

# AppSync 2.2.2 Integration with RecoverPoint and XtremIO

Managing RecoverPoint Snap-based replication for XtremIO using Role Based Users

## Abstract

This white paper describes how to configure EMC® AppSync® to support RecoverPoint® local, remote, or local and remote Snap-Based replication on XtremIO®, specifically designed for role based users.

January 2016

Copyright © 2016 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on [EMC.com](http://EMC.com).

Part Number H14663

## Table of Contents

<b>Executive summary.....</b>	<b>4</b>
Audience .....	4
<b>Introduction.....</b>	<b>4</b>
<b>Prerequisites and Restrictions .....</b>	<b>5</b>
AppSync .....	5
XtremIO .....	5
RecoverPoint .....	6
Replication Types Used.....	6
Application Consistent vs. Crash Consistent .....	7
<b>Technical Overview.....</b>	<b>7</b>
Terminology.....	7
<b>Configuring AppSync.....</b>	<b>8</b>
Enabling XtremIO.....	8
Enabling RecoverPoint.....	8
Enabling Role Based Users and Access Controls .....	8
Role Based Users.....	9
Access Control Lists.....	9
<b>Process Flow.....</b>	<b>10</b>
Creating Users.....	10
Governing Rules for the Data Administrator Role.....	10
Adding Storage.....	10
Adding RecoverPoint .....	11
Adding XtremIO .....	11
Enabling ACL Management.....	11
Subscribing to a Service Plan.....	13
The Bronze Service Plan.....	13
The Silver Service Plan.....	13
Include RecoverPoint copies in expiration rotation policy .....	14
Subscribe the Application to the Service Plans .....	14
Executing Use-Cases.....	15
Backup Acceleration.....	15
Operational Recovery.....	16
Data Repurposing.....	17
Application Considerations.....	19
<b>Conclusion.....</b>	<b>22</b>
<b>References .....</b>	<b>22</b>

## Executive summary

EMC® AppSync® is a service-level agreement (SLA) driven, self-service, software for managing copies of various applications/databases running on various EMC arrays - EMC XtremIO®, EMC VNX®, EMC VNXe2®, EMC VMAX®, EMC RecoverPoint® and EMC ViPR-C®. AppSync provides a web-based interface to centrally managed light-weight application software. Application owners can use AppSync to create and manage copies of their data in a self-service manner. This alleviates many of the conventional inefficiencies associated with copy requests, for things such as creating copies for development, operational recovery, operational patch management, and analytic reporting, to name just a few.

## Audience

This white paper is intended for EMC customers, partners, and employees who want to manage copies on an existing XtremIO arrays using RecoverPoint, with AppSync. Familiarity with AppSync, RecoverPoint, and XtremIO based-solutions is expected.

## Introduction

AppSync provides a web-based user interface. AppSync integrates natively with various applications and databases. It also integrates with RecoverPoint to create RecoverPoint Bookmarks for application objects. AppSync focuses on three primary use-cases:

1. Backup acceleration,
2. Operational recovery
3. Repurposing

AppSync allows role based access control for copy management, restricting user access based on roles and responsibilities.

Access to managing application objects, such as databases and files systems, can be further restricted with Access Control Lists. These items in AppSync are found under 'Copy Management' tab.

XVC Snaps on XtremIO are a perfect way to address the needs of backup acceleration, rapid operational recovery, and the repurposing of data in agile environments.

EMC RecoverPoint provides local, remote, or local and remote continuous data protection, for XtremIO and other block based EMC storage arrays. It offers the ability for disaster recovery at a near zero recovery point objective. RecoverPoint Bookmarks can be created automatically throughout the day, as seen in Figure 1.

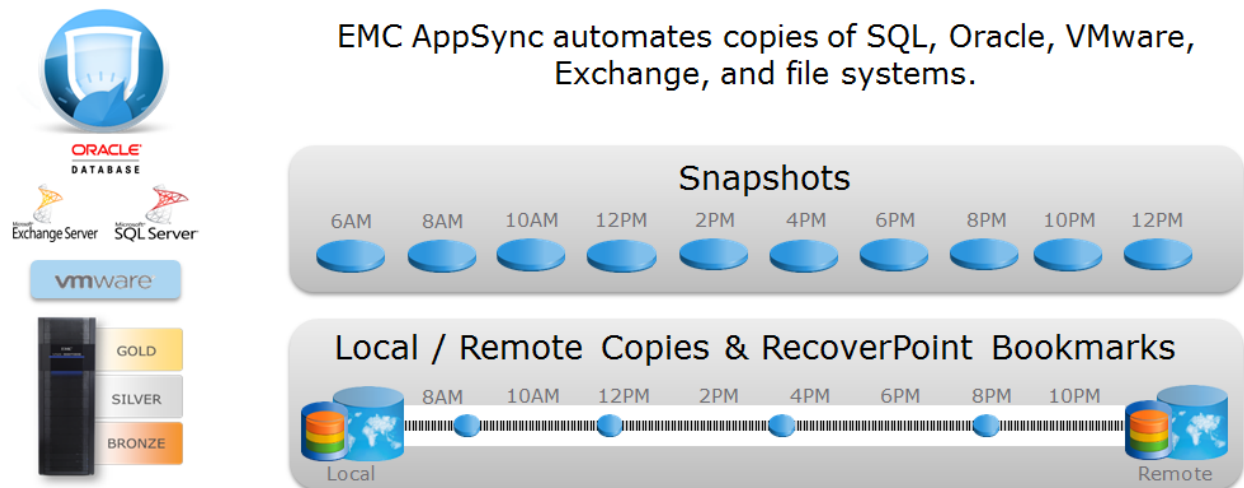


Figure 1

## Prerequisites and Restrictions

### AppSync

- The EMC AppSync server and host plug-in software is assumed to be installed, and the host's applications discovered according to the EMC AppSync Installation and Configuration Guide.

### XtremIO

- Ensure the XtremIO is configured according to the EMC XtremIO documentation. The minimum version supported is 4.0.0-64.
- It is assumed the local and remote arrays are XtremIO. If choosing an alternative array, such as using a VNX at the target site, please plan accordingly.
- There is a new **rp\_user** hidden user account added to XtremIO to support RecoverPoint configurations. This user has the configuration role only, and is not used normally.
  - The **rp\_user** is authorized for all RecoverPoint objects
  - Used when adding XtremIO to RecoverPoint
  - Password must initially be set with the **modify-password usr-id="rp\_user"**
  - Please see the *EMC XtremIO Storage Array Versions 4.0 and 4.0.1 Security Configuration Guide* for more details.

## RecoverPoint

- Ensure the RecoverPoint environment is fully configured according to EMC RecoverPoint documentation, including the setup and configuration of Consistency Groups.
- AppSync supports: Local, Remote, and both Local and Remote replication. The minimum RecoverPoint version supported with XtremIO is 4.1.2.
- AppSync requires that when doing both RecoverPoint Local and Remote, the replication consistency groups have both local and remote copies defined – in anticipation for failover.
- RecoverPoint restricts creating parallel bookmarks, so AppSync cannot protect more than one consistency group, together, in the same Service Plan. This is a RecoverPoint restriction. It is recommended to have one Consistency Group protection per Service Plan, if XtremIO is the backend. RecoverPoint Consistency Groups are fully aligned with XtremIO's Consistency Groups.
- AppSync supports dynamic mounting, where LUNs are mapped to hosts during mount operations. Ensure hosts hosting replicated volumes are zoned appropriately and XtremIO Initiator Groups are defined for all mount hosts to which AppSync mounts XtremIO copies. Dynamic mounting of RecoverPoint Bookmarks also require adding the XtremIO storage array to the AppSync user interface.
- AppSync supports RecoverPoint “Logged Access” mode only, while mounting RecoverPoint copies on an XtremIO backend. Image access for XtremIO volumes is instantaneous, as it does not utilize journals.
- Mounted RecoverPoint copies must be unmounted prior to restoring.
- Snapshots created on the XtremIO by RecoverPoint should not be modified in any way. These snapshots are hidden by default.
- Use the **rp\_user** when adding the XtremIO array to RecoverPoint, depicted in the previous section.
- In addition to creating applications consistent RecoverPoint bookmarks, AppSync also supports creating array based copies off RecoverPoint bookmarks, where the RecoverPoint image is the intermediary copy when using the **Repurposing** workflow.

## Replication Types Used

AppSync undertakes the existing array based, or RecoverPoint technology. RecoverPoint utilizes a series of snapshots on the XtremIO to keep track of changes, rather than the traditional journaling feature. Long term retention is possible by creating array based copies.

Please be aware that XtremIO snapshots are finite, and so are the number of RecoverPoint bookmarks, 500 per volume as of 4.1SP2. RecoverPoint allows the

configuration of the maximum snapshots, per copy, as well as the frequency of RecoverPoint PiT copies – both settings are configurable within RecoverPoint’s consistency group policy. Bookmarks are purged based on the standard RecoverPoint consistency group’s policy. It is recommended to review the *EMC RecoverPoint Replication of XtremIO* white paper in order to ensure the proper protection window is maintained. If RecoverPoint creates, for example, a PiT every minute, and AppSync creates a bookmark every hour, there is a chance that the most recent PiT copy becomes purged, leaving the AppSync bookmark, due to AppSync’s created bookmarks taking priority. In addition, the AppSync bookmarks may be purged before the anticipated time, due to the large number of RecoverPoint generated PiT copies. Settings such as limiting the Copy Policy’s **Maximum Number of Snaps**, or increasing the Link Policy’s **RPO** setting, may be required.

## Application Consistent vs. Crash Consistent

Application consistent bookmarks and crash consistent bookmarks differ in that when performing an application consistent bookmark, the application is momentarily frozen before taking the copy.

- Copies are guaranteed to be recoverable

AppSync supports application consistent copies, which are critical for backup acceleration and operational recovery - after a restore operation. Application consistency can maintain a low recovery point objective, while also minimizing the time it takes to recover - maximizing SLA performance.

Crash consistent copies use array level consistency, bypassing any application freeze. Crash consistency does not guarantee the application is recoverable, but does ensure that the application can be restarted. There are use cases where crash consistency is all that is needed, however, such as an environment where copies are being utilized for development and testing. AppSync offers the ability to support crash consistent copies, which speeds up the copy creation process, and lowers any potential production impact.

## Technical Overview

### Terminology

- Application Objects – The databases, file systems, or VMWare Datastores running on the hosts and which are subscribed to Service Plans – items being managed by AppSync
- Copy Management – The process of creating and managing the lifecycle of copies of various application objects
- Generation – used specifically with repurposed copies to distinguish between how removed the copy is from production, such as with a copy-of-production (Gen 1), or a copy-of-copy-of-production (Gen 2)

- Local and Remote, or Local and Remote Copy, also referred to as the Gold level Service Plan – is both local and remote array based copies or RecoverPoint Bookmarks
- Local or Local Copy, also referred to as the Bronze level Service Plan - is a local array based copy or a local RecoverPoint Bookmark
- Remote or Remote Copy, also referred to as the Silver level Service Plan – is a remote array based copy or a remote RecoverPoint Bookmark
- Repurposing – AppSync’s workflow for the creation of multi-level generation copies of production
- Service Plans – The policies which AppSync uses to abstract the various settings required to create and manage copies. It is broken down into multiple phases and contains application specific settings, storage specific setting, schedule, lifecycle specific setting to name a few.
- User Role or just Role – one or more user object permissions based on user responsibility
- Recover vs. Restore – Recover refers to mounting an application on another host and playing the logs to bring the application to the latest point in time, while restore refers to overwriting the original production volume, with the copy

## Configuring AppSync

### Enabling XtremIO

For long term retention or extended use cases, XtremIO snapshots are preferred over RecoverPoint bookmarks. In order to enable XtremIO snapshots, add the XtremIO Management Server which communicates with the AppSync Server over TCP port 443.

### Enabling RecoverPoint

In order to create local, remote, or both local and remote RecoverPoint Bookmarks with AppSync, the local RecoverPoint appliance is added to the AppSync environment. AppSync communicates with RecoverPoint over TCP port 7225. RecoverPoint is managed as a storage platform. It is not necessary to add the underlying storage array unless also creating snapshots on the array as explained above. Only the local RecoverPoint IP is added to AppSync. The remote appliance is auto discovered, though port 7225 must also be opened between the AppSync Server and the remote RecoverPoint appliance.

### Enabling Role Based Users and Access Controls

AppSync provides role based authentication, allowing, for example, a storage administrator to add and configure the storage, manage licensing, and add hosts. A system administrator can in turn, configure and run Service Plans, and yet another user, such as a database administrator, can manage their own application replication environment; refreshing their UAT/QA environments for example. The following roles in Figure 2 are available for AppSync users. Refer to the “Access control user roles



and permissions” section in the AppSync Security Configuration Guide for additional details.



Figure 2

### Role Based Users

The default **admin** user is a composite of the four roles above. Roles help isolate responsibilities. A combination of roles is also possible.

### Access Control Lists

Access Control Lists (ACLs) are used exclusively with the **Data Administrator** role, either to restrict, or be restricted to, specific application objects.

The default **admin** user has the **Data Administrator** role but is not capable of assigning access controls on application objects. Enabling the **ACL Management** option for the **admin** user, as seen in Figure 3, allows the admin user to enable access controls on application objects.

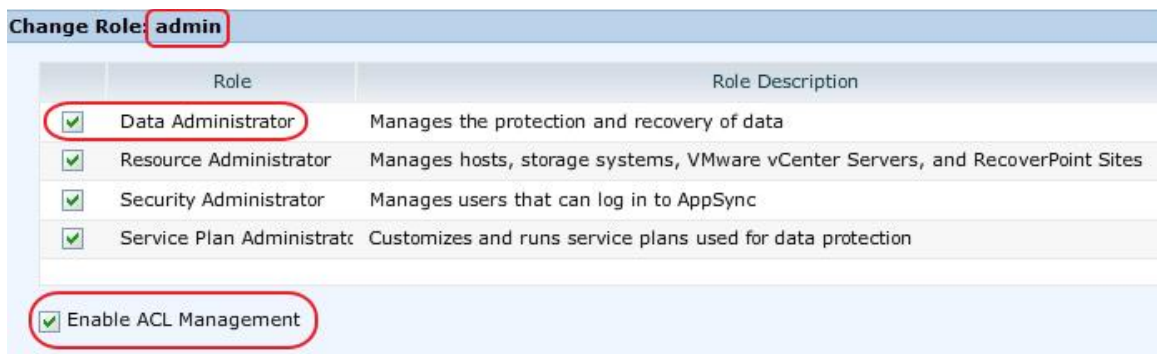


Figure 3

## Process Flow

Please refer to the process flow in Figure 4 for integrating RecoverPoint, XtremIO, and ACL based users within AppSync. The application hosts and their objects are presumed to have already been discovered. Otherwise, a Resource Administrator can add and discover them.

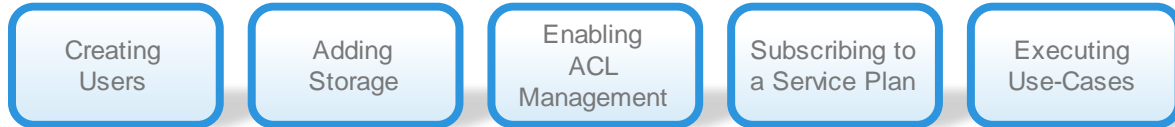
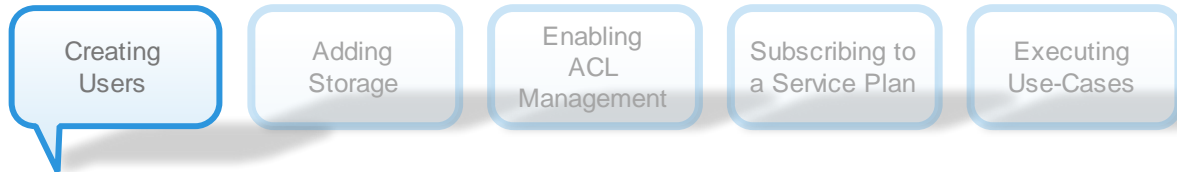


Figure 4

### Creating Users



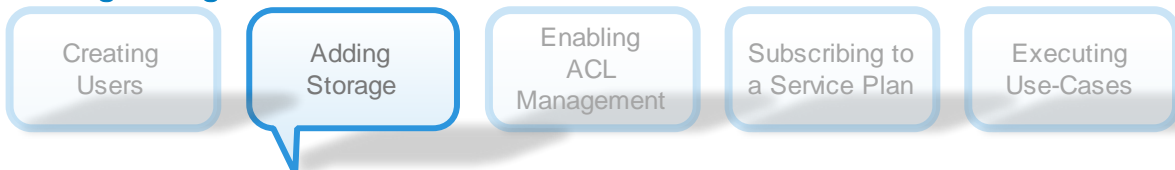
AppSync provides the ability to restrict users based on their roles. A **Role** determines resource level permissions. For example, a **Resource Administrator** can add the RecoverPoint and XtremIO arrays, while a **Data Administrator**, who has been explicitly given credentials to an ACL managed application object, can manage that object, such as a database.

### Governing Rules for the Data Administrator Role

- **Data Administrator + Enabled ACL Management** + optionally any other role - Can enable ACL management on application objects and restrict other Data Administrators without the Enable ACL Management option, to those application objects
- **Data Administrator** only - Can manage non-ACL enabled and explicitly granted ACL enabled application objects

Only a user with the **Data Administrator** role can be restricted by ACLs, as they manage data, such as databases, datastores, and file systems. Only data objects under Copy Management can be restricted by ACLs.

### Adding Storage



## Adding RecoverPoint

The **Resource Administrator** role is used to add the local RecoverPoint cluster by providing the management cluster name, RPA name, or the IP address, and entering a user with RecoverPoint administrative privileges. Any remote cluster is added automatically – AppSync discovers all sites. AppSync does not have a special license for RecoverPoint. It just uses the license of the underlying array, XtremIO in this case.

## Adding XtremIO

The **Resource Administrator** role is used to add the XtremIO arrays by adding the name or IP address of the XtremIO Management Server (XMS) and a user with administrative permissions. Copies can be managed on all the arrays managed by the XMS. AppSync uses bricks based licensing for XtremIO. Licenses are needed for all the bricks in the arrays which need to create and manage copies..

## Enabling ACL Management



ACL Management is first enabled on an application object, and then a **Data Administrator** can be given permission to manage that object, such as protecting a database by subscribing to a service plan for protecting, mounting, repurposing or recovering that application.

To enable ACL Management on a particular application object, refer to Figure 5.

Step 1 - Select the application object\* from the **Copy Management** section

Step 2 - Click **ACL Settings**

Step 3 - Select **Enable ACL support** and the user(s) who should be authorized to manage that particular application object

\*Note: The application object can be the server, or a specific child object. Child objects are inherited from their parent, though additional users can also be added to those child objects.

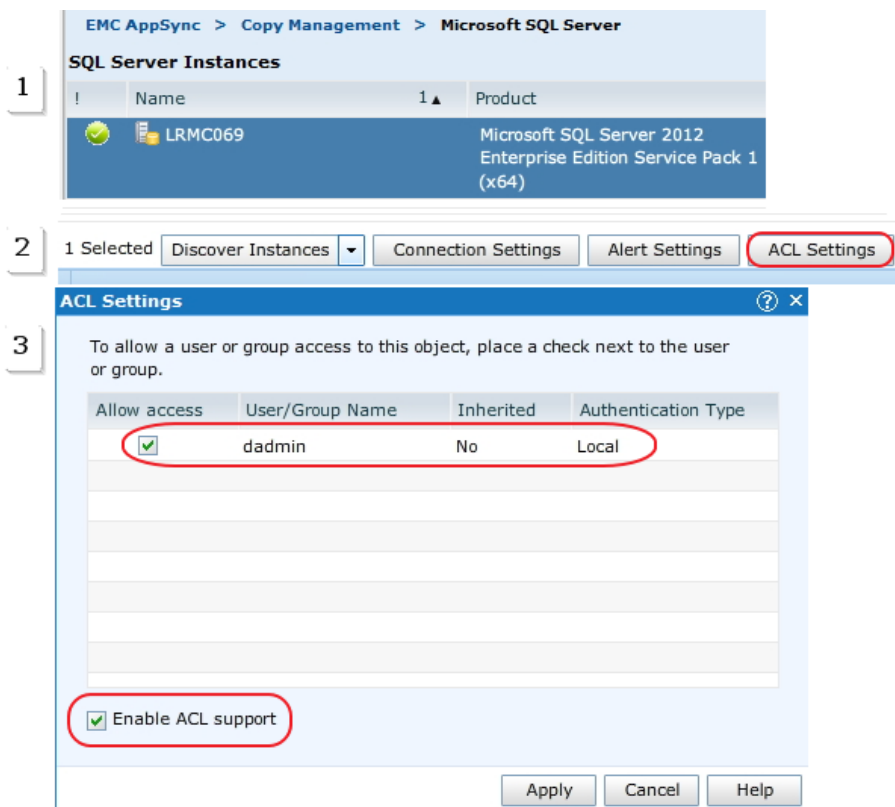


Figure 5

The **dadmin** user, who is an end-user with the Data Administrator role only, as seen below in Figure 6 does not receive the **Enable ACL Management** capability. In this example, the **dadmin** user has access rights to create and manage copies of the lrmc069 instance, though the **dadmin** will not be able to manage object permissions, or grant other users permissions to manage objects.

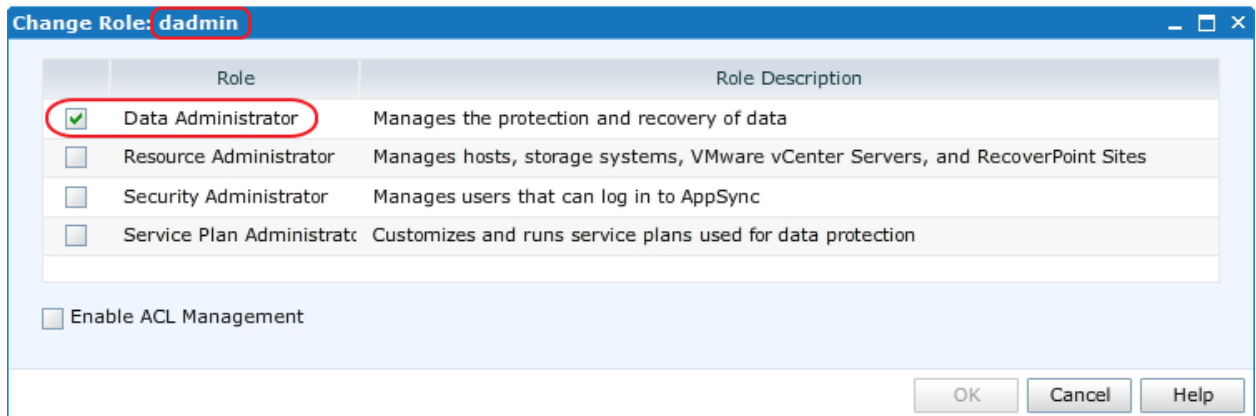
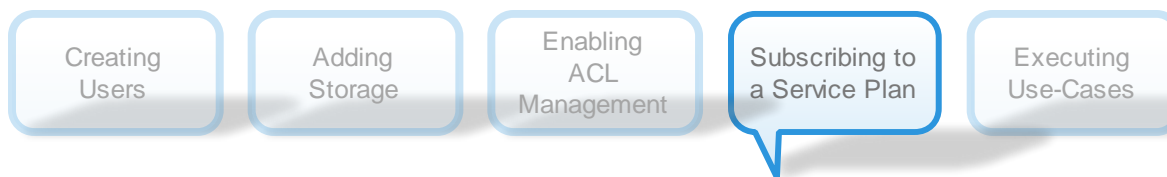


Figure 6

## Subscribing to a Service Plan



AppSync has three types of Service Plans, which are essentially templates for how copies are to be created. There are Create local copy, Create remote copy, and Create local and remote copy. These are translated as Bronze, Silver, and Gold respectively, as depicted in Figure 7.

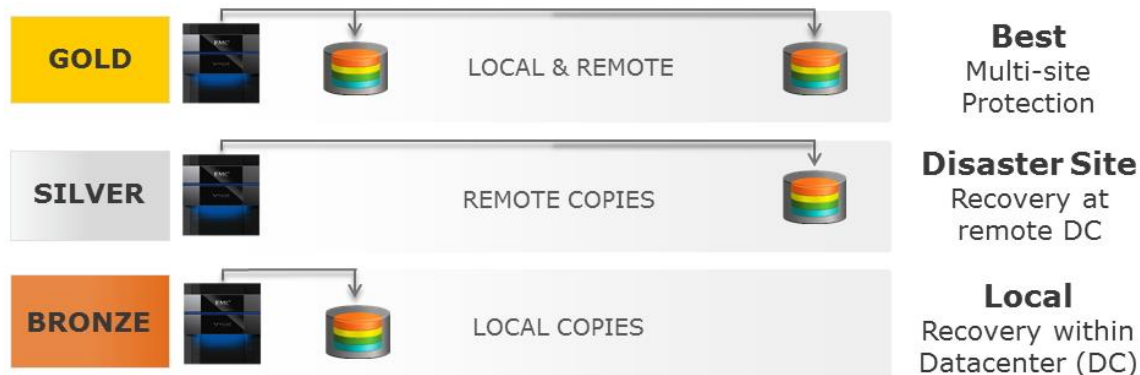


Figure 7

### The Bronze Service Plan

The default Bronze Service Plan can be used for quick protection as it is pre-configured for a 24-hour rotation, keeping seven copies, however, in many cases, a new Service Plan needs to be created based on the Bronze Service Plan template. Please refer to the AppSync User and Administration Guide for more details on configuring Service Plans.

Users with the **Service Plan Administrator** role can create a Bronze level Service Plan which either utilizes local array snap technology or RecoverPoint's local protection on the local XtremIO array. A remote array is unnecessary when creating local copies or bookmarks.

In order to create a local XtremIO snap, the default settings can be used, however, to create a local RecoverPoint Bookmark, the **Storage Ordered Preferences** option under the **Create Local Copy** tree view, needs modification. Ensure **Bookmark** is at the top of the list as seen below in Figure 8.

### The Silver Service Plan

Use the **Service Plan Administrator** to create the Silver Service Plan which utilizes RecoverPoint to create remote bookmarks. Similar to creating the Bronze Service Plan, be sure to modify the **Storage Ordered Preferences** option under **Create Local Copy**, and ensure **Bookmark** is at the top of the list, again, as seen in Figure 8.

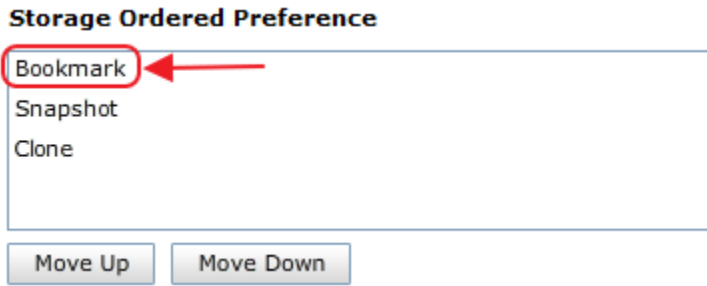


Figure 8

### Include RecoverPoint copies in expiration rotation policy

Under **Create Local Copy**, this option ensures no more than the number of copies specified is maintained by RecoverPoint. Please refer to Figure 9. Leaving this **unchecked** allows bookmarks to accumulate based on the RecoverPoint policy.



Figure 9

### Subscribe the Application to the Service Plans

Before the **Data Administrator** can subscribe application objects to service plans, an ACL Manager, as seen in Figure 3 must first enable that object’s ACL Settings and assign that user to that object, such as the application host as seen in the **Enable ACL Management** section, and in Figure 5.

The Service Plans created previously depict the replication method, local or remote bookmarks or XtremIO snaps. In order for AppSync to create bookmarks or snaps, used in the following use-cases, the application must be “subscribed” to the service plans created previously.

Using the **Data Administrator**, select the application, i.e. an SQL database and **Click** the **Protect** drop-down and next to **Subscribe to Plan**, select the bronze level service plan created previously. Repeat and select the silver level plan created previously, so the application can be subscribed to both service plans as seen in Figure 10.

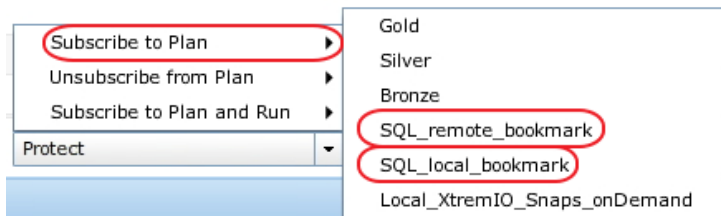
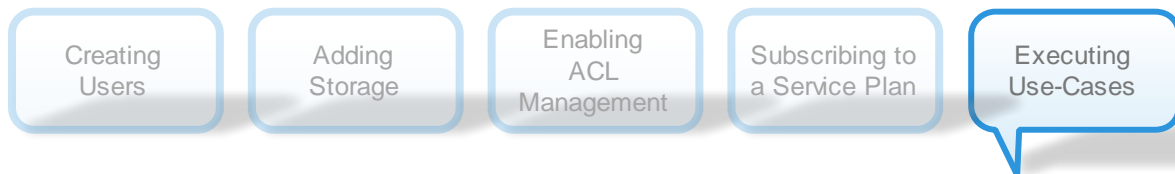


Figure 10

The reason the application can be subscribed to both to demonstrate that an application owner may have different needs locally and remotely.

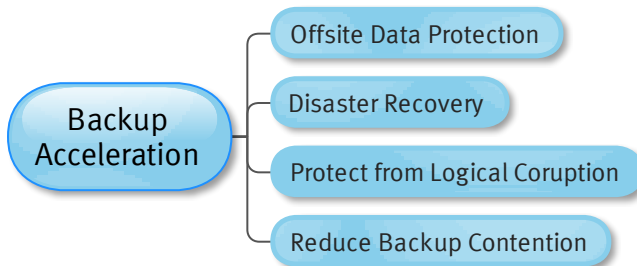
An example is for the application owner to provide local copies for backup operations or patch management test servers, while providing operational recover remotely in anticipation for a site failure.

## Executing Use-Cases



There are different types of scenarios that exist for which AppSync can utilize copies. The three use-cases below are not all-encompassing, though are typical. Please see Table 1 below, for a comparative overview of how Service Plan options are configured for either backup acceleration or operational recovery – data repurposing has a separate workflow and is not configured by Service Plans.

## Backup Acceleration



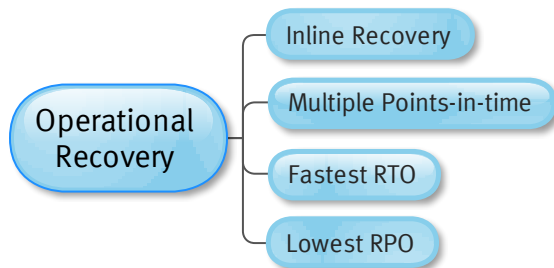
Backup Acceleration provides a means to offload external backup operations from impacting production environments. Application consistent copies are created and typically mounted on an alternate host, and then backed up to another lower cost platform, or off site, and retained for extended periods of time. Backup copies can protect against logical data corruption and serve to adhere to retention regulations.

Creating copies for backup purposes requires an application consistent copy, which serves as a specific point-in-time copy (PIT). However, in most cases, as with databases, a PIT copy can be recovered and subsequent log files applied. This is a critical aspect of data recovery, and thus requires planning. AppSync provides some options in order to ensure the application is not only restartable, but recoverable as well.

In order to create copies for backup acceleration, the Service Plan generally has been configured to mount the copy to an alternate host where another process can take the

copy off offsite, therefore, alleviating contention on the production host. Please reference the **Application Considerations** section for more details.

## Operational Recovery



Operational Recovery provides the ability to quickly recover from data corruption or accidental data loss. With operational recovery, **a series of copies are kept on the local and/or remote arrays**. These copies serve as a means to provide a near zero data loss - the lowest possible recovery point objective, while minimizing the amount of time it takes to recover - the shortest recovery time objective, ultimately increasing service level agreements.

Operational recovery is very similar to backup acceleration, in that application consistency is often desired. AppSync is very efficient in how it quiesces applications, and is designed to create many iterations in short periods of time, offering many different points-in-time for recovery or restoring back to. This provides application owners the ability to simply restore and go, rather than having to roll logs forward, thus decreasing the recovery time objective.

RecoverPoint is a major benefit with the operational recovery use-case. RecoverPoint, by default, creates point-in-time copies on a frequent basis. With RecoverPoint on XtremIO, this translates to a series of snapshots. AppSync does have the ability to create application consistent bookmarks, something RecoverPoint cannot natively do, so the two work collectively to provide the most robust solution, especially when remote replication is desired.

### Considerations:

- AppSync assumes the underlying storage replication technology, thus due to the way RecoverPoint works with XtremIO - snapshots are created rather than RecoverPoint utilizing a preconfigured journal. There are limitations on the number of volumes one consistency group can protect, how many bookmark/snapshots can be taken, etc., so please refer to the RecoverPoint Release Notes for more specifics regarding limitations.
- Typically, mounting options are not configured with the operational recovery use-case. The objective, which is the key differentiation factor between operational recovery and backup acceleration, is to have **a series of copies used for recovering a specific point-in-time**. Each environment may be configured differently, though a series of copies could be created as frequent as every 30 minutes, every few hours, every day, etc., and kept for periods of



days or even weeks. The frequency and retention heavily depends on a number of factors, including the limitations mentioned previously.

## Data Repurposing



Data repurposing, in a general sense, refers to using copies of production in manners other than backup and restore; the discerning difference from the previous two use-cases. These copies are mounted and recovered on hosts for use cases such as what is depicted in the graphic above.

AppSync's **data repurposing** feature refers to **taking multi-generation copies through a built-in utility**. These copies are generally used for undetermined periods of time. There are Generation 1 and 2 copies, depending on how removed the copy is from production, please see the section titled **Repurposing Copies**, below, for more details. Each copy is autonomous; you can refresh the Gen 1 copy without affecting any Gen 2 copy. Similarly, the Gen 2 copies can be refreshed independently as well.

Similar to backup acceleration and operational recovery, data repurposing generally benefits from the application be quiesced before creating the initial Gen 1 copy. There are some key differences with data repurposing, which are listed as follows:

- Data repurposing is not configured within the Service Plan, rather by navigating to **Copy Management**, selecting the application object, such as a particular database, selecting **Repurpose**, and then selecting **Create Repurpose Copy**, as seen in Figure 11.

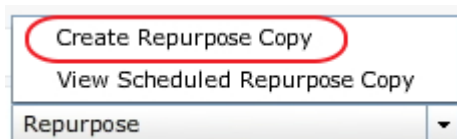


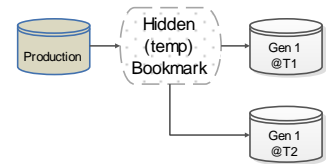
Figure 11

- Data repurposing copies are not generally used for backup/restore, once mounted and recovered, though a Gen 1 copy can be used to restore from if desired
- Data repurposing copies are created on an on-demand basis - there are no scheduling options, other than for the initial Generation 1 copy

## Repurposing Copies:

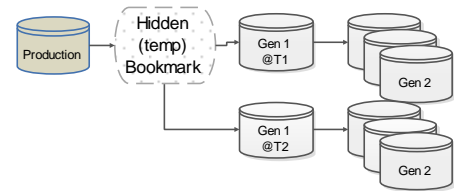
### The First Generation (Gen 1) Copy:

- An application consistent copy of production
- With RecoverPoint, a temporary “hidden” bookmark is created which the Gen 1 copy is created from
- The initial copy can be scheduled, though refreshing is manual
- Can be mounted, though more commonly used as an unaltered “Gold” source copy for Gen 2 copies
- There are no practical limits on the number of Gen 1 copies, however, there are array based limits which should be considered
- Currently, prior to refreshing, the copy must first be unmounted manually



### The Second Generation (Gen 2) Copy:

- A copy of Gen 1
- Does not quiesce the application
- Copies are generally mounted to non-production hosts for extended periods of time, for scenarios similar to the following:
  - Copies for user acceptance and quality assurance testing
  - Copies for training sessions
  - Copies for patch management, performance tuning, and sandbox environments
  - Copies for offloading data analytics and reporting processing
- There is no practical limit on the number of Gen 2 copies, however, there are array based limits which should be considered
- Copies cannot be created off the Gen 2 copy
- Currently, refreshing Gen 2 copies first requires the copy be unmounted manually prior to being refreshed



## Repurposing Limitations:

To date, AppSync only supports limited environments for multi-generation repurposing – always refer to the latest EMC Support Matrix and User and Administration Guide for supported environments and other limitations.

- AppSync’s data repurposing feature is currently supported for SQL and Oracle. Other applications can utilize AppSync’s typical mount and recovery features, as found under the Service Plan or through Copy Management, though there are additional considerations when RecoverPoint is utilized in this scenario – please see the previous section titled **Prerequisites and Restrictions** for RecoverPoint, and refer to the limitation of creating array based copies off of RecoverPoint bookmarks.
- Supports two generations removed from production - Gen 1 and Gen 2
- Copies do not figure into the RPO calculation
- Gen 2 cannot be used for restoring back to production
- Prior to refreshing, the copies must be unmounted

## Application Considerations

Each type of application, depending on the use-case, has different options when configuring Service Plans. Always consult the AppSync User and Administration Guide for more specifics. A few of the more essential considerations are depicted as follows:

- **Considerations with SQL:** Full vs. Copy – both protect the database and the active transaction log, however, **full** flags the database as being backed up and maintains the transaction log sequence number (LSN). The **copy** type does not interfere with the transaction log sequence, and thus is used when another third-party backup application is used. If AppSync is the only application managing the SQL backup, then it is recommended to use **full**, and **copy** when performing data repurposing, so long as another copy is used for backup purposes.
- **Considerations with Oracle:** By default, AppSync is configured to place the database in hot-backup mode and copy the archive logs. This type of backup ensures application recovery, and should be left unchanged for backup acceleration. With operational recovery, it is optional, though recommended. With data repurposing, it is not necessary as the copy will be recovered upon mounting. Please consider whether rolling logs is intended after a recovery, and ensure to use hot-backup mode when required. The following options depending on the purpose of the copy.
  - **Copy the Fast Recover Area** – disabled by default – optionally copy the storage used by the FRA

- **Index and copy the BCT** – disabled by default – optionally create an entry in the Oracle block change tacking file and copies it as a part of the replica
- **Create backup control file for RMAN cataloging** – disabled by default – optionally create a binary backup control file to be used with a remote RMAN catalog
- **Considerations with VMWare Datastores:** Creating VM Consistent (default) vs. Crash Consistent copies differs in that the VM Consistent copy includes the running programs and processes in memory, where the Crash Consistent option does not. The default setting is recommended for backup acceleration and operational recovery scenarios. AppSync does not support VMWare Datastore data repurposing.
  - Choosing to **Ignore VM Snapshots for VMs** allows overrides for specific VMs to be ignored for VM Consistent snapshots
  - **Include Virtual Machine Disk** ensures any datastore also associated with the virtual machines are included in the copy stream. If a datastore contains a VM that also has additional virtual disks, in a different datastore, both datastores are replicated.
- **Considerations with Exchange:** Full vs. Copy vs. Differential – similar to the SQL backup type, where typically only one backup application should maintain the **full** backup type, Exchange also offers the ability for **differential** copies. The choice depends on the backup strategy, though it is common for AppSync to be configured with **full** if it is the only application managing backup acceleration or operational recovery. It is not applicable with data repurposing, as AppSync does not support data repurposing for Exchange.
- If managing **RecoverPoint**, there are three **Image access mode** options to choose from, though these options are not all supported on XtremIO. With XtremIO, all access is immediate; journals are not utilized. Please refer to the *RecoverPoint Replication of XtremIO White Paper* on support.emc.com.
- Typically with the **backup acceleration** use-case, AppSync can initiate a **Post-mount script** in order to move the copy of production off site.
- The **Unmount copy** option can be utilized if the copy should be unmounted after the backup program completes. This renders the **Unmount previous copy** option unnecessary, and relieves the mount host of mounted volumes.

**Table 1- Overview of Service Plans based on Use-Cases\***

Use-Case	Backup Acceleration	Operational Recover
Supported Applications	All <sup>1</sup>	All <sup>1</sup>
Plan Startup	Scheduled	Scheduled
Recovery Point Objective	Optional	Optional
Backup Purpose	Long term - off array	Quick recovery - on array
Backup Type	Full <sup>2</sup>	Full <sup>2</sup>
Application Consistent	Essential	Recommended
Typical Number of Copies	One	Many - series <sup>3</sup>
Typical Rotation Schedule	Every 24hrs	Hourly
Unmount Previous Copy	Yes	Not applicable
Mount Copy	Yes	No
- Recover Copy	No, mount only	Not applicable
- Mount on Server	Yes	Not applicable
- Mount Path	Default Path	Not applicable

\*Repurposing is not an aspect of a Service Plan, so is not depicted in the table above

<sup>1</sup> Limited to AppSync's general application support matrix

<sup>2</sup> Dependent upon being the only application managing backup operations

<sup>3</sup> Limited upon backend technology (i.e. XtremIO or RecoverPoint)

## Conclusion

AppSync uses a self-service driven model to create local, remote, or local and remote copies for different use-cases, namely, backup acceleration, operation recovery, and data repurposing. Often, environments incorporate a combination of use-cases. Considerations are warranted and limitations should be understood when creating Service Plans for backup acceleration and operational recovery. Data Repurposing does not involve Service Plans; rather, copies are managed through the application object reference in Copy Management. Self-service options are available by creating different user roles based on responsibilities, and enabling Access Controls on objects.

RecoverPoint is a key aspect for providing near zero data loss copies, locally and remotely. AppSync is the key stone in copy management, by providing application quiescing, RecoverPoint orchestration, and XtremIO volume management and mapping, in a single user interface that is launched from any computer with access.

## References

The following documents were used in writing this whitepaper. All documents are available at EMC's Support site <https://support.emc.com>.

- [AppSync 2.2.2 Installation and Configuration Guide](#)
- [AppSync 2.2.2 Release Notes](#)
- [AppSync 2.2.2 Security Configuration Guide](#)
- [AppSync 2.2.2 User and Administration Guide](#)
- [EMC XtremIO Storage Array Versions 4.0 and 4.0.1 Security Configuration Guide](#)
- [RecoverPoint Replication of XtremIO White Paper](#)