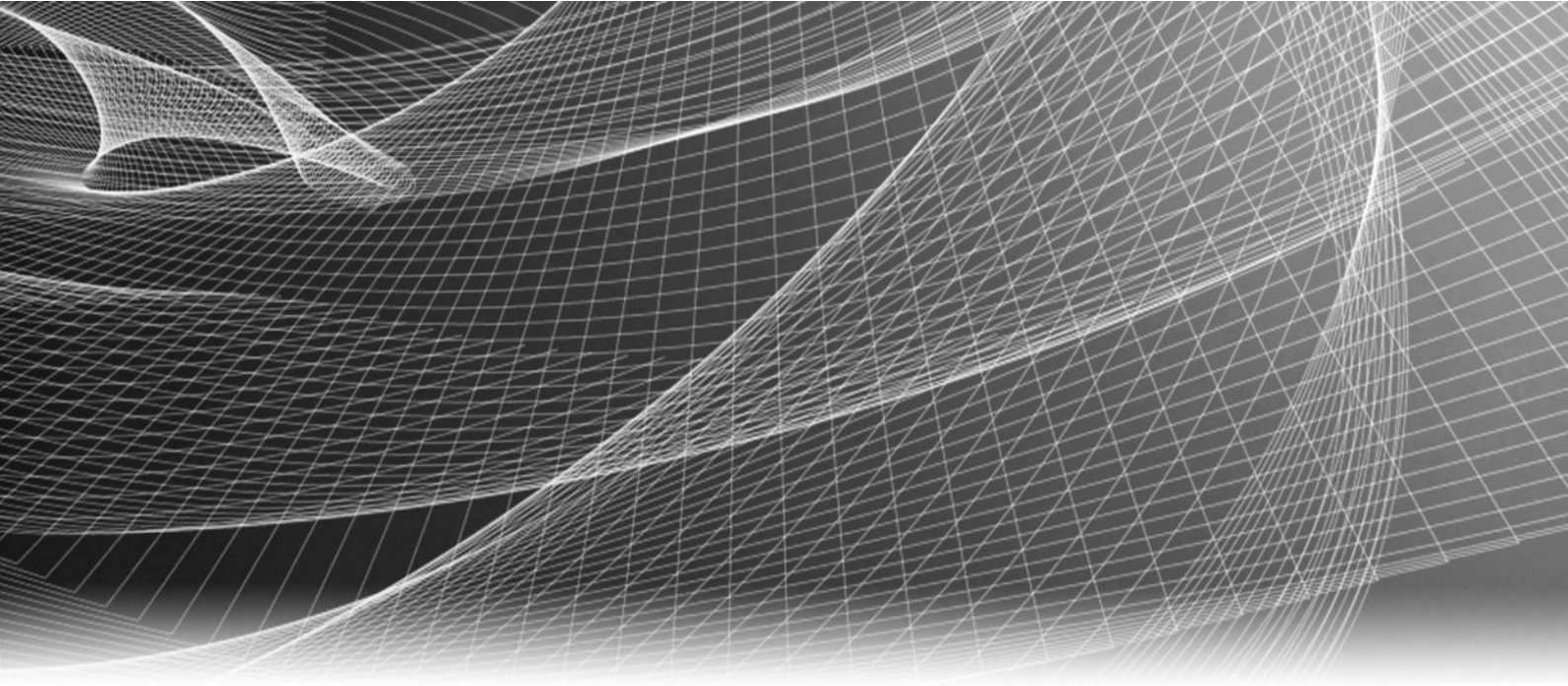


EMC® AppSync™

Version 2.2.2

User and Administration Guide

302-002-307

01

EMC²

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

CHAPTER 1

Introduction

This chapter includes the following topics:

AppSync overview

EMC AppSync offers a simple, SLA-driven, self-service approach for protecting, restoring, and cloning critical Microsoft and Oracle applications and VMware environments. After defining service plans (such as Gold, Silver, and Bronze), application owners can protect, restore, and clone production data quickly with item-level granularity by using the underlying EMC replication technologies. AppSync also provides an application protection monitoring service that generates alerts when the SLAs are not met.

AppSync supports the following applications and storage arrays:

- Applications — Oracle, Microsoft SQL Server, Microsoft Exchange, and VMware VMFS and NFS datastores and File systems.
- Storage — VMAX, VMAX 3, VNX (Block and File), VNXe, XtremIO, and ViPR Controller
- Replication Technologies—VNX Advanced Snapshots, VNXe Unified Snapshot, SRDF, TimeFinder, SnapVX, RecoverPoint, XtremIO Snapshot, and ViPR Snapshot .

Overview of service plans

AppSync protects an application by creating copies of application data.

You indicate to AppSync what you want to protect by subscribing an application object to a *service plan*. When the service plan runs, a copy is created. The service plan can also mount and unmount the copy, validate it, and run user-created scripts. These actions are called phases of the service plan and may differ between applications.

AppSync includes several application-specific plans that work without change. With the **Subscribe to Plan and Run** command, you apply the settings of a service plan to the data and protect it immediately.

Note

These service plans are provided by default. However, you are not restricted to the settings in these plans, you can customize these plans and create the own custom plans.

There are three types of copy selections depending on which plan you use:

- **Create local copy** — For Bronze service plans, creates a local copy (VNX Advanced Snapshot, VMAX TimeFinder Clone, VMAX VP Snap, VMAX 3 SnapVX, Bookmark for RecoverPoint, XtremIO Snapshot, VNX2e Unified Snapshot, VNX File Snapshots, ViPR Snapshot) on the server.
- **Create remote copy** — For Silver service plans, creates a remote copy on the target such as a RecoverPoint Bookmark, VMAX copy off the SRDF target (R2), or VNX Snap off a remote ReplicatorV2 clone.
- **Create local and remote copy** — For Gold service plans, creates both local and remote copies (RecoverPoint bookmarks) on the target.

Service plans also set the preferred order of storage technology to use while creating copies, for example, VNX Snapshot or VMAX clone/snap or RecoverPoint Bookmark.

All service plans can set the period for automatic expiration of copies. When you subscribe an object to a service plan, it joins any other objects that are already part of the plan. All objects in the service plan are subject to the workflows and settings that are defined in the service plan. (The exceptions are the overrides specific to startup or mounting a copy.)

Service plans also offer a few application-specific copy options. For example, Oracle service plan has the following copy options:

- Places database in hot-backup mode (Default: enabled)
- Copies the Fast Recovery Area (Default: disabled)
- Indexes and copies BCT (block change tracking) file (Default: disabled)
- Creates backup control file (Default: disabled)

The default service plans offer tiered levels of protection. If you want to modify a service plan, change its settings to match the requirements, or create a new service plan.

Mount/unmount VMAX 3 copies

Mount/unmount operations on VMAX 3 include masking/unmasking LUNs or a set of LUNs to a host. AppSync relies on the VMAX 3 Auto-Provisioning capability.

The mount host must be zoned to the VMAX 3 array. Next, you can create a masking view with the initiator group, port group, and storage group.

When AppSync performs a mount operation on VMAX 3, it discovers the host initiator for the mount host first, then based on this host initiator, AppSync maps to (or from) the masking view. This operation determines the storage group where the target LUNs are masked/unmasked . For RDM or Vdisk mount/unmount, AppSync identifies the masking view that is based on the host initiator for the ESX server.

You can select the wanted Service Level Objective (SLO) for the target LUN in the mount phase of the service plan. If there is a storage group for the mount host with the wanted SLO, AppSync adds the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host.

If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices are added to the original storage group when the copy is expired.

Role-based management

AppSync supports role-based access to resources and functionality.

You can set up AppSync to have multiple users. Each user can be assigned one or more roles that correspond to their responsibilities and requirements. You can create users that are local to AppSync, and optionally add users through an LDAP server which handles the authorization.

Refer to the *EMC AppSync Security Configuration Guide* available on the EMC Support website for specific user roles and their permissions.

Reports show proven protection

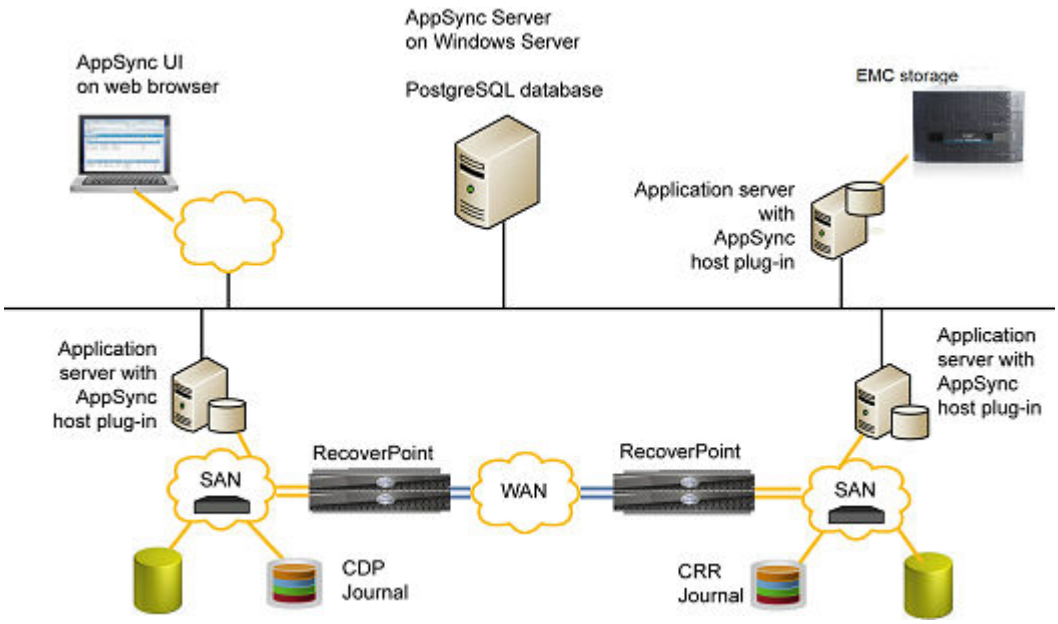
AppSync generates reports that tell you whether your data is protected, recoverable, and compliant with service level agreements.

The reports included with AppSync work without modification. Alerts and reports can be easily viewed at the top level of the AppSync dashboard. Alerts can be sent in email. AppSync can export reports to comma-separated value format.

AppSync architecture

AppSync components include the AppSync server, agent (host plug-in software), and user interfaces (UI or console).

Figure 1 AppSync architecture flow



AppSync server

The AppSync server software resides on a supported Windows system. It controls the service plans and stores data about each copy it creates.

The repository is stored in a PostgreSQL database on the AppSync server.

AppSync agent (host plug-in) overview

AppSync installs light-weight agent plug-in software on the production and mount hosts.

AppSync pushes the plug-in software from the AppSync server to the host when you add the host as a resource. In an environment that prevents the AppSync server from accessing a host, you can install the agent plug-in manually.

Note

With a push-install, the agent host plug-in remains at the same version as the AppSync server. If you want to upgrade the agent host plug-in, select **Update plug-in** with **Settings › Servers**.

For UNIX, tar bundles for AIX and Linux are pushed and extracted on the host during host registration.

Examples of hosts where the plug-in resides are Exchange mailbox servers or Exchange validation or mount hosts. The agent plug-in is not used for protection of VMware data stores.

Linux deployment requirements

For the latest support versions, see the *EMC AppSync Support Matrix*. Linux deployment requirements include:

- Red Hat Linux
- Oracle® Linux
- CentOS
- SuSE Linux
- Compatible Linux sg3_utils package
- Supported Linux host with root SSH enabled or another OS user with SUDO feature enabled.
- Supported Oracle database software that is installed on mount hosts for database recovery.
- Supported Oracle database that is created on production hosts with /etc/oratab entries.
- A valid Oracle database configuration.

AIX deployment requirements

- OpenSSH and OpenSSL packages. OpenSSL is a pre-requisite for OpenSSH installation.
- The following packages are mandatory for AppSync to work with AIX hosts.
  - BZip2 package. This package is also mandatory for AppSync to work with AIX hosts. Zlib package is a prerequisite for Bzip2 installation.
  - SUDO package (only if you want the SUDO feature), or to OpenSSH and OpenSSL. Zlib is a pre-requisite for enabling SUDO feature.
- Supported Oracle database software that is installed on mount hosts for database recovery.
- Supported Oracle database that is created on production hosts with `/etc/oratab` entries.
- Valid Oracle database configurations as described previously in this section.

Package locations:

- OpenSSH and OpenSSL packages are on the OS CD.
- Bzip2, Zlib, and Sudo are on the IBM AIX Toolbox website.

Linux/AIX with sudo user requirements

You can use root user on AppSync production and mount or production hosts. If you do not want to use root, AppSync can use an alternative user with sudo access by creating an operating system user on Oracle production and mount servers, then perform the following edits:

- Edit `sudousers` file using `visudo`, and then add these lines at the end of the file. (You must edit this file as root.)
  - `Defaults:appsync !requiretty`
  - `Defaults:appsync !env_reset`
  - `{user} ALL = (root) NOPASSWD: /{install path}/acp`

where `{user}` is the username you just created and `{install path}` is where you want to install the AppSync agent software. Ensure that the user can write to the directory, for example:

```
appsync ALL = (root) NOPASSWD:
/opt/emc/appsync/acp
```

Install

After performing pre-installation procedure, install AppSync, see the *EMC AppSync Installation and Configuration Guide*.

Supported device configurations

For the latest versions, see the *EMC AppSync Support Matrix* .

Device mapping using:

Table 1 Supported device configurations

AIX	LINUX
Multipath: Multipathing package is required for platforms running VNX, VMAX, or RecoverPoint on VNX in non-virtualized environments. • Native MPIO • PowerPath	Multipath: Multipathing package is required for platforms running VNX, VMAX, or RecoverPoint on VNX in non-virtualized environments. • Native MPIO • PowerPath • Veritas DMP ▪ Supported where both production and mount host have DMP installed and DMP devices do not have a partition. ▪ Supported with non-ASM database on VXDMP devices with or without VXVM Volume manager
Device mapping using: • Symbolic links • mknod devices • Block devices	Device mapping using: • Linux-ASMLib (ASM only) • UDEV bindings • Dev-mapper devices • Block devices with O_DIRECT • Symbolic links
File systems: • jfs and jfs2	

AppSync Console (user interface)

The AppSync console is web-based. Supported browsers are Chrome, Internet Explorer, and Firefox. Refer to an AppSync support matrix for supported versions.

There is an issue with running Flash on Windows Server 2012 R2. Adobe Flash is only installed and enabled when you enable the Desktop Experience. It is not necessary to enable Flash Player on Windows 2008 R2. For Windows 2008 R2, go to the Adobe website to download and install the latest version of Flash Player.

For Windows Server 2008 R2 or Windows Server 2012 R2 you need to turn off Internet Explorer Enhanced Security Configuration. Close any open Internet Explorer windows. Review these scenarios:

1. • If you are running Windows Server 2008 R2, browse to the Security Information section of Server Summary, and then click **Configure IE ESC** to open the **Internet Explorer Enhanced Security Configuration** dialog.
   • If you are running Windows Server 2012, click **Configure this local server** to open the **Local Server** configuration page. Browse to Properties, next to IE Enhanced Security Configuration, and then click **On** to open the Internet Explorer Enhanced Security Configuration dialog.
2. To edit Internet Explorer Enhanced Security Configuration when members of the local Administrator group are logged on, browse to **Administrators**, and then click **Off**.
3. To edit Internet Explorer Enhanced Security Configuration when all other users are logged on, browse to **Users**, and then click **Off** (Recommended).
4. Click **OK** to apply your changes.

Additionally, enable the Desktop Experience on Windows Server 2012. Follow these steps:

1. Open Server Manager and click **Add Roles and Features**.
2. When the Add Roles and Features Wizard appears, specify the values on the Installation Type, Server Selection, and Server Roles pages.
3. On the Features page, expand User Interfaces and Infrastructure and select **Desktop Experience**.
4. On the Confirmation page, select **Restart the destination server automatically if required** and click **Install**.

REST interface

AppSync has a REST interface that allows application programmers to access information controlled by AppSync.

The API is described in the *AppSync REST API Reference Guide*.

Differences between AppSync and Replication Manager

Although they are related products, there are important differences between AppSync and Replication Manager.

AppSync is primarily different from Replication Manager in that it uses the concept of service plans (protection policies) that are designed to meet specific service level requirements. The service plans are fully customizable and can be applied to the application with a single click. AppSync is easy to use for applications administrators as well as storage administrators, because it does not require prior knowledge in data replication technology.

Interoperability of AppSync and Replication Manager

Replication Manager Server and AppSync Server cannot exist on the same host.

The Replication Manager client and the AppSync agent plugin can be installed on the same host and can co-exist together.

CHAPTER 2

AppSync Console

The chapter includes the following topics:

Console overview

The AppSync console is arranged in sections for management, reporting, and administration.

- The **Dashboard** is a customizable view of reports and alerts. The default dashboard shows recovery point objective (RPO) status of protected applications, service plan completion status, most recent alerts, and activity in progress.
- **Copy Management** lists discovered applications such as Microsoft Exchange and Microsoft SQL Server, and provides the application-oriented entry point for protection, mount, restore, service plan subscription, and other operations.
- The **Service Plans** tab lets you view and modify service plan settings, view lists of objects that are subscribed to a service plan, the copies that were made of those objects, and the events that were generated when the service plan was run.
- **Monitoring** displays alerts, recovery point compliance reports, and service plan completion reports.
- **Settings** is for adding servers, VMware vCenter servers, and storage resources to AppSync. License management, user administration, and server settings are also found under Settings.
- **Support** provides access to how-to videos and the AppSync support page on the EMC Support website.

User roles control which sections of the console are displayed and which operations are listed in menus. For example, the console does not display the **Copy Management** and **Service Plans** tabs for a user who has only the Security Administrator role.

Performing actions

To perform an action on an object, select the object and click the action buttons at the bottom of the page. Use the Shift key to select multiple objects. Use Ctrl to select noncontiguous objects. To perform an action on multiple objects, click the action button on the final selection.

Examples of objects are application hosts, storage systems, mailbox servers, databases, copies and users.

Times shown in the console

Times shown in the AppSync console reflect the local time of the AppSync server, not of the console.

Troubleshooting console problems

Unexpected behavior by the AppSync console may be related to the browser and its supporting add-ons and extensions.

Check the latest support matrix for supported browser versions.

Troubleshooting browser display problems

Learn how to resolve data display issues in the AppSync console.

Symptom: AppSync displays stale or corrupted data.

Resolution:

1. Clear browser cache. Refer to the browser sepecific documentation for more information.
2. Clear the Java cache:
   a. Select **Start** › **Control Panel** (Windows 7) or **Start** › **Control Panel** › **Programs** (Windows 2008/2012).
   b. Double-click the Java icon.
   c. Select **Settings** under **Temporary Internet Files**.
   d. Select **Delete Files**.
   e. Select all available options and select **OK**.

Troubleshooting browser refresh issues

Symptom: Some contents in the AppSync console are not displayed.

Cause: You refreshed the browser using the browser's **Refresh** icon or pressing F5 on your keyboard.

Resolution: To refresh content in the AppSync console, use the **Refresh** icon on the console's top right corner.

Setting preferences

You can set the language displayed in the user interface and optimize the console for use over remote connections.

Procedure

1. Select the language of choice from the list of installed languages.

   If you change the language, you must close the browser and launch AppSync again for the settings to take effect.

2. Check **Optimize for Remote Connection** to optimize the user interface for use over remote connections.

   For example, certain visual effects may cause slow screen painting when you remotely access the console. Selecting this option enhances the remote response time but does not affect management options or functionality.

Starting the AppSync console

You can run the AppSync console on a supported web browser from any system that has connectivity to the AppSync server.

Use http://*appsync_server*:8085/appsync to start the console.

If you are running the console on the AppSync server, you can start the console by clicking on the AppSync shortcut on the installer's desktop. *appsync_server* must be a host name, not an IP address.

CHAPTER 3

Service Plans

This chapter includes the following topics:

Service plan overview

Learn about default service plan types, object and copy subscriptions, service plan settings, schedules, and overrides.

For information on how each array type supports service plans, refer to the section on prerequisites in the *EMC AppSync Installation and Configuration Guide*.

AppSync creates and manages copies of application data. A service plan defines the attributes of these copies. You can subscribe application data objects to a service plan, then AppSync runs the service plan and creates copies of the data from attributes that you specified in the plan. Copies that are generated by a service plan are listed in service plan **Copies** tab.

There is no limit to the number of objects you can subscribe to a service plan. AppSync automatically divides up the work for best performance. If you need fine control over which objects are grouped for mounting, scripting, and validating, consider creating multiple service plans and distributing objects among the plans. This technique works when the objects subscribed to a service plan are from the same server. Subscribe no more than 12 objects to any one service plan when using this method.

Service plan types

AppSync provides the following application-specific tiered plans. There are three types of copy selections depending on which plan you use:

- **Create local copy** — For **Bronze** service plans, AppSync creates a local copy on the server with VNX Advanced Snapshot, VMAX TimefinderClone, VMAX VP Snap, VMAX 3 SnapVX, Bookmark for RecoverPoint, XtremIO Snapshot, VNX2e Unified Snapshot, VNX File Snapshots, ViPR Snapshot.
  AppSync also supports ViPR snapshots as copy technology for applications provisioned using ViPR Controller. AppSync only supports applications provisioned by ViPR with block virtual pools that are backed only by VMAX/VPLEX (with VMAX2 and XtremIO)/XtremIO storage systems. Currently only VMware datastore, Oracle, and file system on Linux and AIX are supported.
- **Create remote copy** — For **Silver** service plans, AppSync creates a remote copy (RecoverPoint Bookmark, VMAX2 copy off the SRDF target (R2), VMAX V3 SnapVX, or VNX File Snap off a remote ReplicatorV2 clone on the target.
- **Create local and remote copy** — For **Gold** service plans, AppSync creates both local and remote copies (for example, RecoverPoint Bookmarks) on the target.

Note

Ensure you understand the storage capabilities when selecting a service plan type. Not all storage technologies support Remote Replication, so Silver or Gold service plans may not be successful for the application data.

Bronze, Silver and Gold service plans are provided by default, however you can customize and create the own plans.

Service plan settings

When you subscribe an object to a service plan, it joins other objects that are already part of the plan. All objects in the service plan are subject to the workflow and settings that are defined in the service plan.

Service plans set a storage ordered preference which is the preferred order of storage technology the service plan uses when creating copies. If AppSync cannot satisfy a preference, it tries to use the next preference in the storage ordered preference list. You

can adjust the preferences to create service plans that use the replication technology you want.

The default service plans offer tiered levels of protection. If you must change settings, modify the service plan.

Any service plan can set the automatic expiration of copies which limits the number of copies that AppSync keeps, and automatically expires older copies that exceed the number that is defined for the service plan.

Service plans also offers a few application specific copy options which can be modified. For example, Oracle service plan has the following copy options:

- Place a database in hot-backup mode (Default: enabled)
- Copy the Fast Recovery Area (Default: disabled)
- Index and copy BCT (block change tracking) file (Default: disabled)
- Create backup control file (Default: disabled)

To avoid overutilization and depletion of replication storage, when you set up a service plan, set values in the following fields:

- **RPO** in the service plan **Startup** phase
- **Always keep n Copies** in the **Create copy** phase

Also, monitor the storage system with the storage system user interface on the AppSync console.

Service plan schedule overrides

You can override a service plan's run schedule settings and specify separate schedules for individual objects that are subscribed to the plan.

In the **Plan Startup** phase of the service plan, you select a recurrence type that is based on which service plan is triggered. This recurrence type is applicable for all application objects that are subscribed to a service plan. However, you can override the settings and specify separate settings for selected objects.

You can override only the settings of the **Recurrence Type** already selected for the plan. For instance, the chosen recurrence type is to run **On selected days...** and the settings are to **Run at 12:00 AM on days Fri, Sat**. When you override these settings for an object, you can change only the time and days of the week. You cannot select a different recurrence type as part of the override.

As the Service Plan Administrator, if you change the generic recurrence settings (such as the time to run, or minutes after the hour), there is no impact to the settings of the overrides. If you change the recurrence type itself, then the overrides are no longer valid. The new recurrence type now applies to all objects until you specify individual settings that are based on the new recurrence type.

Note

If an application object is subscribed to multiple plans, the plans must not be scheduled to be running simultaneously.

Service plan events

Events show the progress of an operation. They are generated when a service plan is run, and when a copy is mounted or restored.

Event information includes:

- Type (error, warning, or informational)
- Date and time of the event

- Description
- Server

You can view events at:

- Service plan **Events** tab. For example, on the AppSync console, the **Events** tab in **Service Plans** › **Microsoft Exchange** › **Bronze** shows you the events that are related to the Exchange copy under the plan.
- Application **Copies** page. For example, go to **Copy Management** › **VMware Datacenters** select a data center, then a datastore to view the **Copies** page. Select a copy to view its associated events in the **Events** page.
- Events are also displayed at the time they are generated in the Mount and Restore wizards and when an object is subscribed to a plan and run immediately.

By default only the top level events, which are known as milestone events, are displayed. A milestone event is generated at the completion of each phase in a service plan cycle. You can expand a milestone event to show the other events that were generated in the phase.

Creating a service plan

You can create a new service plan by using an existing plan as a template.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

Procedure

1. Select **Service Plans**.
2. Click **Create**.
3. In the **Create New Plan** dialog box, select an existing plan to use as a template. Enter a name and a description for the new service plan.

Note

The new service plan contains the same schedule and other settings as the template, but there are no objects subscribed to the new service plan.

Running a service plan on demand

Service plans run on a schedule but you can also run a service plan on demand.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Select **Service Plans**.
2. Select the application to protect.
3. Select a plan from the list and click **Run**.

   This service plan run is applicable to all the application objects currently subscribed to the plan.

   The service plan runs immediately. The **Run Service Plan** dialog displays progress as application storage is discovered and mapped, and application protection begins according to service plan settings.

4. Click **Details** to see more events that occurred during each phase.

Disabling and reenabling a service plan

By default all service plans are enabled. You can disable and reenable a service plan.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

Procedure

1. Select **Service Plans**.
2. Select the application.
3. Select the plan and click **Disable** or **Enable**.

Deleting a service plan

You can delete a user-created service plan.

Before you begin

- This operation requires the Service Plan Administrator role in AppSync.
- You cannot delete a built-in service plan (for example, Bronze, Silver, Gold).
- You cannot delete a service plan if the plan has subscriptions or if there are valid copies associated with the plan.

Procedure

1. Select **Service Plans**.
2. Select the application.
3. Select a user-created plan and click **Delete**.
4. Click **Yes** to confirm.

Summary of Exchange service plans settings

The default service plan settings create an application-consistent copy every 24 hours. Only the replication technology, which is specified by the **Copy type** in the Create copy phase, is different from plan to plan.

Table 2 Exchange Service Plan - default settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: Creates a copy every 24 hours, with the first run at midnight (00:00). Recovery Point Objective (RPO): A copy should be created every 24 hours. (Alert is issued if

Table 2 Exchange Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
			objective is not met.)
Application discovery	Enabled	None	Determined by **Plan Startup** phase
Application mapping	Enabled	None	Starts when **Application discovery** phase completes
Pre-copy script	Not enabled	None	Starts when **Application mapping** phase completes

Create copy	Enabled	• Copy type is:
		  ▪ Bronze: Create Local copy
		  ▪ Silver: Create Remote copy
		  ▪ Gold: Create Local and Remote copy (includes VNX File Snapshots).
		• Exchange backup type: Full, Copy or Differential
		• Storage Ordered Preference: Snapshot, Bookmark
		Note
		For silver and gold service plans, Bookmark and VNX File Snapshots are available. VMAX SRDF is supported for Silver service plans(remote copy).
		• Storage Settings:
		  ▪ Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations.
		Note
		If this option is not checked, then RecoverPoint copies accumulate, and remain until the bookmarks for them "fall off" the RecoverPoint appliance.
		• Event Log Scanning:
		  ▪ Fail on -1018 error
		  ▪ Fail on -1019 error
		  ▪ Fail on -1022 error
		  ▪ Fail on Event ID 447
		  ▪ Fail on Event ID 448
		  ▪ Do not allow databases and logs to reside on the same volume
			Starts when **Pre-copy script** phase completes

Table 2 Exchange Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
Post-copy script	Not enabled	None	Starts when **Create copy** phase completes
Unmount previous copy	Not enabled	None	Starts when **Post-copy script** phase completes
Mount copy	Not enabled	• Mount on server: Original Host • Mount with access: Read-only • Mount Path: Default Path **Note** The drive that is specified for mount cannot be a clustered disk. • Copy metadata files to: Default Path • Image access mode: Logged access	Starts when **Unmount previous copy** phase completes
Validate copy	Not enabled	• Check databases and logs in parallel • Do not minimize log checking • Do not perform throttle checking	Starts when **Mount copy** phase completes
Post-mount script	Not enabled	None	Starts when **Validate copy** phase completes
Unmount copy	Not enabled	None	Starts when **Post-mount script** phase completes

Summary of SQL Server service plans settings

Summary of SQL Server service plans settings

Table 3 SQL Server Service Plan - default settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: Creates a copy every 24 hours, with the first run

Table 3 SQL Server Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
			at midnight (00:00). Recovery Point Objective (RPO): A copy should be created every every 24 hours. (Alert is issued if objective is not met).
Application discovery	Enabled	None	Determined by Plan Startup phase
Application mapping	Enabled	None	Starts when Application discovery phase completes
Pre-copy script	Not enabled	None	Starts when Application mapping phase completes
Create copy	Enabled	• Copy type is: ▪ Bronze: Create Local copy ▪ Silver: Create Remote copy ▪ Gold: Create Local and Remote copy • SQL Server Backup Type: Full or Copy ▪ Auto Switch to Copy ▪ Enable Log Backup **Note** This option must be selected to permit on demand log backup runs. • Storage Ordered Preference: Snapshot, Clone, Bookmark • Expiration of database copies: ▪ Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations. **Note** If this option is not checked, then RecoverPoint copies will accumulate, and will remain until the bookmarks for them "fall off" the RecoverPoint appliance. • Transaction Log backup options: ▪ Schedule immediately after database backup = default.	Starts when Pre-copy script phase completes

Table 3 SQL Server Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
		▪ Every 15 or 30 minutes or every 1 to 24 hours are other options. **Note** Scheduled log backups run during times between database backups. ▪ Backup path: Default path ▪ Free space on the volume: 5GB ▪ Backup group size: 5 ▪ Truncate logs: Selected ▪ Checksum the backup: Unselected ▪ Compression: Selected ▪ Expiration of log backups: Minimum retention hours 24	
Post-copy script	Not enabled	None	Starts when Create copy phase completes
Unmount previous copy	Not enabled	None	Starts when Post-copy script phase completes
Mount copy	Not enabled	• Mount Copy ▪ Mount on Server: Original Host ▪ Mount with access: Read only ▪ Mount Path: Default Path **Note** The drive specified for mount can not be a clustered disk. ▪ Copy metadata files to: Default Path ▪ Image Access mode: Logged access	Starts when Unmount previous copy phase completes
Post-mount script	Not enabled	None	Starts when Mount copy phase completes
Unmount copy	Not enabled	None	Starts when Post-mount script phase completes
Pre-log backup script	Not enabled	None	Starts after log backup

Table 3 SQL Server Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
Post-log backup script	Not enabled	None	Starts after log backup

Summary of Oracle service plan settings

Use this list of service-plan default settings for Oracle databases in AppSync.

Table 4 Oracle Server Service Plan - default settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: AppSynccreates a copy every 24 hours, with the first run at midnight (00:00). Recovery Point Objective (RPO): Creates a copy every 24 hours.
Application discovery	Enabled	None	Determined by Plan Startup phase
Application mapping	Enabled	None	Starts when Application discovery phase completes.
Pre-copy script	Enabled	None	Starts when Application mapping phase completes
Create copy	Enabled	The create copy options on the service plan settings provides various controls which influence how the Oracle copy is created. Copy types include: • Bronze: Create Local copy . • Silver: Create Remote copy. • Gold: Create Local copy and Remote copy. Create copy setting options include: • Place database in hot-backup mode (Default: enabled) When enabled, the protection puts the database in hot backup and immediately creates copies of the archive logs. If you disable this option, the database is not placed in hot backup mode and the copy is	Starts when Precopy script phase completes.

Table 4 Oracle Server Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
		created from the live unquiesced data without any instrumentation of the database. • Copy the Fast Recovery Area. (Default: disabled) When enabled, this field tells AppSync to create a copy of the underlying storage that is used by the FRA when protecting the database's archive log files. • Index and copy the BCT (block change tracking) file. (Default: disabled) If enabled, AppSync creates an entry in the Oracle block change tracking file and re-copies the file as part of the protection. This file can then be leveraged as part of a mount and backup use-case to provide accelerated incremental backup. This option requires hot backup mode. • Create backup control file for RMAN cataloging. (Default: disabled) If enabled, AppSync creates a binary backup control file with a request to catalog the database contents in a remote RMAN catalog. This option requires hot backup mode. • Expiration: Include RecoverPoint copies in expiration rotation policy: select this option to include RecoverPoint copies when calculating rotations. If you do not select this option, RecoverPoint copies accumulate and remain until their bookmarks rotate off the RecoverPoint appliance. **Note** If RecoverPoint copies are factored in the rotation policy, bookmarks are created with the ALWAYS_CONSOLIDATE policy. Otherwise, bookmarks are created with the NEVER_CONSOLIDATE policy. Consult the RecoverPoint documentation for a definition of these consolidation policies.	
Post-copy script	Not enabled	None	Starts when Create copy phase completes.
Unmount previous copy	Not enabled	None	Starts when Post-copy phase completes
Pre-mount script	Not enabled	None	Starts when Unmount previous copy phase completes appliance.
Mount and Recovery	Not enabled	Mount and recovery options: • Mount on standalone server (RM-equivalent : No recover) • Mount on standalone server and create RMAN catalog entry (RM-equivalent : Catalog with RMAN)	Starts when Pre-mount script phase completes.

Table 4 Oracle Server Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
		• Mount on standalone server and recover database (RM-equivalent: Recover) • Mount on standalone server and prepare scripts for manual database recovery (RM-equivalent: Prepare-only/generate scripts for manual recovery) • Mount on grid cluster and recover as RAC database (RM-equivalent: Mount as RAC database)	
Post-mount script	Not enabled	None	Starts when mount phase completes.
Unmount copy	Not enabled	None	Starts when Post-mount script phase completes.

Summary of file system service plan settings

Use this table to learn default file system settings for service plan phases including startup, discovery, mapping, pre and post copy scripting, mount/unmount and copy.

Default service plan settings create an application-consistent copy every 24 hours. Only the replication technology that is specified by the Copy type in the Create copy phase varies among plans. The following table summarizes the default settings:

Table 5 Default file system Service Plan Settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: Creates a copy every 24 hours, with the first run at midnight (00:00). Recovery Point Objective (RPO): A copy should be created every 24 hours. (Alert issued if objective is not met.)
Application discovery	Enabled	None	Determined by Plan Startup phase.
Application mapping	Enabled	None	Starts when Application discovery phase completes.

Table 5 Default file system Service Plan Settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
Pre-copy script	Not enabled	None	Starts when Application mapping phase completes.
Create copy	Enabled	Copy type: • Bronze: Create local copy. • Silver: Create remote copy (VMAX v2, VMAX v3, RecoverPoint, and VNX File). • Gold: Create Local and Remote copy (RecoverPoint and VNX File). Also: • Storage Ordered Preference: Snapshot, Clone & Bookmark. • Storage Settings: Include RecoverPoint copies in expiration rotation policy—select this option to include RecoverPoint copies when calculating rotations. If you do not select this option, RecoverPoint copies accumulate and remain until the bookmarks for them "fall off" the RecoverPoint appliance.	Starts when Pre-copy script phase completes.
Post-copy script	Not enabled	None	Starts when Create copy phase completes.
Unmount previous copy	Not enabled	None	Starts when Post-copy script phase completes.
Mount copy (A pre-mount script phase is available for file system service plans)	Not enabled	Mount Copy • Mount on Server: Original Host • Mount with access: Read/write • Mount Path: Default Path Image • Access mode: Logged access • Copy to Mount: Local (Only for Gold Plans) • Use Dedicated Storage Group: Selected by default	Starts when Unmount previous copy phase completes.
Post-mount script	Not enabled	None	Starts when Mount copy phase completes.

Table 5 Default file system Service Plan Settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
Unmount copy	Not enabled	None	Starts when Post-mount script phase completes.

Summary of VMware service plans settings

The default service plan settings create an application-consistent copy every 24 hours. Only the replication technology, which is specified by the **Copy type** in the Create copy phase, is different from plan to plan.

Table 6 VMware Service Plan - default settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: Creates a copy every 24 hours, with the first run at midnight (00:00). Recovery Point Objective (RPO): A copy should be created every 24 hours. (Alert is issued if objective is not met.)
Application discovery	Enabled	None	Determined by Plan Startup phase
Application mapping	Enabled	None	Starts when Application discovery phase completes

Create copy	Enabled	• Copy type is:
		  ▪ Bronze: Create Local copy
		  ▪ Silver: Create Remote copy
		  ▪ Gold: Create Local and Remote copy
		• Copy Consistency:
		  ▪ Virtual machine Consistent with a maximum of 4 simultaneous VM snapshots
			Starts when Application mapping phase completes

Table 6 VMware Service Plan - default settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
		▪ Ignore VM Snapshots for VMs: link to select individual virtual machines to ignore while taking VMware snapshots during the service plan run. ▪ Include Virtual Machine Disk: Select this checkbox to protect virtual machine disks spanning multiple data stores. By default, this option is not selected. • Storage Ordered Preference: Snapshot, Clone, Bookmark **Note** For silver and gold service plans, Bookmark and VNX File, and VMAX SRDF(Remote copy) are available. • Expiration: Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations. **Note** If this option is not checked, then RecoverPoint copies will accumulate, and remain until the bookmarks for them "fall off" the RecoverPoint appliance.	
Unmount previous copy	Not enabled	None	Starts when Create copy phase completes
Mount copy	Not enabled	• No default mount host • Mount using new signature • For RecoverPoint: mount with logged access, and mount local copy (in case of local and remote copy plan) • For VNX file, mount copy with read-only or read/write access for local or remote copies	Starts when Unmount previous copy phase completes
Unmount copy	Not enabled	None	Starts when Mount copy phase completes

CHAPTER 4

AppSync CLI Utility

This chapter includes the following topics:

AppSync CLI Utility tutorial

The AppSync CLI is a utility that is packaged with AppSync and is used for scripting or running tasks through a command line interface

The AppSync CLI is installed in the `EMC\AppSync\appsync-cli` directory. You can run it on Windows with the file `appsync-cli.bat`, and in UNIX using `appsync-cli.sh`.

Pre-requisites

- Java Runtime Environment (JRE) version 7 Update 6 (jre1.7) and above - must be installed and available in path.
- Configured AppSync installation with registered resources
- Discovered applications on registered hosts
- Configured service plans
- For I18N support on Windows, be sure that you set the correct code page before execution.

Using the CLI

You can run the AppSync CLI on the server where the AppSync installation resides. Also, you can move the `\EMC\Appsync\appsync-cli` directory to another location/host. All actions that are performed, for scripting purposes, return code zero 0 for success and local system failure code -1 for Windows or 255 for Linux). The syntax for using the AppSync CLI follows:

`appsync-cli.bat -action options=value`

You preface the action that you want to perform with a hyphenated **`-argument`**. All options specific to that action are **`key=value`** pairs. When using a value that contains spaces such as a file system or path, you are not required to surround the text in double quotations. Do not surround a value that ends with a trailing backslash with double quotes. Java ignores this construct.

The AppSync CLI also has two optional arguments for message handling. At any point, you can use the argument `verbose=true` for a more detailed messaging output, and `silent=true` to suppress all messages.

The AppSync CLI supports the following actions:

- Login/logout
- Run a service plan
- Enable/disable a service plan
- List all copies that are created for a service plan or application object
- List all details of an application object
- Subscribe/unsubscribe an application object to/from a service plan
- Mount/unmount a copy
- Expire a copy
- Run and export AppSync reports

Using the Help "/?" argument

To evoke a detailed help menu for a command, add the **/?** argument. This argument displays all available CLI commands. Because of the complexity and vast number of arguments, the CLI help uses the following help menu partitions:

- **appsync-cli.bat /?** Returns information on all CLI-supported actions.
- **appsync-cli.bat -action /?** Returns non-specific application options available for the selected action.
- **appsync-cli.bat -action app=<value> /?** Returns application-specific options available for the selected action.
- appsync-cli.bat -mount app=<value> option=<value> /? Returns mount-specific options for the provided mount option.

Note

When using the help argument on non-English system locales you must enclose the help argument "/?" in double quotation marks.

CLI actions

Log in/Log out

Before performing CLI actions, authenticate to an AppSync server. The log in command requires server name, https communication port, AppSync user, and corresponding password. For example:

```
appsync-cli.bat -login server=<server> port=8445 user=admin
password=<admin_pass>
```

After you log in, a file that is named LOCAL_TOKEN is created in the current directory containing required authentication information. If this file is deleted or the current session expires, a new session must be created by running the login command once again.

After you complete actions with the AppSync CLI, ensure you log out. The log out command not only closes the current session, but also invalidates it. For example:

```
appsync-cli.bat -logout
```

Run/Enable/Disable a service plan.

Enable, Disable, and Run a service plan by supplying the application name and service plan. For example:

```
appsync-cli.bat -runSP app=sql service_plan=Bronze
```

```
appsync-cli.bat -enableSP app=sql service_plan=Bronze
```

```
appsync-cli.bat -disableSP app=sql service_plan=Bronze
```

Subscribe/Unsubscribe

You can subscribe an application object to a service plan with the CLI. Options vary for each application. Run the help command "/?" for the application that you want to subscribe/unsubscribe for a complete list of required arguments. For example:

```
appsync-cli.bat -subscribe app=oracle service_plan=<sp1>
oracle_server=<server> db_name=<db1>
```

```
appsync-cli.bat -unsubscribe app=sql service_plan=<sp1>
sql_server=<server> instance_name=<instance> db_name=<db1>
```

List Copies and Copy Details

A copy's uuid is required Before you can mount the copy. To get this information, run the `-listCopies` command for either a service plan or an application object. Again, the arguments are application-specific so be sure to use the help command "/?" for more details.

Use the "age" argument to filter viewable copies on the console by the age of a copy. For example:

```
appsync-cli.bat -listCopies app=sql service_plan=Bronze age=month
```

```
appsync-cli.bat -listCopies app=sql instance_name=<value>
db_name=<value> age=all
```

To see more details of an application copy you can run the `-copyDetails` command and supply the copy's uuid. For example:

```
appsync-cli.bat -copyDetails app=<app> copy_ID=<value>
```

Mount/Unmount

The AppSync CLI supports all mount options that are available through the GUI. Options vary for each application. Run the help "/?" command for the application you want to mount to determine mount options. For example:

```
appsync-cli.bat -mount app=filesystem copy_ID=<value>
mount_host=<value>
```

```
appsync-cli.bat -mount app=sql copy_ID=<value> option=recover
recovery_instance=<value> point_in_time=<value>
```

```
appsync-cli.bat -mount app=datastore copy_ID=<value>
mount_host=<value> cluster_mount=yes image_access_mode=virtual_roll
```

```
appsync-cli.bat -mount app=oracle copy_ID=<value> option=rac
mount_cluster=<value> mount_servers=<server1,server2>
```

To unmount a copy you need the application name and the copy `uuid`. For example:

```
appsync-cli.bat -unmount app=<app> copy_ID=<value>
```

To unmount the latest or oldest mounted copy specifically for the database\filesystem \datastore, use the following commands:

- For Datastores: **`appsync-cli.bat -unmount app=datastore datastore=<value> datacenter=<value> vcenter=<value> option=latestMountedCopy/oldestMountedCopy`**
- For SQL application: **`appsync-cli.bat -unmount app=sql instance_name=<value> db_name=<value> option=latestMountedCopy/ oldestMountedCopy`**
- For Oracle application: **`appsync-cli.bat -unmount app=oracle oracle_server=<value> db_name=<value> option=latestMountedCopy/ oldestMountedCopy`**
- For file systems: **`appsync-cli.bat -unmount app=filesystem fs_server=<value> fs_name=<value> fs_type=<value> option=latestMountedCopy/oldestMountedCopy`**

For service plan level, the copy can be of any database that is subscribed to that service plan To unmount a copy you need the application name and the service_plan. For example:

The copy can be of any database that is subscribed to that service plan

To unmount a copy you need the application name and the service_plan. For example:

appsync-cli.bat -unmount app=‹app› service_plan=‹value› option=latestMountedCopy/oldestMountedCopy

X

Expire a copy

To expire a copy, you need the application name and the copy uuid. Type `-listCopies`. For example: `appsync-cli.bat -expire app=datastore copy_ID=<value>`

Run reports

There are four available reports that you can run and export through the AppSync CLI. They include:

- RecoverPoint Objective (rpo)
- Service Plan Completion (spc)
- Alert
- Activity

Run reports in either summary or detailed view using the **`detailed=true/false`** argument. The exception to this rule occurs with an activity report which prints the activity that is currently running.

All reports are exported to a `.csv` file in the current directory with unique name from the report type and local time. For more help, use the help command (/?) for reports. For example:

`appsync-cli.bat -report report_type=rpo detailed=true`

CHAPTER 5

Protect Microsoft Exchange

This chapter includes the following topics:

Overview of Exchange support

Use AppSync to create application-consistent copies of Exchange data.

AppSync support for Microsoft Exchange application includes:

- Protect and manage Microsoft Exchange in standalone and DAG environments (active and passive databases).
- Mount copies to a Windows 2008 or Windows 2012 host for running consistency check or to back up to long-term storage.
- Restore from copies to production Exchange databases in the event that production databases must be brought back to a point-in-time.
- Restore individual mailboxes and mailbox items using Kroll Ontrack®. This action can also be done using EMC ItemPoint™ for Microsoft Exchange until this product reaches End of Service Life (EOSL).
- Support for databases on physical hosts, RDMs, and virtual disks on virtual hosts.

Note

AppSync only supports RDMs in physical compatibility mode. RDMs in virtual mode are not supported.

Exchange Server prerequisites

Verify that the Exchange configuration meets supported version requirements for AppSync, including Windows operating system requirements as well as supported service packs for Exchange. The *AppSync Support Matrix* on https://elabnavigator.emc.com/eln/extendedSupport is the authoritative source of information on supported software and platforms.

AppSync supports protection and operational recovery of Exchange databases in standalone and DAG configurations including:

- Exchange 2010 mailbox servers on Windows Server 2008 SP2 and Windows Server 2008 R2 or later.
- Exchange 2013 mailbox servers on Windows 2008 R2 SP1 or later.
- Microsoft Exchange 2010 and 2013 Database Availability Groups (DAGs) including active and passive copies.

Support for Exchange on virtual disks

You can protect, mount, and restore Exchange databases residing on VMware RDMs in physical compatibility mode and virtual disks. AppSync supports Full, Copy, and Differential backup types.

During protection:

- For successful mapping, the Virtual Center must be added to the AppSync server and discovery must be performed.
- For successful protection, log files and database files must reside on virtual disks. There cannot be a combination of physical and virtual storage.
- Protection of Exchange databases across virtual machines sharing the same datastore is not supported.
- Virtual Disk is supported for Exchange ESX 5.0 and above.
- AppSync versions 1.6.0.1 and above supports circular logging for Exchange Databases.

AppSync interaction with Microsoft VSS

Microsoft Volume Shadow Copy Service (VSS) is the infrastructure that enables AppSync to create application-aware copies.

When it creates a copy, AppSync coordinates with VSS and Exchange to create a shadow copy. The copy is a point-in-time copy of the volumes that contain the data, logs, and system files for Exchange databases.

AppSync coordinates with VSS and Exchange to quiesce input-output to the databases when creating the copy, and then resume the flow of data after the copy has been created. During a restore, AppSync coordinates with VSS and Exchange to recover the point-in-time shadow copy.

Permissions required by Exchange

Accounts that AppSync uses to work with Exchange require special permissions.

- On Exchange standalone servers, the account must be a domain user account with the Databases role.
- On DAG servers, the account must be a domain user account with the Database and Database Copies roles.
- On a mount host, the user account must be a domain user account that is a member of the local Administrators group.
- The account must have **Log on as a batch job** and **Log on as a service** user rights.
- The account can have the **View-only Organization** role. This role is an optional role applicable only for Microsoft Exchange 2013 if you have public folder mailboxes in the environment. AppSync uses this role to determine the database containing the public folder primary hierarchy mailbox.

AppSync Exchange Interface Service Credentials are required the first time that you access the Exchange server. You are prompted to type two sets of credentials for the AppSync Exchange Interface Service configuration.

AppSync uses the first set of credentials to install and configure the AppSync Exchange Interface service on the Exchange production or mount host. The account must have local administrator privileges. AppSync uses the second set of credentials to run the service. A user must be a domain user with the following Exchange roles:

- Database role for standalone server
- Database and Database Copies roles in DAG environment.

Changes to service plans after upgrade

After an AppSync upgrade, changes to the way service plans operate occur.

Consider the following changes:

- Storage ordered preferences — After an upgrade, all service plans will have their storage ordered preferences replaced with the new style preference. After an upgrade, check the **Create Copy** instructions for each service plan to confirm that the storage ordered preference is correct.
- RecoverPoint copy rotation — After an upgrade, all service plans do not perform replica rotation for RecoverPoint copies. If you want to enable replica rotation for any service plan that creates RecoverPoint copies, check the **Create Copy** instructions for the service plan and check the checkbox to include RecoverPoint copies for Expiration.

Deploying AppSync for Exchange protection: summary of steps

A summary of steps from deployment of AppSync to setting up Exchange protection.

Procedure

1. Install the AppSync server.
2. In the AppSync console, navigate to **Settings** › **Storage Infrastructure** and click **Add**.

   This adds the storage system where the Exchange mailbox database resides.
3. Navigate to **Settings** › **Servers** and click **Add**.

   This adds the Exchange standalone mailbox servers or DAG member servers as hosts.
4. Navigate to **Copy Management** › **Microsoft Exchange** and click a server name from the list of Exchange standalone and DAG servers.
5. Enter the credentials to configure and run the AppSync Exchange Interface service.

   The Exchange databases are discovered.
6. Subscribe an Exchange database for protection by choosing one of the following options:
   - Protect immediately with **Subscribe to Plan and Run**, which subscribes the database to a service plan and runs the protection immediately for the selected database only. In the case of databases in a DAG, one of the passive databases is protected by default.
   - **Subscribe to Plan**, which subscribes the database to a service plan, but does not run the plan. Protection occurs according to the service plan's schedule.

Discovering Exchange databases

To keep AppSync up-to-date, you should discover databases on the Exchange server when there is creation, deletion, or renaming of databases.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- The AppSync Exchange Interface service must be running.
- If you are changing a standalone Exchange server that is part of AppSync to be part of a DAG, you should first remove the standalone server (along with its copies, if any) from AppSync prior to performing a discovery. During discovery, the erstwhile standalone server is identified to be part of the DAG.

Procedure

1. Navigate to **Copy Management** › **Microsoft Exchange**.
2. Click an Exchange server to display its databases.
3. Click **Discover Databases** to discover databases for this server.

Removing an Exchange mailbox server

Remove an Exchange mailbox server when there is no longer a need to manage its protection from the AppSync server.

Before you begin

This operation requires the Resource Administrator role in AppSync.
There should be no copies of the mailbox server that you want to remove.

Procedure

1. Select **Settings** › **Servers**.
2. Select the server to remove.
3. Select **Remove** › **Remove servers only**.

   A dialog appears asking for your confirmation.
4. Click **OK** to confirm your action.

Protecting DAG databases in a service plan

AppSync supports protection of Exchange databases that are part of a Database Availability Group (DAG).

When a DAG server is subscribed to an AppSync service plan, it is one of the passive members of the DAG that is selected for protection, by default.

Procedure

- To protect an active DAG database member, select **Active** in the **Copy to Protect** column from the plan **Subscriptions** tab.

Protect an Exchange database

Protect an Exchange database by subscribing it to an AppSync service plan.

AppSync uses service plans as its protection mechanism for databases. You subscribe a database to a service plan and run the service plan immediately, or schedule the service plan to run at a later time.

- Choose **Subscribe to Plan and Run** when you want to protect a selected database immediately. The service plan is executed for the database alone. In the case of DAG, one of the passive databases is protected by default.
- Choose **Subscribe to Plan** when you want to schedule the protection for later. Protection for databases that are part of the service plan are executed at the scheduled time.
- Choose **Run** from the Service Plan page to run the whole plan immediately. All databases subscribed to the plan are protected.

Protecting an Exchange database immediately

Click **Subscribe to Plan and Run** to add a database to an existing service plan and run the service plan immediately for the selected database alone.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft Exchange**
2. Click an Exchange Mailbox Server or DAG from the list to display its databases.
3. From this list, select a database to protect.

   When performing an operation on multiple items, be sure to keep the Shift or Ctrl key depressed.
4. From the **Protect** list, select the appropriate service plan from **Subscribe to Plan and Run**.

In DAG, a passive database is protected by default.

The **Subscribe to Plan and Run** dialog appears displaying the progress through the different phases.

Subscribing an Exchange database to a service plan

Select **Subscribe to Plan** when you want to schedule the protection for later. Protection for all databases that are part of the service plan are executed at the scheduled time.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft Exchange**.
2. Click an Exchange Mailbox Server or DAG from the list to display its databases.
3. From this list, select a database to protect.

   Select multiple databases by holding down the Shift or Ctrl keys on your keyboard.
4. From the **Protect** list, select the appropriate service plan from **Subscribe to Plan**.

   In DAG, a passive database is protected by default. To change the protection type with another option, specify it from the **Subscriptions** tab of the service plan.

   The plan is added to the Plans column for the database.

Unsubscribing a database from a service plan

You can unsubscribe an individual database from a service plan.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft Exchange**
2. Select a mailbox server to display the list of Exchange databases.
3. Select the database to remove from a plan.
   - Select the plan to unsubscribe from **Protect** › **Unsubscribe from Plan**.

     Only plans to which the database is subscribed to are in the popup list.
   - To unsubscribe from all service plans, select **Unsubscribe from Plan** › **All**.

Expiring a copy on demand

Expiring a copy removes it from the AppSync database and can free up storage, depending on the replication technology and copy state.

Before you begin

This operation requires the Data Administrator role in AppSync.

Expiring a copy that was made with RecoverPoint does not remove the corresponding bookmark from RecoverPoint itself.

Procedure

1. Select **Copy Management** › **Microsoft Exchange**.

2. Click an Exchange mailbox server to display its databases.
3. Click an Exchange database to display its copies.
4. Select one or more copies to delete.

   You can also perform this action from the Service Plan **Copies** tab.
5. Select **Expire**.

   Verify that you want to expire the copy you selected and any associated copies listed and confirm.

Creating a database copy from the Copies page

Create a copy of a database by subscribing it to an AppSync Exchange service plan from the **Copies** page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft Exchange**.
2. Click a mailbox server instance.
3. From the list of Exchange databases, click the database to view its copies.
4. From the **Create a copy using plan** list, select the appropriate service plan.

   The service plan runs immediately for the database.

Service plan details

A service plan has the following tabs: Settings, Subscriptions, Copies, Events, and for SQL Server plans, Log Backups .

The **Settings** tab shows the name, description, and status (whether enabled or disabled) of the service plan. Apart from these, the different phases of the plan are also part of this tab. Click on appropriate tabs to see information regarding Subscriptions, Copies created by the plan Events generated during the service plan run, and for SQL Servers, Log Backups created by the plan.

Service plan schedule

The schedule of a service plan is set in the **Plan Startup** phase.

The **Startup Type** (scheduled or on demand) determines whether the plan is run manually, or configured to run on a schedule. Options for scheduling when a service plan starts are:

- Specify a recovery point objective (RPO)
  - Set an RPO of 30 minutes or 1, 2, 3, 4, 6, 8, 12, or 24 hours
  - Minutes after the hour are set in 5 minute intervals
  - Default RPO is 24 hours
- Run every day at certain times
  - Select up to two different times during the day
  - Minutes after the hour is in 5 minute intervals
  - There is no default selected

- Run at a certain time on selected days of the week
  - One or more days of the week (up to all seven days) can be selected
  - There is no default day of the week selected. Default time of day is 12:00 AM.
- Run at a certain time on selected days of the month
  - Select one or more days of the month (up to all days)
  - Select one time of day. Available times are at 15 minute intervals.
  - Default is the first day of the month

Control replication storage utilization

When you set up a service plan, set values in the following fields so that you avoid overutilization and depletion of replication storage:

- RPO value in the Plan Startup phase
- Always keep n Copies in the Create copy phase

You should also monitor your storage system with the storage system user interface.

Overriding service plan schedules

You can set individual schedules for databases subscribed to a service plan, overriding the generic recurrence setting.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

You can override only the settings of the recurrence type already selected for the service plan.

Procedure

1. Navigate to **Service Plans** › **Microsoft Exchange** and select one of the plans from the list.
2. From the **Settings** tab, select the **Plan Startup** phase.
3. From the **Plan Startup Defaults** pane on the right, note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Scheduled** is selected as the **Startup Type**.
4. Click the **Plan Startup Overrides** tab.
5. Set individual schedules for selected databases based on your requirement.

   For example, if the recurrence type you selected is **On specified days of the month**, and the rule setting is to **Run at 12:00 AM** on the **1st day of every month**, you can override the time and the day for individual databases.

Application discovery

Before creating the copy, AppSync examines the Exchange Mailbox Server to look for changes such as addition, deletion, renaming, or movement of databases.

There are no user settings associated with this phase and it cannot be disabled.

Application mapping

After discovering the application, AppSync maps it to array storage, and protection services such as RecoverPoint.

There are no user settings associated with this phase and it cannot be disabled.

Pre-copy script

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters on a service plan's **Settings** tab.

The pre-copy script runs according to the schedule set in the **Plan Startup** phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts). You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default.

AppSync does not support running of PowerShell scripts directly. You usually must wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you must set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full pathname to the PowerShell command file in the .bat file:
   `powershell -command C:\PshellCommands.ps1 <nul`
2. Set the PowerShell execution policy so you can run the script. For example, the first line in the .bat file should look like the following for an unrestricted policy:
   `powershell -command set-executionpolicy unrestricted <nul`
3. To ensure correct termination of the PowerShell session, add ‹nul to the end of the line that calls the PowerShell script. The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Create copy

The Create Copy phase creates a copy based on the replication technology specified in the service plan.

This phase specifies the type of Exchange copy to make, whether to ignore Exchange errors in the Application event log, and if database and logs can reside on the same volume.

Review Overview: Service Plan on page 10 for more service plan copy information.

Exchange backup type

AppSync uses VSS to make a consistent online copy at the volume level.

- **Full** creates a copy of the databases in the service plan using VSS, and includes the database files, transaction logs, and checkpoint files. On successful completion of the backup, the logs are truncated.
- **Copy** creates a copy of the databases in the service plan using VSS, which includes the database files, transaction logs, and checkpoint files, as it does using the **Full** option. However, it does not truncate the logs.

- **Differential** copies the entire transaction log volume. A full backup of the selected database must exist or the backup fails. The transaction logs are not truncated on completion of the backup.

Automatic expiration of copies

The automatic expiration value in a service plan's Create Copy phase specifies the maximum desired number of Snap, Clone or Bookmark copies that can exist simultaneously.

When the "Always keep *x* copies" value is reached, older copies are expired to free storage for the next copy in the rotation. Failed copies are not counted. AppSync does not expire the oldest copy until its replacement has been successfully created. For example, if the number of copies to keep is 7, AppSync does not expire the oldest copy until the 8th copy is created.

AppSync does not expire copies under the following circumstances:

- Mounted copies are not expired.
- A copy that contains the only replica of a database will not be expired.

This setting is independent of the VNX pool policy settings in Unisphere for automatic deletion of oldest snapshots. The service plan administrator should work with the storage administrator to ensure that the VNX pool policy settings will enable the support of the specified number of snapshot copies for the application residing in that pool.

Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations.

Note

If this option is not selected, then RecoverPoint copies will accumulate, and will remain until the bookmarks fall off the RecoverPoint appliance.

Exchange event log errors

Exchange logs certain errors in the Application event log when they occur. These errors indicate a possible corruption of the data in the .edb or log files. They can cause copy creation to fail unless you specifically instruct AppSync to ignore them.

AppSync searches the application event log for these errors every time a copy is created. The first time it runs, AppSync searches the entire log. Subsequent runs search since the last successful run. If there are no existing copies, then AppSync searches the entire log when creating the next copy.

In a service plan's Create copy phase, you can configure AppSync to ignore any or all of these errors.

Table 7 Microsoft Exchange event errors

Error	Meaning
-1018	The database tried and failed to verify information about a particular page in the database.
-1019	Similar to a -1018 error but indicates that the accessed page has returned an invalid page number (usually all zeros) rather than an invalid checksum.
-1022	Indicates major hardware problems, particularly disk subsystem problems. If the database engine requests a page from disk but instead receives an error from the I/O subsystem, a -1022 error results.

Table 7 Microsoft Exchange event errors (continued)

Error	Meaning
447	Indicates corruption in the logical database structure. This accompanies a message stating that the information store terminated abnormally.
448	Indicates an inconsistency or corruption in a table in the Microsoft Jet database. This accompanies a message stating that an information store data inconsistency has been detected in a table.

Database and log layout

Exchange supports environments in which the database and logs reside on the same volume when there is more than one copy of the database in a DAG environment. Service plans can be configured to ignore the restriction that prevents databases and logs from residing on the same volume.

When creating copies of Exchange databases, it is a best practice to restrict a service plan from allowing this configuration because having databases and logs on the same volume limits your restore options. However, you can choose whether service plans with this configuration should succeed or not.

This option is set in the Create Copy phase of a service plan.

When selecting this option, you are limited to restoring the database and logs together. Restore overwrites newer log files. To preserve newer log files for use during recovery, copy them to another volume before restore.

Post-copy script

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters in a service plan's **Settings** tab.

The script runs on successful completion of the **Create copy** phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts). You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default.

When AppSync creates copies of application items in a service plan, it may break up the application items and place them in separate groups for protection. This action can be for performance reasons (for example, VSS for Exchange and SQL) or because items in a service plan may be protected by different replication technologies. For example, a service plan may contain some application items that are protected by VNX Snapshots and some by RecoverPoint bookmarks. As a result, application items in these groups are protected independently.

When AppSync calls a post-copy script, it passes the copies which were created in the group by calling the script with -appCopies ‹APP1› ‹APP2›, where APP1 and APP2 are the names of the application items in that grouping.

AppSync does not support running of PowerShell scripts directly. You usually must wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you must set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full pathname to the PowerShell command file in the .bat file:
   `powershell -command C:\PshellCommands.ps1 <nul`

2. Set the PowerShell execution policy so you can run the script. For example, the first line in the .bat file should look like the following for an unrestricted policy:
   `powershell -command set-executionpolicy unrestricted <nul`
3. To ensure correct termination of the PowerShell session, add ‹nul to the end of the line that calls the PowerShell script.

When AppSync runs the post-copy script, it is run for the application items that are part of a group. If there are multiple groups, the post-copy script runs multiple times. When AppSync runs the post-copy script, it passes the list of application items in the replication group as arguments to the script, right after the user arguments. The syntax is:

```
-applicationCopies <ITEM1> <ITEM2> <ITEM3>
```

where ‹ITEMx› is the name of the application item that is being protected.

The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Unmount previous copy

The service plan unmounts a previously mounted copy after creating the new copy. The exception is a copy that was mounted on-demand as opposed to by the service plan; in this case the on-demand mounted copy is not unmounted.

There are no user settings associated with this phase and it can be enabled or disabled.

Mount copy

The Mount copy phase mounts the copy. This phase can be enabled or disabled.

The **Mount Copy Defaults** settings for the mount host value, mount path and mount access attributes (read-only or read-write) depend on the service plan. Other mount settings determine where the Exchange metadata files are copied, the type of copy to mount and the RecoverPoint image access type.

- **Mount on Server**
  Allows you to choose between Windows hosts you have access to and Original Server. If you have chosen to validate the copies, only servers that have the Exchange Management Tools installed are displayed in the drop down. These servers display on the Microsoft Exchange Protection page as "Utility Host".
- **Mount with access**
  Choose the type of access the copy should be mounted with - Read/Write or Read only
- **Mount Path**
  - **Alternate mount path**
    The default mount path, when the mount host is the same as the production host, is *SystemDrive*:\AppSyncMounts*Production_Server_Name*.

    path is represented in the console as %SystemDrive%\AppSyncMounts\% %ProdServerName%%.

    To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). The default path also contains an

AppSync variable (ProdServerName) that is delimited with two percent signs (% %).

The following characters are not valid in the path:

‹ › : " / | ? *

- **Same as original path** This is another option for the mount path. You can select either of the options.

Note

When performing a DAG mount, do not select the mount path as **Same as original path** if the mount host also happens to be a DAG node having a copy of the database that you are mounting.

- **Copy metadata files to**
  By default, the location to copy VSS metadata files is the default path - *SystemDrive*:\AppSyncMounts*Production_Server_Name*.

  The following characters are not valid in the path:

  ‹ › : " / | ? *

  If you are backing up the database to another media, you must backup these metadata files as well.
- **Image access options during RecoverPoint mount**
  RecoverPoint provides a target-side host application the opportunity to write data to the target-side replication volumes, while still keeping track of source changes.
  - **Slow access time, fast image I/O performance (RecoverPoint access mode: Logged Access)**
    Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host.
  - **Fast access time, Fast after roll image I/O performance (RecoverPoint access mode: Virtual Access with Roll)**
    Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing.
  - **Fast access time, Slow image I/O performance (RecoverPoint access mode: Virtual Access)**
    Provides nearly instant access to the image; it is not intended for heavy processing.
  - **Desired Service Level Objective (SLO)**
    Additionally if you are using a VMAX 3 array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.
- **Copy to mount**
  Displayed for service plans that create both a local and remote copy. You can select the type of copy to mount.
- Additionally if you are using a VMAX 3 array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.

Mount host overrides in service plan

Select different mount hosts for multiple Exchange servers subscribed to a service plan.

In the Mount copy phase of a service plan, you can specify the host that the copy should be mounted on along with related mount options. If you have multiple servers as part of a service plan, you may want to host their copies on different hosts. You can specify different mount hosts and other options from the **Mount Copy Overrides** tab of the **Mount copy** phase in a service plan.

Overriding mount hosts in a service plan

If there are multiple registered hosts and they are subscribed to the same plan, you can select a different mount host for each server, overriding the generic mount host settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Follow these steps when you have multiple hosts subscribed to a plan and you want different mounts hosts for their database copies.

Procedure

1. Navigate to **Service Plans** and select one of the plans from the list.
2. From the **Settings** tab, select **Mount copy** phase.

   In the **Mount Copy Defaults** tab, the list of servers include all Exchange servers whose databases are subscribed to this plan. The mount settings display the default settings.
3. To override the default settings, click **Mount Copy Overrides**.
4. Select the server whose mount settings you wish to override and click **Set Overrides**.
5. In the **Override Default Mount Settings** dialog, select options only for those mount settings that you wish to override.

   For example, if you want to mount a copy to a different path, you would select the path from the **Mount Path** list. Fields that do not have a selection retain their default settings.
6. Select **OK** to save your changes.

   A pencil icon appears in the first column of the server's row whose default mount settings you changed.
7. To revert back to default settings for a server, select the server and click **Use Default Settings**.

Validate copy

Exchange management tools run a consistency check in this phase.

By default, databases and logs are checked sequentially. If the databases are not sharing the same LUN and the mount host has sufficient resources to support parallel consistency checks, use the **In parallel** option. Note that there is a limit of 16 parallel checks that Exchange can handle.

If the consistency check completes successfully, AppSync instructs Exchange to truncate the logs so only the changes that are uncommitted to the database remain.

This phase can be enabled or disabled.

Advanced options for consistency check

AppSync offers advanced options that change how Exchange consistency checks are executed. Enabling these features can impact performance.

- **Minimize log checking**

  Choosing this option speeds up the log checking by instructing the consistency checking software to check only those logs that are required to recover the database. Selecting this option improves the performance of the consistency check. If you disable the option, then consistency check will be performed on all of the database's logs.

  This command instructs AppSync to check only a subset of the Exchange logs that are included in the copy. The subset of the logs are actually the logs that are required to recover the database. If your backup window is small, you may find this option useful. However, the copy contains logs that have not been checked for consistency. If you attempt to restore the log volume, you may find that some log files are corrupt or the log sequence is not complete. Before restoring the log volume, you should mount the replica and run `eseutil /k E`*nn* against the log path.

  For maximum protection, clear **Minimize log checking**. For maximum performance, select it.

  You must also set a working directory, which is where the required log files will be copied for checking.

  The **Minimize log checking** option is not available when the consistency method is Differential.

- **Throttle Checking**

  Consistency checks can be paused to slow down the IOs during the check. You can specify the number of IOs after which to pause, and the duration of the pause.

Post-mount script

Specify a post-mount script and parameters from the Post-mount script option in the **Settings** tab of a service plan.

The script runs on successful completion of the mount copy or mount with recovery phase. This script is typically used for backup.

From the **Server** list, select the server on which to run the script. You can optionally run it on a registered host other than the mount host, and enter credentials to run the script as a specific user.

The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on your script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Unmount copy

The final phase in the service plan unmounts the copy. All the mounted databases are shut down as part of this phase.

This phase is disabled if the **Unmount previous copy** phase is enabled. There are no user settings associated with this phase.

Mounting Exchange copies

AppSync can mount a copy on-demand, or as part of a plan.

Copies created on a standalone production Exchange server can be mounted to:

- An alternate host in the same location as the production host.
- An alternate host in a new location. You specify mount option by adding an alternate path to the start of the path.
- The production host in an alternate location.

Copies created in a DAG can be mounted to:

- An alternate host
- A server in another DAG
- Another server in the same DAG

Note

Copies cannot be mounted to the same DAG server on which the copy was created.

Mount and restore limitations

Limitations to mount and restore or Exchange copies appear in the following list:

- When the root drive letter has mount points on it and they are all included in the same plan, mounts and restores are likely to fail. For instance, if the log and system files are on L:\ and the mailbox stores are on L:\SG1DBMP (where SG1DBMP is a mount point), mounts and restores fail.
- In Windows 2012 and later environments, when doing a restore, the data on LUNs is overwritten even if the volume is in use. This action differs from other Windows platforms in which AppSync displays a warning if the LUN is in use. Since restores overwrite everything, be sure that there is no other data on that volume and the volume is not in use.

Mounting an Exchange copy on-demand

You can initiate an on-demand mount of an Exchange copy from a copy or database.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Select **Recover** › **Mount a Copy** in the **Exchange Databases** page.

   Alternatively, from the **Copies** page or **Copies** tab of the service plan, select a copy and click **Mount**.

2. Use the **Copies** or **Service Plan** filters to select the appropriate copy to mount.

   The Copies list is refreshed based on the filters selected.

3. Select the copy to mount.

   For a RecoverPoint copy, you also have the option to select a copy based on a specific time. Click **Select a point in time** to select a copy with a specific time stamp. The time displayed is the console's time. If the console is in a different time zone from the server, specify the time as per the server's time zone to mount the copy.

4. In the **Mount Additional Copies** page, select one or more additional copies to mount.

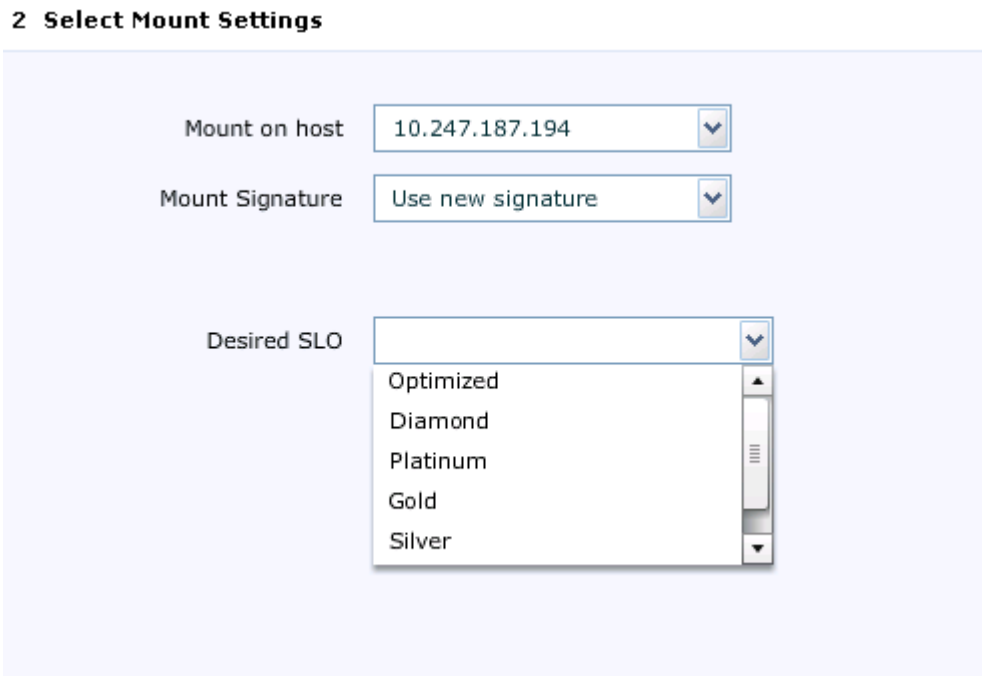
   The copies listed here are of other databases that were protected at the same time and on the same host as the copy you selected in the previous step.

5. In the **Validate Copy** page, select **Yes** to validate the copies and specify validation options. See Mount validation options for details.

6. On the **Mount Options** page, select the mount options.

   - For VMAX 3 arrays (only), you are presented with an SLO drop-down menu. You can select the desired Service Level Objective (SLO) for the mount copy. If there is a storage group for the mount host with the desired SLO. AppSync will add the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host. If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices will be added to the original storage group when the copy is expired. An example of the Desired SLO menu follows:

     Figure 2 For VMAX 3 select Desired SLO

   - **Mount on Server**
     Allows you to choose between Windows hosts you have access to and Original Server. If you have chosen to validate the copies, only servers that have the Exchange Management Tools installed are displayed in the drop down. These servers display on the Microsoft Exchange Protection page as "Utility Host".
   - **Mount with access**
     Choose the type of access the copy should be mounted with - Read/Write or Read only
   - **Mount Path**
     - If you specify non-default mount path, the drive specified for mount can not be a clustered disk.
     - **Alternate mount path**
       The default mount path, when the mount host is the same as the production host, is *SystemDrive*:\AppSyncMounts*Production_Server_Name*.

path is represented in the console as %SystemDrive%\AppSyncMounts\% %ProdServerName%%.

To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). The default path also contains an AppSync variable (ProdServerName) that is delimited with two percent signs (%%).

The following characters are not valid in the path:

‹ › : " / | ? *

- **Same as original path**
  This is another option for the mount path. You can select either of the options.

  Note

  When performing a DAG mount, do not select the mount path as **Same as original path** if the mount host also happens to be a DAG node having a copy of the database that you are mounting.

- **Copy metadata files to**
  By default, the location to copy VSS metadata files is the default path - *SystemDrive*:\AppSyncMounts*Production_Server_Name*.

  The following characters are not valid in the path:

  ‹ › : " / | ? *

  If you are backing up the database to another media, you must backup these metadata files as well.

- **Image access options during RecoverPoint mount**
  RecoverPoint provides a target-side host application the opportunity to write data to the target-side replication volumes, while still keeping track of source changes.

  - **Slow access time, fast image I/O performance (RecoverPoint access mode: Logged Access)**
    Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host.
  - **Fast access time, Fast after roll image I/O performance (RecoverPoint access mode: Virtual Access with Roll)**
    Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing.
  - **Fast access time, Slow image I/O performance (RecoverPoint access mode: Virtual Access)**
    Provides nearly instant access to the image; it is not intended for heavy processing.

7. In the **Configure AppSync Exchange Interface Service** page, provide the credentials to configure the service on the mount server.

   This page is displayed only if you chose to validate the copy if the service is not configured.

8. Review the **Summary** and click **Finish** to mount the copy.
9. In the **Results** page, select **View Details** to see progress of the different phases that are part of mounting a copy.

The last phase completed is displayed at the bottom of the list.

Validation options for a mount copy

Validation for differential backup copies is not supported.

Validate database and logs
When you create a replica of one or more Microsoft Exchange databases, you should mount the replica and test it for consistency. If you choose to automatically mount the replica to an alternate host once it has been created, you should run a consistency check on the replica. The options to validate are:

- Sequentially — Run tests on one database at a time in order (serial mode). Select this option if you have several Exchange databases on one LUN.
- In Parallel — Run tests on several databases simultaneously (parallel mode).

Minimize log checking
By selecting Minimize log checking, AppSync checks a subset of the Exchange logs that are included in the replica. If your backup window is small, you may find this option useful. However, the replica may contain logs that have not been checked for consistency.

For maximum protection, clear Minimize log checking. For maximum performance, select it.

Working directory — This field allows you to specify the directory to which the relevant log files will be moved in order to run the check, since a consistency check can only be run on all logs in a single directory.

Throttle Validation
Select this to throttle the I/Os during a consistency check. This option is for advanced users and typically should not be selected unless you are working with EMC Support to resolve an issue related to I/O throughput. Typically, the throttling option is not required.

If you choose to throttle I/Os, you have the following two options.

- Pause after I/O count of: 100 — This option allows you to choose how many I/Os can occur between pauses. You can choose any value between 100 and 10,000 I/Os.
- Duration of pause (in milliseconds): 1000 — You can specify the duration of the pause in milliseconds. 1000 milliseconds = 1 second. If this option is not available, the pause will be one second long.)

Unmounting an Exchange copy

When you select a copy to unmount, other copies that were mounted along with the selected copy will also be unmounted.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- If the copy is mounted due to performing an item level restore, verify that all work within the ItemPoint application is complete prior to unmounting the copy.

You can unmount a copy only from a list of copies made for a database.

Procedure

1. Navigate to the **Copies** page from the **Data Protection** or **Service Plan** pages:
   - **Copy Management** › **Microsoft Exchange** › select the Exchange Mailbox Server that hosts the database, then select the database with the copy to unmount.

- **Service Plans** › **Microsoft Exchange**› select a service plan, then select the **Copies** tab.

2. From the list of copies, select the copy and click **Unmount**.

   The **Unmount Confirmation** dialog displays copies of other databases that were mounted along with the selected copy to be unmounted.

3. Click **Yes** to confirm the unmount of all the copies shown in the dialog.

   The **Unmount** window displays the progress of the unmount operation. All copies associated with the selected copy will be unmounted.

Overview of Exchange copy restore

Learn about Exchange restore features along with associated storage copy levels.

With AppSync you can restore the following objects:

- A database with its logs.
- A database `.edb` file.
- Only the logs for a database.
- An active or passive database (in conjunction with any one of the three points already mentioned), if the server is a member of a DAG (Database Availability Group).

AppSync restores VNX/VMAX copies at the LUN level and VNXe copies at the LUN group level. In a RecoverPoint environment, restore is at the consistency group level.

Affected entities during restore

When restoring from a copy, you may be prompted to restore items in addition to the ones you selected.

An affected entity is data that resides on your production host that unintentionally becomes part of a replica because of its proximity to the data you intend to protect. You can prevent affected entity situations by properly planning your data layout based on replica granularity. The granularity of a replica depends upon the environment.

If there are *affected entities* in your underlying storage configuration, the Restore Wizard notifies you of these items. The following scenarios produce *affected entities* that require you to acknowledge that additional items will be restored:

- For RecoverPoint, if the databases are in the same consistency group they become *affected entities* when the other database is protected.
- For VNXe, if the databases are in the same LUN group, they become affected entities when another database in the group is protected.
- For VMAX, VNX, VNXe, or XtremIO, if the databases are on the same LUN they become *affected entities* when the other database is protected.
- For VMware virtual disks, since restore involves a datastore, restore of all applications residing on the same datastore (virtual disks on the same datastore) are also affected entities.

If the affected entity was protected along with the database selected for restore, AppSync restores it. Any other database that was not protected but is an affected entity is overwritten. AppSync calculates affected entities for the consistency groups, LUN groups or LUNs of the database that is selected for restore. If the affected databases partially reside on other consistency groups, LUN groups or LUNs, AppSync does not calculate affected entities on those consistency groups. LUN groups or LUNs.

Affected entities are calculated on the basis of restore granularity. If both data and logs are selected for restore, then affected entities are calculated for all the consistency

groups, LUN groups, or LUNs on which the database resides. If only data or only log restore is selected, then the affected entities are only calculated for the selected component's consistency group, LUN Group, or LUN only.

If the database data and log components reside on the same consistency group, LUN group, or LUN, the option to restore only logs or restore only data is not available. You have the option only to restore data and logs. The only exception to this scenario is when you perform a differential copy restore.

Since restore involves a datastore with VMware virtual disks, restore of all applications residing on the same datastore (virtual disks on the same datastore) are also affected entities.

Restoring from an Exchange copy

You can perform a restore of an Exchange copy from a copy or a database.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Select **Recover** › **Restore** › **Databases and logs** from the action buttons at the bottom of the page.
2. Select the copy to restore, and click **Next**.
3. From the **Select Options** page, select the appropriate restore options and click **Next**.

Option	Description
Both data and logs	Available when restoring from full and copy backup.
Data	Available when restoring from full and copy backup.
Logs	Available when restoring from full, copy, and differential backup.
Recover and mount databases after restore	Leave this selected. If not selected, you must recover the database manually.
Allow AppSync to activate databases	Available for DAG only. If selected, the database copy is activated on the server prior to restoring it. **Note** Exchange restores only to the active copy and AppSync restores to the server that created the copy.

   The **Restore Warnings** page is displayed. This page may be displayed if the selected copy has affected entities.

4. Read the warning messages for the affected databases.

   In case of Exchange 2013, AppSync attempts to determine if the selected database or any of the affected entities contain the public folder primary hierarchy mailbox. If a match is found, you see an error message that the restore operation cannot continue.

   To determine where the public folder primary hierarchy mailbox resides, AppSync requires your user profile to have an additional Exchange role - the View-only Organization role. If your account does not have this role, you see a warning message.

5. Select the checkbox to indicate your agreement to restore other entities along with the selected copy.

   You must manually unmount the databases that will be overwritten.

6. Review the **Summary** page and click **Finish** to restore the copy.
7. In the **Results** page, click **View Details** to see progress of the different phases that are part of restoring a copy.

   The last phase completed is displayed at the bottom of the list.

Recovering an Exchange database manually

Perform a manual recovery when you have not selected the **Recover and mount the databases after restore** option in the Restore wizard.

Before you begin

When you are recovering just a database file, verify that the transaction log files needed for recovery are present. An unbroken sequence is required. To determine the minimum required range of logs, run the following command against each database after the restore and before running recovery: `ESEUTIL /mh <database name>`. Look for the Log Required information in the ESEUTIL output.

If the database is the active copy, it must first be unmounted in order to run the ESEUTIL command successfully.

Procedure

1. Delete the checkpoint file (Enn.chk).

   This is optional.

2. Delete the restore.env file (EnnRESTORE.env).
3. Recover the databases manually in soft recovery mode using the `ESEUTIL` command.

   ```
   eseutil /r E<nn> /l <logpath> /s <chkpt file path> /d
   <database path>
   ```

4. Use Exchange Management Console to mount all the restored databases.

Restoring a standalone Exchange database on XtremIO

This procedure is applicable only for XtremIO 3.x. XtremIO 4.0 and later has a formal restore using the Restore Wizard.

Review and follow these steps to restore an XtremIOSnap copy of a standalone Exchange database that resides on an XtremIO 3.x array.

The mounted copy is validated before manual restore (Mount with Validation phase) with this procedure.

Note

Restrictions: Renamed and deleted databases cannot be restored. Restore of data (only) or logs (only) is not supported.

Procedure

1. Suspend AppSync schedules that affect the copy being restored.
2. To restore the copy to the production host, use the AppSync console to mount the copy. Ensure that you select the Validation phase.

a. Ensure a read/write mount.

b. Mount with default path or any user-defined path

3. Stop the production application, using the Exchange Management Console, **Dismount Production database**.
4. Dismount the Exchange database from the Exchange Management Console.
5. Remove drive letters for production database drives.
6. Assign production database drive letters to mounted database (data and log drives respectively), and then verify data and log paths.
7. In the Exchange Management Console, mount the production database.
8. To remove copies from the AppSync database, click **Remove** on the copies page of the AppSync console,

   The Remove function is the similar to Expire, but Remove does not delete the copies from storage.
9. On the AppSync console, move mounted snapshots to the production folder in the XtremIO array.
10. Test restored contents to confirm successful restore.
11. Remove the production volumes on XtremIO with the AppSync console.

    Snapshots of deleted volumes become production volumes.
12. If data and log drives were vDisks, perform VMware Virtual Center re-discovery in AppSync.
13. To create a fresh copy of restored data, run the service plan.
14. Resume any suspended schedules.
15. Optionally, clean-up or delete production devices from production host and remove AppSync mount points that are created during the mount-phase.

Restoring an Exchange database DAG on XtremIO

This procedure is applicable only for XtremIO 3.x. XtremIO 4.0 and later has a formal restore using the Restore button and the Restore Wizard.

These steps show you how to restore an XtremIOSnap copy of an Exchange database with DAG that resides on an XtremIO 3.x array.

The mounted copy is validated before manual restore (Mount with Validation phase) with this procedure.

Note

Restrictions: Renamed and deleted databases cannot be restored. Restore of data (only) or logs (only) is not supported.

Procedure

1. Suspend AppSync schedules that affect the copy being restored.
2. To restore the copy to the production host, use the AppSync console to mount the copy. Ensure that you select the Validation phase.

   a. Ensure a read/write mount.

   b. Mount with default path or any user-defined path (DAG member on which the copy was protected).

3. Stop the production application using the Exchange Management Console, suspend passive copies and then dismount the Production[Active] database.
4. Remove drive letters for production database drives.
5. Assign production database drive letters to mounted database (data and log drives respectively), and then verify data and log paths.
6. In the Exchange Management Console, mount the production database.
7. To update passive copies, run the following command for all DAG members : `Update-MailboxDatabaseCopy -Identity <Database Name>\<DAG member> -SourceServer <DAG Member>`
8. On the AppSync console, click **Remove** on the AppSync copies page to remove copies from the AppSync database.

   The Remove function works like Expire, but Remove does not delete the copies from storage.
9. On the AppSync console, move mounted snapshots to the production folder in the XtremIO array.
10. Test restored contents to confirm successful restore.
11. Remove the production volumes on XtremIO with the AppSync console.

    Snapshots of deleted volumes become production volumes.
12. If data and log drives were vDisks, perform VMware Virtual Center re-discovery with AppSync.
13. To create a fresh copy of restored data, run the service plan.
14. Resume suspended schedules.
15. Optionally, clean-up or delete production devices from production host and remove AppSync mount points that are created during the mount-phase.

Partial restore

In a partial restore, you restore data alone or restore data and then restore the logs separately.

Before you perform a partial restore, ensure that the database layout fulfills some conditions.

Partial restore considerations

In a RecoverPoint environment, the granularity of restore is at the consistency group level. When you restore a database from a bookmark, any bookmarks that are newer than the bookmark being restored are deleted. The corresponding application copies are also deleted. The following best practices are recommended:

- The database and logs must reside in different consistency groups.
  If you have data and logs for an Exchange database in the same consistency group, partial restore is not supported.
- The logs should be restored from a newer Differential backup copy. AppSync does not support restoring just the logs from a Full or Copy backup in a RecoverPoint environment.

In a VMAX/VNX environment, the database and logs must reside on different LUNs.

Restore data

Restore data from a Full or Copy backup. You can restore data only to preserve the logs that are on the production host.

In the Restore wizard, restore data from the most recent copy and select the **Recover and mount the databases after restore** option.

Restore logs

Restore data from a Full or Copy backup and then restore the logs from a later copy to make the copy current.

Restoring a copy from the logs is a two-step process. Run the Restore wizard and select a full backup copy to restore only data. Do not opt to **Recover and mount the databases after restore** in this run.

Run the Restore wizard again and select a backup copy (a differential backup in case of RecoverPoint) to restore only the logs. This time, select the **Recover and mount the databases after restore** option. This copy must be later than the backup copy that you selected during the first run.

Note

If the restore operation includes restoring logs, the restore overwrites any logs that are created since the copy was created. Therefore, after the restore, the database reflects the point in time when the copy was created. If you want to preserve logs that are created since the copy, restore only the databases, preventing AppSync from restoring older logs over the newer logs. You can also make a copy of the current log files on another volume.

Restoring logs from crash-consistent (APiT) copy

Restore an any point in time (APiT) copy using logs.

Before you begin

This is applicable only in a RecoverPoint environment.

Note

Restoring logs from a crash-consistent copy is not a recommended practice as the backup is not taken with the Exchange writer. However, the option can be used to minimize data loss when application consistent copies for that time window are not available to restore from.

Procedure

1. Restore a database from an application-consistent copy without recovering it.
2. Mount a copy from a newer point in time.
3. Copy the newer log files to the production log volume.
4. Use `ESEUTIL /k Enn` (Enn is the log prefix for the database) to check the logs, then recover and mount the database.

Restoring a deleted Exchange database

AppSync can restore a database even if it is deleted from Exchange in standalone and DAG environments.

Before you begin

- If you deleted the database files and created an empty database, dismount the database and delete its files. The database that you are restoring should not have data and log files at the original location where they were when the empty database was created. The log file signatures will not match those in the AppSync copy and the restore will fail.
- If you completely remove the database and recreate it, the database name and its file path and names should be exactly the same as those in your AppSync copy. If you do not recreate the deleted database, AppSync recreates it.
- In a DAG environment:
  - There should be no active or passive copies of the deleted DAG database.
  - AppSync recreates and restores only the active database copy to the server that created the AppSync copy. After the database has been restored and recovered, you can recreate the DAG passive copies.

If you have not selected the **Recover and mount the databases after restore** option in the Restore wizard, perform the following manual steps to recover the database.

Procedure

1. Copy the required logs from `_restoredLogs` directory to the directory where the current logs reside.
2. If the log file prefix changed, rename the required log files to use the new prefix.
3. Delete the `E<nn>restore.env file`.
4. Recover the databases manually in soft recovery mode using the `ESEUTIL` command.

   ```
   eseutil /r E<nn> /l <logpath> /s <chkpt file path> /d
   <database path>
   ```

5. Delete the `_restoredLogs` directory that should be empty after the database is recovered.

Item level restore

AppSync can restore individual Exchange 2010 and 2013 mailboxes and messages when EMC ItemPoint™ for Microsoft® Exchange™ Server is installed.

The following software must be installed and running on the mount host where you want to perform item level restores:

- AppSync host plug-in
- EMC ItemPoint for Microsoft Exchange Server
- Microsoft Exchange MAPI client
- Microsoft Outlook 32-bit client

Refer to the ItemPoint documentation on the EMC Support website for further information on ItemPoint.

Restoring individual mailboxes and mailbox items

Use ItemPoint to restore individual Exchange mailboxes and mailbox items.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Logon to the mount host as the user that will be running ItemPoint. You must be a local administrator.
2. Select **Recover** › **Restore** › **Individual items** on a **Databases** or **Copies** page.
3. From the **Select Copy** page, select a copy from the list.

   If the copy was made with RecoverPoint, you can **Add a desired point in time** and select that copy. Specify a date and time (and DAG server if appropriate) when you select this option. (If you started the wizard from a copy, you do not perform this step.)
4. If the copy is unmounted you will then select mount options. From the **Select Mount Options** page, select the mount host and the mount path (original path or default).
5. From the **Item Level Restore Settings** page, enter user name and password credentials to access the item level restore wizard, and select a temporary directory.

   The temporary directory is used by ItemPoint to store files used to recover data. These files may require disk space equal to the size of the .log files. Use the user credentials discussed in Step 1.

   This operation requires the Microsoft Exchange MAPI client and Outlook 32-bit client. For additional details on the required Exchange roles and permissions for the account used to access ItemPoint, refer to the EMC ItemPoint for Microsoft Exchange Server documentation.
6. From the **Summary** page, confirm your settings and select **Finish** to launch EMC ItemPoint for Microsoft Exchange Server.

After you finish

- After you finish, use ItemPoint to restore mailbox items. For more information about using EMC ItemPoint for Microsoft Exchange Server, refer to the EMC ItemPoint for Microsoft Exchange Server documentation.

Note

Do not unmount the copy that is being restored using Item Point until the entire process is completed within Item Point.

Troubleshooting the EMC AppSync Exchange Interface service

Troubleshooting tips follow:

Is a reboot required?

If you are installing the AppSync host plug-in for the first time, you may need to reboot your Exchange server after the install completes. In some environments, the install of the Visual C++ 2010 runtimes require a reboot. In prior releases of AppSync, the install would reboot automatically without warning. The automatic reboots have been removed with

AppSync 2.0 and above. To verify if a reboot is required, look in `Windows\temp\appsync_host_plugin_setup.log` for the following:

```
 >: "C:\Program Files\EMC\AppSync Host
Plug-in\msredist\vcredist-10.0.40219.1-x64.exe" /q
Command.run(): starting stdout monitor...
Command.run(): starting stderr monitor...
Command.complete(): waiting for process to complete.
Command.complete(): process completed with exit
code: 3010
```

The exit code of 3010 indicates that a reboot is required.

Does the user account have the correct rights?

If the EMC AppSync Exchange Interface service fails to register properly, check the `ExchangeInterfaceInstall.log` file in the AppSync host plug-in\logs directory. A common problem is that the user account for running the service was not granted the `Log on as a batch job` permission.

If AppSync fails to discover databases, verify the EMC AppSync Exchange Interface service user account has been granted the correct Exchange permissions.

How to manually register the service.

1. Grant the user account that will run the EMC AppSync Exchange Interface service `Log on as a batch job` and `Log on as a service` user rights.
2. Open a command prompt and navigate to the directory where the AppSync Host Plug-in is installed. The default location is `C:\Program Files\EMC\AppSync Host Plug-in`.
3. Run the following command to register the service and the DCOM component: `awExchangeInterface /service /user <"domain\username"> /password <"password"> /nopriv` For example: `awExchangeInterface /service /user mydomain /appsyncexchuser /password mYp@55W0rd`.
4. To configure the password for the DCOM component, run `DCOMCNFG`.
5. Expand **Component Services › Computers › My Computer › DCOM Config**.
6. Right click on **EMC AppSync Exchange Interface** and select **Properties**.
7. Click on the `Identity` tab.
8. Select **This user** and enter the user account and password from step 3.
9. Click OK.
10. Verify that you can start the EMC AppSync Exchange Interface service by running: `net start appsyncexchangeinterface`.
11. Use the AppSync console to rediscover the server. Go to **Settings › Servers**, select the server, and then click **Rediscover**.
12. Discover the Exchange mailbox databases. Go to **Copy Management › Exchange** and click on the Exchange server. You may have to re-enter the credentials.

What to do if the service is partially registered?

If the rights and permissions are not granted properly to the user account, or if conflicting software is installed, the EMC AppSync Exchange Interface service will not register correctly. You may need to do a manual cleanup. Follow these steps:

1. Open a command prompt and navigate to the directory where the AppSync host plug-in is installed. The default location is `C:\Program Files\EMC\AppSync Host Plug-in`.
2. Run the following command to remove the service and delete the DCOM component: `awExchangeInterface /unregserver`
3. Using the Services console (service.msc), verify that the EMC AppSync Exchange Interface service is removed. If it persists, run: `sc delete AppSyncExchangeInterface`
4. Using the Component Services console (DCOMCNFG), verify that the EMC AppSync Exchange Interface DCOM component was removed. **Expand Component Services › Computers › My Computer › DCOM Config**.
5. If the component persists, click **DCOM Config**, then in the center pane, click **EMC AppSync Exchange Interface**, and then click **Delete**.

CHAPTER 6

Protect SQL Server

This chapter includes the following topics:

Overview of SQL Server support

Use AppSync to create and manage application-consistent copies of Microsoft SQL Server databases.

AppSync support for Microsoft SQL applications includes:

- AlwaysOn Availability Group support.
- Dynamic discovery of user databases during service plan run.
- Support for databases on physical hosts, RDMs, and virtual disks on virtual hosts.

  Note

  AppSync only supports RDMs in physical compatibility mode. There is no support for RDMs in virtual mode.

- Protection for standalone and clustered production SQL Server instances.
- Mount on a standalone server or cluster nodes of alternate cluster or production cluster as non-clustered resource. Mount with recovery on a non-clustered instance.

Support for Repurposing SQL server database copies.

SQL Server prerequisites

Verify that the SQL Server configuration meets the prerequisites that are listed here. The *AppSync Support Matrix* on https://elabnavigator.emc.com/eln/extendedSupport is the authoritative source of information on supported software and platforms.

- SQL Server database and its transaction logs must be on disks in the same storage array.
- The SQL Server database must be online during replication.
- Full-text catalogs that are associated with a file group are included as part of a replica of that file group. If the full-text catalogs are not located on supported storage, protection fails. When using full-text catalogs, ensure that the storage device where the catalog is located does not include data that is not related to the database.
- If you want to recover databases from the mounted copy, the mount host must have an installed SQL Server. It is recommended to use the same version of SQL Server on the production and mount hosts.
- In Hyper-V environments, AppSync requires the storage for SQL database and log files to be on NPIV Fibre devices, iSCSI direct attached devices, or SCSI pass-through devices. SCSI Command Descriptor Block (CDB) filtering must be turned off in the parent partition. It is turned on by default. For SQL Server cluster, AppSync requires storage to be on NPIV Fibre devices or iSCSI direct attached devices.
- System databases are not supported.
- SQL Server database snapshots are not discovered.
- Creating a copy of a database mirror is not supported. Trying to do so results in an error that the database is not in a valid state.

SQL Server supported configurations

AppSync provides support for the SQL configurations listed here.

- Multiple SQL Server databases can exist on the same volume, or across multiple volumes. However, it is best practice to not mix databases from more than one SQL Server instance on a volume.
- Multiple SQL Server instances can coexist on the same host.

Support for SQL Server on virtual disks

You can protect, mount and restore SQL Server standalone and clustered databases residing on VMware virtual disks.

During protection:

- For successful mapping, the Virtual Center must be added to the AppSync server and discovery must be performed.
- For successful protection, log files and database files must reside on virtual disks. There cannot be a combination of physical and virtual storage.
- Protection of SQL Server databases across virtual machines sharing the same datastore is not supported.
- When restoring SQL Server clustered databases, you must add all the owner nodes of the SQL Server clustered instance to AppSync.

Required permissions and rights

Users require certain permissions and rights to protect databases in a SQL Server environment. The user account must be configured to use either SQL Server authentication or Windows authentication.

The Windows user account can either be a member of the local Administrators group or a non-Administrator account with the restrictions outlined next.

In SQL Server 2012, the default virtual account used in the service startup account of the database engine does not have the requisite file system permissions for accessing the mounted or restored database files. Therefore, recovery of SQL databases may fail. To overcome this, you must change the service startup account for the SQL Server database engine to use a domain user account with appropriate privileges and permissions.

Setting up permissions for a domain account that does not have local administrator privileges

Additional setup is required if you need to use a domain account that does not have local administrator privileges.

Procedure

1. Create a Windows domain user (for example, sqluser) and make it part of the Domain Users group.
2. In SQL Server Management Studio, create a new login, using the newly created domain account and select Windows authentication.
3. In the **General** page, select **master** as the default database.
4. In the **Server Roles** page, select **sysadmin** and **public**.
5. In the **User Mapping** page, set the database role membership to **public**.
6. Add the user to each SQL Server instance on which this user needs access:

a. On the domain controller: On the hosts added to the domain: **Start** › **Programs** › **Administrative Tools** › **Domain Controller Security Policy**

   On the hosts added to the domain: **Start** › **Programs** › **Administrative Tools** › **Local Security Policy**

b. Access security settings and allow login locally (**Security Settings** › **Local Policies** › **User Rights Assignment** › **Allow log on locally**)

c. Add the user (the example is sqluser) you created earlier.

7. Log in to the domain controller machine for each host added to that domain that uses AppSync and set the Security policy.
8. Grant this user read and write permissions on the directory where the AppSync plug-in is installed (typically `C:\Program Files\EMC\AppSync Host Plug-in`).
9. Use this user from AppSync when you configure protection or perform other actions that require access to SQL Server.
10. At the time of restore, if you select the option to back up the transaction logs to a file, the user must have rights to the target directory.

Setting permissions for a local, non-administrator user

A user account that does not have local administrator privileges needs certain permissions before it can be used to access SQL Server from AppSync.

Procedure

1. Create a Windows user and make it part of the Users group.
2. In SQL Server Management Studio, create a new login, using the newly created account. For the authentication type, select Windows authentication.
3. In the **Server Roles** page, select **sysadmin** and **public**.
4. In the **User Mapping** page, set the database role membership to **public**.
5. Add the user to each SQL Server instance on which this user needs access:

   a. On the host running the plug-in, set the security policy. On the domain controller, run **Start** › **Programs** › **Administrative Tools** › **Local Security Policy**.

      On the hosts added to the domain: **Start** › **Programs** › **Tools** › **Local Security Policy**.

   b. Access security settings and allow login locally (**Security Settings** › **Local Policies** › **User Rights Assignment** › **Allow log on locally**).

   c. Add the user (the example is sqluser) you created earlier.

6. Grant this user read and write permissions on the folder where the AppSync plug-in is installed.
7. If you select the restore option to back up the transaction logs to a file, the user must have rights to the target directory.

Update login credentials for a SQL Server instance

If the credentials for a SQL Server instance have changed, you need to update them in AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync. In addition, you should know the new credentials for the SQL Server instance.

Procedure

1. Select **Copy Management**.
2. Select **Microsoft SQL Server**.
3. Select an instance.
4. Click **Connection Settings** from the row of buttons below.
5. Enter the SQL Server credentials.

   The credentials can be a Windows user or a SQL user with required privileges.

Support for AlwaysOn Availability Groups

The Availability Groups can be part of clustered and non-clustered SQL Server instances installed on AlwaysOn Failover clusters.

AppSync supports Full or Copy backups of primary databases and Copy backups of secondary databases. The **Auto Switch to Copy** option in the SQL Server service plan's **Create copy** phase allows you to switch from **Full** to **Copy** for secondary databases.

Special considerations when you are using AlwaysOn Availability Groups:

- To protect secondary databases, they must be read-only. The `Readable Secondary` option in the SQL Server Management Studio must be set to `Yes`; `Read-intent only` is not supported.
- Do not use the original path when mounting an AppSync copy to a node in the same cluster if that node hosts a copy of the database.
- It is recommended to protect replicas in the Synchronous-commit mode.
- The considerations for working with SQL Server in a cluster also apply to Availability Groups. See Considerations for SQL in a cluster on page 86.
- Multi-subnets are supported for AlwaysOn Availability Groups as long as none of the database copies belong to a clustered SQL Server instance.

SQL Server transaction log backup

AppSync 2.1 and above supports SQL Server transaction log backup. Get key considerations as well as restrictions before implementing your backups.

Every SQL Server database has a transaction log. Write the log backups to EMC storage systems that are supported by AppSync so you can create copies of the log backup volume. If you back up logs for databases in a failover cluster environment, use shared storage or a network share so the log backups are written to the same location.

You can use transaction log backups during recovery of a production database or when making a copy of a production database. Depending on the database recovery model, the transaction log can become full. To prevent the accumulation of logs, regularly run transaction log backups with truncation enabled.

AppSync can backup transaction logs in AlwaysOn Availability Group (AAG) environments. It can back up primary or secondary database copies. If truncation is enabled, to initiate truncation, back up either the primary or secondary database transaction log.

Transaction log backups are supported using only streaming back up; they are not supported using VSS hardware snapshot technology. You can use AppSync to back up transaction logs to a file. The file can be written to a local volume or network share using a UNC path.

Restrictions

- To back up a transaction log, the database recovery model must be either “Full” or “Bulk-logged.” AppSync skips backing up the log for any database with the simple recovery model.
- To create any log backups with log truncation, first create at least one full database backup.
- To truncate transaction logs, AppSync must have a Full database backup copy.
- Subscribe a database to only one service plan with log backup enabled.
- To truncate logs in an AAG environment, subscribe only one copy of a database to a service plan that is configured for Full database backups and transaction log backups with log truncation.
- To back up transaction logs for databases that belong to an availability group, alter the schedule so that different copies of the database are not backed up at the same time.

Related topics

- Configure SQL Server transaction log backup on page 78
- Run log backup on demand on page 81
- View log backups for a service plan on page 82
- View log backup list for a single database on page 84

Configure SQL Server transaction log backup

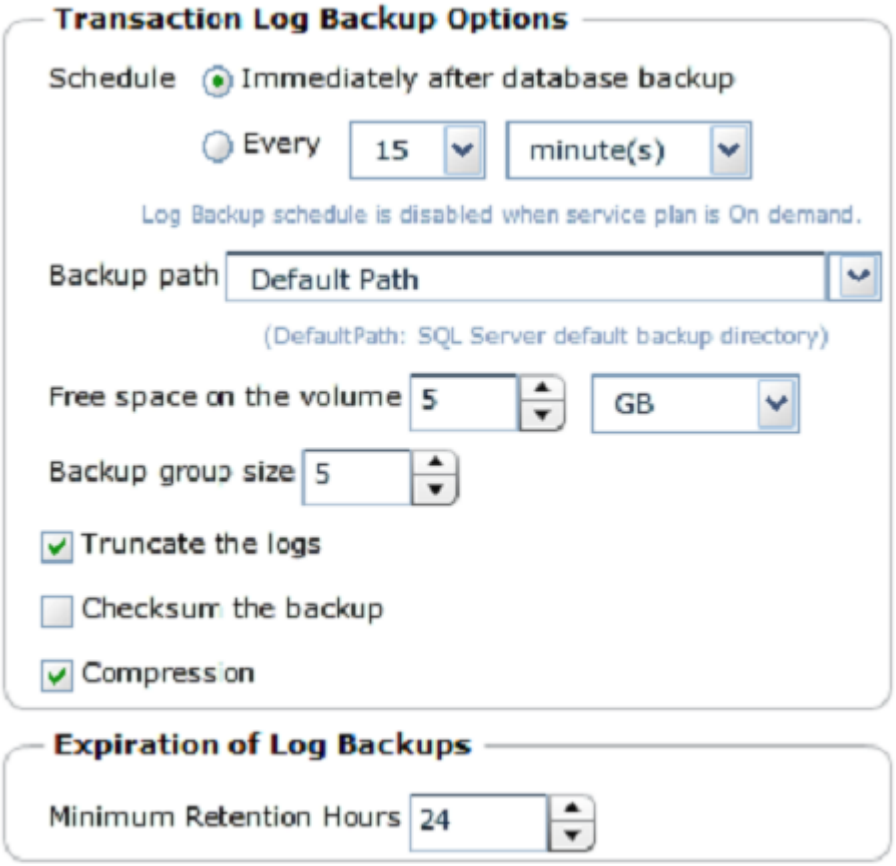
Learn how to enable transaction log backups for an SQL Server service plan, by selecting the **Enable log backup** checkbox on the Create Copy options page of the AppSync console.

Before you begin

Verify that the user account you select for backups has full control of the directory. This account is the user account that you entered when discovering databases. Also verify that the account configured for the SQL Server Database Engine Service of the SQL Server instance being protected has full control of the backup directory.

After you select this checkbox, the **Transaction Log Backup Options** dialog box is enabled where you can customize when and how to run log backups and where to write the log backup files. Transaction log backups run sequentially.

Figure 3 Transaction Log Backup Options dialog box



Procedure

1. Use the **Schedule** field to set log backup runs.

   You can select to run the transaction log backup once, immediately after a database backup is run, or you can select to schedule log backups. You can set log backup schedules to run every 15 or 30 minutes or every 1 to 24 hours. If you set a service plan to run on demand, you disable the log backup schedule.

   When you schedule log backups to run at a specified interval, the service plan will have two schedules associated with it: one for database backups and one for log backups. The log backup is referred to as the alternate schedule. Log backups run between database backups using the alternate schedule.

2. Edit the **Backup path** field to set the location where AppSync writes log backup files.

   Default path uses the SQL Server instance default backup directory. You can also enter a path on any volume on the server or the UNC path of a network share.

   AppSync creates the directory if it does not exist. It creates a subdirectory using the name of the SQL Server instance. The log backup file names have the following format: `EMC_AppSync_databasename_timestamp.trn`, for example, `EMC_AppSync_AdventureWorks_2014_10_18_15_38_32.trn`

3. Use the **Free space on volume** field to set a value to verify the amount of free space on the volume before AppSync begins a transaction log backup.

   If not enough free space is available, an alert is generated and the log backup fails.

4. Use the **Backup group size** field to control the number of parallel log backups for an SQL Server instance. The default value is 5, (AppSync runs log backups in groups of five).

   For example, if you subscribe 15 databases from the same SQL Server instance to a service plan, three log backups will run in parallel. Transaction log backups run sequentially.

5. Select or clear the **Truncate the logs** field when you create Full database backups.

   This field is checked by default when you select Full backup type, and it is disabled when you select Copy . To protect secondary databases, truncate logs, select **Auto switch to Copy** and **Truncate the logs**.

6. To perform a checksum on the log backup, select the **Checksum the backup** field.
7. Set **Minimum Retention Hours** option to control when transaction log backup files are deleted.

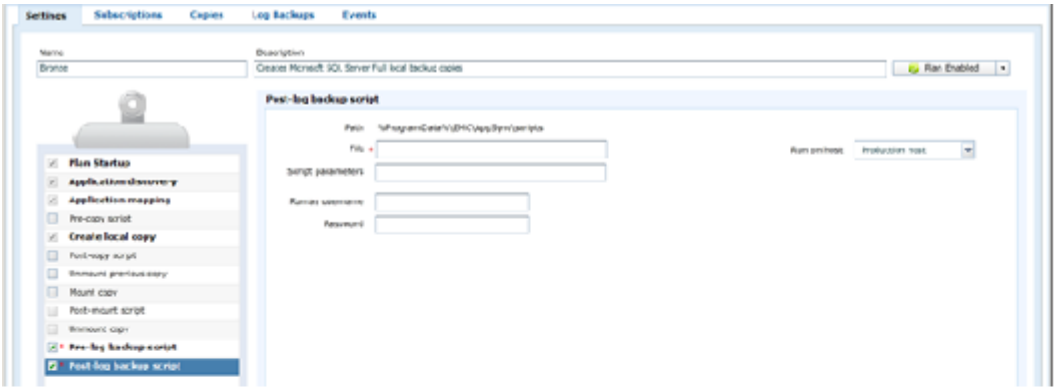
   Transaction log backup expiration is done when no older database backups exist. AppSync deletes the log backup files and the log backup information contained in the AppSync database. The default setting is 24 hours which means that AppSync will not expire any log backup before it is a minimum of 24 hours old. The valid range is 0 to 10,000 hours.

Configure log backup scripts

You can run scripts before and after log backups by enabling the pre- and post- log backup scripts.

The pre-log backup script runs on the production host. The post-log backup script can run on the production host or the mount host (if mount is enabled), or you can specify a server. The server must have the AppSync host plug-in installed.

Figure 4 Configure log backup scripts



Run log backup on demand

You can schedule and run SQL Server log backups, or you can run log backups on demand.

Before you begin

To run log backups, make sure you check the service plan's **Enable Log Backup** option.

You can run a log backup on demand for an entire service plan, or run a log backup on demand for a single database instance.

Procedure

1. To run a log backups on demand for an entire service plan, go to **Service Plans › Microsoft SQL Server**, select the desired service plan enabling the **Run Log Backups** button, and then click **Run Log Backups** to run the backup for the entire service plan.
2. To run a log backup for a single database go to **Copy Management › Microsoft SQL Server**, select an SQL Server instance, select the desired database, and then select the **Log Backups** tab. Finally, select the appropriate service plan from the **Create log backup using plan** list to run the log backup.

View log backups for a service plan

The list of SQL Server log backups can be viewed from the Service Plan Log Backups tab or from the Database Log Backups tab.

Before you begin

This operation requires the Data Administrator role in AppSync.

The list of copies can be filtered by time of creation, and by service plan. In the Service Plan Copies tab, you can also filter by instance.

Procedure

1. To view the list of all log backups for a service plan, navigate to **Service Plans** › **Microsoft SQL Server**.
2. Select a service plan.
3. Click the **Log Backups** tab.

Results

You can now view the log backup list for the service plan. The following table describes details about the log backup:

Table 8 Service Plan log backup details

Column	Description
Status	• Green: successful • Yellow: some log backups completed with errors when the service plan ran. • Red: failed
Instance	SQL Server instance name
Database	SQL Server database name
Name	Name of the log backup copy. The copy is named with the time at which it was made.
Service Plan	Name of the service plan associated with the log backup.
Truncated	Indicates if the transaction log was truncated by the log backup. Yes, if the log was truncated, otherwise No.
Backup File	The name of the log backup file and its location.

View SQL database copies

View the list of database copies by browsing to **Copy Management** › **Microsoft SQL Server** and selecting a SQL Server, then a database.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can also see details of a copy from the Copies tab of the service plan.
You can filter the list of copies by time of creation, and by service plan. In the Service Plan Copies tab, you can also filter by instance.

Table 9 Service Plan Copy details

Column	Description
Status	• Green: successful • Yellow: completed with errors • Red: failed
Name	Name of the copy. The copy is named with the time at which it was made.
Service Plan	Name of the service plan that is associated with the copy. Service plan field is blank for Repurpose copies.
SQL Server Backup Type	Type of SQL backup: Full or Copy • Full protects the database, and the active part of the transaction log. Copy protects the database and the active part of the transaction log without affecting the sequence of backups. • Secondary databases are read-only and can only be backed up with the Copy backup type. **Auto Switch to Copy** is enabled only when Full is selected as the backup type. However it is unchecked by default. Checking Auto Switch to Copy tells AppSync to check if the database role is Secondary, and if so, to switch the backup type to Copy. If Auto Switch to Copy is not enabled, backups fail for all secondary databases.
Mount Status	Shows if the copy is mounted. If mounted, the name of the mount host displays.
Recovery Status	Available values: • Not Recovered - when copy is not mounted or it is a file system mount • Successful - when Recovery is successful • Failed - when Recovery failed
Availability Group	The Availability Group column lists the availability group the database belongs to.
Generation	Used for repurposed copies, this column describes how many generations removed the copy is from the production database.
Source	This column displays the source database or copy from which a copy was created.
Copy Type	Type of copy can be one of the following: • RecoverPoint Continuous Data Protection Bookmark • RecoverPoint Continuous Remote Replication Bookmark • VNX Snap • VNXeSnap • VNXe FileSnap • VMAX Snap, VMAX Clone

Table 9 Service Plan Copy details (continued)

Column	Description
	For the preceding copy types, the following additional details are displayed in the Service Plan Copies tab: • Instance: The SQL Server instance that hosts the database. • Database name: The name of the copy's database. • Time: The time at which the database copy was made. • Server/cluster: Name of the server or the cluster that hosts the SQL Server instance. • Site: RecoverPoint Copy type continued: • XtremIO snapshot • VMAX 3 SnapVXClone, SnapVXSnap

Note

A **Repurpose** button on this page is enabled. When you select a **1st Generation copy**, the Repurpose wizard launches where you can create 2nd Generation copies.

View log backup list for a single database

You can also view log backups for a single database.

Follow these steps:

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**, and then select an SQL Server instance.
2. Click the **User Databases** folder.
3. Click on a database in the list and select the **Log Backups** tab.

Results

You can now view log the log backup list for the database. The following table describes details about the log backup:

Table 10 Database log backup details: SQL Server instance

Column	Description
Status	• Green: successful • Yellow: some log backups completed with errors when the service plan ran. • Red: failed
Name	Name of the log backup copy. The copy is named with the time at which it was made.
Service Plan	Name of the service plan associated with the log backup.

Table 10 Database log backup details: SQL Server instance (continued)

Column	Description
Truncated	Indicates if the transaction log was truncated by the log backup. Yes, if the log was truncated, otherwise No.
Backup File	The name of the log backup file and its location.

Log backup expiration

AppSync expires log backups when the service plan runs to create a new log backup. During expiration, AppSync deletes the log backup file and removes information about the backup from the AppSync database.

Log backups are always based off the previous Full database backup. However, you do not have to use AppSync to create the Full database backup. You can use AppSync to create a Copy database and log backup.

Additionally, AppSync can create Full database backups and log backups with, or without log truncation. Log backup expiration behavior depends on the type of database backup you create.

Log backups are eligible for expiration when the following conditions occur:

- The log backup is older than the service plan Minimum Retention Hours setting.
- All older database backups are expired. The database backups included in this check depends on the SQL Server Backup Type.
  - If the log backup service plan has SQL Server Backup Type set to Copy, only database backups created by that service plan are considered when looking for older database backups.
  - If the log backup service plan has SQL Server Backup Type set to Full, then Full database backups created by any service plan are considered.

Example 1: consider the following scenario:

- Service plan has log backup enabled.
- Database backup type set to Copy.
- Rotation set to one.
- Log backup minimum retention is set to 24 hours.

The service plan has run several times, creating a database backup and several log backups. The service plan runs again, creating a database backup and expiring the first database backup. This leaves several log backups with no older database backup. The service plan runs again, creating a log backup and expiring all of the previous log backups that are at least 24 hours old.

Example 2: consider the following scenario:

- You have two service plans.
- Both have database backup type set to Full.
- Service plan 1 is scheduled to run a database backup once a week with rotation set to four.
- Service plan 2 is scheduled to run daily at 8 PM with a rotation of seven.
- Service plan 2 has log backup enabled to run every hour and the log backup minimum retention is set to 24 hours.

- Both service plans have been running.
- Service plan 1 has four database copies and service plan 2 has seven database copies. Service plan 2 also has many log backups that were run between each of the seven database copies.
- Service plan 2 runs again and creates a database copy and then expires its oldest copy. It runs an hour later to create a log backup and looks for log backups that are eligible for expiration.

No log backups are eligible because service plan 1 has Full database backups that are older than all of the log backups. The next time service plan 1 runs, the oldest database backup will be expired. Log backups will then be eligible for expiration.

Manual expiration of log backups

You can also expire log backups manually.

To expire log backups for several databases:

1. Navigate to **Service Plans** › **Microsoft SQL Server**, and click on a service plan.
2. Click the **Log Backups** tab.
3. Select the log backups that you would like to expire and then click **Expire**.
4. Click **OK** on the confirmation dialog. AppSync will delete the log backup file and remove information about the backup from the AppSync database.

To expire log backups for a single database:

1. Navigate to **Copy Management** › **Microsoft SQL Server** and select an SQL Server instance.
2. Click the **User Databases** folder.
3. Click on a database in the list and select the **Log Backups** tab.
4. Select the log backups that you would like to expire and then click **Expire**.
5. Click **OK** on the confirmation dialog.

Considerations for working with SQL Server in a cluster

There are special considerations when working with SQL Server in a cluster.

When protecting SQL Server databases in a clustered environment, you must install the AppSync host plug-in on all of the nodes that are possible owners of a SQL Server instance. You can use the AppSync console to install the plug-in or manually install the plug-in on each server. Once the plug-in is installed, use the AppSync console to add the network name or IP address of the SQL Server clustered instances.

When protecting clustered SQL Server instances:

- You must add SQL Server virtual server to AppSync after installing the AppSync host plug-in software on each node.
- Only single subnets are supported.
- Mounting AppSync copies:
  - You can mount AppSync copies created on clustered databases to a standalone server or cluster node.
  - You can mount AppSync copies created on standalone databases to standalone server or a cluster node.

When mounting a SQL Server copy to a cluster:

- Supports mount to either alternate cluster or production cluster as non-clustered resource.
- Only supports mount to a cluster node, does not support mount to virtual server or mount and recover to clustered instance.
- Mount is supported in the environments of VMAX, VNX, VNXe, XtremIO or RecoverPoint. The *AppSync Installation and Configuration Guide* describes the required storage configuration steps.
- Select the appropriate mount option that applies for cluster mount based on your cluster and storage configuration.
- Manually disable `automount`. Run `diskpart` at a command prompt then enter **`automount disable`** at the `DISKPART>` prompt.

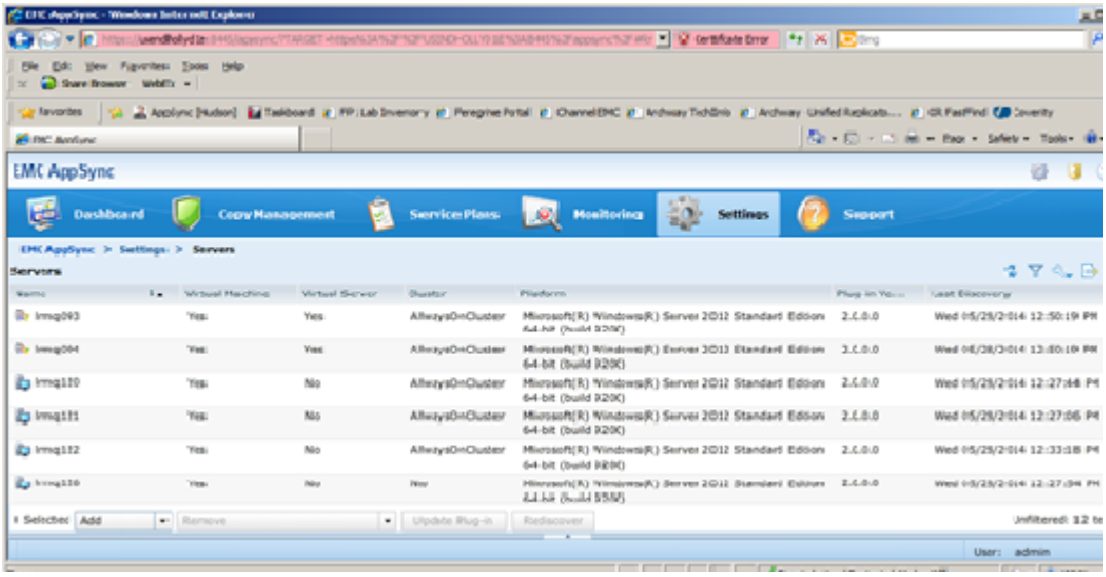
Special considerations for mount to production cluster:

- Mounting to a production cluster node using the original path is not supported.
- If the original server is a virtual server, mounting to a production cluster using the "original server" option is not supported and mounts fail.
- Statically mounting RecoverPoint SQL copies to production clusters is not supported. You must use dynamic mounts for this scenario.
- Performing a RecoverPoint mounted restore while the copy is mounted to a production cluster is not supported.
- Mounting RecoverPoint SQL APIT copies to production cluster nodes is not supported.

Example 1 Protect databases owned by clustered instances of SQL Server

In this example, you want to protect databases owned by clustered instances of SQL Server. In addition, some of those databases belong to AlwaysOn availability groups. Refer to the following figure for this example:

Figure 5 Cluster information



This cluster has the following configuration:

Example 1 Protect databases owned by clustered instances of SQL Server (continued)

- lrmq093 is a SQL Server virtual server and it hosts databases belonging to AlwaysOn Availability Groups.
- lrmq094 is a SQL Server virtual server.
- lrmq120, lrmq121, and lrmq122 belong to a SQL Server AlwaysOn failover cluster.
- lrmq120 and lrmq121 are possible owners of the clustered SQL Server instances owned by lrmq093 and lrmq094.
- lrmq122 has a standalone instance of SQL Server installed that hosts databases belonging to AlwaysOn availability groups.
- lrmq126 is the mount host with a standalone instance of SQL Server installed

To protect the databases belonging to the clustered and standalone instance, follow these steps:

1. Use the AppSync console to add lrmq120, lrmq121, and lrmq122. AppSync will install the plug-in on these servers and discover any non-clustered instances. If you need a mount host, you can add lrmq126 now.
2. With the AppSync console, add the virtual servers for the clustered instances, add lrmq093 and lrmq094.

SQL Server User Databases folder

The SQL Server User Database folder contains all the user databases for this SQL Server instance that have been discovered and stored in the AppSync database.

From the **Protect** button, you can subscribe the folder to a plan. By doing so, all the databases part of this folder are also protected. Once protected, the **Service Plan** column displays the name of the plan.

Clicking on the **User Databases** folder lists the individual databases part of this SQL Server instance.

In the Databases page, an entry in the **Service Plans** column tells you that all the databases that are part of the folder are protected. Any user databases added to the instance will also be protected. AppSync will automatically stop protecting any databases removed from the instance.

Note

If one or more user databases for an SQL Server instance are subscribed to a service plan, you cannot subscribe the User Databases folder to the same service plan. Conversely, if the User Databases folder is subscribed to a service plan, you cannot subscribe individual user database instances to the same service plan.

Discover SQL Server instances

To keep AppSync up-to-date, you should discover SQL Server instances when there is creation or deletion of instances.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**.
2. From the **Discover Instances** popup button below:
   - Select **On Server** and select one of the servers to discover instances from.
   - Select **Add Servers** to add a new server to AppSync.

Discovering SQL Server databases

AppSync discovers new user databases on demand or automatically on a service plan run.

When you click the User Databases folder the first time, AppSync discovers databases and lists them. To manually discover databases again, click **Discover Databases** in the **Databases** page.

On the other hand, when you subscribe the User Databases folder to a plan, databases are automatically discovered on each run of the plan. All databases that are currently ONLINE, including those that were added to the SQL instance after the last service plan run, are automatically protected.

If individual databases are subscribed to a plan instead of the User Databases folder, AppSync does not automatically discover any new databases that were created after the last run of the plan. In this case, AppSync rediscovers the database information of all the databases originally subscribed to the plan and protects the ones that are ONLINE.

Protect a SQL Database

Protect a SQL database by subscribing it to an AppSync service plan.

To optimize performance, AppSync creates copies of a maximum of 35 databases per instance. If more than 35 databases are subscribed per instance, AppSync breaks them into groups of 35 and creates copies of the groups sequentially. If more than 35 databases are subscribed to a service plan, and the databases reside on same storage unit (CG, LUN, DS, and so on), the split into groups with 35 databases does not occur. A single copy is desirable for a configuration when storage is on the same storage unit.

This number (35) is a server setting and can be modified, if required. Contact EMC Support to do so.

You can protect objects in different ways from different places in AppSync:

- Choose **Subscribe to Plan and Run** when you want to protect a selected database immediately. The service plan is run for the database alone.
- Choose **Subscribe to Plan** when you want to schedule the protection for later. Protection for databases that are part of the service plan are run at the scheduled time.
- Choose an appropriate service plan from **Create copy using plan** in the database Copies page.
- Choose **Run** from the SQL Server Service Plans page to run the whole plan immediately.

Configuring protection for SQL Server database

You subscribe a database or the User Databases folder to a service plan and run the service plan immediately, or schedule the service plan to run at a later time.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**.
2. Click a server instance to display its databases.
   - To protect all databases within the User Database folder, select the **User Database** folder.
   - To protect an individual database, click **User Databases** and select a database from the list.
3. From the **Protect** popup button below, select the appropriate service plan from:

Option	Description
Subscribe to Plan and Run	To subscribe the database for protection and run the plan immediately for the selected database(s).
Subscribe to Plan	To subscribe the database for protection. Protection for all databases that are part of the service plan are executed at the scheduled time.

Unsubscribing a database from a service plan

When you unsubscribe an individual database from a service plan, all existing database copies will be retained; only further protection will be removed.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**.
2. Click the SQL server instance.
3. Click **User Databases**.
4. Select the database to unsubscribe from a service plan.
   - Select the plan to unsubscribe from **Protect** › **Unsubscribe from Plan**. Only plans to which the database is subscribed to are in the popup list.
   - To unsubscribe from all service plans, select **Unsubscribe from Plan** › **All**.

Discovering SQL Server databases

Use the **Discover New Databases** command to update the SQL Server databases known to AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**.
2. Click a server instance, then the **User Databases** folder.
3. In the User Databases page, click **Discover New Databases** from the row of buttons below.

   Discovery can take several minutes to complete depending on the size of the instance.

Creating a database copy from the Copies page

Create a copy of a database by subscribing it to an AppSync SQL Server service plan from the Copies page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Microsoft SQL Server**.
2. Click a server instance and then click **User Databases** to display its databases.
3. Click on a folder to display **User Databases**.
4. From this list, click the database to view its copies.
5. From the **Create a copy using plan** list, select the appropriate service plan.

   The service plan runs immediately for the database.

Expiring an SQL database copy on demand

Expiring a database copy removes it from the AppSync database and can free up storage, depending on the replication technology and copy state.

Before you begin

This operation requires the Data Administrator role in AppSync.

Expiring a copy that was made with RecoverPoint does not remove the corresponding bookmark from RecoverPoint itself.

Procedure

1. Select **Copy Management** › **Microsoft SQL Server**.
2. Click a SQL Server instance to display its database folders.
3. Click the **User Database** folder.
4. Click the database whose copies you want to expire.
5. From the **Copies** page, select one or more copies to expire.

   You can also perform this action from the Service Plan's **Copies** tab.

6. Select **Expire** from the row of buttons below.

   Verify that you want to expire the copy you selected and any associated copies listed and confirm.

Service plan summary and details

The service plan **Settings** tab shows the name, description, schedule, and status of the service plan. Click the phases for detailed service plan settings and other tabs for information about subscriptions, lists of copies and events generated by the plan.

Service plan schedule

The schedule of a service plan is set in the **Plan Startup** phase.

The **Startup Type** (scheduled or on demand) determines whether the plan is run manually, or configured to run on a schedule. Options for scheduling when a service plan starts are:

- Specify a recovery point objective (RPO)
  - Set an RPO of 30 minutes or 1, 2, 3, 4, 6, 8, 12, or 24 hours
  - Minutes after the hour are set in 5 minute intervals
  - Default RPO is 24 hours
- Run every day at certain times
  - Select up to two different times during the day
  - Minutes after the hour is in 5 minute intervals
  - There is no default selected
- Run at a certain time on selected days of the week
  - One or more days of the week (up to all seven days) can be selected
  - There is no default day of the week selected. Default time of day is 12:00 AM.
- Run at a certain time on selected days of the month
  - Select one or more days of the month (up to all days)
  - Select one time of day. Available times are at 15 minute intervals.
  - Default is the first day of the month

Overriding service plan schedules

You can set individual schedules for databases subscribed to a service plan, overriding the generic recurrence setting.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

You can override only the settings of the recurrence type already selected for the service plan.

Procedure

1. Navigate to **Service Plans** and select one of the plans from the list.
2. From the **Settings** tab, select the **Plan Startup** phase.

   You will see the **Plan Startup Defaults** pane on the right.
3. Note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Scheduled** is selected as the **Startup Type**.
4. Select the **Start service plan** phase.

   You will see the **Start service plan** pane on the right.

5. Note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Automatic** is selected in the **Startup**.

6. Click the **Plan Startup Overrides** tab.

   You can see the list of all databases subscribed to the plan.

7. Select one or more databases and click **Override Schedule**.

   The **Override Schedule** dialog is displayed.

8. Set the schedule based on your requirement and click **OK**.

   For example, if the default recurrence type is **On specified days of the month**, and the rule setting is to **Run at 12:00 AM** on the **1st day of every month**, you can override the time and the day for individual datastores.
   A Pencil icon indicates that default settings have been overidden.

Application discovery

Before creating the User Database folder's copy, AppSync examines the SQL Server instance to look for changes such as addition, deletion, renaming, or movement of databases. If individual databases are being protected, AppSync rediscovers information about the selected database. A database is protected only if it is in the ONLINE state.

There are no user settings associated with this phase and it cannot be disabled.

Application mapping

After discovering the application, AppSync maps it to array storage, and protection services such as RecoverPoint.

There are no user settings associated with this phase and it cannot be disabled.

Pre-copy script

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters on a service plan's **Settings** tab.

The pre-copy script runs according to the schedule set in the **Plan Startup** phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts). You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default.

AppSync does not support running of PowerShell scripts directly. You usually must wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you must set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full pathname to the PowerShell command file in the .bat file:
   `powershell -command C:\PshellCommands.ps1 <nul`
2. Set the PowerShell execution policy so you can run the script. For example, the first line in the .bat file should look like the following for an unrestricted policy:
   `powershell -command set-executionpolicy unrestricted <nul`
3. To ensure correct termination of the PowerShell session, add ‹nul to the end of the line that calls the PowerShell script. The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Create copy

The **Create Copy** phase creates a copy based on the replication technology specified in the service plan.

This phase specifies the backup type of SQL Server copy to make. For VNX Snapshot copies, this phase also sets the period for automatic expiration of the copies.

Review Overview: Service Plan on page 10 for more service plan copy information.

SQL Server backup type

Two main backup types are supported: Full and Copy.

- **Full** protects the database, and the active part of the transaction log. This copy type is typically used when the copy will be considered a backup of the database or when the copy will be mounted in order to use a third-party product to create a backup of the database. This type of copy allows you to restore transaction logs to bring the database forward to a point in time that is newer than the copy, assuming you have backed up those transaction logs. AppSync uses Microsoft SQL Server's VDI snapshot feature to create this type of copy.
  - **Auto Switch to Copy** is enabled only when **Full** is selected as the backup type. However it is unchecked by default. Checking **Auto Switch to Copy** tells AppSync to check if the database role is Secondary, and if so, to switch the backup type to **Copy**.

    Note

    If **Auto Switch to Copy** is not enabled, backups fail for all secondary databases.
- **Copy** protects the database and the active part of the transaction log without affecting the sequence of backups. This provides DBAs with a way to create a copy without interfering with third-party backup applications that may be creating full and/or differential backups of the SQL Server databases. AppSync uses Microsoft SQL Server's VDI snapshot feature to create this type of copy.

  Note

  Secondary databases are read-only and can only be backed up with the **Copy** backup type.

Automatic expiration of copies

The automatic expiration value in a service plan's Create Copy phase specifies the maximum desired number of Snap, Clone or Bookmark copies that can exist simultaneously.

When the "Always keep *x* copies" value is reached, older copies are expired to free storage for the next copy in the rotation. Failed copies are not counted. AppSync does not expire the oldest copy until its replacement has been successfully created. For example, if the number of copies to keep is 7, AppSync does not expire the oldest copy until the 8th copy is created.

AppSync does not expire copies under the following circumstances:

- Mounted copies are not expired.
- A copy that contains the only replica of a database will not be expired.

This setting is independent of the VNX pool policy settings in Unisphere for automatic deletion of oldest snapshots. The service plan administrator should work with the storage

administrator to ensure that the VNX pool policy settings will enable the support of the specified number of snapshot copies for the application residing in that pool.

Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations.

Note

If this option is not selected, then RecoverPoint copies will accumulate, and will remain until the bookmarks fall off the RecoverPoint appliance.

Post-copy script

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters in a service plan's **Settings** tab.

The script runs on successful completion of the **Create copy** phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts). You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default.

When AppSync creates copies of application items in a service plan, it may break up the application items and place them in separate groups for protection. This action can be for performance reasons (for example, VSS for Exchange and SQL) or because items in a service plan may be protected by different replication technologies. For example, a service plan may contain some application items that are protected by VNX Snapshots and some by RecoverPoint bookmarks. As a result, application items in these groups are protected independently.

When AppSync calls a post-copy script, it passes the copies which were created in the group by calling the script with -appCopies ‹APP1› ‹APP2›, where APP1 and APP2 are the names of the application items in that grouping.

AppSync does not support running of PowerShell scripts directly. You usually must wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you must set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full pathname to the PowerShell command file in the .bat file:
   `powershell -command C:\PshellCommands.ps1 <nul`
2. Set the PowerShell execution policy so you can run the script. For example, the first line in the .bat file should look like the following for an unrestricted policy:
   `powershell -command set-executionpolicy unrestricted <nul`
3. To ensure correct termination of the PowerShell session, add ‹nul to the end of the line that calls the PowerShell script.

When AppSync runs the post-copy script, it is run for the application items that are part of a group. If there are multiple groups, the post-copy script runs multiple times. When AppSync runs the post-copy script, it passes the list of application items in the replication group as arguments to the script, right after the user arguments. The syntax is:

```
-applicationCopies <ITEM1> <ITEM2> <ITEM3>
```

where ‹ITEMx› is the name of the application item that is being protected.

The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Unmount previous copy

The service plan unmounts a previously mounted copy after creating the new copy. The exception is a copy that was mounted on-demand as opposed to by the service plan; in this case the on-demand mounted copy is not unmounted.

All the recovered databases are shut down as part of this phase. There are no user settings associated with this phase and it can be enabled or disabled.

Mount copy

The Mount copy phase either mounts the copy or mounts and recovers the copy. This phase can be enabled or disabled.

In the **Mount Copy Defaults** settings, you can set values to Mount copy or Mount and recover copy.

In the **Mount copy** settings, you set the mount host value, mount path and mount permissions (read-only or read-write). Other mount settings determine where the SQL metadata files are copied and the RecoverPoint image access type.

Field	Description
Mount on Server	The server on which to mount the copy. Only the nodes of the cluster or standalone hosts are available for selection. SQL virtual machines are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount path	• The **Default Mount Path** is `%SystemDrive%\AppSyncMounts\%%ProdServerName%%`. • To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). • The default path also contains an AppSync variable (ProdServerName) which is delimited with 2 percent signs (%%). • The following characters are not valid in the path:‹ › : " / | ? * • The mount path could also be **Same as Original Path**. However, this option is not available when the mount host is the same as production host. • If you specify a non-default mount path, the drive that is specified for mount cannot be a clustered disk.
Copy metadata files to	• The **Default Path** is the location to copy VDI and VSS metadata files:`%SystemDrive%\AppSyncMounts\%%ProdServerName%%` • The following characters are not valid in the path: ‹ › : " / | ? * • If you back up the database to another media, back up the metadata files as well.

Field	Description
	• AppSync can integrate with third-party backup software to create tape backups of SQL Server copies. The target directory that is specified here must be part of the backup.
Image access mode (during RecoverPoint mount)	• **Logged access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. Logged access is the only option available when you mount to the production host. • **Virtual access with roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. With RP VMAX, and RP XtremIO, virtual access with roll is not supported. • **Virtual access**: Provides nearly instant access to the image. Virtual access is not intended for heavy processing. Virtual access with RP VMAX and RP XtremIO is not supported.
Service Level Objective (SLO)	For VMAX 3 arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.
Use Dedicated Storage Group	• Applicable only for physical hosts or virtual machines with direct iSCSI as part of cluster. • Checked by default, enabling this option allows AppSync to enforce a dedicated VMAX , VNX, or XtremIO storage group for a mount. (A dedicated VMAX or VNX storage group contains the selected mount host only.) For XtremIO, this option applies to an XtremIO initiator group that only contains an initiator for the mount host. The mount fails if you are mounting to a node of a cluster that is in a storage group that is shared with the other nodes. **Note** Use this option to mount the copy to a node for copy validation or backup to tape. In this scenario, you need two storage groups. One storage group is dedicated to the passive node being used as a mount host and the other storage group is for the remainder of the nodes in the cluster. Both storage groups contain the shared storage for the cluster. • If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount. **Note** Uncheck this option for manually adding the target devices as clustered storage and presenting them to clustered SQL Server instances for data repurposing and data mining.

In the **Mount and recover copy** settings, you specify the recovery instance, the type of recovery, and the database naming details. Other settings are similar to the Mount copy settings such as mount path and image access type.

Field	Description
Recovery Instance	The SQL Server instance to be used for recovery. If the connection settings are not set or are invalid for the instance, the SQL Server Connection Settings dialog appears. Click **Connection Settings** to reset the credentials. **Note** Clustered SQL Server instances are filtered out of this view. If you are using a VMAX 3 array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group
Recovery Type	Available options are: Recovery (default), No Recovery, and Standby
Database renaming	This drop down includes: • **Use original database names (default if alternate instance):** This is not available for selection if the **Recovery Instance** is the production instance. • **Use original database names with suffix:** This is the default if **Recovery Instance** is the production instance.
Naming Suffix	Only displayed when **Original database names with Suffix** is selected in the **Database renaming** dropdown. The default value is **AppSync**.
Mount path	• The default mount path, when the mount host is the same as the production host, is `%SystemDrive%\AppSyncMounts\%%ProdServerName%%`. • To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). • The default path also contains an AppSync variable (ProdServerName) which is delimited with two percent signs (%%). • The following characters are not valid in the path: < > : " / | ? * • The mount path could also be **Same as Original Path**. You can select either of the options. • If you specify a non-default mount path, the drive specified for mount cannot be a clustered disk.
Copy metadata files to	• By default, the location to copy VSS metadata files is the same as the mount path. • If the mount path is Same as Original Path, then this defaults to %SystemDrive%\AppSyncMounts\%%ProdServerName%%. • The following characters are not valid in the path: < > : " / | ? * • If you are backing up the database to another media, you must backup these metadata files as well.

Field	Description
	• AppSync can integrate with third-party backup software to create tape backups of SQL Server copies. The target directory specified here must be part of the backup.
Image access mode (during RecoverPoint mount)	• **Logged Access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host. • **Virtual Access with Roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. • **Virtual Access**: Provides nearly instant access to the image; it is not intended for heavy processing.
Use Dedicated Storage Group	• Applicable only for physical hosts or virtual machines with direct iSCSI part of cluster. • Checked by default, enabling this option allows AppSync to enforce a dedicated VMAX, VNX, or XtremIO storage group. For XtremIO, this option applies to an XtremIO initiator group that only contains an initiator for the mount host. The storage group contains the selected mount host only for a mount and the mount will fail if you are mounting to a node of a cluster that is in a storage group shared with the other nodes. **Note** Use this option to mount the copy to a node for copy validation or backup to tape. In this scenario, you will need two storage groups. One storage group is dedicated to the passive node being used as a mount host and the other storage group is for the remainder of the nodes in the cluster. Both storage groups contain the shared storage for the cluster. • If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount and the mount will proceed. Host initiators can only belong in one initiator group in XtremIO, so use this option to ensure that you mount to a mount host that is the only host in the initiator group. **Note** Uncheck this option for manually adding the target devices as clustered storage and presenting them to clustered SQL Server instances for data repurposing and data mining.

Overriding mount settings in a service plan

If multiple registered SQL Servers are subscribed to the same plan, you can select different mount and recover settings for each SQL Server, overriding the generic settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Service Plans** › **Microsoft SQL Server** and click one of the plans from the list.
2. From the **Settings** tab, select the **Mount copy** phase.
3. On the right pane, select the **Mount Copy Overrides** tab.

   The list of servers include all SQL servers whose databases are subscribed to this plan.

   Based on whether **Mount copy** or **Mount and recover copy** is selected, the default settings display for all the Servers.
4. Select the Server whose settings you want to override and click **Set Overrides**.

   The **Override Default Mount Settings** dialog is displayed.
5. Select options only for those mount settings that you wish to override.

   Fields that do not have a selection retain their default settings.
6. Click **OK.**

   A pencil icon appears in the first column of the Server's row whose default mount settings you changed.
7. To revert back to default settings for a server, click **Use Default Settings**.

Post-mount script

Specify a post-mount script and parameters from the Post-mount script option in the **Settings** tab of a service plan.

The script runs on successful completion of the mount copy or mount with recovery phase. This script is typically used for backup.

From the **Server** list, select the server on which to run the script. You can optionally run it on a registered host other than the mount host, and enter credentials to run the script as a specific user.

The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on your script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Unmount copy

The final phase in the service plan unmounts the copy. This phase is disabled if the **Unmount previous copy** phase is enabled. There are no user settings associated with this phase.

If you have chosen to **Mount and recover copy** in the **Mount copy** phase, all the mounted databases are shut down as part of this phase.

Custom shutdown script prior to unmount

Prior to unmount, if you wish to perform a customized shut down of the databases, you can place a script at the following location: `%ProgramData%\EMC\AppSync\script`.

The script name must be in this format:
`<ServicePlanName>_<host_ProductionInstanceName OR ProductionInstanceName>_ ShutdownSQL.bat` where:

- `ServicePlanName` is the name of the service plan that the database is subscribed to
- `host_ProductionInstanceName` OR `ProductionInstanceName`:
  - In `host_ProductionInstanceName` , you can replace `host` by another name, the `ProductionInstanceName` is needed irrespective of whether there are different SQL instances or not.
  - Use `ProductionInstanceName` in case of default production instance which is equal to the host name.

Note

- It is recommended that you run the script as a Windows user. To run the script as a SQL Server user in SQL Server 2012 environment, the Local System user must have the sysadmin role.
- Using the _ as a separator in the script file name is mandatory.

In the absence of a customized script, AppSync will perform a shut down of the databases prior to unmount.

Mount considerations for SQL Server

Get mount host requirements including rules for mount and production host versions and virtual machine mount host support.

The mount host requires the same versions of the AppSync agent plug-in, SQL Server, and HBA drivers as the production host. Mount hosts must have an SQL Server installed if you want to recover databases from the mounted copy. If database recovery is not performed, then SQL Server is not required on the mount host.

Mount and production host versions

- If you are mounting to the node of Windows failover cluster, please see the section "Microsoft cluster server mounts" in the *EMC AppSync Installation and Configuration Guide*.
- If the major version of the SQL Server instance on the production mount host is later than that of the mount host, recovery will fail for all databases belonging to that instance.
- If the major version of the SQL Server instance on the production mount host is earlier than that of the mount host, recovery will succeed only if the recovery type is either RECOVERY or NORECOVERY. Recovery will fail if recovery type is STANDBY.
- If the major version of the SQL Server instance on the production mount host is same as that of the mount host, but the minor version is earlier, recovery will fail for all databases belonging to that instance.
- If the major version of the SQL Server instance on the production mount host is same as that of the mount host, but the minor version is later, recovery will succeed only if the recovery type is either RECOVERY or NORECOVERY. Recovery will fail if recovery type is STANDBY.

Virtual disk support

If the mount host is a virtual machine, the Virtual Center must be registered with AppSync. This is needed to mount RDMs.

For virtual disks:

- Production mount is not supported if the ESX host version is prior to 5.0.
- Non-persistent virtual disks are not supported.
- For datastore and virtual disk mounts on ESXi 5.x and RecoverPoint 4.1.7.7 environments, disable hardware acceleration to ensure successful virtual access type mounts. For more details, refer VMware Knowledge Base article 2006858.

For Hyper-V SCSI pass-through, the mount host cannot be a Hyper-V host it has to be a physical host or VM with NPIV or iSCSI direct attached.

Mount SQL Server database copy on-demand

You can initiate an on-demand mount of a database copy from a copy or a database.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. In the Databases page, select **Recover** › **Mount a Copy**.

   From the Copies page, select a copy and click **Mount**.

   The SQL Server Mount wizard launches.

2. Use the **Database**, **Copies** or **Service Plan** filters to select the appropriate copy to mount.

   The copies list is refreshed based on the filters selected.

3. Select the copy to mount.

   For a RecoverPoint copy, you also have the option to select a bookmark based on a specific time. However, there should be a copy available in AppSync prior to the time you select **Mount**.

   Click **Select a point in time** to select a copy with a specific time stamp. The time shown here is the console's time. If the console is in a different time zone from the RecoverPoint Appliance (RPA), specify the time as per the server's time zone to mount the copy.
   For VMAX 3 arrays, you are presented with an SLO drop-down menu. You can select the desired Service Level Objective (SLO) for the mount copy. If there is a storage group for the mount host with the desired SLO. AppSync will add the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host. If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices will be added to the original storage group when the copy is expired.

4. In the **Mount Additional Copies** page, select one or more additional copies to mount. The copies listed here are of other databases that were protected at the same time and on the same SQL Server as the copy you selected in the previous step.
5. On the **Select Mount Options** page, select **Mount copy** or Mount and recover copy.
6. In the **Summary** page, review the choices you made in the previous pages and click **Finish** to mount the copy.
7. In the **Results** page, select **View Details** to see progress of the different phases that are part of mounting a copy.

   The last phase completed is displayed at the bottom of the list.

SQL Server Mount Copy options

Review SQL server mount copy fields and descriptions.

Field	Description
Mount on Server	The server on which to mount the copy. Only the nodes of the cluster or standalone hosts are available for selection. SQL virtual machines are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount path	• The **Default Mount Path** is `%SystemDrive%\AppSyncMounts\%%ProdServerName%%`. • To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). • The default path also contains an AppSync variable (ProdServerName) which is delimited with 2 percent signs (%%). • The following characters are not valid in the path:‹ › : " / | ? * • The mount path could also be **Same as Original Path**. However, this option is not available when the mount host is the same as production host. • If you specify a non-default mount path, the drive that is specified for mount cannot be a clustered disk.
Copy metadata files to	• The **Default Path** is the location to copy VDI and VSS metadata files:`%SystemDrive%\AppSyncMounts\%%ProdServerName%%` • The following characters are not valid in the path: ‹ › : " / | ? * • If you back up the database to another media, back up the metadata files as well. • AppSync can integrate with third-party backup software to create tape backups of SQL Server copies. The target directory that is specified here must be part of the backup.
Image access mode (during RecoverPoint mount)	• **Logged access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. Logged access is the only option available when you mount to the production host. • **Virtual access with roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. With RP VMAX, and RP XtremIO, virtual access with roll is not supported. • **Virtual access**: Provides nearly instant access to the image. Virtual access is not intended for heavy processing. Virtual access with RP VMAX and RP XtremIO is not supported.

Field	Description
Service Level Objective (SLO)	For VMAX 3 arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.
Use Dedicated Storage Group	• Applicable only for physical hosts or virtual machines with direct iSCSI as part of cluster. • Checked by default, enabling this option allows AppSync to enforce a dedicated VMAX , VNX, or XtremIO storage group for a mount. (A dedicated VMAX or VNX storage group contains the selected mount host only.) For XtremIO, this option applies to an XtremIO initiator group that only contains an initiator for the mount host. The mount fails if you are mounting to a node of a cluster that is in a storage group that is shared with the other nodes. **Note** Use this option to mount the copy to a node for copy validation or backup to tape. In this scenario, you need two storage groups. One storage group is dedicated to the passive node being used as a mount host and the other storage group is for the remainder of the nodes in the cluster. Both storage groups contain the shared storage for the cluster. • If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount. **Note** Uncheck this option for manually adding the target devices as clustered storage and presenting them to clustered SQL Server instances for data repurposing and data mining.

SQL Server Mount and Recover copy options

SQL Server mount and recover copy options are explained in the following table:

Field	Description
Recovery Instance	The SQL Server instance to be used for recovery. If the connection settings are not set or are invalid for the instance, the SQL Server Connection Settings dialog appears. Click **Connection Settings** to reset the credentials. **Note** Clustered SQL Server instances are filtered out of this view. If you are using a VMAX 3 array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group
Recovery Type	Available options are: Recovery (default), No Recovery, and Standby

Field	Description
Database renaming	This drop down includes: • **Use original database names (default if alternate instance):** This is not available for selection if the **Recovery Instance** is the production instance. • **Use original database names with suffix:** This is the default if **Recovery Instance** is the production instance.
Naming Suffix	Only displayed when **Original database names with Suffix** is selected in the **Database renaming** dropdown. The default value is **`AppSync`**.
Mount path	• The default mount path, when the mount host is the same as the production host, is `%SystemDrive%\AppSyncMounts\%%ProdServerName%%`. • To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). • The default path also contains an AppSync variable (ProdServerName) which is delimited with two percent signs (%%). • The following characters are not valid in the path: ‹ › : " / | ? * • The mount path could also be **Same as Original Path**. You can select either of the options. • If you specify a non-default mount path, the drive specified for mount cannot be a clustered disk.
Copy metadata files to	• By default, the location to copy VSS metadata files is the same as the mount path. • If the mount path is Same as Original Path, then this defaults to %SystemDrive%\AppSyncMounts\%%ProdServerName%%. • The following characters are not valid in the path: ‹ › : " / | ? * • If you are backing up the database to another media, you must backup these metadata files as well. • AppSync can integrate with third-party backup software to create tape backups of SQL Server copies. The target directory specified here must be part of the backup.
Image access mode (during RecoverPoint mount)	• **Logged Access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host. • **Virtual Access with Roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. • **Virtual Access**: Provides nearly instant access to the image; it is not intended for heavy processing.
Use Dedicated Storage Group	• Applicable only for physical hosts or virtual machines with direct iSCSI part of cluster.

Field	Description
	• Checked by default, enabling this option allows AppSync to enforce a dedicated VMAX, VNX, or XtremIO storage group. For XtremIO, this option applies to an XtremIO initiator group that only contains an initiator for the mount host. The storage group contains the selected mount host only for a mount and the mount will fail if you are mounting to a node of a cluster that is in a storage group shared with the other nodes. **Note** Use this option to mount the copy to a node for copy validation or backup to tape. In this scenario, you will need two storage groups. One storage group is dedicated to the passive node being used as a mount host and the other storage group is for the remainder of the nodes in the cluster. Both storage groups contain the shared storage for the cluster. • If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount and the mount will proceed. Host initiators can only belong in one initiator group in XtremIO, so use this option to ensure that you mount to a mount host that is the only host in the initiator group. **Note** Uncheck this option for manually adding the target devices as clustered storage and presenting them to clustered SQL Server instances for data repurposing and data mining.

Supported mount recovery modes

The following mount recovery types are available when you are recovering a SQL database copy.

Recovery Type	Description
Recovery	Instructs the restore operation to roll back any uncommitted transactions. After the recovery process, the database is ready for use.
No Recovery	Instructs the restore operation not to roll back any uncommitted transactions. When in No Recovery mode, the database is unusable. This option is useful when the Database Administrator needs to restore one or more transaction log backups. Database is attached to the instance selected for recovery and is left in the "Restoring" state.
Standby	Restores files and opens the database in read-only mode. Subsequently, the Database Administrator can manually apply additional transaction log backups.

Recovery Type	Description
	Note If you are restoring a database from an older version of SQL Server onto a newer SQL Server version, do not use standby mode. If you use standby, the upgrade to the newer version cannot happen and that will result in a failure of the operation.

Unmounting an SQL Server copy

When you select an SQL Server copy to unmount, other copies that were mounted along with the selected copy will also be unmounted.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can unmount a copy only from a list of copies made for a database.

Procedure

1. Navigate to the Copies page from the Copy Management or Service Plan pages:
   - **Copy Management** › **Microsoft SQL Server** › select the server which hosts the filesystem you want to unmount, then select the database instance with the copy to unmount.
   - **Service Plans** › **Microsoft SQL Server**› select a service plan, then select the **Copies** tab.
2. From the list of copies, select the copy and click **Unmount** from the button in the lower part of the page.

   The **Unmount Confirmation** dialog displays all the copies of other databases that were mounted along with the selected copy to be unmounted.
3. Click **Yes** to confirm the unmount of all the copies shown in the dialog.

   The **Unmount** page displays the progress of the unmount operation. All copies associated with the selected copy will be unmounted.

SQL Server database restore overview

Review and consider the following sections regarding SQL Server database restore options.

These include:

- Restore considerations for databases in an Availability Group
- Affected entities during restore
- Restoring a primary database or a secondary database with failover
- Restoring a secondary database without failover
- How AppSync manages damaged SQL databases
- Restoring an SQL Server copy
- Restoring an SQL Server copy on XtremIO

- SQL restore utility (`assqlrestore`)

Restore considerations for databases in an Availability Group

AppSync restores copies of primary and secondary databases. Consider the following when restoring a database in an Availability Group.

- Restore is at the LUN level and must be restored back to the source LUN that was used to create the AppSync copy.
- AppSync suspends data movement as part of the restore process.
- A database cannot be restored if it is part of an Availability Group. AppSync removes the database from the Availability Group as part of the restore process.
- AppSync does not put the database back in the Availability Group. For more information on restoring databases in an Availability Group, see "Restoring a primary database or a secondary database with failover" and "Restoring a secondary database without failover".

Affected entities during restore

When restoring from a copy, you may be prompted to restore items in addition to the ones you selected.

An affected entity is data that resides on your production host that unintentionally becomes part of a replica because of its proximity to the data you intend to protect. You can prevent affected entity situations by properly planning your data layout based on replica granularity. The granularity of a replica depends upon the environment.

If there are *affected entities* in your underlying storage configuration, the Restore Wizard notifies you of these items. The following scenarios produce *affected entities* that require you to acknowledge that additional items will be restored:

- For RecoverPoint, if the databases are in the same consistency group they become *affected entities* when the other database is protected.
- For VNXe, if the databases are in the same LUN group they become affected entities when the other database is protected.
- For VNX/VMAX, VNX, VNXe, or XtremIO, if the databases are on the same LUN they become *affected entities* when the other database is protected.
- For VMware virtual disks, since restore involves a datastore, restore of all applications residing on the same datastore (virtual disks on the same datastore) are also *affected entities*.

If the affected entity was protected along with the database that is selected for restore, it will be restored by AppSync. Any other database that was not protected but is an affected entity will be overwritten.

AppSync calculates affected entities for the consistency groups or LUN groups of the database that is selected for restore. If the affected databases in turn partially reside on other consistency groups or LUNs groups, AppSync does not calculate affected entities on those consistency groups or LUN groups.

Depending upon the type of affected entity, the affected databases are detached by AppSync or you must manually detach them from the SQL Server instance.

Affected entities are calculated only for the SQL Server instances where the credentials are configured. AppSync does a fresh database discovery for all these instances before calculating the affected entities.

Restoring a primary database or a secondary database with failover

Once you click the **Finish** button in the **SQL Server Restore** wizard, AppSync performs the following actions:

1. If you had selected the **Failover the Availability Group if the current role is Secondary** checkbox, AppSync verifies the health of the databases in the Availability Group that are not being restored. If they are not healthy, AppSync cannot perform the failover and the restore operation fails. You must retry the restore operation without selecting the checkbox.
2. If you had chosen to backup the transaction log, AppSync backs up the transaction log.
3. AppSync suspends data movement for all replicas of the selected database before removing all replicas of the selected database from the Availability Group.
4. If the database being restored is secondary, AppSync initiates the failover.
5. AppSync restores the LUNs of the selected database.
6. Finally, AppSync recovers the database and leaves it in the Recovery state that you selected in the **SQL Server Restore** wizard.

After AppSync completes the restore, you must perform the following steps.

Procedure

1. Restore any log backups and recover the primary database.
2. Add the database back into the Availability Group.
3. If the primary database was rolled forward so it is at the same time as the secondary database, re-join the secondary copies to the Availability Group.
4. If the primary database was not rolled forward:
   a. Delete any secondary copies of the restored database.
   b. Reseed and re-join the secondary database replicas to the availability group.

Note

After AppSync removes the primary database copy, the copy is in the recovered state if it is healthy. If you restored a secondary copy with failover, the primary role will have moved to another SQL Server instance. You must delete the original primary database and reseed it.

Restoring a secondary database without failover

Once you click the **Finish** button in the **SQL Server Restore** wizard, AppSync performs the following actions:

1. If you had chosen to backup the transaction log, AppSync backs up the transaction log.
2. AppSync suspends data movement for the selected secondary database replica. Replication continues to work for other replicas of the database.
3. AppSync removes the selected secondary database replica from the Availability Group.
4. AppSync restores the LUNs of the selected database.

5. Finally, AppSync recovers the database and leaves it in the Recovery state that you selected in the **SQL Server Restore** wizard.

After AppSync completes the restore, you must perform the following steps.

Procedure

1. Restore any log backups and leave the secondary database in a "NO RECOVERY" state.
2. Join the secondary database back into the Availability Group.

How AppSync manages damaged SQL databases

Damaged databases may have data files missing or damaged with their log files intact. AppSync can take tail log backups for damaged databases. A damaged database must not contain bulk-logged changes and it must not be in OFFLINE state.

If the production database is damaged and you select the **Database is damaged** checkbox during restore, AppSync backs up the tail log of the damaged database before proceeding with restore. If the damaged database is in RECOVERY_PENDING or SUSPECT state, AppSync first tries to detach the database by setting the EMERGENCY mode on it. If AppSync fails to set EMERGENCY mode on the database, it drops the database and then proceeds with the restore. Once the restore is successful, you can recover the database manually using the tail log backup.

Refer also to Restore procedures with XtremIO on page 198.

Restoring a SQL Server copy

You can perform a restore of an SQL Server copy from the Server's Copies page, service plan's Copies page or from the Databases page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. In the Databases page, select **Recover** › **Restore** .

   In the Copies page, select a copy and click **Restore**.

   The **SQL Server Restore** wizard launches.
2. Select the copy to restore.

   Use the **Time** or **Service Plan** filters to select the appropriate copy to restore. The copies list is refreshed based on the filters selected.
3. Click **Next**.

   If the selected copy has affected entities, the **Restore Warnings** page is displayed.
4. Read the warning messages for the affected databases. Select the checkbox to indicate your agreement to restore other entities along with the selected copy.
5. In the **Backup Transaction Logs** step, select **Yes** to backup logs prior to restore.
   a. In the **Back up to** box, enter the location where the logs will be backed up. The files will bear the name of the database.
   b. Select the **Add a file extension to the backup file name** checkbox and specify an extension for the backed up files. The default extension is .trn.
   c. Select the **Add a prefix to the backup file names** checkbox and specify a prefix for the backed up files. The default prefix is AppSync.

d. Select the **Database is damaged** checkbox to backup tail log files.

e. Select the **Truncate the transaction logs** checkbox as required.

This checkbox is not available for selection if you selected the **Database is damaged** checkbox.

f. Select the **Overwrite existing backup files** checkbox as required.

This checkbox is not available for selection if you selected the **Database is damaged** checkbox.

6. Click **Next** for the **Restore Options**.

The **Restore Options** page is displayed.

7. Select the appropriate recovery or restore options.

a. To recover the database, choose from one of these options:

- **Leave database ready to use**: This option is not available if you have chosen to backup transaction logs.
- **Leave databases non-operational**

Note

Select this option when restoring a secondary database without failover. This leaves the secondary database in the restoring state so transaction logs can be restored allowing the database to rejoin the Availability Group.

- **Leave databases in read-only mode**: If you select this option, specify the location in the

Standby file location box where the standby files must be stored. The default path is C:\temp.

b. To force a restore by overwriting the existing database, select the **Overwrite the existing databases** checkbox.

This option is not required in the normal circumstances.

This option is not available if you have chosen to backup transaction logs.

c. In case of Availability Group, select the **Failover the Availability Group if the current role is Secondary** checkbox to initiate a failover before restore if you are restoring to a secondary database.

A warning message is displayed that the database will be removed from the Availability Group and that you must rejoin it after AppSync restores the volume.

d. Select the **I have read and understand the warning above, and want to continue with the restore** checkbox to acknowledge the message.

8. Click **Next**.

The **Summary** page is displayed.

9. Review the **Summary** page and click **Finish** to perform the restore.

10. In the **Results** page, click **View Details** to see progress of the different phases that are part of restoring a copy.

The last phase completed is displayed at the bottom of the list.

11. After AppSync restores a database in an Availability Group, perform additional steps as needed:

- Restore a primary database or a secondary database with failover on page 109.
- Restore a secondary database without failover on page 109.
- Manually restore an SQL Server copy on XtremIO on page 112

Restoring an SQL Server copy on XtremIO

Version 2.2.2 and higher of AppSync supports automated restore of copies on XtremIO 4.0 and higher. This topic shows you how to use AppSync versions 2.1 - 2.2.1 and an XtremIO version lower than 4.0 to restore an SQL Server database to a point in time with a semi-manual restore process. Restore of SQL Server transaction log backups are not supported.

Before you begin

For automated restore, refer to Restoring an SQL Server copy on page 110.

For semi-manual restore ensure the following pre-requisites, then perform the procedure:

- SQL Server databases and XtremIO storage running on the AppSync configuration.
- An AppSync service plan that replicates the database.

Procedure

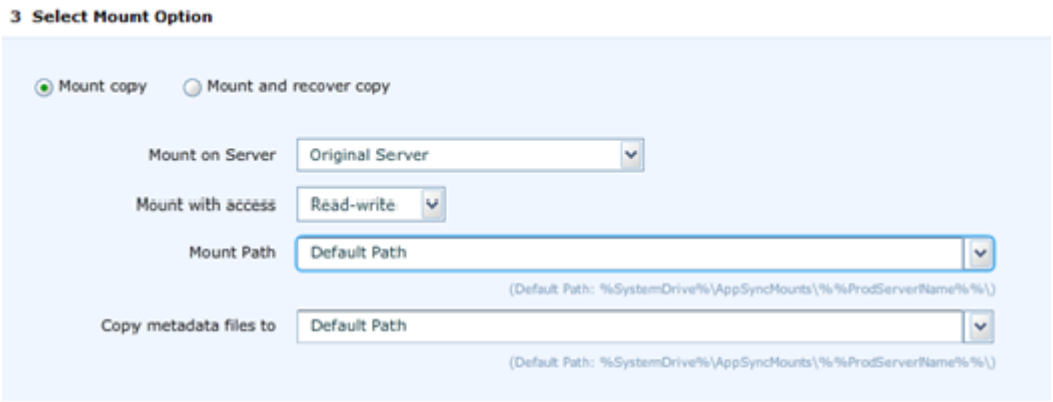
1. On the AppSync console, select **Service Plans** › **Microsoft SQL Server** , and then click the wanted service plan, for example, **Bronze**.

   The **Copies** page displays existing copies.

2. Mount the copies that you want to restore. When prompted to `Mount Additional Copies`, select all database copies that reside on the disk drives you are replacing.

   The Select Mount Option dialog box opens.

   Figure 6 Select Mount Option



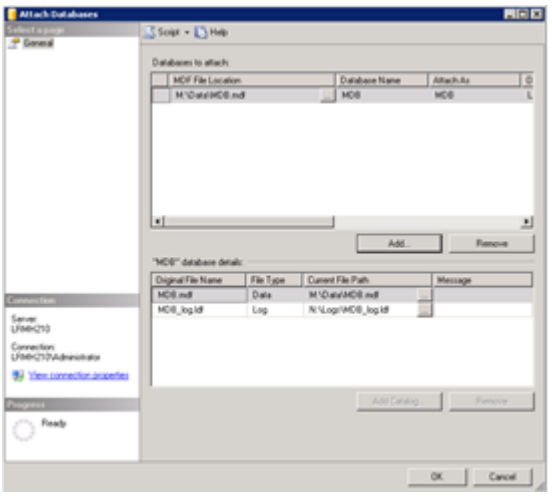
3. In the **Select Mount Option** dialog box, select **Mount copy**.
4. Since AppSync does not allow you to recover to the production instance, select **Original Server** from the **Mount on Server** list box.
5. Select **Read-write** from the **Mount with access** list box.

6. Select **Default Path** from the **Mount Path** list box (because you mount to the original server).
7. On the production host, stop any application that uses the databases that you are restoring.
8. Using the SQL Server Management Studio, take the databases offline, and then detach them.

   Remember that you replace the production disk drives with the AppSync snapshots, so detach any databases that are using the same devices.
9. After you detach the affected databases, use Windows Server Manager to delete the drive letter or mount point for the disks that you are restoring. Record the disk number and drive letter assignments in case you need to undo the restore steps.

   After the AppSync mount completes, the drives for the restore copies are located as mount points in `C:\AppSyncMounts\<SERVERNAME>`.
10. Start Windows Server Manager to find the mounted devices, and then assign drive letters or mount points to replace the ones that you removed in Step 8.
11. Use SQL Server Management Studio to attach the databases that you want to restore. Point to the mounted AppSync copies for the databases. If the database has 17 or more files, use **`CREATE DATABASE database_name FOR ATTACH`**.

Figure 7 Attach Databases



At this point, all the restored databases should be online, and you then can restart any database application that you previously stopped. You can perform the following steps without affecting SQL Server.

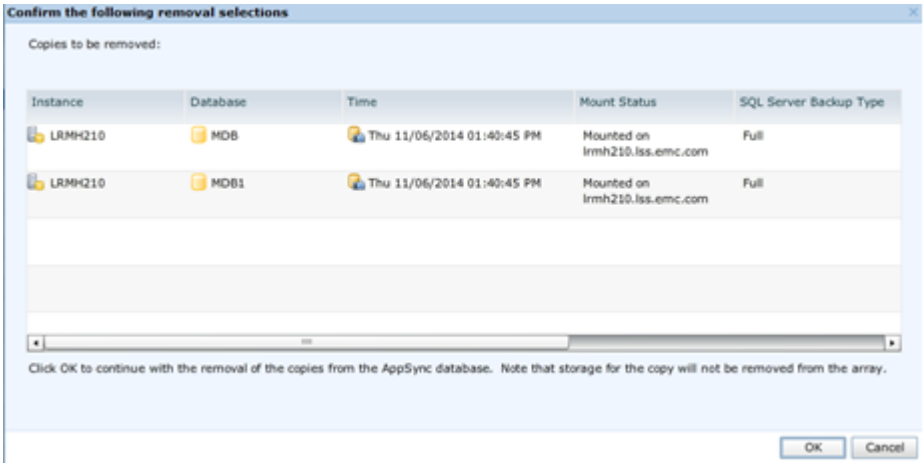
12. On the AppSync console, return to the Database Copies page that is described in Step 1, and then click **Remove** for each mounted copy.

    This action removes the copy from the AppSync database, without removing the snapshots on the production mount host, or on the XtremIO storage array. You receive a warning message.

Note

If the service plan contains multiple databases, the storage for all databases in the service plan remains on the XtremIO storage array. You can remove them at your discretion.

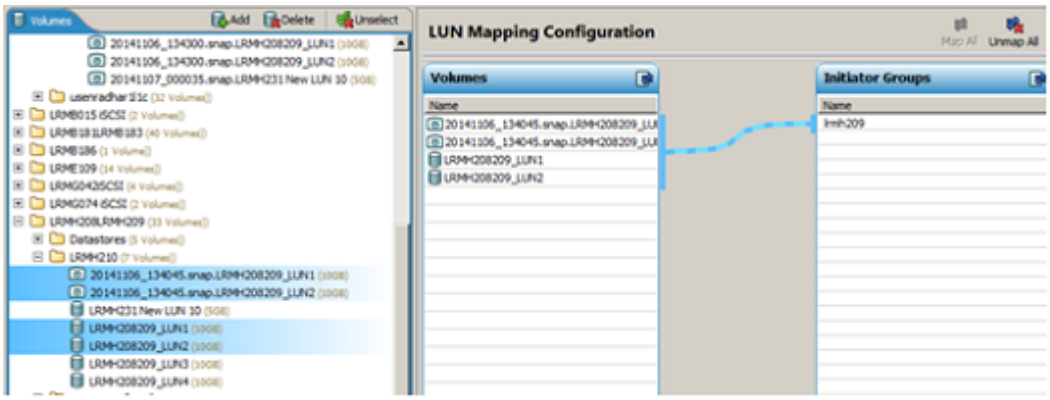
Figure 8 Confirm the following removal selections



13. Move the mounted snapshots from the `/AppSyncSnapshots` folder to the folder where the production LUN that is being replaced resides. Be sure to move the snapshots that are mounted, that is, the snapshots that are currently masked to the ESX initiator group (if production host is virtual machine). If the production host is a physical host, move the snapshots to the folder where the production LUNs are located.

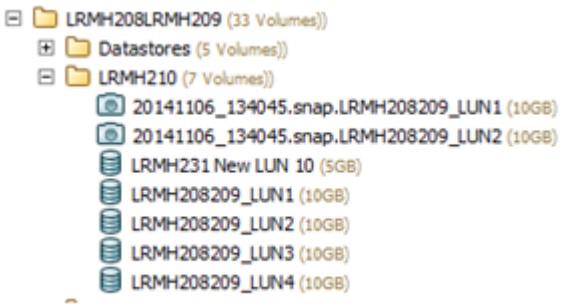
    The production LUN and the snapshot appear in the same folder.

Figure 9 LUN Mapping Configuration



After the move, notice that the restored devices are a snapshot and the production devices are volumes (LUN).

Figure 10 Snapshot and LUN example



14. Perform this step only if the production host is a virtual machine.

a. Unmap the original production volumes from the production host.

b. Rescan the ESX host.

c. Remove the RDMs from the production virtual machine configuration.

15. `Perform this step only If the production host is a physical machine.`

a. Unmap the original production volumes from the production host.

b. Perform a device rescan on the host to remove the old production devices.

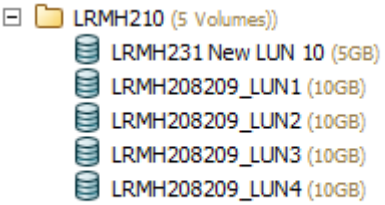
16. Remove the production volumes.

This action causes the restored snapshots to become volumes.

Figure 11 Restored snapshots become volumes

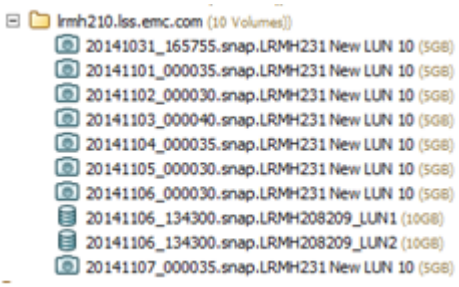
17. Rename the snapshots to the production volume names.

Figure 12 Rename snapshots to production volume names



In the AppSync XtremIO console, notice that the other snapshots in the `/AppSyncSnapshots` folder for the production XtremIO volumes that you removed in the previous step have also become volumes.

Figure 13 Snapshots become LUNs



18. Run the database service plan to create a snapshot of the restored databases.

SQL Server restore utility (assqlrestore)

AppSync includes a SQL Server restore utility called `assqlrestore`.This section describes it's function and uses.

The `assqlrestore` utility lets you restore individual SQL Server databases from a tape backup or mounted copy without reverse-syncing the target device over the source device. It can restore a database, filegroup, or file. The utility can restore to the original database or to a new database. SQL Server VDI metadata that was created as part of the replication activity is required to restore a database using `assqlrestore`.

`assqlrestore` is a command line interface that you run from a command prompt window on the AppSync client. It is installed on the client as part of the AppSync installation.

Restoring an individual database from a mounted copy is especially useful when you need to recover only one database and do not want to overwrite an entire device which occurs with a normal AppSync restore.

Assqlrestore command syntax with examples

This topics lists the command syntax for the `assqlrestore` commend followed by examples of the commands.

Command syntax

The following table lists the command syntax for the `assqlrestore` command.

Table 11 `assqlrestore` Command Syntax

Option	Description
Required	
-s	SQL Server name including instance name (host\instance).
-f	Metadata filename and location.
-d	Database name.
Connection Types (-E or -U)	
-E	User used for Windows Authentication (specify username)
-U	SQL Server login ID.
-P	Clear text password (used with -E and -U options).
-p	Encrypted password (used with -E and -U options).
Optional	
-r	Recover option – `RECOVERY`, `NORECOVERY` (default), or `STANDBY`.
-u	Undo filename, required for STANDBY
-m	Move file. Option has two parameters: `logical_file_name` and `operating_system_file_name`. Pathnames must exist. Repeat option for each file, including log files or full text catalog files. If you are restoring to a new database name, use the -m option so you do not

Table 11 `assqlrestore` Command Syntax (continued)

Option	Description
	overwrite the original files. For example: `-m logicalfilename S:\existingdir\newfilename.mdf`
-fg	Filegroup to restore. Repeat option for each filegroup.
-lf	Logical file to restore. Repeat option for each logical file.
-e	Displays encrypted password when unencrypted password is specified as an argument. Not used with other parameters.
-v	Verbose mode.
-q	Quiet mode. Will not ask questions.
-l ‹log_dir›	Creates log files in the specified directory.
-h	Help.

Example 2 Command syntax examples

Command options are case-sensitive. Refer to the "SQL Server books online" for a description of the T-SQL

Note

Command parameters have changed from the Replication Manager utility (`rmsqlrestore`)

- Using Windows authentication, restore without applying logs.

```
 assqlrestore exe -E Administrator -P password -s sql1\instance1 -
d custinfo
-f "C:\AppSyncMounts\sql1\APPSYNC_VDI_INSTANCE1_ custinfo.bin" -r
RECOVERY
```

- Restore to a new database name and move files using a SQL login and encrypted password:

```
 assqlrestore -s sql1\instance1
-d custinfoTest
-f "C:\AppSyncMounts\sql1\APPSYNC_VDI_INSTANCE1_ custinfoTest.bin"
-r RECOVERY
-m custinfo_Data S:\custinfoTest.mdf
-m custinfo_Log T:\custinfoTest.ldf
-U sa -p 1EMC_4roJdyU5;x
```

  - To get the encrypted password:

```
assqlrestore -e <unencrypted_password>
```

Restoring an SQL Server database with `assqlrestore`

The basic steps to restore a database are provided here. You may need additional steps but use these as a framework.

Before you begin

Log in to the SQL Server system as a user with Administrator rights, then back up the SQL Server transaction log.

Procedure

1. Take the target SQL Server database offline.
2. Restore the database files (.ldf, .ndf, and .mdf) from tape, or copy them from a mounted replica. You can copy them over the original files or to a new location.
3. Open a command prompt window and cd to: `C:\Program Files\EMC\AppSync\Host Plug-in\`
4. Run the `assqlrestore` command.

   Refer to the Assqlrestore command syntax with examples section for sample commands. The basic command syntax is:

   ```
   assqlrestore -s <SQLservername> -d <databasename> -f
   <metadatafile> -r <recovery_type>
   ```

5. If required, apply transaction logs and recover the database.

Restoring a file or filegroup with the SQL Server restore utility

Learn how to restore a file or filegroup with the SQL Server `assqlrestore` utility.

Before you begin

Be sure you understand how restore of files and filegroups behave in SQL Server before proceeding.

Note

You cannot use the `assqlrestore` utility to restore a SQL Server filegroup if the filegroup name contains non-ASCII characters.

Log in to the SQL Server system as a user with Administrator rights, then back up the SQL Server transaction log. For file or filegoroup restore, the database must be online.

Procedure

1. Open a command prompt window and cd to: `C:\Program Files\EMC\AppSync\Host Plug-in\`
2. Run the `assqlrestore` command.
   a. When `assqlrestore` displays the restore command that it is about to run, verify with **Y** if it is correct.
   b. When `assqlrestore` prompts, `restore the files you are recovering`, enter **Y** to continue.

To restore two files, for example, run:

```
assqlrestore -s <SQLservername> -d <databasename>
-f <metadatafile> -lf <logical_filename1>
-lf <logical_filename2> -r norecovery
```

To restore two filegroups, run:

```
 assqlrestore
-s <SQLservername>
-d <databasename>
-f <metadatafile>
-lf <logical_filename1>
-fg <logical_filegroupname1>
-fg <logical_filegroupname2>
-r norecovery
```

Do not use the quiet mode for a file or filegroup restore. You can use -lf and -fg in the same restore command.

Repurposing SQL Server database copies

This topic explains how to use the AppSync repurposing feature for database and Bookmark copies. ,

Review and consider the following information regarding repurposing features:

- Repurposing creates a multi-level tree of copies of the database.
- AppSync identifies copies that are created from a repurpose action by a "generation removed" number from the production source data, for example, Gen 1, Gen 2, and so on.
- There is no practical limit to the number of generations, but support is limited to two generations that are removed from the production data.
- A first generation(1st Gen) copy creates a copy that can be used as source for other copies. This action creates a copy-of-copy.
- Repurpose copies are meant to be mounted for extended periods of time for various purposes.
- After use, repurpose copies are either discarded or refreshed.
- Repurpose copies do not figure into RPO calculations.
- You can run 1st Gen copies now or schedule them to run at a future time.

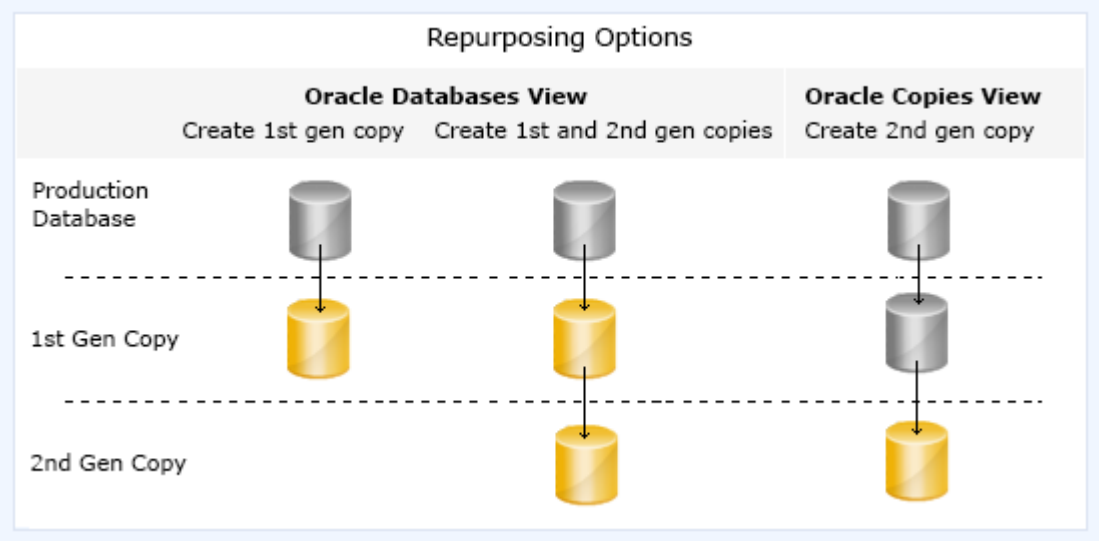
The console displays all scheduled repurpose actions. Select any of them, and then select the Delete button. The scheduled activity is removed.

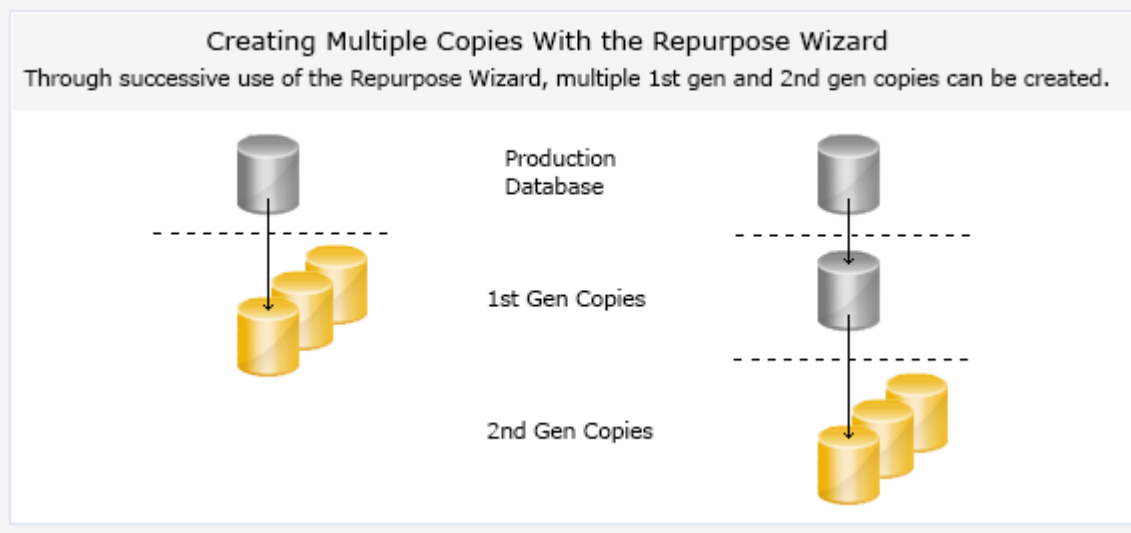
If you enable hot-backup, the 1st Gen copy of the database creates the application consistent copy. It Includes application discovery, mapping, and database freeze/thaw. AppSync does not set database freeze/thaw as the default for 1st Gen repurpose copies.

Second generation (2nd Gen) copies are created as copies-of-copies, using the 1st Gen copy as the source. They do not include application discovery, mapping, and database freeze/thaw. As a result, 2nd Gen copies are created much faster than 1st Gen copies.

Note

Repurposing copies are not supported for Oracle databases on VNX File storage, or NFS file systems.





Repurpose refresh

Refresh means to discard the current copy (expire), and recreate the copy contents using its parent.

- 1st Gen and 2nd Gen copies can be refreshed.
- Refreshing a 1st Gen copy creates an application consistent copy with a new time.
- 2nd Gen copies are not modified if you refresh 1st Gen copy.
- Refresh of 2nd Gen copy resynchronizes that 2nd Gen copy with the 1st Gen parent. (Use for throwing away changes of 2nd Gen copy and starting over.)
- 2nd Gen timestamp is the same as the 1st Gen copy.
- With refresh, it is possible to have first and 2nd Gen copies with different copy time stamps.
- If you specified Unmount Previous Copy when creating the 2nd Gen copy, AppSync unmounts the copy before creating the new copy.
- Refresh of a 1st Gen copy on XtremIO : If the number of LUNs in the source database changes, then create only new snapshots. For example, AppSync uses the refresh provided by the XtremIO array from source LUNs to create the 1st Gen snapshot copy.
- Refresh of 2nd Gen copy on XtremIO: If you refresh the source 1st Gen copy and the number of LUNs in the source database changed, then create only new snapshots.

Otherwise, use the refresh provided by the XtremIO array from 1st Gen snapshots to 2nd Gen snapshot copies.

- After the refresh, AppSync remounts the copy if the copy was mounted.
- 2nd Gen copy is recreated from 1st Gen parent. If 1st Gen parent no longer exists, then the refresh fails.
- 1st Gen copy is recreated from the application.
- The current copy that you want to refresh must be unmounted (if it is mounted). If you selected **Mount Copy** in the Repurpose wizard, AppSync mounts the copy again.

You can refresh a repurposed copy at any time. To start the refresh:

1. From the **Applications** tab of the AppSync console, select the repurposed copy that you want to refresh.
2. Click **Refresh**.

SQL Server repurpose caveats

AppSync supports SQL Server repurposing in standalone environments and failover cluster environments with or without AlwaysOn Availability Groups.

Repurposing SQL Server copies supports multiple database selection for repurposing copies. AppSync does not support multiple array repurposing or dynamic database subscription. The 1st Gen copy can be taken only for a single database or a set of databases belonging to the same host within the same array. The refresh works only for those databases that were previously subscribed. AppSync does not subscribe the whole user database folder to the SQL repurposing service plan.

The system displays repurposed copies of an SQL Server database hierarchically. The system displays the 1st Gen (parent) copy , and then it displays 2nd Gen copies as children of the 1st Gen copy.

Note

If you are using XtremIO 3.x as the 1st Gen copy source, and then upgrade to XtremIO 4.x, and try to create a 2nd Gen copy, refresh the 1st Gen copy or the operation fails.

Using the Repurpose wizard

Use the Repurpose wizard to schedule or immediately create 1st Gen or 2nd Gen copies as needed.

Before you begin

You need AppSync administrative privileges to Repurpose the database instance.

To display the list of available applications.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.

Option	Description
To Repurpose an SQL copy:	Select SQL Server
To Repurpose an Oracle copy:	Select Oracle

A list of available databases for the application choice loads.

2. Click the database instance you want to Repurpose, and then select **Repurpose** from the drop-down list in the lower left of the console screen.

This action launches the Repurpose wizard, and leads you to the Intentions page where you can tell AppSync which action you want to perform:

- **Create First Generation copy**
- **Create First Generation copy and a Second Generation copy**

3. Select the desired copy type, and select **Local** or **Remote** in the Site drop-down to continue creating the copy.
4. Click **Next** to launch the **Settings** screen.

   From the Settings screen, you can define the specific options for 1st and 2nd gen copies. Specifically you can

   - Define labels for each copy to help identify the copy purpose.
   - Select application-specific copy options for 1st gen copy only.
   - Choose appropriate copy type (wizard fails if incorrect type is chosen).
5. Select the desired options for the copy, and then click **Next**.

   The schedule page of the wizard appears allowing you to identify when the 1st generation copy should be created. Create the copy now or schedule the copy for a convenient time.
6. Select **Run now** or **Run later** followed by typing run- time date and time, and then press **Next** to complete the wizard.

After you finish

The Repurpose Monitor

The Repurpose Monitor allows you to view all currently running repurpose activities, and monitor their progress. The Repurpose Monitor shows the item being repurposed (source) and the label of the item being created or refreshed along with the application type. Refer to The Repurpose Monitor on page 211.

View or cancel scheduled repurpose copies

You can view or cancel any scheduled first generation repurpose copy.

Procedure

1. From the Appsync console, navigate to **Application** › **Copy Management**, and then select the appropriate database.
2. Select **Repurpose** › **View Scheduled Repurpose Copy** to view all scheduled repurpose actions.
3. To delete an action, select one or more desired actions, and click **Delete** to remove the action.

CHAPTER 7

Protect Oracle

This chapter includes the following topics:

Overview of Oracle support

Use AppSync to create and manage application consistent (using hot backup mode) and crash consistent (without hot backup mode) copies of Oracle® databases. The copies can be used for mount (with/without recovery) and restore.

The *AppSync Support Matrix* on https://elabnavigator.emc.com/eln/extendedSupport is the authoritative source of information on supported software and platforms..

AppSync supports:

- Oracle - (Standalone and Oracle Real Application Cluster) and on Linux and AIX.
- Oracle installations on physical hosts as well as virtual machines (with pRDMs and Vdisks) - There is no support for RDMs in virtual mode.
- Oracle databases residing on NFS file systems with VNX storage.
- Oracle databases residing on ASM and file systems.
- RMAN cataloging of databases to a remote catalog.
- Repurposing of Oracle database copies. Refer to the repurposing overview topic earlier in this document for details.

Oracle permissions

These permissions are required for AppSync to work with Oracle.

- Root or sudo access to Oracle production server and mount server.
- When connecting to Oracle databases, AppSync uses a bequeath connection and always connects as SYSDBA.
- When connecting to Oracle ASM, AppSync uses a bequeath connection and always connects as SYSASM.

Red Hat Cluster Services Integration with AppSync

AppSync can work with standalone Oracle databases that are configured to failover from node to node in an RHCS (Red Hat Cluster Services) environment.

Overview

During a replication process, if the node you used to create a service plan is not accessible, AppSync runs the replication on another node in the cluster. If the node you used to create the original copy is not accessible, AppSync does not rely on the Virtual IP of the Oracle service group. Therefore, ensure that you register all nodes in the RHCS cluster in the AppSync server for database replication.

From a restore perspective, AppSync can only restore to the node where the copy was originally created, therefore the original node must be active, otherwise the restore process fails.

Requirements

Review the following requirements to use a standalone database that fails over as part of an RHCS cluster:

- The AppSync host plug-in must be installed on all nodes of the cluster.
- The IP resource must be configured in the Oracle service group for the clustered database.

- If a failover occurs while running a replication or restore process, the operation fails. Node failover should occur before running the service plan, before the start of a replication, or start of a restore.
- The Oratab file should have an entry for all possible SIDs that can run on the specified node (passive and active instances).
- The package sg3_utils, which contains utilities for accessing devices that use SCSI command sets, must be installed on all nodes.

Mount considerations

- The mount host must not be part of the RHCS cluster.
- The mount host run the same Oracle version as the copy host.
- The AppSync host plug-in must be installed on the mount host.
- The package sg3_utils, which contains utilities for accessing devices that use SCSI command sets, must be installed on the mount host.

Restore considerations

- AppSync can only restore to the node where the copy was originally created, therefore the original node must be active. Otherwise, the restore process fails, and corrupts the database. The console provides a detailed warning message before the restart of the restore.
- To perform a restore in an RHCS environment, follow these steps:
  1. Perform the restore.
  2. Start the mount instance.
  3. Perform a manual recovery.
  4. Shut down abort database.
  5. Enable the Service Group.

Oracle Data Guard support

AppSync supports an Oracle Data Guard configuration for a primary (source database) and a physical standby (target database) which is open in active or passive/non-active mode.

There are three types of standby databases:

- Physical standby
- Logical standby
- Snapshot standby

All three configurations can be opened in one of the following modes:

- Active standby mode—Standby database in read-only or read/write mode
- Passive/non-active standby mode—Standby database in mounted mode

AppSync currently only supports Data Guard physical standby configuration in active or non-active mode.

When a physical standby database is open in active mode, the standby database can be opened in read-only mode while logs are applied. This action allows you to query the database for information while Data Guard applies logs.

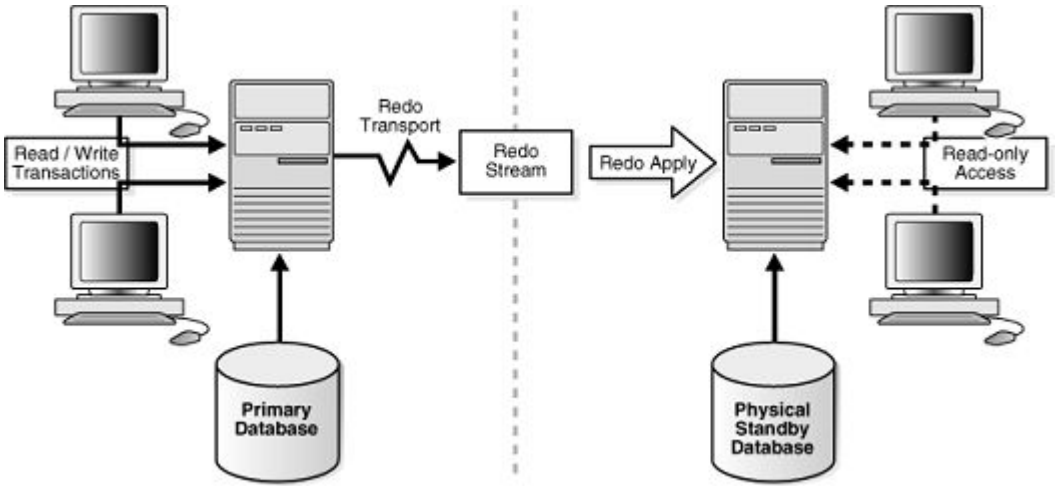
Snapshot and logical standby configurations also allow the database to be open in read/write mode. A passive/non-active setting means that the database can start in mounted mode and logs can be applied in the background.

Physical standby

In a physical standby environment, archive logs are applied when they are received. A physical standby has a 1:1 mapping of the file and storage layout from primary to standby. A physical standby database can be open in both read-only or mounted mode which means it can be either an active or passive/non-active configuration.

The following diagram displays a typical primary/standby (source/target) Data Guard configuration:

Figure 14 Physical standby environment



Copy Management

On the AppSync console, go to the **Copy Mangement** › **Oracle** page. A Data Guard relationship column now displays. If you have an existing Data Guard relationship, you can view two databases that are part of a Data Guard configuration. One database is the primary database and one is the physical standby (non-active)database.

Review the following copy management considerations for Data Guard:

- To protect a primary Data Guard database (source database), create a copy like any other standalone database. You can take a hot backup copy.
- For protection of an active standby Data Guard database (Target Database): Protection in hot backup mode of an active standby database is not allowed because the standby database is in read-only mode. Also, the standby database contains up-to-date archive logs and is an exact copy of the primary and does not require archive logs to be copied for recovery. You can however take a non-hot backup copy of a Standby database.
- For protection of a passive/non-active standby Data Guard database (target database): A passive/non-active standby database operates the same way as an active standby database. Hot backup copy of the database is not allowed. The difference here is that the copy is created from the mounted database without opening the database in read-only or read/write mode.
- Creating a copy of a mounted database only succeeds for a passive/non-active Data Guard standby database in mounted state. Standalone Oracle databases that are mounted cannot be protected. They appear as offline on the database protection page of the console.

Mount and restore (recover)

Review the following mount and restore considerations for Data Guard:

- For a primary database (Source database): Mount and restore operate the same way with a Primary Data Guard database as any Oracle Standalone database. If you use

RAC to configure the Primary database then the RAC mount/restore rules for AppSync apply.

- For an active standby database (target database): Mount and restore operate the same for an active standby Data Guard database as any other Oracle standalone database. If the standby database is configured using RAC then the RAC mount/restore rules for AppSync apply.
- For a passive/non-active standby database (target database): Mount and restore operate the same for a passive/non-active standby Data Guard database as any other Oracle standalone database. If the standby database is configured using RAC, then the RAC mount/restore rules for AppSync apply.

Note

If you mount and restore either a primary or standby database, the database appears on the console as a standalone Oracle database. No Data Guard configuration persists.

Repurposing (copy or a copy) Data Guard databases

For general repurposing information, refer to the AppSync user documentation.

Review the following repurpose considerations for Data Guard:

- Repurposing a primary database (source database): Repurposing operates the same for a primary Data Guard database like any Oracle standalone database.
- Repurposing an active standby database (target database): Repurposing operates the same for an active standby Data Guard database as any Oracle standalone database. You cannot hot backup a standby database for a repurposed copy.
- Repurposing a passive/non-active standby database (target database): repurposing operates the same for a passive/non-active standby Data Guard database as any Oracle standalone database. You cannot hot backup a standby database for a repurposed copy.

Restore Data Guard databases

Restore for a primary database (source database): Restore for a primary Data Guard database operates the same way for any Oracle standalone database. Manually recover the database and then resynchronize the primary and standby databases after the AppSync restore process completes.

Veritas Cluster Services integration

AppSync can work with standalone Oracle databases that are configured to failover from node to node in a VCS (Veritas Cluster Services) environment.

Introduction

During a replication process, if the node that was used to create the service plan is not accessible, AppSync runs the replication on another node in the cluster. AppSync does not rely on the Virtual IP of the Oracle service group. Therefore, register all nodes in the VCS cluster to the AppSync server before you replicate the database.

From a restore perspective, AppSync can only restore to the node where the copy was originally created. The original node must be active, otherwise the restore process fails.

Requirements

The following are the requirements for using a standalone database that fails over as part of a VCS cluster:

- Install the AppSync host plug-in on all nodes of the cluster.
- Configure the IP resource in the Oracle service group for a clustered database.

- If a failover occurs while running a replication or restore process, then the operation fails. Node failover occurs before running a service plan, before the start of a replication, or a restore.
- The Oratab file should have an entry for all possible SIDs that can run on the specified node (passive and active instances).
- Ensure `tnsnames.ora` files on all nodes contain entries of all standalone instances, including the virtual IP address of the Oracle service group (per Symantec documentation).
- The following files should be accessible to all nodes on the cluster where the database runs:
  - Database `init/spfile`
  - Password file
- Install package `sg3_utils`, which contain utilities to access devices that use SCSI command sets, on all nodes.

Mount considerations

- The mount host must not be part of the VCS cluster.
- The mount host requires installation of VxVM Storage Foundations minimum 6.1.
- The package `sg3_utils`, which contain utilities for accessing devices that use SCSI command sets, must be installed on the mount host.

Restore considerations

AppSync can only restore to the node where the copy was originally created, therefore the original node must be active. To perform a restore in a VCS environment, follow these steps:

1. Freeze the Oracle service group: `>hagrp -freeze <service_group_name>`
2. Perform the restore.
3. Start the instance.
4. Perform a manual recovery.
5. Open the database.
6. Unfreeze the Oracle service group: `>hagrp -unfreeze <service_group_name>`.

Note

AppSync can only restore to the node where the copy was originally created, therefore the original node must be active. Otherwise, the restore process fails, and leaves the database in a corrupt state. The console provides a detailed message warning you of this scenario before the restart of the restore.

HACMP cluster integration

AppSync can work with standalone Oracle databases that are configured to failover from node to node in an IBM® HACMP cluster environment.

Introduction

AppSync protects the database on the node where the current state is active before the Service Plan run. AppSync does not rely on the Virtual IP of the Oracle service group. Therefore, all nodes in the HACMP cluster should be registered in the AppSync server to

replicate the database if the node that was used to create the original copy is not accessible.

AppSync restores to the cluster node where the copy was originally created. The restore process fails if the node is not active during the restore process.

Prerequisites for HACMP environment to work with AppSync

The following are the requirements for protecting a standalone database that fails over as part of a HACMP cluster:

- The AppSync host plug-in must be installed on all nodes of the cluster.
- The IP resource must be configured in the Oracle service group for the clustered database.
- If a failover occurs while running a replication or restore process, the operation fails. Node failover should occur before running the service plan, or at the start of a restore.
- The Oratab file should have an entry for all possible SIDs that can run on the specified node (passive and active instances).
- The following files should be accessible to all nodes on the cluster where the database runs:
  - Database `init/spfile`
  - Password file

Mount considerations

- The mount host must not be part of the HACMP cluster.
- The AppSync host plug-in must be installed on the mount host.

Restore considerations

AppSync can only restore to the node where the copy was originally created, therefore the original node must be active. To perform a restore in an HACMP environment, follow these steps:

1. Freeze the Oracle service group: `>hagrp -freeze <service_group_name>`
2. Perform the restore.
3. Start the instance.
4. Perform a manual recovery.
5. Open the database.
6. Unfreeze the Oracle service group: `>hagrp -unfreeze <service_group_name>`.

Note

AppSync can only restore to the node where the copy was originally created, therefore the original node must be active, otherwise the restore process fails, and leaves the database in a corrupted state. The console provides a detailed message warning you of this scenario before the restart of a restore.

Post restore procedure in an HACMP environment

Learn how to perform manual steps with a restore in an HACMP environment after a restore.

After restore, a file system mounts to the production host in non-concurrent mode. Remove the file system from the resource group, make it a concurrent volume group, and then add it back to the resource group.

Perform these steps on an active node:

Procedure

1. Unmount file system.
2. Execute **`Varyoffvg`**
3. Execute **`Varyonvg`** with -c option (to make it concurrent)
4. Run **`importvg`** on the passive node.

   Verification:
   The `lspv` command should show `vg` as concurrent on both nodes as follows:

```
node 2
hdiskpower8     00c2bfb0f1ee76ca  oradata concurrent
hdiskpower9     00c2bfb0f1f434e3  oralogs concurrent

node 1
hdiskpower18    00c2bfb0f1ee76ca  oradata concurrent
hdiskpower19    00c2bfb0f1f434e3  oralogs concurrent
```

5. Add file system back to resource group.
6. Verify and synchronize configuration.

Prerequisites and supported configurations

Learn about prerequisites and supported configurations for Oracle with AppSync. Included is information about supported device configurations, Oracle on file systems, logical volume managers and ASM-based storage, RecoverPoint consistency group-based storage, Linux and AIX-based configurations including sudo user, and support for virtualization setups.

AppSync can create application-consistent (using Oracle hot backup) and crash-consistent (without hot backup) copies. For AppSync to create app-consistent copies of Oracle databases, the data files and archive logs must not share the file system, volume group, ASM disk group, RP consistency group, or data store. If the Oracle configuration is such that the data files and archive logs share any of these groupings, then AppSync can create crash-consistent copies for such databases.

When using VNX, ensure all consistency groups are VNX consistency groups. When using ViPR controller, ensure all consistency groups are ViPR consistency group. Additionally, the archive log files must be on a different CG from the rest of the database files.

Oracle on file system-based storage configurations

Some examples of Oracle configurations for which AppSync can offer both app-consistent as well as crash-consistent copies follow:

- Single database: database files on, for example, `/data`; archive log files on, for example, `/archive`.
- Multiple databases sharing single archive log location: for example, Database 1 on `/db1`, Database 2 on `/db2`, archive logs on `/arch`.
- Multiple databases sharing data location and archive log locations: for example, Database 1, 2, 3 files on `/data`, database 1, 2, 3 archive log locations on `/archive`.
- Affected databases scenario: Two filesystems on one volume group with two more filesystems on another volume group, such that one Oracle database has data on fs1 in vg1 and logs on fs1 on vg2 and second Oracle database has data on fs2 on vg1 and logs on fs2 on vg2.

Note

AppSync does not support the following configuration: one oracle database has data files on fs1 in vg1 and logs on fs1 on vg2, and a second Oracle database has data files on fs2 on vg2 and logs on fs2 on vg1.

Oracle on logical volume managers-based storage configurations (LVM/VxVM)

- Single database: Database files on a volume in, for example, `datavg`, and then archive log files in a volume on, for example, `archvg`.
- Multiple databases sharing single archive log location: Database 1 files on a volume in, for example, `data1vg`, and Database 2 files on a volume in, for example, `data2vg`, and then archive logs in a volume on, for example, `archvg`.
- Multiple databases sharing data location and archive log locations: Databases 1, 2, 3 files in a volume on, for example, `datavg`, and then Database 1, 2, 3 archive log locations in a volume on, for example `archvg`.

Oracle on ASM-based storage configurations

- Single database: Database files on, for example, diskgroup `+data`, then archive log files on, for example, diskgroup `+arch`.
- Multiple databases sharing a single archive log location: Database 1 files on, for example, diskgroup `+data1`, and database 2 files on, for example, diskgroup `+data2`, then archive logs on, for example, diskgroup `+fra`.
- Multiple databases sharing a single archive log location: Database 1 files on, for example, diskgroup `+data1`, and database 2 files on, for example, diskgroup `+data2`, then archive logs on, for example, diskgroup `+fra`.

Oracle on RecoverPoint consistency group-based storage

- Single database: Database files on LUNs in RP consistency group, for example, `DATACG` and archive log files in RP consistency group, for example, `ARCHCG`.
- Multiple databases sharing single archive log location: Database 1 files on LUNs in RP consistency group, for example, `DATA1CG`, then database 2 files on LUNs in RP consistency group `DATA2CG` and then archive log files in RP consistency group, for example, `ARCHCG`.
- Multiple databases sharing data location and archive log locations: Database 1, 2, 3 files on LUNs in RP consistency group, for example, `DATACG`, then database 1, 2, 3 archive logs on LUNs in RP consistency group, for example, `ARCHCG`.

Oracle on datastore-based storage layouts

- Single database: Database files on vDISKs from data store, for example, `DATADS` and archive log files on vDISKs from data store, for example, `ARCHDS`.
- Multiple databases sharing single archive log location: Database 1 files on vDISKs from data store, for example, `DATA1DS`, then database 2 files on vDISKs from data store `DATA2DS` and then archive log files on vDISKs from data store, for example, `ARCHDS`.
- Multiple databases sharing data location and archive log locations: Database 1, 2, 3 files on vDISKs from data store, for example, `DATADS`, then database 1, 2, 3 archive logs on vDISKs from data store, for example, `ARCHDS`.

Oracle on VNXe LUN Group-based storage

The following configurations are supported

- Single database: Database files on LUNs in VNXe LUN group, for example, data files in LUN Group DATALUNGRP and archive log files in LUN group ARCHCG.
- Multiple databases sharing single archive log location: Database 1 files on LUNs in VNXe LUN group, for example, DATA1LUNGRP, then database 2 files on LUNs in VNXe LUN group DATA2LUNGRP, and then archive log files in VNXe LUN group, for example, ARCHLUNGRP.
- Multiple databases sharing data location and archive log locations: Database 1, 2, 3 files on LUNs in VNXe LUN group, for example, DATALUNGRP, then database 1, 2, 3 archive logs on LUNs in VNXe LUN group, for example, ARCHLUNGRP.

Supported virtualization configurations

AppSync supports protection, mount, and restore of Oracle databases on vDisks in standalone and RAC.

AppSync does not support configuration where data and archive logs are on mix of RDM and VDisks.

Considerations:

- For Oracle databases on VDisks on VMs on ESX:
  - Disable the `VMFS3hardwareaccelated` locking flag on the ESX that is hosting the VMs hosting the Oracle databases on vDisks.
  - If ATS locking is enabled for VMFS3/5 datastore, AppSync datastore mount fails.
- To run SCSI commands from AppSync, set `disk.EnableUUID` on the VM.
- Ensure your VM datastore does not share the same VMFS as your Oracle databases

Note

AppSync does not support the following configurations:

- ASM database on VXVM volume groups
- ASM database on VXDMP devices
- ASM database on raw devices under the control of VXVM
- Non-ASM database on Native LVM volume group residing on VXDMP devices

Support for Oracle on VMware virtual disks

You can protect, mount and restore Oracle standalone and clustered databases residing on VMware virtual disks.

Consider the following information when working with Oracle and VMware virtual disks.

- For successful mapping, add the vCenter to the AppSync server and then perform discovery before adding the Oracle host. Otherwise you must rediscover the Oracle host after adding the vCenter.
- For successful protection, log files and database files must reside on virtual disks. There cannot be a combination of physical and virtual storage.
- AppSync **does not** support:
  - NFS datastores
  - Protection of Oracle databases across virtual machines sharing the same datastore
- To perform Oracle mount and recovery to a virtualized host, you need VMware permissions to modify the VMware configuration of the mount VM (create RDM / SCSI adapter), as well as rescan datastores/VMFS.

Refer also to Oracle vDisk restore with affected entities on page 152.

Support for VIO vSCSI

Oracle with AIX LPARs can now also use "virtual" connections to the storage.

Overview: Support for VIO (Virtual I/O disk) vSCSI
Previously, AppSync supported Oracle on AIX physical machines and on AIX virtual machines (LPARs) that use physical or NPIV connections to the array storage. AppSync now supports Oracle AIX LPARs with virtual connections.

All supported applications and use cases for AIX Hosts using physical or NPIV storage connections are now also supported on VIO VSCSI devices. Two restrictions apply to this support:

- Mounting of replicas must be done to mount hosts using physical or NPIV storage connections. Mounts cannot be created as virtual disks .
- The VIO Server must map whole raw disks to the VIO Clients. Do not map logical volumes from the VIO Server.

In addition AppSync can coexist with AIX Live Partition Mobility. AppSync will continue to protect and repurpose applications after the migration of a client partition to a new managed server.

Supported versions
When referring to an AppSync support matrix, AIX Virtual I/O disks are supported as a valid virtual disk type known as Virtualization Server Solutions.

Protecting a database

To protect a database, subscribe it to an AppSync service plan.

You can protect objects in different ways from different places in AppSync:

- Select **Subscribe to Plan and Run** when you want to protect a selected database immediately. The service plan is executed for that database alone.
- Select **Subscribe to Plan** when you want to schedule protection for later. Protection for databases that are part of a service plan is executed at a scheduled time.
- Select an appropriate service plan from **Create copy** using a plan in the database Copies page.
- Select **Run** from the Oracle Service Plans page to run the entire plan immediately.

Discovering databases

To keep AppSync up-to-date, you should discover databases on the Oracle server when there is creation, deletion, or renaming of databases.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Oracle** to display the Databases page.

   Only databases that are started and are in an open state show up as online on the databases page. Databases that do not have an entry in the `/etc/oratab` file as well as shutdown databases do not appear.

2. From the **Discover Databases** drop-down menu on the bottom left of the screen, click **On Server**, and then click on the desired server where the database you want to discover resides.

Subscribe a database to a service plan

You can subscribe a database to a service plan and run the service plan immediately, or schedule the service plan to run at a later time.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Oracle**.
2. Select one or more Oracle databases.
3. From the **Protect** popup button, select the appropriate service plan, for example:

Table 12 Sevice plan protection options

Option	Description
Subscribe to Plan and Run	To subscribe the database for protection and run the plan immediately for any selected database(s).
Subscribe to Plan	To subscribe the database for protection. Protection for all databases that are part of the service plan is executed at the scheduled time.

Unsubscribe database from a service plan

When you unsubscribe an individual database from a service plan, AppSync retains all existing database copies; only further protection will be removed.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Oracle**.
2. Select the database to unsubscribe from a service plan.
   - Select the plan to unsubscribe from: **Protect** › **Unsubscribe from Plan**. Only plans to which the database was subscribed appear in the popup list.
   - To unsubscribe from all service plans, select **Unsubscribe from Plan** › **All**.

Oracle copies page

You can see details of a copy from the Copies tab of the Service Plan. The list of copies can be filtered by time of creation, and by service plan.

Table 13 Copy page fields

Column	Description
Status	• Green: successful

Table 13 Copy page fields (continued)

Column	Description
	• Yellow: completed with errors • Red: failed
Name	Name of the copy. The copy name is the time AppSync created it.
Service Plan	Name of the service plan associated with the copy.
Label	Label assigned to the copy in case of repurposing.
Application Consistent	• Yes, if database was successfully put in hot backup mode while creating the copy. • No, if hot backup mode was not selected in the Create Copy phase. • No, if hot backup mode was selected and database failed to go into hot backup mode.
Mount Status	Status of the copy: mounted or not mounted. If mounted, the name of the mount host displays.
Recovery Status	Was copy recovered post mount or not. Values are: • Not Recovered - copy was not mounted or copy was a filesystem mount. • Successful - recovery was successful. • Failed - recovery failed.
Copy Type	• CDP Bookmark • CRR Bookmark • VNX Snap, VNXeSnap • VMAX Clone • VMAX Snap • VMAX V3: SnapVXSnap, SnapVXClone • XtremIO Snap • ViPRSnap
Generation	First or second generation copy - for repurposing
Source	Production database (for first generation copy) or a copy of a copy (second generation) copies.
Site	RecoverPoint site information.
Storage System	Array serial number/name

Viewing database copies

Follow these steps to view an Oracle database copy on the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Oracle**
2. Click a database to view existing copies of the database.

   You can see details of a copy from the Copies tab of the Service Plan. The list of copies can be filtered by time of creation, and by service plan.

Creating a database copy from the Copies page

Create a copy of a database by subscribing it to an AppSync Oracle service plan from the **Copies** page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **Oracle**
2. Click a database to view existing copies.
3. From the **Create a copy using a service plan** list, select the appropriate service plan.

   The service plan runs immediately for the selected database.

Expiring a database copy on demand

Expiring a database copy removes it from the AppSync database and can free up storage, depending on the replication technology and copy state.

Before you begin

This operation requires the Data Administrator role in AppSync.

Expiring a copy that was made with RecoverPoint does not remove the corresponding bookmark from RecoverPoint itself.

Procedure

1. Navigate to **Copy Management** › **Oracle**.
2. Click the desired database for copy expiration.
3. From the **Copies** page, select one or more copies to expire.

   You can also perform this action from the service plan's **Copies** tab.
4. Select **Expire** from the row of buttons on the lower part of the screen.
5. Verify that you selected the appropriate copy, and any associated copies that are also listed and confirm.

Service plan summary and details

The service plan **Settings** tab shows the name, description, schedule, and status of the service plan.

Click the phases for detailed service plan settings and other tabs for information about subscriptions, lists of copies and events generated by the plan.

Review Overview: Service Plan on page 10 for more service plan copy information.

Service plan schedule

The schedule of a service plan is set in the **Plan Startup** phase. The **Startup Type** (scheduled or on demand) determines whether the plan is run manually, or configured to run on a schedule.

Options for scheduling when a service plan starts include:

- Specify a recovery point objective (RPO).
  - Set an RPO of 30 minutes or 1, 2, 3, 4, 6, 8, 12, or 24 hours
  - Set minutes after the hour in 5 minute intervals.
  - Default RPO is 24 hours.
- Runs every day at specific times.
  - Select up to two different times during the day.
  - Select minutes after the hour in 5 minute intervals.
  - There is no default selected.
- Run at a certain time on selected days of the week.
  - You can select one or more days of the week (up to seven days).
  - There is no default for day of the week. Default time of day is 12:00 AM.
- Runs at a certain time on selected days of the month.
  - Select one or more days of the month (up to all days).
  - Select one time of day. Available times are at 15 minute intervals.
  - Default is the first day of the month.

Overriding service plan schedules

You can set individual schedules for databases subscribed to a service plan by overriding the generic recurrence setting.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

You can only override the settings of the recurrence type previously selected for the service plan.

Procedure

1. Navigate to **Service Plans** and select one of the plans from the list.
2. From the **Settings** tab, select the **Plan Startup** phase.

   The **Plan Startup Defaults** pane appears on the right.
3. Note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Scheduled** was set as the **Startup Type**.
4. Select the **Start service plan phase**.

   You will see the Start service plan pane on the right.
5. Note the Recurrence Type selected for the plan.

   A recurrence type can be set only if **Automatic** is selected in the **Startup** phase.

6. Click the Plan Startup Overrides tab.

   You can view the list of all databases subscribed to the plan.

7. Select one or more databases and click **Override Schedule**.

   The Override Schedule dialog appears.

8. Set the schedule based on your requirement and then click **OK**.

   For example, if the default recurrence type is for specified days of the month, and the rule setting is to Run at 12:00 AM on the 1st day of every month, you can override the time and the day for individual datastores.

Results

A Pencil icon indicates that default settings have been overidden.

Application discovery

Before creating the database copy, AppSync examines the Oracle database on the host to look for changes such as addition, removal, and shutdown or for changes in open status.

A database is protected only if it is in the ONLINE state. This means the database(s) must be in **open** mode (databases started in **nomount** mode or in **mount** mode and offline databases are not protected).

There are no user settings associated with this phase and it cannot be disabled.

Application mapping

After discovering the application, AppSync maps it to array storage, and protection services such as RecoverPoint.

There are no user settings associated with this phase and it cannot be disabled.

Storage preferences

Sets the preferred order of storage technology to use while creating copies, for example, VNX Snapshot or VMAX-Clone/Snap or RecoverPoint Bookmark.

Use the **Move Up** and **Move Down** buttons. Copies are made using the first technology preference when possible. If conditions are such that the first technology can no longer be used, then any remaining copies will be handled by the next preference instead. For example, if your first preference was a bookmark but not all the application data in the service plan could be mapped to RecoverPoint, then AppSync uses Snap instead.

Note

A single service plan can contain a mix of datasets configured on VNX/VMAX block/file and RecoverPoint. For example, with VNX, if you have a Bronze service plan for Oracle, the databases subscribed can on a mix of RecoverPoint and VNX/VMAX block objects.

A database mix of VNX and VMAX is not supported. Also to get an RP bookmark copy for a database, all LUNs in that database should be configured with RecoverPoint protection; if not Snap copies are created for that database.

Pre-copy script

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters on a service plan's **Settings** tab.

The pre-copy script runs according to the schedule set in the **Plan Startup** phase. AppSync executes this script once per host per service plan run on the production host.

All script phases are non-blocking, which means that even if they fail, service plan execution does not terminate and the next phase continues.

This operation requires the Data Administrator role in AppSync.

For a successful script run ensure:

- The script phase is enabled.
- The script exists in the specified path. You provide absolute path to script; there is no default location.
- You use valid script formats: all executables on UNIX are supported. The script requires execute permissions for the specified user.
- The pre-copy script runs per the schedule set in the Plan Startup phase.
- The script runs as Local System by default for Windows only.
- The script does not put the database/tablespaces in backup mode.
- The script does not shut down the database.

Table 14 Pre-copy script console fields

Field in UI	Description
Full path to script	The complete path to the script location.
Script parameters	Parameters that will be passed to the script during the run.
Run as username	User that has execute permissions on the script.
Password	Password of the user.

Create copy

The Create Copy phase creates a copy that is based on the replication technology that is specified in the service plan.

The Create copy phase specifies the backup type for the Oracle database copy that AppSyncs creates including: Snap (VNX Snapshot, XtremIO Snapshot, VNX File SnapSure, TimeFinder VP Snap), Clone (TimeFinder Clone), or bookmark (RecoverPoint CDP/CRR/CLR) .

This phase also sets the period for automatic expiration of the copies.

There are three types of copy phases depending on which plan you use :

- Create local copy—For Bronze service plans, creates a local copy on the production storage system or local site. Copy type includes:
  - Snap—VNX Snapshot, VNX File SnapSure, TimeFinder VP Snap, XtremIO Snapshot, VNX2e Advanced Snapshot, ViPR Snapshot, VMAX3 SnapVX Snapshot in NoCopy mode
  - Clone—TimeFinder Clone
  - Bookmark—RecoverPoint RecoverPoint Continuous Data Protection, VMAX3 SnapVX snapshot in Copy mode
    - Source VNX volume, target VNX volume—virtual and virtual with roll access modes are supported.
    - VMAX V3 with RecoverPoint is not supported. VMAX V2 with RecoverPoint is supported in 2.2.2 and later.

- Create remote copy—For Silver service plans, creates a remote copy on the remote storage system (across RemoteReplicator or SRDF) on remote site. Copy type includes:
  - Bookmark—RecoverPoint RecoverPoint Continuous Remote Replication
    - Source VNX volume, target VMAX volume—virtual and virtual with roll access modes are not supported.
    - Source VMAX volume, target VNX volume—virtual and virtual with roll access modes are supported.
- Create local and remote copy—For Gold service plans, creates both local and remote copies. Copy type includes:
  - Snap— VNX File SnapSure
  - Clone—TimeFinder Clone
  - Bookmark—RecoverPoint CLR

Automatic expiration of copies

The automatic expiration value in a service plan **Create Copy** phase specifies the maximum desired number of Snap, Clone or Bookmark that can exist simultaneously.

When the "Always keep x copies" value is reached, older copies are expired to free storage for the next copy in the rotation. Failed copies are not counted. AppSync does not expire the oldest copy until its replacement has been successfully created. For example, if the number of copies to keep before expiration is 7; AppSync does not expire the oldest copy until the 8th copy is created. AppSync does not expire copies under the following circumstances:

- Mounted copies are not expired.
- A copy that contains the only replica of a database will not be expired.

This setting is independent of any storage policy setting (for example the VNX pool policy settings in Unisphere for automatic deletion of oldest snapshots.) The service plan administrator should work with the storage administrator to ensure that the Storage policy settings will enable the support of the specified number of snap copies for that application.

Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations.

Note

If this option is not selected, then RecoverPoint copies accumulate, and remain until the bookmarks fall off the RecoverPoint appliance.

Post-copy script

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters in the service plan **Settings** tab.

The pre-copy script runs as per the schedule set in the **Plan Startup** phase. You can execute this phase once per host per service plan run. If this script phase is enabled but the permissions to run it are improper, or if the script does not exist in the specified path, the Service Plan run fails with appropriate error.

This process requires the role of AppSync Data Administrator. AppSync executes this script once per host per service plan run on the production host.

All script phases are non-blocking, which means that even if they fail, service plan execution does not terminate and the next phase continues.

For a successful script run ensure:

- The script exists in the specified path. You provide absolute path to script; there is no default location.
- You use valid script formats: all executables on UNIX are supported. The script requires execute permissions for the specified user.

Table 15 Post copy script console fields

Field in UI	Description
Full path to script	The complete path to the script location.
Script parameters	Parameters passed to the script during the run.
Run as username	User that has execute permissions on the script.
Password	Password of the user.

Unmount previous copy

The service plan unmounts a previously mounted copy after creating the new copy.

The exception is a copy that was mounted on-demand instead of mounted by the service plan; in this case the on-demand mounted copy is not unmounted.

All the recovered databases are shut down as part of this phase. There are no user settings associated with this phase and it can be enabled or disabled.

Pre-mount script

You can enable this phase if you want to run a script prior to AppSync performing a mount operation.

This script will be executed once per host per service plan run. If you enable the script phase but the permissions to run it are improper, or if the script does not exist in the specified path, the service plan run fails with appropriate error.

Show caution when using several mount hosts in a Service Plan run. (Refer to Overriding mount settings on a service plan on page 142. You must select **Same as mount host** in the **Run on host** option so that the script runs on all mount hosts.

Table 16 Pre-mount script field descriptions

Field in UI	Description
Full path to script	The complete path to the script location
Script parameters	Parameters passed to the script during the run
Run as username	User with execute permissions on the script
Password	Password of the user
Run on host	Host where the script needs to run. Select **Same as mount host** if several mount hosts are involved.

Mount copies

The Mount copy phase either mounts the copy or mounts and recovers the copy. This phase can be enabled or disabled.

In Mount Copy Defaults settings, you can set values to Mount copy or Mount and recover copy.

For **Mount copy settings**, you can set the mount host value and mount path and the RecoverPoint image access type.

For **Mount and recover copy** settings, you specify the recovery instance, the type of recovery, and the database naming details. Other settings are similar to the Mount copy settings such as mount path and image access type.

For **Mount on standalone server and prepare scripts for Manual Recovery** Oracle mount option, if you enable script phase after the mount operations completes AppSync creates scripts on the mount host that you run to recover the database. The scripts are two types, RMAN and SQL. The scripts are created under `/tmp/<MOUNTED_SID_NAME>/RecoveryScripts`.

Console field descriptions:

- **Host name**: This field is used to specify the host where you want to mount the Oracle copy.
- **Mount to path**: The path on which to mount database files and file systems. For ASM RAC, this setting is unused/ignored.
- **Service Level Objective (SLO)**: If you are using a VMAX 3 array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.
- **Database name**: This field represents the format of the mounted database name. To specify the original database name use the token **`%DB%`** . For example: To use the original name that is prefixed by TEST, use **`TEST%DB%`**.
- **SID name**: This field represents the format of the mounted instance name. To specify the original instance name use the token **`%SID%`**. For example: To use the original name that is prefixed by TEST, use **`TEST%SID%`**.
- **ASM Diskgroup**: This field represents the format of the ASM disk group. To specify the original disk group name use the token **`%DG%`**. For example: To use the original name that is prefixed by TEST, use **TEST%DG%**.
- **Custom initialization parameters**: This field is a multi-line field which allows you to specify settings which override any original database setting on the mounted database copy. This field is useful for editing options such as memory settings.

Overriding mount settings in a service plan

If multiple registered databases are subscribed to the same plan, you can select different mount settings for each database, overriding the generic settings. Recovery settings cannot be overridden.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Service Plans** › **Oracle** and click one of the service plans from the list.

2. From the **Settings** tab, select **Mount copy** phase.
3. On the right pane, select the **Mount Copy Overrides** tab.

   The list of servers includes all Oracle hosts whose databases are subscribed to this plan.
4. Select the server for settings override, and then click **Set Overrides**.

   The Override Default Mount Settings dialog displays.
5. Select options for the mount settings that you want to override.

   Fields that do not have a selection; they retain their default settings.
6. Click **OK**.

   A pencil icon appears in the first column of the row of the server with your changed settings.
7. To revert back to default settings for a server, click **Use Default Settings**.

Post mount script

You can enable this phase if you want to run a script after AppSync performs a mount operation.

This script will be executed once per host per service plan run. If you enable the script phase but the permissions to run it are improper, or if the script does not exist in the specified path, the service plan run fails with appropriate error.

Show caution when using several mount hosts in a Service Plan run. (Refer to the Overriding mount settings on a service plan section. You must select **Same as mount host** in the **Run on host** option so that the script runs on all mount hosts.

Table 17 Post-mount script field descriptions

Field in UI	Description
Full path to script	The complete path to the script location
Script parameters	Parameters passed to the script during the run
Run as username	User with execute permissions on the script
Run on host	Host where the script needs to run. Select **Same as mount host** if several mount hosts are involved.

Unmount copy

The final phase in the service plan unmounts the copy.

This phase is disabled if the **Unmount previous copy** phase is enabled. There are no user settings associated with this phase.

If you have chosen to mount with recovery options (standalone, RMAN, or cluster mount) in the **Mount copy** phase, all the mounted databases are shut down as part of this phase.

Mount an Oracle copy

Before performing an oracle mount on a standalone server, you need to understand the AppSync console Mount fields and their meanings.

Mount operations

Table 18 Console field descriptions

Field	Description
Mount on Server	The server on which to mount the copy.
Mount path	The Default Mount Path is `/appsync`. The mount path could also be **Same as Original Path**. However, this option is not available when the mount host = production host. You can also change Default Mount Path, for example, `/EMC` instead of `/AppSync`.
Image access mode (during RecoverPoint mount)	• Logged access: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host. Virtual access with RP-VMAX, is not supported. • Virtual access with roll: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. With RP-VMAX, and RP-XtremIO, virtual access with roll is not supported. • Virtual access: provides nearly instant access to the image; it is not intended for heavy processing. With RP-VMAX, and RP-XtremIO, virtual access is not supported.

You can mount a copy created on any multipathing device production host, and mount it on any multipathing device mount host. This means you can create a copy on Block/ PowerPath/MPIO devices and mount it on a mount host with any of these combinations.

For DMP, make sure you install DMP on both production and mount hosts.

Addition server information

- With AppSync 2.2.1 and above, you can configure a temporary location per UNIX host from the AppSync console in the Servers page.
  - AppSync uses the set temporary location during Oracle mount operations for storing information that previously resided in `/tmp/<SID>/`.
  - **`/tmp/`** is the default temporary location unless you specify otherwise.

Mounting a copy using the Oracle Mount wizard

From the AppSync console, you can perform a mount of a copy using the Oracle Mount wizard .

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the Databases page, select **Recover** › **Mount a Copy**.

   A list of the Oracle database instances appears.

2. From the Copies page, select a copy and click **Mount**

   The Oracle Mount wizard launches.

3. Use the **Copies** or **Service Plan** or **Type** filters to select the copy to mount.

   The copies list is refreshed based on the filters selected.

4. Select the wanted copy to mount. (For a RecoverPoint copy, you also have the option to select a bookmark that is based on a specific time, however, ensure that there is a copy available in AppSync.) Select the copy, and click **Mount** to launch the **Mount Copy of Oracle** wizard.

5. Click **Select a point in time** to select a copy with a specific timestamp. The time that is shown here is the console's time. If the console is in a different time zone from the RecoverPoint Appliance (RPA), specify the time in the server's time zone to mount the copy.

6. From the Mount Options page, Mount operation drop-down list, select one of the following options: **Mount on standalone server**, **Mount on standalone server and create RMAN catalog entry**, **Mount on standalone server and recover**, **Mount on standalone server and prepare scripts for manual recovery**, or **Mount on grid cluster and recover as RAC database**.

   If you select **Mount on standalone server and recover**, **Mount on standalone server and prepare scripts for manual recovery**, or **Mount on grid cluster and recover as RAC database** , with read/write open mode for recovery, the **Create TempTable Space** option is enabled. This option is used to create the TEMP TableSpace on the recovery-mounted database copy. After you select Create TEMP TableSpace, AppSync shows two other options:

   a. Number of TEMPFILES': Number of files to be added to TEMP TableSpace, each of size specified in 'Size of each file' option

   b. The `size_clause` specifies a number of bytes, kilobytes (K), megabytes (M), gigabytes (G), terabytes (T), petabytes (P), or exabytes (E) . The `size_clause` allows you to establish amounts of disk or memory space, for example 10M. The size of the `TempTable Space` equals the Temp table file that is multiplied by the size of each file . For example, if the Temp table file count = 2 and the size of each file = 10M, the TempTable Space Size = 20M.

   AppSync generates the name of the `TempTable Space` in the form of `<DBNAME>_TEMP`. This newly created TableSpace is set as the default TEMP TableSpace of the mounted database instance. During unmount, AppSync drops the created TEMP TableSpace.

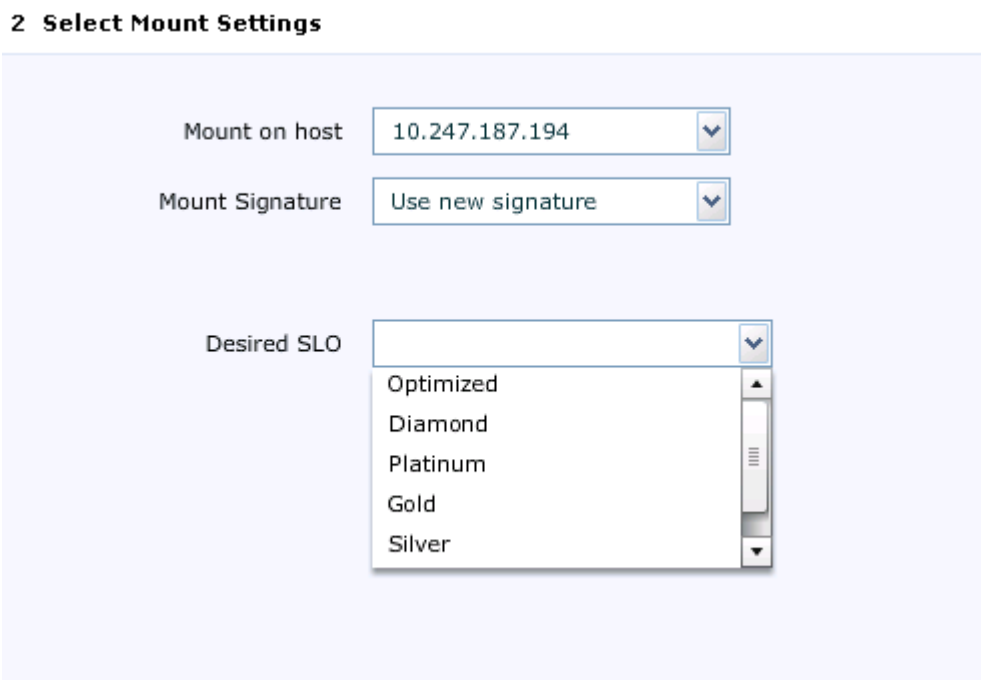
Note

- With manual recovery mount, scripts are prepared to both create ('Step-5_createTempTableSpace.sql') and drop ('Step-6_dropTempTableSpace.txt') TEMP TableSpace. You should drop the created TEMP TableSpace manually before unmounting a copy with AppSync.
- If AppSync fails to drop the TEMP Tablespace during unmount, and if a restore operation is performed using this copy, the tablespace is restored.
- If you attempt to restore a RecoverPoint copy, the TEMP TableSpace, if created during mount with recovery, is also restored to production. You should drop the TEMP TableSpace manually from the mounted database copy, and then attempt a restore.

7. Review the default Mount and Recovery settings and make changes if wanted.

   For VMAX 3 arrays, you are presented with an SLO drop-down list. You can select the Service Level Objective (SLO) for the mount copy. If there is a storage group for the mount host with the wanted SLO. AppSync adds the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host. If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices are added to the original storage group when the copy is expired. An example of the SLO menu follows:

   Figure 15 For VMAX3™ select SLO



8. Click **Next** to display the **Summary** page.
9. Review the mount settings and click **Finish** to complete the mount.
10. In the **Results** page, you can view the progress of the different phases that are part of mounting a copy.

The last phase that is completed displays at the bottom of the list.

RMAN cataloging feature

This section includes prerequisites and restrictions for creating RMAN catalog entry, and copying BCT file.

Mount Operation: Mount on standalone server and create RMAN catalog entry

Table 19 Console field descriptions

Field in UI	Description
RMAN user	Catalog owner
RMAN password	Catalog owner's password
RMAN connect string	The TNS alias used to connect to remote RMAN catalog
TNS_ADMIN	Path of the tnsnames.ora file where the TNS alias is specified. (Default Path : $ORACLE_HOME\network\admin\)
ORACLE_HOME	ORACLE_HOME path for the Oracle binaries. Default: Same as production host
ASM Diskgroup Name	Specify prefix or suffix to rename diskgroups on mount host or %DG% (if production ASM diskgroup name is to be used during mount). Default: APS%DG%
Skip Data Files	Skip cataloging of database data files. Default: Not selected.

Notes on prerequisites

- RMAN catalog database must exist and be accessible on the same network as the mount host.
- The `tnsnames.ora` file on the mount host must contain a TNS alias that points to the RMAN catalog database where EMC AppSync should catalog the copy.
- The catalog and catalog owner must be created prior to mounting a copy to be cataloged.
- Production database must be registered in the RMAN catalog before mounting the copy.
- The Oracle version running the RMAN catalog database must be equal to or greater than the highest Oracle version of all production databases registered to that catalog.
- Copies mounted with RMAN integration cannot be renamed using the database rename option. This also implies that only one copy per database can be mounted on a mount host for RMAN cataloging, and **Mount to Original Host** is not possible.
- Copies mounted with Read-only access cannot be cataloged using RMAN.
- Database must be put in hot backup mode.
- **Create backup controlfile** must be selected in **Create Copy** phase.

Mount on standalone server and prepare scripts for manual recovery

This action overrides mount settings on a service plan. This section includes prerequisites and details for performing a standalone mount of an Oracle copy for use with script-assisted manual recovery steps.

Console field description:

- **Mount to server**: This field is used to specify the host where you want to mount the Oracle copy.
- **Mount to path**: The path on which to mount database files and filesystems. For ASM RAC, this setting is unused/ignored.
- **Database name**: This field represents the format of the mounted database name. To specify the original database name use the token **%DB%** . For example: to use the original name prefixed by TEST, use **TEST%DB%**.
- **SID name**: This field represents the format of the mounted instance name. To specify the original instance name use the token **%SID%**. For example: to use the original name prefixed by TEST, use **TEST%SID%**.
- **ASM Diskgroup**: This field represents the format of the ASM diskgroup. To specify the original diskgroup name use the token **%DG%**. For example: to use the original name prefixed by TEST, use **TEST%DG%**.
- **Custom initialization parameters**: This field is a multi-line field which allows the you to specify settings which will override any original database setting on the mounted database copy. This is useful for editing options such as memory settings.

After the mount operations complete AppSync will create scripts on the mount host that you must execute to recover the database. The scripts are RMAN scripts and SQL scripts. The scripts are created in `/tmp/<MOUNTED_SID_NAME>/RecoveryScripts`. The script files are named as `Step-<number>_<operation>.<extension>`. The `<number>` represents the file thas must be run first and so on. The `<operation>` signifies what the script does. The `<extension>` specifies the type of script, either RMAN or SQL. Depending on the type of script, either execute it in RMAN or execute through SQLPlus. The generated filenames follow:

```
Step-1_DatabaseRename.sql
Step-1_DatabaseFileRename.sql
Step-2_RecoverDatabase.rman
Step-3_RecoverDatabase.sql
Step-4_OpenDatabase.sql
```

There is only one Step-1 file created depending on whether the recovery operation was performed using the production SID name or an altered SID name. In order to execute the scripts, follow these steps as an Oracle user:

1. Export the Oracle SID as the SID used during recovery.
2. When executing an SQL script, login to SQLPlus using `sqlplus /` as `sysdba`. You can then run the script: `@/tmp/<MOUNTED_SID_NAME>/RecoveryScripts/Step-<number>_<operation>.sql`
3. When executing an RMAN script, login to RMAN using `rman target=/`. You can then run the script as, `@/tmp/<MOUNTED_SID_NAME>/RecoveryScripts/Step-<number>_<operation>.rman`.

Note

Make sure you follow the order of these steps during recovery.

Mount on cluster and recover

This section includes prerequisites and details for performing a mount of a copy containing an Oracle RAC database as a RAC database on another cluster or, if renamed, back to the same cluster. The settings for this are as follows:

Console field descriptions:

- **Mount to cluster**: This field is used to specify the cluster where you want to mount the copy. Alternatively, it can be Original cluster to mount back to the production cluster.
- **Mount to servers**: You can select a subset of nodes from the selected cluster, or alternatively, all nodes in the cluster that have been added to AppSync.

  Note

  AppSync will only mount to cluster nodes which have been registered; unregistered nodes will not be used.

- **Mount to path**: For ASM RAC, ignore this setting
- **Database name**: This field represents the format of the mounted database name. To specify the original database name use the token **`%DB%`** . For example: to use the original name prefixed by TEST, use **`TEST%DB%`**.
- **SID name**: This field represents the format of the mounted instance name. To specify the original instance name use the token **`%SID%`**. For example: to use the original name prefixed by TEST, use **`TEST%SID%`**

  Note

  For RAC mounts, each node in the cluster receives a unique instance name, postfixed by an numeral.

- **ASM Diskgroup**: This field represents the format of the ASM diskgroup. To specify the original diskgroup name use the token **`%DG%`**. For example: to use the original name prefixed by TEST, use **TEST%DG%**.
- **Custom initialization parameters**: This field is a multi-line field which allows you to specify settings which will override any original database setting on the mounted database copy. This is useful for editing options such as memory settings.

Mount/unmount VMAX 3 copies

Mount/unmount operations on VMAX 3 include masking/unmasking LUNs or a set of LUNs to a host. AppSync relies on the VMAX 3 Auto-Provisioning capability.

The mount host must be zoned to the VMAX 3 array. Next, you can create a masking view with the initiator group, port group, and storage group.

When AppSync performs a mount operation on VMAX 3, it discovers the host initiator for the mount host first, then based on this host initiator, AppSync maps to (or from) the masking view. This operation determines the storage group where the target LUNs are masked/unmasked . For RDM or Vdisk mount/unmount, AppSync identifies the masking view that is based on the host initiator for the ESX server.

You can select the wanted Service Level Objective (SLO) for the target LUN in the mount phase of the service plan. If there is a storage group for the mount host with the wanted SLO, AppSync adds the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host.

If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices are added to the original storage group when the copy is expired.

Restoring an Oracle copy

You can perform a restore of an Oracle copy using the Oracle Restore wizard from the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Note

For AppSync 2.2.2 and later and XtremIO 4.0 and later the Restore button is enabled in the wizard for automated restore. If you are restoring two copies, one for XtremIO 3.x and another for XtremIO 4.0 AppSync restores only the 4.0 copy (warning for 3.x copy appears).

Procedure

1. On the AppSync console, click the **Copy Management** tab, then select **Oracle** from the drop-down list.

   A list of the Oracle database instances appears.
2. Select a database to open the **Copies Page** page for the selected Oracle database which lists available copies with dates of copy.
3. Select the desired copy, and then click **Restore** to launch the **Oracle Restore** wizard.

   You may receive the following warning message: `You are attempting to perform a restore on a cluster. Please follow the instructions in the AppSync documentation for specific cluster restore procedures.`
4. Select the copy to restore, and then click **Next**.

   The Restore Options page appears.
5. Click the Restore drop-down list and select one of the following options to restore: **Data**, **Archive logs**, or **Both Data and Archive logs**.

   If the database being restored affects any other database. you may receive an affected entity warning message.
6. Click **Next** to display the **Summary** page.
7. Review your restore settings and click **Finish** to complete the restore.

   On the **Results** page you can view the progress of the different phases that are part of restoring a copy.

Results

Appsync only displays restore warnings for databases discoverable by AppSync that are common to that host. No warnings display for any databases which either are not common to the host or not discoverable.
Refer also to Restoring a RAC copy on page 152.

Affected entities during restore

When restoring from a copy, you may be prompted to restore items in addition to the ones you selected.

An affected entity is data that resides on your production host that unintentionally becomes part of a replica because of its proximity to the data you intend to protect. You can prevent affected entity situations by properly planning your data layout based on replica granularity. The granularity of a replica depends upon the environment.

For Oracle, an affected entity can only be another Oracle Database data file(s) or archive logs. You can choose to restore using one of three options. This will determine the level to which affected entities are determined.

- Data only
- Archive Logs only
- Data and Archive Logs

Affected entities only display according to the restore option. If you select, **Data**, Appsync looks for affected entities with respect to the Oracle database data filesystems and storage. AppSync does not use Oracle database(s) archive log storage for checking for affected entities.

If you select, **Archive logs**, the reverse is true. Only the Oracle database archive logs filesystems and storage are used for checking affected entities and not the Oracle database(s) data filesystems.

If you select both **Data** and **Archive logs**, then filesystems and storage from both the Oracle database(s) data files and archive logs will be used for checking for affected entities.

If there are *affected entities* in your underlying storage configuration, the Restore Wizard notifies you of these items. The following scenarios produce *affected entities* that require you to acknowledge that additional items will be restored:

- For RecoverPoint and ViPR Controller, if the databases are in the same consistency group they become *affected entities* when the other database is protected.
- For VNX, VNXe, VMAX, XtremIO, and ViPR Controller, if the databases are on the same LUN they become *affected entities* when the other database is protected. For VNXe, if the databases are in the same LUN group they become affected entities when the other database is protected.
- For vDISK/datastore - If data files of two data bases: DB1 and DB2 reside on datastore [DS1] and or similarly archive logs of same two databases resides on datastore [DS2], then both become affected entities.

If the affected entity was protected along with the Oracle database selected for restore, AppSync restores it. Any other Oracle database that was not protected but is an affected entity is overwritten.

AppSync calculates affected entities for the consistency groups or LUNs of the Oracle database that is selected for restore. If the affected databases partially reside on other consistency groups, LUN groups, or LUNs, AppSync does not calculate affected entities on those consistency groups, LUN groups, or LUNs.

Affected entities are calculated on the basis of restore granularity. If both data and log are selected for restore, then affected entities are calculated for all the consistency groups, LUN groups, LUNs, or datastores on which the database resides. If only data or only log restore is selected, then the affected entities are only calculated for the selected component's consistency group, LUN group, LUN, or datastore.

If the database's data and log components reside on the same consistency group or LUN, the option to restore only logs or restore only data is not available. You have the option

only to restore data and logs. The only exception to this scenario is when you choose to do a differential copy restore.

Vdisk restore with affected entities

Review this information for a Vdisk restore with affected entities.

- During restore, if there are affected databases on virtual disks that are not protected by AppSync, shutdown the these databases including all unmounted filesystems. Additionally, remove Vdisks from VM before proceeding with LUN level restore.
- If affected databases reside on any volume or disk groups, then deport or dismount VGs and DGs before restore and then manually import and mount them post-restore. (Since Appsync does not control these entities, a post storage LUN restore can fail when attempting import/mount of affected VGs and DGs on the production host.)
- Affected entity databases on Vdisks with VG or ASM are not supported.

Restoring a RAC copy

Follow this procedure to restore a RAC copy.

Before you begin

On remote nodes follow these steps:

1. Shutdown all impacted databases as oracle user: `oracle> srvctl stop instance -d <RACDB> -i <DbInstanceOnRemoteNodes>`
2. Dismount all impacted ASM disk groups as grid user: `grid> asmcmd umount <DG>`

On the restore node, perform the restore. Follow these steps:

Procedure

1. On the AppSync console, go to **Copy Management** › **Oracle**.
2. Select the desired database, and then from the drop-down menu in the lower center of the screen click **Recover** and select **Restore**.

   The Oracle Restore wizard launches.
3. On the Select Copy page, select the copy you want to restore, and then click **Next**.
4. Under **Restore Options**, select the option you want, and then click **Next**.

   The Summary page opens.
5. Review your restore actions and click **Finish**.
6. Verify that the selected database is being shut down.
7. Verify the message that disk goups and devices are being unmounted.
8. Verify that the restore was successful.

Results

After the restore:

1. Remount the diskgroups on the remote nodes as grid user:`grid> asmcmd mount <DG>`.
2. On any node, perform recovery of the restored database using redo or archive with resetlogs:

   ```
   Oracle > startup mount

   Oracle > recover database
   ```

3. Open the database on the recovery node:
   Oracle > alter database open
4. Bring up the instances on the additional nodes:
   srvctl start instance -d <RACDB> -i <DbInstanceOnRemoteNodes>

Restoring a RAC copy for affected entities

Follow these steps to create your restore.

Before you begin

On remote nodes follow these steps:

1. Shutdown all impacted databases as oracle user: `oracle> srvctl stop instance -d <RACDB> -i <DbInstanceOnRemoteNodes>`
2. Shutdown other affected databases: `oracle>` **`srvctl stop database -d <RACDB2>`**
3. Dismount all impacted ASM disk groups as grid user: `grid> asmcmd umount <DG>`

On the restore node, perform the restore. Follow these steps:

Procedure

1. On the AppSync console, go to **Copy Management** › **Oracle**.
2. Select the desired database, and then from the drop-down menu in the lower center of the screen click **Recover** and select **Restore**.

   The Oracle Restore wizard launches.
   Verify the Warning:

   ```
   You are attempting to perform a restore on a cluster. Please
   follow the instructions in the AppSync documentation for
   specific cluster restore procedures.
   ```

3. On the Select Copy page, copy should already be selected. Click **Next**.
4. Under **Restore Options**, select **Data**, and then click **Next**.

   Verify that the Affected Entities warning has been displayed that there is an database that is impacted and that you need to shutdown the database manually.

   Note

   A database may have associated entities on the same storage but in a different node. If this is the case this warning will not display.

5. Click **Next** at the Affected Entities screen.
6. Review the Summary and then click **Finish**.
7. Verify that the selected database is being shut down.
8. Verify the message that disk goups and devices are being unmounted.
9. Verify that the restore was successful.

Results

After the restore:

1. Remount the diskgroups on the remote nodes as grid user:`grid> asmcmd mount <DG>`.

2. On any node, perform recovery of the restored database using redo or archive with resetlogs:
   Oracle > startup mount

   Oracle > recover database
3. Open the database on the recovery node:
   Oracle > alter database open
4. Bring up the instances on the additional nodes:
   srvctl start instance -d <RACDB> -i <DbInstanceOnRemoteNodes>
5. Repeat steps 2 and 3 to recover affected database <RACDB2>
6. Bring up affected database <RACDB2>

Restore a copy from XtremIO

Review this information regarding restoring an Oracle copy from XtremIO.

For AppSync 2.2.2 and later and XtremIO 4.0 and later the Restore button is enabled in the Oracle Restore wizard for automated restore. If you are restoring two copies, one for XtremIO 3.x and another for XtremIO 4.0 AppSync restores only the 4.0 copy (warning for 3.x copy appears).

To restore an Oracle database for XtremIO 3.x, mount the desired AppSync copy on the production host, and then use RMAN to recover the database to the desired point in time (includes RAC configurations).

If you cannot recover the database using RMAN, you might need to perform the following restore steps to replace (restore) the Oracle database completely. Because Oracle configurations on Linux environments vary (ASM, udev, MPIO, LVM, and so on), test and document the full restore procedures on a non-production Oracle configuration that is configured similarly to your production host before you use the procedures in a real disaster recovery situation. Doing so ensures a successful restore scenario. The following full restore procedure example is based on a stand-alone Oracle database on ASM that uses udev devices.

The main concern to observe during the restore procedure is to prevent a conflict between the production configuration and the mounted configuration. Ensure that you shut down the production object (for example, Oracle database, ASM disk group, and so on) before you attempt to convert the copy to production.

Restore Oracle database copy with AppSync and XtremIO

This section includes steps to perform a manual restore of an Oracle database copy residing on an XtremIOarray for 2.2.1 and earlier and XtremIO versions before 4.0.

Before you begin

With AppSync 2.2.2 and later and XtremIO 4.0 and later use the Restore Wizard to restore copies. Refer to Restoring an Oracle copy on page 150.

For manual restore, you need an Oracle database copy on XtremIO storage with an AppSyncservice plan that replicates the database. Suspend any AppSync service plans that might replicate the database that you are trying to restore

Procedure

1. In the AppSync console, mount the Oracle copy that you want to restore. Select **Mount on standalone server**, and then select **Original Server** or specify the production host where you want to mount the copy.

   Because you are mounting to the original server, select **Default Path** for the mount path.

2. On the production host, stop any application that uses the database being restored.
3. On the production host, shut down the Oracle instance being restored.

   ASM configuration is assumed.
4. Identify the ASM disk groups for the Oracle database being restored, and then dismount them.

Figure 16 Dismount ASM disk groups

```
SQL> select name,state from v$asm_diskgroup;

NAME                           STATE
------------------------------ -----------
ARCHDG                         MOUNTED
DATADG                         MOUNTED
FRADG                          MOUNTED
REDODG                         MOUNTED
XIO_DATADG                     MOUNTED
XIO_FRADG                      MOUNTED
XIO_REDODG                     MOUNTED
APSARCHDG                      DISMOUNTED
APSDATADG                      DISMOUNTED
APSREDODG                      DISMOUNTED

10 rows selected.
```

Figure 17 Change disk groups

```
SQL>  alter diskgroup XIO_DATADG dismount;

Diskgroup altered.

SQL> alter diskgroup XIO_FRADG dismount;

Diskgroup altered.

SQL> alter diskgroup XIO_REDODG dismount;

Diskgroup altered.
```

5. Check the ASM disk string parameter (`asm_diskstring`), and then remove the production ASM device pattern.

   The mounted ASM devices have `/dev/emc-appsync` pattern as a prefix. In the following example, the production ASM disks used `/dev/asm-disk*` as a device pattern.

Figure 18 Pattern = `/dev/asm-disk*`

```
grid@lrmh231:-> sqlplus '/ as sysasm'

SQL*Plus: Release 11.2.0.1.0 Production on Thu Dec 4 10:54:00 2014

Copyright (c) 1982, 2009, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Automatic Storage Management option

SQL> show parameter asm_diskstring

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
asm_diskstring                       string      ORCL:*, /dev/asm-disk*, /dev/e
                                                 mc-appsync-*
SQL> alter system set asm_diskstring='ORCL:*','/dev/emc-appsync-*' scope=both;

System altered.
```

6. Mount the ASM disk groups, which point to the mounted snapshot copy.

Figure 19 Mount ASM disk groups

```
SQL> select name,state from v$asm_diskgroup;

NAME                           STATE
------------------------------ -----------
ARCHDG                         MOUNTED
DATADG                         MOUNTED
FRADG                          MOUNTED
REDODG                         MOUNTED
APSARCHDG                      DISMOUNTED
APSDATADG                      DISMOUNTED
APSREDODG                      DISMOUNTED
XIO_DATADG                     DISMOUNTED
XIO_REDODG                     DISMOUNTED
XIO_FRADG                      DISMOUNTED

10 rows selected.

SQL> alter diskgroup XIO_DATADG mount;

Diskgroup altered.

SQL> alter diskgroup XIO_REDODG mount;

Diskgroup altered.

SQL> alter diskgroup XIO_FRADG mount;

Diskgroup altered.
```

7. Adjust the disk group bindings so that they do not use the EMC bindings. You can perform this task now or later.

   If you adjust the disk group bindings later, stop Oracle, and then dismount the disk groups. For ASM using udev devices on SuSe Linux, includes changing the rules files in `/etc/udev/rules.d`. Each version of Linux is different, so be sure to understand the environment, and how Oracle is configured. If you perform this step now, add the original ASM bindings back to `asm_diskgroup`.

8. Start Oracle, and then recover the database.

Figure 20 Start, and then recover database

```
SQL> startup;
ORACLE instance started.

Total System Global Area 1603411968 bytes
Fixed Size                  2213776 bytes
Variable Size            1258293360 bytes
Database Buffers          335544320 bytes
Redo Buffers                7360512 bytes
Database mounted.
ORA-10873: file 1 needs to be either taken out of backup mode or media
recovered
ORA-01110: data file 1: '+XIO_DATADG/lincoln/datafile/system.256.854372799'


SQL> recover database;
Media recovery complete.
SQL> alter database open;

Database altered.
```

The restored database should be online.

9. Restart any database application that you stopped in step 2.
10. On the AppSync console, select **Remove** to remove the mounted copy.

    This action removes the copy from the AppSync database but does not remove the snapshot on the production mount host or on the XtremIO storage array. You can remove a mounted copy, but you cannot set the expiration of a mounted copy.
11. Move the mounted snapshot from the `/AppSyncSnapshots` folder to the folder where the production LUNs to be replaced reside.

    Move the mounted snapshot (the snapshot that is currently masked to the ESX initiator group) if the production host is a virtual machine. If the production host is a physical host, move the snapshot to the folder where the production LUNs reside. After you finish, you see the production LUNs and the snapshots in the same folder.

Figure 21 Before snapshot moves

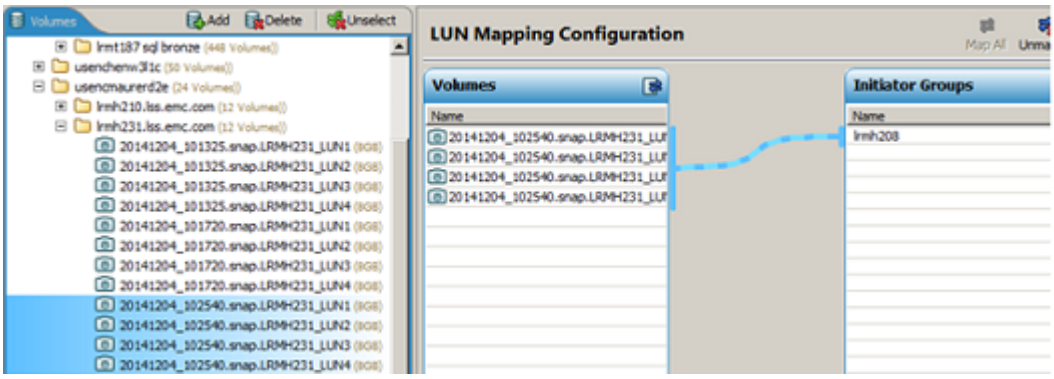
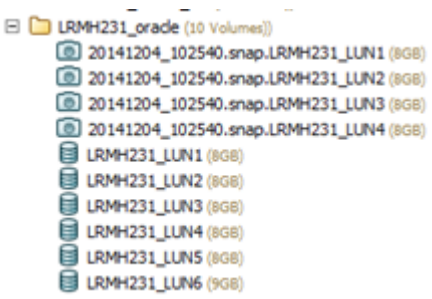


Figure 22 After snapshot moves



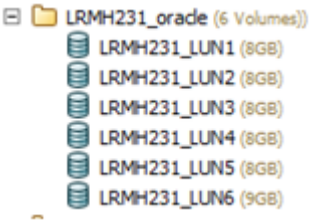
12. If the production host is a virtual machine, unmap the original production volumes from the ESX server, rescan the ESX host, and then remove the RDMs from the production virtual machine configuration. If the production host is a physical host, unmap the original production volumes from the production host, and then perform a device rescan on the host to remove the old production devices.
13. Remove the former production volumes from the XtremIO console.

    The restored snapshots become volumes.

    Figure 23 Restored snapshot becomes volumes

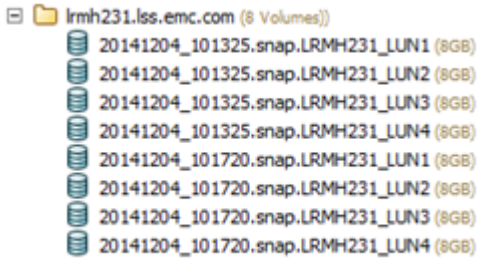
14. Rename the snapshots to the production volume names.

    Figure 24 Rename snapshots



    The other snapshots in the `/AppSyncSnapshots` folder for the old production XtremIO volumes that you removed in Step 11 also become volumes.

    Figure 25 Removed snapshots become volumes



15. Rediscover the production host to refresh the AppSync console view of the ASM configuration. Next, run the service plan to create a snap of the restored database, and then enable any service plans suspended in Step 1.

Repurposing overview

This topic explains how to use the AppSync repurposing feature for database and Bookmark copies.

AppSync supports the ad-hoc creation of Oracle and SQL Server on page 119 database copies, as well as RecoverPoint Bookmark copies, followed by the creation of copies of those copies. This practice is referred to as repurposing. Repurposing serves many useful functions including test-dev, break-fix, data mining, and reporting.

Review and consider the following information regarding repurposing features:

- Repurposing creates a multi-level tree of copies of the database.
- AppSync identifies copies that are created from a repurpose action by a "generation removed" number from the production source data, for example, Gen 1, Gen 2, and so on.
- There is no practical limit to the number of generations, but support is limited to two generations removed from the production data.
- A first generation(1st Gen) copy creates a copy that can be used as source for other copies. This action creates a copy-of-copy.
- Repurpose copies are meant to be mounted for extended periods of time for various purposes.
- After use, repurpose copies are either discarded or refreshed.
- Repurpose copies do not figure into RPO calculations.
- You can run 1st Gen copies now or schedule them to run at a future time.
- AppSync-supported copy types include VNX Snap, TimeFinder clone of clone, Snapshot of clone on VMAX, SnapVx of SnapVx for VMAX 3, XtremIO Snapshot, and RecoverPoint Bookmarks.
- Restore is not supported from 2nd Gen copies.

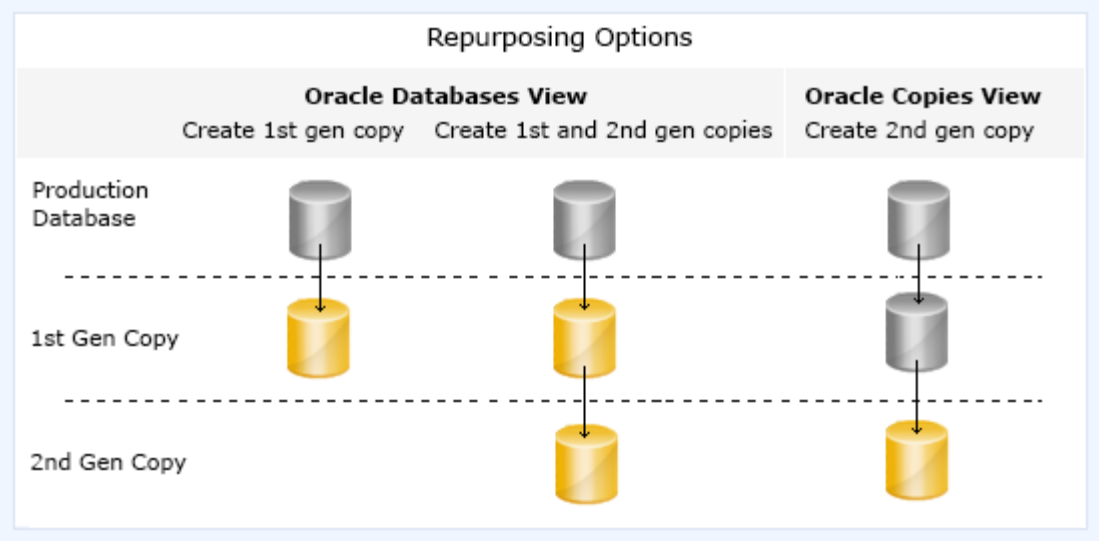
The console displays all scheduled repurpose actions. Select any of them, and then select the Delete button. The scheduled activity is removed.

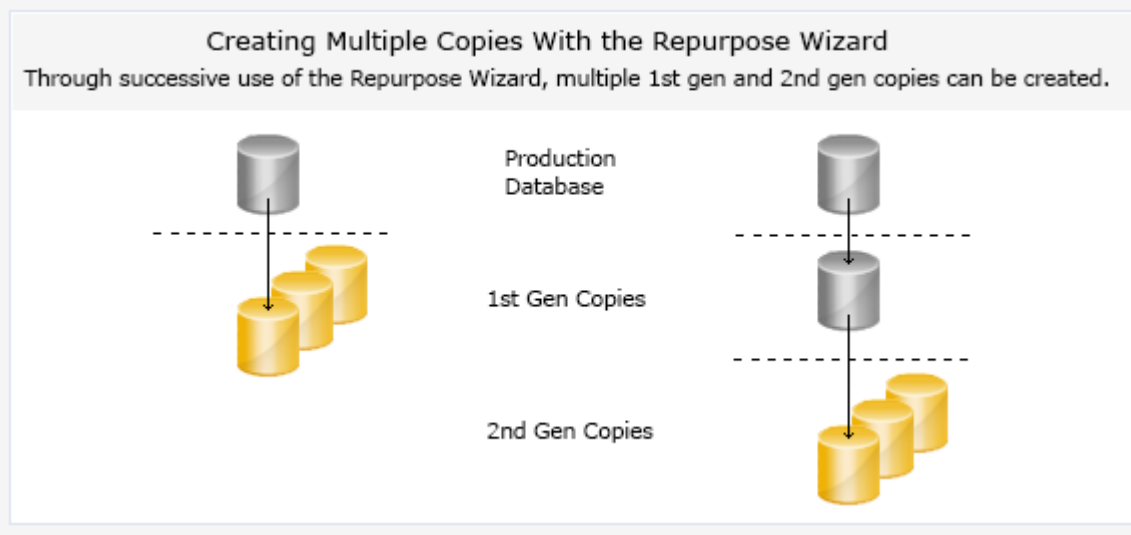
If you enable hot-backup, the 1st Gen copy of the database creates the application consistent copy. It Includes application discovery, mapping, and database freeze/thaw. AppSync does not set database freeze/thaw as the default for 1st Gen repurpose copies.

Second generation (2nd Gen) copies are created as copies-of-copies, using the 1st Gen copy as the source. They do not include application discovery, mapping, and database freeze/thaw. As a result, 2nd Gen copies are created much faster than 1st Gen copies.

Note

Repurposing copies are not supported for Oracle databases on VNX File storage, or NFS File systems.





Repurpose refresh

Refresh means to discard the current copy (expire), and recreate the copy contents using its parent.

- 1st Gen and 2nd Gen copies can be refreshed.
- Refreshing a 1st Gen copy creates an application consistent copy with a new time.
- 2nd Gen copies are not modified if you refresh 1st Gen copy.
- Refresh of 2nd Gen copy resynchronizes the 2nd Gen copy with the 1st Gen parent. (Use for discarding changes of 2nd Gen copy and starting over.)
- 2nd Gen timestamp is the same as the 1st Gen copy.
- With refresh, it is possible to have first and 2nd Gen copies with different copy time stamps.
- If you specified Unmount Previous Copy when creating the 2nd Gen copy, AppSync unmounts the copy before creating the new copy.
- Refresh of a 1st Gen copy on XtremIO: If the number of LUNs in the source database changes, then create only new snapshots. For example, AppSync uses the refresh provided by the XtremIO array from source LUNs to create the 1st Gen snapshot copy.
- Refresh of 2nd Gen copy on XtremIO: If you refresh the source 1st Gen copy and the number of LUNs in the source database changed, then create only new snapshots. Otherwise, use the refresh provided by the XtremIO array from 1st Gen snapshots to 2nd Gen snapshot copies.
- After the refresh, AppSync remounts the copy if the copy was mounted.
- 2nd Gen copy is recreated from 1st Gen parent. If 1st Gen parent no longer exists, then the refresh fails.
- 1st Gen copy is recreated from the application.
- The current copy that you want to refresh must be unmounted (if it is mounted). If you selected **Mount Copy** in the Repurpose wizard, AppSync mounts the copy again.

You can refresh a repurposed copy at any time. To start the refresh:

1. From the **Applications** tab of the AppSync console, select the repurposed copy that you want to refresh.
2. Click **Refresh**.

Repurpose expire
Expiring first or 2nd Gen copies removes the ability to refresh the copy. Expiration of a 1st Gen copy fails when a 2nd Gen copies is created from the 1st Gen copy.

Use expire if you are finished with a copy.

Using the Repurpose wizard

Use the Repurpose wizard to schedule or immediately create 1st Gen or 2nd Gen copies as needed.

Before you begin

You need AppSync administrative privileges to Repurpose the database instance.

To display the list of available applications.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.

Option	Description
To Repurpose an SQL copy:	Select SQL Server
To Repurpose an Oracle copy:	Select Oracle

   A list of available databases for the application choice loads.
2. Click the database instance you want to Repurpose, and then select **Repurpose** from the drop-down list in the lower left of the console screen.

   This action launches the Repurpose wizard, and leads you to the Intentions page where you can tell AppSync which action you want to perform:

   - **Create First Generation copy**
   - **Create First Generation copy and a Second Generation copy**

3. Select the desired copy type, and select **Local** or **Remote** in the Site drop-down to continue creating the copy.
4. Click **Next** to launch the **Settings** screen.

   From the Settings screen, you can define the specific options for 1st and 2nd gen copies. Specifically you can

   - Define labels for each copy to help identify the copy purpose.
   - Select application-specific copy options for 1st gen copy only.
   - Choose appropriate copy type (wizard fails if incorrect type is chosen).
5. Select the desired options for the copy, and then click **Next**.

   The schedule page of the wizard appears allowing you to identify when the 1st generation copy should be created. Create the copy now or schedule the copy for a convenient time.
6. Select **Run now** or **Run later** followed by typing run- time date and time, and then press **Next** to complete the wizard.

After you finish

The Repurpose Monitor

The Repurpose Monitor allows you to view all currently running repurpose activities, and monitor their progress. The Repurpose Monitor shows the item being repurposed (source)

and the label of the item being created or refreshed along with the application type. Refer to The Repurpose Monitor on page 211.

View or cancel scheduled repurpose copies

You can view or cancel any scheduled first generation repurpose copy.

Procedure

1. From the Appsync console, navigate to **Application** › **Copy Management**, and then select the appropriate database.
2. Select **Repurpose** › **View Scheduled Repurpose Copy** to view all scheduled repurpose actions.
3. To delete an action, select one or more desired actions, and click **Delete** to remove the action.

Mounting and recovering an Oracle clone of clone of RecoverPoint Bookmark

These steps show you how to mount and recover an Oracle database clone of clone for a RecoverPoint Bookmark copy on VMAX.

Before you begin

Ensure the AppSync configuration has one Oracle database copy on RecoverPoint with VMAX. Enable hot backup for 1st Gen copies for guaranteed recovery.

Procedure

1. On the AppSync console go to **Applications** › **Oracle**, select an Oracle database that is on VMAX storage, and then select **Repurpose**.

   The action launches the **Intentions** page of the Repurpose wizard.
2. On the Intentions page, select **create 1st Gen** and **create 2nd Gen** copies, select **Use Bookmark as an intermediate step**, and then click **Next**.
3. On **Settings** › **1st Gen copy** › **Create a label** select **Clone** copy type.
4. On the settings page for 2nd Gen copy, select a label, and then select **Clone** as copy type.
5. Select mount settings for the 1st Gen copy, and then select **Unmount** phase for 1st gen copy.
6. Select mount settings as **Mount and Recovery** for the 2nd Gen copy, and then select **Unmount** phase for 2nd gen copy.
7. On the Schedule page, select **Run Now** to finish the wizard.

Mounting and recovering an Oracle Snap of Clone RecoverPoint Bookmark

These steps show you how to mount and recover an Oracle database Snap of Clone for a RecoverPoint Bookmark copy on VMAX.

Before you begin

Ensure the AppSync configuration has one database on RecoverPoint VNX storage and another on RecoverPoint VMAX storage. Snap of Snap for VNX and Snap of Snap for VMAX is not supported.

Select 1st Gen copies with **Hot backup enabled** for guaranteed recovery.

Procedure

1. On the AppSync console go to **Applications** › **Oracle**, select an Oracle database that is on VMAX storage, and then select **Repurpose**.

The action launches the **Intentions** page of the Repurpose wizard.

2. On the Intentions page, select **create 1st Gen** and **create 2nd Gen** copies, select **Use Bookmark as an intermediate step**, and then click **Next**.
3. Go to **Settings** › **1st Gen copy** › **Create a label** and then select **Clone** copy type.
4. Go to **Settings** › **2nd Gen copy** › **Select Snap copy type**, then select a label.
5. Select **Mount Settings** for the 2nd Gen copy.
6. On the Schedule page, select **Run Now** and **Finish**.

CHAPTER 8

Protect file systems

This chapter includes the following topics:

Overview of file system support

Use AppSync to create and manage application-consistent copies of file systems.

File system features include:

- Dynamic discovery of file systems during service plan run.
- Protection of file systems with service plan or with copy now option. You can select one or more file systems to protect at one time or click **SELECT ALL** to protect all the file systems on the list of file systems page.
- List copies that you can filter by time of creation, copy status, and service plan.
- Mount on a standalone server

Protect NFS file systems on VNX storage

Learn how AppSync supports protection of NFS file systems on VNX storage.

AppSync supports protecting NFS file systems on Linux (RHEL, SUSE, and OEL) and AIX. You can use these copies for operational recovery.

Use Bronze, Silver, and Gold service plans. For service plans configured for remote protection, the NFS copy is created as a SnapSure Snapshot on the local and/or remote file system. Copies of NFS data stores can be created from service plans configured for local, remote, and local and remote protection. AppSync can also create copies for file system on an Oracle database for Bronze, Silver, and Gold service plans.

During restore from an NFS copy, AppSync creates a roll back snapshot for every file system that has been restored. The name of each roll back snapshot can be found in the restore details. You can manually delete the roll back snapshot after verifying the contents of the restore. Retaining these snapshots beyond their useful life can fill the VNX snap cache and cause resource issues.

Review the following pre-requisites for Silver and Gold copies:

- Register remote VNX arrays with AppSync.
- Create Remote Replication sessions with corresponding remote arrays for each NFS file system where you want creation of Silver and Gold copies. Ensure array status is OK.

Host file systems page

The Host file systems page shows all the host instances currently registered with AppSync.

You can add a host (Windows and UNIX) from this page and can discover file systems available on the hosts.

For further information on file systems, refer to:

- File systems page on page 166
- File system copies page on page 167
- Mounting a copy with the File System Mount wizard on page 175

Filesystem page

The Filesystem page lists all the available filesystems that are discovered for the selected server instance.

Click on a filesystem name to display copies of the filesystem.

Filesystem information includes:

- Status of service plan run, for example checkmark in a green circle = successful
- Name
- Type, for example, NTFS
- Format, for example MBR
- Service plan, for example Bronze
  Some filesystems can be subscribed to multiple serviceplans.
- Storage size in GB
- Send alerts to (if requested)

You can select one or more filesystems to protect at one time. Click **SELECT ALL** to protect all the filesystems on this page (except a filesystem C:\ which contains host system information). For further information on filesystems, refer to:

- Filesystem copies page on page 167
- Filesystem hosts page on page 166
- Mounting a copy with the Filesystem Mount wizard on page 175

Filesystem Copies Page

In this page you can view the list of filesystem copies.

The list of copies can be filtered by time of creation, the status of the copies that are created and service plan.

Select a copy to display events for that copy in the Details panel located on the bottom of the Copies page.

From the Copies page you can select to mount, restore or expire copies.

For further information on filesystems, refer to:

- Filesystems page on page 166
- Filesystem hosts page on page 166
- Mounting a copy with the Filesystem Mount wizard on page 175

Summary of file system service plan settings

Use this table to learn default file system settings for service plan phases including startup, discovery, mapping, pre and post copy scripting, mount/unmount and copy.

Default service plan settings create an application-consistent copy every 24 hours. Only the replication technology that is specified by the Copy type in the Create copy phase varies among plans. The following table summarizes the default settings:

Table 20 Default file system Service Plan Settings

Setting	Enabled/Not enabled	Default settings	Schedule
Plan Startup	Enabled	Automatic schedule	Recurrence type: Creates a copy every 24 hours, with the first run at midnight (00:00).

Table 20 Default file system Service Plan Settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
			Recovery Point Objective (RPO): A copy should be created every 24 hours. (Alert issued if objective is not met.)
Application discovery	Enabled	None	Determined by Plan Startup phase.
Application mapping	Enabled	None	Starts when Application discovery phase completes.
Pre-copy script	Not enabled	None	Starts when Application mapping phase completes.
Create copy	Enabled	Copy type: • Bronze: Create local copy. • Silver: Create remote copy (VMAX v2, VMAX v3, RecoverPoint, and VNX File). • Gold: Create Local and Remote copy (RecoverPoint and VNX File). Also: • Storage Ordered Preference: Snapshot, Clone & Bookmark. • Storage Settings: Include RecoverPoint copies in expiration rotation policy—select this option to include RecoverPoint copies when calculating rotations. If you do not select this option, RecoverPoint copies accumulate and remain until the bookmarks for them "fall off" the RecoverPoint appliance.	Starts when Pre-copy script phase completes.
Post-copy script	Not enabled	None	Starts when Create copy phase completes.
Unmount previous copy	Not enabled	None	Starts when Post-copy script phase completes.
Mount copy (A pre-mount script phase is available for file	Not enabled	Mount Copy • Mount on Server: Original Host • Mount with access: Read/write • Mount Path: Default Path Image	Starts when Unmount previous copy phase completes.

Table 20 Default file system Service Plan Settings (continued)

Setting	Enabled/Not enabled	Default settings	Schedule
system service plans)		• Access mode: Logged access • Copy to Mount: Local (Only for Gold Plans) • Use Dedicated Storage Group: Selected by default	
Post-mount script	Not enabled	None	Starts when Mount copy phase completes.
Unmount copy	Not enabled	None	Starts when Post-mount script phase completes.

Subscribing a file system to a service plan

This sections shows you how to subscribe a file system to a service plan. Protection for all file systems that are part of a service plan runs at the scheduled time.

Procedure

1. Browse to **Copy Management** › **Filesystem**.
2. Click the desired server.

   The File Systems Page loads for the selected server.
3. Select the file systems that you want to protect, then click **Subscribe to Service Plan** on the **Protect** drop-down list.
4. Select **Gold**, **Silver**, or **Bronze** service plan.

   You can also select **Subscribe to Service Plan and run** for immediate subscription and protection.

Overriding service plan schedules

You can set different schedules for individual applications that are subscribed to a service plan, overriding the generic recurrence setting.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can override only the settings of the recurrence type that is already selected for the service plan.

Procedure

1. Browse to **Service Plans** and select one of the plans from the list.
2. From the **Settings** tab, select the **Plan Startup** phase.
3. In the **Plan Startup Defaults** pane on the right, note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Scheduled** is selected as the **Startup Type**.
4. Click the **Plan Startup Overrides** tab.

You can see the list of all applications that are subscribed to the plan.

5. Select one or more applications and click **Override Schedule**.
6. In the **Override Schedule** dialog box, set the schedule that is based on your requirement and click **OK**.

   For example, if the default recurrence type is **On specified days of the month**, and the rule setting is to **Run at 12:00 AM** on the **1st day of every month**, you can override the time and the day for individual applications.
   A Pencil icon indicates that default settings have been overridden.

Service plan schedule

The schedule of a service plan is set in the **Plan Startup** phase.

The **Startup Type** (scheduled or on demand) determines whether the plan is run manually, or configured to run on a schedule. Options for scheduling when a service plan starts are:

- Specify a recovery point objective (RPO)
  - Set an RPO of 30 minutes or 1, 2, 3, 4, 6, 8, 12, or 24 hours
  - Minutes after the hour are set in 5 minute intervals
  - Default RPO is 24 hours
- Run every day at certain times
  - Select up to two different times during the day
  - Minutes after the hour is in 5 minute intervals
  - There is no default selected
- Run at a certain time on selected days of the week
  - One or more days of the week (up to all seven days) can be selected
  - There is no default day of the week selected. Default time of day is 12:00 AM.
- Run at a certain time on selected days of the month
  - Select one or more days of the month (up to all days)
  - Select one time of day. Available times are at 15 minute intervals.
  - Default is the first day of the month

Application discovery

Before creating a file system copy, AppSync examines the file system to look for changes such as addition, deletion, renaming, or movement of file systems. If individual file systems are being protected, AppSync rediscovers information about the selected file system.

There are no user settings associated with this phase and it cannot be disabled.

Application mapping

After discovering the application, AppSync maps it to array storage, and protection services such as RecoverPoint.

There are no user settings associated with this phase and it cannot be disabled.

Pre-copy script phase

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters on a service plan's Settings tab.

This operation requires the Service Plan Administrator role in.

The pre-copy script runs according to the schedule set in the Plan Startup phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts) for Windows and .sh for UNIX.

AppSync does not support running of PowerShell scripts directly. You usually have to wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you will need to set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full path name to your PowerShell command file in the .bat file:
   `powershell -command C:\PshellCommands.ps1 <nul`
2. Set the PowerShell execution policy so you can run your script. For example, the first line in the .bat file should look like the following for an unrestricted policy:
   `powershell -command set-executionpolicy unrestricted <nul`
3. To ensure correct termination of your PowerShell session, add ‹nul to the end of the line that calls your PowerShell script.

For Windows you can optionally enter credentials to run the script as a specific user. The script runs as Local System by default. For UNIX the credentials are mandatory.

For Windows the default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

For UNIX the File field should have the full path to the scripts that are to be executed.

Exact parameters depend on your script. Parameters with spaces must be enclosed in double quotes. This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Create copy phase features freeze and thaw callout scripts

The Create copy phase creates a copy that is based on the replication technology that is specified in the service plan. You can configure and run freeze and thaw callout scripts in this phase

Configuring and running freeze and thaw callout scripts

AppSync provides two scripting opportunities during the execution of Create copy phase, called the freeze and thaw callout scripts. Unlike pre-copy and post-copy script phases which are run before and after the Create copy phase, freeze and thaw scripts are unspecifiable by the GUI. The scripts are placed in a pre-defined location with a pre-defined name. You can use these scripts to quiesce (suspend I/O) and thaw on any AppSync unsupported databases residing on the subscribed file systems for a short period (usually few seconds). During this time the copy is activated. The scripts are run with the user credentials used to register host-plugin with AppSync.

During the Create copy phase, when AppSync executes these scripts, a temporary XML file is provided as the only argument to these callout scripts. This XML file has the list of file systems being protected by the Create copy phase.

AppSync continues with normal copy creation if no callout script is found or if the callout script in not executable. If either of the callout scripts fail (non-zero exit value), copy creation fails and the Create copy phase ends with an error. If the freeze callout script

runs successfully, and then copy creation fails due to any storage issue, the thaw callout script is run before ending the create copy phase with an error.

For a **Windows** host-plugin, place the callout executable scripts in the `%ProgramData%\ EMC\AppSync\scripts` folder and name it `appsync_freeze_filesystem_<service plan name in lower case>.bat` for the freeze callout. Name the thaw callout script: `appsync_thaw_filesystem_<service plan name in lower case>.bat`

For example, AppSync runs this script as follows:

`C:\ProgramData\EMC\AppSync\scripts\appsync_freeze_filesystem_bronze.bat`, `C:\Windows\TEMP\d575f2e6-7dc4-4389-87c9-491effc57318.xml`

Where `C:\Windows\TEMP\d575f2e6-7dc4-4389-87c9-491effc57318.xml` file content is in the following form:

```
<Application type='Filesystem'><sourceVolumePath>F:\</sourceVolumePath><sourceVolumePath>G:\</sourceVolumePath></Application>
```

For a **UNIX** host-plugin, place the callout executable scripts in the `/var/opt/emc/appsync/scripts` folder name as `appsync_freeze_filesystem_<service plan name in lower case>` for the freeze callout and `appsync_thaw_filesystem_<service plan name in lower case>` for the thaw callout. Do not use a file name extension such as .pl or .sh. The scripts should be executable.

AppSync runs this script as follows:

```
/var/opt/emc/appsync/scripts/appsync_freeze_filesystem_bronze /tmp/904f510f-47ce-402f-a27a-b3a48840a279ybo61k.xml
```

Where `/tmp/904f510f-47ce-402f-a27a-b3a48840a279ybo61k.xml` file content is in the following form: `<Application type='Filesystem'><filesystems><filesystem><name>/FS1</name></filesystem><filesystem><name>/FS2</name></filesystem></filesystems></Application>`

Post-copy script phase

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters in a service plan's **Settings** tab.

This operation requires the Service Plan Administrator role in AppSync.

The script runs on successful completion of the **Create copy** phase. Valid script formats are .bat, .exe, and .ps1 (PowerShell scripts) for Windows and .sh for UNIX.

AppSync does not support running of PowerShell scripts directly. You usually must wrap them in a .bat file. The other option is to make the default "Open" on ps1 files `C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe`. When the PS script runs, you may get an error and you must set an appropriate execution policy.

To run PowerShell commands from scripts:

1. Specify the full pathname to the PowerShell command file in the .bat file: `powershell -command C:\PshellCommands.ps1 <nul`
2. Set the PowerShell execution policy so you can run the script. For example, the first line in the .bat file should look like the following for an unrestricted policy: `powershell -command set-executionpolicy unrestricted <nul`

3. To ensure correct termination of the PowerShell session, add ‹nul to the end of the line that calls your PowerShell script.

For Windows, you can optionally enter credentials to run the script as a specific user. The script runs as Local System by default. For UNIX, the credentials are mandatory.

For Windows, the default location of the script is `%ProgramData%\EMC\AppSync \scripts\` on the application host.

For UNIX, the File field should have the full path to the scripts to be run.

Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes. This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Unmount previous copy

The service plan unmounts a previously mounted copy after creating the new copy. The exception is a copy that was mounted on-demand as opposed to by the service plan; in this case the on-demand mounted copy is not unmounted.

There are no user settings associated with this phase and it can be enabled or disabled.

Mount copy

The Mount copy phase mounts the copy. This phase can be enabled or disabled.

Field	Description
Mount on Server	The server on which to mount the copy. Only the nodes of the cluster or standalone hosts are available for selection.
Mount with access	Type of access the copy should be mounted with.
Mount path	The **Default Mount Path** is `%SystemDrive%\AppSyncMounts\% %ProdServerName%%`. To specify the value of a Windows environment variable in the mount path, delimit the variable name with single percent signs (%). The default path also contains an AppSync variable (ProdServerName) which is delimited with two percent signs (%%). The following characters are not valid in the path:‹ › : " / | ? * . The mount path could also be **Same as Original Path**. However, this option is not available when the mount host is the same as production host.
Desired SLO (VMAX 3 only)	Select the desired SLO for the target LUN. If there is a storage group for the mount host with the desired SLO, the LUN will be added to the storage group. If it does not exist, AppSync will add it to any storage group that is masked to the host.
Image access mode (during RecoverPoint mount)	• **Logged Access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. This is the only option available when you mount to the production host. • **Virtual Access with Roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access,

Field	Description
	allowing heavy processing. With RP-VMAX and RP-XtremIO, virtual access with roll is not supported. • **Virtual Access**: Provides nearly instant access to the image; it is not intended for heavy processing. Virtual access with RPVMAX and RP XtremIO is not supported.
Use Dedicated Storage Group	• Applicable only for physical hosts or virtual machines with direct iSCSI part of cluster. • Checked by default, enabling this option allows AppSync to enforce a dedicated VMAX or VNX storage group for a mount. (A dedicated VMAX or VNX storage group contains the selected mount host only). The mount will fail if you are mounting to a node of a cluster that is in a storage group shared with the other nodes. **Note** Use this option to mount the copy to a node for copy validation or backup to tape. In this scenario, you will need two storage groups. One storage group is dedicated to the passive node being used as a mount host and the other storage group is for the remainder of the nodes in the cluster. Both storage groups contain the shared storage for the cluster. • If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount.

Override mount settings in a service plan

If there are multiple file systems that are subscribed to the same plan, you can select different mount settings for each file system, overriding the generic mount settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Browse to **Service Plans** › **FileSystems** and click one of the plans from the list.
2. From the **Settings** tab, select the **Mount copy** phase.
3. On the right pane, select the **Mount Copy Overrides** tab.

   The list of file systems includes all file systems subscribed to this plan. The mount settings display the default settings.
4. Select the file system whose settings you want to override and click **Set Overrides**.

   Press and hold the Shift or Ctrl keys to select multiple file systems.
5. On the **Mount Copy Overrides** dialog box, select options only for those mount settings that you want to override.

   For example, if you want to mount a copy to the production host, you would select **Use new signature** from the **Mount Signature** drop-down.

   Fields that do not have a selection retain their default settings.

6. Click **OK.**

   A pencil icon appears in the first column of the file system's row whose default mount settings you changed.
7. To revert to default settings, select the file systems and click **Use Default Settings**.

Post-mount script

Specify a post-mount script and parameters from the Post-mount script option in the **Settings** tab of a service plan.

The script runs on successful completion of the mount copy or mount with recovery phase. This script is typically used for backup.

From the **Server** list, select the server on which to run the script. You can optionally run it on a registered host other than the mount host, and enter credentials to run the script as a specific user.

The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

Exact parameters depend on your script. Parameters with spaces must be enclosed in double quotes.

This phase can be enabled or disabled. This operation requires the Service Plan Administrator role in AppSync.

Mounting a copy with the File System Mount wizard

Use the File System Mount wizard to create any point-in-time mount for RecoverPoint copies.

Before you begin

This task requires the Data Administrator role in AppSync.

For UNIX, the File field should have a full path to the scripts to be run. You need user credentials to run the script.

Follow these steps:

Procedure

1. On the AppSync console, go to **File systems** › **Copies** to display available copies.
2. Select a copy to mount, and then click **Mount**.

   The Select Copy to Mount page of the File System Mount wizard launches.
   You can select any copy to be mounted. By default the copy that you selected before selecting Mount is highlighted, however other copy instances also appear.
3. Select the copy to mount, and click **Next**.

   The Specify Mount Settings page launches where you can select the **Mount on Host** (mount host drop-down), and a mount path location either **To original path**, or **Mount to alternate path** (drop-down). The mount path is the location where the copy is mounted on the mount host. By default AppSync displays the path of the mount host you selected. You can also edit and mount the copy to a user-defined location.
   You can also select Mount Options including **Mount with access** (read-only or read/write), and **Image access mode** (drop-down). Image access mode allows you to mount the file system with proper access mode in case the selected copy is a RecoverPoint bookmark.

   For VMAX 3 arrays, you are presented with an SLO drop-down list. You can select the Service Level Objective (SLO) for the mount copy. If there is a storage group for the

mount host with the desired SLO. AppSync adds the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host. If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices are added to the original storage group when the copy is expired.

4. Type mount location information and mount options, and click **Next**.

   The Summary page launches.

5. Review the mount information and if it is correct click **Finish**.

   The Results page launches with mount result information.

Changing the mount point for an affected file system

Follow this procedure to manually change the mount point for an affected file system.

Assume VG1 is the source volume group.

Procedure

1. Get the list of LVs using the `lsvg -l VG1` command, and check which file systems show mount point on `/tmp/EMCAppsync **` directory.
2. Run `chfs -m <Original MT Pt> /tmp/EMCAppsync6922/vg1_logs` command where `<Original Mt Pt>` is the mount point where the file system was originally mounted.
3. Run `fsck` on the source Logical Volume `fsck -y /dev/fslv01`.
4. Run mount command using the log logical volume and make sure that the source has been mounted successfully `mount -v jfs2 -o rw,log=/dev/loglv00 /dev/fslv01 <Orig Mt Pt>`

Unmounting a file system copy

When you select a copy to unmount, other copies that were mounted along with the selected copy will also be unmounted.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can unmount a copy only from a list of copies made for a file system.

Procedure

1. Navigate to the Copies page from the Copy Management or Service Plan pages:
   - **Copy Management** › **FileSystems** › select the server which hosts the file system you want to unmount, then select the file system with the copy to unmount.
   - **Service Plans** › **File systems**› select a service plan, then select the **Copies** tab.
2. From the list of copies, select the copy and click **Unmount** from the button in the lower part of the page.

   The **Unmount Confirmation** dialog displays all the copies of other file systems that were mounted along with the selected copy to be unmounted.

3. Click **Yes** to confirm the unmount of all the copies shown in the dialog.

   The **Unmount** page displays the progress of the unmount operation. All copies associated with the selected copy will be unmounted.

Override mount settings in a service plan

If there are multiple file systems that are subscribed to the same plan, you can select different mount settings for each file system, overriding the generic mount settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Browse to **Service Plans** › **FileSystems** and click one of the plans from the list.
2. From the **Settings** tab, select the **Mount copy** phase.
3. On the right pane, select the **Mount Copy Overrides** tab.

   The list of file systems includes all file systems subscribed to this plan. The mount settings display the default settings.
4. Select the file system whose settings you want to override and click **Set Overrides**.

   Press and hold the Shift or Ctrl keys to select multiple file systems.
5. On the **Mount Copy Overrides** dialog box, select options only for those mount settings that you want to override.

   For example, if you want to mount a copy to the production host, you would select **Use new signature** from the **Mount Signature** drop-down.

   Fields that do not have a selection retain their default settings.
6. Click **OK.**

   A pencil icon appears in the first column of the file system's row whose default mount settings you changed.
7. To revert to default settings, select the file systems and click **Use Default Settings**.

Restoring a file system

Use the File System Restore wizard to restore an existing file system copy.

Procedure

1. On the AppSync console go to **Copy Management** › **File systems**.

   The file system Hosts page launches displaying available servers.
2. Select the server which has the file systems for restore, to launch the file systems page.
3. Select the file system that you want to restore (**Select All** option appears in lower left of page), and then click **Restore** from the Recover menu in the lower left area of the file system page.

   This action launches the File System Restore wizard. All protected copies are listed in the wizard. You can only select one file system copy at a time for restore. The copy date, file system name, server name, service plan, and copy type appear for each copy.
4. Select the file system copy for restore and click **Next**.

   The Restore Warnings page launches. The Restore Warnings page lists the file system which belongs to the same consistency group or volume group where the copy is restored. If this file system is protected as well as the selected file system copy, this file system is overwritten.

The restore warning page also lists any application that is installed in the file system that is being restored.

5. Read the warnings and click the "I have read warnings" checkbox and click **Next** to continue with the restore.

   This action launches the Summary page of the wizard.

6. If the Summary page looks correct, click **Finish**.

   The Results page loads where you can view the restore results.

Restore a file system copy manually on XtremIO

Automated restore of an XtremIO 4.0 (minimum version) copy with AppSync 2.2.2 and higher is supported. This topic shows you how to manually restore a copy on an XtremIO version lower than 4.0 with AppSync 2.2 through 2.2.1.

Before you begin

Refer to Restoring a file system copy on page 177 for automated restore.

To manually achieve a granular restore of files and folders in a file system, mount a file system copy and use selective file/folder copy, you need the following configuration:

- Host file system that resides on XtremIO storage
- AppSync service plan that replicates the file system

Procedure

1. On the AppSync console, select **Service Plans** › **Filesystem** and the wanted service plan, for example **Bronze**.

   The **Copies** page displays existing copies.

2. Disable any service plans scheduled to run, which includes the file system that you plan to restore.

   This action prevents a copy from being made during the restore procedure.

3. To mount the copy that you want to restore to production host, click **mount to default location**.

   Mount the copy with read/write access.

4. Perform one of the following steps depending on the operating system:

   a. For Windows: Record the NAA Identifier for the production volume and the mounted snapshot, and then remove the drive letter of the production device on the production host.

   b. Linux/AIX: Unmount the file system.

5. Assign the drive letter of mounted snapshot copy on production host (Windows) or remount file system (Linux/AIX).

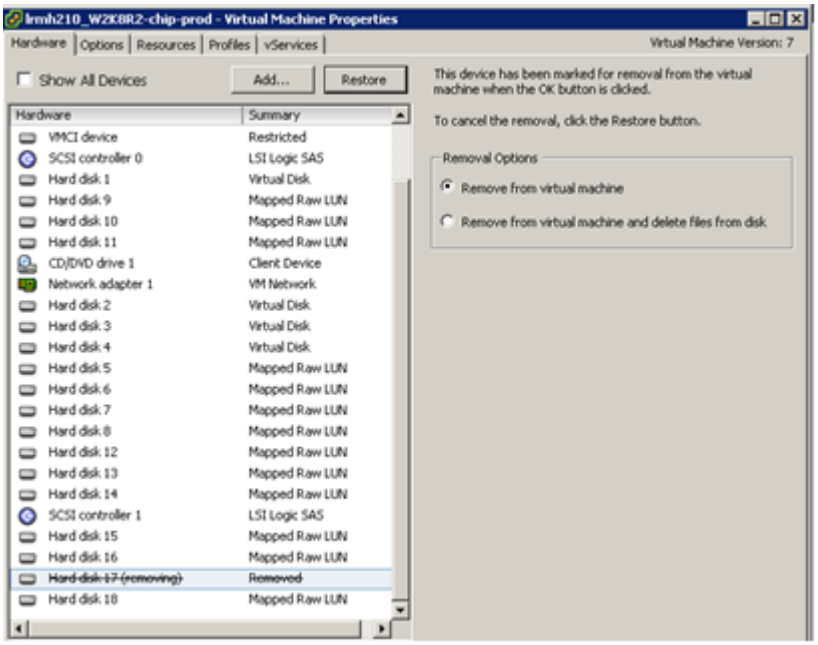
6. Select **Remove** for the mounted copy.

   This action removes the copy from the AppSync database without changing the snapshot on the mount host or the XtremIO storage array. The system displays a message that discusses this action.

7. If the production host is a virtual machine, use the NAA Identifier that you previously recorded to remove the old production LUN from the host inventory.

   This action removes the volume from the host (host device rescan might be necessary). No more action is required on the production host.

Figure 26 Virtual machine: Remove old production LUN

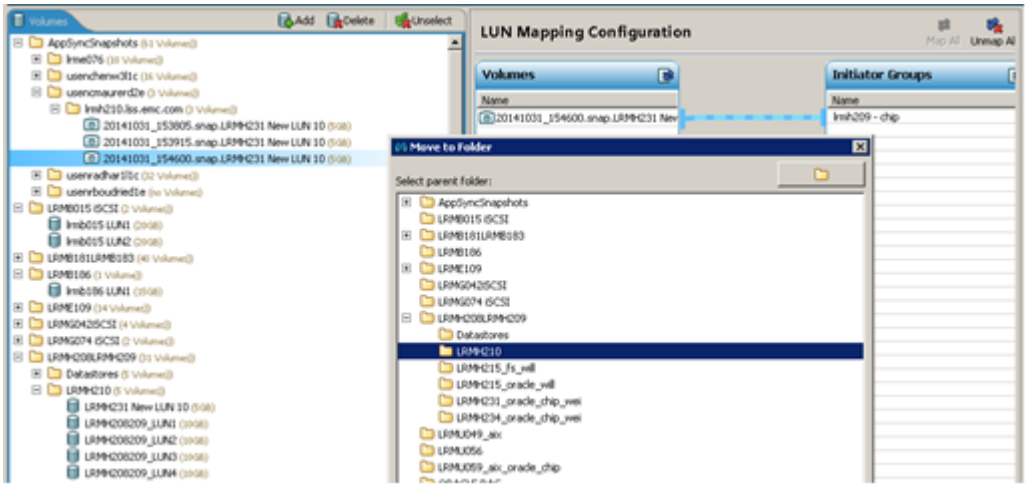


8. Remove the old production LUN from the initiator group.
9. Move the mounted snapshot from the `/AppSyncSnapshots` folder to the folder of the production LUN that you are replacing.

   Move the snapshot that is mounted (the snapshot that is currently masked to the production host initiator group or the ESX initiator group).

   After you finish, you will see the production LUN and the snapshot.

Figure 27 Production LUN and snapshot



One is a snapshot. The other is a volume.

Figure 28 One snapshot and one volume

10. Remove the volume that you want to replace.

    The snapshot becomes a volume.

Figure 29 Snapshot becomes volume

11. Rename the snapshot (now a volume) to the name of the volume that you replaced, and then run the file system service plan to create a snapshot of the "restored" file system.

CHAPTER 9

Protect VMware Datacenters

This chapter includes the following topics:

Configuration prerequisites

AppSync can create, mount, and restore copies in VMware vStorage VMFS and NFS data store configurations. Configuration prerequisites are required to integrate AppSync with VMware vStorage VMFS protection. Configure RecoverPoint and VMware according to the product documentation.

VMware configuration prerequisites

- VMware vCenter Server must be used in the environment.
- AppSync supports VMware's use of VSS with VM snapshots when a supported version of vSphere is installed and the VMware Tools facility is present on the virtual machine on the VMFS you are replicating. Refer to VMware documentation for information on the VSS-related characteristics in an AppSync copy. Contact VMware regarding considerations that are related to VSS in this configuration.
- When there is a configuration change in the vCenter Server, perform a discovery of data centers in the vCenter Server from the AppSync console before you protect a data store. Ensure that the VMFS UUID is unique in the virtual center inventory across all data centers.

Note

You can also create and manage copies of VMware data stores with the VSI for VMware vSphere web Client. The plug-in is available as a separate download from the AppSync Online Support page at support.EMC.com.

RecoverPoint configuration prerequisites

- Configure RecoverPoint protection (CDP/CRR/CLR) for the production LUNs before deploying AppSync. Refer to RecoverPoint documentation to create consistency groups and define replication sets.
- In an ESX cluster, target LUNs should be made visible to all the ESX hosts in the cluster.
- The AppSync server must connect to the RPA through the network.

VMware vStorage VMFS requirements

Some considerations apply when AppSync is introduced into a VMware environment for protecting VMware data stores.

All VMware specific operations occur through the VMware vCenter Server.

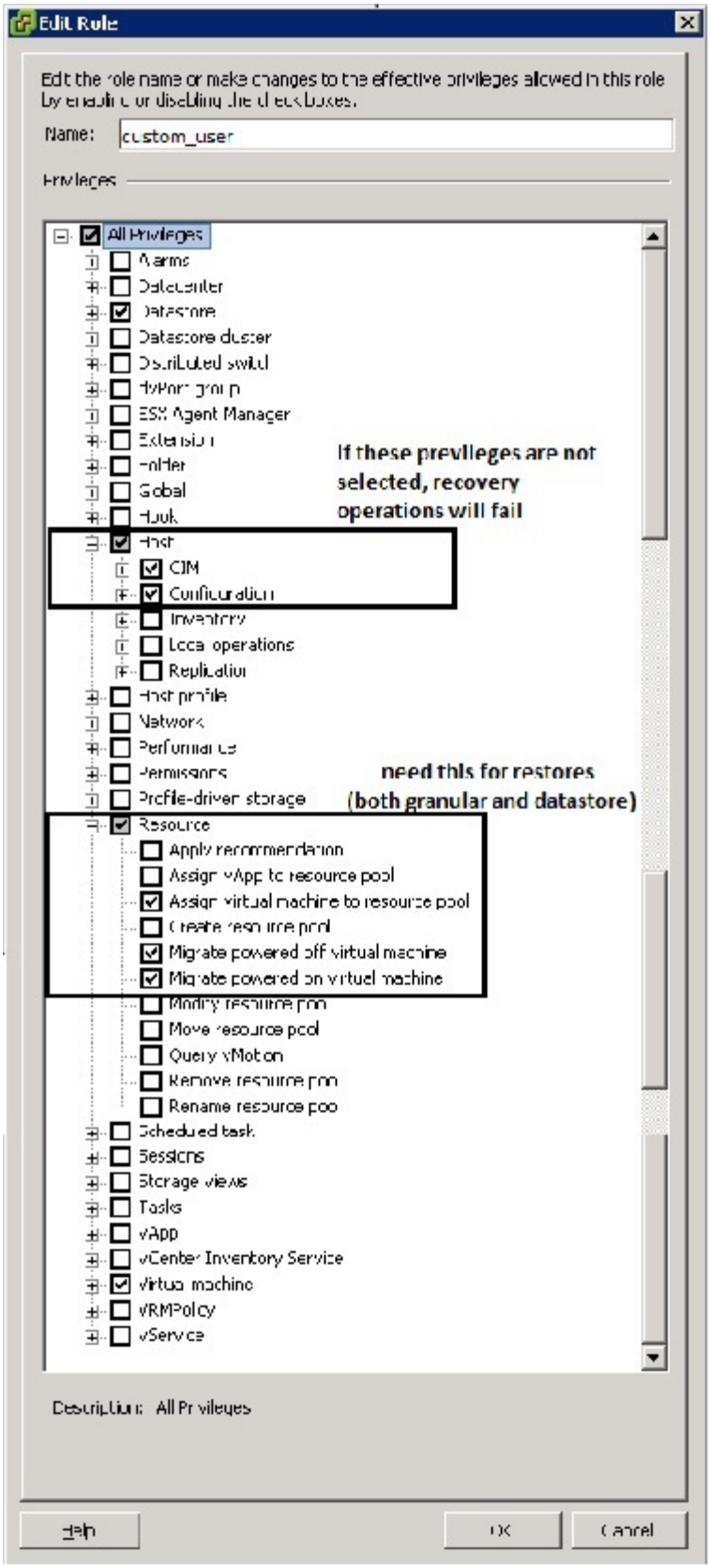
AppSync can be configured to require vCenter Server login credentials to allow protection of a certain VMFS for security purposes. Unless you instruct AppSync to omit this feature, AppSync takes a VMware Snapshot for each virtual machine that is online and residing on the VMFS before protection. This action ensures operating system consistency for the resulting replica. The following user roles for a Virtual Center ESX cluster are allowed with AppSync:

- Administrator
- VM power user
- VM user
- Resource pool Administrator
- VMware consolidated backup user

- Data store consumer
- Network Administrator

The following Edit Role screen capture shows privileges that you need to select for roles.

Figure 30 Privileges needed for VC roles for AppSync



AppSync supports VMware's use of VSS with VM snapshots when a supported version of vSphere is installed and VMware Tools are present on the virtual machine on the VMFS you are protecting. Refer to VMware documentation for use of the VSS-related characteristics in the AppSync copy and contact VMware regarding considerations that are related to VSS in this configuration.

If virtual machines in the data store have RDMs or iSCSI LUNs visible to them, the resulting copy does not contain those LUNs. If the virtual machine has virtual disks other than the boot drive located in other data stores, it is possible to capture these disks by configuring the service plan to include virtual machine disks.

Discovering datacenters

To keep AppSync up to date, discover datacenters on the VMware vCenter Server when there is a change in the configuration of the vCenter Server.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- At least one vCenter server must be added to AppSync.

Procedure

1. Browse to **Copy Management** › **VMware Datacenters**.
2. On the VMware Datacenters page, click **Discover Datacenters** › **On Virtual Center** and select a vCenter server to discover its datacenters.

   Optionally, you can also add a vCenter server by clicking **Add vCenter Server**. See Add a vCenter Server on page 186.

List of datacenters

The top level of the VMware Datacenters page shows all datacenters registered with AppSync.

Column	Description
Protection status of datacenter	• Green: Latest copies of all datastores on the datacenter protected successfully • Yellow: One or more of the latest datastore copies on the datacenter completed with errors • Red: One or more of the latest datastore copies on the datacenter failed to complete • "i" symbol: One or more datastores on the datacenter are either not subscribed to service plans or do not have copies associated with them
Name	Name of the datacenter on the vCenter server.
vCenter Server	Name of the vCenter server that hosts the datacenter.
Last Discovery	Time when a discovery was last performed on the vCenter server.
Alert Recipients	List of email aliases to receive email alerts.

Clicking on a datacenter name shows the datastores.

Adding a VMware vCenter Server

Add a VMware vCenter Server to AppSync when a virtual machine is used as a mount host for a VNX Snapshot copy.

Before you begin

- This operation requires the Resource Administrator role in AppSync.
- Ensure that you know the credentials of an account with Administrator privileges on the vCenter Server.

Procedure

1. Select **Settings** › **VMware vCenter Servers**.
2. Click **Add**.
3. Type the vCenter Server name.
4. Type the credentials for an account that has Administrator privileges on the vCenter Server.

List of VMware datastores

The list contains VMware datastores that have been discovered and stored in the AppSync database.

Clicking on the datastore name displays the copies of the datastore.

The Service Plan column shows the plans that the datastore is subscribed to. Other details include the type of datastore (VMFS or NFS), and name of the ESX server.

Protect a VMware datastore

Protect a VMware datastore by subscribing it to an AppSync VMware service plan.

AppSync's protection mechanism for datastores is by means of service plans. You subscribe a datastore to a service plan and run the service plan immediately, or schedule the service plan to run at a later time.

- Choose **Subscribe to Plan and Run** when you want to protect selected datastores immediately. The service plan is executed for the datastores alone.
- Choose **Subscribe to Plan** when you want to schedule the protection for later. Protection for datastores that are part of the service plan are executed at the scheduled time.
- Choose an appropriate service plan from **Create a copy using** in the datastore **Copies** page.
- Choose **Run** from the VMware Datacenters Service Plan page to run the whole plan immediately.

Subscribing VMware datastores to a service plan

The **Subscribe to Plan** operation schedules the protection for later. Protection for all datastores that are part of the service plan are executed at the scheduled time.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenters**.
2. Click a datacenter to display its datastores.
3. From this list, select the datastore to protect.

   Select multiple datastores by holding down the Shift or Ctrl keys on your keyboard.
4. From the **Protect** list, select the appropriate service plan from **Subscribe to Plan**.

   The selected plan appears in the Service Plan column for the datastore.

Protecting VMware datastores immediately

The **Subscribe to Plan and Run** operation adds datastores to an existing service plan and runs the service plan immediately for the selected datastores only.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenters**.
2. Click a datacenter to display its datastores.
3. From this list, select a datastore to protect.

   Select multiple datastores by holding down the Shift or Ctrl keys on your keyboard.
4. From the **Protect** list, select the appropriate service plan from **Subscribe to Plan and Run**.

   The **Subscribe to Plan and Run** dialog appears displaying the progress through the different phases.

List of protected virtual machines

The list contains virtual machines belonging to datastores that are protected as part of a service plan run.

Click on the virtual machine name to display copies of the virtual machine. To perform a restore operation, select a virtual machine and click **Restore**.

Other details include the OS platform on the virtual machine, the version of the virtual machine, the ESX host on which the virtual machine resides, as well as the path to the virtual machine file. In the path, the name of the datastore that the virtual machine resides on is within the [ ] parentheses.

Unsubscribing datastores from a service plan

You can unsubscribe datastores from a service plan or from all service plans that they are subscribed to.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenters**.
2. Click a datacenter to display its datastores.
3. From this list, select the datastore to remove from a service plan.

   You can select multiple datastores if they are subscribed to the same service plan. Select multiple datastores by holding down the Shift or Ctrl keys on your keyboard.

4. From the **Protect** list, select a service plan from **Unsubscribe from Plan**, or select **All** to remove the datastore(s) from all plans.

   The service plan name is removed from the **Service Plan** column for the datastore(s).

VMware snapshots

When the VM consistency option is selected, AppSync creates snapshots of all the virtual machines that are in powered on state while the datastore is being replicated.

AppSync creates a Quiesced snapshot of the virtual machines that are in powered on state. VMware Tools is used to quiesce the file system in the virtual machine. Quiescing a file system is a process of bringing the on-disk data of a physical or virtual computer into a state suitable for backups. This process might include operations such as flushing dirty buffers from the operating system's in-memory cache to disk, or other higher-level application-specific tasks. If the VM consistency option is not set, AppSync skips the process of creating the virtual machine snapshots.

Viewing datastore copies

The copies are named with the time at which they were made.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenters**.
2. Select a datacenter, then a datastore to view its copies.

   You can see other copy details such as copy type, mount status, the VM consistency status and the service plan associated with the copy.
3. Select a copy to see more details in the **Details** pane.
   - **Virtual Machines** tab: lists the virtual machines that are part of the selected datastore copy.
   - **Virtual Disks** tab: lists the virtual disks that are part of the selected datastore copy.
   - **Events** tab: lists the events that occurred when the datastore copy was created.

Viewing virtual machine copies

View the list of copies for a virtual machine based on the time they were made.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenter**.
2. Select a datacenter, then the **Protected Virtual Machines** tab.
3. Select a virtual machine from the list to view its copies.

   You can see copy details such as the size of the copy, storage on the disk, mode of the disk, and so on.
4. Select a copy to see additional details in the **Details** pane.
   - **Virtual Disks** tab: lists the virtual disks that are part of the selected virtual machine copy.

- **Events** tab: lists the events that occurred when the virtual machine copy was created.

Creating a datastore copy from the Copies page

Create a copy of a datastore by subscribing it to an AppSync VMware service plan from the **Copies** page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Copy Management** › **VMware Datacenters**.
2. Click a datacenter to display its datastores.
3. From this list, click the datastore to view its copies.
4. From the **Create a copy using** list, select the appropriate service plan.

   The service plan runs immediately for the datastore.

Expiring a datastore copy on demand

Expiring a copy removes it from the AppSync database and can free up storage, depending on the replication technology and the copy state.

Before you begin

This operation requires the Data Administrator role in AppSync.

Expiring a copy that was made with RecoverPoint does not remove the corresponding bookmark from RecoverPoint itself.

Procedure

1. Select **Copy Management** › **VMware Datacenters**.
2. Click a datacenter to display its datastores.
3. Click the datastore whose copies you want to expire.
4. From the **Copies** page, select one or more copies to expire.

   You can also perform this action from the Service Plan's **Copies** tab.
5. Select **Expire**.
6. Verify that you want to expire the copy you selected and any associated copies listed and confirm.

Service plan schedule

The schedule of a service plan is set in the **Plan Startup** phase.

The **Startup Type** (scheduled or on demand) determines whether the plan is run manually, or configured to run on a schedule. Options for scheduling when a service plan starts are:

- Specify a recovery point objective (RPO)
  - Set an RPO of 30 minutes or 1, 2, 3, 4, 6, 8, 12, or 24 hours
  - Minutes after the hour are set in 5 minute intervals
  - Default RPO is 24 hours
- Run every day at certain times

- Select up to two different times during the day
- Minutes after the hour is in 5 minute intervals
- There is no default selected

- Run at a certain time on selected days of the week
  - One or more days of the week (up to all seven days) can be selected
  - There is no default day of the week selected. Default time of day is 12:00 AM.
- Run at a certain time on selected days of the month
  - Select one or more days of the month (up to all days)
  - Select one time of day. Available times are at 15 minute intervals.
  - Default is the first day of the month

Overriding service plan schedules

You can set different schedules for individual datastores subscribed to a service plan, overriding the generic recurrence setting.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can override only the settings of the recurrence type already selected for the service plan.

Procedure

1. Navigate to **Service Plans** and select one of the plans from the list.
2. From the **Settings** tab, select the **Plan Startup** phase.
3. In the **Plan Startup Defaults** pane on the right, note the **Recurrence Type** selected for the plan.

   A recurrence type can be set only if **Scheduled** is selected as the **Startup Type**.
4. Click the **Plan Startup Overrides** tab.

   You can see the list of all datastores subscribed to the plan.
5. Select one or more datastores and click **Override Schedule**.
6. In the **Override Schedule** dialog, set the schedule based on your requirement and click **OK**.

   For example, if the default recurrence type is **On specified days of the month**, and the rule setting is to **Run at 12:00 AM** on the **1st day of every month**, you can override the time and the day for individual datastores.
   A Pencil icon indicates that default settings have been overidden.

Application discovery

Before creating the copy, AppSync performs discovery on the selected datastores and updates the AppSync database if there is any change in configuration of the vCenter server.

There are no user settings associated with this phase and it cannot be disabled.

Application mapping

After discovering the application, AppSync maps it to array storage, and protection services such as RecoverPoint.

There are no user settings associated with this phase and it cannot be disabled.

Create copy

The Create Copy phase creates a copy based on the preferred storage type specified by the user.

This phase specifies the type of datastore copy to make, and the storage settings for the copies. The copy phase creates a local copy, remote copy, or a local and remote copy based on whether you have chosen the bronze, silver, or gold service plan.

Review Overview: Service Plan on page 10 for more service plan copy information.

Datastore copy options

Select the copy type, the virtual machines to ignore for snaps, storage preferences, and the number of snapshot copies to retain.

- **Copy Consistency**

  `VM Consistent` creates a copy of the datastores in the service plan including running programs, processes, and even windows that were open at the time of the snapshot. `Maximum Simultaneous VM Snapshots` is the number of simultaneous snapshots of all VMs present. The default value is four snapshots.

  `Crash Consistent` creates a copy of the datastores in the service plan. Crash consistent copies have everything except data from the memory at the time of taking the snapshot.

  `Ignore VM Snapshots for VMs` link allows you to select virtual machines from the datastores added to the service plan. The selected VMs are ignored while taking VMware snapshots during the service plan run.

  `Include Virtual Machine Disk` includes all the datastores that are associated with the virtual machines running on the datastores being protected. For example, Datastore DS1 is subscribed to the service plan. Virtual Machine VM1 which is a part of DS1 has virtual disks in Datastores DS2 and DS3. When the service plan runs, datastores DS2 and DS3 are protected along with DS1. However, datastores DS2 and DS3 are not subscribed to the service plan.

- **Storage Ordered Preference**- the preferred order of storage technology to use while creating copies. Use the **Move Up** and **Move Down** buttons. Copies are made using the first technology preference when possible. If conditions are such that the first technology can no longer be used, then any remaining copies are processed in the next preference instead. For example, if the first preference was a bookmark but not all the application data in the service plan could be mapped to RecoverPoint, then AppSync uses VNX snapshots instead.

  Note

  A single service plan can contain a mix of VNX block, VNX file, and RecoverPoint replication objects. For example, if you have a Bronze service plan for VMware, the datastores can be a mix of RecoverPoint, VNX file, and VNX block replication.

- **Expiration** - the maximum desired number of RecoverPoint, VNX and VNX File Snapshot copies that can exist simultaneously.

Automatic expiration of RecoverPoint, XtremIO, VNX and VNX File, VMAX, and ViPR Controller snapshot copies
The automatic expiration value in a service plan's Create Copy phase specifies the maximum number of snapshot copies that can exist simultaneously.

When the "Always keep *x* copies" value is reached, older copies are expired to free storage for the next copy in the rotation. Failed copies are not counted. AppSync does not expire the oldest copy until its replacement has been successfully created. For instance, if the number of copies to keep is 3, AppSync does not expire the oldest copy until the fourth copy is created successfully.

This setting is independent of the VNX pool policy settings in Unisphere for automatic deletion of oldest snapshots. The service plan administrator should work with the storage administrator to ensure that the VNX pool policy settings enable the support of the specified number of snapshot copies for the application residing in that pool.

AppSync does not expire copies under the following circumstances:

- Mounted copies are not expired.
- A copy that contains the only replica of a datastore is not expired.

Include RecoverPoint copies in expiration rotation policy: Check this option to include RecoverPoint copies when calculating rotations.

Note

If this option is not selected, then RecoverPoint copies accumulates, and will remain until the bookmarks expire from the RecoverPoint appliance.

Unmount previous copy

The service plan unmounts a previously mounted copy after creating the new copy. The exception is a copy that was mounted on-demand as opposed to by the service plan. The on-demand mounted copy is not unmounted.

There are no user settings associated with this phase and it can be enabled or disabled.

Mount copy

The Mount copy phase mounts all the datastore copies created by that service plan run.

The **Mount Copy Defaults** settings for the copy to mount depends on the service plan. Other mount settings determine the mount host, access mode and mount signature.

This phase can either be enabled or disabled.

General Settings:

- **Mount on host**: lists all the ESX servers discovered on the registered vCenter servers.
- **Mount Signature**: lists **Use original signature** and **Use new signature** to select from. When **Use new signature** is selected, AppSync resignatures the VMFS volume on mount. Applicable only for VMware VMFS datastores.
- **Cluster Mount**: Select Yes or No .

RecoverPoint Settings:

- **Image access mode** (during RecoverPoint mount):
- **Logged Access**:
  Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes.
- **Virtual Access with Roll**:
  Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the

RPA transparently switches to direct replica volume access, allowing heavy processing.

- **Virtual Access**:
  Provides nearly instant access to the image; it is not intended for heavy processing.
- Desired Service Level Objective (SLO): Specifies the required VMAX 3 Service Level Objectives. SLO defines the service time operating range of a storage group.

VNX File Settings: This option is available only for VMware VNXFile datastores.

- **Mount Copy with access**: Select the type of access the copy should be mounted with - Read-only or Read-Write.

Overriding mount settings in a service plan

If there are multiple VMware datastores subscribed to the same plan, you can select different mount settings for each datastore, overriding the generic mount settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Navigate to **Service Plans** › **VMware Datacenters** and click one of the plans from the list.
2. From the **Settings** tab, select the **Mount copy** phase.
3. On the right pane, select the **Mount Copy Overrides** tab.

   The list of datacenters includes all vCenter datacenters whose datastores are subscribed to this plan. The mount settings display the default settings. Additionally, for VMAX v3 Datastores, SLO Service Level Objective appears as another option.
4. Select the datastore whose settings you want to override and click **Set Overrides**.

   Select multiple datastores by holding down the Shift or Ctrl keys on your keyboard.
5. On the **Mount Copy Overrides** dialog, select options only for those mount settings that you wish to override.

   For example, if you want to mount a copy to the production host, you would select **Use new signature** from the **Mount Signature** drop-down.

   Fields that do not have a selection retain their default settings.
6. Click **OK.**

   A pencil icon appears in the first column of the datastore's row whose default mount settings you changed.
7. To revert back to default settings, select the datastore(s) and click **Use Default Settings**.

Unmount copy

The final phase in the service plan unmounts the copy.

This phase is disabled if the **Unmount previous copy** phase is enabled. There are no user settings associated with this phase.

Considerations when mounting a VMFS copy

When you mount a VMFS copy to an alternate ESX Server, AppSync performs all tasks necessary to make the VMFS visible to the ESX Server.

- After these tasks complete, further administration tasks such as restarting the virtual machines and the applications must be completed by scripts or manual intervention.
- For datastore and virtual disk mounts on ESXi 5.x and RecoverPoint 4.0 environments, disable hardware acceleration to ensure successful virtual access type mounts. For more details, refer VMware Knowledge Base article 2006858.

Mounting a datastore copy on-demand

You can initiate an on-demand mount of a datastore copy from the datastore's **Copies** page, service plan's **Copies** tab or from a datacenter's **Datastore** page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. From the **Recover** popup button, select **Mount a Copy** in the **Datastore** or **Copies** page or Service Plan **Copies** tab.
2. Use the **Copies** or **Service Plan** filters to select the appropriate copy to mount.

   The copies list is refreshed based on the filters selected.
3. Select the copy to mount.

   For a RecoverPoint copy, you also have the option to select a bookmark based on a specific time. However, there should be a copy available in AppSync prior to the time you select.

   Click **Select a point in time** to select a copy with a specific time stamp and select the location of the copy (remote or local). Select **remote** to mount remote copy or **local** to mount local copy. The time shown here is the AppSync console's time. If the console is in a different time zone from the RecoverPoint Appliance (RPA), specify the time as per the server's time zone to mount the copy.
4. In the **Mount Additional Copies** page, select one or more additional copies to mount. The copies listed here are of other datastores that were protected at the same time and on the same datacenter as the copy you selected in the previous step.
5. On the **Select Mount Settings** page:
   a. From the **Mount on Host** list, select the host on which to mount the copy.

      All ESX Servers under the vCenter Server registered with AppSync are listed as possible mount host candidates. If a selected ESX is part of an ESX cluster, another field, Clutser Mount, is displayed, which can be set to Yes or No. If the ESX Server is part of a cluster you also have the option of mounting to all nodes of the cluster or just to the mount host you choose.

   b. From the **Mount Signature** list, select from one of these options: **Use new signature**, **Use original signature**. Applicable only for VMware VMFS datastores.

   c. In case of a RecoverPoint copy, from the **Image Access Options** list, select from one of these options:

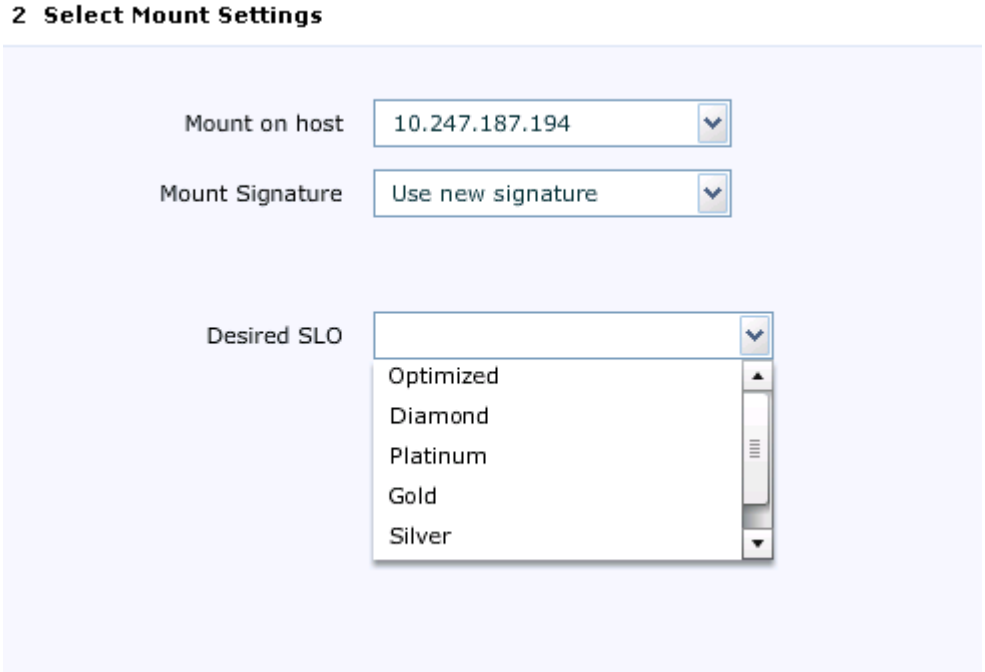
- **Logged access**: Use this mount option if the integrity check entails the scanning of large areas of the replicated volumes. Logged access is the only option available when you mount to the production host.
- **Virtual access with roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing. With RP VMAX, and RP XtremIO, virtual access with roll is not supported.
- **Virtual access**: Provides nearly instant access to the image. Virtual access is not intended for heavy processing. Virtual access with RP VMAX and RP XtremIO is not supported.

d. From the **Mount copy with access** drop-down list, select the type of access the copy should be mounted with: **Read-only** or **Read-write**. Applicable only for VMware VNXFile datastores.

e. For VMAX 3 arrays, you are presented with an SLO drop-down menu. You can select the desired Service Level Objective (SLO) for the mount copy.

If there is a storage group for the mount host with the desired SLO. AppSync will add the LUN to the storage group. If this storage group does not exist, AppSync adds the LUN to any storage group that is masked to the host. If a storage group is configured to pick target devices, AppSync removes the devices from the storage group at the time of mount and adds them to the storage group for the mount host. The devices will be added to the original storage group when the copy is expired. An example of the Desired SLO menu follows:

Figure 31 For VMAX 3 select Desired SLO



6. From the **Summary** page, review the copy and mount settings that you chose in the previous pages and click **Finish** to mount the copy.
7. In the **Results** page, click **Details** link to see the progress of the different phases that are part of mounting a copy.

The last phase completed is displayed at the bottom of the list of phases.

Unmounting a VMware datastore copy

When you select a copy to unmount, other copies that were mounted along with the selected copy are unmounted.

Before you begin

This operation requires the Data Administrator role in AppSync.

You can unmount a copy only from a list of copies made for a datastore.

Procedure

1. Navigate to the **Copies** page from the **Protection** or **Service Plan** pages:
   - **Copy Management** › **VMware Datacenters** › select the VMware datacenter that hosts the datastore, then select the datastore with the copy to unmount.
   - **Service Plans** › **VMware Datacenters**› select a service plan, then select the **Copies** tab.
2. From the list of copies, select the datastore copy and click **Unmount** from the button below.

   The **Unmount Confirmation** dialog displays all the copies of other datastores that were mounted along with the selected copy to be unmounted.
3. Click **Yes** to confirm the unmount of all the copies shown in the dialog.

   The **Unmount** window displays the progress of the unmount operation. All copies that were mounted along with the selected copy will be unmounted.

Restoring a datastore from a copy

You can perform a restore of a datastore copy from the datastore's Copies page, service plan's Copies tab or from a datacenter's Datastore page.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- Prior to restoring a datastore, it is recommended that you power off the VMs in the datastore.

Procedure

1. Select **Recover** › **Restore** from Datastore or Copies page or Service Plan Copies tab.

   The Datastore Restore wizard launches.
2. Select the copy to restore.

   Use the **Copies** or **Service Plan** filters to select the appropriate copy to restore. The copies list is refreshed based on the filters selected.

   For a RecoverPoint copy, you also have the option to select a bookmark based on a specific time. However, there should be a copy available in AppSync prior to the time you select.

   Click **Select a point in time** to select a copy with a specific time stamp. The time shown here is the console's time. If the console is in a different time zone from the RPA, specify the time as per the server's time zone to restore the copy.
3. Click **Next**.

If the selected copy has affected entities, the **Restore Warnings** page is displayed.

4. Read the warning messages for the affected datastores. Select the checkbox to indicate your agreement to restore other entities along with the selected copy.

   You can manually unmount the datastores that will be overwritten prior to restore.

   Only RecoverPoint copies have affected entities.

5. In the **Virtual Machine Operations** step, select the appropriate actions that you want AppSync to perform before and after restore. See Virtual Machine Operations on page 197 for details.
6. In the **Summary** page, review the settings that you selected in the previous pages and click **Finish** to perform the restore.
7. In the **Results** page, click **View Details** to see progress of the different phases that are part of restoring a copy.

   The last phase completed is displayed at the bottom of the list.

Virtual Machine Operations during restore

AppSync can perform operations on the virtual machines associated with the datastores selected for restore.

Table 21 Virtual Machine operations

Virtual Machine Operation	Description
VMs present at start of restore	**Power down VMs at start of restore**: If the virtual machines are present at the start of restore, AppSync shuts them down prior to beginning the restore operation. This is important for a successful restore.
Perform VM operations after restore	• **Return VMs back to state found at start of restore**: After restore, AppSync powers on the virtual machines and returns them to the same state they were at prior to restore. • **Register all virtual machines**: After restore, AppSync registers all virtual machines to the vCenter inventory. • **Register and power up all virtual machines**: After restore, AppSync powers on the virtual machines and registers them to the vCenter inventory. You can select only one of these options.
VMs not present at start of restore. Perform VM operations after restore.	• **Register all virtual machines**: After restore, AppSync registers all virtual machines to the vCenter inventory. • **Register and power up all virtual machines**: AppSync powers on the virtual machines and registers them to the vCenter inventory.

Datastore affected entities during restore

When you restore a datastore, AppSync calculates affected entities for other datastores that share the same storage.

An affected entity is data that resides on your ESX server that unintentionally becomes part of a replica because of its proximity to the data you intend to protect. You can prevent affected entity situations by properly planning your data layout.

In case of RecoverPoint or ViPR Controller, the granularity is at the consistency group (CG) level. If the CG is selected for restore, AppSync identifies other datastores residing on the same CG that were also protected alongside, and restores them. If the affected entity was not protected, AppSync will not be able to restore it properly. This is displayed as a warning in the Restore wizard.

There are no affected entities for VNX because multiple datastores cannot span the same LUN and multiple datastores cannot be hosted on the same File System.

If there are affected entities in your underlying storage configuration, the Restore Wizard notifies you of these items requiring you to acknowledge that additional items will be restored.

Restoring a VMware Datastore copy from XtremIO

Learn to semi-manually restore a Datastore copy on XtremIO with AppSync. Automated restore is available with AppSync version 2.2.2 and above and XtremIO 4.0 and above.

Before you begin

For automated restore, refer to Restoring a Datastore copy using the Restore Wizard on page 200.

For manual restore, ensure the following pre-requisites exist, then follow the steps:

- VMware Datastore copy residing on an XtremIO array.
- An AppSync service plan that replicates the Datastore.

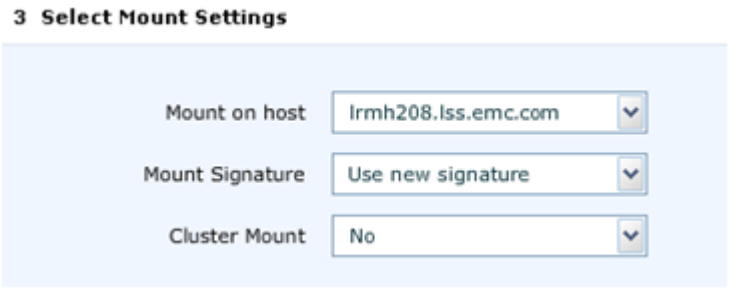
Procedure

1. On the AppSync console, select **Service Plans** › **VMware Datacenters**, and then click the wanted service plan, for example, **Bronze**.

   The **Copies** page displays existing copies.

2. Select the **Mount** copy to restore to production the ESX server.

   Figure 32 Select Mount Settings dialog box

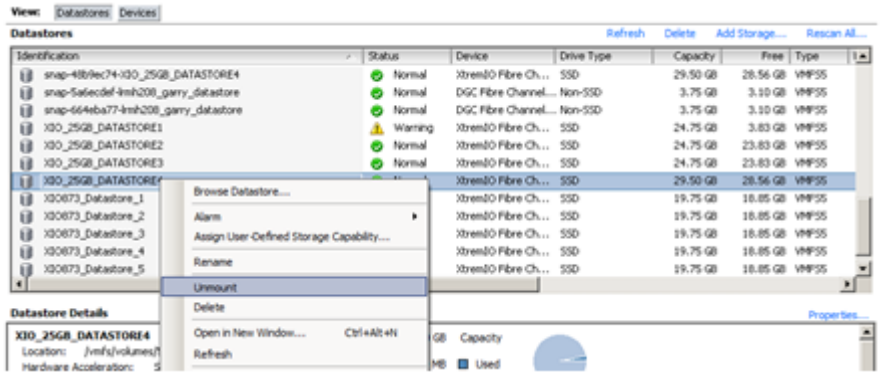


3. Stop any virtual machines from the Datastore that are being restored.

   If you do not want a virtual machine to be restored, use VMware vMotion to move it to another database. it to another Datastore.

4. Remove virtual machines on the Datastore that you are restoring from vCenter inventory.
5. Unmount the Datastore that you are restoring.

Figure 33 Unmount Datastore

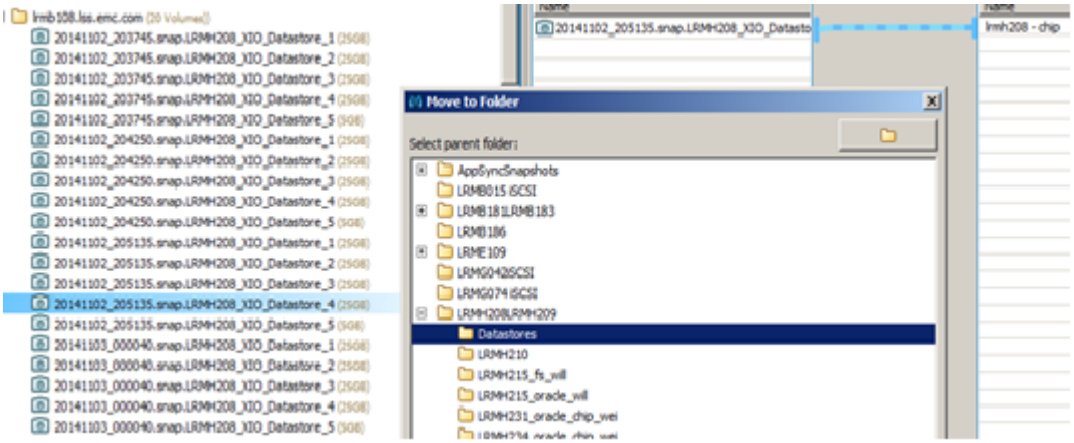


6. Delete the Datastore that you are restoring.
7. Rename the Datastore that is mounted by AppSync to the name of the production Datastore.
8. Select the **Remove** action against the mounted copy.

   This action removes the copy from the AppSync database without removing the snapshot on the mount host or on the XtremIO array. You receive a message that explains the **Remove** action. If the service plan has multiple Datastores, the storage for all Datastores in the service plan remain on the XtremIO storage array.
9. Remove the old production LUNs from the initiator group for the ESX.
10. Move the mounted snapshot from the `/AppSyncSnapshots` folder to the folder where the production LUN that you are replacing resides.

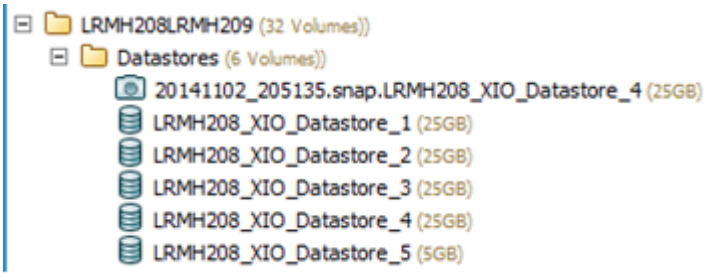
    Move the mounted snapshot (that is, the snapshot that is currently masked to the ESX initiator group). After you finish, the production LUN and the snapshot appear in the same folder.

Figure 34 Move mounted snapshot



After the move one Datastore becomes a snapshot, the other becomes a volume.

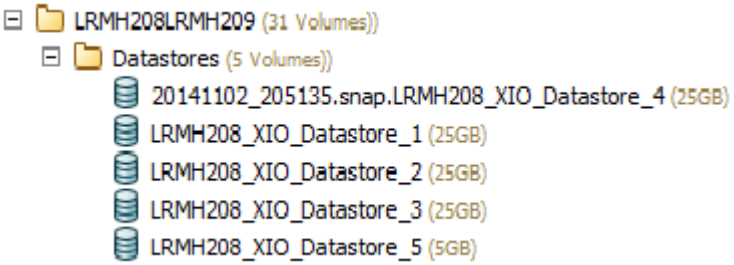
Figure 35 Snapshot and volume



11. Remove the volume that you want to replace with the snapshot.

    The snapshot becomes a volume.

Figure 36 Snapshot becomes volume



Note

All other snapshots in the `/AppSyncSnapshots` folder for the Datastore XtremIO volume that you just removed have also become volumes.

12. Rename the snapshot (now a volume) to the name of the volume that you replaced, and then perform any necessary virtual machine actions for the "restored" Datastore, such as VMware vMotion or add to the inventory.
13. Start all virtual machines in the Datastore that you want to run.

    The restored Datastore has a new Datastore ID in vCenter.
14. Unsubscribe the old Datastore from the service plan, subscribe the new Datastore , and then run the Datastore service plan to create a snapshot of the "restored" Datastore.

Restoring a virtual machine from a copy

You can perform a restore of a virtual machine from the **Protected Virtual Machines** tab or the virtual machine's **Copies** page.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- You must be using vSphere Enterprise Edition.
- All datastores used by the virtual machine must be protected by selecting the **Include Virtual Machine Disk** option in the **Create copy** phase of the service plan.
- The virtual machine should not have any pre-existing snapshots.
- Virtual machines with RDMS cannot be restored.

Procedure

1. Select **Restore** from the **Protected Virtual Machines** tab or the virtual machine's **Copies** page.

   The virtual machine Restore Wizard launches.

2. Select the copy to restore.

   Use the **Copies** or **Service Plan** filters to select the copy to restore. The copies list is refreshed based on the filters selected.

   For a RecoverPoint copy, you also have the option to select a bookmark based on a specific time. However, there should be a copy available in AppSync before the time you select.

   Click **Select a point in time** to select a copy with a specific timestamp. The time shown here is the console's time. If the console is in a different time zone from the RPA, specify the time according to the server's time zone to restore the copy.

3. Click **Next**.

   If other VMs were also protected along with the selected virtual machine, the **Multiple VM Restore** page is displayed.

   Select one of the following options:

   - Continue to restore only one virtual machine
   - View and/or select the other VMs for restore

4. In the **Select Restore Location** page, make the selections. See Virtual Machine restore options on page 202 for details.

5. In the **Select Mount Host** page:

   a. Select the mount ESX.

      If production data resides on RecoverPoint storage, the target devices should be visible to the selected mount host. In case of VNX, the mount host should be registered to the VNX.

   b. Select the RecoverPoint image access mode from the list - Logged Access, Virtual Access, or Virtual Access with Roll.

   c. Click **Next**.

   Note

   AppSync employs VMware vMotion technology to move the virtual machine from mount host to restore location. Therefore, the mount host and host at the restore location should satisfy the VMware vMotion prerequisites such as network requirement.

   In the **Choose Instant Restore** page, you can make a selection only if one of the following conditions is met:

   - The mount and restore hosts are the same.
   - The mount and restore hosts are different but are nodes of the same ESX cluster.

6. In the **Choose Instant Restore** page, select **Yes** or **No** for the **Do you want to perform an instant restore option** option, based on whether you want to perform an instant restore.

During instant restore, you can continue to use the virtual machine. Though the virtual machine is powered on, the VMs are restored in the background.

If you select **No**, and if you had chosen to restore multiple virtual machines in Step 2 of this wizard, specify a number in the **Maximum number of simultaneous virtual machines to be restored** box. By default, the number is 2.

Note

If you are restoring multiple virtual machines belonging to a vApp, set **Maximum number of simultaneous virtual machines to be restored** to 1.

If the source devices are think, the Instant restore option is not available for VMAX copies.

7. On the **Summary** page, review the settings that you selected in the previous pages and click **Finish** to perform the restore.
8. In the **Results** page, click **View Details** to see progress of the different phases that are part of restoring a virtual machine.

   The last phase completed is displayed at the bottom of the list.

Virtual Machine Restore options

You can select the restore location as well as restore operations.

Table 22 Virtual machine restore options

Restore Option	Description
Original location	Restores to the location where the virtual machine was present at the time of protection. **Note** For a RecoverPoint copy, restoring to the original location is not recommended. AppSync displays an appropriate warning when you select this option.
Alternate location	Restores to a location selected from the following options. All are mandatory. • vCenter Server: You can select either the same vCenter Server where the datastore with the virtual machine was at the time of protection or a different server. • Datacenter • Host • Datastore
Options if the VM being restored already exists in the restore location	• Fail the restore: AppSync checks for the existence of the virtual machines in the restore location. For those virtual machines that exist in the restore location, the restore operation is aborted. For the rest, the restore operation continues. This is a precautionary option. • Create a new virtual machine: AppSync creates a new virtual machine before restoring.

Table 22 Virtual machine restore options (continued)

Restore Option	Description
	• Unregister the virtual machine: If the virtual machines selected for restore exist in the restore location, AppSync unregisters them from the inventory before restoring. • Delete from disk before performing restore: If the virtual machines being restored exist in the restore location, AppSync deletes them before restoring. **Note** It is recommended you take a backup of the virtual machine before proceeding with the restore operation. • Delete from disk after performing restore: If the virtual machines being restored exist in the restore location, AppSync deletes them after restoring.

File or folder restore with VMFS or NFS datastores

Files or folders stored on virtual disks on a virtual machine in VMFS and NFS datastores can be restored through AppSync.

The virtual disks stored in a VMFS or NFS datastore that are protected by an AppSync service plan can be used for file or folder level restore by specifying the location for mounting the virtual disk copy.

Within AppSync, file or folder level restore is a three phase process: To complete the restore, the final step is performed manually outside of AppSync. You must copy the files or folders from the location where the virtual disk is mounted to a location of your choice.

1. AppSync mounts the datastore snapshots to the ESX server on which the virtual machine with the AppSync agent resides.
2. The vCenter server adds the virtual disks from the datastore snapshots to the mount VM without powering off the VM.
3. AppSync agent performs a filesystem mount to the mount VM.

Restore of files or folders from virtual disks with multiple partitions is supported.

If the ESX server version is 5.0 and higher, the original VM can also be the mount VM.

Restrictions

- File or folder level restore is not possible on dynamic disks.
- Virtual disks belonging to same phase pit cannot be mounted to the same virtual machine even when created using the Gold service plan. In other words, if a virtual disk from a local copy is mounted; then the same virtual disk from a remote copy cannot be mounted.
- To perform an Any Point in Time (APiT) file restore, you must first perform an APiT mount of the datastore and then launch the Granular File Restore wizard from the APiT copy.

Restoring a file or folder from a virtual disk

You can perform the restore of a file or folder of a virtual disk from the **Protected Virtual Machines** tab or the virtual machine's **Copies** page.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- You must be using vSphere Enterprise Edition.
- The virtual machine on which the copy is mounted and restored must be 64-bit with Windows 2008 or Windows 2012 as the operating system. The AppSync host plugin must be installed on it and it should be registered with the AppSync server.

Procedure

1. Select **Restore** › **File** from the **Protected Virtual Machines** tab or the virtual machine's **Copies** page.

   The Granular File Restore Wizard launches.

2. Select the copy to restore.

   Use the **Copies** or **Service Plan** filters to select the appropriate copy to restore. The copies list is refreshed based on the filters selected.

3. Click **Next**.

   The **Select Virtual Disk** page appears displaying the virtual disks in the selected virtual machine.

4. Select the virtual disks whose files or folders must be restored and click **Next**.
5. In the **Select Host** page:

   a. Select the virtual machine on which the copy must be mounted.

      In addition, specify the location in the selected virtual machine where the disk must be restored to. By default, the files are restored to the following location: `%system drive%\AppSyncMounts\<VM_name>\<copy_id>\Hard disk#` where:

      - `%system drive%` is system drive of the selected virtual machine on which the copy is to be mounted
      - `<VM_name>` is the name of the virtual machine whose virtual disks are being restored
      - `<copy_id>` is an AppSync generated ID
      - `Hard disk#` is the number of the hard disk in the virtual machine. This number is the same as on the original virtual machine.

   b. Select the RecoverPoint image access mode from the list - Logged Access, Virtual Access or Virtual Access with Roll.

6. In the **Summary** page, review the settings that you selected in the previous pages and click **Finish** to start the restore of the disk.
7. In the **Results** page, click **View Details** to see progress of the different phases that are part of restoring a virtual disk.

   The last phase completed is displayed at the bottom of the list.

8. Next, perform the manual step of copying the required files or folders from the mount location to a location of your choice.

9. Optionally, unmount the datastore. Unmount a datastore copy on page 196.

CHAPTER 10

Monitor AppSync

This chapter includes the following topics:

RPO concepts and best practices

A recovery point objective (RPO) is one of several scheduling options that can be selected as part of a service plan's Plan Startup phase.

When you subscribe an object (such as an Exchange database) to a service plan that uses RPO as its recurrence type, the object acquires the recovery point objective specified in the service plan.

Since you can subscribe an object to more than one service plan, it is possible for an object to have more than one recovery point objective. When an object has more than one RPO, the service plan with the highest RPO frequency (that is, the lowest RPO hours value) is used for calculation and reports.

As a best practice, you should subscribe an object to only one RPO-enabled service plan. If you subscribe an object to additional service plans, they should not use the RPO-based recurrence type.

Recovery point compliance report

The recovery point compliance report shows the recoverability for all objects that are subscribed to service plans with an RPO recurrence type. The report is at **Monitoring › Recovery Point Compliance Report**.

Table 23 Recovery Point Compliance Report

Column	Description
Server	Host level object, such as a Microsoft Exchange Mailbox Server
Application	Name of the protected object, such as a Microsoft Exchange database. Click the name to go to the list of copies for the object.
Recovery Point Objective	The recovery point objective as defined in the Start phase of the associated service plan.
Time Since Last Recovery Point	Amount of time since the last copy or bookmark created by the associated service plan. A green icon indicates the copy is RPO compliant. A red icon indicates non-compliance.
Service Plan	Name of the service plan. Click the name to go to the service plan definition.

Exporting an RPO compliance report to CSV

You can create a recovery point objective (RPO) compliance report in comma-separated value format.

Before you begin

No particular AppSync role is required for this operation.

Procedure

1. Navigate to **Monitoring › Recovery Point Compliance Report**.
2. Sort and arrange columns as desired for the report.
3. Click **Export** to run the Export wizard.

You have the option to include table headers and export only selected rows. The default file name is "Recovery Point Objectives_*mm_dd_yyyy_hh_mm_ss*.csv".

Summary of RPO compliance

The Recovery Point Objectives (RPO) summary on the dashboard shows the percentage of RPOs met across all objects that are subscribed to RPO-enabled service plans.

Alerts and associated events

AppSync generates an alert when a service plan phase fails, when a recovery point objective (RPO) is not met, or when a mount or restore fails.

Service plan failure alerts are generated immediately on failure of a service plan phase. When an application goes out of RPO compliance, the associated alert is generated within 1 hour. Refer to Acknowledging alert icons for database, file system, and data store service plan runs on page 210, for information.

AppSync displays alerts in the console at **Monitoring** › **Alerts**.

Table 24 Details of alerts

Column	Description
Alert (!)	Level of alert
Time	Date and time of the alert.
Server	Application server, such as a Microsoft Exchange server.
Application	Replicated object, such as a Microsoft Exchange database.
Category	Phase Failure, RPO
Service Plan	Service plan that was running when the alert was generated, or the service plan that created the copy that failed a mount or restore.
Message	Describes the cause of the alert.

You can filter alerts by the time they were generated and by the associated service plan.

View the associated events that led up to the alert by clicking the alert. Expand the top-level events to see additional details. You can filter associated events by any column.

Acknowledging alerts

With AppSync version 2.2.2 and later you can acknowledge alerts. Refer to Acknowledging alerts on page 209, and Acknowledging alert icons for database, file system, and data store service plan runs on page 210 for more information.

Acknowledging alerts

These steps show you how to acknowledge alerts for monitoring.

You can choose to acknowledge alerts that are shown in the console, **Monitoring** › **Alerts**. The alerts page display shows a column for **Alert Acknowledged**.
A value of No is the default. When you acknowledge an alert, the value of the alert changes to YES from the default value NO.

Procedure

1. Go to **Monitoring** › **Alerts** and select an alert from the alerts table with a current value of **NO** in the Alert Acknowledged column.
2. Click **Acknowledge Alert**.

Results

The alert displays a value of **YES** in the Alert Acknowledged column of the Alert table.

Acknowledging alert icons for database, file system, and data store service plan runs

You can acknowledge an alert icon within the AppSync console for Oracle and SQL databases, file systems, and data stores.

An alert icon indicates the status of the most recent service plan run. The icon appears beside a database, file system, or data store after the run.
After you acknowledge the icon in the Acknowledge column, AppSync changes the icon to an information icon. Also, you can acknowledge the alert after every Service Plan run. You are not restricted to acknowledge an alert only once.

Note

If a delete is pending, then the Acknowledge button becomes disabled for the database, file system, or data store.

The following procedure shows you how to view and acknowledge the alert.

Procedure

1. Select an alert from the database, file system, or data store table that has an alert icon that is associated with the last service plan run.
2. Click the **Acknowledge Alert** button that is located below the database, file system, or data store table.

   The alert icon changes to an information icon.
3. If wanted, re-run the service plan on the same database, file system, or data store to display the alert icon for this run.

Sending alerts via email

You can configure AppSync to send failure alerts via email to a list of recipients.

You enable alert emails and add recipients per application instance, such as an Exchange mailbox server.

Note

You can also configure AppSync to send email after successful completion of a scheduled service plan. This is disabled by default. Contact Customer Support if you want this enabled.

Configuring server settings for email alerts

Configure SMTP services on a machine that the AppSync server can access.

Before you begin

This operation requires the Resource Administrator role in AppSync.
Refer to SMTP documentation for configuration procedures.

Procedure

1. Select **Settings** › **AppSync Server Settings**.
2. Under **Send Mail** settings, enter values for SMTP server, port, and sender.

   Use **Test** to validate the settings. Enter a recipient's address and then check the recipient's inbox. You can also select **Insert Default Values**.
3. Click **Apply**.

Specifying email alert recipients

Configure email alerts per application instance level.

Before you begin

- This operation requires the Data Administrator role in AppSync.
- SMTP services must be configured on a machine accessible by the AppSync server. See Configuring server settings for email alerts on page 210.

Procedure

1. Select **Copy Management** › **Application (select application)**.
2. Select the application object for which to set alert settings.
3. Select **Alert Settings**.
4. Enter one or more email recipients, separated by commas (,) and click **OK**.

   A test email is sent to recipients for verification.

Repurpose Monitor

This topic describes the Repurpose Monitor.

The Repurpose Monitor shows all in-progress Repurpose and Refresh processes. It enables you to view currently running repurpose activities and to monitor their progress. It shows the current copy you are repurposing (making a snap of a snap copy), and related copy labels such as 1st Gen (generation) or 2nd Gen.

You typically use the Repurpose Monitor for long-running repurpose activities (for example, VMAX Clone synchronization). When you select this monitor, it lists all the repurpose activities in progress. Select any repurpose activity, and then select **Monitor** to launch a progress dialog to directly view the progress of the selected activity.

To launch the Repurpose Monitor:

1. On the AppSync console select **Monitoring**.
2. Select **Repurpose Monitor** on the Monitoring page to launch.