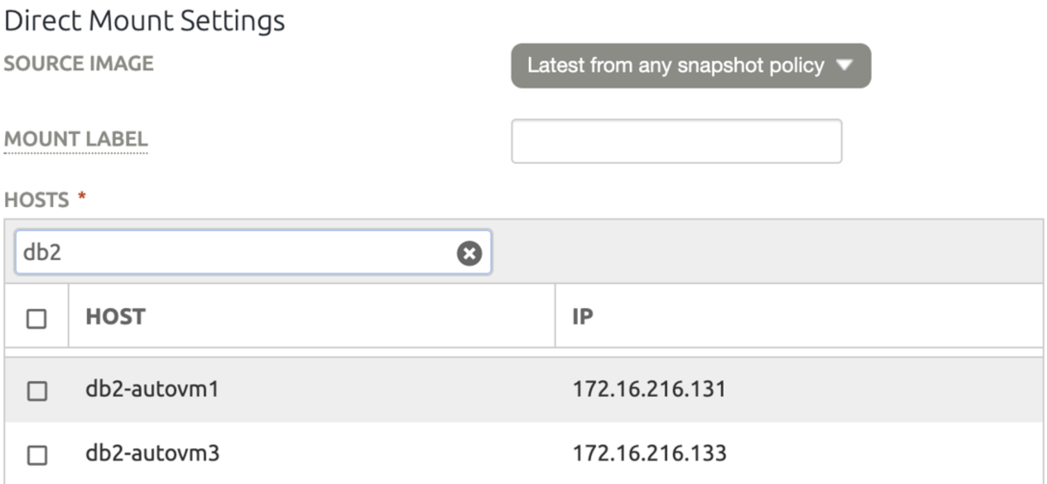
WORKFLOW NAME *

WORKFLOW TYPE * DIRECT MOUNT

APPLIANCE localhost.localdom

   - 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 databases copy will be created.

Note: *Be sure that the target instance has no databases with the same name as any of the source databases or the new target database name selected for the source database(s) during the mount.*



Direct Mount Settings

SOURCE IMAGE: Latest from any snapshot policy

MOUNT LABEL

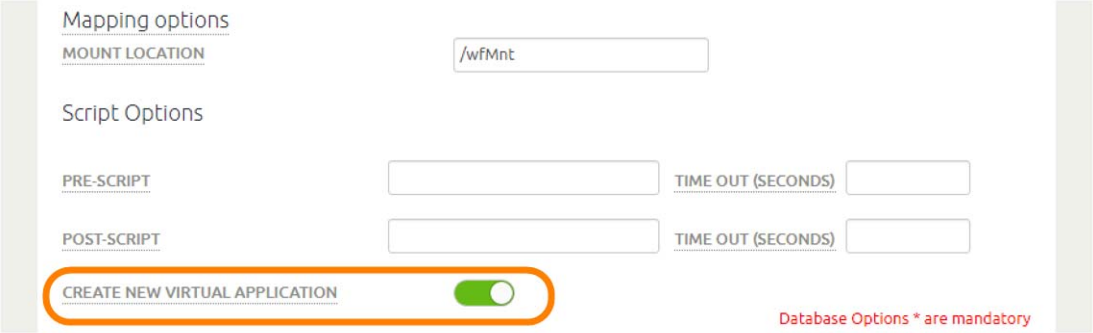
HOSTS *

db2

□	HOST	IP
□	db2-autovm1	172.16.216.131
□	db2-autovm3	172.16.216.133

   - 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.
- Post-Script (optional): Specify a postscript name to be run at the end of refresh. Pre- and Post- scripts are detailed in ***Network Administrator's Guide to Actifio VDP***.
- Create New Virtual Application: Enable **Create New Virtual Application**.



Mapping options

MOUNT LOCATION: /wfMnt

Script Options

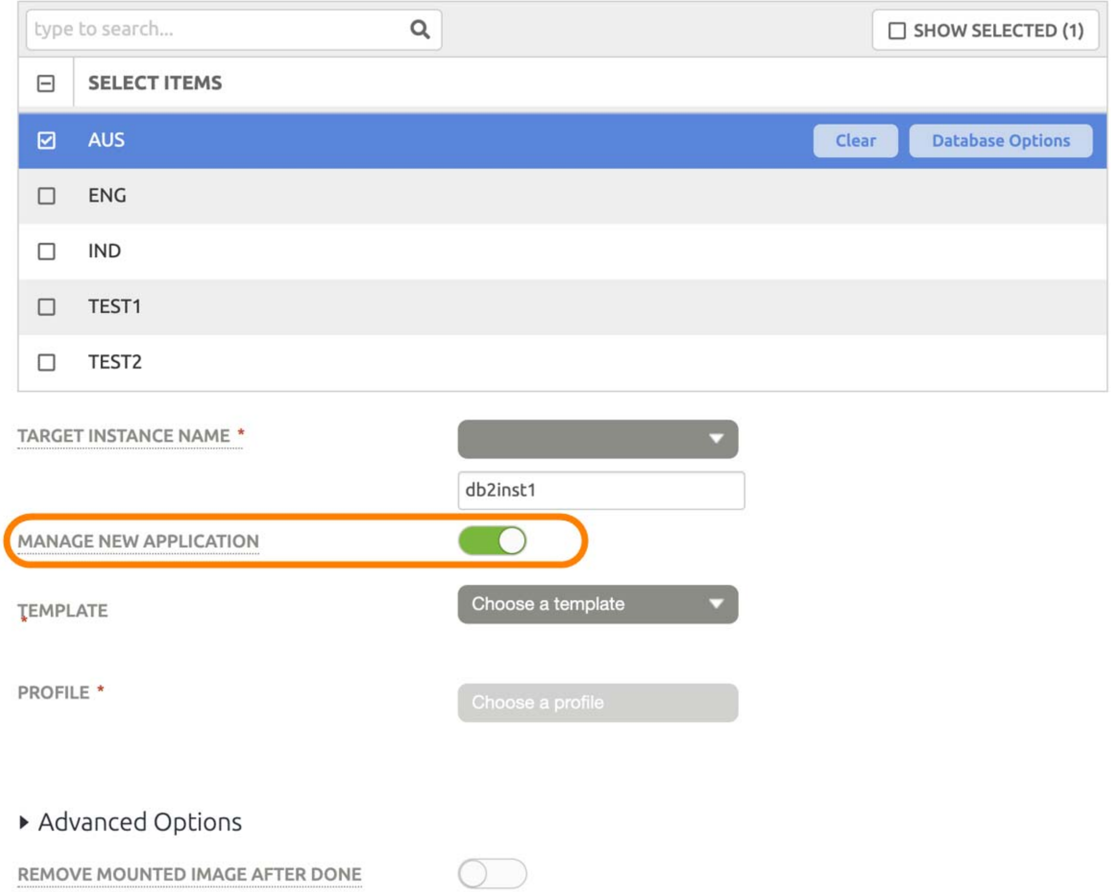
PRE-SCRIPT | TIME OUT (SECONDS)

POST-SCRIPT | TIME OUT (SECONDS)

CREATE NEW VIRTUAL APPLICATION: on

Database Options * are mandatory

- Select Items: Select the databases to refresh on target and specify the target dbname from 'Database Options' for each database.
- TARGET INSTANCE NAME: If target instance is visible, then select it, otherwise specify the target instance name.



type to search... | □ SHOW SELECTED (1)

⊟	SELECT ITEMS
☑	AUS — Clear — Database Options
□	ENG
□	IND
□	TEST1
□	TEST2

TARGET INSTANCE NAME *: db2inst1

MANAGE NEW APPLICATION: on

TEMPLATE: Choose a template

PROFILE *: Choose a profile

▸ Advanced Options

REMOVE MOUNTED IMAGE AFTER DONE: off

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

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

6 Restoring and Recovering a Db2 Instance Back to the Source

This section describes:

- Recovering a Db2 Instance from a Volume-Based Snapshot on page 27
- Recovering a Single Db2 Database from a Volume-Based Snapshot on page 29
- Recovering from a Full+Incremental Snapshot on page 31
- Recovering to a New Target from a Full+Incremental Snapshot on page 32

Recovering a Db2 Instance from a Volume-Based Snapshot

Use this procedure to restore and recover the source Db2 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.*

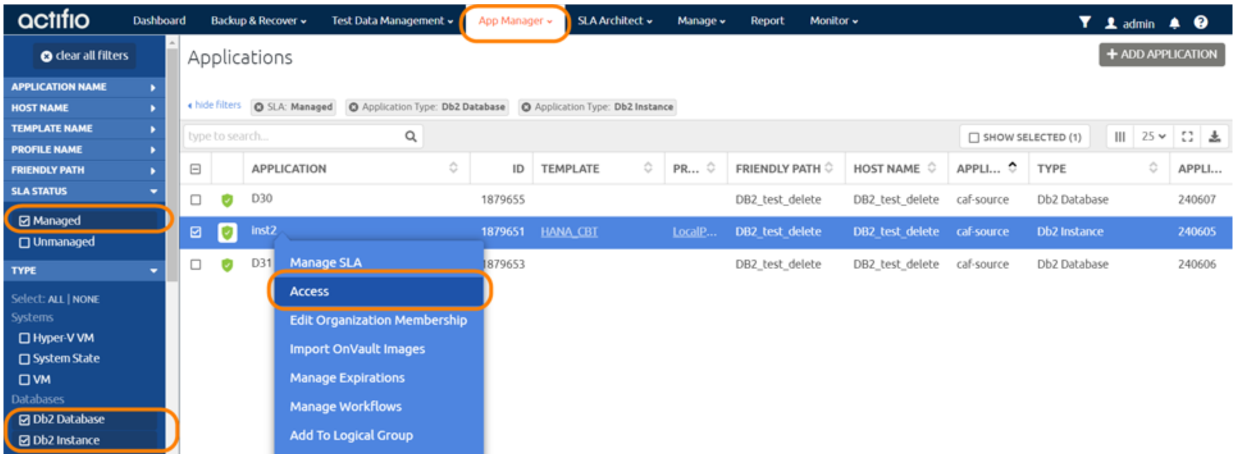
Note: *If multiple instances share the same volume/filesystem(s), then restoring back to the source is not supported. To restore such applications, mount the image to the host and use the procedure to perform single database recovery detailed in* Recovering a Single Db2 Database from a Volume-Based Snapshot *on page 29.*

Note: *If there are nested mountpoints under the production volumes being backed up, then restore and migrate operations will fail as the production volumes are busy and cannot be unmounted. To overcome this limitation, use the appliance CLI to set this configuration parameter in /act/config/connector.conf on the host:*

```
udstask chconnectorconfig -host <HOSTID> -param UnmountNestedVolumesForRestore -value true
```

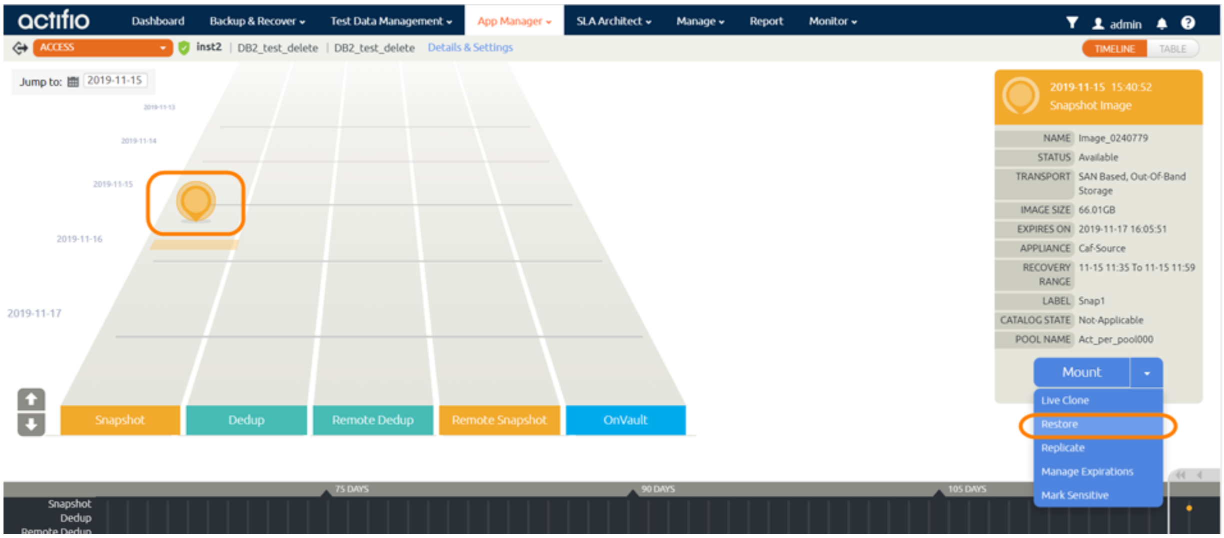
To recover back to the source:

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.



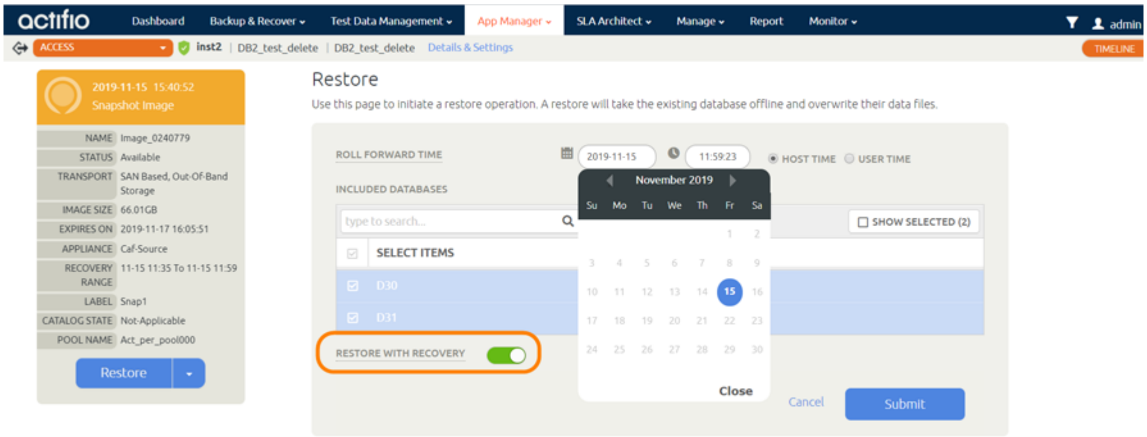
		APPLICATION	ID	TEMPLATE	PR...	FRIENDLY PATH	HOST NAME	APPLI...	TYPE	APPLI...
□		D30	1879655			DB2_test_delete	DB2_test_delete	caf-source	Db2 Database	240607
☑		inst2	1879651	HANA_CBT	LocalP...	DB2_test_delete	DB2_test_delete	caf-source	Db2 Instance	240605
□		D31	1879653			DB2_test_delete	DB2_test_delete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

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



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

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



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

Restore

Use this page to initiate a restore operation. A restore will take the existing database offline and overwrite their data files.

ROLL FORWARD TIME 2019-11-15 11:59:23 ● HOST TIME ○ USER TIME

INCLUDED DATABASES

☑ SELECT ITEMS
☑ D30
☑ D31

RESTORE WITH RECOVERY

4. Enable **Restore With Recovery** to apply recovered logs.

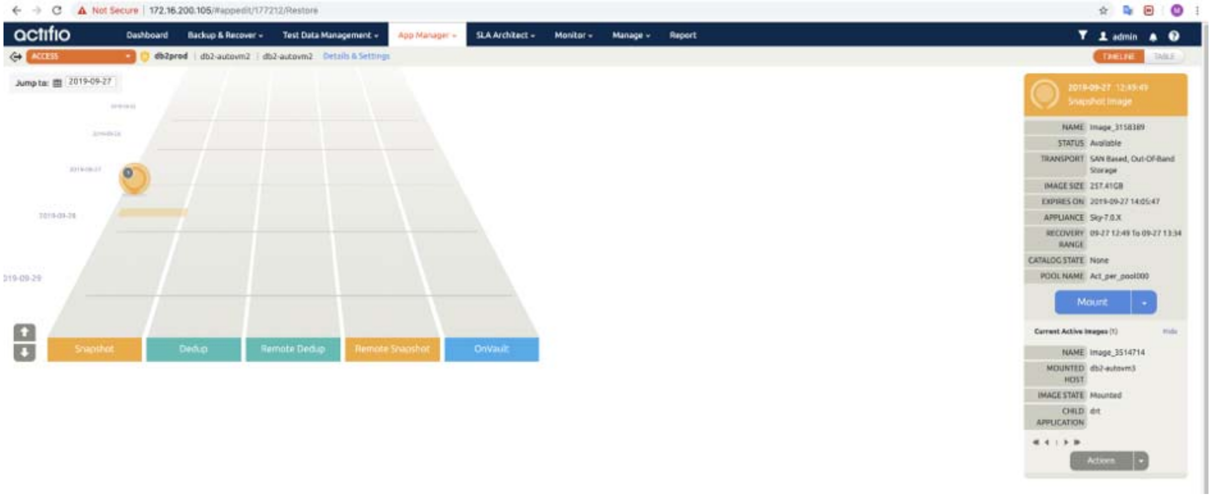
5. Click **Submit**.

Recovering a Single Db2 Database from a Volume-Based Snapshot

To restore a single LVM backup image to its 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.*



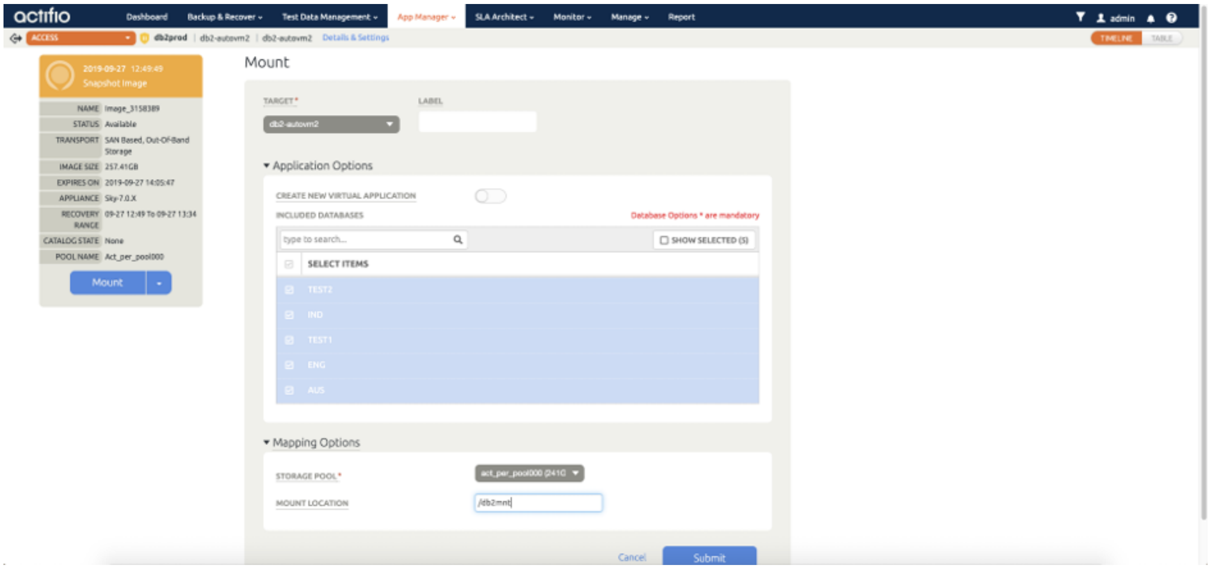
2019-09-27 12:49:49
Snapshot Image

NAME Image_3158389
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 257.41GB
EXPIRES ON 2019-09-27 14:05:47
APPLIANCE Sky-7.0.X
RECOVERY RANGE 09-27 12:49 To 09-27 13:34
CATALOG STATE None
POOL NAME Act_per_pool000

Current Active Images (1)

NAME Image_3514714
MOUNTED HOST db2-autovm3
IMAGE STATE Mounted
CHILD APPLICATION drt

2. Select the latest snapshot to recover, and choose Mount.



Mount

TARGET* db2-autovm2
LABEL

Application Options

CREATE NEW VIRTUAL APPLICATION
INCLUDED DATABASES
Database Options * are mandatory

☐ SHOW SELECTED (5)

SELECT ITEMS
☑ TEST2
☑ IND
☑ TEST1
☑ ENG
☑ AUS

Mapping Options

STORAGE POOL* act_per_pool000 (2410
MOUNT LOCATION /db2mnt

3. Provide a mount point under mount location, for example: /db2mnt. The database backup will be mounted under /db2mnt and log backup will be mounted under /db2mnt_archivelog

4. Log into the database server as root. On the server, change directory to /act/custom_apps/db2/restore.

5. Get the JobID of the mount from /var/act/log/UDSAgent.log. To find the jobid, run:

```
grep "mount -t " /var/act/log/UDSAgent.log | grep -w "<mountPoint from Step 3>"|tail -1
```

For example:

```
# grep "mount -t " /var/act/log/UDSAgent.log | grep -w "/db2mnt" |tail -1
2019-11-18 23:59:19.740 GEN-INFO  [22488] Job_0404207 Spawning cmd: mount -t ext4 /dev/
act403764_DBDump_1574101677612/act_staging_vol /db2mnt 2>&1
```

6. ARCHIVELOG_MNT will be equals to <mountPoint provided in Step 3>_archivelog.

```
#cd /act/custom_apps/db2/restore
```

7. Run the script from command line (as root) act_db2_lvm_customdb_recovery.sh on target with arguments;

```
#/act/custom_apps/db2/restore/act_db2_lvm_customdb_recovery.sh
JOBID=Job_0348096 SOURCE_INSTANCE=db2ts DB_NAME=NCR UNTIL_TIME=2019-10-17-14.45.45.000
ARCHIVELOG_MNT=/db2mnt_archivelog  TARGET_MNT=/db2mnt
```

Arguments to the Script

SOURCE_INSTANCE = <Db2 Instance name>

DB_NAME=<Db2 Database name to be recovered (Single)>

TARGET_MNT = <Db2 Database image mountpoint name>

ARCHIVELOG_MNT= <Archive Log backup mount point name>

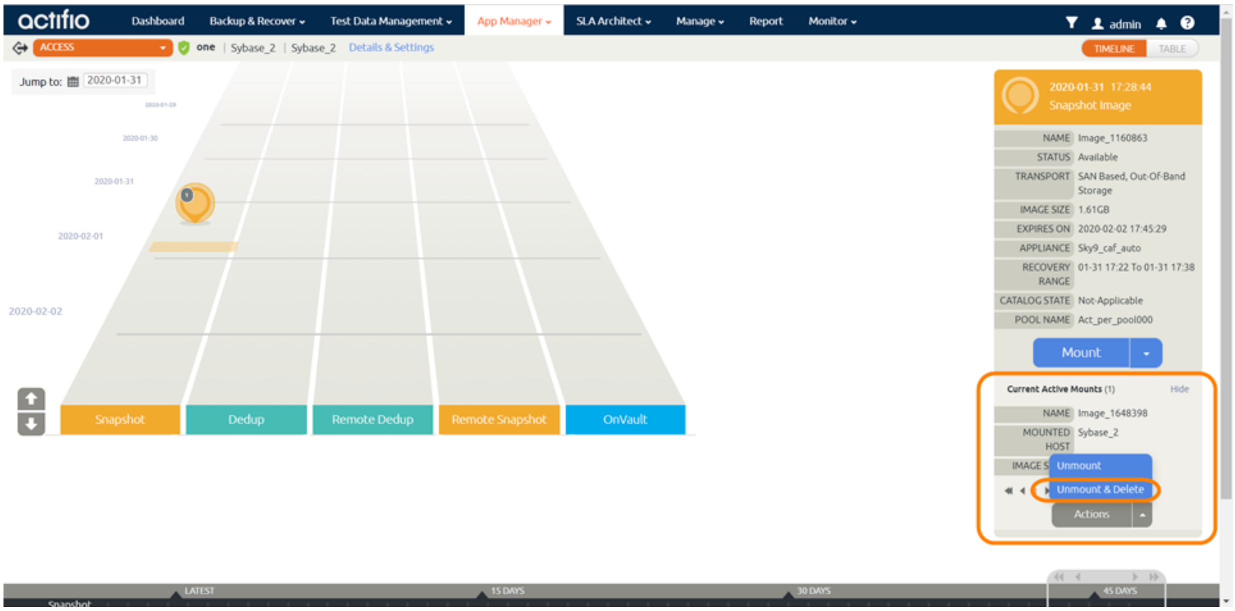
UNTIL_TIME = <Recovery Time(Format: "YYYY-MM-DD-HH.MI.SS")>

JOBID = <Database mount Job name>

8. Connect to Db2 instance and confirm that the databases are recovered and online.

```
db2  connect to <dbname>
db2  'select db_status FROM SYSIBMADM.SNAPDB'
```

9. Unmount the mounted dump snapshot image.



2020-01-31 17:28:44
Snapshot Image

NAME Image_1160863
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 1.61GB
EXPIRES ON 2020-02-02 17:45:29
APPLIANCE Sky9_caf_auto
RECOVERY RANGE 01-31 17:22 To 01-31 17:38
CATALOG STATE Not-Applicable
POOL NAME Act_per_pool000

Current Active Mounts (1) Hide

NAME Image_1648398
MOUNTED HOST Sybase_2
IMAGE S

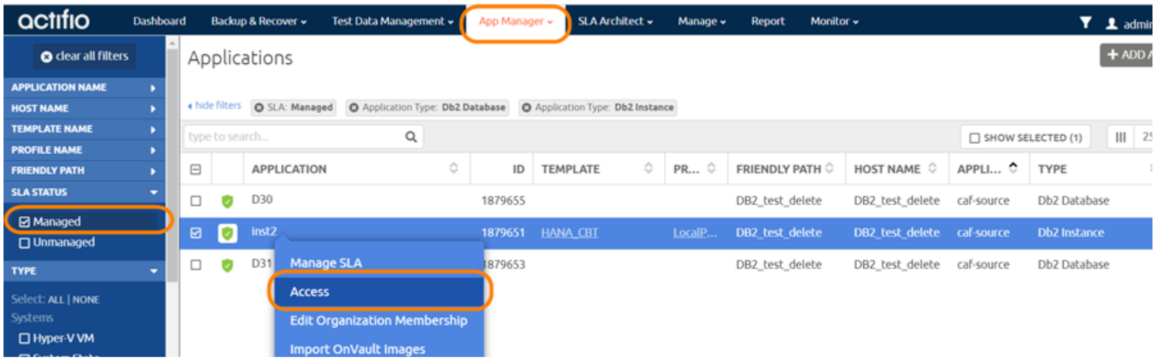
Recovering from a Full+Incremental Snapshot

Use this procedure to restore and recover the source Db2 database. This procedure overwrites the source data.

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**.

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



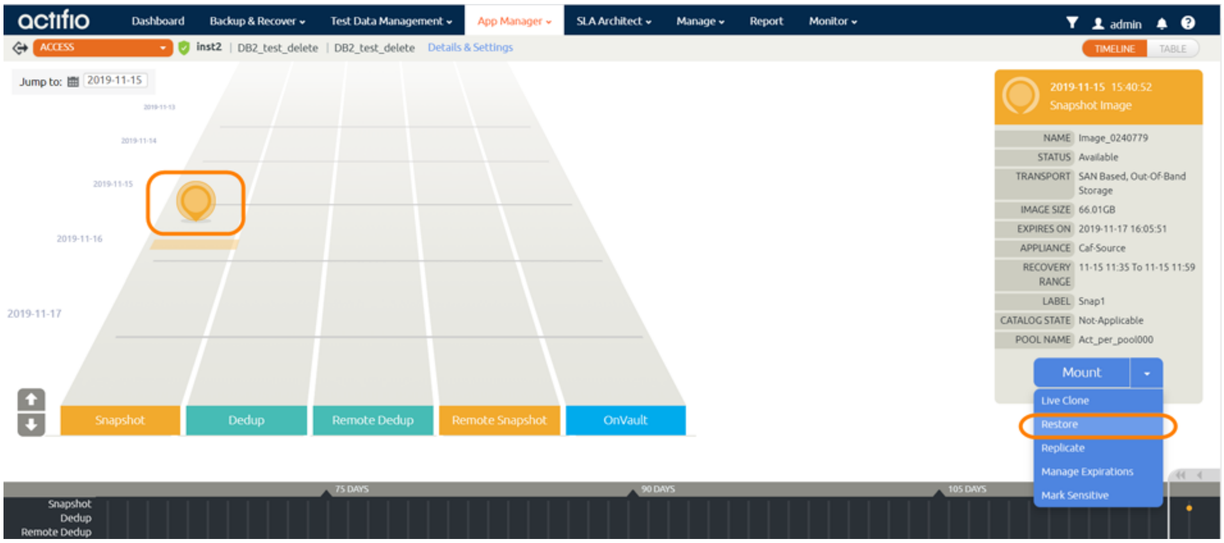
Applications

☑ Managed
☐ Unmanaged
☐ Hyper-V VM

SLA: Managed | Application Type: Db2 Database | Application Type: Db2 Instance

⊟		APPLICATION	ID	TEMPLATE	PR...	FRIENDLY PATH	HOST NAME	APPLI...	TYPE
☐		D30	1879655			DB2_test_delete	DB2_test_delete	caf-source	Db2 Database
☑		inst2	1879651	HANA_CBT	LocalP...	DB2_test_delete	DB2_test_delete	caf-source	Db2 Instance
☐		D31	1879653			DB2_test_delete	DB2_test_delete	caf-source	Db2 Database

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



inst2 | DB2_test_delete | DB2_test_delete

2019-11-15 15:40:52
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

3. For a database protected with logs, on the Restore page, choose a date and then 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 using Db2 recover commands.

Recovering to a New Target from a Full+Incremental Snapshot

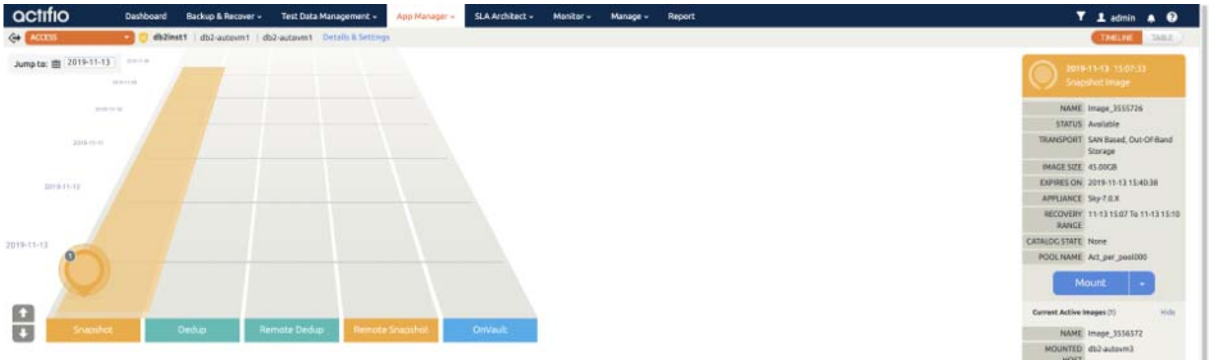
To restore a Db2 dump-based backup image to a new target:

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 the latest snapshot to recover, and choose Mount.

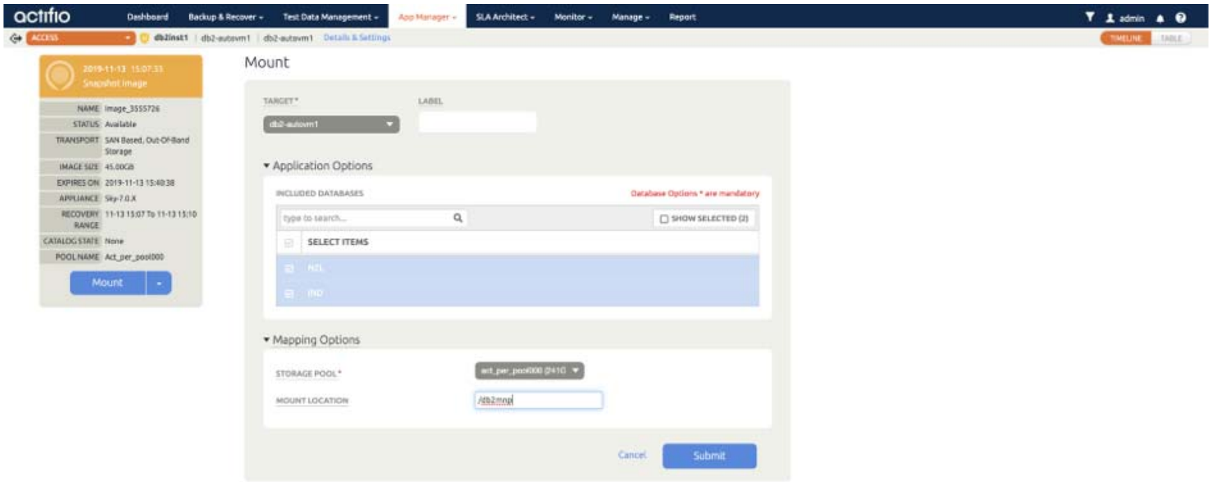


2019-11-13 15:07:33
Snapshot Image

NAME Image_3555726
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 45.00GB
EXPIRES ON 2019-11-13 15:40:38
APPLIANCE Sky-7.0.X
RECOVERY RANGE 11-13 15:07 To 11-13 15:10
CATALOG STATE None
POOL NAME Act_per_pool000

NAME Image_3556372
MOUNTED HOST db2-autovm3

3. Provide a mount point under mount location, for example: /db2mnp.



2019-11-13 15:07:33
Snapshot Image

NAME Image_3555726
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 45.00GB
EXPIRES ON 2019-11-13 15:40:38
APPLIANCE Sky-7.0.X
RECOVERY RANGE 11-13 15:07 To 11-13 15:10
CATALOG STATE None
POOL NAME Act_per_pool000

TARGET* db2-autovm1
LABEL
INCLUDED DATABASES
□ SHOW SELECTED (2)
NZL
IND
STORAGE POOL* act_per_pool000 (2410)
MOUNT LOCATION /db2mnp

4. The database backup will be mounted under /db2mnp and the log backup will be mounted under /db2mnp_archivelog

5. JobID of the mount can be get form /var/act/log/UDSAgent.log. Run the below command, which will output some lines where we can see the jobid.

```
grep "mount -t " /var/act/log/UDSAgent.log  | grep -w "<mountPoint provided in step2>"|tail -1
```

   For example:

```
# grep "mount -t " /var/act/log/UDSAgent.log  | grep -w "/db2mnp" |tail -1
2019-11-18 23:59:19.740 GEN-INFO  [22488] Job_0404207 Spawning cmd: mount -t ext4 /dev/
act403764_DBDump_1574101677612/act_staging_vol /db2mnp 2>&1
```

6. ARCHIVELOG_MNT will be equal to <mountPoint provided in Step 3>_archivelog. See Step 4.

7. Login to the database server as root. On the server, change the directory to

```
/act/custom_apps/DB2/dump
#cd /act/custom_apps/DB2/dump
```

8. Run the script from command line (as root) ACT_DB2_dumprestore_newTarget.sh on target with arguments;

```
#/act/custom_apps/db2/dump/ACT_DB2_dumprestore_newTarget.sh
SOURCE_INSTANCE=db2inst1 TARGET_MNT=/db2mnp             DB_LIST=NZL,IND ARCHIVELOG_MNT=/
db2mnp_archivelog SOURCE_LOGARCHMETH1=/db2logbackup UNTIL_TIME=2019-11-13-09.37.41.000000
```

Arguments to the Script

SOURCE_INSTANCE = < Db2 Instance name >

DB_LIST=<Comma separated database list to restore>

TARGET_MNT = <Mount point specified during mount>

ARCHIVELOG_MNT= <Archive Log backup mount point name>

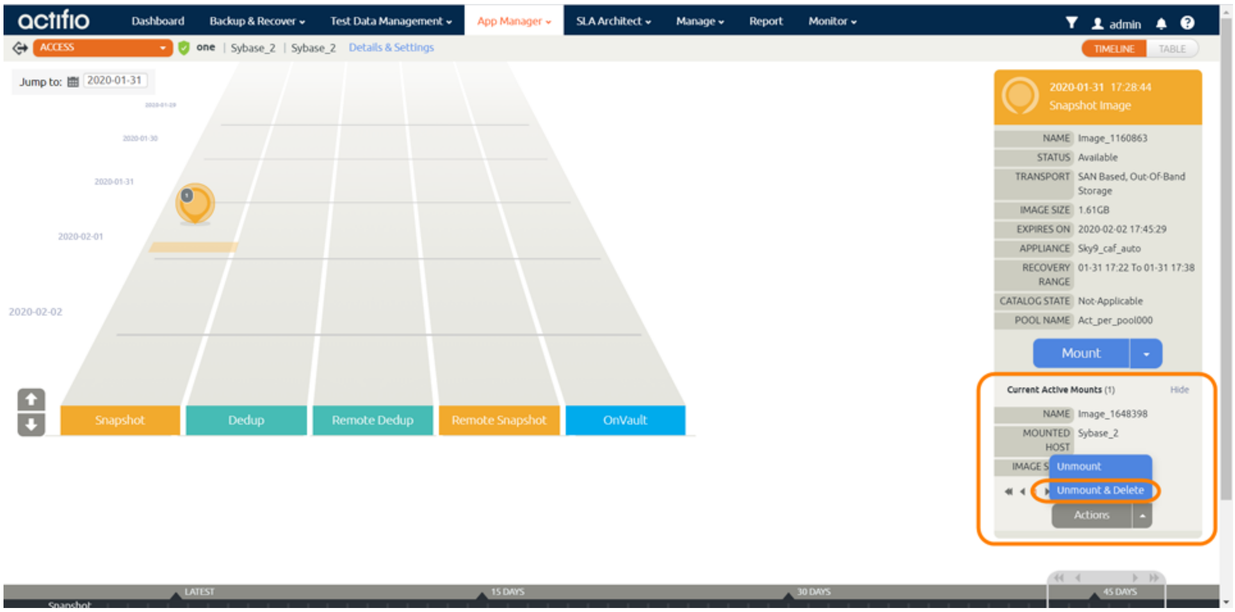
UNTIL_TIME = < Recovery Time (Format: "YYYY-MM-DD-HH.MI.SS")>

SOURCE_LOGARCHMETH1= <Db2 Source database archivelog location>

9. Connect to the Db2 instance and confirm that the databases are recovered and online.

```
db2 connect to <dbname>
db2  'select db_status FROM SYSIBMADM.SNAPDB'
```

10. Unmount the mounted dump snapshot image.



2020-01-31 17:28:44
Snapshot Image

NAME Image_1160863
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 1.61GB
EXPIRES ON 2020-02-02 17:45:29
APPLIANCE Sky9_caf_auto
RECOVERY RANGE 01-31 17:22 To 01-31 17:38
CATALOG STATE Not-Applicable
POOL NAME Act_per_pool000

Current Active Mounts (1)
NAME Image_1648398
MOUNTED HOST Sybase_2

7 Migrating a Db2 Instance for Instant Access or Recovery

A Mount and Migrate operation allows you to restore a database with near-zero downtime by first mounting it locally, and then migrating it to the original location or to a new location. Users have normal access to the database while it is mounted, and the migration step is very fast.

Once you have protected a Db2 instance, you can mount it and migrate it:

Mount and Migrate Back to the Source Instance on page 35

Mount and Migrate to a New Instance on page 37

Mount and Migrate Back to the Source Instance

To mount a database from an image and migrate the mounted 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. Mount the image as a standard mount as detailed in Mounting a Db2 Database as a Standard Mount on page 21.

   If under mount location, you use the mount point: /db2gj, then:

   - The database backup will be mounted under /db2gj
   - The log backup will be mounted under /db2gj_archivelog
3. Disable the application SLA to ensure no new jobs interfere with this job.
4. Once the mount job is completed, run this script with parameters in Arguments to the Script.

```
/act/custom_apps/db2/clone/ACT_DB2_mountrecover.sh TARGET_MNT=<TARGET_MNT>
TARGET_INSTANCE=<TARGET_INSTANCE>  TARGET_DBNAME_LIST=<TARGET_DBNAME_LIST>
[UNTIL_TIME=<UNTIL_TIME>]  JOBID=<JOBID>
```

Example

```
/act/custom_apps/db2/clone/ACT_DB2_mountrecover.sh TARGET_MNT=/db2gj TARGET_INSTANCE=db2prod
TARGET_DBNAME_LIST=ENG,TEST1,IND UNTIL_TIME="2020-02-12-04.14.41" JOBID=Job_12332
```

5. Once the mountrecover script is completed, run the ACT_DB2_lvm_migrate_newtarget script with parameters in Arguments to the Script.

```
/act/custom_apps/db2/restore/ACT_DB2_lvm_migrate_newtarget.sh
SOURCE_INSTANCE=<SOURCE_INSTANCE> TARGET_DBNAME_LIST=<comma seperated DB LIST> JOBID=<JOBID>
DATAVOL_DISK_MAPPING=<Actifio Mountpoint>:<prod equivalent lvm device name>
ARCHIVELOG_LOC=<PROD Archivelog location>
```

Arguments to the Script

SOURCE_INSTANCE = <DB2 instance name>

TARGET_DBNAME_LIST=<comma separated list of database names>

JOBID = <Simple mount job-id>

ARCHIVELOG_LOC = <Log backup mount point name> [Mount point should be in local storage]

DATAVOL_DISK_MAPPING = Colon separated list of <Actifio_mount_point>:<production host lvm device name>

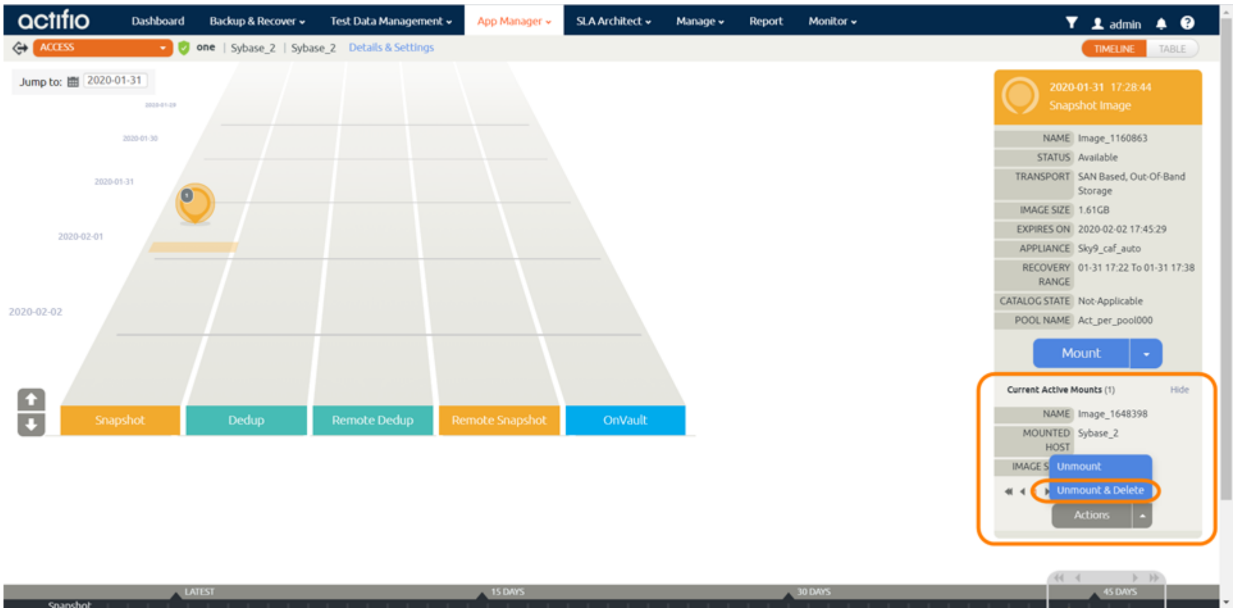
Example

```
/act/custom_apps/db2/restore/ACT_DB2_lvm_migrate_newtarget.sh SOURCE_INSTANCE=db2prod
TARGET_DBNAME_LIST=TEST1,TEST2 JOBID=Job_4488748 ARCHIVELOG_LOC=/db2gj_archivelog
DATAVOL_DISK_MAPPING=/db2gj/db2/data:/dev/mapper/vg00-vol_data,/db2gj/db2/log:/dev/mapper/
vg01-vol_log
```

6. Once the above script has completed successfully,

   a. Go to AGM and perform **Unmount+Delete**.

   b. Re-enable the Db2 instance’s SLA to trigger the scheduled jobs.



2020-01-31 17:28:44
Snapshot Image

NAME Image_1160863
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 1.61GB
EXPIRES ON 2020-02-02 17:45:29
APPLIANCE Sky9_caf_auto
RECOVERY RANGE 01-31 17:22 To 01-31 17:38
CATALOG STATE Not-Applicable
POOL NAME Act_per_pool000

Current Active Mounts (1)

NAME Image_1648398
MOUNTED HOST Sybase_2

Mount and Migrate to a New Instance

To mount a database image as a virtual database and the migrate it to a new target:

1. Perform the Application Aware mount as detailed in Mount a Virtual Database from a Block-Based Volume Snapshot Image to the Source or to an Existing Db2 Instance on page 23.

   > ***Note:*** *Enable both* ***Create New Virtual Application*** *and* ***Manage New Application****.*

2. Once the mount is completed, run the `ACT_DB2_lvm_migrate_newtarget` script with the parameters in Arguments to the Script:

```
/act/custom_apps/db2/restore/ACT_DB2_lvm_migrate_newtarget.sh
SOURCE_INSTANCE=<SOURCE_INSTANCE> TARGET_DBNAME_LIST=<comma separated DB LIST> JOBID=<JOBID>
DATAVOL_DISK_MAPPING=<Actifio mountpoint>:<prod equivalent lvm device name>
ARCHIVELOG_LOC=<PROD Archivelog location>
```

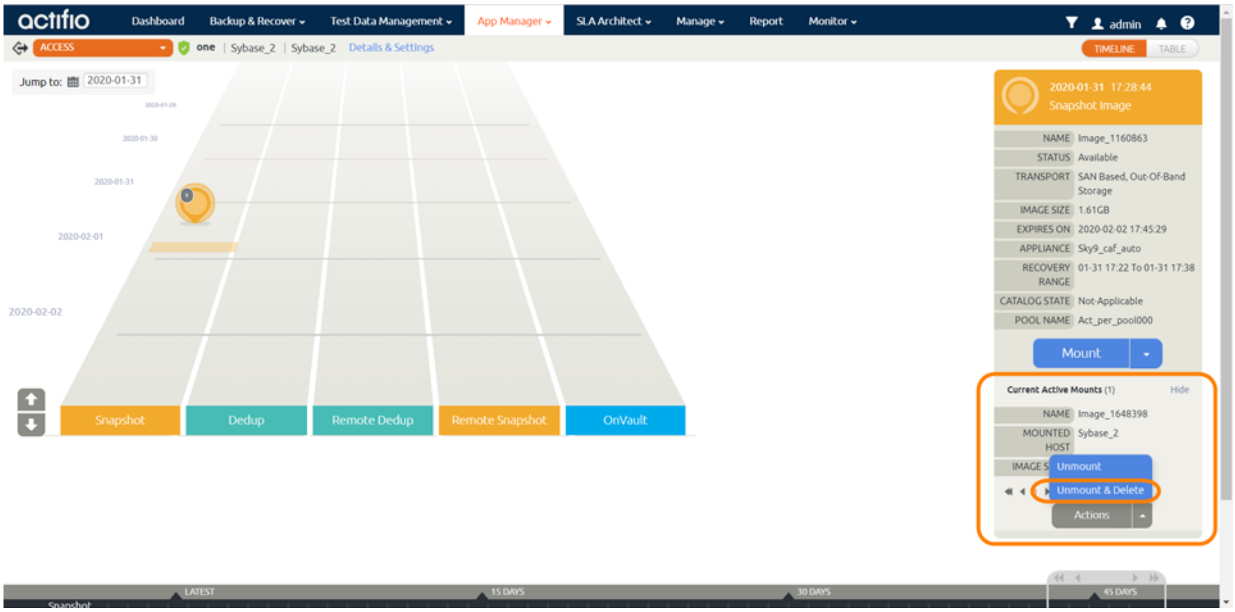
Arguments to the Script

```
SOURCE_INSTANCE = <DB2 instance name>
TARGET_DBNAME_LIST=<comma separated list of database names>
JOBID = <Simple mount job-id>
ARCHIVELOG_LOC = <Log backup mount point name> [mount point should be in local storage ]
DATAVOL_DISK_MAPPING = Colon separated list of <Actifio_mount_point>:<production host lvm
device name>
```

Example

```
/act/custom_apps/db2/restore/ACT_DB2_lvm_migrate_newtarget.sh SOURCE_INSTANCE=db2prod
TARGET_DBNAME_LIST=TEST1,TEST2 JOBID=Job_4488748 ARCHIVELOG_LOC=/db2gj_archivelog
DATAVOL_DISK_MAPPING=/db2gj/db2/data:/dev/mapper/vg00-vol_data,/db2gj/db2/log:/dev/mapper/
vg01-vol_log
```

3. Once the script completes successfully, go to AGM and perform an Unmount+Delete.



2020-01-31 17:28:44
Snapshot Image

NAME Image_1160863
STATUS Available
TRANSPORT SAN Based, Out-Of-Band Storage
IMAGE SIZE 1.61GB
EXPIRES ON 2020-02-02 17:45:29
APPLIANCE Sky9_caf_auto
RECOVERY RANGE 01-31 17:22 To 01-31 17:38
CATALOG STATE Not-Applicable
POOL NAME Act_per_pool000

Current Active Mounts (1)

NAME Image_1648398
MOUNTED HOST Sybase_2
IMAGE S

8 Converting Existing Generic Applications to the New Framework

Actifio VDP 10.0.2 introduced a new, more robust framework for database applications running on Linux. In earlier versions, databases were captured using the generic application framework. In most cases, it is worth recapturing the database using the new framework.

The new DB Application framework provides these benefits:

- No manual intervention needed for discovery, protection and recovery
- Application aware - discovers the database as an application
- No more need to configure pre and post scripts like with Generic applications.
- Automated protection for databases as well as logs under a single application
- Automated point in time recovery
- App Aware mount capability for LVM snapshot-based protection

To switch from Generic Application protection to the new DB App Framework:

1. Disable the protection schedule on the Generic Application.
2. Under AGM Application tab, look for the database instance name as a discovered application. If it's not discovered, run a discovery on the host as described in Discovering the Db2 Instance Application from the App Manager.
3. Apply the SLA to the discovered database instance as detailed in Chapter 4, Protecting the Db2 Instance and its Logs.
4. Let the generic app backup images expire on their own schedule while you build your new repository of backup images using new database allocation framework.