SAP ASE DBA's Guide to Actifio GO

Updated August 24, 2022

Actifio GO

Contents

Preface

The information presented in this guide is intended for users who are familiar with basic Actifio processes as described in ***Getting Started with Actifio GO*** and who are qualified to administer SAP ASE databases.

The ActifioNOW Customer Portal

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

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

To log into the ActifioNOW customer portal:

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

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

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

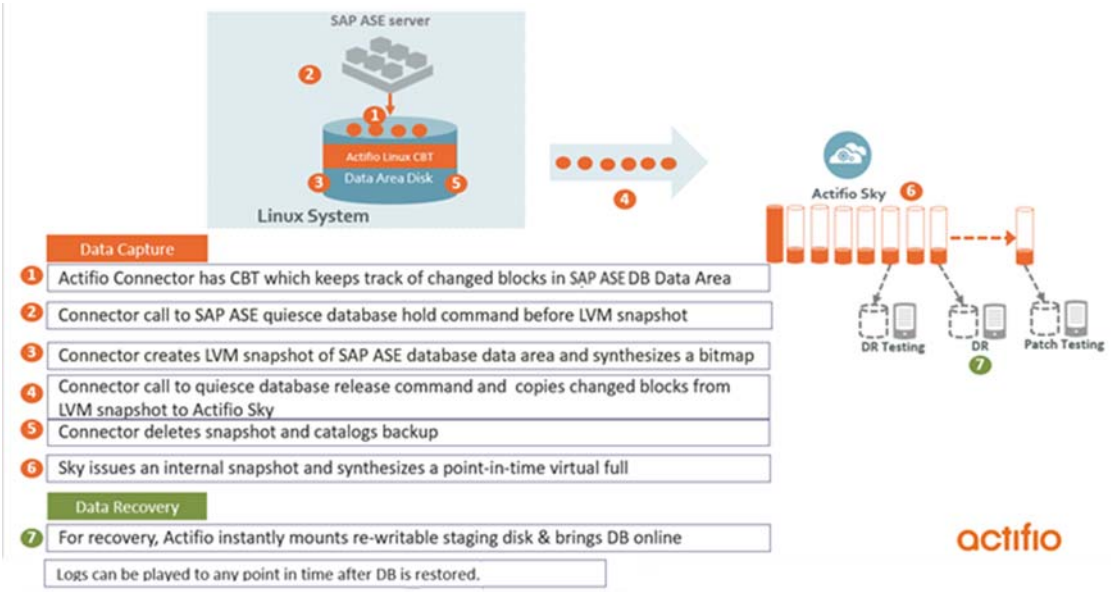
Actifio Data Virtualization

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.

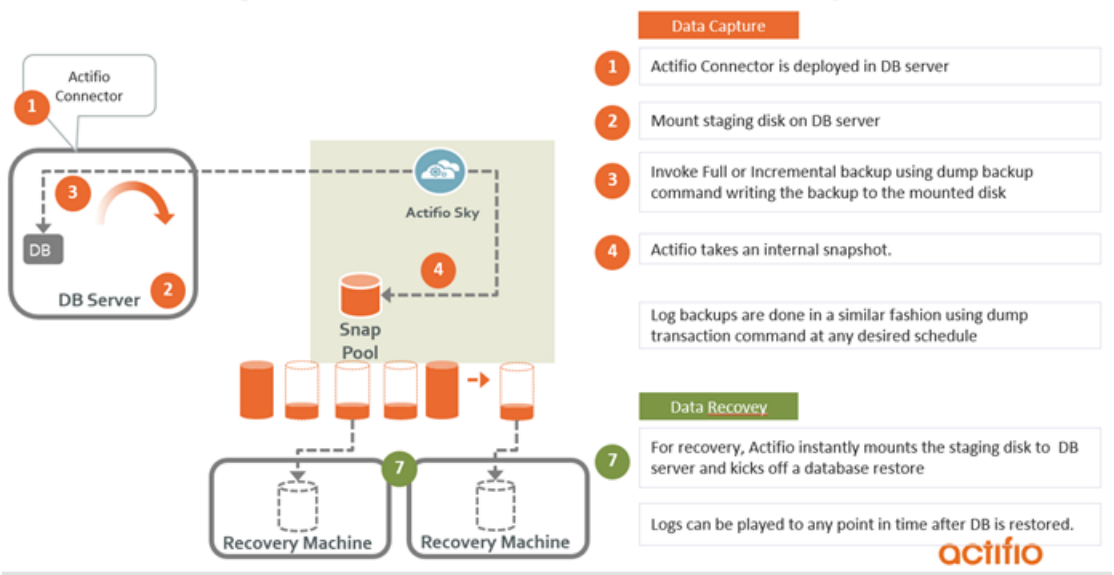
SAP ASE (formerly Sybase ASE) is a is a family of relational database management systems within SAP Information Management division that is centered on several relational database management system offerings. This DBA Guide explains how to protect SAP ASE application consistent database data with Actifio VDP in a Linux environment.

Actifio VDP uses these SAP ASE backup APIs:

- **Linux CBT and LVM snapshot**: SAP ASE "quiesce database hold and quiesce database release" API with Linux CBT and LVM snapshot
- **File-based backups**: SAP ASE "dump database" File-based backups API. This provides the full and incremental backups of the database in backup format. On recovery, the restore db API will recover the database by physically overwriting the data area.
- **Log backup**: During a log backup the "dump transaction" API called to dump logs to an Actifio log staging disk.



SAP ASE Volume-Based Backup with Linux Change Block Tracking



SAP ASE full+incremental File-Based Backup

Capturing Data

Capturing data consists of four simple steps:

1. Add servers that host databases.
2. Discover the databases.
3. Define Actifio Policy Templates and Resource Profiles according to your RPOs and RTOs.
4. Assign Actifio Policy Templates and Resource Profiles to discovered databases. The jobs will run on schedule defined in the policy template.

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:

- Uses Linux changed block tracking to capture data at block level in incremental forever fashion.
- Identifies changes to database data for VDP'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 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). Accessing protected data is discussed in Chapter 5, Accessing an SAP ASE Instance as a Standard Mount or as a Virtual Database.

Access options include:

- Mounts
- LiveClones
- Restores
- Workflows

Mounts

The 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. Application Aware mounts are described in Chapter 5, Accessing an SAP ASE Instance as a Standard Mount or as a Virtual Database.

LiveClones

The LiveClone is an independent copy of data that can be refreshed when the source data changes. The advantage of LiveClones is that they are independent copies of data that can be incrementally refreshed and masked before being made available to users. This allows teams such as development and test to ensure they are working on the latest set of data without having to manually manage the data and not access or interfere with the production environment.

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. Restores are described in Chapter 6, Restoring and Recovering an SAP ASE Instance Back to the Source.

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.

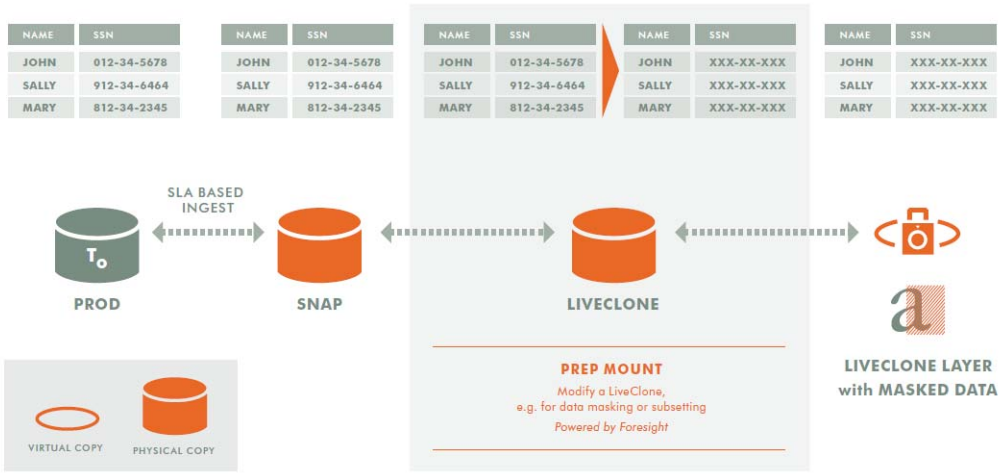
Combining VDP's automated data capture and access control with Workflows and their optional data masking capabilities allows you to create self-provisioning environments. Now, instead of having to wait for DBAs to update test and development environments, users can provision their own environments almost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

Table 1: Actifio Benefits: SAP ASE Platform

Activity	Actifio Benefits
Backup	Manual and/or scheduled online backups (incremental forever full snapshots).
Test/Dev Copy	Multiple point in time copies and instant Test/Dev refresh.
	Accelerate and automate Test/Dev provisioning.
	Migration of SAP ASE from a physical to a virtualized environment.
Recovery	Recovery of a database to its most recent state.
	Recovery of a database to a specific point in time of data backup, or log backup.
	Recovery to the original host or an alternate host.
Backup Catalog View	Actifio Global Manager (AGM)

SAP ASE Configurations Support

SAP ASE Primary and Standby protection can be set from Primary or the Standby. Protection is at the instance level residing on protected LVM. Transaction log protection is from the Primary instance only.

2 Preparing an SAP ASE Instance for Protection

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

Before You Begin

Before you begin, on the SAP ASE server:

- The Actifio backup and recovery process requires a single ASE database user account with these privileges.

For backup operation	Quiesce Any Database (to quiesce databases for LVM backups)
	Dump Any Database (for log backup and dump based backups)
	Manage Server Configuration (to enable dump history if required)
	Manage Dump Configuration (to execute sp_dump_history)
For restore operation	Load Any Database (for log recovery and dump based backup restore)
	Online Any Database (to bring database online after LVM or dump restore)
	Shutdown (in case of LVM based backup restores)
	Unmount Any Database
	Mount Any Database

- The backup username/password must be configured with host configuration. Create the user without a password to run the quiesce command on the source with sa_role or with quiesce privileges.
  To create the user, run:

```
isql -Usa -P<password> -S<SAP ASE_Server_Name>
1>sp_addlogin actuser, '<password>'
2>go
1>grant role sa_role to actuser
2>go
```

To configure the user login without a password requirement, set the password to null, then run:

```
1>sp_configure "minimum password length", 0
2>go
1>sp_modifylogin actuser, "min passwd length", "0"
2>go
3>exit
isql -Uactuser -P'<password>' -S<server_name>
> sp_password '<password>', NULL
>go
>sp_configure "minimum password length", 8
>go
```

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

- Install the Actifio Connector on the SAP ASE server (see ***Network Administrator's Guide to Actifio GO***.)
- To enable transaction log backup, TRUNCATE ON CHKPT FALSE must be set at the database level for each database of the SAP ASE instance.
- For volume level backups:
  - the SAP ASE instance must reside under LVM and it must not be the boot volume.
  - The LVM volume from which the SAP ASE volumes are provisioned should have at least 20% free space.

Adding an SAP ASE Host and Discovering the Instance

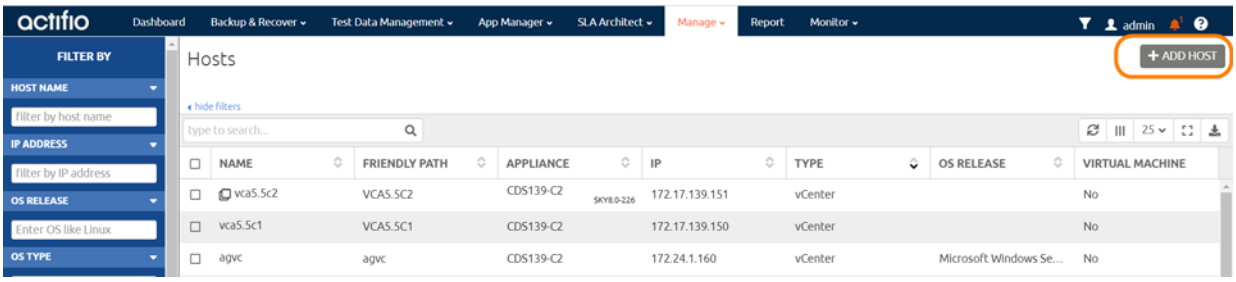
Before you can protect an SAP ASE instance, you must add the host and discover the instance. This requires:

1. Adding the Host to AGM on page 9
2. Discovering the SAP ASE Instance Application from the App Manager on page 11
3. Finding the Discovered SAP ASE Instance in the App Manager on page 11

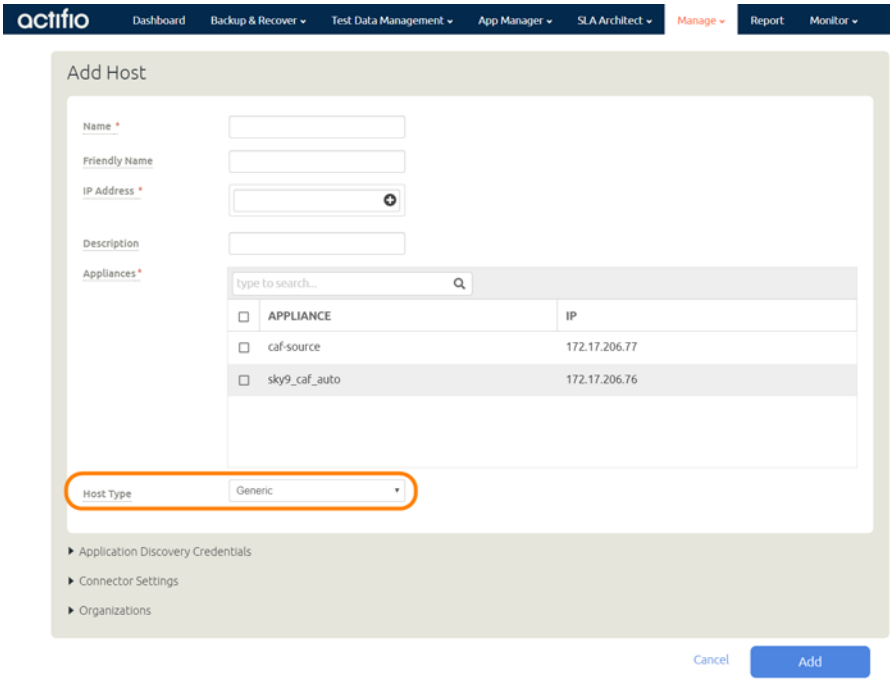
Adding the Host to AGM

Add the host from the Manage, Hosts list. If the host is already added, then edit the host and make sure to set the Staging Disk Format correctly as detailed in Ensuring that the Staging Disk Format is Set Correctly on page 14.

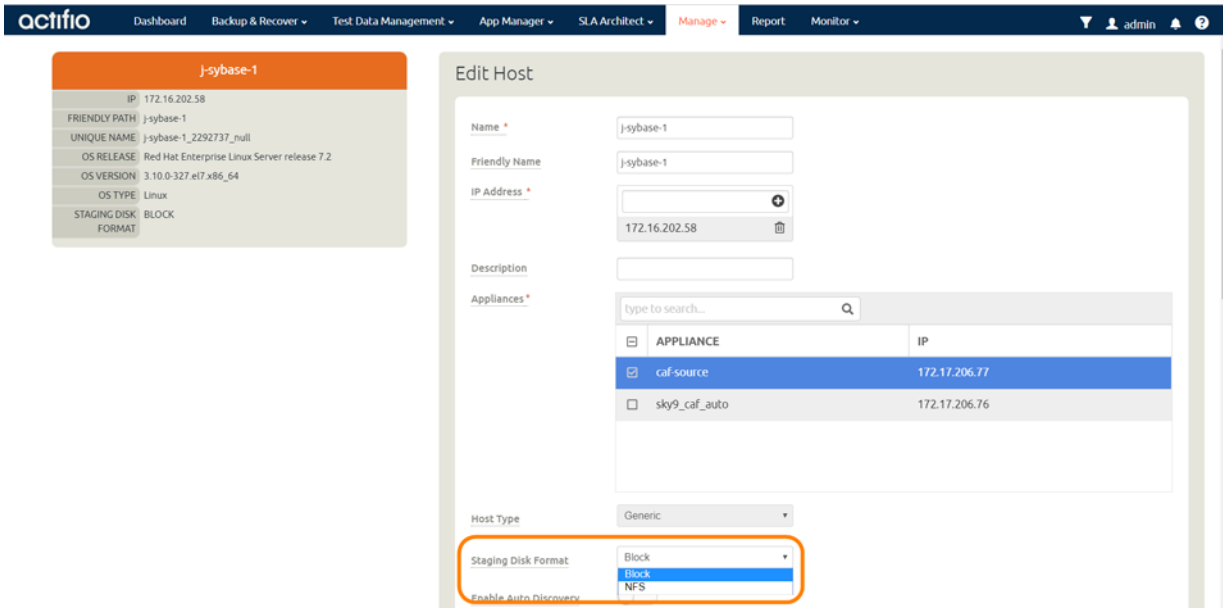
1. From the AGM Manage, Hosts list, click **+Add Host**.



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



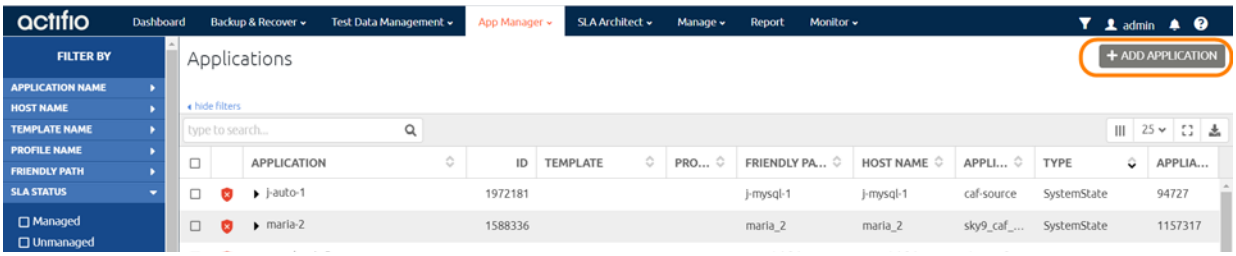
3. Click **Add** at bottom right to add the host. The Host will be added.
4. Right-click the host and select **Edit**.
5. On the Edit Host page, select the staging disk format:
    - **Block** -based staging disks are the most useful for both backup/recovery and TDM usage. Actifio changed-block tracking (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.
6. Select **Save** at the bottom of Edit Host page.



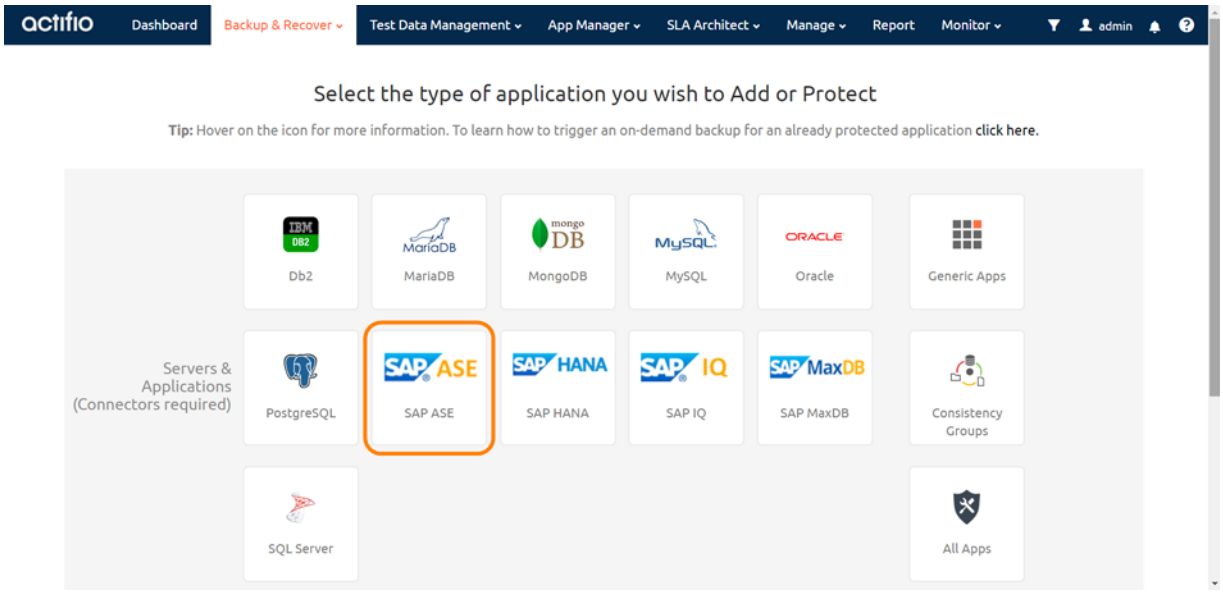
Discovering the SAP ASE Instance Application from the App Manager

To discover the SAP ASE instance:

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



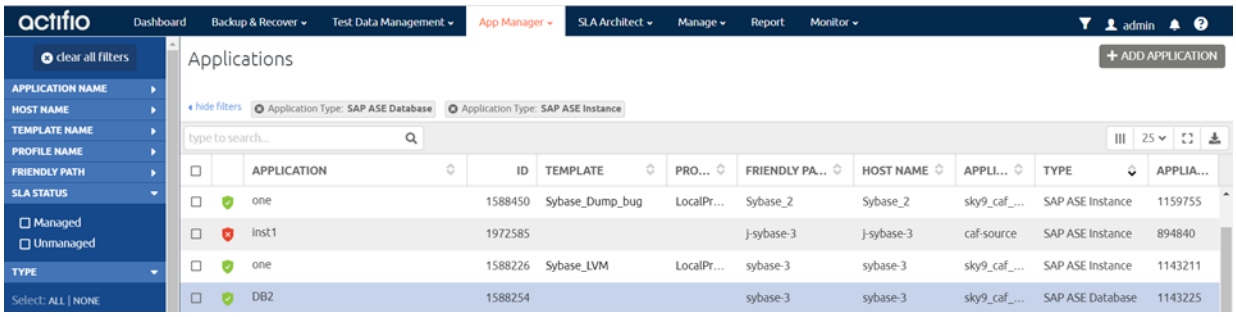
2. The Onboarding Wizard opens. Select **SAP ASE**.



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

Finding the Discovered SAP ASE Instance in the App Manager

To find the newly-discovered instance, go to the App Manager Applications List. All applications known to the AGM of all types are listed. Use the Type application filter on left pane to show only SAP ASE instances and databases.



3 Configuring the SLA, Including the Backup Method

After the instance is prepared and discovered as explained in Chapter 2, Preparing an SAP ASE Instance for Protection, 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 ASE DBA.

The backup method is limited by the staging disk format set in Adding an SAP ASE Host and Discovering the Instance on page 9:

- **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 database copies from the snapshot images. The production instance/database must be present on the LVM volume.
- **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. This method only supports traditional backup a physical recovery.

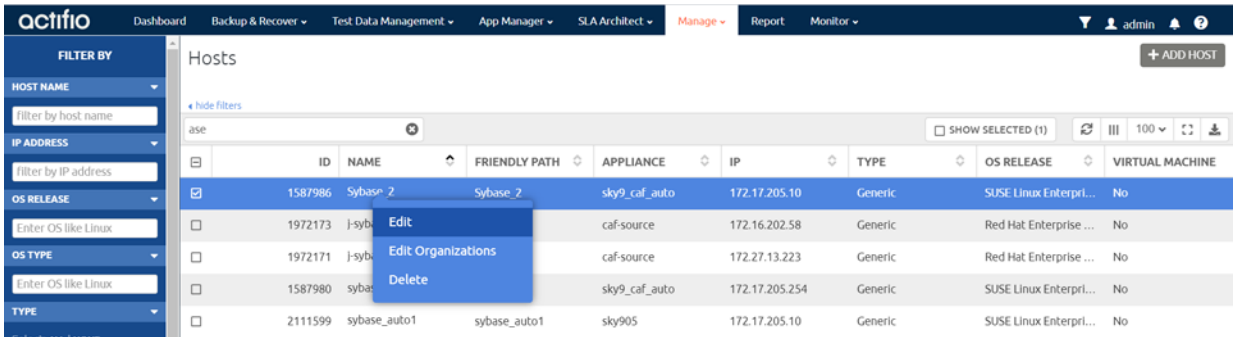
Note: *With one exception, protection is set for the entire SAP ASE Instance. You can include/exclude specific databases during the process using a Database Inclusion Rule from the Manage SLA pages. The exception: A virtual database can be protected individually.*

Whichever method you select involves these steps:

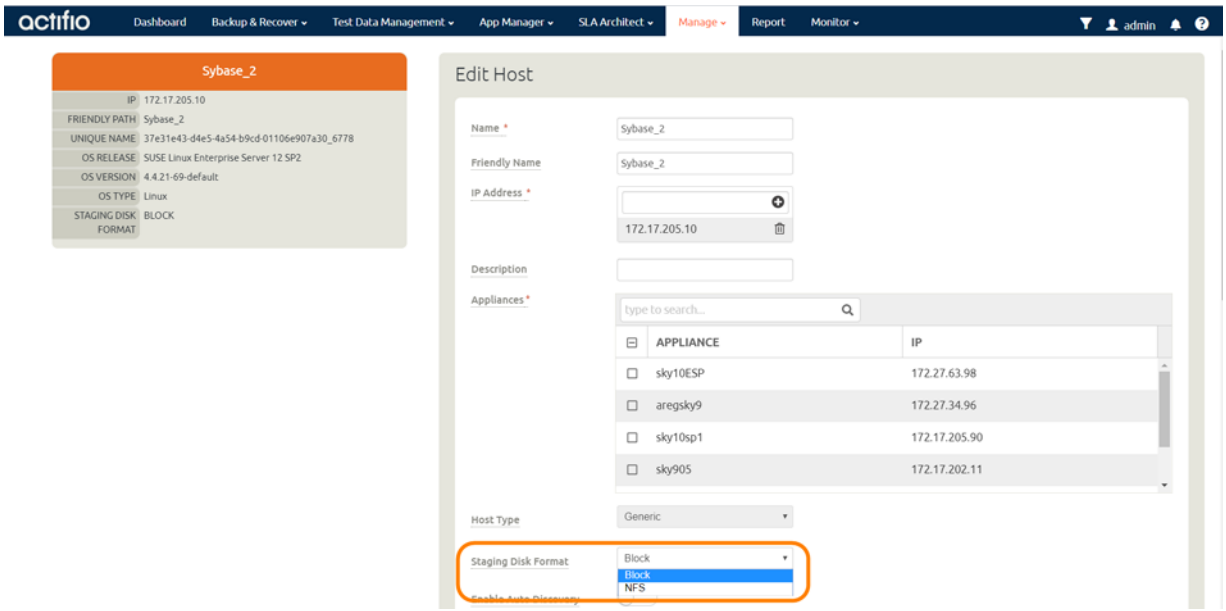
Ensuring that the Staging Disk Format is Set Correctly

To check the staging disk format:

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



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.

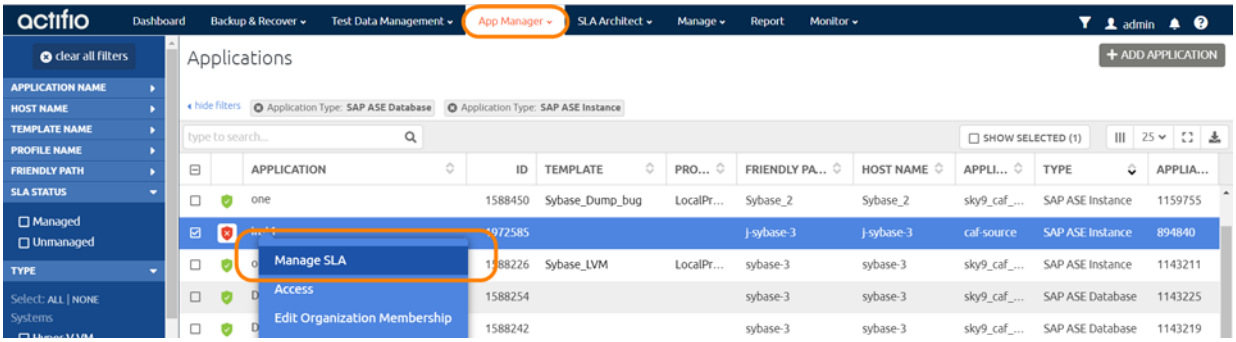


3. If the staging disk format is set incorrectly, change it now and click **Save** before continuing.

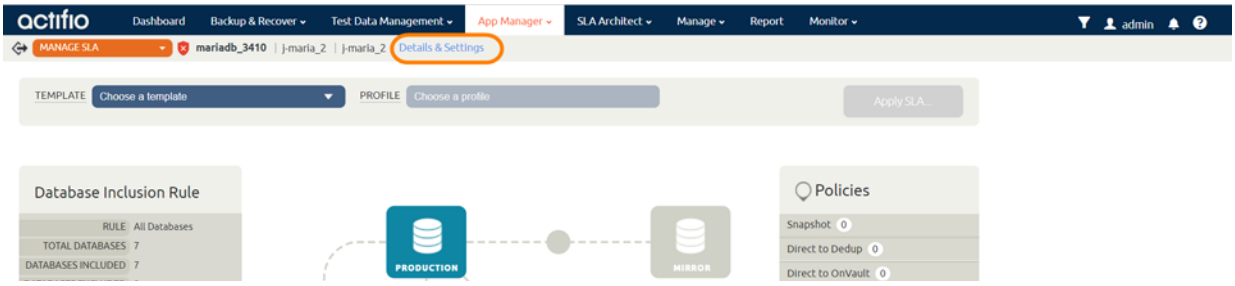
Configuring the Backup Capture Method and Other SLA Settings

To configure the instance SLA settings:

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

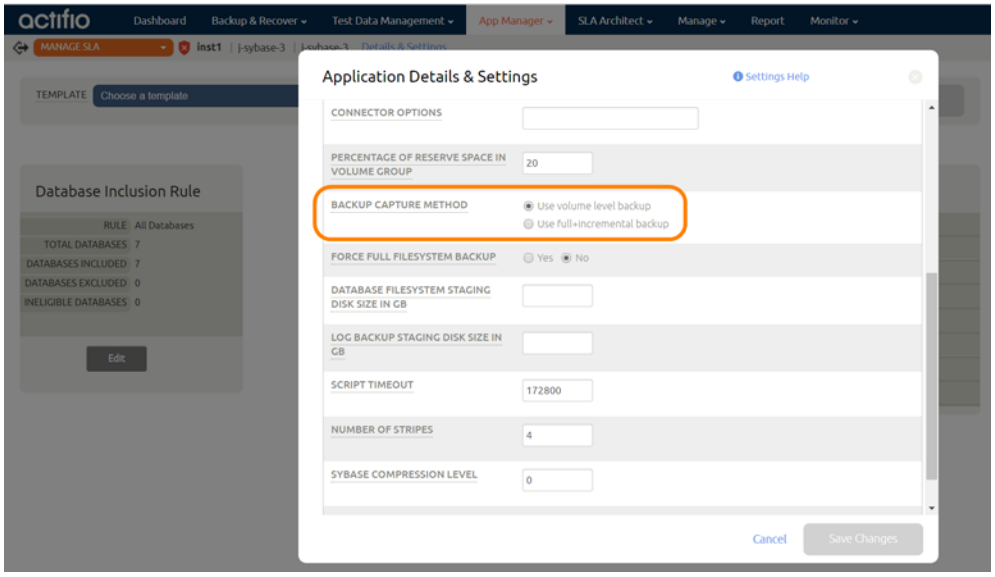


2. At the top of the Manage SLA page, select the **Details & Settings** link:



This opens the details and settings for this 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.



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

Table 1: SAP ASE Application Details & Settings

Setting	Linux CBT and LVM Snapshot (Block only)	File-Based Backup & Recovery
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% recommended for LVM snapshot temporary space. Not applicable for protecting virtual databases.	Not applicable
Backup Capture Method	Use volume level backup	Use full+incremental backup
Force Full Filesystem Backup	Not applicable	Use for an on-demand backup
Database Filesystem Staging Disk Size in GB	Not applicable	Use the calculation: (instance size * 1.5) + 10% Disks will grow dynamically.
Log Backup Staging Disk Size in GB	By default, VDP calculates this as (daily log generation * retention of log backup SLA) + 20% for a buffer. If you provide a value, then it will override the default calculation and the log disk will not grow dynamically. This will become a fixed size. Use the default value unless instructed by Actifio Support.	
Script Timeout	This value is applied to internal backup and recovery scripts called by the Actifio Connector. Use the default value unless instructed by Actifio Support.	
Number of Stripes	Striping is reading or writing a single dump to multiple files. Increase stripes used by the backup server to increase I/O. The default value is 4.	
Compression Level	Not applicable	Select a compression level (0-9, or 100 or 101, any other value is read as 0.)

Note: *Only volume-based snapshots can be mounted as virtual databases. Snapshots taken using the full+incremental backup method are filesystem based; these cannot be mounted as virtual databases.*

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

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

Setting the Schedule for Dumps

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

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

For example, "FIIIIII" results in:

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

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

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

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

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

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

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

Replace "FIIIIII" as needed.

Example

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

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

4 Protecting an SAP ASE Instance and its Logs

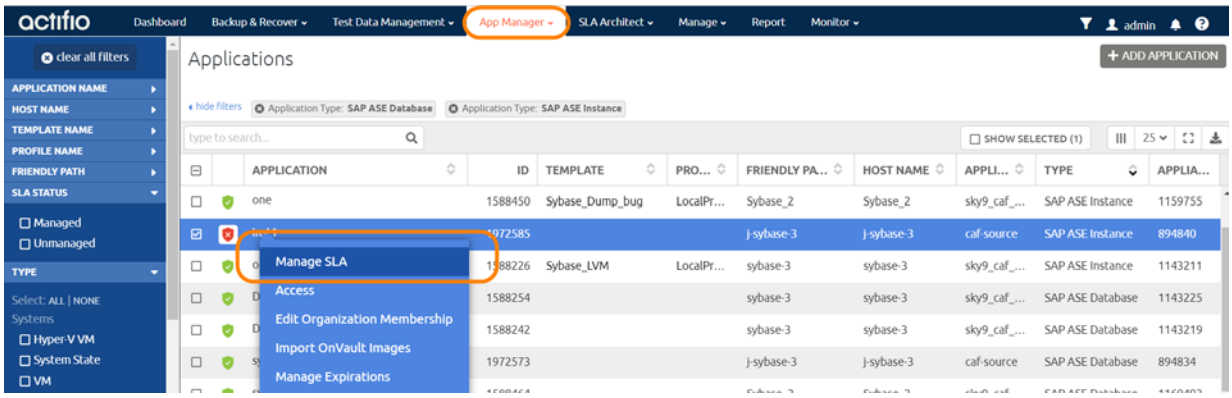
Protecting an SAP ASE instance includes both:

Note: *With one exception, protection is set for the entire SAP ASE 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.*

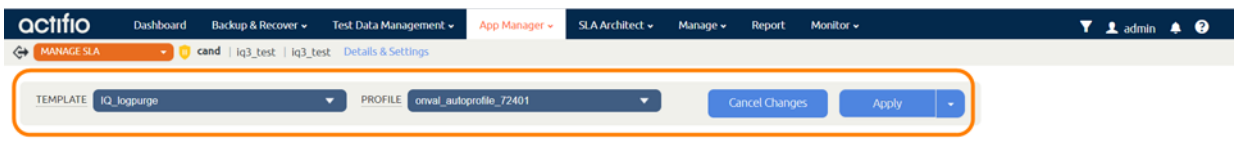
Protecting an SAP ASE Instance

To protect the instance:

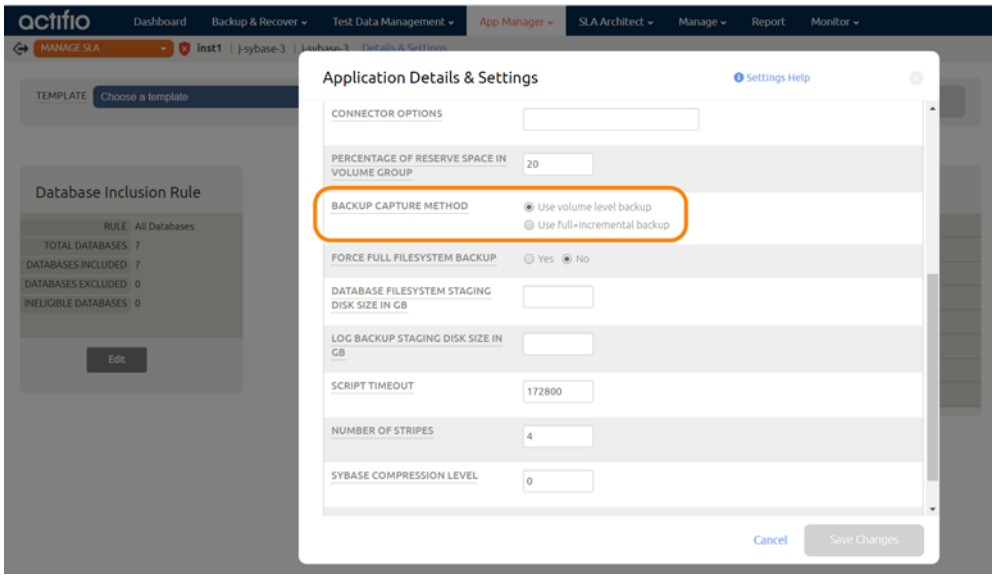
1. From the App Manager, Applications list, right-click the instance and select **Manage SLA**. You can use the Type filter to restrict the list to SAP ASE Instances, and set SLA Status to Unmanaged.



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

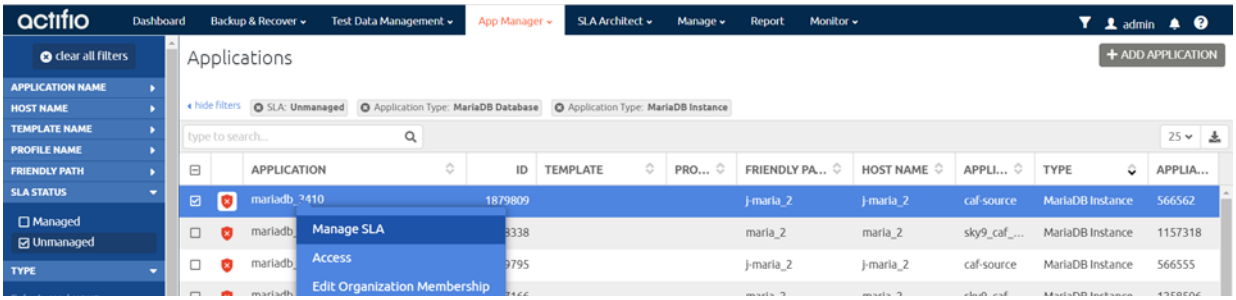


3. On the Apply SLA page, make sure that the backup capture method matches the type of backup set in Chapter 3, Configuring the SLA, Including the Backup Method. Click **Apply SLA** or **Save Changes**. The instance appears in the Application Manager with a green shield icon.

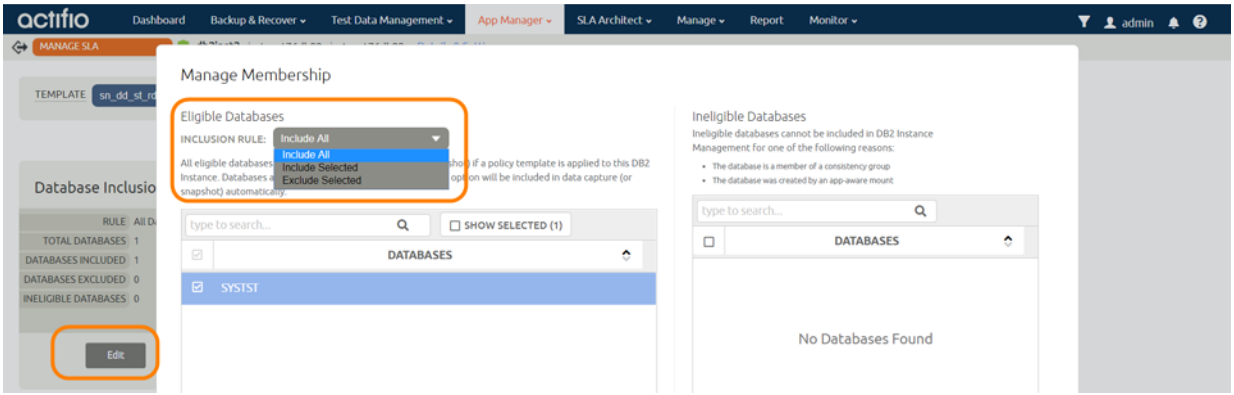


The instance will be protected when the snapshot job runs according to the schedule in the template.

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



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

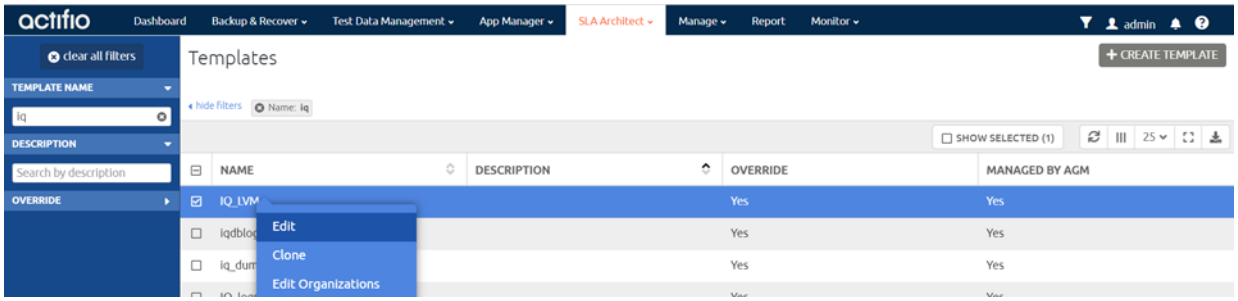


6. Select an Inclusion Rule (Include All, Include Selected, or Exclude Selected). Select the databases to include or exclude, then click **Save**.

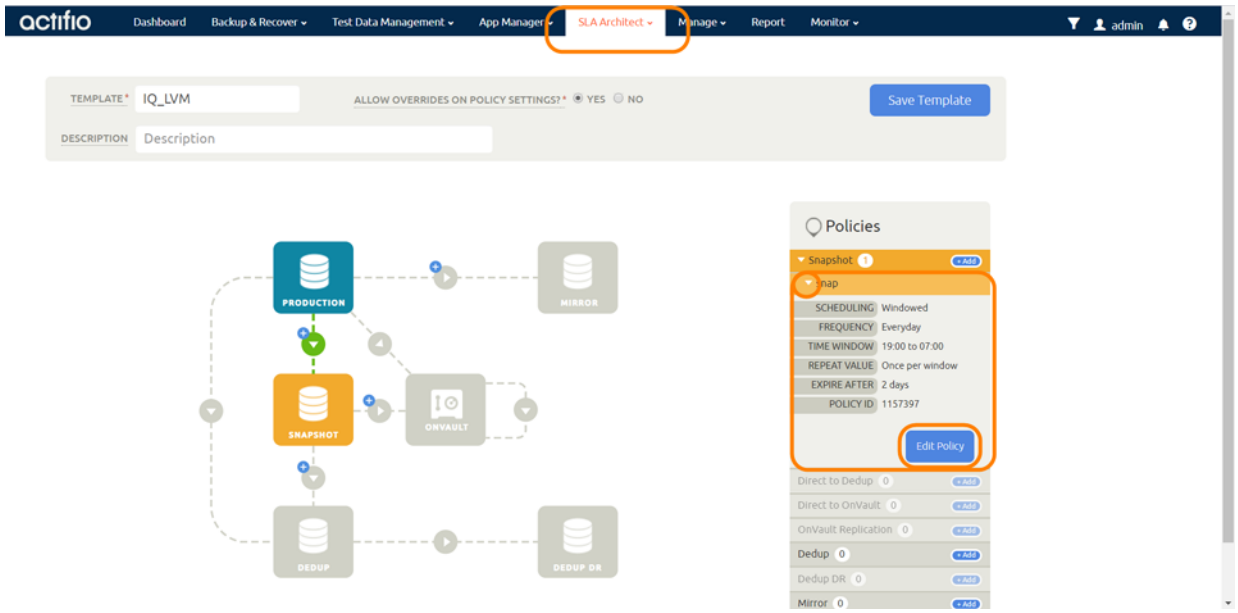
Protecting SAP ASE Database Logs

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

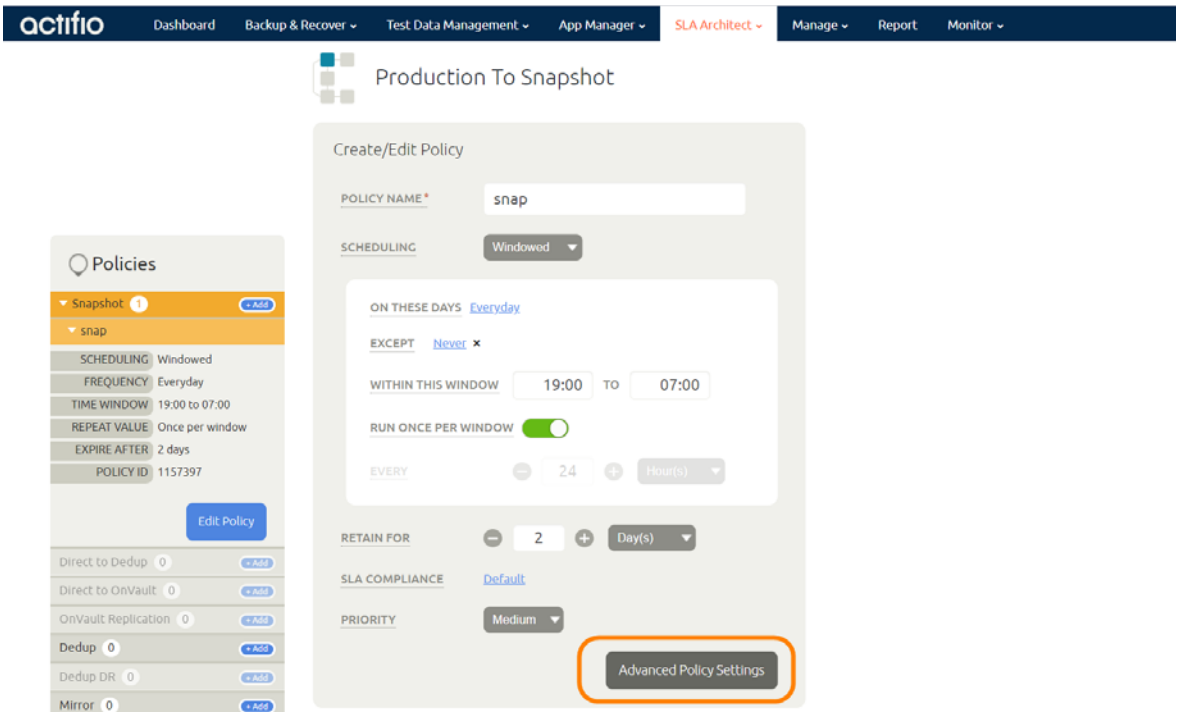
1. From the SLA Architect, Templates list, right-click the template for SAP ASE instance protection. Click **Edit**.



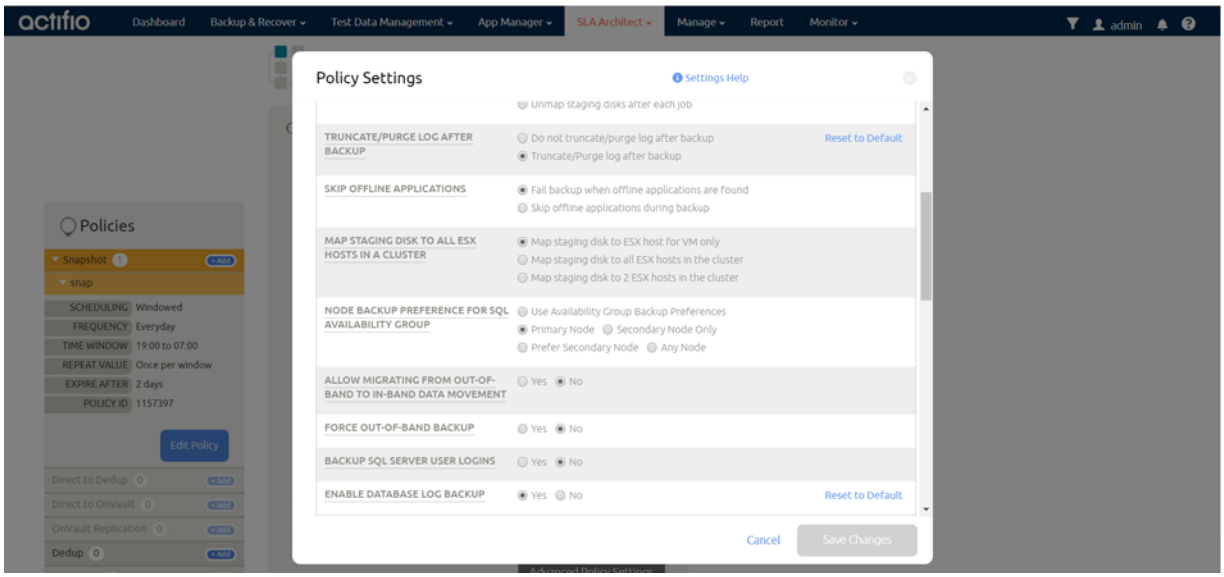
2. Click the arrow beside the Snapshot policy to open up the details, then click **Edit Policy**.



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



4. Set the log policy options (you will have to scroll to see them all):
   - Enable **Truncate/Purge log after backup**.
   - Set **Enable Database Log Backup** to **Yes**.
   - For **RPO (Minutes)**, enter the desired frequency of log backup.
   - Set **Log Backup Retention Period (in Days)** for point in time recovery.
   - Set **Replicate Logs (Uses StreamSnap Technology)** to **Yes** if you want to enable StreamSnap replication of log backup to a DR site.
   - Set **Send Logs to OnVault Pool** to **Yes** if you want the database logs to be sent to an OnVault Pool, enabling for point-in-time recoveries from OnVault on another site.
   - **Log Staging Disk Growth Size (in percent)**: Grow the log staging disk by the specified percentage as needed. The value must be between 5 and 100 percent.
   - **Compress Database Log Backup**: Set this to Yes if you want the SAP ASE host to perform compression during log backup.



5. Click **Save Changes**.

5 Accessing an SAP ASE Instance as a Standard Mount or as a Virtual Database

There are several ways to access a protected SAP ASE instance:

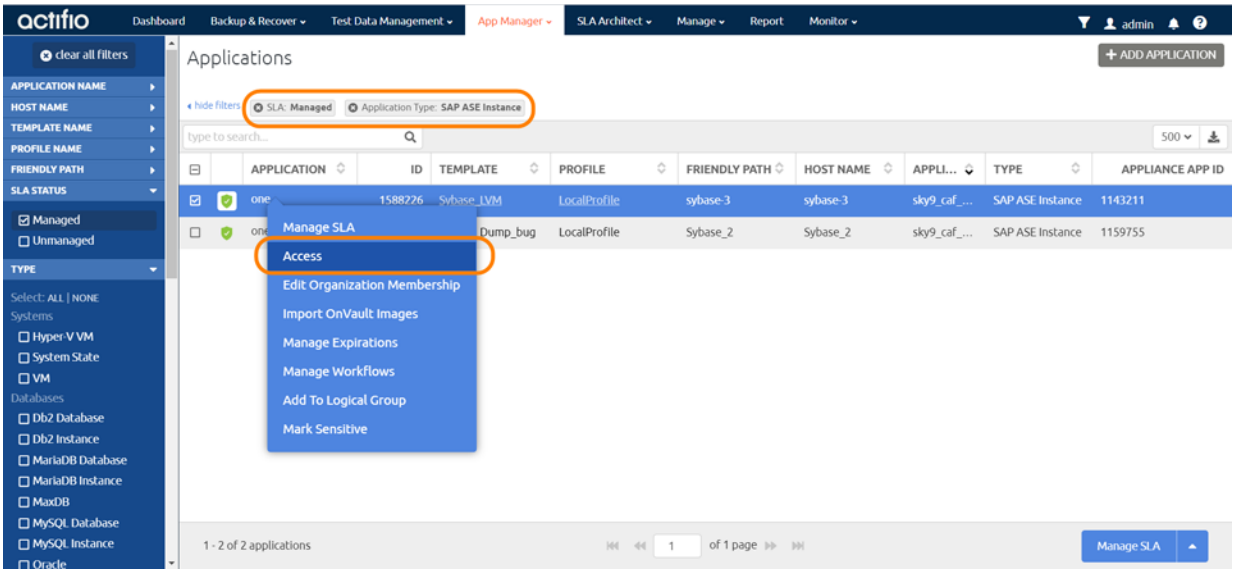
Mounting an SAP ASE Instance as a Standard Mount

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 SAP ASE Instance on page 25.

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.*

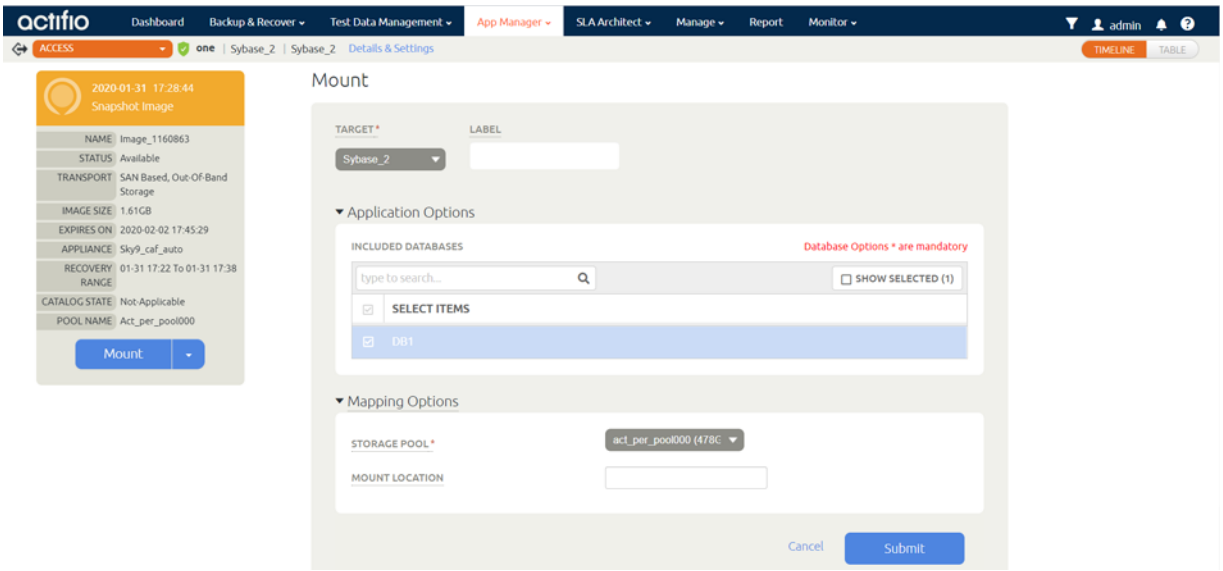


2. Select a snapshot image and choose **Mount**.

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

> ***Note:*** *If you do not see the Create New Virtual Application option, then the image is from a file-based full+incremental snapshot, so a virtual database is not possible.*

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



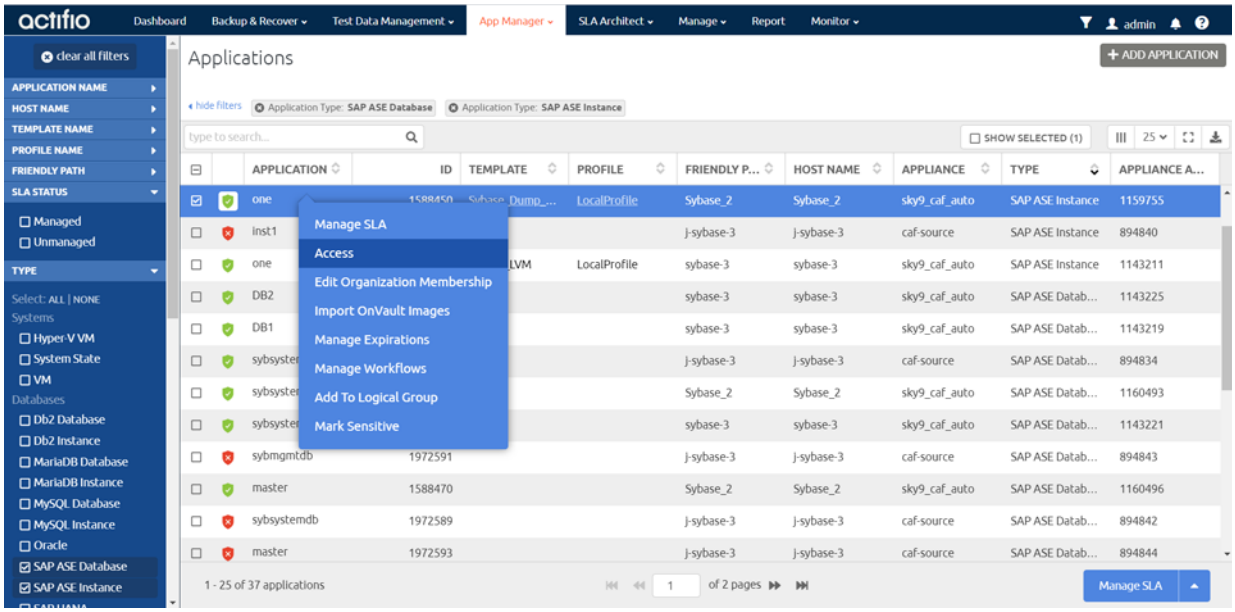
6. Click **Submit**. You can monitor the job progress from the Monitor, Jobs page.

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

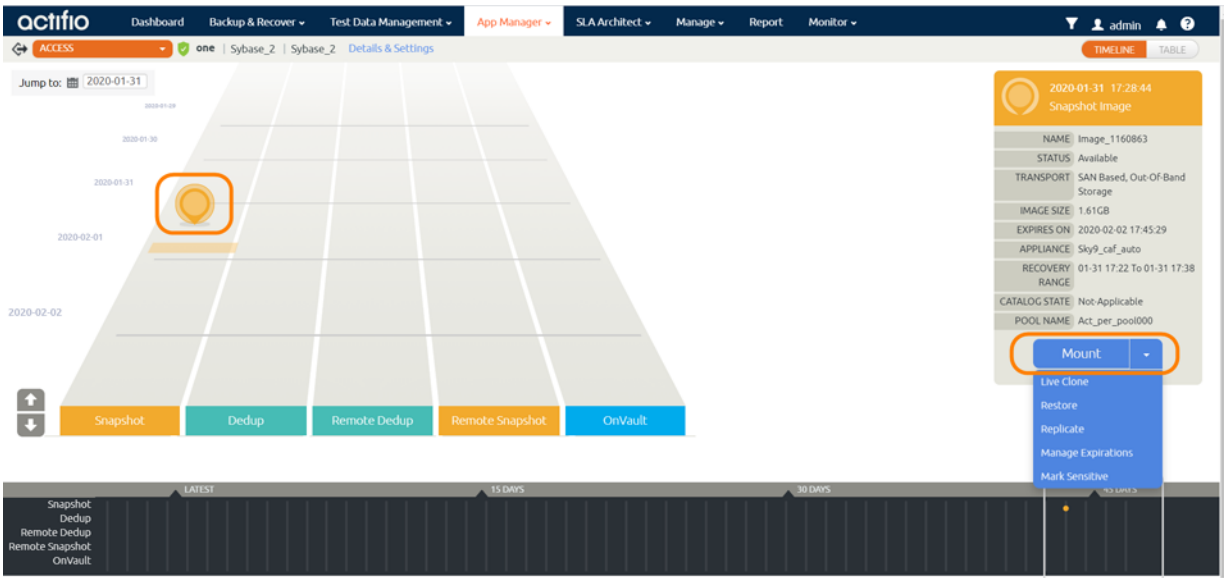
This is the procedure to mount a virtual database (an applicaiton-aware mount). To make a standard mount, see Mounting an SAP ASE Instance as a Standard Mount on page 23. To restore an instance back over a corrupted version at the source, see Chapter 6, Restoring and Recovering an SAP ASE Instance Back to the Source.

To mount a virtual database (application aware mount) to an existing target:

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

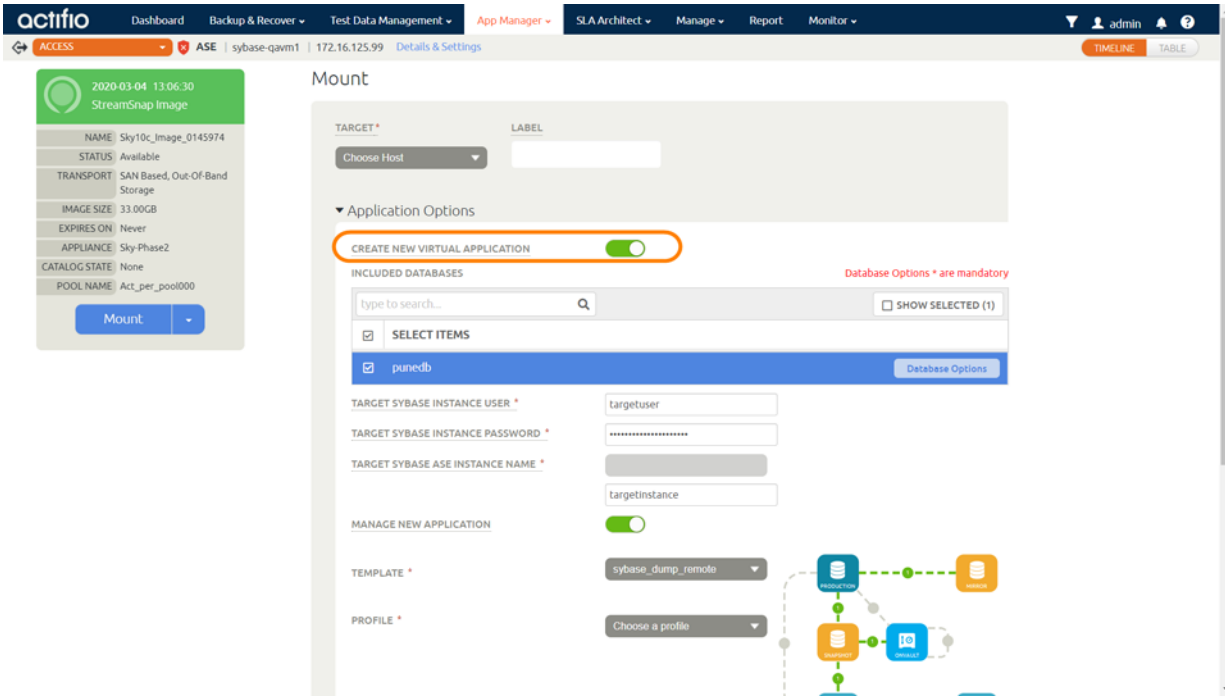


2. Select a snapshot image and choose **Mount**.



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

Note: *Only volume-based snapshots can be mounted as virtual databases. Snapshots taken using full+incremental are filesystem based; these cannot be mounted as virtual databases.*



5. At Included Databases, Select Items, choose one or more databases to virtualize:
   - A single database will be managed as standalone virtual copy
   - Multiple databases will be managed as a consistency group
6. Click each selected database to specify the target database details for the new virtual copy.
7. For a database protected with log roll-forward, choose a target point in time.

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

   TARGET SAP ASE INSTANCE NAME: From the drop down, select a target SAP ASE instance to attach the selected database as a virtual copy.

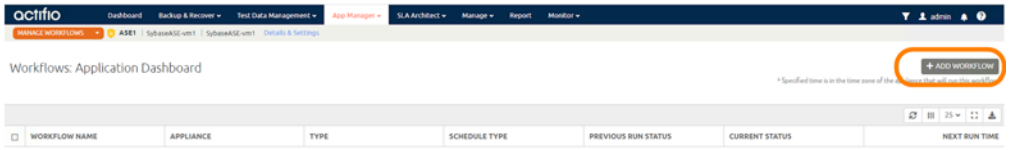
   Manage New Application:
   - To protect the new virtual database, click and enable Manage New Application.
   - Choose a template and a resource profile to protect the database.
8. In Advanced Options:
   - Enter the **Home Directory** of the database (optional).
   - **Overwrite Existing Database**, 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.
9. The Mapping Options depend upon the target. Both physical hosts and VMs require a Mount Location; specify a target mount point to mount the new virtual database to. VM targets also have VM-specific requirements that are detailed in the AGM online help.
10. Click **Submit**.
11. Perform Unmount+Delete for the database mount-point.


actifio
Dashboard
Backup & Recover
Test Data Management
App Manager
SLA Architect
Manage
Report
Monitor
admin
ACCESS
one
Sybase_2
Sybase_2
Details & Settings
TIMELINE
TABLE
Jump to:
2020-01-31
2020-01-30
2020-01-31
2020-02-01
2020-02-02
Snapshot
Dedup
Remote Dedup
Remote Snapshot
OnVault
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
Mount
Current Active Mounts (1)
Hide
NAME
Image_1648398
MOUNTED HOST
Sybase_2
Unmount
Unmount & Delete
Actions
LATEST
15 DAYS
30 DAYS
45 DAYS

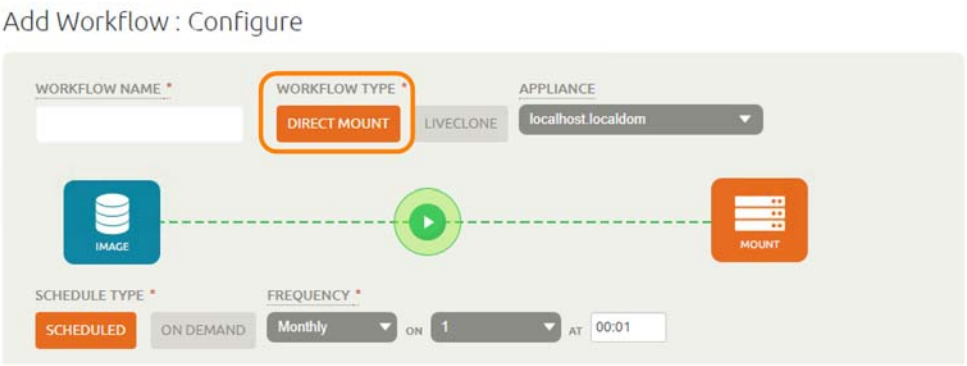
Refreshing a Virtual Database Using an Actifio Workflow

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

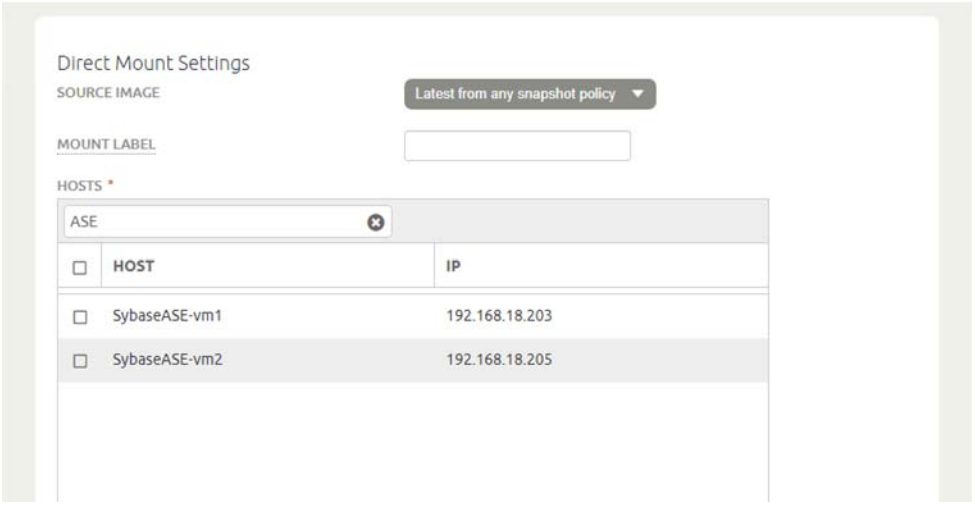
1. From the AGM App Manager, right-click the SAP ASE Instance and select **Manage Workflows**.
2. In the upper right corner of the Workflows: Application Dashboard page, click **+ Add Workflow**.



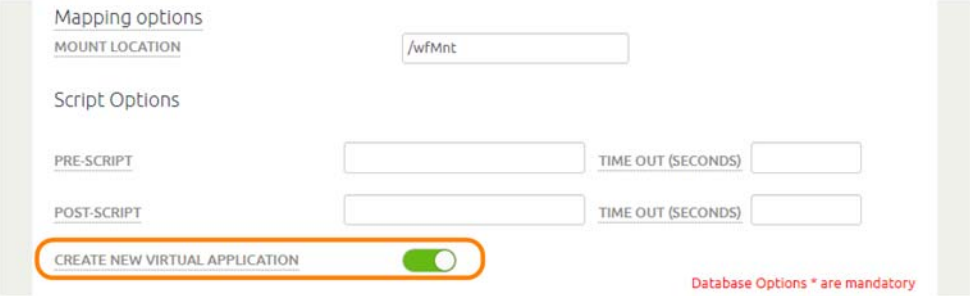
3. Specify:
   - Workflow Name: Enter a name for this workflow.
   - Workflow Type: Select **Direct Mount**.
   - Schedule Type: Choose Scheduled or On Demand based on your requirement. For a scheduled workflow, specify the frequency as well.



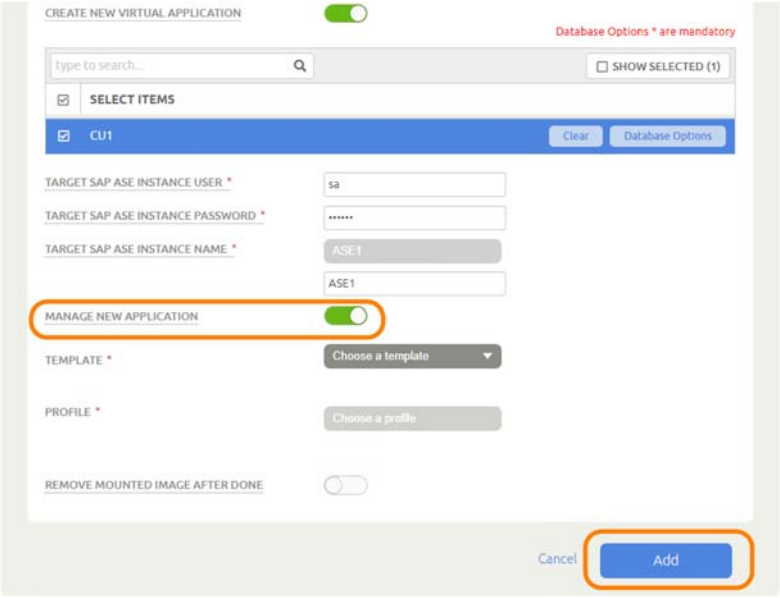
   - Source Image: Select based on requirements.
   - Mount Label: (Optional) Specify a mount label for the mounted image.
   - Hosts: Select the target host or hosts where the virtual SAP ASE Instance databases copy will be created.



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



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



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

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

6 Restoring and Recovering an SAP ASE Instance Back to the Source

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

Note: *This chapter details how to restore an instance back over a corrupted version at the source. To access an SAP instance or database as a new virtual database that can be refreshed, see* Chapter 5, Accessing an SAP ASE Instance as a Standard Mount or as a Virtual Database.

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 SAP ASE Database from a Volume-Based Snapshot *on page 33.*

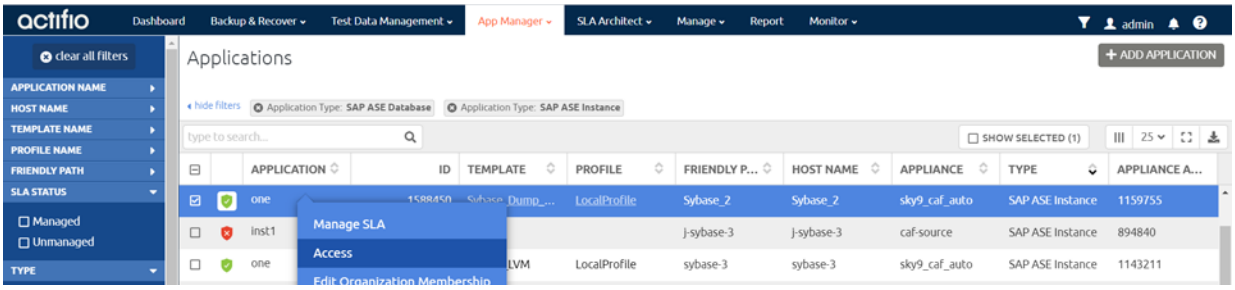
Recovering an SAP ASE Instance from a Volume-Based Snapshot

Use this procedure to restore and recover the source SAP ASE instance. This procedure uses physical recovery of the source data area. This procedure requires that the image was captured using volume-level backup for Backup Capture Method in the application Details & Settings.

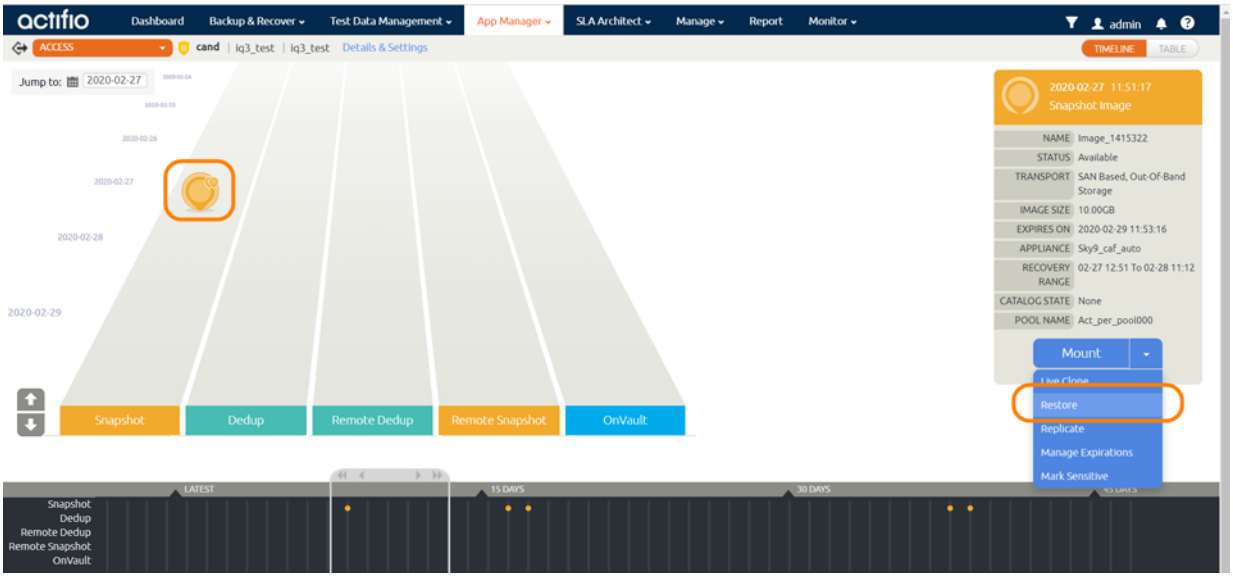
Note: *System databases on a root partition backed up as LVM snapshots can be mounted as virtual databases, but they cannot be used in a traditional Restore operation as the root partition cannot be unmounted. This will need manual restore and recovery from a simple mount back to the same host.*

To recover back to the source:

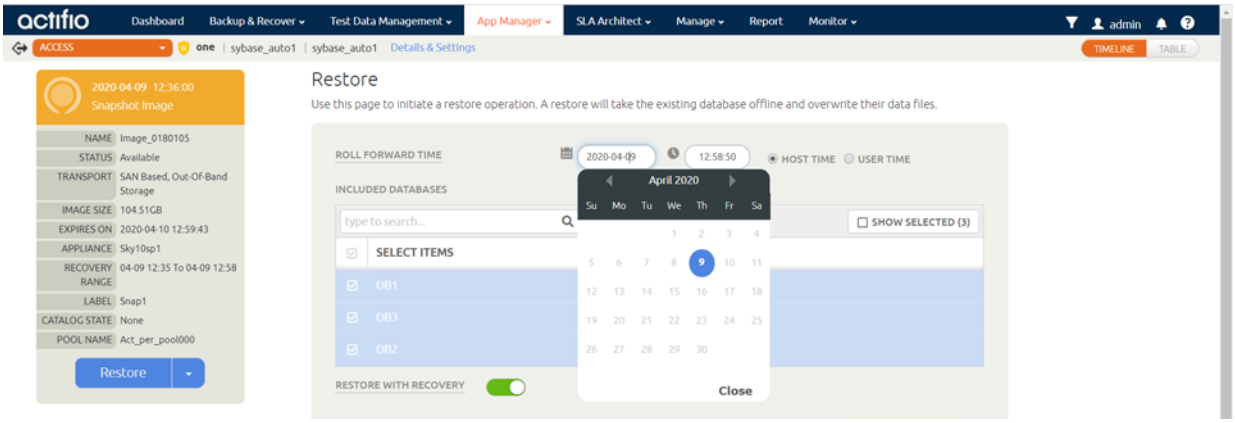
1. From the App Manager, Applications list, right-click the protected instance and select **Access**. You can use the Managed SLA Status filter to show only protected instances.



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



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



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

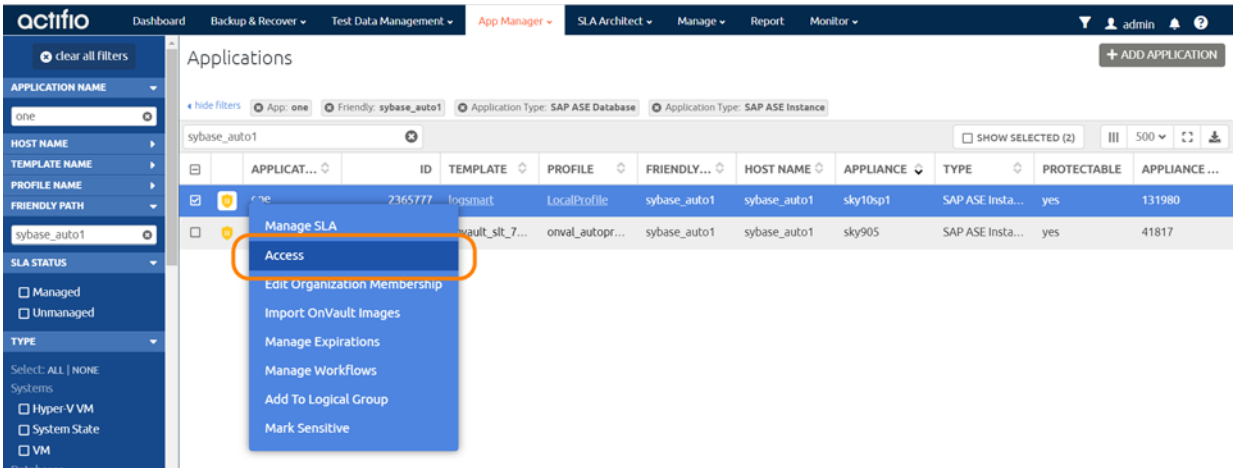
Recovering a Single SAP ASE Database from a Volume-Based Snapshot

Use this procedure to restore and recover a single database from the source SAP ASE instance. This procedure uses physical recovery of the source data area. This procedure requires that the image was captured using volume-level backup for Backup Capture Method in the application Details & Settings.

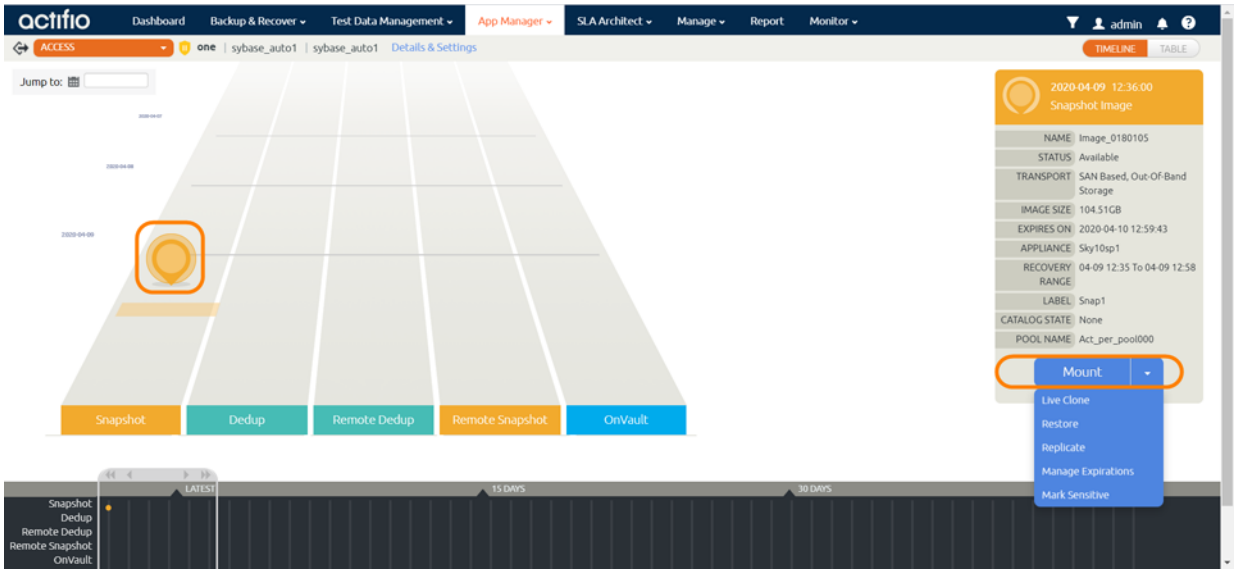
Note: *System databases on a root partition backed up as LVM snapshots can be mounted as virtual databases, but they cannot be used in a traditional Restore operation as the root partition cannot be unmounted. This will need manual restore and recovery from a simple mount back to the same host.*

To recover a single database from an LVM image of an instance:

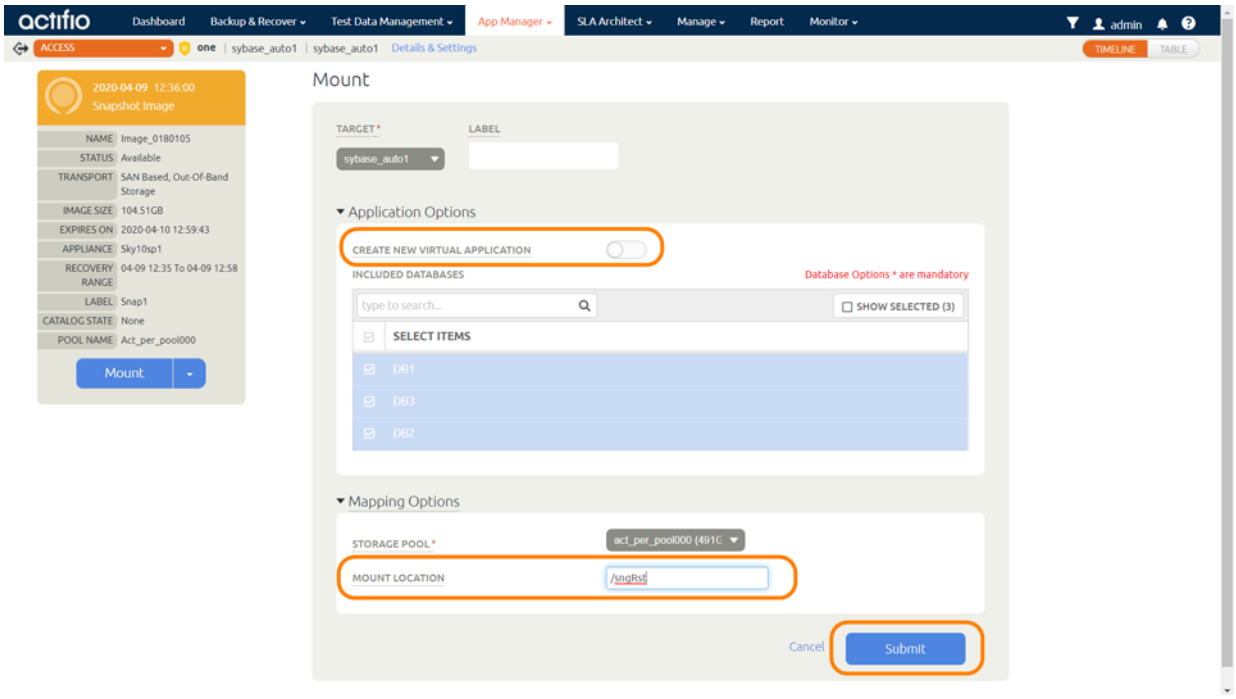
1. From App Manager, Applications list, right-click the instance that has the database to be recovered and select **Access**.



2. On the timeline, select the latest snapshot to recover, and choose **Mount**.



3. In the Application Options, **disable** Create New Virtual Application. In Mapping Options, provide the mount-point location. Click **Submit**.



4. Check the Monitor, Jobs page to see when the mount job is finished. When the job is finished, return to the SAP ASE host, and change the directory to /act/custom_apps/sybase/restore. Run the script act_sybase_lvm_customdb_recovery.sh with the arguments below.

```
./act_sybase_lvm_customdb_recovery.sh OSUSER=sybase TARGET_SYBASE_SQLD=/home/sybase/
Sybase16Home/OCS-16_0 TARGET_MNT_PNT=/sngRst TARGET_SERVER_NAME=ASE1 TARGET_DB_USER=sa
STRIPEON=4 TARGET_DBUSER_PASSWD=sybase SRC_DBNAME=CU1 LOG_BKP_MNTPT=/sngRst_archivelog
UNTIL_TIME="2019-11-07 20:31:27" BEGIN_TIME="2019-11-07 19:31:27" JOBID="Job_2677627"
```

Arguments to the Script

OSUSER = SAP Ase OS owner name
TARGET_SYBASE_SQLD = SAP ASE iSQL path on the target recovery host
TARGET_MNT_PNT = SAP ASE Instance image mountpoint name
TARGET_SERVER_NAME = SAP ASE data server name on the target recovery host
TARGET_DB_USER = SAP ASE Instance username on the target recovery host
TARGET_DBUSER_PASSWD = SAP ASE Instance user password on the target recovery host
SRC_DBNAME = SAP ASE Database name to be recovered (Single)
LOG_BKP_MNTPT = SAP ASE Log image mountpoint name
BEGIN_TIME= Backup begin time (Format: "YYYY-MM-DD HH24:MI:SS")
UNTIL_TIME = Point in time to recover the database (Format: "YYYY-MM-DD HH24:MI:SS")
JOBID = Database mount Job name

5. Connect to the SAP ASE database and verify the data.

6. In the AGM, access the image again and Unmount+Delete the database mount-point.

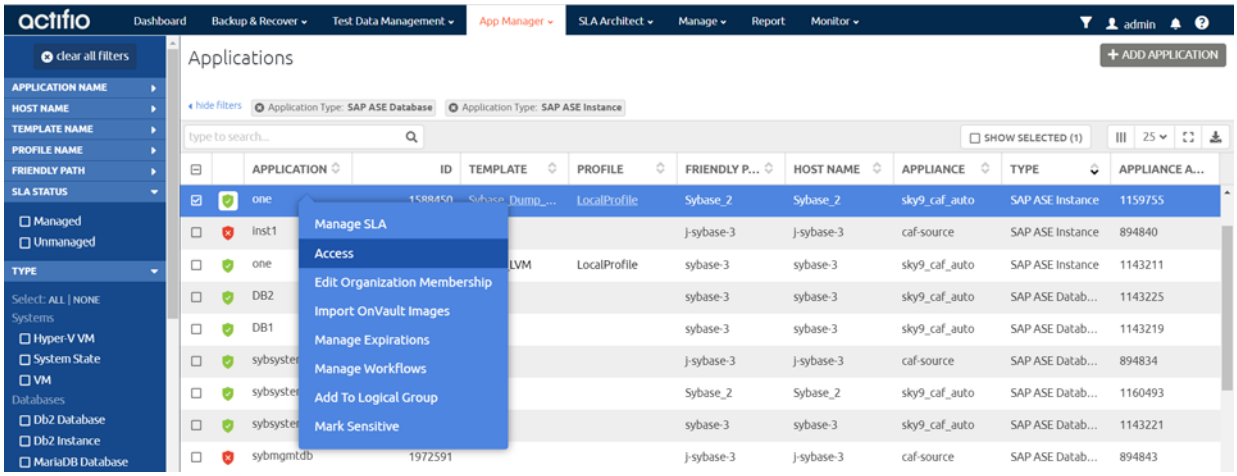

actifio
Dashboard
Backup & Recover
Test Data Management
App Manager
SLA Architect
Manage
Report
Monitor
admin
ACCESS
one
Sybase_2
Sybase_2
Details & Settings
TIMELINE
TABLE
Jump to:
2020-01-31
2020-01-30
2020-01-31
2020-02-01
2020-02-02
Snapshot
Dedup
Remote Dedup
Remote Snapshot
OnVault
2020-01-31 17:28:44
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
Mount
Current Active Mounts (1)
Hide
NAME
Image_1648398
MOUNTED HOST
Sybase_2
Unmount
Unmount & Delete
Actions
LATEST
15 DAYS
30 DAYS
45 DAYS

Recovering from a Full+Incremental Snapshot

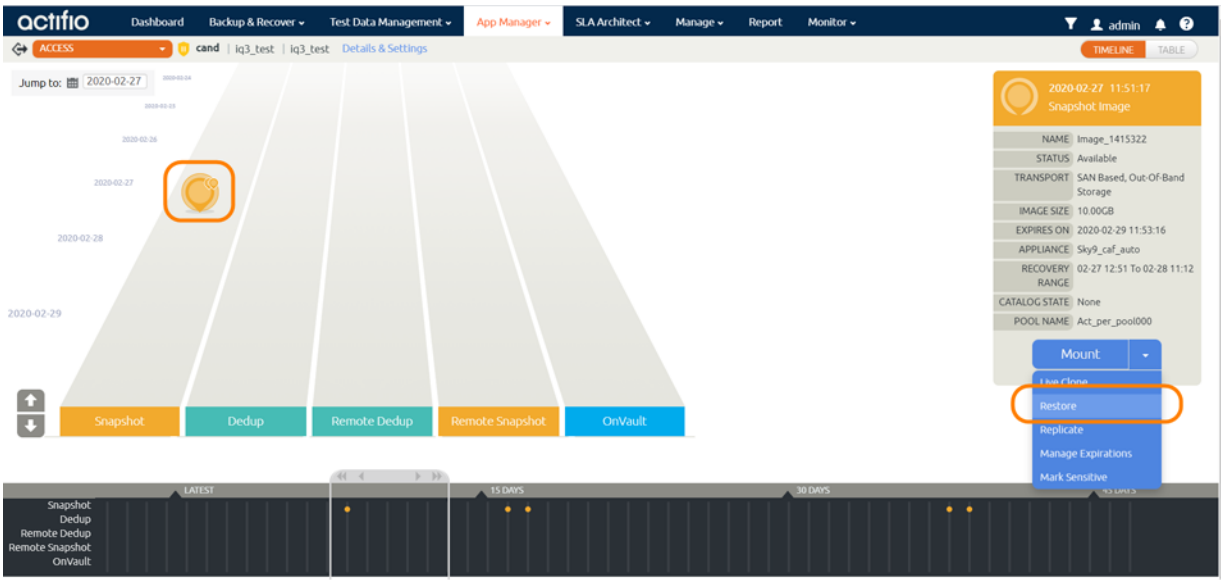
Use this procedure to restore and recover the source SAP ASE instance. This procedure overwrites the source data. This procedure requires that the image was captured using full+incremental backup for Backup Capture Method in the application Details & Settings.

To recover back to the source, overwriting it:

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



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



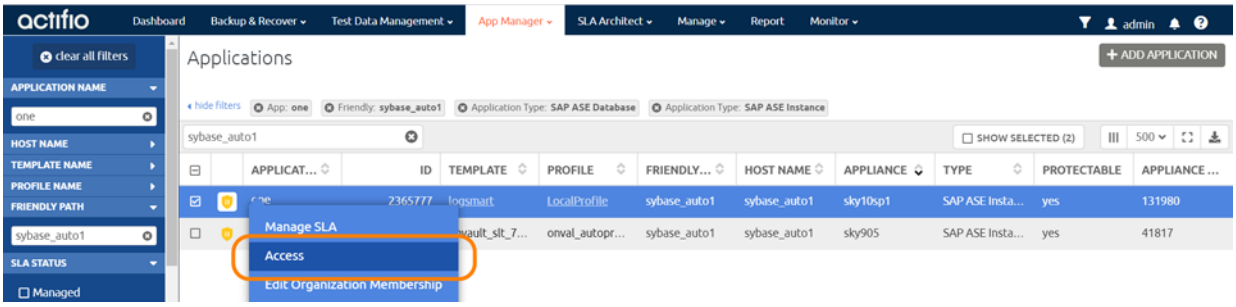
3. For an instance protected with logs, on the Restore page, choose a date and a point in time.
4. Use Select Items to choose one or more instances to restore.
5. Click **Submit**. This will start the source instance physical recovery using SAP ASE recover commands.

Recovering to a New Target from a Full+Incremental Snapshot

Use this procedure to restore and recover the source SAP ASE instance to a new, existing target server. This procedure requires that the image was captured using full+incremental backup for Backup Capture Method in the application Details & Settings.

To restore:

1. From App Manager, Applications list, right-click the instance that has the database to be recovered and select **Access**.



2. On the timeline, select the latest snapshot to recover, and choose **Mount**.

3. Provide a mount point under mount location. For example: /dmpRstNew
4. DB backup will be mounted under /dmpRstNew and log backup will be mounted under /dmpRstNew_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 "/dmpRstNew" |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 /dmpRstNew 2>&1
```

6. BEGIN_TIME of the snapshot image can be found from /var/act/log/UDSAgent.log. Run:

```
grep <JobID> /var/act/log/UDSAgent.log | grep BEGIN_TIME |head -1
```

For example:

```
# grep Job_0404207 /var/act/log/UDSAgent.log | grep BEGIN_TIME |head -1
```

```
2019-12-06 18:10:59.868 GEN-INFO  [6752] Job_0654683
UnixCustomApplication::setAppSpecificProperty - Setting app specific property BEGIN_TIME ==>
2019-12-06 16:55:39
```

7. LOG_BKP_MNTPT will be equals to <mountPoint provided in Step2>_archivelog. Refer Step3.
8. Login to the SAP ASE server as root. On the server, change the directory to /act/custom_apps/sybase/dump

```
#cd /act/custom_apps/sybase/dump
```

9. Run the script from the command line (as root) ACT_SYBASE_dumprestore_newTarget.sh on target with arguments

```
#/act/custom_apps/sybase/dump/ACT_SYBASE_dumprestore_newTarget.sh SYBOSUSER=sybase
SRC_SYBASE_SQLD=/home/sybase/Sybase16Home/OCS-16_0 TARGET_DB_USER=sa
TARGET_DBUSER_PASSWD=sybase ACT_NAME=ASE1 TARGET_MNT_PNT=/dmpRstNew SRC_DBNAME=CU1
UNTIL_TIME="2019-10-22 22:13:40" BEGIN_TIME="2019-10-22 19:07:00" LOG_BKP_MNTPT=/
dmpRstNew_archivelog SRC_PAGE_SIZE=2048
```

Arguments to the script

SYBOSUSER = <Target ASE OS user>

SRC_SYBASE_SQLD = <Target ASE OCS location ($SYBASE/$SYBASE_OCS)>

TARGET_DB_USER = <Target ASE instance username>

TARGET_DBUSER_PASSWD = <Target ASE instance password>

ACT_NAME = <Target ASE server name>

TARGET_MNT_PNT = <Mount point specified during mount>

SRC_DBNAME = <Comma separated db list to restore>

BEGIN_TIME = <Dump backup begin time (Format: YYYY-MM-DD HH24:MI:SS)>

UNTIL_TIME = <Recovery time (Format: YYYY-MM-DD HH24:MI:SS)>

LOG_BKP_MNTPT = <Logbackup mount point name>

SRC_PAGE_SIZE = <Source database page_size>

10. Connect to the SAP ASE instance and confirm that the databases are recovered and online.

```
#isql -U<username> -P<password> -S<ASE server name>
sp_helpdb
go
```

11. Unmount the mounted dump snapshot image.

7 Migrating an SAP ASE 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 an SAP ASE database, you can mount it and migrate it:

Mount and Migrate Back to the Source Instance on page 39
Mount and Migrate to a New Instance on page 41

Note: *Before running the migration, run the query* `sp_helpdevice` *and find device_names that are stale entries or have their physical_name pointing to the migrating mount points, and drop them using command* `sp_dropdevice device_name`.

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. Unmount the source databases, if you want to replace them with databases with the same name.

```
unmount database <DBNAME> to '<ManifestFile>'
```

Example

```
1> unmount database CU1 to '/tmp/CU1.mf'
2> go
```

2. Login to AGM, select the application and mount a virtual database to the source as detailed in Mount a Virtual Database from a Block-Based Volume Snapshot Image to the Source or to an Existing SAP ASE Instance on page 25.

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

3. From the App Manager, Applications list, right-click the new protected instance and select **Access**. You can use the Managed SLA Status filter to show only protected instances.
4. Once the mount job is completed, run this script with parameters in Arguments to the Script.

```
/act/custom_apps/sybase/lvm_migrate/ACT_SYBASE_lvm_migrate_newTarget.sh
DATAVOL_DISK_MAPPING=<DATAVOL_DISK_MAPPING> TARGET_SERVER_NAME=<TARGET_SERVER_NAME>
TARGET_DB_USER=<TARGET_DB_USER> TARGET_DBUSER_PASSWD=<TARGET_DBUSER_PASSWD>
TARGET_DBNAME_LIST=<TARGET_DBNAME_LIST> JOBID=<JOBID>
```

Arguments to the Script

DATAVOL_DISK_MAPPING = Comma separated list of <Actifio_mount_point>:<equivalent target host lvm device name>

TARGET_SERVER_NAME = Target ASE server name

TARGET_DB_USER = Target instance db username

TARGET_DBUSER_PASSWD = Target instance password

TARGET_DBNAME_LIST = Comma separated list of <source_db_name>:<Target_db_name> / /Can be found in /var/act/log/customapp-sybaseinstance.log

JOBID = Actifio mount job id

Note: *Target lvm devices should be empty.*

Example

```
/act/custom_apps/sybase/lvm_migrate/ACT_SYBASE_lvm_migrate_newTarget.sh DATAVOL_DISK_MAPPING=/
mntNT/log/CU1:/dev/mapper/vg2-lv2,/mntNT/data/CU1:/dev/mapper/vg2-lv1 TARGET_SERVER_NAME=ASE1
TARGET_DB_USER=sa TARGET_DBUSER_PASSWD=sybase TARGET_DBNAME_LIST=CU1:SU2 JOBID=Job_12345
```

5. Once the above script has completed successfully, go to AGM and perform Unmount+Delete.

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. Login to AGM, select the application and perform the AppAware mount as detailed in Mount a Virtual Database from a Block-Based Volume Snapshot Image to the Source or to an Existing SAP ASE Instance on page 25.

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

---

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

```
/act/custom_apps/sybase/lvm_migrate/ACT_SYBASE_lvm_migrate_newTarget.sh
DATAVOL_DISK_MAPPING=<DATAVOL_DISK_MAPPING> TARGET_SERVER_NAME=<TARGET_SERVER_NAME>
TARGET_DB_USER=<TARGET_DB_USER> TARGET_DBUSER_PASSWD=<TARGET_DBUSER_PASSWD>
TARGET_DBNAME_LIST=<TARGET_DBNAME_LIST> JOBID=<JOBID>
```

Arguments to the Script

DATAVOL_DISK_MAPPING = Comma separated list of<Actifio_mount_point>:<equivalent target host lvm device name>

TARGET_SERVER_NAME = Target ASE server name

TARGET_DB_USER = Target instance db username

TARGET_DBUSER_PASSWD = Target instance password

TARGET_DBNAME_LIST = Comma separated list of <source_db_name>:<Target_db_name> //Can be found in /var/act/log/customapp-sybaseinstance.log

JOBID = Actifio mount job id

Note: *Target lvm devices should be empty.*

Example

```
/act/custom_apps/sybase/lvm_migrate/ACT_SYBASE_lvm_migrate_newTarget.sh DATAVOL_DISK_MAPPING=/
mntNT/log/CU1:/dev/mapper/vg2-lv2,/mntNT/data/CU1:/dev/mapper/vg2-lv1 TARGET_SERVER_NAME=ASE1
TARGET_DB_USER=sa TARGET_DBUSER_PASSWD=sybase TARGET_DBNAME_LIST=CU1:SU2 JOBID=Job_12345
```

3. Once the above script completed successfully, go to AGM, perform Unmount+Delete.