
IBM Db2 DBA's Guide to Actifio Copy Data Management

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2019 Actifio, Inc. All rights reserved.

Actifio[®], AnyIT[®], Dedup Async[®], OnVault[®], Enterprise Data-as-a-Service[®], FlashScan[®], AppFlash DEVOPS Platform[®], Copy Data Cloud[®], and VDP[®] are registered trademarks of Actifio, Inc.

Actifio Sky[™], Actifio One[™], and Virtual Data Pipeline[™] are trademarks of Actifio, Inc.

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

Actifio, Inc., is a provider of data protection and availability products. Actifio's technology is used in products sold by the company and products and services sold and offered by its commercial partners. The current list of Actifio patents is available online at: <http://www.actifio.com/patents/>

Actifio believes the information in this publication is accurate as of its publication date. Actifio reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ACTIFIO, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This software and the associated documentation are proprietary and confidential to Actifio. Use, copying, and distribution of any Actifio software described in this publication requires an applicable software license. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

Actifio strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to docs@actifio.com.

Contents

The ActifioNOW Customer Portal.....v	v
Actifio Support Centersv	v
Chapter 1 - Introducing the Actifio Virtual Data Pipeline for IBM Db2 Databases	1
Actifio Data Virtualization	1
Capturing Data.....	3
Replicating Data	3
Accessing Data	4
Chapter 2 - Adding a Db2 Database Host and Discovering the Database	7
Adding the Host from the Domain Manager	7
Discovering the Db2 Database from the Application Manager	9
Finding the Discovered Db2 Database in the Application Manager.....	9
Chapter 3 - Configuring the Backup Method	11
Configuring SLA Settings	11
Ensuring that the Backup Capture Method is Set Correctly.....	13
Ensuring that the Disk Preference on the Host is Set Correctly.....	14
Disk Preference: File-Based Traditional Backup and Recovery in NFS/Block.....	14
Disk Preference: LVM Snapshot with Change Block Tracking on Linux	15
Disk Preference: GPFS on AIX.....	16
Setting the Schedule for Dumps	17
Chapter 4 - Protecting the Db2 Database	19
Protecting an IBM Db2 Database	19
Protecting IBM Db2 Database Logs	21
Chapter 5 - Restoring, Accessing, or Recovering a Db2 Database	25
Mount and Refresh from Block-Based Volume Snapshot to a Target Db2 Instance as a Virtual Application 25	
Restoring and Recovering a Db2 Database.....	28
Recovering from Volume based Snapshot.....	28
Recovering from a Full+Incremental Backup.....	30

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.

Full documentation is in the AGM online help, and on ActifioNOW. The following guides will be of particular interest:

- ***Connecting Hosts to Actifio Appliances***
- ***Network Administrator's Guide to Actifio VDP***

The ActifioNOW Customer Portal

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

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

To log into the ActifioNOW customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

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

From anywhere: +1.315.261.7501

US Toll-Free: +1.855.392.6810

Australia: 0011 800-16165656

Germany: 00 800-16165656

New Zealand: 00 800-16165656

UK: 0 800-0155019

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](#) on page 1

[Capturing Data](#) on page 3

[Replicating Data](#) on page 3

[Accessing Data](#) on page 4

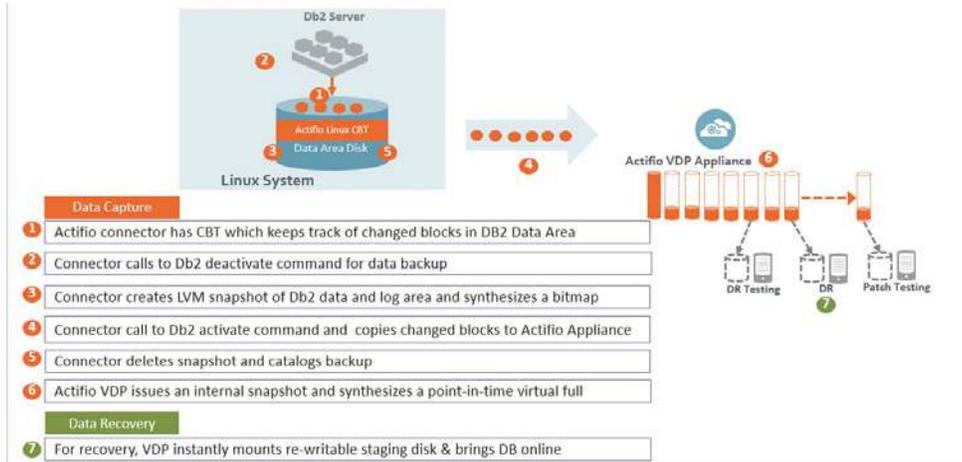
Actifio Data Virtualization

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.

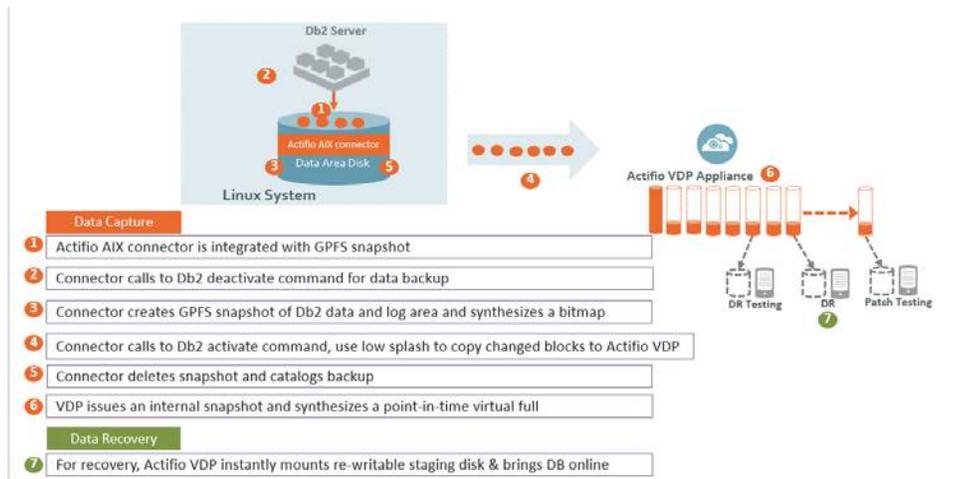
Db2 is a family of relational database management systems within IBM's Information Management division that is centered on several relational database management system offerings. This section explains how to protect Db2 application consistent database data with Actifio VDP in Linux and AIX environments.

Db2 backup API used by Actifio:

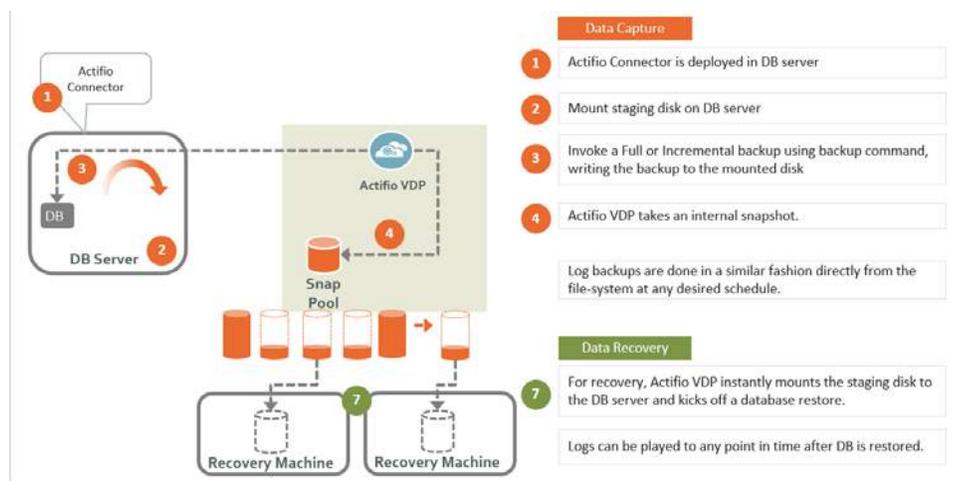
- Linux CBT and LVM snapshot: Db2 database deactivate and activate API with Linux CBT and LVM snapshot
- IBM Spectrum Scale (GPFS) snapshot on AIX: Db2 database deactivate and activate API with GPFS snapshot on AIX.
- File-based backups: Db2 database API "Db2 backup db online" file-based backups provide 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.



Db2 with Actifio Linux CBT



Db2 with Actifio GPFs Snapshot on AIX



Db2 with Actifio File-Based Backup

Capturing Data

Capturing data consists of four simple 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 a generic 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 addresses these issues with a global deduplication and compression approach that:

- 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 VMware Site Recovery Manager (SRM) and 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.
- Dedup Backup to Dedup DR policies use a fixed, Actifio-proprietary replication engine to replicate data to a second Actifio Appliance. In addition, Dedup Backup to Dedup DR policies allow you to replicate data to two locations.
- 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, Restoring, Accessing, or Recovering a Db2 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.

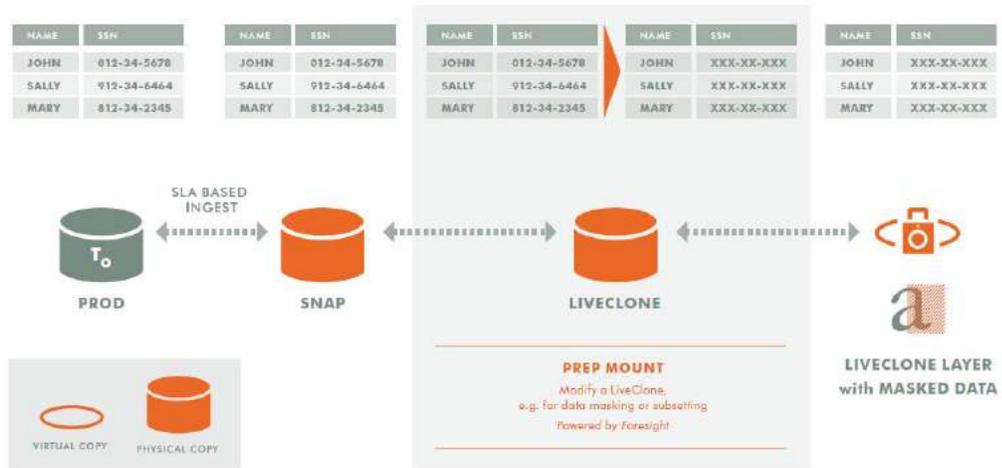
Combining VDP's automated data capture and access control with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait for DBAs to update test and development environments, users can provision their own environments almost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



Workflow With Masked Social Security Data

2 Adding a Db2 Database Host and Discovering the Database

Before You Begin

The 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

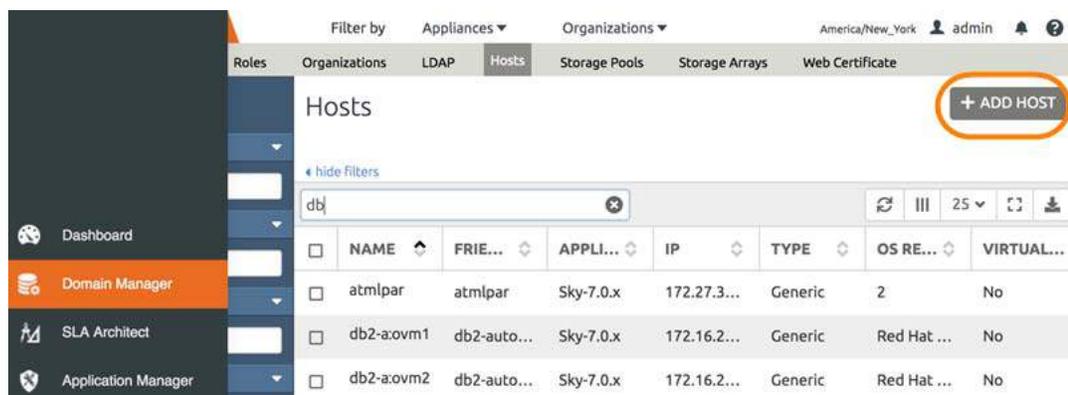
Before you can protect a Db2 database, you must add the host and discover the database. This requires:

1. [Adding the Host from the Domain Manager](#) on page 7
2. [Discovering the Db2 Database from the Application Manager](#) on page 9
3. [Finding the Discovered Db2 Database in the Application Manager](#) on page 9

Adding the Host from the Domain Manager

Add the host to Domain Manager. If the host is already added then edit the host and make sure to set the Disk Preference correctly.

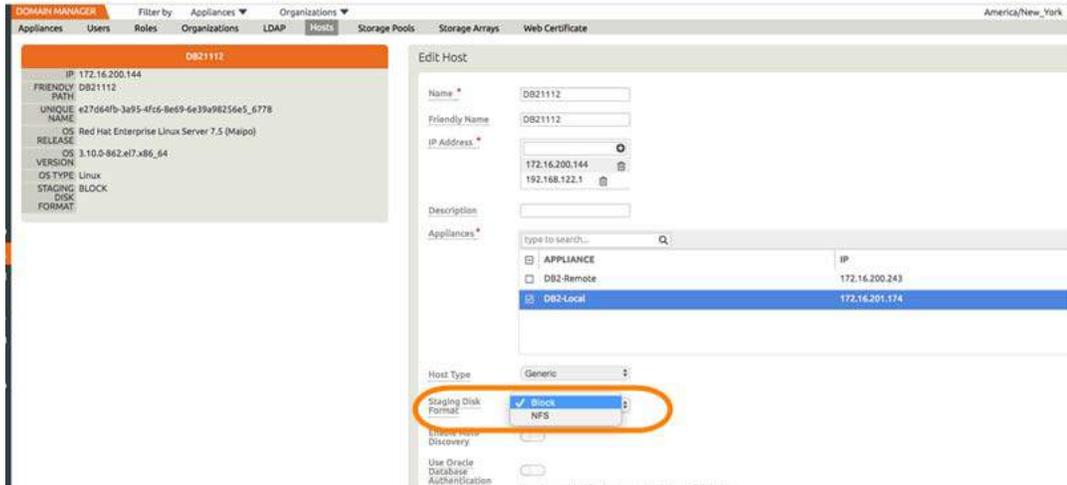
1. From the AGM Domain Manager, Hosts tab, click **+Add Host**.



2. On the Add Host page:
 - o **Name:** Provide the database server name.
 - o **IP Address:** Provide the database server IP and click the + sign on the right corner.
 - o **Appliances:** Select the check box for the appliance.
 - o **Host Type:** Make sure this is Generic.
3. Click **Add** at bottom right to add the host.

The Host is added.

4. Right-click the host and select **Edit**.
5. On the Edit Host page: Select the **disk preference**:
 - o For block-based backup with CBT or GPFS: select **Block**
 - o For file-based backup with Full+Incremental file system backup: select **Block** or **NFS**



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

Discovering the Db2 Database from the Application Manager

To discover the Db2 database application:

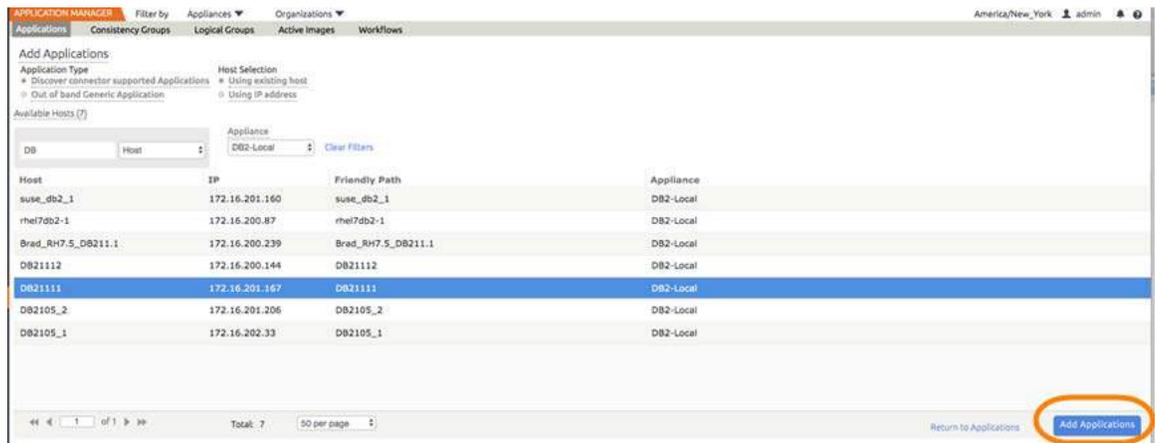
1. From the AGM Application Manager, Applications tab, select **Add Application** in the upper right corner.



2. On the Add Application page, select **Discover connector supported applications** and **Using existing host**, then select the Db2 database host. If you have many hosts, you can use the search feature or use the filter to see only hosts that are managed by a specific Actifio Appliance.



3. Select the host and click **Add Applications** in the bottom right corner. This will run the discovery on the database host and will discover all Db2 databases running on it.



Finding the Discovered Db2 Database in the Application Manager

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



3 Configuring the Backup Method

After the database is prepared and discovered as explained in [Chapter 2, Adding a Db2 Database Host and Discovering the Database](#), you can configure a VDP backup method for the database.

Whichever method you select involves these steps:

[Configuring SLA Settings](#) on page 11

[Ensuring that the Backup Capture Method is Set Correctly](#) on page 13

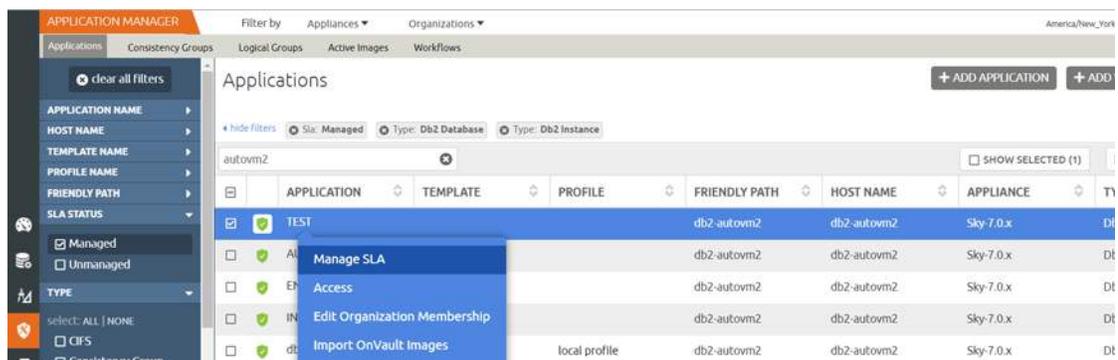
[Ensuring that the Disk Preference on the Host is Set Correctly](#) on page 14

[Setting the Schedule for Dumps](#) on page 17

Configuring SLA Settings

To configure the database SLA settings:

1. In the AGM Application Manager, 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 specific details and settings for this database. Of particular importance is Backup Capture Method.

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

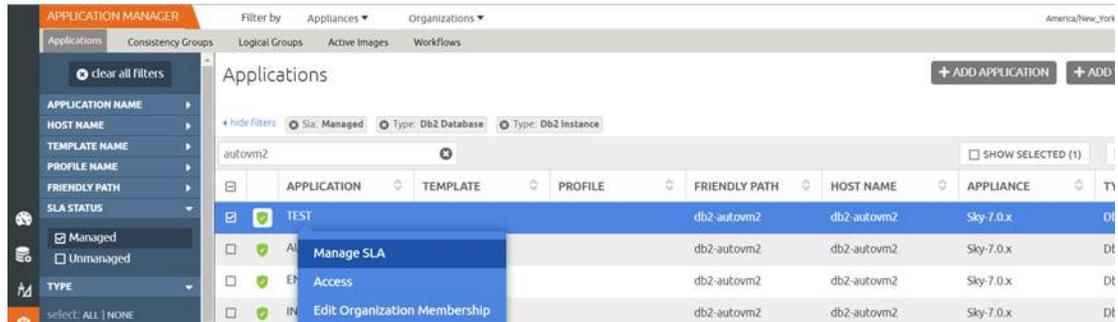
Setting	Block-Based LVM Snapshot with CBT on Linux	Block-Based GPFS Snapshot on AIX	File-Based Backup and Recovery, Block or NFS
Percentage of Reserve Space in Volume Group	This is needed for LVM snapshot temporary space. Recommended value is 20%		Not applicable
Backup Capture Method	Use Volume Level Backup		Use full+incremental filesystem backup
Force Full Filesystem Backup	Not applicable		Use for an ad hoc 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.		

File-based backup also requires the dump schedule to be configured. See [Setting the Schedule for Dumps](#) on page 17.

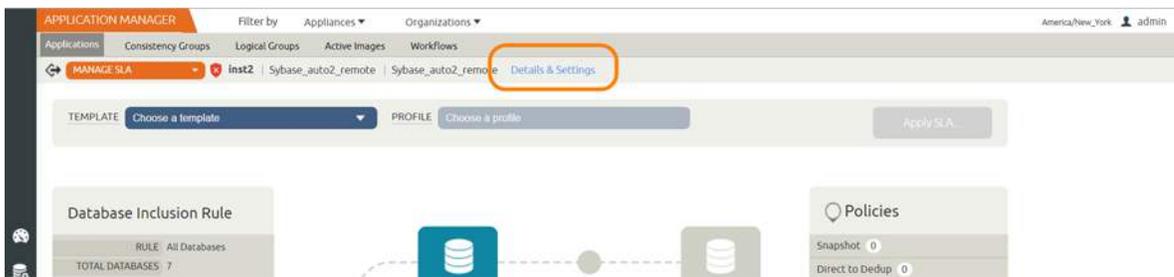
Ensuring that the Backup Capture Method is Set Correctly

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

1. In the AGM Application Manager, right-click the database and select **Manage SLA**.

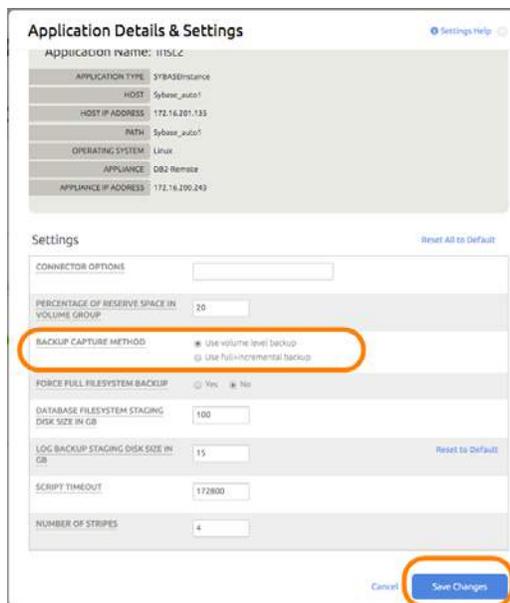


2. At the top of the Manage SLA page, select the **Details & Settings** link:



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

- o Db2 Traditional Backup and Recovery API "file-based" backups: **Use full+incremental backup**
- o LVM Snapshot with Change Block Tracking: **Use volume level backup**
- o GPFS on AIX: **Use volume level backup**



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

Ensuring that the Disk Preference on the Host is Set Correctly

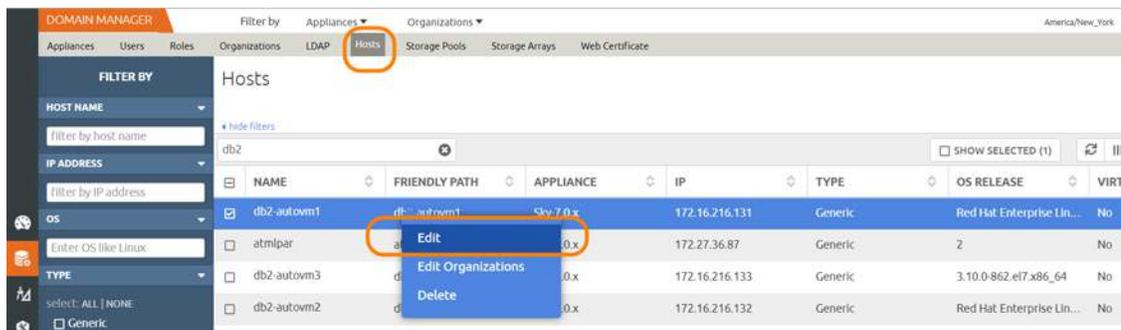
Choose between:

- Disk Preference: File-Based Traditional Backup and Recovery in NFS/Block on page 14
- Disk Preference: LVM Snapshot with Change Block Tracking on Linux on page 15
- Disk Preference: GPFS on AIX on page 16

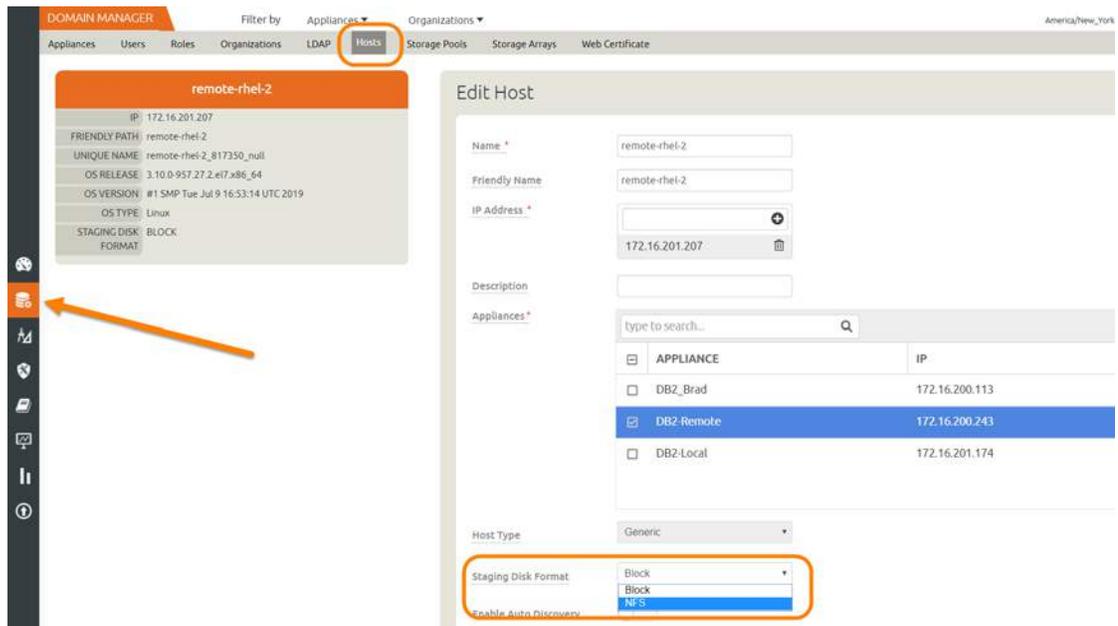
Disk Preference: File-Based Traditional Backup and Recovery in NFS/Block

To set disk preference for storage snapshots:

1. From AGM Domain Manager, Hosts tab, right-click the host and select **Edit**.



2. Set Disk Preference to **NFS** or to **Block**.



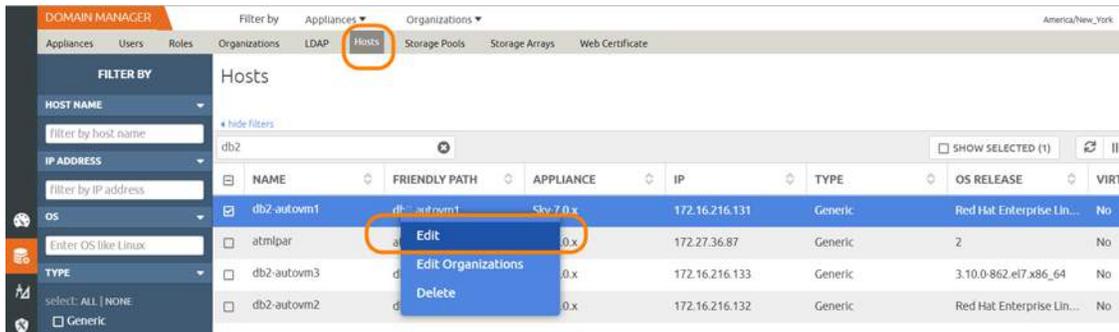
3. Then click **Save** at the bottom of the page.

Note: File-based backup also requires the DB dump schedule be configured. See [Setting the Schedule for Dumps](#) on page 17.

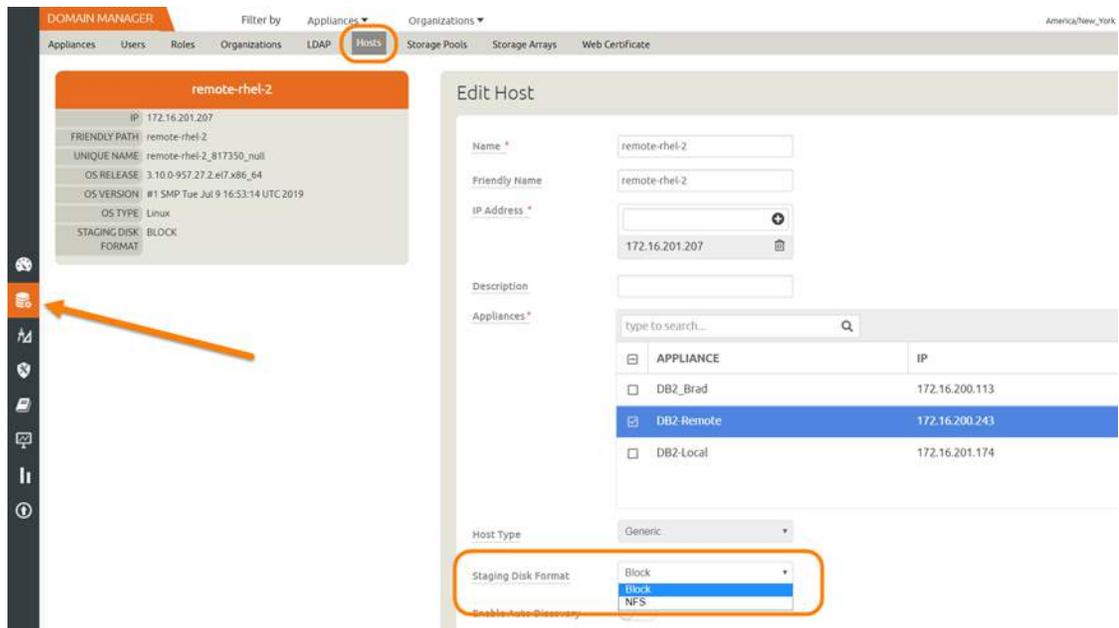
Disk Preference: LVM Snapshot with Change Block Tracking on Linux

To set disk preference for storage snapshots:

1. From AGM Domain Manager, Hosts tab, right-click the host and select **Edit**.



2. Set Disk Preference to **Block**.

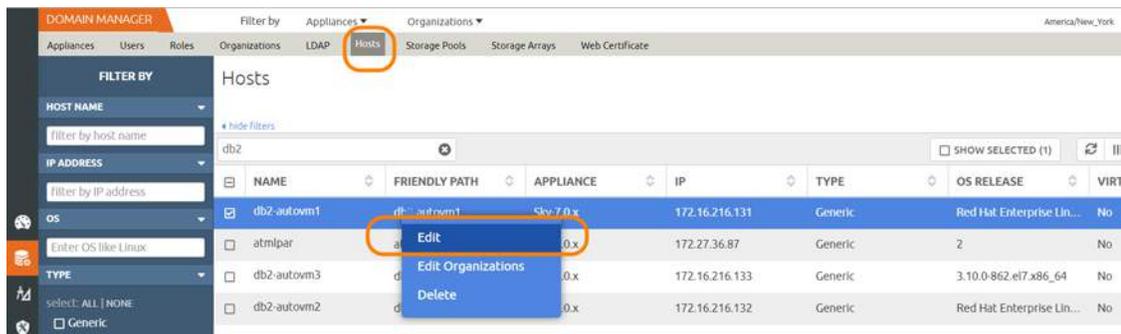


3. Then click **Save** at the bottom of the page.

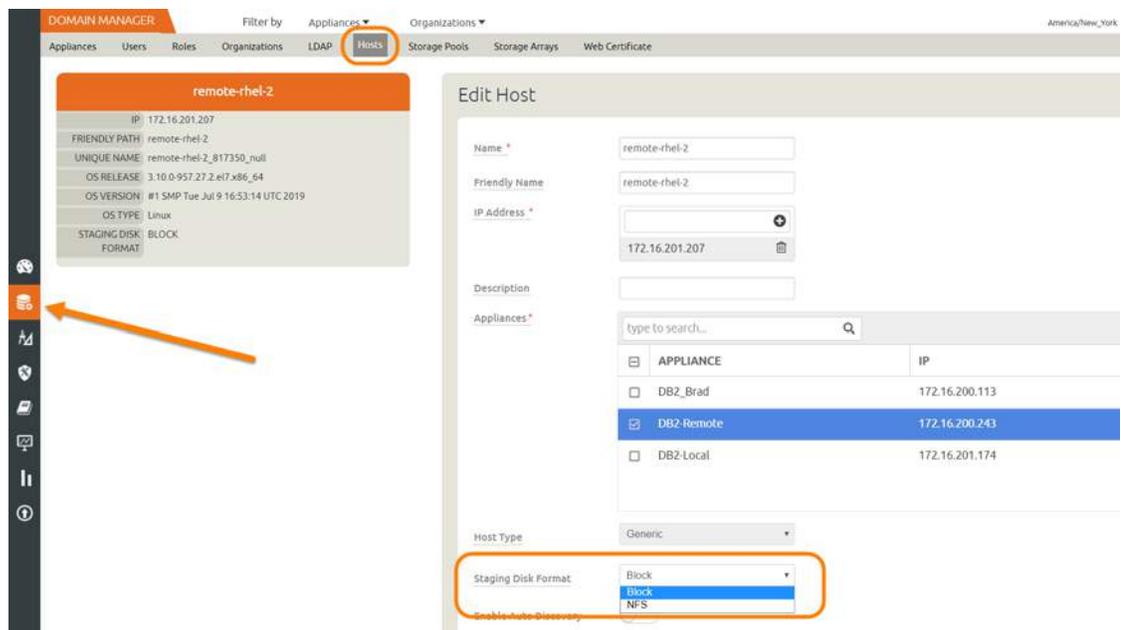
Disk Preference: GPFS on AIX

To set disk preference for storage snapshots:

1. From AGM Domain Manager, Hosts tab, right-click the host and select **Edit**.



2. Set Disk Preference 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 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 Appliance:

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

Replace `<appid>` with the application id of the Db2 application.

Replace "FIIIIII" as needed.

Example

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

4 Protecting the Db2 Database

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

This chapter includes:

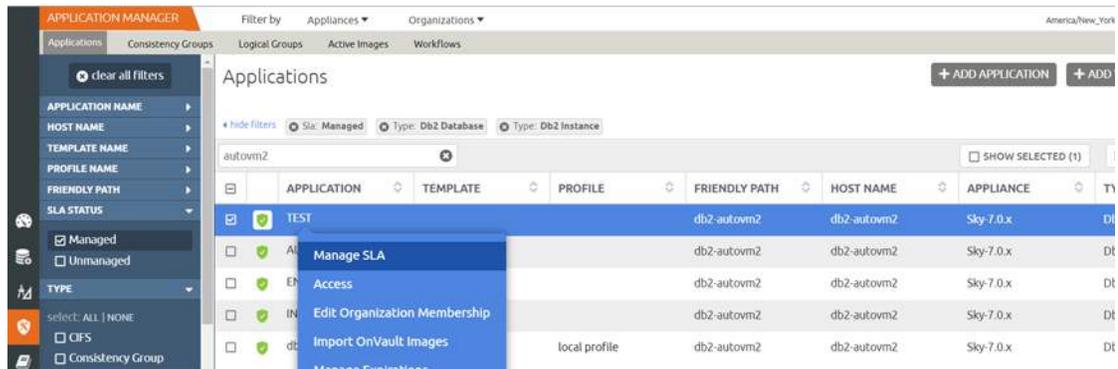
[Protecting an IBM Db2 Database](#) on page 19

[Protecting IBM Db2 Database Logs](#) on page 21

Protecting an IBM Db2 Database

To protect the database:

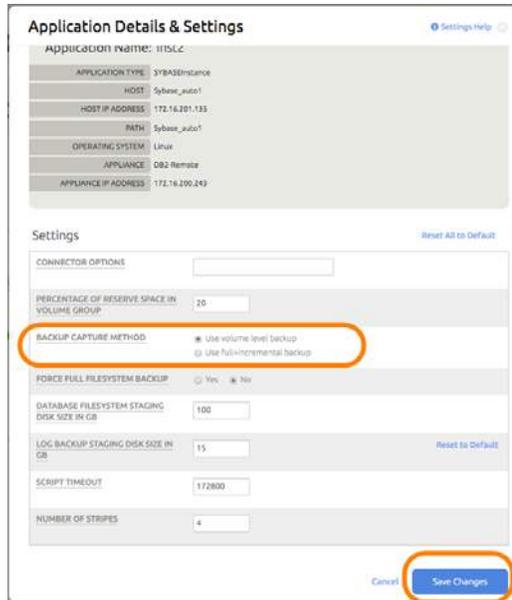
1. From the AGM Application Manager, right-click the database and select **Manage SLA**.



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

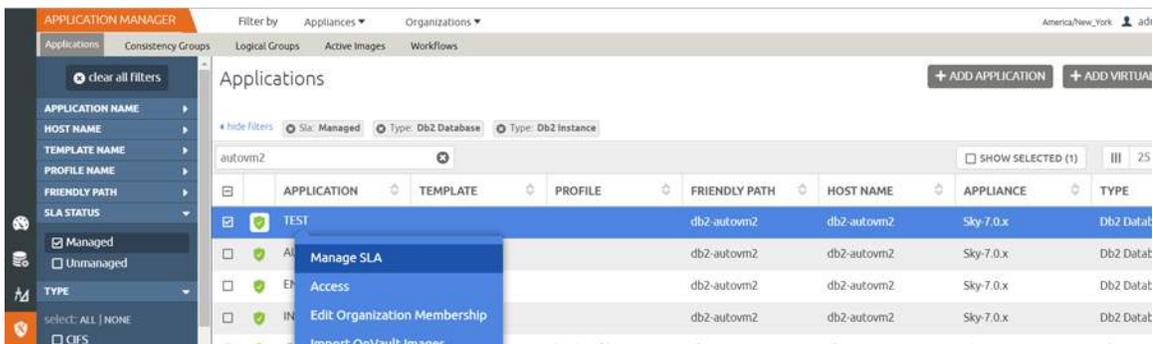


3. On the Apply SLA page, make sure that the backup capture method matches the type of backup set in [Chapter 3, Configuring the Backup Method](#). Click **Apply SLA** or **Save Changes**.

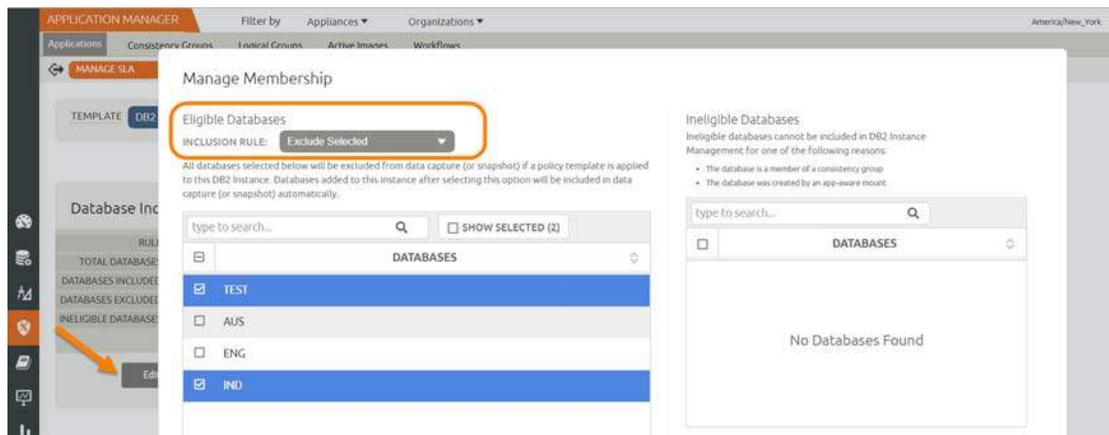


The database will be protected when the snapshot job runs according to the schedule in the template. After the first successful snapshot job the database appears in the Application Manager with a green shield icon.

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



5. Under Database Inclusion Rule, click **Edit**.

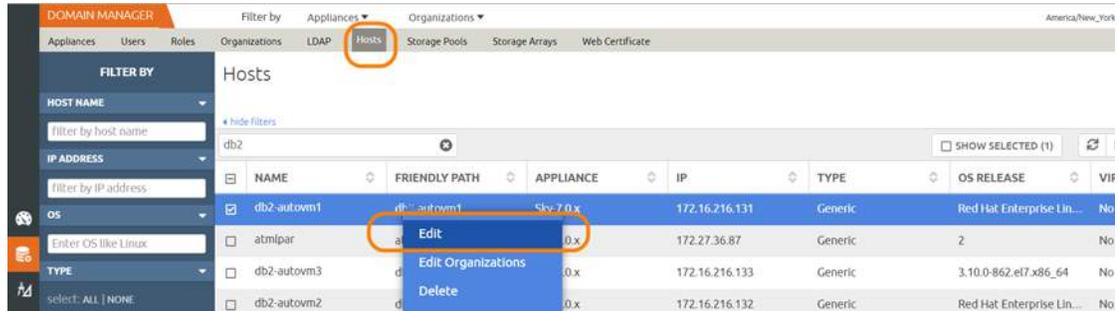


6. Select an Inclusion Rule (Include All, Include Selected, or Exclude Selected) and then select the databases to include or exclude, then click **Save**.

Protecting IBM Db2 Database Logs

To enable and set up the Db2 database log backup:

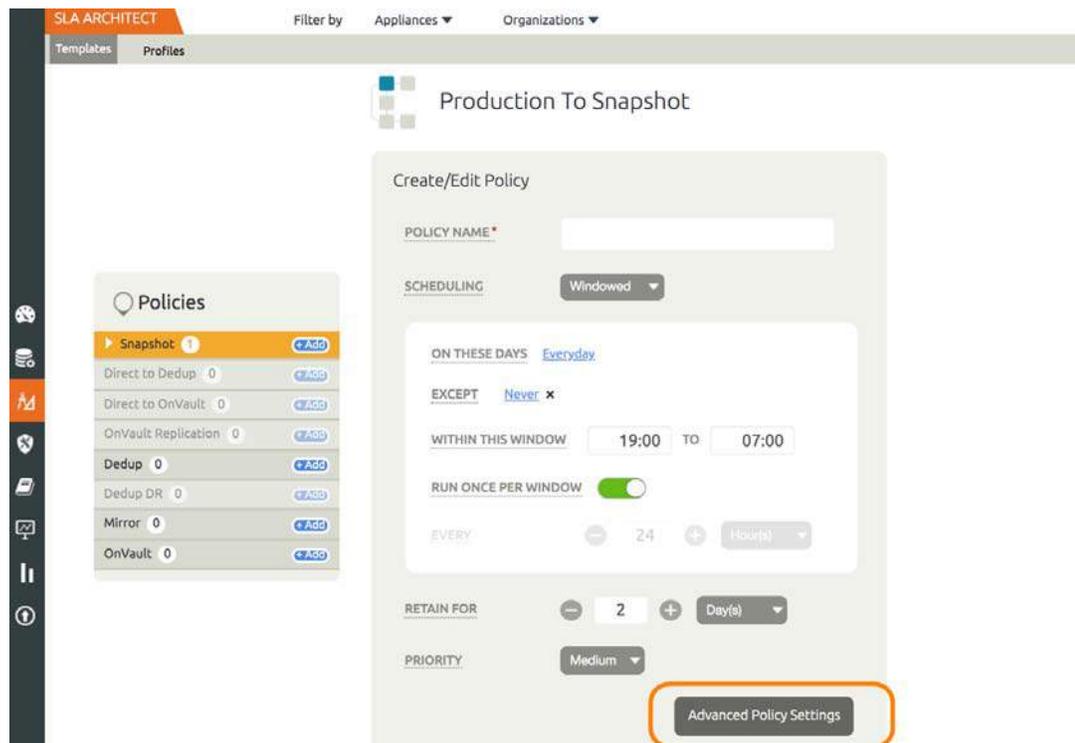
1. From the AGM SLA Architect page, right-click the template for Db2 database protection and click **Edit**.



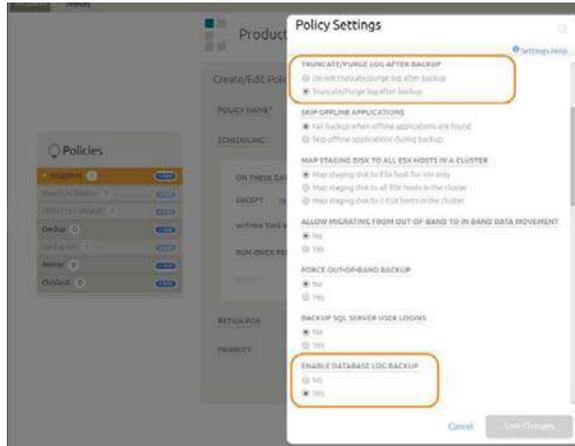
2. Click the arrow beside the Snapshot policy to open up the details, then click **Edit Policy**.



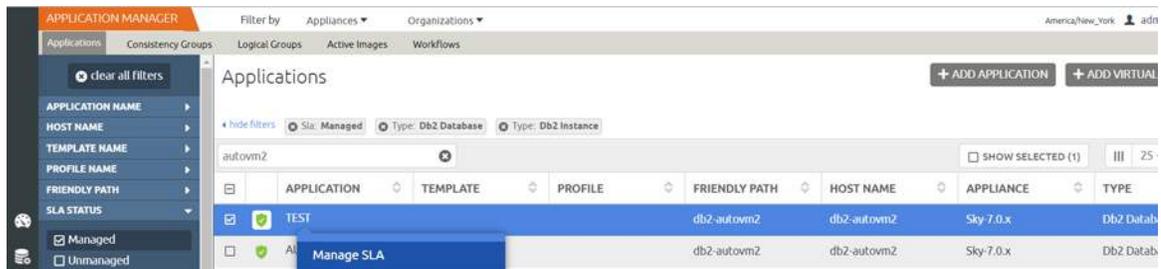
3. Near the bottom, select **Advanced Policy Settings**.



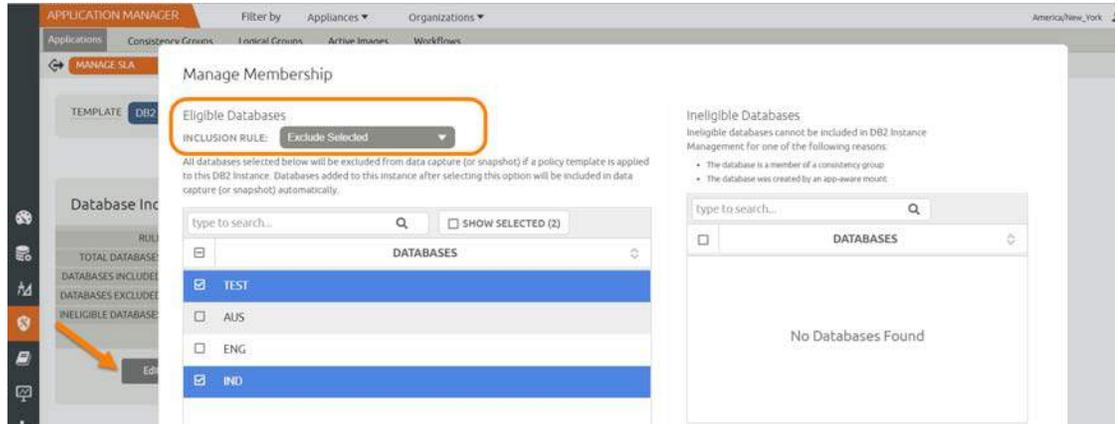
4. Set the log policy options (you will have to scroll to see them all):
 - o Enable **Truncate/Purge log after backup**.
 - o Set **Enable Database Log Backup** to **Yes**.
 - o For **RPO (Minutes)**, enter the desired frequency of log backup.
 - o Set **Log Backup Retention Period (in Days)** for point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



5. Click **Save Changes**.
6. From Application Manager, 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 than the # of days specified. Default value is 0 days. With the default value, all logs prior to last log backups are purged.
9. You can include or exclude specific database logs during backup. From the Application Manager, select the Db2 Instance. Select **Manage SLA**.
10. Under Database Inclusion Rule, click **Edit**.



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

5 Restoring, Accessing, or Recovering a Db2 Database

This section describes:

[Mount and Refresh from Block-Based Volume Snapshot to a Target Db2 Instance as a Virtual Application on page 25](#)

[Restoring and Recovering a Db2 Database on page 28](#)

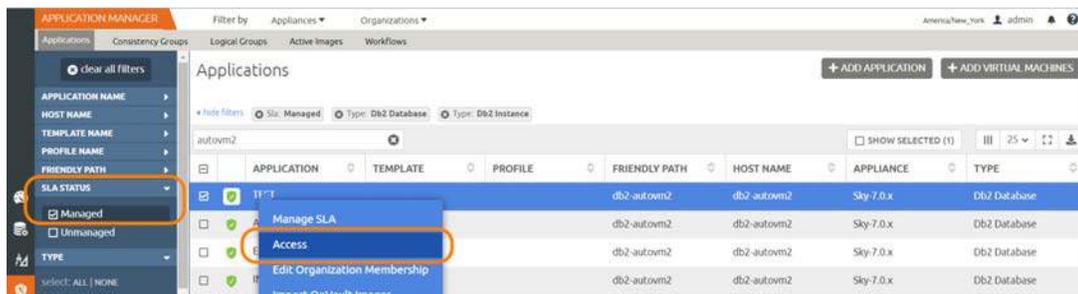
- o [Recovering from Volume based Snapshot on page 28](#)
- o [Recovering from a Full+Incremental Backup on page 30](#)

Mount and Refresh from Block-Based Volume Snapshot to a Target Db2 Instance as a Virtual Application

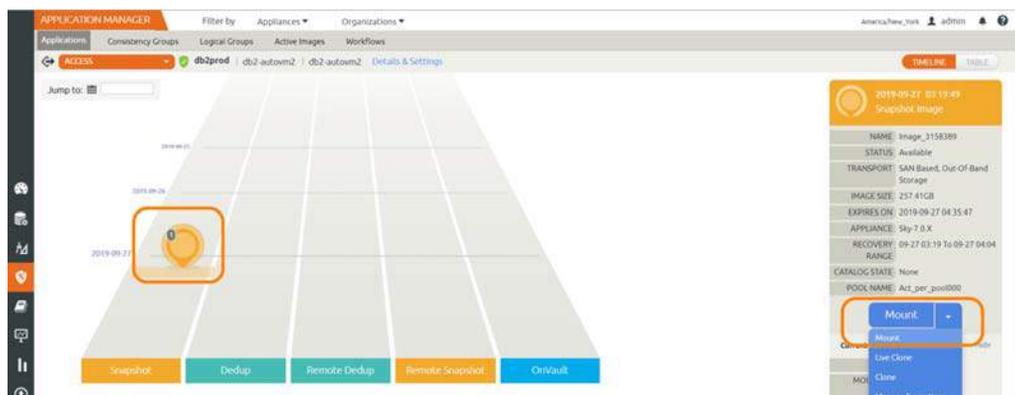
To mount the database image as a virtual application (an application aware mount) to a new target:

1. From the AGM Application Manager, right-click the protected database and select **Access**.

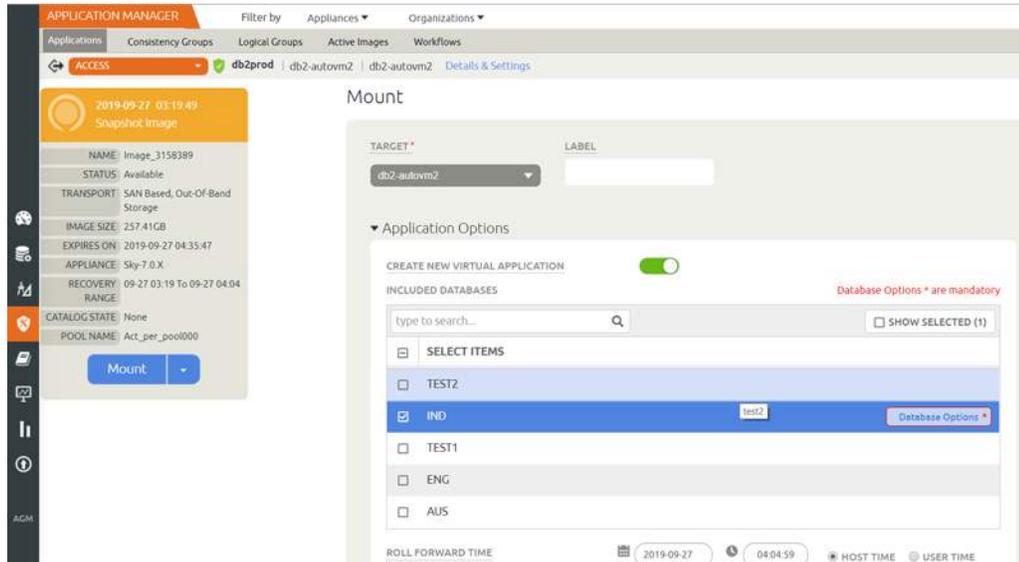
Note: You can use the Managed SLA Status filter to show only protected databases.



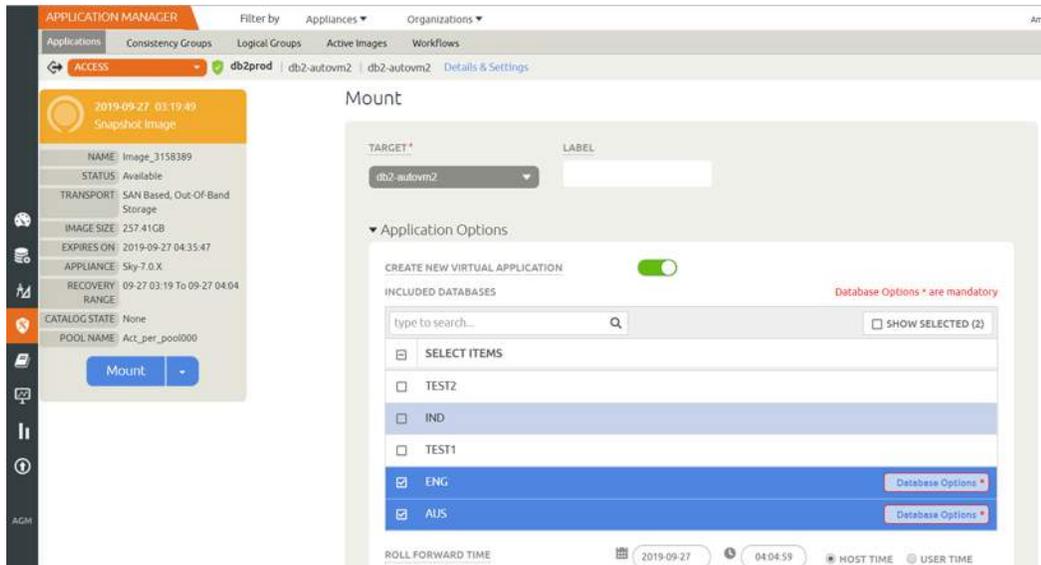
2. Select a snapshot image and choose **Mount**.



3. On the Mount page, from Target, choose the desired target Db2 server from the dropdown.
4. Under Application Options, enable **Create New Virtual Application**.
5. At Included Databases, Select Items, choose one or more databases to virtualize:
 - o A single database will be managed as standalone virtual copy
 - o Multiple databases will be managed as a consistency group

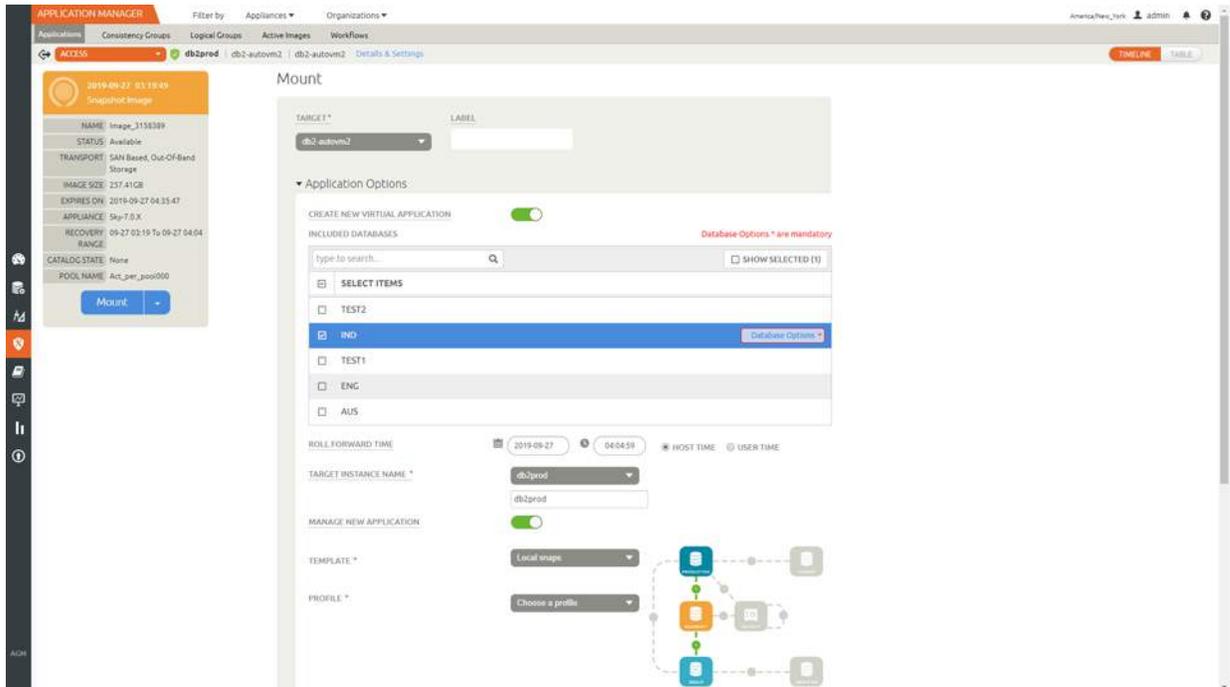


Selecting a Single Database



Selecting Multiple Databases

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



- Choose a target point in time for a database protected with log roll-forward.

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

TARGET Db2 INSTANCE NAME: From drop down select target Db2 instance to attach the selected database as virtual copy.

Manage New Application

 - To protect the new virtual database, click and enable Manage New Application.
 - Choose a template and a resource profile to protect the database.
- Under Mapping Options, Mount Location, specify a target mount point to mount the new virtual database to.
- Click **Submit**.

Restoring and Recovering a Db2 Database

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

[Recovering from Volume based Snapshot](#) on page 28

[Recovering from a Full+Incremental Backup](#) on page 30

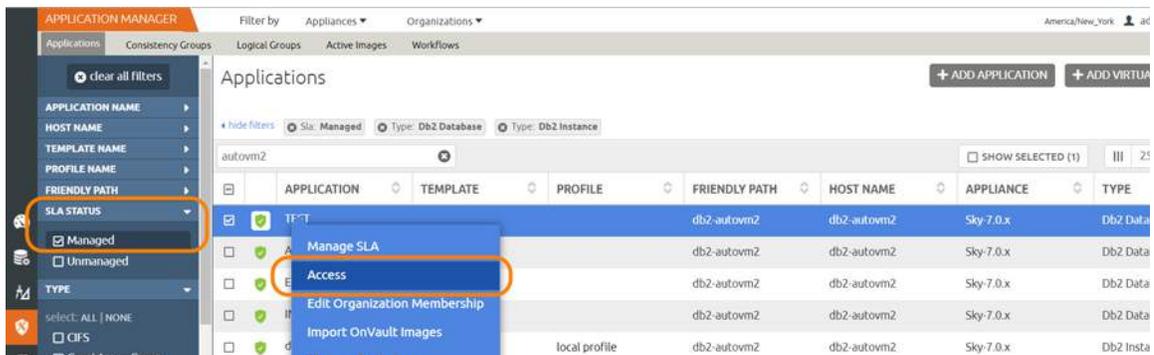
Recovering from Volume based Snapshot

Use this procedure to restore and recover the source Db2 database. This procedure uses physical recovery of the source data area.

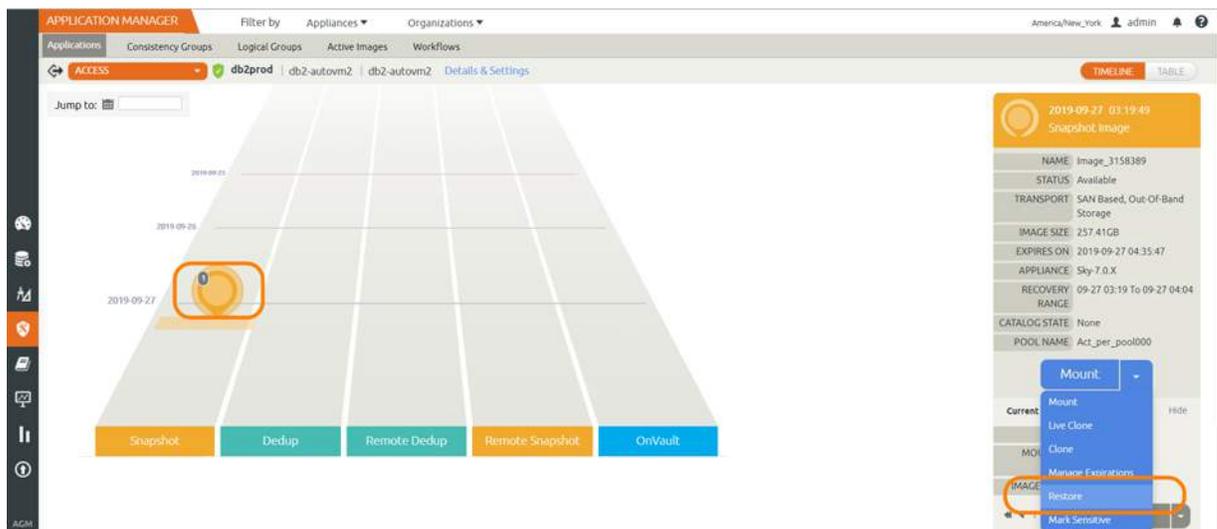
To recover back to the source:

1. From the AGM Application Manager, right-click the protected database and select **Access**.

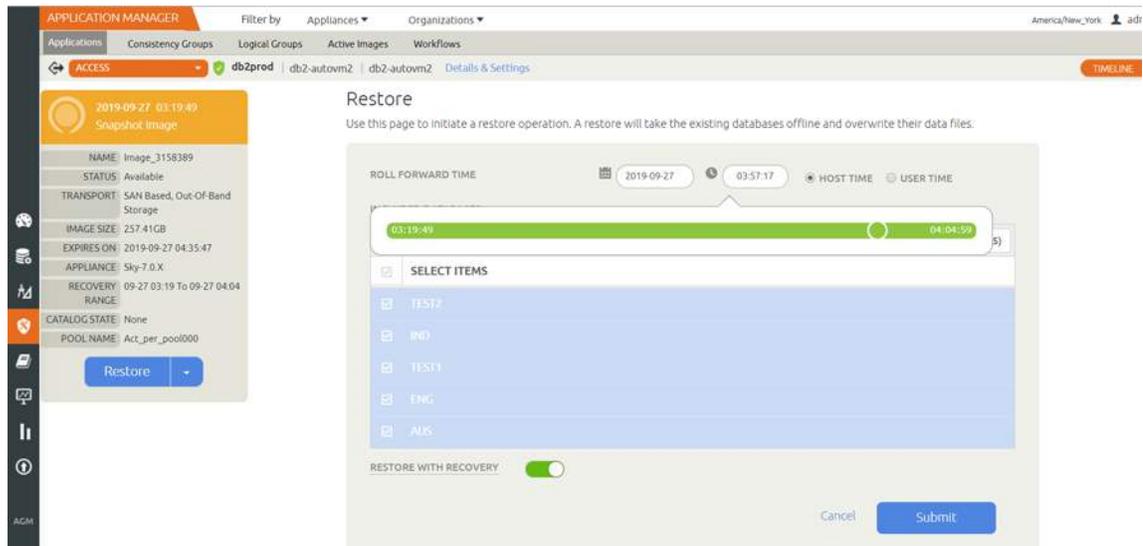
Note: You can use the Managed SLA Status filter to show only protected databases.



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



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



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

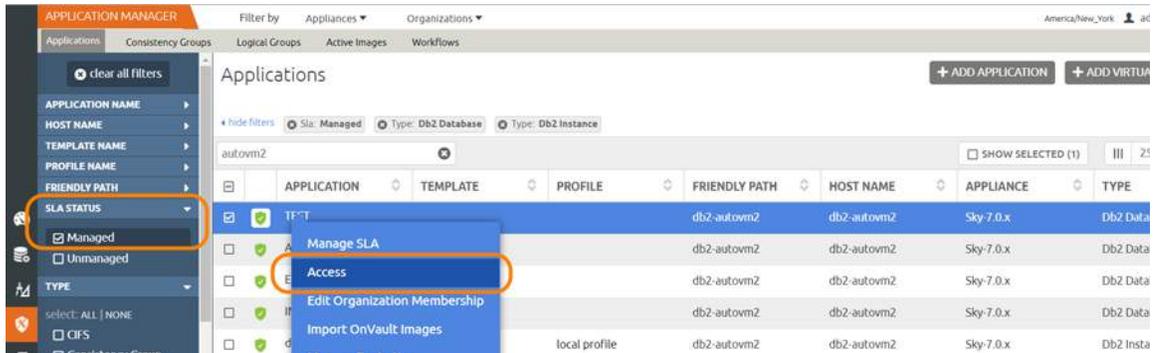
Recovering from a Full+Incremental Backup

Recovering Back to the Source: Use this procedure to restore and recover the source Db2 database. This procedure overwrites the source data.

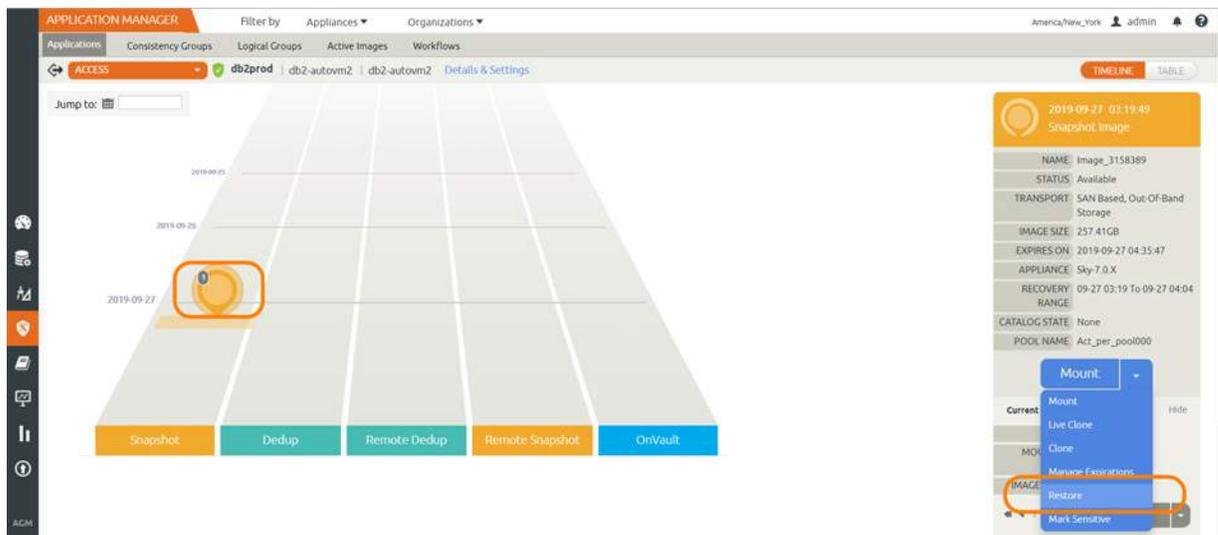
Recovering Back to the Source

1. From the AGM Application Manager, right-click the protected database and select **Access**.

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



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



3. 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.