

Dell EMC AppSync

Version 4.1

User and Administration Guide

May 2020

Copyright © 2020 Dell Inc. or its subsidiaries. All rights reserved.

Dell 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.” DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

	Preface	11
Chapter 1	Introduction	13
	AppSync overview	14
	Overview of service plans.....	15
	Role-based management.....	15
	AppSync reports	16
	AppSync architecture.....	16
	AppSync server	16
	AppSync agent (host plug-in) overview.....	16
	AppSync console (user interface).....	17
	REST interface.....	17
Chapter 2	AppSync Console	19
	Console overview.....	20
	AppSync Dashboard Overview.....	20
	Times shown in the console.....	22
	Start the AppSync console.....	22
Chapter 3	AppSync CLI Utility	23
	AppSync CLI Utility.....	24
	CLI actions.....	25
	Login.....	25
	Logout.....	26
	refresh.....	26
	runSP.....	27
	enableSP.....	27
	disableSP.....	28
	report.....	29
	expire.....	30
	subscribe.....	31
	unsubscribe.....	32
	listCopies.....	34
	copyDetails.....	36
	mount.....	36
	unmount.....	48
Chapter 4	Service Plans	51
	Service plan overview.....	52
	Create a service plan.....	55
	Run a service plan on demand	64
	Enable and disable a service plan	64
	Delete a service plan.....	64
	Edit a Service Plan for an Oracle database.....	65
	Edit a Service Plan for a SQL database.....	66
	Edit a Service Plan for a File system.....	68
	Edit a Service Plan for VMware.....	70

	Edit a Service Plan for Exchange.....	71
	Unsubscribe from a service plan.....	72
	Enable or disable automatic expiry of a copy	73
	Service Plan Events.....	73
	Oracle service plan details.....	74
	SQL Server service plan details.....	78
	File system service plan details.....	83
	VMware Datacenter service plan details.....	86
	Microsoft Exchange service plan settings.....	88
Chapter 5	Protect Microsoft Exchange	93
	Overview of Exchange support	94
	Deploying AppSync for Exchange protection.....	95
	Discover Exchange Database.....	96
	Removing an Exchange mailbox server	96
	Protecting DAG databases in a service plan.....	96
	Convert a standalone Exchange server to a DAG member.....	96
	Protect an Exchange database	97
	Protecting an Exchange database immediately.....	97
	Subscribe an Exchange database to a service plan.....	97
	Unsubscribe Exchange from a service plan.....	98
	Expire an Exchange copy.....	99
	Overriding service plan schedules.....	99
	Service plan details.....	100
	Service plan schedule.....	100
	Pre-copy script	101
	Create a Copy.....	101
	Post-copy script.....	104
	Mount copy.....	104
	Validate copy.....	106
	Post-mount script.....	107
	Unmount copy.....	107
	Mounting Exchange copies.....	108
	Mount and restore limitations.....	108
	Mount a copy using the Exchange Mount wizard.....	108
	Unmount an Exchange copy from the Copies page.....	110
	Unmount an Exchange copy from the Service Plan page.....	111
	Enable or disable an Exchange copy.....	111
	Expire an Exchange copy.....	111
	Path mapping.....	112
	Overview of Exchange copy restore.....	113
	Affected entities during restore.....	113
	Restore an Exchange copy.....	114
	Recovering an Exchange database manually.....	115
	Partial restore.....	115
	Restoring a deleted Exchange database.....	116
Chapter 6	Protect SQL Server	119
	Overview of SQL Server support.....	120
	SQL Server prerequisites.....	120
	SQL Server supported configurations.....	121
	Considerations for SQL Server in a VMware environment.....	121
	Required permissions and rights.....	122
	Set up SQL Server connection settings.....	124

- Support for AlwaysOn Availability Groups..... 125
- SQL Server transaction log backup..... 125
 - Configure SQL Server transaction log backup..... 126
 - Create log backup for SQL.....127
 - Configure log backup scripts.....127
 - Run Log Backups for a SQL database..... 127
 - View log backups for a service plan..... 128
 - Log backup expiration.....128
- Considerations for working with SQL Server in a cluster..... 130
- SQL Server User Databases folder..... 131
 - Discovering SQL Server databases..... 131
 - Discover SQL Server databases.....132
- Protect a SQL Database..... 132
 - Subscribe a SQL database to a service plan.....132
 - Create a SQL database copy..... 133
 - Microsoft SQL Server copies list 134
 - Unsubscribe database from a service plan..... 135
 - Overriding service plan schedules.....136
 - View SQL database copies.....136
 - Expire a SQL copy..... 139
 - Service plan summary and details..... 139
- Mount considerations for SQL Server..... 149
 - Mount a copy using the SQL Mount wizard..... 151
 - Path mapping..... 155
- Unmount a SQL copy from the Copies page..... 157
- Unmount a SQL copy from the Service Plan page..... 157
- Create SQL repurpose copies..... 157
- Create second generation copies..... 159
- Enable or disable a SQL copy expiry..... 160
- Expire a SQL copy..... 160
- SQL Server database restore overview..... 161
 - Restore considerations for databases in an Availability Group..... 161
 - Affected entities during restore..... 161
 - Restoring a primary database or a secondary database with failover.. 162
 - Restoring a secondary database without failover.....163
 - Restore a SQL copy.....163
 - SQL Server restore utility (assqlrestore)..... 164

- Chapter 7 Protect Oracle 169**
- Overview of Oracle support..... 170
 - Oracle permissions.....170
 - Red Hat Cluster Services Integration with AppSync 171
 - Oracle Data Guard support..... 171
 - Veritas Cluster Services integration.....174
 - PowerHA (HACMP) cluster integration..... 175
 - Prerequisites and supported configurations..... 176
- Protecting a database.....184
 - Discover an Oracle database.....184
 - Subscribe a database to a service plan..... 185
 - Unsubscribe database from a service plan..... 186
 - Creating an Oracle database copy from the Copies page.....186
 - Create Oracle repurpose copies.....187
 - Create second generation copies.....188
 - Oracle Copies page.....189
- Service plan summary and details.....191

	Service plan schedule.....	191
	Overriding service plan schedules.....	192
	Storage preferences.....	192
	Pre-copy script.....	193
	Create copy.....	193
	Automatic expiration of copies.....	193
	Post-copy script.....	194
	Unmount previous copy.....	194
	Pre-mount script.....	195
	Mount copies	195
	Overriding mount settings in a service plan.....	196
	Post mount script.....	196
	Unmount copy.....	197
	Mount an Oracle copy.....	197
	Mount a copy using the Oracle Mount wizard.....	202
	Unmount an Oracle copy from the Copies page.....	205
	Unmount an Oracle copy from the Service Plan page.....	205
	Expire an Oracle copy.....	206
	Enable or disable expiry of an Oracle copy.....	206
	RMAN cataloging feature	206
	Mount on standalone server and prepare scripts for manual database recovery.....	207
	Mount on Grid Cluster and recover as RAC database.....	208
	Path mapping.....	209
	Retry recovery of a mounted and recovered Oracle copy.....	210
	Restore an Oracle copy.....	211
	Restore a standalone local copy	212
	Affected entities during restore.....	214
	Vdisk restore with affected entities.....	216
	Restoring a RAC copy for affected entities.....	216
Chapter 8	Protect File Systems	219
	Overview of File System support.....	220
	Protect NFS file systems on VNX and Unity storage.....	220
	PowerHA (HACMP) cluster integration.....	223
	Windows failover clustered file systems.....	224
	File system service plan details.....	225
	Discover File Systems.....	229
	Subscribe a File System to a service plan.....	229
	Unsubscribe File Systems from a service plan.....	230
	Create a File System copy.....	230
	Create File System repurpose copies.....	231
	Create second generation copies.....	233
	Overriding service plan schedules.....	234
	Mount a copy using the File System Mount wizard.....	234
	Changing the mount point for an affected file system.....	236
	Override mount settings in a service plan.....	236
	Nested mount support for File systems.....	237
	Mounting a UNIX file system after reboot	237
	Unmount a File System copy from the Copies page.....	238
	Unmount a File System copy from the Service Plan page.....	238
	Enable or disable a File system copy.....	239
	Expire a File system copy.....	239
	Path mapping.....	239
	Restore a Filesystem copy.....	241

Chapter 9	Protect VMware Datacenters	243
	Configuration prerequisites	244
	VMware vStorage VMFS requirements	244
	Discover VMware Datacenters.....	246
	List of datacenters	246
	Add a VMware vCenter Server.....	246
	List of VMware datastores	247
	Considerations when mounting a VMFS copy	258
	Mount a copy using the VMware Mount wizard.....	258
	Unmount a VMware copy from the Copies page.....	259
	Unmount a VMware copy from the Service Plan page.....	260
	Restoring a VMware datastore from a copy.....	260
	Datastore affected entities during restore.....	261
	Restoring a virtual machine from a copy.....	261
	Virtual Machine Restore options.....	263
	File or folder restore with VMFS or NFS datastores.....	264
	Restoring a file or folder from a virtual disk.....	265
Chapter 10	Repurposing	267
	Repurposing overview.....	268
	Repurpose schedule.....	269
	Modifying a repurpose plan.....	270
	Repurpose refresh.....	270
	Repurpose expire.....	271
	Data masking using scripts.....	271
	Creating Repurpose copies.....	272
	View or delete repurpose copy schedules.....	274
	View repurposed copies.....	275
Chapter 11	Monitor AppSync	277
	RPO concepts and best practices.....	278
	Recovery point compliance report.....	278
	Exporting an RPO compliance report to CSV.....	278
	View the Service Plan Completion Report.....	279
	View the Recovery Point Compliance Report.....	280
	View the Automated Log Collection Status Report.....	280
	Alerts and associated events.....	281
	Acknowledging alerts.....	281
	Acknowledging alert icons for database, file system, and Datastore service plan runs.....	282
	Email alerts.....	282
	Configure server settings for email alerts.....	283
	Specify email alert recipients.....	283
	View Jobs.....	284
	View Job Status progress.....	284
Chapter 12	Storage considerations	285
	VNX Block	286
	Service plan considerations for applications on VNX Block storage....	287
	Dynamic mounts	287
	Microsoft Cluster Server mounts for SQL Server.....	287
	SAN policy on Windows Server Standard Edition	288
	VNX file	288

Service plan considerations for an application on VNX File storage....	289
VNX file mount.....	290
VMAX V2.....	290
Service plan considerations for applications on VMAX V2 storage....	290
Mount and unmount VMAX V2 copies.....	292
Microsoft Cluster Server mounts for SQL Server.....	292
Repurpose copies on VMAX V2.....	293
VMAX V2 restore.....	293
VMAX3/PowerMAX and VMAX All Flash.....	294
Service plan considerations for applications on VMAX All Flash and VMAX3/PowerMAX storage.....	294
Mount/unmount VMAX3/PowerMAX and VMAX All Flash copies.....	295
VMAX3/PowerMAX and VMAX All Flash repurpose overview.....	296
XtremIO.....	297
Restore options with XtremIO storage.....	299
RecoverPoint	300
Service plan considerations for applications with RecoverPoint protection.....	300
RecoverPoint prerequisites.....	300
Dynamic or static mounts.....	301
Repurpose RecoverPoint Bookmark copies of Oracle or SQL Server databases.....	302
Unity	303
Service plan considerations with Unity.....	304
Mounting and unmounting Unity NFS datastore copies.....	304
Mounting and unmounting Unity copies.....	304
Mounting and unmounting Unity NFS File system copies.....	305
Unity restore considerations.....	305
Repurposing copies on Unity.....	305
VPLEX.....	306
Service plan considerations for applications on VPLEX storage.....	306
Mount and unmount VPLEX copies	307
VPLEX restore considerations.....	308
Dell SC.....	308
Service plan considerations for applications on Dell SC storage.....	309
Mount and unmount Dell copies.....	309
PowerStore.....	309
Add a PowerStore appliance to AppSync.....	309
Service plan considerations with PowerStore.....	310
Mount and Unmount PowerStore copies.....	311
PowerStore restore considerations.....	311
Repurposing copies on PowerStore.....	311

Chapter 13	Troubleshooting AppSync	313
Automated log collection.....		314
Collect Logs.....		314
Dell EMC SupportAssist.....		317
Dell EMC SupportAssist.....		317
Configuration information sent to Dell EMC via Dell EMC SupportAssist		318
AppSync issues.....		319
User account does not have the correct permissions.....		319
AppSync Exchange Interface service is partially registered.....		320
VSS timeout issue.....		320
Host installation and deployment issue.....		320

Oracle ASM disk groups cannot be mounted after a host reboot..... 321

Mount of ASM disk groups fail on RHEL 6.x and 7.x MPIO configurations..... 321

AppSync fails to mount Oracle ASM disk groups (Event - ORCL_000043) 321

AppSync fails to unmount Oracle ASM disk groups (Event - ORCL_000044)..... 322

Oracle database discovery failure.....322

Oracle database discovery failure - / file system full.....322

Oracle database fails to start after a reboot.....323

Restore of Oracle database causing server service to crash..... 323

Oracle restart script not removed for UNIX hosts registered using a SUDO user on agent uninstallation..... 324

AppSync requires higher ulimit settings for the root user than the Oracle user.....324

AppSync fails to create symlinks.....324

Checking system logs for Oracle restart..... 324

Database fails to start with the created SPFile 325

Oracle recovery failure.....325

Oracle 12.2 RAC database discovery failure..... 326

Oracle database recovery failure during `prerecoverdb` operation...326

AppSync fails to freeze the SQL Server database in a timely manner (Event - SQL_000018)..... 326

SQL Cluster - second generation copy mount failure..... 327

Timeout error during SQL database discovery.....327

SQL recovery failure..... 327

SQL database protection failure.....327

<AppSync>\jboss\standalone\tmp\vfs\ folder disk usage..... 328

XtremlO copy creation takes time.....328

Changing an XMS IP..... 328

Error during datastore or virtual disk mount.....328

Virtual disk mapping failure..... 329

Protection of File systems or Oracle applications on MPIO devices fail during mapping..... 329

Mount of a File system or an Oracle database on RHEL 7.x fails..... 330

Repurposing file systems on multiple LUNs fail..... 330

Changed file system type not updated after host discovery.....330

Mount of a file system snapshot to RHEL7 fails..... 331

CST lockbox restore failure..... 331

Protection and repurposing failure on VMAX V2..... 331

AppSync services do not start after reboot.....332

Windows server configuration issue..... 332

Scheduled service plan fails..... 332

AppSync fails to launch on Google Chrome 333

AppSync upgrade failure..... 333

AppSync server database failure..... 333

Mount failure on RHEL 7.4..... 333

Mount host fails to respond during an unmount operation..... 334

Recovery of 2nd-gen copy fails if the SQL backup type of the 1st-gen service plan is altered.....335

Unmount does not remove used devices from storage groups 335

Datastore mount fails when ATS locking is enabled.....335

Error handling..... 335

Event logging..... 337

Glossary	339
Index	343

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. All the versions of the software or hardware that are currently in use, might not support some functions that are described in this document. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

 **Note:** This document was accurate at publication time. Go to support.dell.com to ensure that you are using the latest version of this document.

Purpose

This document is part of the AppSync documentation set, and includes information about using and managing AppSync.

Audience

This guide is intended for use by customers and service providers to use and configure AppSync.

Related documentation

The following publications provide additional information:

- AppSync Installation and Configuration Guide
- AppSync Release Notes

Special notice conventions used in this document

Dell EMC uses the following conventions for special notices:

 **DANGER** Indicates a hazardous situation which, if not avoided, results in death or serious injury.

 **WARNING** Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

 **CAUTION** Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

 **NOTICE** Addresses practices that are not related to personal injury.

 **Note:** Presents information that is important, but not hazard-related.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Table 1 Typographical conventions

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks).
<i>Italic</i>	Used for full titles of publications referenced in text.
Monospace	Used for:

Table 1 Typographical conventions (continued)

	<ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables
Monospace bold	Used for user input
[]	Square brackets enclose optional values.
	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z.
...	Ellipses indicate nonessential information that is omitted from the example.

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about Dell EMC products, go to support.dell.com.

Technical support

Go to support.dell.com and click Service Center. Several options for contacting Dell EMC Technical Support are available. To open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to community.dell.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all Dell EMC products.

Your comments

Your suggestions help continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

CHAPTER 1

Introduction

This chapter includes the following topics:

- [AppSync overview](#) 14
- [AppSync architecture](#)..... 16

AppSync overview

AppSync is software that enables Integrated Copy Data Management (iCDM) with the primary storage systems of Dell EMC.

AppSync simplifies and automates the process of generating and consuming copies of production data. AppSync abstracts the underlying storage and replication technologies. Through deep application integration, AppSync enables application owners to satisfy copy demand for operational recovery and data repurposing on their own. In turn, storage administrators need only be concerned with initial setup and policy management, resulting in an agile, frictionless environment.

AppSync automatically discovers application databases, learns the database structure, and maps it through the virtualization layer to the underlying storage LUN. It then orchestrates all the activities that are required from copy creation and validation through mounting at the target host and launching or recovering the application. Supported workflows also include refresh, expire, and restore production.

Key features

- Supports physical, virtual, and mixed host environments across Dell EMC Block and File storage.
- Integrates with Oracle, SQL server, Exchange, VMware vCenter, and more.
- Supports customer applications (EPIC, DB2, and so on) through file system copies with callout script integration to provide application consistency.
- Supports application consistent, crash consistent, and virtual machine consistent (with individual virtual machine recovery) copies.
- Supports Snaps, Clones, and RecoverPoint Bookmarks.
- Supports on-demand and scheduled plans.
- Repurpose wizard supports application consistent copy creation and manual modifications. Second-generation copies of the modified copy are then distributed and optionally deleted upon configured expiration.

Supported applications and storage

AppSync supports the following applications and storage arrays:

- Applications
 - Oracle
 - Microsoft SQL Server
 - Microsoft Exchange
 - VMware vStorage VMFS datastores
 - VMware NFS datastores
 - Windows, UNIX, and NFS file systems
- Storage
 - VMAX V2
 - VMAX3/PowerMAX
 - ⓘ **Note:** In this document, all mentions of VMAX3 includes information and instructions for VMAX All Flash and PowerMAX arrays.
 - VMAX All Flash

- PowerStore (Block only)
- VNX (Block and File)
- XtremIO
- VPLEX
- Unity (Block and File)
- Dell SC (Block only)
- Replication Technologies
 - VNX Advanced Snapshots
 - VNX File Snapshot
 - PowerStore Snapshot
 - PowerStore Thin Clone
 - TimeFinder Clone
 - TimeFinder VP Snap
 - SRDF
 - SnapVX
 - RecoverPoint Bookmarks
 - XtremIO Virtual Copies
 - Unity Unified Snapshot
 - Unity Thin Clone
 - Dell SC Series Snapshots

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.

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

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.

The following table describes the user roles.

Table 2 User roles

Role	Function
Security Administrator	Manages users access to AppSync.
Resource Administrator	Manages hosts, storage systems, servers, and RecoverPoint sites.

Table 2 User roles (continued)

Role	Function
Service Plan Administrator	Customizes and runs service plans used for data protection.
Data Administrator	Manages the protection and recovery of data.

The *AppSync Security Configuration Guide* provides more information on the specific user roles and their permissions.

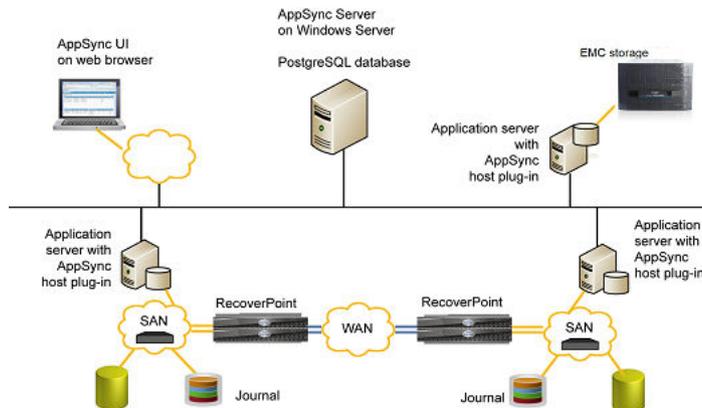
AppSync reports

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

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, go to **Settings > Infrastructure Resources > SERVERS / CLUSTERS**, select a host, and click **UPDATE PLUG-IN**.

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.

The *AppSync Installation and Configuration Guide* provides more information about installing the AppSync agent.

AppSync console (user interface)

The AppSync console is web-based, with the following support:

- Minimum resolution: 1366X768 (best viewed in 1920x1080)
- Supported Browser: Google Chrome (latest version) and Internet Explorer.

REST interface

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

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

CHAPTER 2

AppSync Console

The chapter includes the following topics:

- [Console overview](#) 20
- [Start the AppSync console](#) 22

Console overview

The AppSync console is arranged in the Dashboard, Copy Management, Alerts, Reports, and Jobs tabs.

- The **Dashboard** is a customizable view of reports and alerts. The default dashboard shows Recovery Point Objective (RPO) status of protected applications, service plan job status, most recent alerts, summary of copies, and activities in progress.
- **Copy Management** provides an action-oriented entry to the copy management or service plan pages for applications such as Microsoft Exchange and Microsoft SQL Server. It also provides an application-oriented entry point for protection, mount, restore, service plan subscription, and other operations.
- The **Alerts** view and acknowledge alerts, filter alerts based on alert state, time, server, application, and so on, and view details of the alerts in the right pane.
- **Reports** displays automated log collection status reports, recovery point compliance reports, and service plan completion reports.
- The **Jobs** tab displays a list of all active jobs in AppSync.
- The **Settings** section contains all the settings that you can configure for AppSync. This section also allows you to do the following:
 - Configure Infrastructure Resources
 - Configure Licenses
 - Register Dell EMC SupportAssist
 - Configure Notification
 - Configure Users and Roles
 - Configure Advanced Settings
 - Configure Logs
 - View AppSync Support tools

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** tab for a user who has only the Security Administrator role.

AppSync Dashboard Overview

The Dashboard is a customizable view of reports, alerts, and summaries.

The default dashboard shows Recovery Point Objective (RPO) status of protected applications, service plan job status, most recent alerts, summary of copies, and activities in progress.

View Alerts in the Dashboard

The Alerts summary on the dashboard shows the total number of alerts, and the doughnut chart displays the distribution of the alerts among categories such as Service Plan, License, Maintenance, RPO, and so on.

About this task

To view the details of the alerts listed in the Dashboard:

Procedure

1. Log in to the AppSync console.

2. In the Alerts widget, click the **Details** link to see a list of all the alerts in AppSync.
3. On the Dashboard, click the **Refresh** icon on the top of the widget to refresh the results.

View Service Plan Completion Status in the Dashboard

The Service Plan Completion Status summary on the dashboard shows the status of service plan jobs, and the doughnut chart displays the distribution of the number of service plan jobs in the Successful, Completed with Errors, and Failed categories.

About this task

To view the details of the service plan jobs listed in the Dashboard:

Procedure

1. Log in to the AppSync console.
2. In the Service Plan Completion Status widget, click the **Details** link to see the percentage of the service plans that completed successfully, the ones that completed with errors, and the ones that failed.
3. On the Dashboard, click the **Refresh** icon at the top of the widget to refresh the results.

View Recovery Point Objectives in the Dashboard

The Recovery Point Objectives (RPO) summary on the dashboard shows the number of RPOs met across all objects that are subscribed to RPO-enabled service plans. The doughnut chart displays the distribution of the number of RPOs in the Satisfied and Not Satisfied categories.

About this task

To view the details of the RPOs listed in the Dashboard:

Procedure

1. Log in to the AppSync console.
2. In the RPO region, click the **Details** link to see the recoverability for all objects that are subscribed to service plans with an RPO recurrence type.
3. On the Dashboard, click the **Refresh** icon at the top of the widget to refresh the results.

View Copy Summary in the Dashboard

The Copy Summary on the dashboard shows the number of protection copies and the repurposed copies for each application type. This dashboard includes the number of applications that were copied, discovered, and the service plans that were created.

 **Note:** You can customize the number of applications that are displayed in this widget. To do so, click the **settings** icon in the widget, select the applications that you want displayed, and click **Apply**.

View Job Status in the Dashboard

The Job Status summary on the dashboard shows the number of active and completed jobs. The list view displays the number of jobs that are completed across the Completed Successfully, Completed with Errors, and Failed categories.

About this task

To view the details of the jobs listed in the Dashboard:

Procedure

1. Log in to the AppSync console.

2. In the Job Status region, click the drop-down list and select one of the following choices:

- LAST 24 HOURS
- All

The displayed results are filtered based on the time period you select.

3. Click the **Details** link to see a list of all active jobs in AppSync.

Times shown in the console

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

Start the AppSync console

You can launch 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.

Minimum resolution: 1366X768 (best viewed in 1920x1080)

Supported Browser: Google Chrome (latest version)

CHAPTER 3

AppSync CLI Utility

This chapter includes the following topics:

- [AppSync CLI Utility](#)..... 24
- [CLI actions](#)..... 25

AppSync CLI Utility

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`. If you want to use the AppSync CLI from UNIX, copy `EMC\AppSync\appsync-cli` directory to the UNIX host and run `appsynccli.sh`.

Pre-requisites

- Java Runtime Environment (JRE) version 8 - must be installed and available in path.
- Configured AppSync installation with registered resources
- Discovered applications on registered hosts
- Configured service plans
- If you are using the CLI on a non-English host, ensure that you set the correct code page before execution. To set the code page, use `chcp` on the command prompt.

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 or 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 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 about all CLI-supported actions.
- `appsync-cli.bat -action /?` Returns nonspecific 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

This section describes the AppSync CLI actions.

The AppSync CLI supports the following actions:

- Login and logout.
- Run a service plan.
- Enable or 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 or unsubscribe an application object to or from a service plan.
- Mount or unmount a copy.
- Expire a copy.
- Run and export AppSync reports.
- Refresh.

Login

Authenticates the AppSync server.

Syntax

```
-login
server value
port value
user value
password value
/?
```

Arguments

server <i>value</i>	The server that you want to authenticate. The default is server=localhost.
port <i>value</i>	The HTTPS port of AppSync server. The default port is 8445.
user <i>value</i>	Specifies the user to be authenticated. The default user is admin.
password <i>value</i>	Specifies the password for the user. You are prompted to enter a password, if no password is set.
/?	Displays command-line help.

Description

This command authenticates the AppSync server. It requires the server name, https communication port, AppSync user, and the 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.

See also

logout

Logout

Invalidates an open AppSync CLI connection.

Syntax

```
-logout
```

```
/?
```

Arguments

/?	Displays command-line help.
----	-----------------------------

Description

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

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

See also

login

refresh

Refreshes the specified copy.

Syntax

```
-refresh
```

```
app value
```

```
copy_ID value
```

```
/?
```

Arguments

app <i>value</i>	The application that you want to refresh. The value can be one of the following: <ul style="list-style-type: none"> sql oracle
copy_ID <i>value</i>	The UUID of the copy to be refreshed.
/?	Displays command line help.

Description

This command refreshes the specified application copy. For example:

```
appsync-cli.bat -refresh app=sql
```

See also

expire

runSP

Runs the specified service plan.

Syntax

```
-runSP
service_plan value
app value
log_backup_only value
/?
```

Arguments

service_plan <i>value</i>	The service plan that you want to run.
app <i>value</i>	Specifies the application. Values: <ul style="list-style-type: none"> • sql • oracle • filesystem • datastore • exchange
log_backup_only <i>value</i>	Use for on-demand SQL database log backup. Values: <ul style="list-style-type: none"> • true • false
/?	Displays command line help.

Description

You can run a service plan by specifying the application name and the service plan. For example:

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

See also

```
enableSP
disableSP
```

enableSP

Enables the specified service plan.

Syntax

```
-enableSP
service_plan value
app value
/?
```

Arguments

<code>service_plan <i>value</i></code>	The service plan that you want to enable.
<code>app <i>value</i></code>	Specifies the application. Values: <ul style="list-style-type: none"> • sql • oracle • filesystem • datastore • exchange
<code>/?</code>	Displays command line help.

Description

You can enable a service plan by specifying the application name and the service plan. For example:

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

See also

runSP

disableSP

disableSP

Disables the specified service plan.

Syntax

```
-disableSP
```

```
service_plan value
```

```
app value
```

```
/?
```

Arguments

<code>service_plan <i>value</i></code>	The service plan that you want to disable.
<code>app <i>value</i></code>	Specifies the application. Values: <ul style="list-style-type: none"> • sql • oracle • filesystem • datastore • exchange
<code>/?</code>	Displays command line help.

Description

You can disable a service plan by specifying the application name and the service plan. For example:

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

See also

runSP
enableSP

report

Run and export AppSync reports.

Syntax

```
-report
report_type value
detailed value
category value
age value
service_plan value
app value
/?
```

Arguments

report_type <i>value</i>	The type of report that you want to run. The value can be one of the following: <ul style="list-style-type: none"> • rpo • spc • alerts • activity
detailed <i>value</i>	The report format. You can run a detailed report or a summary report. The value can be true or false.
category <i>value</i>	The category of the alerts. Values: <ul style="list-style-type: none"> • all • rpo • other • license • maintenance
age <i>value</i>	Specifies the duration of the events. The value can be one of the following: <ul style="list-style-type: none"> • day • week • month • all
service_plan <i>value</i>	Displays alerts for the specified service plan. The default value is all.
app <i>value</i>	The application name. The value can be one of the following:

	<ul style="list-style-type: none"> • sql • oracle • filesystem • datastore • exchange
/?	Displays command line help.

Description

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
```

See also

expire

expire

Expires a specified copy.

Syntax

```
-expire
app value
copy_ID value
force value
/?
```

Arguments

app <i>value</i>	<p>The application name. The value can be one of the following:</p> <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
copy_ID <i>value</i>	The UUID of the copy you want to expire.

<code>force value</code>	Removes a copy which has multiple associated copies. The value can be true or false.
<code>/?</code>	Displays command line help.

Description

To expire a copy, you must specify the application name and the copy UUID. For example:
`appsync-cli.bat -expire app=datastore copy_ID=<value>`

See also

`refresh`

subscribe

Subscribes a data object to the specified service plan.

Syntax

`-subscribe`

`service_plan value`

`app value`

`/?`

Arguments

<code>service_plan value</code>	The service plan that you want to subscribe to.
<code>app value</code>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
<code>/?</code>	Displays command line help.

Description

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

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

This table describes the application specific options.

Table 3 Application specific options

Application specific options	Description
SQL	
<code>sql_server value</code>	The SQL server of the desired database. The default is <code>sql_server=localhost</code> .

Table 3 Application specific options (continued)

Application specific options	Description
<code>instance_name value</code>	The SQL instance of the desired database. The default is <code>instance_name=MSSQLSERVER</code>
<code>db_name value</code>	The SQL database that you want to subscribe.
<code>user_databases value</code>	Allows subscription of the user database folder. The value can be true or false.
Oracle	
<code>oracle_server value</code>	The Oracle server of the desired database. The default is <code>oracle_server=localhost</code>
<code>db_name value</code>	The Oracle database that you want to subscribe.
File system	
<code>fs_server value</code>	The server of the desired file system. The default is <code>fs_server=localhost</code> .
<code>fs_name value</code>	The name of the file system. The default is <code>fs_name=C:\.</code>
<code>fs_type value</code>	The format of the file system. The default is <code>fs_type=ntfs</code> .
Datastore	
<code>datastore value</code>	The datastore that you want to subscribe.
<code>datacenter value</code>	The datacenter to find the datastore.
<code>vcenter value</code>	The vCenter server to find the datastore. The default is <code>vcenter=localhost</code> .
Exchange	
<code>ex_server value</code>	The Exchange server that you want to subscribe.
<code>db_name value</code>	The Exchange database that you want to subscribe.

See also

unsubscribe

unsubscribe

Unsubscribes a data object from the specified service plan.

Syntax

```
-unsubscribe
service_plan value
app value
```

/?

Arguments

<code>service_plan</code> <i>value</i>	The service plan that you want to unsubscribe from.
<code>app</code> <i>value</i>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
/?	Displays command line help.

Description

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

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

Table 4 Application specific options

SQL	
<code>sql_server</code> <i>value</i>	The SQL server of the desired database. The default is <code>sql_server=localhost</code> .
<code>instance_name</code> <i>value</i>	The SQL instance of the desired database. The default is <code>instance_name=MSSQLSERVER</code> .
<code>db_name</code> <i>value</i>	The SQL database that you want to unsubscribe.
<code>user_databases</code> <i>value</i>	Allows you to unsubscribe the user database folder. The value can be true or false.
Oracle	
<code>oracle_server</code> <i>value</i>	The Oracle server of the desired database. The default is <code>oracle_server=localhost</code> .
<code>db_name</code> <i>value</i>	The Oracle database that you want to unsubscribe.
File system	
<code>fs_server</code> <i>value</i>	The server of the desired file system. The default is <code>fs_server=localhost</code> .
<code>fs_name</code> <i>value</i>	The name of the file system. The default is <code>fs_name=C:\.</code>
<code>fs_type</code> <i>value</i>	The format of the file system. The default is <code>fs_type=ntfs</code> .

Table 4 Application specific options (continued)

Datastore	
<code>datastore <i>value</i></code>	The datastore that you want to unsubscribe.
<code>datacenter <i>value</i></code>	The datacenter to find the datastore.
<code>vcenter <i>value</i></code>	The vCenter server to find the datastore. The default is <code>vcenter=localhost</code> .
Exchange	
<code>ex_server <i>value</i></code>	The Exchange server that you want to unsubscribe. In the case of DAG, the server name is the DAG name.
<code>db_name <i>value</i></code>	The Exchange database that you want to unsubscribe.

See also

subscribe

listCopies

Displays all copies that meet the specified application specific properties.

Syntax

```
-listCopies
service_plan value
app value
age value
/?
```

Arguments

<code>service_plan <i>value</i></code>	The service plan that you want to unsubscribe from.
<code>app <i>value</i></code>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
<code>age <i>value</i></code>	Filters viewable copies on the console by the age of a copy. The value can be one of the following: <ul style="list-style-type: none"> • day • week • month • all

/?	Displays command line help.
----	-----------------------------

Description

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. The arguments are application-specific so ensure that you use the help command `"/?"` for details. For example:

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

Table 5 Application specific options

SQL	
<code>instance_name</code> <i>value</i>	The SQL instance of the desired database. The default is <code>instance_name=MSSQLSERVER</code> .
<code>db_name</code> <i>value</i>	Displays the specified SQL database.
<code>log_backup_only</code> <i>value</i>	Determines whether the database log back up must be displayed or not. The value can be true or false.
<code>onlyRepurposeCopies</code> <i>value</i>	Determines whether repurposed copies must be displayed or not. The value can be true or false.
Oracle	
<code>oracle_server</code> <i>value</i>	The Oracle server of the desired database. For an Oracle RAC, enter all the nodes as a comma separated string. For example, <code>oracle_server=node1,node2</code> .
<code>db_name</code> <i>value</i>	Displays the specified Oracle database.
<code>onlyRepurposeCopies</code> <i>value</i>	Determines whether repurposed copies must be displayed or not. The value can be true or false.
File system	
<code>fs_server</code> <i>value</i>	The server of the desired file system. The default is <code>fs_server=localhost</code> .
<code>fs_name</code> <i>value</i>	The name of the file system. The default is <code>fs_name=C:\.</code>
<code>fs_type</code> <i>value</i>	The format of the file system. The default is <code>fs_type=ntfs</code> .
Datastore	
<code>datastore</code> <i>value</i>	The name of the desired datastore.
<code>datacenter</code> <i>value</i>	The datacenter to find the datastore.
<code>vcenter</code> <i>value</i>	The vCenter server to find the datastore. The default is <code>vcenter=localhost</code> .

Table 5 Application specific options (continued)

Exchange	
<code>ex_server</code> <i>value</i>	Name of the Exchange server that you want to display. In the case of DAG, the server name is the DAG name.
<code>db_name</code> <i>value</i>	Displays the specified Exchange database.

See also

`copyDetails`

copyDetails

Displays information about a specified copy.

Syntax

```
-copyDetails
app value
copy_ID value
/?
```

Arguments

<code>app</code> <i>value</i>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
<code>copy_ID</code> <i>value</i>	The UUID of the copy that you want to display.
<code>/?</code>	Displays command line help.

Description

A copy's uuid is required before you can mount the copy. To fetch additional information of an application copy, run the `-copyDetails` command for either a service plan or an application object. The arguments are application-specific so ensure that you use the help command `"/?"` for details. For example:

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

See also

`listCopies`

mount

Mounts a specified copy.

Syntax

```
-mount
```

copy_ID *value*

app *value*

/?

Arguments

copy_ID <i>value</i>	The UUID of the copy that you want to mount.
app <i>value</i>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
/?	Displays command line help.

Description

The AppSync CLI supports all mount options that are available through the GUI. The options vary for each application. Run the help "/" command for the application that you want to mount to determine the 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>`

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

Table 6 SQL specific options

SQL	
copy_ID <i>value</i>	The UUID of the copy that you want to mount.
option <i>value</i>	Specifies the copy recovery option. The value can be mount or recover.
Mount Standalone SQL options	
mount_host <i>value</i>	The host on which to mount the copy.
mount_all_copies <i>value</i>	Determines whether to mount all copies. The value can be true or false.
qos_policy <i>value</i>	Name of GoS policy as it appears in XtremIO.
mount_access <i>value</i>	Type of access the copy must be mounted with.

Table 6 SQL specific options (continued)

<code>mount_path</code> <i>value</i>	<p>The non-default path to mount a copy. The value can be one of the following:</p> <ul style="list-style-type: none"> • Mapped path • Default path <pre>UNIX DEFAULT: /appsync-mounts WIN DEFAULT: SystemDrive \AppSyncMounts\ProdServerName</pre>
<code>mapped_path</code> <i>value</i>	<p>The map of source to target path. This option is applicable only to mapped path.</p> <pre>UNIX: /source:::/target,/abc:::/xyz WIN: R:\:::S:\,T: \MountPoint:::U:\</pre>
<code>metadata_path</code> <i>value</i>	The non-default path to mount copy metadata.
<code>image_access_mode</code> <i>value</i>	<p>The access mode for the image. The value can be one of the following:</p> <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>dedicated_sg</code> <i>value</i>	Specifies the dedicated storage group.
<code>disable_rp_srm</code> <i>value</i>	Disables RecoverPoint SRM (Site Recovery Manager). This option is only applicable to RecoverPoint 4.1 and later. The value can be true or false.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
Mount and Recover SQL options	
<code>recovery_instance</code> <i>value</i>	The SQL Server instance to be used for recovery.
<code>recovery_type</code> <i>value</i>	The type of recovery desired.
<code>db_naming_suffix</code> <i>value</i>	Specify a suffix that must be appended to the database after mount.

Table 6 SQL specific options (continued)

<code>mount_path</code> <i>value</i>	<p>The non-default path to mount a copy. The value can be one of the following:</p> <ul style="list-style-type: none"> • Mapped path • Default path <pre>UNIX DEFAULT: /appsync-mounts WIN DEFAULT: SystemDrive \AppSyncMounts\ProdServerName</pre>
<code>mapped_path</code> <i>value</i>	<p>The map of source to target path. This option is applicable only to mapped path.</p> <pre>UNIX: /source:::/target,/abc:::/xyz WIN: R:\:::S:\,T: \MountPoint:::U:\</pre>
<code>metadata_path</code> <i>value</i>	The non-default path to mount copy metadata.
<code>image_access_mode</code> <i>value</i>	<p>The access mode for the image. The value can be one of the following:</p> <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>dedicated_sg</code> <i>value</i>	Specifies the dedicated storage group.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
<code>vmware_vdisk_mode</code> <i>value</i>	<p>Allows you to mount copies as independent disks. The value can be one of the following:</p> <ul style="list-style-type: none"> • independent_persistent • independent_nonpersistent
<code>unlink_copy_before_unmount</code> <i>value</i>	Allows you to unlink the SnapVX snap during mount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

Table 7 Oracle specific options

Oracle	
<code>copy_ID</code> <i>value</i>	The UUID of the copy that you want to mount.
<code>option</code> <i>value</i>	Specifies the copy recovery option. The value can be one of the following: <ul style="list-style-type: none"> • mount • rman • recover • manual • rac
Mount Standalone Oracle options	
<code>mount_host</code> <i>value</i>	The host on which to mount the copy.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_path</code> <i>value</i>	The non-default path to mount a copy.
<code>qos_policy</code> <i>value</i>	Name of GoS policy as it appears in XtremIO.
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>disable_rp_srm</code> <i>value</i>	Disables RecoverPoint SRM (Site Recovery Manager). This option is only applicable to RecoverPoint 4.1 and later. The value can be true or false.
<code>filesystem_check</code> <i>value</i>	Performs a file system check during mount. This is only applicable to UNIX and LINUX hosts. The value can be true or false.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
<code>vmware_vdisk_mode</code> <i>value</i>	Allows you to mount copies as independent disks. The value can be one of the following: <ul style="list-style-type: none"> • independent_persistent • independent_nonpersistent

Table 7 Oracle specific options (continued)

Mount RMAN Oracle options	
<code>mount_host</code> <i>value</i>	The host on which to mount the copy.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_path</code> <i>value</i>	The non-default path to mount a copy.
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>rman_user</code> <i>value</i>	Specifies the RMAN user name.
<code>rman_password</code> <i>value</i>	Specifies the RMAN password.
<code>rman_connect_string</code> <i>value</i>	Specifies the RMAN connect string.
<code>tns_admin</code> <i>value</i>	The non-default path of TNS_ADMIN.
<code>oracle_home</code> <i>value</i>	The non-default path of ORACLE_HOME.
<code>asm_dg_name</code> <i>value</i>	The non-default name for the ASM disk group.
<code>skip_data_files</code> <i>value</i>	Allows you to skip data files.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
Mount and Recover Oracle options	
<code>mount_host</code> <i>value</i>	The host on which to mount the copy.
<code>mount_path</code> <i>value</i>	The non-default path to mount a copy.
<code>image_access_mode</code> <i>value</i>	Access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>open_mode</code> <i>value</i>	Specifies the open mode for the copy after recovery.
<code>oracle_home</code> <i>value</i>	The non-default path of ORACLE_HOME.

Table 7 Oracle specific options (continued)

<code>database_name value</code>	The non-default name for the database.
<code>sid_name value</code>	The non-default name for the SID.
<code>asm_dg_name value</code>	The non-default name for the ASM disk group.
<code>init_params value</code>	Specifies the custom init parameters for recovery.
<code>point_in_time value</code>	Allows you to mount a point in time copy.
<code>desired_SLO value</code>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST value</code>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount value</code>	Specifies the VPLEX mount options.
<code>enable_cluster_mount value</code>	Enables VMware cluster mount.
<code>spfile_asm value</code>	Creates an SPFILE on ASM.
<code>add_control_files value</code>	Creates additional control files.
<code>change_db value</code>	Specifies the database ID of the mounted database.
<code>use_adr_dest value</code>	Forces the mounted database to use the ADR home directory instead of TEMP for diagnostic logs.
<code>disable_arch value</code>	Disables the ARCHIVELOG mode on a mounted database.
<code>unlink_copy_before_unmount value</code>	Allows you to unlink the SnapVX snap during mount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Mount Manual Recovery ORACLE	
<code>mount_host value</code>	The host on which to mount the copy.
<code>mount_path value</code>	The non-default path to mount a copy.
<code>image_access_mode value</code>	Access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>open_mode value</code>	Specifies the open mode for the copy after recovery.
<code>oracle_home value</code>	The non-default path of ORACLE_HOME.
<code>database_name value</code>	The non-default name for the database.

Table 7 Oracle specific options (continued)

<code>sid_name value</code>	The non-default name for the SID.
<code>asm_dg_name value</code>	The non-default name for the ASM disk group.
<code>init_params value</code>	Specifies the custom init parameters for recovery.
<code>point_in_time value</code>	Allows you to mount a point in time copy.
<code>desired_SLO value</code>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST value</code>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount value</code>	Specifies the VPLEX mount options.
<code>enable_cluster_mount value</code>	Enables VMware cluster mount.
Mount RAC	
<code>mount_cluster value</code>	The cluster you wish to mount a copy to. The default is Original Cluster.
<code>mount_server value</code>	The server on which to mount the copy.
<code>mount_path value</code>	The non-default path to mount a copy.
<code>image_access_mode value</code>	Access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>open_mode value</code>	Specifies the open mode for the copy after recovery.
<code>oracle_home value</code>	The non-default path of ORACLE_HOME.
<code>database_name value</code>	The non-default name for the database.
<code>sid_name value</code>	The non-default name for the SID.
<code>asm_dg_name value</code>	The non-default name for the ASM disk group.
<code>init_params value</code>	Specifies the custom init parameters for recovery.
<code>point_in_time value</code>	Allows you to mount a point in time copy.
<code>desired_SLO value</code>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST value</code>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount value</code>	Specifies the VPLEX mount options.

Table 7 Oracle specific options (continued)

<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
--	-------------------------------

Table 8 File system specific options

File system	
<code>copy_ID</code> <i>value</i>	The UUID of the copy that you want to mount.
<code>option</code> <i>value</i>	Specifies the copy recovery option. The value can be mount or recover.
<code>mount_host</code> <i>value</i>	The host on which to mount the copy. The default is original host.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_access</code> <i>value</i>	Type of access the copy must be mounted with. The value can be readonly or readwrite.
<code>mount_path</code> <i>value</i>	The path to mount a copy. The value can be one of the following: <ul style="list-style-type: none"> Mapped path Default path <pre>UNIX DEFAULT: /appsync-mounts WIN DEFAULT: SystemDrive \AppSyncMounts\ProdServerName</pre>
<code>mapped_path</code> <i>value</i>	The map of source to target path. This option is applicable only to mapped path. <pre>UNIX: /source:::/target,/abc:::/xyz WIN: R:\:::S:\,T:\MountPoint:::U:\</pre>
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> logged virtual virtual_roll
<code>disable_rp_srm</code> <i>value</i>	Disables RecoverPoint SRM (Site Recovery Manager). This option is only applicable to RecoverPoint 4.1 and later. The value can be true or false.
<code>qos_policy</code> <i>value</i>	Name of QoS policy as it appears in XtremIO.
<code>filesystem_check</code> <i>value</i>	Performs a file system check during mount. This is only applicable to UNIX and LINUX hosts. The value can be true or false.

Table 8 File system specific options (continued)

<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy. (FORMAT: \ <code>"MM/dd/yyyy hh:mm:ss am/pm \"</code>)
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount. The value can be true or false.
<code>dedicated_sg</code> <i>value</i>	Specifies the dedicated storage group. The value can be true or false.
<code>vmware_vdisk_mode</code> <i>value</i>	Allows you to mount copies as independent disks. The value can be one of the following: <ul style="list-style-type: none"> <code>independent_persistent</code> <code>independent_nonpersistent</code>
<code>unlink_copy_before_unmount</code> <i>value</i>	Allows you to unlink the SnapVX snap during mount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

Table 9 Datastore specific options

Datastore	
<code>copy_ID</code> <i>value</i>	The UUID of the copy that you want to mount.
<code>mount_host</code> <i>value</i>	The host on which to mount the copy. The default is original host.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_signature</code> <i>value</i>	Allows you to specify whether you want to use the original or new mount signature. The value can be new or original.
<code>cluster_mount</code> <i>value</i>	Specifies whether you want to mount to a cluster or not. The value can be yes or no.
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> <code>logged</code> <code>virtual</code> <code>virtual_roll</code>
<code>qos_policy</code> <i>value</i>	Name of QoS policy as it appears in XtremIO.

Table 9 Datastore specific options (continued)

<code>disable_rp_srm</code> <i>value</i>	Disables RecoverPoint SRM (Site Recovery Manager). This option is only applicable to RecoverPoint 4.1 and later. The value can be true or false.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy. (FORMAT: \ "MM/dd/yyyy hh:mm:ss am/pm \")
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V22 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>unlink_copy_before_unmount</code> <i>value</i>	Allows you to unlink the SnapVX snap during mount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

Table 10 Exchange specific options

Exchange	
<code>copy_ID</code> <i>value</i>	The UUID of the copy that you want to mount.
<code>option</code> <i>value</i>	Specifies the copy recovery option. The value can be mount or validate.
Mount Standalone Exchange options	
<code>mount_host</code> <i>value</i>	The host on which to mount the copy.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_access</code> <i>value</i>	Type of access the copy must be mounted with.
<code>mount_path</code> <i>value</i>	The path to mount a copy. The value can be one of the following: <ul style="list-style-type: none"> • Mapped path • Default path <pre>UNIX DEFAULT: /appsync-mounts WIN DEFAULT: SystemDrive \AppSyncMounts\ProdServerName</pre>

Table 10 Exchange specific options (continued)

<code>mapped_path</code> <i>value</i>	The map of source to target path. This option is applicable only to mapped path. <pre>UNIX: /source:::/target,/abc:::/xyz WIN: R:\:::S:\,T:\MountPoint:::U:\</pre>
<code>qos_policy</code> <i>value</i>	Name of QoS policy as it appears in XtremIO.
<code>metadata_path</code> <i>value</i>	The non-default path to mount copy metadata.
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>disable_rp_srm</code> <i>value</i>	Disables RecoverPoint SRM (Site Recovery Manager). This option is only applicable to RecoverPoint 4.1 and later. The value can be true or false.
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
<code>vmware_vdisk_mode</code> <i>value</i>	Allows you to mount copies as independent disks. The value can be one of the following: <ul style="list-style-type: none"> • independent_persistent • independent_nonpersistent
<code>unlink_copy_before_unmount</code> <i>value</i>	Allows you to unlink the SnapVX snap during mount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Mount and Validate Standalone Exchange	
<code>mount_host</code> <i>value</i>	The host on which to mount the copy.
<code>mount_all_copies</code> <i>value</i>	Determines whether to mount all copies. The value can be true or false.
<code>mount_access</code> <i>value</i>	Type of access the copy must be mounted with.

Table 10 Exchange specific options (continued)

<code>mount_path</code> <i>value</i>	The non-default path to mount a copy.
<code>metadata_path</code> <i>value</i>	The non-default path to mount copy metadata.
<code>image_access_mode</code> <i>value</i>	The access mode for the image. The value can be one of the following: <ul style="list-style-type: none"> • logged • virtual • virtual_roll
<code>point_in_time</code> <i>value</i>	Allows you to mount a point in time copy.
<code>desired_SLO</code> <i>value</i>	Specifies the desired service level objectives for VMAX3/PowerMAX arrays.
<code>desired_FAST</code> <i>value</i>	Specifies the FAST policy for VMAX V2 copies.
<code>vplex_mount</code> <i>value</i>	Specifies the VPLEX mount options.
<code>enable_cluster_mount</code> <i>value</i>	Enables VMware cluster mount.
<code>validate_copies</code> <i>value</i>	Determines whether the copies will be validated as part of the mount.
<code>db_logs</code> <i>value</i>	Validate databases and logs. The value can be Sequentially or inparallel.
<code>log_check</code> <i>value</i>	Enables you to minimize log checking. The value can be true or false.
<code>working_dir</code> <i>value</i>	Specifies the working directory.
<code>throttle_validation</code> <i>value</i>	Enables you to throttle the validation. The value can be true or false.
<code>pause_after_I/O_count_of</code> <i>value</i>	Specifies the pause after the I/O count. The default is 100.
<code>pause_duration</code> <i>value</i>	Specifies the pause duration. The default is 1000 milliseconds.
<code>skip_db_validation</code> <i>value</i>	Skips database validation. The value can be true or false.

See also

unmount

unmount

Unmounts a specified copy.

Syntax

-unmount

`copy_ID` *value*

app *value*

/?

Arguments

copy_ID <i>value</i>	The UUID of the copy that you want to unmount.
app <i>value</i>	The application name. The value can be one of the following: <ul style="list-style-type: none"> • sql • oracle • filesystems • datastore • exchange
/?	Displays command line help.

Description

To unmount a copy you must specify 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 a database, filesystem, or a datastore, use the following commands:

- **For Datastores:** `appsync-cli.bat -unmount app=datastore datastore=<value> datacenter=<value> vcenter=<value> option=latestMountedCopy/oldestMountedCopy`
- **For SQL:** `appsync-cli.bat -unmount app=sqlinstance_name=<value> db_name=<value> option=latestMountedCopy/oldestMountedCopy`
- **For Oracle:** `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`

See also

mount

CHAPTER 4

Service Plans

This chapter includes the following topics:

- [Service plan overview](#) 52
- [Oracle service plan details](#) 74
- [SQL Server service plan details](#) 78
- [File system service plan details](#) 83
- [VMware Datacenter service plan details](#) 86
- [Microsoft Exchange service plan settings](#) 88

Service plan overview

This section describes the default service plans available in AppSync, service plan operations, service plan settings, schedules, subscriptions and overrides.

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 applications 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. It is not recommended to subscribe 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 service plans:

- **Bronze** — You can use the Bronze service plan to create local copies of your applications.
- **Silver** — You can use the Silver service plan to create remote copies of your applications.
- **Gold** — You can use the Gold service plan to create both local and remote copies of your applications.

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 your own plans.

The following table describes the service plans and applications supported.

Storage	Replication type	Bronze	Silver	Gold	RP support	Application support	Repurposing support
VNX	Advanced Snapshot	Yes	No	No	Yes	All applications AppSync supports	Yes
	File Snapshot ^a	Yes	Yes	Yes	No	VMware datastores, File systems, and Oracle	No
VMAX V2	VP Snap	Yes	No	No	Yes	All applications AppSync supports	Yes
	Timefinder Clone	Yes	No	No	Yes	All applications AppSync supports	Yes
	SRDF/A Local	Yes	No	No	Yes	All applications AppSync supports	Yes
	SRDF/A Remote ^b	No	Yes	No	No	VMware datastores and Oracle	

Storage	Replication type	Bronze	Silver	Gold	RP support	Application support	Repurposing support
	SRDF/S Local	Yes	No	No	Yes	All applications AppSync supports	Yes
	SRDF/S Remote	No	Yes	No	No		
PowerStore	Snapshot	Yes	Yes	Yes	No	All applications AppSync supports	Yes ^c
	Thin Clone	Yes	Yes	Yes	No		
Unity	Unified Snapshot	Yes	Yes	Yes	Yes	All applications AppSync supports	Yes
	Unified File Snapshot	Yes	No	No	No	VMware datastores, Oracle, and File systems	No
	Thin Clone ^d	No	No	No	No	Microsoft SQL, Oracle, and File systems	Yes
XtremIO	Snapshot	Yes	Yes	No	Yes	All applications AppSync supports	Yes
VMAX3/ PowerMAX / VMAX All Flash	SnapVX Snap	Yes	No	No	No	All applications AppSync supports	Yes
	SnapVX Clone	Yes	No	No	No	All applications AppSync supports	Yes ^e
	SRDF/A Local	Yes	No	No	No	All applications AppSync supports	Yes
	SRDF/A Remote ^f	No	Yes	No	No	VMware datastores, Oracle, and UNIX file systems	
	SRDF/S Local	Yes	No	Yes	No	All applications AppSync supports	Yes
	SRDF/S Remote	No	Yes	Yes	No	All applications AppSync supports	
	SRDF / Metro	No	No	No	No	SQL, File System, and Oracle	Yes ^g
VPLEX ^h	VPLEX Snap ⁱ	Yes	No	No	No	All applications AppSync supports	XtremIO - Yes Unity - Yes ^j VMAX3/ PowerMAX, VMAX All Flash - Yes
	VPLEX Clone	Yes	No	No	No		
RecoverPoint	Local bookmark	Yes	No	No	Yes	All applications AppSync supports	Yes
	Remote bookmark	No	Yes	No	Yes	All applications AppSync supports	Yes

Storage	Replication type	Bronze	Silver	Gold	RP support	Application support	Repurposing support
	Local and remote bookmark	No	No	Yes	Yes	All applications AppSync supports	No
Dell SC	Dell SC Series Snapshots	Yes	No	No	No	All applications AppSync supports ^k	No

- a. The same is also applicable to eNAS on VMAX3/PowerMAX.
- b. AppSync does not support remote protection of Windows applications on VMAX3/PowerMAX and SRDF/A storage.
- c. The first generation copy is a Snapshot or a Thin Clone. However, the second generation copy is always a Thin Clone.
- d. The first generation copy is always a Snap. However, the second generation copy can either be a Snap or a Clone.
- e. Repurposing clone from a snap is not supported.
- f. AppSync does not support remote protection of Windows applications on VMAX3/PowerMAX and SRDF/A storage.
- g. Only local repurposing is supported for SRDF Metro.
- h. VPLEX is only supported on XtremIO, VMAX3/PowerMAX, VMAX All Flash, and Unity back-end arrays.
 - i. This is the snapshot on the back-end array.
 - j. Unity thin clone is only supported on second generation copies.
 - k. AppSync only supports VM and granular file restore on Dell SC arrays.

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 copy priority 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 selected preference in the Copy Priority list. You can adjust the preferences to create service plans that use the replication technology you want on priority. If you want AppSync to skip using a particular replication technology, deselect that preference from the Copy Priority list.

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 for RMAN cataloging (Default: disabled)

To avoid overutilization and depletion of replication storage, when you set up a service plan, set Retention in the **Define the copy** screen and RPO in **Schedule** screen of the service plan.

i **Note:** AppSync expiry of old copies works based on the current subscription in a service plan. If applications are added or removed to a service plan, the current expire copy count and number of copies retained might not match. To avoid this, subscribe new applications to newly added service plan than altering the application subscription often.

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.

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.

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.

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.

Click any event to view the details in the right pane of the page. The event status, date and time, host, description, and event ID details are shown for each event.

You can view events at:

- Service plan **Events** tab. For example, on the AppSync console, go to the **Events** tab in **Copy Management > Select View > Service Plans > Select Application > Microsoft Exchange**, to view the copies. Select the specific copy and click on the events in properties. This displays the events that are related to the Exchange copy.
- Events displays the events that were generated as part of the service plan run.

By default only the top level events, which are known as milestone events, are displayed. You can expand a milestone event to show the other events that were generated.

Create a service plan

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

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

Note: The new service plan will contain the same schedule and other settings as the template, with no object subscribed to the service plan, the user is allowed to change the settings of the service plan during creation.

Create a Service Plan for an Oracle database

Perform the following procedure to create a service plan.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle** to display the service plan page.
4. Click **CREATE SERVICE PLAN**.
5. Click **SELECT TEMPLATE** and select one of the following options to use as the template to create the service plan and click **OK**:
 - Bronze
 - Gold
 - Silver

Note: User-created service plans are listed in this page. You can also use user-created service plans as templates.

6. In the **Define the copy** page, configure values for the following options:

- a. Provide a name for the service plan in the **Service Plan Name** field.
- b. Provide a description for the service plan in the **Description** field.
- c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
- d. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
- e. In the **Retention** field, specify the number of copies to retain.
 Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
7. Click **NEXT**.
8. In the Create the Copy page, do the following:
 - a. Select the desired Oracle Options:
 - **Place the database in hot backup mode**
 - **Select archive destination for hot backup mode**
 - **Index and copy the BCT(block change tracking) file**
 - **Create backup control file for RMAN cataloging**
 - **Copy the Fast Recovery Area**
 - b. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - c. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - d. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - e. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - f. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
9. Click **NEXT**.
10. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

 **Note:** This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

 - a. **Full Path to Script**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
11. Click **NEXT**.
12. In the Schedule/Run page, select one of the following scheduling options:
 - **Run Now** - Creates a service plan when you click **Finish** on this wizard.

- **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to run the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.
13. Click **NEXT**.
 14. Review the Service Plan creation settings and click **FINISH**.

Create a Service Plan for a SQL database

Perform the following procedure to create a service plan.

Procedure

1. On the AppSync console, select **Copy Management**.
 2. From the **Select View** drop-down, select **Service Plan**.
 3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the service plans page.
 4. Click **CREATE SERVICE PLAN**.
 5. Click **SELECT TEMPLATE** and select one of the following options to use as the template to create the service plan and click **OK**:
 - Bronze
 - Gold
 - Silver
-  **Note:** User-created service plans are listed in this page. You can also use user-created service plans as templates.
6. In the **Define the copy** page, configure values for the following options:
 - a. Specify a name for the service plan in the Service Plan Name field.
 - b. You can edit the description for the service plan in the Description field.
 - c. Configure the Service Plan State option to either **Enabled** or **Disabled**.
 - d. Configure the Mount Copy option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - e. In the Retention field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
 - f. In the Advanced plan settings field, specify the number of sql databases.

 **Note:** 35 is the recommended value for this option.
 7. Click **NEXT**.
 8. In the Create the Copy page, do the following:
 - a. Configure the SQL Server Backup Type settings to either **Full**, **Copy**, **Non-VDI**, or **Crash-Consistent**.

Note:

- **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. When Non VDI or Crash Consistent backup type is selected, Auto Switch to Copy and Enable log backup are disabled.
- Select **Enable Log Backup** to enable the log backup. However, when Non-VDI or Crash Consistent backup type is selected, Enable log backup is disabled. Configure the following log backup settings:
 - Configure the **Schedule** field to either **Immediately after database backup**, or **Every** and select the frequency of the log backup subsequent drop-down lists.
 - Specify the path for backup in the **Backup path** field.
 - Configure the **Free space on the volume** field, and select the wanted values from the subsequent drop-down lists.
 - Select the **Truncate the logs** field, if you want to truncate the logs.
 - Select the **Checksum the backup** field, if you want to perform a checksum on the log backup.
 - Select the **Compression** field, if you want to enable compression.
 - Configure the **Minimum Retention Hours** field, to control when transaction log backup files are deleted.

- b. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - d. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - e. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - f. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - g. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the required order.
9. Click **NEXT**.
 10. In the Scripts page select the pre-copy or post-copy scripts that you want to run and configure the following fields:

Note: This step displays the post-mount scripts if the mount option is selected. This step displays Pre Log-backup and Post Log-backup scripts if the **Enable log backups** option is selected.

- a. **Full Path to Script**
- b. **Script Parameters**

- c. **Run as User Name**
 - d. **Password**
11. Click **NEXT**.
 12. In the Schedule/Run page, select one of the following scheduling options:
 - **Run Now** - Creates a service plan when you click **FINISH** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the preferred frequency of creation.
 - In the **Every** drop-down list, select the preferred time to run the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the required time frame.
 13. Click **NEXT**.
 14. Review the Service Plan creation settings, and click **FINISH**.

Create a Service Plan for File Systems

Perform the following procedure to create a service plan.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **File Systems** to display the service plan page.
4. Click **CREATE SERVICE PLAN**.
5. Click **SELECT TEMPLATE** and select one of the following options to use as the template to create the service plan and click **OK**:
 - Bronze
 - Gold
 - Silver

 **Note:** User-created service plans are listed in this page. You can also use user-created service plans as templates.

6. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Mount Copy** option to **No**, **Yes, Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - e. In the **Retention** field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
 - f. In the **Advanced plan settings** field, you can configure the following settings

- **Enable CallOut scripts**
 - **Callout timeout(in minutes)**
7. Click **NEXT**.
 8. In the Create the Copy page, do the following:
 - a. Configure the UNIX Filesystem consistency settings to either **Filesystem Consistent** or **Crash Consistent**.
 - b. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - d. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - e. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - f. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - g. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
 9. Click **NEXT**.
 10. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

 **Note:** This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

 - a. **File**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
 11. Click **NEXT**.
 12. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **FINISH** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to run the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.
 13. Click **NEXT**.
 14. Review the Service Plan creation settings and click **FINISH**.

Create a Service Plan for VMware

Perform the following procedure to create a service plan.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **VMware Datacenters** to display the service plan page.
4. Click **CREATE SERVICE PLAN**.
5. Click **SELECT TEMPLATE** and select one of the following options to use as the template to create the service plan and click **OK**:
 - Bronze
 - Gold
 - Silver

 **Note:** User-created service plans are listed in this page. You can also use user-created service plans as templates.

6. Click **OK**.
7. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - e. In the **Retention** field, specify the number of copies to retain.
 Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
8. Click **NEXT**.
9. In the **Create the Copy** page, do the following:
 - a. Configure the copy consistency settings to either **VM Consistent** or **Crash Consistent**.
 - b. Configure the **Maximum Simultaneous VM Snapshots** field.
 - c. Optionally you can select, the **Include Virtual Machine Disk** option.
 - d. Optionally you can select, the **Wait for VMAX3/PowerMAX clone sync to complete**. This option only applies to VMAX3/PowerMAX arrays.
 - e. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - f. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - g. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - h. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.

10. Click **NEXT**.
11. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **FINISH** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to run the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.
12. Click **NEXT**.
13. Review the Service Plan creation settings and click **FINISH**.

Create a Service Plan for Exchange

Perform the following procedure to create a service plan.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft Exchange** to display the service plan page.
4. Click **CREATE SERVICE PLAN**.
5. Click **SELECT TEMPLATE**, then select one of the following options to use as the template to create the service plan:
 - Bronze
 - Gold
 - Silver

 **Note:** User-created service plans are listed in this page. You can also use user-created service plans as templates.

6. Click **OK**.
7. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - e. Configure the **Validate Copy** option to **Yes** or **No**.
 - f. In the **Retention** field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
8. Click **NEXT**.

9. In the Create the Copy page, do the following:
 - a. Configure the Exchange Backup Type to either **Full**, **Copy**, or **Differential**.
 - b. Optionally you can select, the **Allow databases and logs to reside on the same volume** option.
 - c. Configure Event log Scanning settings by selecting the following options:
 - **-1018 error (JET Read/Verify Failed)**
 - **-1019 error (JET Page Not Initialized)**
 - **-1022 error (JET Disk I/O Failure)**
 - **Event ID 447**
 - **Event ID 448**
 - d. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - e. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - f. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - g. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - h. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - i. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
10. Click **NEXT**.
11. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:
 - a. **Path**
 - b. **File**
 - c. **Script Parameters**
 - d. **Run as User Name**
 - e. **Password**
12. Click **NEXT**.
13. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **FINISH** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to run the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.

14. Click **NEXT**.
15. Review the Service Plan creation settings and click **FINISH**.

Run 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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange** to display the service plan page.
4. Select the service plan you want to run 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 progress dialog displays information as application storage is discovered and mapped, and application protection begins according to service plan settings.

5. Click **Details** to see more events.

Enable and disable a service plan

By default all service plans are enabled. You can disable a service plan or enable a disabled service plan.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange** to display the service plan page.
4. Select the plan and click **ENABLE** or **DISABLE**.

Delete 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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange** to display the service plan page.

4. Select a user-created plan and click **DELETE**.

Edit a Service Plan for an Oracle database

Perform the following procedure to edit a service plan for an Oracle database.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle** to display the service plan page.
4. Select the service plan you want to edit and click **EDIT** in the **Service Plan Details** pane.
5. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Copy Location** option to **Local**, **Remote**, or **Local and Remote**.
 - e. Configure the **Mount Copy** option to **No**, **Yes, Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. In the **Retention** field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
6. Click **NEXT**.
7. In the Create the Copy page, do the following:
 - a. Select the desired Oracle Options:
 - **Place the database in hot backup mode**
 - **Select archive destination for hot backup mode**
 - **Index and copy the BCT(block change tracking) file**
 - **Create backup control file for RMAN cataloging**
 - **Copy the Fast Recovery Area**
 - b. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - c. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - d. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - e. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - f. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
8. Click **NEXT**.
9. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

Note: This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

a. **Full Path to Script**

b. **Script Parameters**

Note: Parameters must be separated by space. Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes. For example: “username” “password”, or “F:\” “G:\”.

c. **Run as User Name**

d. **Password**

10. Click **NEXT**.

11. In the Schedule/Run page, select one of the following scheduling options:

- **Run Now** - Creates a service plan when you click **Finish** on this wizard.
- **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to create the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.

12. Click **NEXT**.

13. Review the Service Plan creation settings and click **FINISH**.

Edit a Service Plan for a SQL database

Perform the following procedure to edit a service plan for a SQL database.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the service plans page.
4. Select the service plan you want to edit and click **EDIT** in the **ServicePlan Details** pane.
5. In the **Edit Service Plan** pane, edit the values for the following options:
 - a. Edit the name of the service plan in the **Service Plan Name** field.
 - b. Edit the description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Copy Location** option to **Local**, **Remote**, or **Local and Remote**.
 - e. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. In the **Retention** field, edit the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.

g. In the **Advanced plan settings** field, edit the number of sql databases.

 **Note:** 35 is the recommended value for this option.

6. Click **Next**.

7. In the Create the Copy page, do the following:

a. Configure the SQL Server Backup Type settings to either **Full, Copy, Non-VDI**, or **Crash-Consistent**.

 **Note:**

- **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. When Non VDI or Crash Consistent backup type is selected, Auto Switch to Copy and Enable log backup are disabled.
- Select **Enable Log Backup** to enable the log backup. However, when Non VDI or Crash Consistent backup type is selected, Enable log backup is disabled. Edit the following log backup settings:
 - Configure the **Schedule** field to either **Immediately after database backup**, or **Every** and select the frequency of the log backup subsequent drop-down lists.
 - Specify the path for backup in the **Backup path** field.
 - Configure the **Free space on the volume** field, and select the desired values from the subsequent drop-down lists.
 - Select the **Truncate the logs** field, if you want to truncate the logs.
 - Select the **Checksum the backup** field, if you want to perform a checksum on the log backup.
 - Select the **Compression** field, if you want to enable compression.
 - Configure the **Minimum Retention Hours** field, to control when transaction log backup files are deleted.

b. Edit the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.

c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.

d. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.

e. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.

f. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.

g. Configure the Copy Type settings to either **Snapshot, Clone**, or **Bookmark**.

8. Click **Next**.

9. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

a. **Full Path to Script**b. **Script Parameters**

 **Note:** Parameters must be separated by space. Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes. For example: “username” “password”, or “F:\” “G:\”.

c. **Run as User Name**d. **Password**

10. Click **Next**.

11. In the Schedule/Run page, select one of the following scheduling options:

- **Run Now** - Creates a service plan when you click **Finish** on this wizard.
- **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, edit the desired time to create the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, edit the desired time frame.

12. Click **Next**.

13. Review the Service Plan creation settings and click **Finish**.

Edit a Service Plan for a File system

Perform the following procedure to edit a service plan for File Systems.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **File Systems** to display the service plan page.
4. Select the service plan you want to edit and click **EDIT** in the **ServicePlan Details** pane.
5. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Copy Location** option to **Local**, **Remote**, or **Local and Remote**.
 - e. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. In the **Retention** field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
 - g. In the **Advanced plan settings** field, you can configure the following settings

- **Enable CallOut scripts**
 - **Callout timeout(in minutes)**
6. Click **NEXT**.
 7. In the Create the Copy page, do the following:
 - a. Configure the UNIX Filesystem consistency settings to either **Filesystem Consistent** or **Crash Consistent**.
 - b. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - d. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - e. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - f. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - g. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
 8. Click **NEXT**.
 9. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

 **Note:** This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

 - a. **File**
 - b. **Script Parameters**

 **Note:** Parameters must be separated by space. Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes. For example: “username” “password”, or “F:\” “G:\”.
 - c. **Run as User Name**
 - d. **Password**
 10. Click **NEXT**.
 11. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **Finish** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to create the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.

12. Click **NEXT**.
13. Review the Service Plan creation settings and click **FINISH**.

Edit a Service Plan for VMware

Perform the following procedure to edit a service plan for VMware Datacenters.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **VMware Datacenters** to display the service plan page.
4. Select the service plan you want to edit and click **EDIT** in the **ServicePlan Details** pane.
5. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Copy Location** option to **Local**, **Remote**, or **Local and Remote**.
 - e. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. In the **Retention** field, specify the number of copies to retain.
 Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
6. Click **NEXT**.
7. In the **Create the Copy** page, do the following:
 - a. Configure the copy consistency settings to either **VM Consistent** or **Crash Consistent**.
 - b. Configure the **Maximum Simultaneous VM Snapshots** field.
 - c. Optionally you can select, the **Include Virtual Machine Disk** option.
 - d. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - e. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - f. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - g. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - h. Configure the Copy Priority to settings by dragging and dropping the **Snapshot**, **Clone**, and **Bookmark** options in the desired order.
8. Click **NEXT**.
9. In the **Schedule/Run** page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **Finish** on this wizard.

- **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to create the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.
10. Click **NEXT**.
 11. Review the Service Plan creation settings and click **FINISH**.

Edit a Service Plan for Exchange

Perform the following procedure to edit a service plan for Microsoft Exchange.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft Exchange** to display the service plan page.
4. Select the service plan you want to edit and click **EDIT** in the **Service Plan Details** pane.
5. In the **Define the copy** page, configure values for the following options:
 - a. Provide a name for the service plan in the **Service Plan Name** field.
 - b. Provide a description for the service plan in the **Description** field.
 - c. Configure the **Service Plan State** option to either **Enabled** or **Disabled**.
 - d. Configure the **Copy Location** option to **Local**, **Remote**, or **Local and Remote**.
 - e. Configure the **Mount Copy** option to **No**, **Yes**, **Yes - Keep it mounted(Previous copy will be unmounted)**, or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. Configure the **Validate Copy** option to **Yes** or **No**.
 - g. In the **Retention** field, specify the number of copies to retain.

Select the **Include RecoverPoint copies in expiration rotation policy**, if you want to include RecoverPoint copies in the expiration rotation policy.
6. Click **NEXT**.
7. In the Create the Copy page, do the following:
 - a. Configure the Exchange Backup Type to either **Full**, **Copy**, or **Differential**.
 - b. Optionally you can select, the **Allow databases and logs to reside on the same volume** option.
 - c. Configure Event log Scanning settings by selecting the following options:
 - **-1018 error (JET Read/Verify Failed)**
 - **-1019 error (JET Page Not Initialized)**
 - **-1022 error (JET Disk I/O Failure)**
 - **Event ID 447**
 - **Event ID 448**

- d. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - e. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - f. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - g. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - h. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - i. Configure the Copy Priority to settings by dragging and dropping the **Snapshot, Clone, and Bookmark** options in the desired order.
8. Click **NEXT**.
 9. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:
 - a. **Path**
 - b. **File**
 - c. **Script Parameters**

 **Note:** Parameters must be separated by space. Exact parameters depend on the script. Parameters with spaces must be enclosed in double quotes. For example: “username” “password”, or “F:\” “G:\”.
 - d. **Run as User Name**
 - e. **Password**
 10. Click **NEXT**.
 11. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a service plan when you click **FINISH** on this wizard.
 - **Schedule** - Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan:
 - In the **Recurrence Type** drop-down list, select the desired frequency of creation.
 - In the **Every** drop-down list, select the desired time to create the service plan.
 - Select the **Enable Recovery Point Objective** to enable the RecoveryPoint objective.
 - In the **RPO** drop-down list, select the desired time frame.
 12. Click **NEXT**.
 13. Review the Service Plan creation settings and click **FINISH**.

Unsubscribe from a service plan

You can unsubscribe applications that are subscribed to bronze, silver, gold, or the custom service plans.

Procedure

1. On the AppSync console, go to **Copy Management**.

2. Click **Select View > Service Plan**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems / VMware Datacenters / Microsoft Exchange**.

4. Click the desired service plan.

The details are displayed in the right pane of the page for the selected service plan.

5. Select the **SUBSCRIBERS** tab.

The subscribers of the selected service plan displays.

6. Select an instance, application, datastore, or server and click **UNSUBSCRIBE**.

The selected application is no more subscribed to the service plan.

 **Note:** You can also select multiple instances and unsubscribe all of them together.

Enable or disable automatic expiry of a copy

You can enable or disable automatic expiry of a copy during rotation.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems / VMware Datacenters / Microsoft Exchange**.
4. Click the name of the desired service plan.
5. In the **Copies** page, select a copy, and click **MORE**.
6. Select one of the following choices:
 - Select **Enable Copy Rotation** to enable automatic expiry of a copy during rotation.
 - Select **Disable Copy Rotation** to disable automatic expiry of a copy during rotation.

You can also navigate to **Copy Management Select View > Copies > Select Application > Oracle / Microsoft SQL Server / File Systems / VMware Datacenters / Microsoft Exchange**, and navigate to the copies page to disable automatic expiry of a copy.

Service Plan Events

The events page displays a list of the events associated with the service plan.

Click any event to view the details in the right pane of the page. To do so:

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems / VMware Datacenters / Microsoft Exchange**.
4. Click the name of the desired service plan.
5. In the **Events** tab, select an entry to view detailed events generated during the service plan run on the right pane.

The event status, date and time, host, description, and event ID details are shown for each event. Use the **Show/Hide Columns** button to view or hide event details.

Oracle service plan details

Lists the Oracle Database service plan settings with their default values.

This table describes the Oracle service plan details.

Table 11 Oracle database Service Plan details

Name	Description
Service Plan Name	Type of service plan.
Description	Describes the function of the service plan.
Enabled	Specifies if the service plan is enabled or disabled.
Location	Specifies if the location is local, remote, or local and remote..
Mount	Specifies the type of Mount Copy option is enabled or disabled.
Retention	Specifies the configured copy retention number.
Schedule	Specifies the recurrence type that is configured for the service plan.
Pre-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on Production host before creating a copy in AppSync.
Post-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a copy in AppSync.
Post-mount script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after the copy is mounted by the service plan run.
Mount copy	<ul style="list-style-type: none"> Mount on Standalone server :Original Host Mount Path: Default Path Image Access mode: Logged access
Copy to mount	<p>Allows user to select if the local or remote copy has to be mounted as part of service plan run.</p> <p> Note: Applies to service plans that create local and remote copies simultaneously.</p>
Recovery settings	<ul style="list-style-type: none"> Mount and recovery operations: <ul style="list-style-type: none"> Mount on standalone server (RM-equivalent : No recover) Mount on standalone server and create RMAN catalog entry (RM-equivalent : Catalog with RMAN) 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) Recovery Settings: <ul style="list-style-type: none"> Open-mode: Read-write

Table 11 Oracle database Service Plan details (continued)

Name	Description
	<ul style="list-style-type: none"> ▪ ORACLE_HOME: Same as production host ▪ Database name: APS is the prefix, %DB% is the variable which will be replaced with the production database name during run time. ▪ SID name: APS is the prefix, %SID% is the variable which will be replaced with the production database SID during run time. ▪ ASM diskgroup name: APS is the prefix, %DG% is the variable which will be replaced with the production ASM diskgroup name during run time. i Note: If multiple diskgroups are involved, a prefix or suffix is mandatory. ▪ Customize Initialization Parameters: This field will be blank. You can fill in one parameter per line, for example, memory_target=629145600 ▪ Create TEMP Tablespace: Use this option to create the Temp Tablespace on the recovery mounted database copy. This setting is enabled when you select the following mount operations with Read/Write Open-mode: 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. When you select the Create TEMP Tablespace option, two additional options display: <ul style="list-style-type: none"> ▪ Number of Tempfiles: The number of files to be added to Temp Tablespace. The size of the files are specified in the Size of each file setting. ▪ Use BIGFILE option: Use the BIGFILE option when creating the new temp file. If this option is selected, the number of temp files is 1. ▪ Size of each file: The size of each temp file (in kilobytes (K), megabytes (M), gigabytes (G), or terabytes (T)). ▪ Restart databases after reboot: Select this option to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled. <ul style="list-style-type: none"> i Note: This option is not available for RMAN and mount with generate scripts. ▪ Create SPFile: Select this option to create an SPFile. The SPFile is created in the default location (<code>\$ORACLE_HOME/dbs</code>), with the name <code>spfile<SID>.ora</code>. During unmount, the SPFile is removed from the <code>\$ORACLE_HOME/dbs</code> folder. ▪ Create on ASM disk: Select this option to create the SPFile on the primary ASM diskgroup. • Advanced Recovery Options <ul style="list-style-type: none"> ▪ Create Control file copies: Select this option to create 0-3 additional control file copies for redundancy purposes. The default is 0. ▪ Change Database ID: Select this option to change the database ID of the mounted database. By default, this option is disabled. ▪ Use ADR (Automatic Diagnostic Repository) home directory for DIAGNOSTIC_DEST: Select this option to force the mounted database to use the ADR home directory instead of TEMP for diagnostic logs (default: off). By default, this option is disabled. ▪ Disable archive log mode: Select this option to force the mounted database to start with archive logging disabled. By default, this option is disabled.
Create Copy details	

Table 11 Oracle database Service Plan details (continued)

Name	Description
Copy Priority	<ul style="list-style-type: none"> • Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. • Allows you to order, select, or clear storage preferences. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Place the database in hot backup mode	This option is enabled by default. 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. The copy is created from the live unquiesced data without any instrumentation of the database.
Archive destination for hot backup mode	<p>Select archive destination for hot backup mode.</p> <ul style="list-style-type: none"> • This option is disabled by default. This means that all configured archive destinations are protected. • This option is enabled only if you select Place database in hot-backup mode. You can specify up to 10 archive log destinations. AppSync discovers the specified archive destinations and maps them during protection. For example, consider archive destination 1 is on file system 1 and archive destination 2 is on file system 2. If you select only archive destination 1, then AppSync maps and protects only file system 1.
Index and copy the BCT (block change tracking) file	<ul style="list-style-type: none"> • This option is disabled by default. • 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 catalog	<ul style="list-style-type: none"> • This option is disabled by default. • 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.
Select Storage Pools to be used for VMAX-2 Array(s)	Select the preferred storage pools to use if you are configuring VMAX V2 Arrays.
Select Storage Groups to be used for VMAX-3 Array(s)	Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX Arrays.
Select the cluster and arrays in preferred order for VPLEX metro configuration	Allows you to configure array preference by dragging and dropping the available options in the preferred order.
Copy the Fast Recovery Area	When enabled, this field tells AppSync to create a copy of the underlying storage the FRA uses when protecting the archive log files of database.
Mount on Server	The server on which to mount the copy.
Mount path	The Default Mount Path is <code>/appsync</code> . 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, <code>/EMC</code> instead of <code>/AppSync</code> .

Table 11 Oracle database Service Plan details (continued)

Name	Description
Quality of Service Policy	For XtremIO only, an option called Quality of Service policy appears in the wizard. You can select the desired Quality of Service policy for mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> • 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 V2, 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 V2, 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 V2, and RP-XtremIO, virtual access is not supported.
Restart databases after reboot	Use this option to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired SLO appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes.
Enable VMware cluster mount	Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Allow Unmount Of OnDemand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.
Enable VMware cluster mount	<ul style="list-style-type: none"> • Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. • If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMWare SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.

Table 11 Oracle database Service Plan details (continued)

Name	Description
VMware Virtual Disk Mode	Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
Mount Operation	Allows the following mount operations: <ul style="list-style-type: none"> • 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 • Mount on grid cluster and recover as RAC database
Run Filesystem Check	During a mount operation, theAppSync agent checks file system data consistency by executing the <code>fsck</code> command. This operation can be time consuming. You can clear this option to skip file system check during a mount operation. By default, file system check is enabled. <p> Note:</p> <ul style="list-style-type: none"> • In the case of a restore operation, the Run Filesystem Check option is enabled by default. You cannot disable it. • The Run Filesystem Check option is not applicable to ASM file systems.

SQL Server service plan details

Summary of SQL Server service plan details.

This table describes the SQL Server service plan details.

Table 12 SQL Server Service Plan details

Name	Description
Service Plan Name	Name of the service plan.
Description	Describes the function of the service plan.
Enabled	Specifies if the service plan is enabled or disabled.
Location	Specifies if the location is local or remote.
Mount Copy	Specifies if the following options for mounting a copy: <ul style="list-style-type: none"> • No • Yes • Yes - Keep it mounted(Previous copy will be unmounted) • Yes - Mount the copy, but after the post mount scripts run, unmount the copy
Copy to mount	Allows user to select if the local or remote copy has to be mounted as part of service plan run.

Table 12 SQL Server Service Plan details (continued)

Name	Description
	<p> Note: Applies to service plans that create local and remote copies simultaneously.</p>
Mount and recover copy	Allows you to select both clustered and standalone instances to mount a SQL Server Database either as a clustered or standalone database with recovery. For mounting as a clustered or standalone database, you can mount to the original path or to the alternate mount point.
Retention	Specifies the configured copy retention number. Enable Include RecoverPoint copies in expiration rotation policy options to include the Recover point copies
Schedule	Specifies the recurrence type that is configured for the service plan.
Maximum number of sql databases	Specifies the maximum number of sql databases allowed to be configured in AppSync.
Mount on Server	The server on which copy has to be mounted. Only the nodes of the cluster and standalone hosts are available for selection. SQL virtual servers are filtered out.
Mount with access	Type of access the copy should be mounted with. (read-only or read-write)
Mount on path	<ul style="list-style-type: none"> • 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. • Select Mapped Path to specify the path where you want to mount the database.
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Copy metadata files to	<ul style="list-style-type: none"> • 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. <p> Note:</p> <ul style="list-style-type: none"> • Metadata is not created for Non VDI copies. • VSS or VDI metadata is not generated for Crash Consistent copies.

Table 12 SQL Server Service Plan details (continued)

Name	Description
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> • 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 V2, 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 V2 and RP XtremIO is not supported.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes.
Use Dedicated Storage Group	<ul style="list-style-type: none"> • 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 V2 , VNX storage group, PowerStore host group or XtremIO initiator group for a mount. (A dedicated VMAX V2 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. <ul style="list-style-type: none"> ⓘ 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. <ul style="list-style-type: none"> ⓘ 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.
Enable VMware cluster mount	If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMware SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.

Table 12 SQL Server Service Plan details (continued)

Name	Description
VMware Virtual Disk Mode	<p>Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.</p> <ul style="list-style-type: none"> • Enable VMWare Virtual Disk Mode and select Persistent to mount the copy in an independent persistent mode. • Enable VMWare Virtual Disk Mode and select Non Persistent to mount the copy in an independent non persistent mode.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Allow Unmount Of OnDemand Mounted Copy	Enabling this option will unmount the on demand mounted during next Service plan run.
Pre-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on Production host before creating a copy in AppSync.
Post-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a copy in AppSync.
Post-mount script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after the copy is mounted by the service plan run.
Pre-log backup script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on production host before creating a log backup copy of the database in AppSync.
Post-log backup script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a log backup copy of the database in AppSync.
Create Copy details	
Copy Priority	<ul style="list-style-type: none"> • Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. • Allows you to order, select, or clear storage preferences. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Backup Type	<ul style="list-style-type: none"> • SQL Server Backup Type: Full, Copy, Non VDI, or Crash Consistent <ul style="list-style-type: none"> ▪ 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. ▪ Non VDI - protects the database without using VDI, and depends on VSS to create crash consistent copies. ▪ Crash Consistent - protects the database without using VSS or VDI, and depends on the array to create crash consistent copies.
Auto Switch to Copy	The Auto Switch to Copy option is enabled only when Full is selected as the backup type. However, it is unchecked by default. Checking the Auto Switch to Copy option 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. When Non VDI

Table 12 SQL Server Service Plan details (continued)

Name	Description
	<p>or Crash Consistent backup type is selected, Auto Switch to Copy and Enable log backup are disabled.</p> <p>Secondary databases are read-only and can be backed up with the Copy backup type.</p>
VSS Retry Count	<p>Specifies the number of times the VSS retry option is run. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry count.</p>
VSS Retry Interval(In Seconds)	<p>Specifies the timeframe (in seconds) between VSS retries. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry interval.</p>
Enable log backup	<p>Specifies if the Enable log backup is enabled or disabled.</p>
LogBackup Schedule	<p>Specifies the schedule for log backups.</p>
Free Space on Volume	<p>AppSync verifies if the specified amount of free space is available on the volume before beginning transaction log backup.</p>
LogBackup Path	<p>Sets 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.</p>
Backup Group size	<p>Controls the number of parallel log backups for a 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.</p>
Truncate the logs	<p>Specifies whether to truncate the logs when you create Full database backups. This field is checked by default when you select the 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.</p>
Checksum the backup	<p>Specifies whether to perform a checksum on the log backup.</p>
Compression	<p>Specifies if compression is enabled or disabled.</p>
Minimum Retention Hours	<p>Controls 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.</p>
Wait for VMAX3/PowerMAX clone sync to complete	<p>Allows you to specify if AppSync must wait for the clone sync to complete for VMAX3/PowerMAX Arrays.</p>
Select Storage Groups for VMAX-3 Array(s)	<p>Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX Arrays.</p>
Select Storage Pools to be used for VMAX-2 Array(s)	<p>Select the preferred storage pools to use if you are configuring VMAX V2 Arrays.</p>

Table 12 SQL Server Service Plan details (continued)

Name	Description
Select the cluster and arrays in preferred order for VPLEX metro configuration	Allows you to configure array preference by dragging and dropping the available options in the preferred order.

File system service plan details

Use this table to learn file system service plan details.

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 a Copy step varies among plans. The following table summarizes the service plan details:

This table describes the File System service plan details.

Table 13 File System Service Plan details

Name	Description
Service Plan Name	Type of service plan.
Description	Describes the function of the service plan.
Service Plan State	Specifies if the service plan is enabled or disabled.
Copy Location	Specifies if the location is local, remote, or local and remote.
Mount Copy	Specifies the following options for mounting a copy: <ul style="list-style-type: none"> • No • Yes • Yes - Keep it mounted (Previous copy will be unmounted) • Yes - Mount the copy, but after the post mount scripts run, unmount the copy
Retention	Specifies the configured copy retention number.
Schedule	Specifies the recurrence type that is configured for the service plan.
Advanced plan settings	Specifies if the Enable callout script is enabled or disabled. By default, this option is enabled. Clear Enable CallOut Scripts to disable call out scripts.  Note: For repurposing, if you want to disable callout scripts during refresh, edit the repurpose plan and then clear Enable CallOut Scripts under service plan settings.
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 servers are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount on path	<ul style="list-style-type: none"> • 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 (%).

Table 13 File System Service Plan details (continued)

Name	Description
	<ul style="list-style-type: none"> 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. Select Mapped Path to specify the path where you want to mount the database.
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> 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 V2, 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 V2 and RP XtremIO is not supported.
Use Dedicated Storage Group	<ul style="list-style-type: none"> 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 V2 , VNX storage group, PowerStore host group or XtremIO initiator group for a mount. (A dedicated VMAX V2 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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.

Table 13 File System Service Plan details (continued)

Name	Description
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes. • Enable VMware cluster mount:
Enable VMware cluster mount	<ul style="list-style-type: none"> • Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. • If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMWare SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
VMware Virtual Disk Mode	<p>Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.</p> <ul style="list-style-type: none"> • Enable VMWare Virtual Disk Mode and select Persistent to mount the copy in an independent persistent mode. • Enable VMWare Virtual Disk Mode and select Non Persistent to mount the copy in an independent non persistent mode <p> Note: AppSync does not support:</p> <ul style="list-style-type: none"> • Protection of applications created on independent non persistent virtual disk. • Mounting application copies to a virtual server or shared instance (such as SQL Failover cluster and Oracle RAC) as independent non persistent disk.
Select the cluster/ arrays in preferred order for VPLEX metro configuration	In the Select the cluster and arrays in preferred order for VPLEX metro configuration section, you can drag and drop the arrays to change array preference.
Allow Unmount Of On Demand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.
Pre-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on Production host before creating a copy in AppSync.
Post-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a copy in AppSync.
Post-mount script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after the copy is mounted by the service plan run.

Table 13 File System Service Plan details (continued)

Name	Description
Run Filesystem Check	<p>During a mount operation, the AppSync agent checks file system data consistency by executing the <code>fsck</code> command. This operation can be time consuming. You can clear this option to skip file system check during a mount operation. By default, file system check is enabled.</p> <p>Note: In the case of a restore operation, the <code>Run Filesystem Check</code> option is enabled by default. You cannot disable it.</p>
Copy to mount	<p>Allows user to select if the local or remote copy has to be mounted as part of service plan run.</p> <p>Note: Applies to service plans that create local and remote copies simultaneously.</p>
Create Copy details	
Copy Priority	<ul style="list-style-type: none"> Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. Allows you to order, select, or clear copy priority. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Unix Filesystem Consistency	<ul style="list-style-type: none"> FS Consistent - If you select this option, the file system is frozen during copy creation. This pauses writes on the file system. You can create UNIX file system consistent copies using the UNIX <code>fsfreeze</code> utility. Crash Consistent - This is the default option. In this case, the file system is not frozen during copy creation.
Wait for VMAX3/PowerMAX clone sync to complete	Allows you to specify if AppSync must wait for the clone sync to complete for VMAX3/PowerMAX Arrays.
Select Storage Groups for VMAX-3 Array(s)	Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX arrays.
Select Storage Pools to be used for VMAX-2 Array(s)	Select the preferred storage pools to use if you are configuring VMAX V2 arrays.
VSS Retry Count	Specifies the number of times the VSS retry option is run. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry count.
VSS Retry Interval(In Seconds)	Specifies the timeframe (in seconds) between VSS retries. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry interval.

VMware Datacenter service plan details

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 a Copy step, is different from plan to plan.

This table describes the VMware service plan details.

Table 14 VMware Service Plan details

Name	Description
Service Plan	Type of service plan.
Description	Describes the function of the service plan.
Enabled	Specifies if the service plan is enabled or disabled.
Location	Specifies if the location is local or remote.
Mount copy	Specifies the following options for mounting a copy: <ul style="list-style-type: none"> • No • Yes • Yes - Keep it mounted (Previous copy will be unmounted) • Yes - Mount the copy, but after the post mount scripts run, unmount the copy
Mount on host	Lists all the ESX servers discovered on the registered vCenter servers.
Mount Copy with access	Select the type of access the copy should be mounted with Read-only or Read-Write .
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.
Retention	Specifies the configured copy retention number.
Schedule	Specifies the recurrence type that is configured for the service plan.
Desired SLO	Select the SLO for the mount copy. This is only applicable for VMAX3/PowerMAX arrays.
Configure Quality of Service Options	Select a Quality of Service policy. This is only applicable for XtremIO.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
VPLEX Mount option	Select a VPLEX mount option.
Enable VMware cluster mount	If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMware SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Copy to mount	Allows user to select if the local or remote copy has to be mounted as part of service plan run.  Note: Applies to service plans that create local and remote copies simultaneously.

Table 14 VMware Service Plan details (continued)

Name	Description
Select Storage Groups for VMAX-3 Array(s)	Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX Arrays.
Select Storage Pools to be used for VMAX-2 Array(s)	Select the preferred storage pools to use if you are configuring VMAX V2 Arrays.
Select the cluster and arrays in preferred order for VPLEX metro configuration	Allows you to configure array preference by dragging and dropping the available options in the preferred order
Wait for VMAX3/PowerMAX clone sync to complete	Allows you to specify if AppSync must wait for the clone sync to complete for VMAX3/PowerMAX Arrays.
Copy Priority	<ul style="list-style-type: none"> Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. Allows you to order, select, or clear storage preferences. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Configure VM Snapshots for VMs	Allows you to select virtual machines from the datastores added to the service plan. You can explicitly include or exclude virtual machines in the VMware Snapshot process (all virtual machines are already included by default) This feature is enabled when you select a virtual machine either to include or exclude. When you select a virtual machine to exclude, the selected virtual machine is ignored while taking VMware snapshots during the service plan run. If you select the Include VM or VMs for Snapshot option, only the selected virtual machines are considered for VMware snapshot creation during the service plan run.
Include Virtual Machine Disk	Specifies is this option is enabled or disabled. Includes all the datastores that are associated with the virtual machines running on the datastores being protected. Select this checkbox to protect virtual machine disks spanning multiple data stores. By default, this option is not selected.
Maximum Simultaneous VM Snapshots	Specifies the number of simultaneous snapshots of all VMs present. The default value is four snapshots.

Microsoft Exchange service plan 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 a Copy step, is different from plan to plan.

This table describes the Exchange service plan details.

Table 15 Exchange Service Plan details

Name	Description
Service Plan	Type of service plan.
Description	Describes the function of the service plan.

Table 15 Exchange Service Plan details (continued)

Name	Description
Enabled	Specifies if the service plan is enabled or disabled.
Location	Specifies if the location is local or remote.
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 servers are filtered out.
Mount Copy	<p>Specifies the following options for mounting a copy:</p> <ul style="list-style-type: none"> • No • Yes • Yes - Keep it mounted (Previous copy will be unmounted) • Yes - Mount the copy, but after the post mount scripts run, unmount the copy
Mount with access	Type of access the copy should be mounted with.
Mount on Path	<p> Note: The drive that is specified for mount cannot be a clustered disk.</p> <ul style="list-style-type: none"> • 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. • Select Mapped Path to specify the path where you want to mount the database.
Configure Quality of Service	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Copy metadata files to	Defines the path where metadata files are copied.
Image access mode	<ul style="list-style-type: none"> • 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 V2, 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 V2 and RP XtremIO is not supported.
Copy to mount	<p>Allows user to select if the local or remote copy has to be mounted as part of service plan run.</p> <p> Note: Applies to service plans that create local and remote copies simultaneously.</p>

Table 15 Exchange Service Plan details (continued)

Name	Description
Desired SLO	Select the SLO for the mount copy. This is only applicable for VMAX3/PowerMAX arrays.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Wait for VMAX3/PowerMAX clone sync to complete	Allows you to specify if AppSync must wait for the clone sync to complete for VMAX3/PowerMAX Arrays.
Select Storage Groups for VMAX-3 Array(s)	Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX Arrays.
Select Storage Pools to be used for VMAX-2 Array(s)	Select the preferred storage pools to use if you are configuring VMAX V2 Arrays.
Select the cluster and arrays in preferred order for VPLEX metro configuration	Allows you to configure array preference by dragging and dropping the available options in the preferred order
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes. • Enable VMware cluster mount:
Enable VMware cluster mount	If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMware SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
VMWare Virtual Disk Mode	<p>Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.</p> <ul style="list-style-type: none"> • Enable VMWare Virtual Disk Mode and select Persistent to mount the copy in an independent persistent mode. • Enable VMWare Virtual Disk Mode and select Non Persistent to mount the copy in an independent non persistent mode <p> Note: AppSync does not support:</p> <ul style="list-style-type: none"> • Protection of applications created on independent non persistent virtual disk.

Table 15 Exchange Service Plan details (continued)

Name	Description
	<ul style="list-style-type: none"> Mounting application copies to a virtual server or shared instance (such as SQL Failover cluster and Oracle RAC) as independent non persistent disk.
Validate Copy	Specifies if the Validate Copy option is enabled or disabled.
Retention	Specifies the configured copy retention number.
Schedule	Specifies the recurrence type that is configured for the service plan.
Pre-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on Production host before creating a copy in AppSync.
Post-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a copy in AppSync.
Post-mount script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after the copy is mounted by the service plan run.
Validate copy options	<ul style="list-style-type: none"> Check databases and logs: Select one of the following options. <ul style="list-style-type: none"> Sequentially In parallel Minimize log checking: User defined path can be specified. Throttle the validation: Specify values for the following options. <ul style="list-style-type: none"> Pause after I/O count of Pause duration Skip database validation (.edb file check only for DAG)
Copy Priority	<ul style="list-style-type: none"> Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. Allows you to order, select, or clear storage preferences. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Backup Type	Exchange backup type: Full, Copy, or Differential
Allow databases and logs to reside on the same volume	Specifies if the Allow databases and logs to reside on the same volume option is enabled or disabled.
Fail copy creation if -1018 error (JET Read/Verify Failed) detected	Specifies if the copy creation must fail if this error is detected.
Fail copy creation if -1019 error (JET Page Not Initialized) detected	Specifies if the copy creation must fail if this error is detected.
Fail copy creation if -1022 error (JET Disk I/O Failure) detected	Specifies if the copy creation must fail if this error is detected.

Table 15 Exchange Service Plan details (continued)

Name	Description
Fail copy creation if Event ID 447 detected	Specifies if the copy creation must fail if this error is detected.
Fail copy creation if Event ID 448 detected	Specifies if the copy creation must fail if this error is detected.
VSS Retry Count	Specifies the number of times the VSS retry option is run. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry count.
VSS Retry Interval(In Seconds)	Specifies the timeframe (in seconds) between VSS retries. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry interval.

CHAPTER 5

Protect Microsoft Exchange

This chapter includes the following topics:

- [Overview of Exchange support](#) 94
- [Deploying AppSync for Exchange protection](#)..... 95
- [Protect an Exchange database](#) 97
- [Service plan details](#)..... 100
- [Mounting Exchange copies](#)..... 108
- [Overview of Exchange copy restore](#)..... 113

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 supported Windows host for running consistency check or to back up to long-term storage.
- Support for the Quality of Service feature for XtremIO release 6.2 and later.
- 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®.
- 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/modernHomeDataProtection> 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.

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.
- AppSync supports circular logging for Exchange Databases.

Support for Exchange on Hyper-V

In Hyper-V environments, AppSync requires the storage for Exchange to be on iSCSI direct attached devices, Virtual Fiber Channel (NPIV), or SCSI pass-through devices. SCSI Command Descriptor Block (CDB) filtering must be turned off in the parent partition for SCSI pass-through. It is turned on by default. This is also applicable for databases in DAG configurations.

For Hyper-V SCSI pass-through, the mount host cannot be a Hyper-V host. It has to be a physical host or a virtual machine added with Virtual Fiber Channel adapter or iSCSI direct attached.

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.

Deploying AppSync for Exchange protection

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

Procedure

1. Install the AppSync server.
2. On the AppSync console, select **Settings > Infrastructure Resources > SERVERS / CLUSTERS**.
3. Click **ADD APPLICATION HOST**.
4. Log in to the AppSync console and select **Copy Management**.
5. Click **Select View > Copies**.
6. Click **Select Application > Microsoft Exchange** and click a server name from the list of Exchange standalone and DAG servers.
7. Enter the credentials to configure and run the AppSync Exchange Interface service.
The Exchange databases are discovered.
8. Subscribe an Exchange database for protection by choosing one of the following options:
 - Protect immediately with **Subscribe to Service 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 Service Plan (with option to override)**, which subscribes the database to a service plan, but does not run the plan. Protection occurs according to the service plan's schedule.

Discover Exchange Database

Perform this procedure to discover Microsoft Exchange Databases.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft Exchange**.
4. Under the Name column, click the desired instance.
5. In the Databases page, click **MORE > Discover Databases**.

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. On the AppSync console, select **Settings > Infrastructure Resources**.
2. Click the **SERVERS / CLUSTERS** tab.
3. Select the Exchange mailbox you want to remove and click **Remove**.

Protecting DAG databases in a service plan

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

About this task

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.

Convert a standalone Exchange server to a DAG member

Procedure

1. Remove all the subscriptions and copies of the standalone Exchange server registered with AppSync.

2. Remove the host from the Servers page that was hosting the standalone Exchange server.
3. After the standalone Exchange server is added as a DAG member, add the host back to the AppSync server.

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 Service 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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft Exchange**.
4. In the Name Column, click the desired Exchange instance.
5. Select the desired Exchange database, and click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. From the **Protect** list, select the appropriate service plan from **Subscribe to Service Plan and Run**.

In DAG, a passive database is protected by default.

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

Subscribe an Exchange 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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.

3. From the **Select Application** drop-down, select **Microsoft Exchange**.
4. In the Name Column, click the desired Exchange instance.
5. Click the desired Exchange database, and click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select the appropriate option.

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

8. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold

 **Note:** User defined service plans are also listed.
9. Click **OK**.
10. Click **NEXT** to review your selection.
11. Click **FINISH**.

Unsubscribe Exchange 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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft Exchange**.
4. In the Name Column, click the preferred instance.
5. Select the database you want to unsubscribe, and click **More > UNSUBSCRIBE**.
6. In the Unsubscribe page, select the service plan and click **OK**.

 **Note:** You can also unsubscribe applications from a service plans, from the Service Plan page.

Expire an Exchange copy

You can expire an Exchange copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. In the Name Column, click the database that contains the copy.
6. Select the copy that you want to expire and click **More > EXPIRE**.
7. Click **OK**.

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.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. Select the desired database and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select **Subscribe to Service Plan (with option to override)**.
8. Select the service plan that you want to subscribe to.
9. Click **NEXT**.

The Override Schedule page appears.

10. Select one or more databases and click **OVERRIDE SCHEDULE**.
11. Specify 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 databases.

12. Click **NEXT** to review your selection.
13. Click **FINISH**.

Service plan details

A service plan has the following tabs: Settings, Subscriptions, Copies, and Events.

The **Settings** tab shows the name, description, and status (whether enabled or disabled) of the service plan. Click on the appropriate tabs to see information regarding subscriptions, copies created by the plan, and events generated during the service plan run.

Service plan schedule

The service plan scheduling options determine whether the plan is run manually, or is 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 different times during the day.
 - Minutes after the hour are set in 1 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.
 - Select **Last** to select the last 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
- Always keep *n* Copies
 -  **Note:** Here *n* represents the value that you configure in this field.

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 by overriding the generic recurrence setting.

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. Select the desired database and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select **Subscribe to Service Plan (with option to override)**.
8. Select the service plan that you want to subscribe to.
9. Click **NEXT**.

The Override Schedule page appears.

10. Select one or more databases and click **OVERRIDE SCHEDULE**.
11. Specify 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 databases.

12. Click **NEXT** to review your selection.
13. Click **FINISH**.

Pre-copy script

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters.

For the pre-copy script, the valid script formats are `.bat`, `.ps1`, and `.exe`. You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default. The default location of the script is `%ProgramData%\EMC\AppSync\scripts\` on the application host.

AppSync now supports running of PowerShell scripts. The following points apply:

1. The execution policy on the Windows host is set to either Unrestricted or RemoteSigned.
2. If the script is set to run as a non-Default user, this user must have administrative rights to execute the PowerShell commands in the script.
3. The `.ps1` script will run using system `PowerShell.exe` assuming that the system drive is located on the default `C:\` drive.
4. Currently, parameters such as `$true`, `$false`, output redirect using `|out-file <filename>` are not supported.

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

Create a Copy

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

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

Review [Overview: Service Plan](#) 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 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.

You can configure AppSync to ignore any or all of these errors.

Table 16 Microsoft Exchange event errors

Error	Meaning
-1018	The database tried and failed to verify information about a particular page in the database.

Table 16 Microsoft Exchange event errors (continued)

Error	Meaning
-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.
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.

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.

Configure retry on VSS failure

You can configure a VSS retry count while creating a copy of a service plan. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze/thaw operation again based on the specified retry count and interval. This option is supported only on Windows applications - File system, Microsoft SQL, and Microsoft Exchange. This option is not used while creating Crash consistent copies of SQL databases.

Note: AppSync does not perform a VSS retry, if the application freeze itself fails. If the application is not in a state to create a copy, AppSync fails to quiesce it, and does not retry the VSS freeze/thaw operation. The application must be brought back to a state where it can be quiesced and then the service plan must be re-run.

Post-copy script

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters.

The script runs on successful completion copy creation. Valid script formats are `.bat` and `.exe`. 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 now supports running of PowerShell scripts. The following points apply:

1. The execution policy on the Windows host is set to either Unrestricted or RemoteSigned.
2. If the script is set to run as a non-Default user, this user must have administrative rights to execute the PowerShell commands in the script.
3. The `.ps1` script will run using system `PowerShell.exe` assuming that the system drive is located on the default `C:\` drive.
4. Currently, parameters such as `$true`, `$false`, output redirect using `|out-file <filename>` are not supported.

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.

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

This operation requires the Service Plan Administrator role in AppSync.

Mount copy

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 VMAX3/PowerMAX array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
- **Quality of Service Policy**
You can select the type of Quality of Service policy while mounting a copy. This option is applicable for XtremIO only.
- **Unlink the SnapVX snapshots in unmount**

Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

- **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 VMAX3/PowerMAX array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX3/PowerMAX 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 options, 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** option in the **Details** page in the right pane.

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.

About this task

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

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Microsoft Exchange**.
4. Click a service plan, and expand the right pane.
5. Click the **OVERRIDES** tab.
6. Select **Mount Overrides**.
7. Select an entry, and click **OVERRIDE MOUNT**.
8. Edit the required fields, and click **APPLY CHANGES** to save the settings.
9. To revert back to default settings for a server, select the server and click **Use Default Settings**.

Validate copy

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.

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 Enn` 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.

- **Skip database validation(.edb file check only for DAG)**

If you select this option, AppSync skips database validation in the case of DAG, if it has:

- One active and mounted database copy, and at least one passive and healthy database copy
- Or
- Two passive and healthy database copies

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 run. This script is typically used for backup.

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.

Unmount copy

All the mounted databases are shut down as part of unmount.

This option is disabled if the **Unmount previous copy** option is enabled.

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.
- A single mount host with Exchange 2013 Management Tools can be used to run consistency check for Exchange 2010 and Exchange 2013 copies.

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.

Mount a copy using the Exchange Mount wizard

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. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. In the Name Column, click the database that contains the copy you want to mount.
6. Select the copy you want to mount and click **Mount Copy**.

If multiple databases were protected together, you may see the additional copies to mount option. Select the copies you prefer and click **NEXT**.

7. In the Select Mount Options page, under **General Settings**, do the following:
 - a. From the **Mount on Server** list, select the server on which to mount the copy.
 - b. From the **Mount with access** list, select the type of access the copy must be mounted with: **Read-only** or **Read-write**.
 - c. From the **Mount Location** list, select a mount path location either to **Default path**, **Same as original path**, or **Mapped Path**. 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.
 - d. For the **Copy metadata files to** option, specify a path. By default the path is `SystemDrive\AppData\Mounts\ProdServerName\`.
 - e. In case the selected copy is a RecoverPoint bookmark, from the **Image access mode** list, select one of the following 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 V2X, 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 V2 and RP XtremIO is not supported.
 - f. Expand **XtremIO QOS** and select the desired Quality of Service policy from the list. This option is only applicable to XtremIO 6.2 or later.
 - g. For VMAX3/PowerMAX arrays, from the **Desired SLO** list, select the desired Service Level Objective (SLO) for the mount copy.

 **Note:** The SLO values are dynamically fetched from the VMAX3/PowerMAX arrays, and only the unique values are displayed.
 - h. For XtremIO 6.2 and later, click the **Quality of Service policy** option to select the desired Quality of Service policy while mounting a copy.
 - i. For VMAX3/PowerMAX SnapVxSnap, select the **Unlink the SnapVX snapshots in unmount** option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
 - j. For VMAX V2 arrays, select the desired FAST policy for the mount copy.
 - k. Clear the **Use Dedicated Storage Group** option, if you do not want AppSync to enforce the use of a dedicated storage group for a mount. By default, this option is enabled.
 - l. From the **VMware Settings**, configure the following:
 - **Enable VMware cluster mount:** Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled.
 - **Disable VMware SRM:** This option is applicable only for RP 4.1 and above.
 - **VMware Virtual Disk Mode:** Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.

8. Click **Next** to review the mount options.
9. Click **Finish**.

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 Dell 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.)

Skip database validation(.edb file check only for DAG)

If you select this option, AppSync skips database validation in the case of DAG.

Unmount an Exchange copy from the Copies page

You can unmount a copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the desired instance.

5. In the Name Column, click the database that contains the copy you want to unmount.
6. Select the copy you want to unmount and click **UNMOUNT**.
7. Click **OK**.

Unmount an Exchange copy from the Service Plan page

You can unmount an Exchange copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Microsoft Exchange**.
4. Click the name of the service plan you prefer in the Service Plan column.
5. Select the copy you want to unmount and then click **Unmount**.
6. Click **OK**.

Enable or disable an Exchange copy

You can enable or disable expiry of a copy during rotation using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. Click the name of a database to go to the copies page.
6. Select the copy that you want to enable or disable and click **More**.
7. Click one of the following options depending on the action you want to perform:
 - **Enable Copy Rotation:** To enable automatic expiry of a copy during rotation.
 - **Disable Copy Rotation:** To disable automatic expiry of a copy during rotation.
8. Click **OK**.

Expire an Exchange copy

You can expire an Exchange copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the desired instance.
5. In the Name Column, click the database that contains the copy.
6. Select the copy that you want to expire and click **More > EXPIRE**.

7. Click **OK**.

Path mapping

The path mapping option mounts the copy to a host using a path mapping table set to user-defined locations. When you use a path mapping table, you have more control over where data is located.

You must specify the path where you want to mount a specific file system. You must provide a path map where the source file system and the target mount point is specified.

The following is a sample path mapping table for Windows.

The first two target paths, G:\ and H:\ drives must already be available on the mount host. That is, the root drive for the mount path must pre-exist before attempting a mount.

Source file system	Target mount path
D:\Test1	G:\Test1
E:\	H:\Test2
F:\Test3	I:\
L:\	N:\

Note:

- If a target path is not provided for a source path, then it is mounted to a path same as the source path on the mount host.
- Ensure that you type in the absolute mount path on the target host. If the path is invalid, mount fails.
- Mount copy overrides is unavailable, if you select the mount path as Mapped path.
- For Windows, if one of the entered path is invalid, VSS import fails. Therefore, the entire mount fails. Partial failed scenarios are not supported for Windows mount.
- For Windows and NFS file systems on Unix, nested target mount points are not supported.
- Path Mapping is not applicable to metadata paths for Microsoft Exchange and Microsoft SQL Server.

Specify path mapping settings

You can specify the path where you want to mount a specific copy.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange**.
4. Navigate to the folder that contains the copies.
5. Select the copy you want to mount, then click **MOUNT COPY**.
6. In the **Mount Copy** options, under the **Specify Mount Settings** section:
 - a. Select the mount host.
 - b. From the **Mount on Path** list, select **Mapped Path**.

The Path Mapping Settings link appears.

7. Click on the link to open the Path Mapping Settings window.

8. From the **Select Source Host** list, select a host.

All the file systems on the selected host are displayed in the source path column.

9. Specify the target path.
10. Click **Save** to save your settings.

If you want to set the target path for a file system on another source host, repeat steps 8 to 10.

11. Click **Reset**, to clear all the entered target paths for the selected source host.
12. Click **OK** to exit the Path Mapping window.

Note: If you change the path mapping settings, the earlier saved path mapping settings is not valid and the new path mapping settings takes precedence. Therefore, ensure that you save the path mapping settings for all the hosts before changing it.

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 V2, or VMAX3/PowerMAX copies at the LUN level, Unity copies at the consistency group level, and PowerStore copies at the Volume Group level. In a RecoverPoint environment, restore is at the consistency group level.

Note: Ensure that no virtual machine snapshots are present before protecting a datastore. If virtual machine snapshots are present, protection succeeds, but AppSync fails to perform a file or virtual machine restore.

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 Unity, if the databases are in the same consistency group, they become affected entities when another database in the group is protected.
- For VMAX V2, VNX, Unity, PowerStore, 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.
- For PowerStore, while restoring from remote copy, if the databases are in the same volume group and the replication session is created for volume group, they become *affected entities* when another database in the group is protected.

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.

Restore an Exchange copy

You can perform a restore of an Exchange server copy using the Appsync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft Exchange**.
4. In the Name Column, click the instance that contains the database.
5. In the Name Column, click the database that contains the copy you want to restore.
6. Select the copy you want to restore and click **More > Restore**.
7. In the **Select a Copy** page, select the copy you want to restore and click **NEXT**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

 **Note:** You can perform this step only if you have multiple applications that share the same LUN or file systems.

8. Click **NEXT**.
9. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.

- **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.

Note: In the case of SnapVX/XtremIO Snap/PowerStore Snap mounted copies, when you perform restore, AppSync restores the data from the snapshots created on the array to the source devices, or from linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

- **Restore from snapshot:** Restores copies from original snapshots.
- **Restore from changed data:** Restores from the linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

10. Click **NEXT**.
11. In the **Review** page, review the restore options and click **FINISH**.

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.

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 V2, VMAX3/PowerMAX, or 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 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.

About this task

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.

CHAPTER 6

Protect SQL Server

This chapter includes the following topics:

• Overview of SQL Server support	120
• Support for AlwaysOn Availability Groups	125
• SQL Server transaction log backup	125
• Considerations for working with SQL Server in a cluster	130
• SQL Server User Databases folder	131
• Protect a SQL Database	132
• Mount considerations for SQL Server	149
• Unmount a SQL copy from the Copies page	157
• Unmount a SQL copy from the Service Plan page	157
• Create SQL repurpose copies	157
• Create second generation copies	159
• Enable or disable a SQL copy expiry	160
• Expire a SQL copy	160
• SQL Server database restore overview	161

Overview of SQL Server support

Use AppSync to create and manage application-consistent or crash-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 an alternate clustered instance belonging to an alternate or production failover cluster.
- 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/modernHomeDataProtection> 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.
- When mounting with recovery to an alternate clustered instance, you must add all the owner nodes of the SQL Server clustered instance to AppSync.
- When restoring SQL Server clustered databases, you must add all the owner nodes of the SQL Server clustered instance to AppSync.
- In Hyper-V environments, AppSync requires the storage for SQL database and log files to be on iSCSI direct attached devices, Virtual Fiber Channel (NPIV), or SCSI pass-through devices. SCSI Command Descriptor Block (CDB) filtering must be turned off in the parent partition for SCSI pass-through. It is turned on by default. This is also applicable for SQL cluster servers.
 - For Hyper-V SCSI pass-through, the mount host cannot be a Hyper-V host. It has to be a physical host or a virtual machine added with Virtual Fiber Channel adapter or iSCSI direct attached.
- 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.

- Protection of Transparent Data Encryption (TDE) enabled databases is not supported.

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.

Considerations for SQL Server in a VMware environment

You can protect, mount and restore SQL Server standalone and clustered databases residing on VMware virtual disks (VDisks) or raw device mappings (RDMs).

During protection of SQL on RDM or VDisks:

- 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.
 - If multiple SQL databases from different virtual machines on the same datastore are subscribed to the same service plan, protection works, but multiple copies of the same datastore are created. This causes issues during mount and restore operations.
 - If multiple SQL databases from different virtual machines on the same datastore are subscribed to a different service plan, protection, mount, and restore works. However, restore causes problems for databases in other virtual machines that are hosted on the same datastore. It is recommended that multiple SQL databases on different virtual machines be hosted on different datastores.
- Multiple SQL databases from the same host can reside on the same or different virtual disk that are on the same VMFS datastore, and protected by the same service plan. However, restore of one database on this VMFS datastore restores other databases on the same datastore, which are listed as affected entities during restore.
- When restoring SQL Server clustered databases, you must add all the owner nodes of the SQL Server clustered instance to AppSync.
- If the mount host is a virtual machine, the Virtual Center must be registered with AppSync. This is required to mount RDMs.
- For virtual disks:
 - 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 the relevant VMware Knowledge Base article. For Hyper-V SCSI pass-through, the mount host cannot be a Hyper-V host. It must be a physical host or virtual machine with NPIV or iSCSI direct attached.
- If databases reside on raw device mappings in VMWare environments, the SQL Server cluster nodes must reside across different ESXi. This is a requirement from VMWare. For database on virtual disks, SQL Server cluster nodes can reside on the same ESX server.

- AppSync only supports RDMs in physical compatibility mode. There is no support for RDMs in virtual compatibility mode.
- For VMware virtual disks, restore of all applications residing on the same datastore (virtual disks on the same datastore) are also affected entities because restore involves a datastore.

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 (that has log on locally rights) or a non-Administrator account with the restrictions outlined next. The SQL Server services must be restarted after performing these changes. AppSync does not support SQL, if the SQL Service is running as a Service Account.

For setting up SQL Server with AppSync, there are 2 types of users that are required for different purposes:

1. First user is used to run "SQL Server" and "Sql Server Agent" service. The SQL Server service and SQL Server Agent service can be run as Local System or Local Administrator or default service accounts or a domain user. It is recommended that the 2 SQL services - "SQL Server" and "SQL Server Agent" service to have same user for "Log on As" on both the source instance and mount instance.

For setting up SQL services to be run using domain user, the following privileges must be granted to the user through group policy management editor from domain controller or through local security policy editor on the domain computers - Log on as a service (SeServiceLogonRight), Replace a process-level token (SeAssignPrimaryTokenPrivilege), Bypass traverse checking (SeChangeNotifyPrivilege), Adjust memory quotas for a process (SeIncreaseQuotaPrivilege). These privileges are automatically granted during SQL server setup installation.

Also, domain user must be given full file system permissions on source database file system. There are many ways to give permissions. One of the easiest ways is given below:

- a. Using Windows Explorer, navigate to the file system location where the database files are stored. Right-click the file system or folder, and then click Properties.
 - b. On the "Security tab", click Edit, and then Add.
 - c. In the "Select Users, Computer, Service Account, or Groups" dialog box, click Locations, at the top of the location list, select your computer or domain name, and then click OK.
 - d. In the "Enter the object names to select" box, type the username.
 - e. Click "Check Names" to validate the entry. Click OK again to return to the Permissions dialog box.
 - f. In the Group or user names box, select the per-service SID name, and then in the Permissions for <name> box, select the Allow check box for "Full control". Click Apply, and then click OK twice to exit.
2. Second user is used to login to SQL instance. This is the username that is required by AppSync for performing sql operations. It is recommended not to provide default service accounts for use with AppSync. If a domain user is provided here, then it should have below privileges or permissions:

"Allow log on locally" through group policy management editor from domain controller or through local security policy editor on domain computers as explained below. Also, the domain user should be given "public" and "sysadmin" as Server Roles in both source and mount SQL instance.

An AppSync user may configure same domain user to perform both the above purposes. However, if there are different users running SQL Services at mount and source host, then please follow below guidelines:

- a. Recovery of SQL databases will not work for domain user if using cross-domain mount and recovery, that is source instance and mount instances are in two different domains.
- b. The "mount host" domain user used for running SQL services for mount instances must be given these privileges on mount instance.
Log on as a service (SeServiceLogonRight), Replace a process-level token (SeAssignPrimaryTokenPrivilege), Bypass traverse checking (SeChangeNotifyPrivilege), Adjust memory quotas for a process (SeIncreaseQuotaPrivilege). Also, this domain user must have full file system permissions on source database files.
- c. If there is different domain user provided to AppSync for mount instance, then it must have below permissions on source database:
 - Using SQL Studio and connecting to the Source host Database
Add the user the SQL Service and SQL Agent run as on the Mount host.
 - In properties for the user(right click user, select properties), check off public and sysadmin for Server Roles.
 - In properties for the user(right click user, select properties), check off public for User Mappings.
 - Also, this domain user must have full file system permissions on source database files.

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.

Set up SQL Server connection settings

Perform this procedure to set up the SQL Server connection settings.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the instance page.
4. Select a database and click **CONNECTION SETTINGS**.
The SQL Server Connection settings dialog appears.
5. In the `Authentication` field, select one of the following:
 - Windows Authentication
 - SQL Server Authentication
6. Specify values for the following fields:
 - Username
 - Password
7. Click **OK**.

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** step 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](#).
- 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 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 Dell 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.

 **Note:** AppSync supports UNC path of a network share only if both the machines are in the same domain.

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.

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.

About this task

To configure SQL server transaction log backup, edit the respective service plan and enable the **Enable log backup** option in the Create the Copy step. Then, 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.

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.

Create log backup for SQL

You can create log backups for SQL Servers in the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance.
5. In the user database folder, click the preferred server folder.
6. In the Name Column, click the preferred database and then click the **Log Backups** tab.
7. Click **Create Log Backup Using Plan**.
8. In the Create Log Backup page, select the service plan, and Click **OK**.

 **Note:** The Enable log backup option should be enabled in the service plan.

The Subscribe to Plan Status window displays the status of the job.

9. Click **Close**.

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.

Run Log Backups for a SQL database

Perform the following procedure to run log backups for a SQL database.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the instances page.
4. Select the service plan for which you want to run log backup and click **RUN LOG BACKUPS**.

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.

About this task

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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server**.
4. Click the name of a service plan.
5. 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 17 Service Plan log backup details

Column	Description
Status	<ul style="list-style-type: none"> • Green: successful • Yellow: some log backups completed with errors when the service plan ran. • Red: failed
Log Backup Name	Name of the log backup copy. The copy is named with the time at which it was made.
Instance	SQL Server instance name
Database	SQL Server database name
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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server**.
4. Click the name of a service plan.
5. Click the **LOG BACKUPS** tab.

6. Select the log backups that you would like to expire and then click **EXPIRE**.
7. 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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, and select the desired application.
4. Navigate to the Databases page.
5. Click on a database in the list and select the **LOG BACKUPS** tab.
6. Select the log backups that you would like to expire and then click **EXPIRE**.
7. 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 clustered SQL Server instance. You can use the AppSync console to install the plug-in or manually install the plug-in on each server.

Note: In a Windows cluster environment, AppSync agent port must be the same across all the nodes participating in the cluster. Otherwise, AppSync operations fail.

Protecting clustered SQL Server instances:

- It is mandatory to add all the possible nodes of a clustered SQL Server instance and then add SQL Server virtual server (network name or IP address) to AppSync after installing the AppSync host plug-in software on each node.
 - Note:** The SQL Server virtual server is different from the failover cluster name.
- Only single subnets are supported.
- Production VMWare virtual disk with multi writer option enabled is supported for SQL server failover cluster
- Mounting AppSync copies as a standalone resource:
 - You can mount AppSync copies of clustered databases as a standalone database to a standalone server or any cluster node.
 - You can mount AppSync copies of standalone databases as a standalone database to a standalone server or any cluster node.

Mounting a SQL Server copy as a clustered resource:

- Supports mount to either an alternate cluster or a production cluster as a clustered resource. On the production cluster, you must select an alternate clustered instance for mount with recovery.
- Mount is supported in the environments of VMAX V2, VMAX3/PowerMAX, VNX, Unity, PowerStore, 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.
- Virtual servers are filtered out while using the "mount copy" to server option. Only cluster nodes or standalone servers are visible.
- Mount with Recovery as a clustered resource to a clustered production server is supported.
- For Mount with Recovery as a clustered resource to a production virtual server, consider the following:
 - Mounting to a different clustered SQL server instance is supported.
 - Mounting to a production clustered SQL server instance is not supported.
 - Mounting to an alternate mount path is supported. The root disk for the alternate mount point must be a clustered disk, and must be added as a dependency to SQL server.
 - Mounting to the original path is not supported.
- Performing a RecoverPoint mounted restore while the copy is mounted to a production cluster is not supported.

 **Note:** When AppSync mounts and recovers clustered SQL databases, AppSync stops and starts the SQL instance on the mount host. This is an expected behavior.

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.

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.

Discover SQL Server databases

Perform this procedure to update the SQL Server databases that are known to AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the databases page.
4. Click **DISCOVER INSTANCES**.
5. In the Discover Microsoft SQL Server instance dialog, select a host and click **OK**.

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), modify the **Maximum number of Databases** value under the **Service Plan > Define the Copy** options, accordingly.

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

- Choose an appropriate service plan from **CREATE COPY WITH PLAN** in the database Copies page.
 - 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 Service Plan** (with option to override schedule selected), 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 **RUN** from the SQL Server Service Plans page to run the whole plan immediately.

 **Note:** Ensure that the database you are protecting is not configured for backup at the same time using a non-AppSync backup tool. This might interfere with AppSync copy operation and result in unexpected errors.

Subscribe a SQL 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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.

3. From the **Select Application** drop-down, select **Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the user databases folder, select one or more SQL databases, and then click **CREATE COPY WITH PLAN**.
7. Select the purpose as **Data Protection**.
8. Select the appropriate option.

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

9. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold

 **Note:** User defined service plans are also listed.
10. Click **OK**.
11. Click **NEXT** to review your selection.
12. Click **FINISH**.

Create a SQL database copy

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

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display SQL instances page.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User databases folder.
6. Select one or more SQL databases, and then click **CREATE COPY WITH PLAN**.
7. Select the purpose as **Data Protection**.
8. Select the appropriate option.

Option	Description
Subscribe to Service Plan and Run	To subscribe the database for protection and run the plan immediately for any selected databases.
Subscribe to Service Plan (with option to override)	To subscribe the database for protection. Protection for all databases that are part of the service plan is run at the scheduled time.

9. Click **Select** and select the service plan that you want to subscribe to from the following options:

- Bronze
- Silver
- Gold

 **Note:** User defined service plans are also appear in this list.

10. Click **OK**.

11. Click **NEXT** to review your selection.

12. Click **FINISH**.

Microsoft SQL Server copies list

The list contains SQL Server copies that have been discovered and stored in the AppSync database.

Clicking on a database name shows the AppSync copies of the database.

Each entry shows the subscribed service plans, mount status, Backup type, protected server information, site, and copy type details.

Column	Description
Status	Green: successful Yellow: Completed with errors Red: failed
Service Plan	Name of the service plan that is associated with the copy. For repurposed copies, a Repurpose link displays in this column. Click this link to edit the Service Plan for 1st or 2nd generation copies.  Note: In the service plan for repurposed copies, the options to schedule and mount overrides will be disabled.
Backup Type	Describes the type of backup.
Mount Status	Hostname to which the copy is mounted, or Not Mounted
Mount Type	If copy is mounted as part of service plan run, value for Mount Type is ServicePlan. If copy is mounted as OnDemand, value for Mount Type is OnDemand.

Column	Description
Copy Type	<p>Replication technology that is used to create the copy: CLR Bookmark, CDP Bookmark, CRR Bookmark, VNXSnap, VPSnap, TFClone, XtremIO Snapshot, DellSCSnap, and VPLEXSnap.</p> <p>The copy can be one of the following types:</p> <ul style="list-style-type: none"> RecoverPoint Continuous Data Protection Bookmark RecoverPoint Continuous Remote Replication Bookmark Unity Snap VMAX V2 Snap, VMAX V2 Clone XtremIO snapshot VMAX3/PowerMAX SnapVXClone, SnapVXSnap VPLEX Snap, VPLEX Clone DELLSC Snap PowerStore Snapshot PowerStore Thin Clone
Site	Site where the copy is located.
<i>The following additional details are displayed in the Service Plan Copies tab:</i>	
Source	This column displays the source database or copy from which a copy was created.
Automatic Expiration	Determines whether automatic expiration is enabled or disabled for the selected copy.
Generation	Used for repurposed copies, this column describes how many generations the copy is from the production database.
Label	1st or 2nd generation copy label
Storage system	Storage array on which the copy is created.

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. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Microsoft SQL Server** to display the databases page.

4. In the Name Column, click the server instance that contains the database.
5. In the user database page, click the user database that contains the database.
6. In the Name Column, click the database you want to protect.
7. Select the database you want to unsubscribe, and click **UNSUBSCRIBE**.
8. In the Unsubscribe dialog, select the service plan and click **OK**.

 **Note:** You can also unsubscribe applications from a service plans, from the Service Plan page.

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.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the user databases folder, select one or more SQL databases, and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select **Subscribe to Service Plan (with option to override)**.
8. Select the service plan that you want to subscribe to.
9. Click **NEXT**.

The Override Schedule page appears.

10. Select one or more databases and click **OVERRIDE SCHEDULE**.
11. Specify 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 instances.

12. Click **NEXT** to review your selection.
13. Click **FINISH**.

View SQL database copies

View the list of database copies by navigating 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.

About this task

You can also 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. In the Service Plan Copies tab, you can also filter by instance.

Table 18 Service Plan Copy details

Column	Description
Status	<ul style="list-style-type: none"> 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 associated with the copy. Service plan field will be blank for Repurpose copies.
SQL Server Backup Type	<p>Type of SQL backup: Full or Copy</p> <ul style="list-style-type: none"> 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	Whether the copy is mounted or not. If mounted, displays the name of the mount host.
Recovery Status	<p>Available values:</p> <ul style="list-style-type: none"> Not Recovered - when copy is not mounted or it is a filesystem 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	<p>Type of copy can be one of the following:</p> <ul style="list-style-type: none"> CDP Bookmark CRR Bookmark VNX Snap

Table 18 Service Plan Copy details (continued)

Column	Description
	<ul style="list-style-type: none"> • VNXeSnap • VNXe FileSnap • VMAX Snap, VMAX Clone • XtremIO Snapshot • VPLEX Snap
The following additional details are displayed in the Service Plan Copies tab:	
Instance	The SQL Server instance that hosts the database.
Database	The name of the copy's database.
Name	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 and VNX file site information.

 **Note:** A **Repurpose** button on this page is enabled. When you select a **1st Generation copy** and then click this button, the Repurpose wizard is launched 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.

About this task

Follow these steps:

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, and select the desired application.
4. Navigate to the Databases page.
5. Click on a database and select the **LOG BACKUPS** tab.

Results

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

Table 19 Database log backup details: SQL Server instance

Column	Description
Status	<ul style="list-style-type: none"> • Green: successful • Yellow: some log backups completed with errors when the service plan ran. • Red: failed

Table 19 Database log backup details: SQL Server instance (continued)

Column	Description
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.

Expire a SQL copy

You can expire a SQL copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the Name Column, click the database that contains the copy.
7. Select the copy that you want to expire and click **More > Expire**.
8. Click **OK**.

Service plan summary and details

The service plan **Settings** tab shows the name, description, schedule, and status of the service plan. Click the tabs in the **Details** pane on the right for information about subscriptions and events generated by the plan.

Service plan schedule

The service plan scheduling options determine whether the plan is run manually, or is 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 different times during the day.
 - Minutes after the hour are set in 1 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.
 - Select **Last** to select the last 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.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the user databases folder, select one or more SQL databases, and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select **Subscribe to Service Plan (with option to override)**.
8. Select the service plan that you want to subscribe to.
9. Click **NEXT**.

The Override Schedule page appears.

10. Select one or more databases and click **OVERRIDE SCHEDULE**.
11. Specify 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 instances.

12. Click **NEXT** to review your selection.
13. Click **FINISH**.

Pre-copy script

To perform preparatory steps before creating a copy, specify a pre-copy script and parameters.

For the pre-copy script, the valid script formats are `.bat`, `.ps1`, and `.exe`. You can optionally enter credentials to run the script as a specific user. The script runs as Local System by default.

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

AppSync now supports running of PowerShell scripts. The following points apply:

1. The execution policy on the Windows host is set to either `Unrestricted` or `RemoteSigned`.
2. If the script is set to run as a non-Default user, this user must have administrative rights to execute the PowerShell commands in the script.
3. The `.ps1` script will run using system `PowerShell.exe` assuming that the system drive is located on the default `C:\` drive.
4. Currently, parameters such as `$true`, `$false`, output redirect using `|out-file <filename>` are not supported.

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

Create copy

The **Create a Copy** options specify the criteria to a copy based on the replication technology specified in the service plan.

For VNX Snapshot copies, you can also set the period for automatic expiration of the copies during copy creation.

Review [Overview: Service Plan](#) for more service plan copy information.

SQL Server backup type

The four main backup types supported are: Full, Copy, Non VDI, and Crash Consistent.

- **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.
- **Non VDI** protects the database with the non VDI approach. This creates crash consistent copies of SQL using the VSS freeze/thaw framework. No VDI meta data is generated for non VDI copies. You can mount Non VDI SQL copies using the Attach Database and Mount Copy options. You can restore a Non VDI copy using the No Recovery mode.
- **Crash Consistent** protects the database without any agent involvement, that is, VSS or VDI are not used. This backup type creates crash consistent copies of SQL databases using array level features. You can use this backup type to re-snap, if the copy recovery fails. This eliminates intervention on the production side. There is no VSS and VDI metadata generated for Crash Consistent copies. Crash Consistent SQL copies are mounted using VDS mount and

are recovered with the `Attach Database` recovery option. You can restore a Crash Consistent copy using the `No Recovery` mode. Crash Consistent backup type is supported on all supported arrays and RecoverPoint with the following restrictions:

- For VNX and Unity, the SQL database must reside on the LUNs that are in a consistency group.
- For PowerStore, the SQL database must reside on the volumes that are in a write-order-consistent Volume group.
- For VPLEX virtual volumes on Unity, the SQL database must reside on the Unity LUNS that are in a consistency group.
- For VPLEX virtual volumes on PowerStore, the SQL database must reside on the PowerStore volumes that are in a write-order-consistent Volume group.
- There is no restriction for VMAX V2, VMAX3/PowerMAX, RecoverPoint, XtremIO, and VPLEX virtual volumes on XtremIO.
- RecoverPoint bookmarks shows Snap consistency as **Crash Consistent** in the RecoverPoint GUI.

Automatic expiration of copies

The automatic expiration value 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.

Configure retry on VSS failure

You can configure a VSS retry count while creating a copy of a service plan. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze/thaw operation again based on the specified retry count and interval. This option is supported only on Windows applications - File system, Microsoft SQL, and Microsoft Exchange. This option is not used while creating Crash consistent copies of SQL databases.

 **Note:** AppSync does not perform a VSS retry, if the application freeze itself fails. If the application is not in a state to create a copy, AppSync fails to quiesce it, and does not retry the VSS freeze/thaw operation. The application must be brought back to a state where it can be quiesced and then the service plan must be re-run.

Post-copy script

To perform cleanup or other post-copy steps after creating a copy, specify a post-copy script and parameters.

The script runs on successful completion copy creation. Valid script formats are `.bat` and `.exe`. 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 now supports running of PowerShell scripts. The following points apply:

1. The execution policy on the Windows host is set to either Unrestricted or RemoteSigned.
2. If the script is set to run as a non-Default user, this user must have administrative rights to execute the PowerShell commands in the script.
3. The `.ps1` script will run using system `PowerShell.exe` assuming that the system drive is located on the default `C:\` drive.
4. Currently, parameters such as `$true`, `$false`, output redirect using `|out-file <filename>` are not supported.

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.

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

This operation requires the Service Plan Administrator role in AppSync.

Mount copy

The Mount copy step either mounts the copy, or mounts and recovers the copy.

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 servers are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount on path	<ul style="list-style-type: none"> 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. Select Mapped Path to specify the path where you want to mount the database.
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Copy metadata files to	<ul style="list-style-type: none"> 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. <p>Note:</p> <ul style="list-style-type: none"> Metadata is not created for Non VDI copies. VSS or VDI metadata is not generated for Crash Consistent copies.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> 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

Field	Description
	<p>transparently switches to direct replica volume access, allowing heavy processing. With RP VMAX V2, and RP XtremIO, virtual access with roll is not supported.</p> <ul style="list-style-type: none"> • Virtual access: Provides nearly instant access to the image. Virtual access is not intended for heavy processing. Virtual access with RP VMAX V2 and RP XtremIO is not supported.
Desired SLO	<p>For VMAX3/PowerMAX arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.</p>
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes. • Enable VMware cluster mount:
Use Dedicated Storage Group	<ul style="list-style-type: none"> • 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 V2, VMAX3/PowerMAX, VNX storage group, PowerStore host group, or XtremIO initiator group for a mount. (A dedicated VMAX V2 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. <ul style="list-style-type: none"> ⓘ 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. <ul style="list-style-type: none"> ⓘ 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.
Enable VMware cluster mount	<ul style="list-style-type: none"> • Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. • If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage

Field	Description
	system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMWare SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
VMware Virtual Disk Mode	Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Allow Unmount Of OnDemand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.

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. If you are using a VMAX3/PowerMAX array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group
Recovery Type	Available options are: Recovery (default), No Recovery, Standby, and Attach Database
Database renaming	This drop down includes: <ul style="list-style-type: none"> • 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 <code>AppSync</code> .
Mount path	<ul style="list-style-type: none"> • The default mount path, when the mount SQL instance is a standalone instance (<code>%SystemDrive%\AppSyncMounts\%%ProdServerName%</code>). • 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.

Field	Description
	<ul style="list-style-type: none"> If you specify a non-default mount path for mounting to a standalone instance, the drive specified for mount cannot be a clustered disk. For mounting to a clustered SQL instance, the “Same as Original Path” and alternate mount paths are supported. “Default mount path” is not supported. Instead, you can type this option to specify an alternate mount path. The root disk for the alternate mount path must be clustered and a dependency must exist for SQL server on the clustered disk.
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Copy metadata files to	<ul style="list-style-type: none"> 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. <p>Note:</p> <ul style="list-style-type: none"> Metadata is not created for Non VDI copies. VSS or VDI metadata is not generated for Crash Consistent copies.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 V2, VMAX3/PowerMAX, PowerStore host group, 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. <p>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</p>

Field	Description
	<p>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.</p> <ul style="list-style-type: none"> 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. <p>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.</p>
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

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. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Microsoft SQL Server**.
4. Select a service plan and on the right pane, select **Overrides > Mount Overrides**.

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.

5. Select the Server whose settings you want to override and click **OVERRIDE MOUNT**.

The **Override Default Mount Settings** dialog is displayed.

6. Select options only for those mount settings that you wish to override.

Fields that do not have a selection retain their default settings.

7. Click **OK**.

Note: The **OVERRIDE** text appears in the last column of the row for which the default settings are being overridden.

8. To revert back to default settings for a server, click **SET TO DEFAULT**.

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 run. This script is typically used for backup.

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.

Unmount copy

The unmount copy option in the service plan unmounts the copy. This option is disabled if the **Unmount previous copy** option is enabled.

If you choose to mount and recover the copy in the **Mount copy** options, all the mounted databases are shut down during unmount.

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

This section describes the 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.

Note:

- When you mount a replica of a SQL Server database to the production server, do not mount it using the same instance of SQL Server that the production database is using. You must use a different instance of SQL Server.
- The mount path must not exceed 32,767 characters in length.

- During a mount operation, do not use the MS SQL root directory as the mount path. If you select the root path, mount succeeds, but unmount fails with the following error:

```
ERROR_DEPENDENT_RESOURCE_EXISTS
5001 (0x1389)
The operation cannot be completed because other resources are dependent on this
resource.
```

- Appsync supports the Quality of Service feature for XtremIO release 6.2 and later.

Mount and production host versions

- If you are mounting to the node of Windows failover cluster, please see the section [Microsoft Cluster Server mounts for SQL Server](#).
- 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.
- If an AppSync created SQL database copy is recovered on a higher version of SQL Server instance on the mount host, recovery of the same copy on a lower version of SQL Server instance fails.

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 Cluster as a clustered resource

[Considerations for working with SQL Server in a cluster](#) provides information on adding and discovering clustered resources.

- To mount a copy from a production cluster to an alternate cluster as a clustered resource, you must select a clustered SQL server instance of the alternate cluster on the **Mount with recovery** page. Mount as a clustered resource to any other clustered instance on the production cluster is supported. Mount as a clustered resource to the production cluster instance is not supported.
- Mount as a clustered resource is supported for SQL Server databases that reside on paths starting with drive letters such as P:\mysqldb\ or Q:\mysqldb. Mount as a clustered resource is not supported if production databases reside on clustered mount points such as I:\mount_point\, where I: is a clustered drive and another drive is mounted at I:\mount_point\.

- Mount to Same as Original Path is supported.
- Mount to an alternate path on the mount host is supported. You must specify the alternate mount path in the Mount path options. The root disk for the alternate mount point must be a clustered disk and SQL Server must have a dependency on the clustered disk.
- Multiple copies of the same database can be mounted to an alternate cluster at the same time.
- All recovery types are supported.
- Repurposing is supported.
- Databases can reside on any storage supported by AppSync.
- If databases reside on raw device mappings in VMWare environments, the SQL Server cluster nodes must reside across different ESXi. This is a requirement from VMWare. For database on virtual disks, SQL Server cluster nodes can reside on the same ESX server.
- Raw device mapping in virtual compatibility mode is not supported.
- Static mounts are supported for RecoverPoint.

Mount a copy using the SQL Mount wizard

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

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the user databases folder, click the database that contains the copy you want to mount.
6. Select the copy you want to mount and click **MOUNT**.

If multiple databases were protected together, you may see the additional copies to mount option. Select the copies you prefer and click **NEXT**.

7. In the Select a Copy page, select a copy and click **NEXT**.
8. In the Select Mount Options page, select one of the following options:
 - Mount copy
 - Mount and recover copy
9. In the **General Settings** section, configure the following to mount the copy:
 - a. From the **Mount on Server** list, select the server on which to mount the copy.
 - b. From the **Mount with access** list, select the access permission to **read-write** or **read-only**.
 - c. From the **Mount on Path** list, select a mount path location either to **Default path**, **Same as original path**, or **Mapped Path**. The mount path is the location where the copy is mounted on the mount host.
 - d. From the **Copy metadata files to** list, select **Default path**.
10. Under **Storage Settings**, do the following:
 - a. For VMAX3/PowerMAX arrays, select the Service Level Objective (SLO) for the mount copy.

- b. For VMAX V2 arrays, select the desired FAST Policy. Each FAST Policy is associated with a storage group on the array. Select the storage group to use for the mount operation by selecting the FAST policy associated with that storage group.
 - c. For XtremIO 6.2 and later, click the **Quality of Service policy** option to select the desired Quality of Service policy while mounting a copy.
 - d. **VMware Virtual Disk Mode** - Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
11. Under **VMware Settings**, do the following:
 - a. **Enable VMware cluster mount** checkbox - If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. Then the target LUN is made visible only to the ESX cluster on which the mount host resides. This is applicable for both RDM and vDisk device types.
 - b. **VMware Virtual Disk Mode** - Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
 12. Click **NEXT** to review the mount options.
 13. Click **FINISH**.

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 servers are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount on path	<ul style="list-style-type: none"> • 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. • Select Mapped Path to specify the path where you want to mount the database.

Field	Description
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Copy metadata files to	<ul style="list-style-type: none"> 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. <p>Note:</p> <ul style="list-style-type: none"> Metadata is not created for Non VDI copies. VSS or VDI metadata is not generated for Crash Consistent copies.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> 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 V2, 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.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX3 Service Level Objectives. SLO defines the service time operating range of a storage group.
VPLEX Mount option	<ul style="list-style-type: none"> Native array: Use this option if you want to mount the copy as native array volumes. VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes. Enable VMware cluster mount:
Use Dedicated Storage Group	<ul style="list-style-type: none"> 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 V2, VMAX3/PowerMAX, VNX storage group, PowerStore host group, or XtremIO initiator group for a mount. (A

Field	Description
	<p>dedicated VMAX V2 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.</p> <p>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.</p> <ul style="list-style-type: none"> If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount. <p>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.</p>
Enable VMware cluster mount	<ul style="list-style-type: none"> Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMWare SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
VMware Virtual Disk Mode	Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Allow Unmount Of OnDemand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.

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.  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.
Attach Database	Mounts the file system on which the database files are located, and then attaches the database to the SQL Server. The Attach Database option is only available for Non VDI and Crash Consistent copies because all the data necessary to attach the database is part of the copy. You might have to perform additional steps for full recovery of the database.

Note:

- Recovery, No recovery, and Standby modes are not supported for Non VDI and Crash Consistent copies.
- Attach Database is not supported for Full or Copy SQL copies.

Path mapping

The path mapping option mounts the copy to a host using a path mapping table set to user-defined locations. When you use a path mapping table, you have more control over where data is located.

You must specify the path where you want to mount a specific file system. You must provide a path map where the source file system and the target mount point is specified.

The following is a sample path mapping table for Windows.

The first two target paths, G:\ and H:\ drives must already be available on the mount host. That is, the root drive for the mount path must pre-exist before attempting a mount.

Source file system	Target mount path
D:\Test1	G:\Test1
E:\	H:\Test2
F:\Test3	I:\
L:\	N:\

Note:

- If a target path is not provided for a source path, then it is mounted to a path same as the source path on the mount host.
- Ensure that you type in the absolute mount path on the target host. If the path is invalid, mount fails.
- Mount copy overrides is unavailable, if you select the mount path as Mapped path.
- For Windows, if one of the entered path is invalid, VSS import fails. Therefore, the entire mount fails. Partial failed scenarios are not supported for Windows mount.
- For Windows and NFS file systems on Unix, nested target mount points are not supported.
- Path Mapping is not applicable to metadata paths for Microsoft Exchange and Microsoft SQL Server.

Specify path mapping settings

You can specify the path where you want to mount a specific copy.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange**.
4. Navigate to the folder that contains the copies.
5. Select the copy you want to mount, then click **MOUNT COPY**.
6. In the **Mount Copy** options, under the **Specify Mount Settings** section:
 - a. Select the mount host.
 - b. From the **Mount on Path** list, select **Mapped Path**.

The Path Mapping Settings link appears.

7. Click on the link to open the Path Mapping Settings window.
8. From the **Select Source Host** list, select a host.
All the file systems on the selected host are displayed in the source path column.
9. Specify the target path.
10. Click **Save** to save your settings.

If you want to set the target path for a file system on another source host, repeat steps 8 to 10.

11. Click **Reset**, to clear all the entered target paths for the selected source host.
12. Click **OK** to exit the Path Mapping window.

Note: If you change the path mapping settings, the earlier saved path mapping settings is not valid and the new path mapping settings takes precedence. Therefore, ensure that you save the path mapping settings for all the hosts before changing it.

Unmount a SQL copy from the Copies page

You can unmount a SQL copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the Name Column, click the database that contains the copy you want to unmount.
7. Select the copy you want to unmount and click **UNMOUNT**.
8. Click **OK**.

Unmount a SQL copy from the Service Plan page

You can unmount a SQL copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Microsoft SQL Server**.
4. Click the name of the service plan you prefer in the Service Plan column.
5. Select the copy you want to unmount and then click **Unmount**.
6. Click **OK**.

Create SQL repurpose copies

You can create first generation or second generation repurpose copies in AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the server folder that contains the database.

6. In the Name Column, select the database and click **CREATE COPY WITH PLAN**.
7. In the Subscribe to Existing Service Plan page, select **Data Repurposing > NEXT**.
8. Define the following properties for the copy:
 - a. The **Service Plan Name** field is defined by default.
 - b. The **Description** field provides a brief description of the copy.
 - c. The **Copy Label** field provides an autogenerated label for the copy.
 - d. The **Copy Location** list allows you to select a copy location either to **Local** or **Remote**.
 - e. Configure the **Use bookmark as intermediate step** option.
 - f. The **Mount Copy** list allows you to select mount options for the copy. You can configure this option to either **No**, **Yes**, **Yes - Keep it mounted** (where the previous copy will be unmounted), or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - g. The **2nd Generation Copies** list allows you to select either **Yes** or **No**.
9. Click **NEXT**.
10. In the Create the Copy page, do the following:
 - a. Configure the SQL Server Backup Type settings to either **Full**, **Copy**, **Non-VDI**, or **Crash-Consistent**.

Note: **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. When Non VDI or Crash Consistent backup type is selected, Auto Switch to Copy and Enable log backup are disabled.
 - b. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - d. In the **Array Selection** section, click **Select an Array** to choose the preferred array from the list.

Note: This is applicable only for SRDF/Metro.
 - e. In the **Storage Group to be used for VMAX-3 Array(s)** option, select the preferred storage group.
 - f. In the Select the cluster and arrays in preferred order for VPLEX metro configuration section, you can drag and drop the arrays to change array preference.
 - g. In the **Select Storage Pools to be used for VMAX-2 Array(s)**: select the preferred storage pool.
 - h. Configure the Copy Type settings to either **Snapshot** or **Clone**.
11. Click **NEXT**.
12. In the Scripts page select the pre-copy or post-copy scripts that you want to run and configure the following fields:

 **Note:** If you selected mount options, you will see the post-mount script in same page.

- a. **Full Path to Script**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
13. Click **NEXT**.
 14. In the Schedule/Run page, select one of the following scheduling options:
 - **Run Now** - Creates a copy when you click **FINISH** on this wizard.
 - **Schedule** - Creates a copy, that is based on the specified recurrence type. On the first schedule, a repurposed copy is created, and on subsequent schedules, it refreshes the copy.
 - **Run Only Once At later time** - Creates a copy only once on the specified date and time.
 15. Click **NEXT**.
 16. Review the repurpose copy creation settings, and click **FINISH**.

Create second generation copies

Perform this procedure to create a second-generation copy from a first-generation existing copy.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User databases folder.
6. Click the database that contains a first-generation copy.
7. Select a first-generation copy, and then click **CREATE 2ND GEN COPY**.

The **Create 2nd-gen Copy** wizard opens.

8. In the **Define the 2nd-gen Copy** page, configure the following:
 - a. `2nd-gen copies label` - Specify a label for the copy.
 - b. `Mount 2nd-gen copies` - Configure this field to one of the following options:
 - **No**
 - **Yes**
 - **Yes - Keep it mounted(Previous copy will be unmounted)**
 - **Yes - Mount the copy, but after the postmount scripts run, unmount the copy**
 - c. `2nd-gen copies type` - Configure this field to one of the following options:
 - **Snap**
 - **Clone**

9. Click **NEXT** to review your selection.
10. In the **Scripts for 2nd-gen Copy** page, select the pre-copy scripts and post-copy scripts you want to run.
 -  **Note:** This step also displays the post-mount scripts if you selected the mount option.
11. Click **NEXT** to review your selection.
12. In the **Schedule** page, select one of the following options:
 - **Run now**
 - **Run Recurrently As Per Schedule**
 - **Run Only Once At Later Time**
13. Click **NEXT** to review your selection.
14. Review the configurations for the second-generation copy and click **FINISH**.

Enable or disable a SQL copy expiry

You can enable or disable expiry of a copy during rotation using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the user databases folder, click the database that contains the copy.
7. Select the copy that you want to enable or disable and click **More**.
8. Click one of the following options depending on the action you want to perform:
 - **Enable Copy Rotation:** To enable automatic expiry of a copy during rotation.
 - **Disable Copy Rotation:** To disable automatic expiry of a copy during rotation.
9. Click **OK**.

Expire a SQL copy

You can expire a SQL copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the Name Column, click the database that contains the copy.
7. Select the copy that you want to expire and click **More > Expire**.

8. Click OK.

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`)

i **Note:** Ensure that no virtual machine snapshots are present before protecting a datastore. If virtual machine snapshots are present, protection succeeds, but AppSync fails to perform a file or virtual machine restore.

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 Unity, if the databases are in the same consistency group they become affected entities when the other database is protected.

- For VMAX V2, VMAX3/PowerMAX, VNX, Unity, Powerstore, 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*.
- For PowerStore, while restoring from remote copy, if the databases are in the same volume group and the replication session is created for volume group, they become *affected entities* when another database in the group is protected.

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

About this task

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

About this task

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.

Restore a SQL copy

You can perform a restore of a SQL server copy using the Appsync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Microsoft SQL Server**.
4. In the Name Column, click the server instance that contains the database.
5. In the Folder Name Column, click the User Databases folder.
6. In the Name Column, click the database that contains the copy.

7. Select the copy that you want to restore and click **More > Restore**.
8. In the **Select a Copy** page, select the copy you want to restore and click **NEXT**.
9. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

Note: You can perform this step only if you have multiple applications that share the same LUN or file systems.

10. Click **NEXT**.
11. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.

Note: In the case of SnapVX/XtremIO Snap/PowerStore Snap mounted copies, when you perform restore, AppSync restores the data from the snapshots created on the array to the source devices, or from linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

 - **Restore from snapshot:** Restores copies from original snapshots.
 - **Restore from changed data:** Restores from the linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).
12. Click **NEXT**.
13. In the **Review** page, review the restore options and click **FINISH**.

SQL Server restore utility (assqlrestore)

AppSync includes a SQL Server restore utility called `assqlrestore`. This section describes its 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`.

Note: For Non VDI and Crash Consistent copies, you cannot restore a database using `assqlrestore` because no metadata is created.

`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. This utility supports item level restore from a mounted copy.

Assqlrestore command syntax with examples

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

Command syntax

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

Table 20 `assqlrestore` Command Syntax

Option	Description
Required	
-s	SQL Server name including instance name (host\instance).
-f	Metadata filename and location (the path selected in the GUI under Copy metadata files to).
-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: <code>logical_file_name</code> and <code>operating_system_file_name</code> . 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 overwrite the original files. For example: <code>-m logicalfilename S:\existingdir \newfilename.mdf</code>
-fg	Filegroup to restore. Repeat option for each filegroup.
-lf	Logical file to restore. Repeat option for each logical file.

Table 20 `assqlrestore` Command Syntax (continued)

Option	Description
-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 1 Command syntax examples

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

- 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 the default Administrator, then back up the SQL Server transaction log. Ensure that the default administrator has the policy - Create Global Objects (SeCreateGlobalPrivilege) granted, along with the privileges mentioned in "Required permissions and rights".

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 copy. 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 filegroup 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.

CHAPTER 7

Protect Oracle

This chapter includes the following topics:

- [Overview of Oracle support](#)..... 170
- [Protecting a database](#)..... 184
- [Service plan summary and details](#)..... 191
- [Mount an Oracle copy](#)..... 197
- [Restore an Oracle copy](#)..... 211

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/modernHomeDataProtection> 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 File, and Unity File storage.
- Oracle databases residing on ASM disks.
- Oracle databases residing on file systems.
- Oracle Container Databases.
- Oracle PDB granular restore.
- Oracle ASM 4KB sector disk drives.
- Oracle Flex ASM.
- RMAN cataloging of databases to a remote catalog.
- Repurposing of Oracle database copies.

Note:

- AppSync does not support file systems or ASM diskgroups on Linux operating system devices which are not full block devices (such as /dev/sdc) or primary first partition (such as /dev/sdc1).
- AppSync does not support Flex ASM clusters.
- When creating an ASM database, ensure that the diskstring is not in the /dev/sd* format. If the diskstring is in the /dev/sd* format, the devices are not considered as UDEV devices, and protection fails.
- Appsync supports the Quality of Service feature for XtremIO release 6.2 and later.

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 from which the database is subscribed to a service plan is not accessible, AppSync does not automatically run the replication on another node in the cluster because 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. Disable Resource Group service.
 2. Perform restore from AppSync.
 3. Enable Resource Group service.
 4. Mount and recover the database manually.

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.

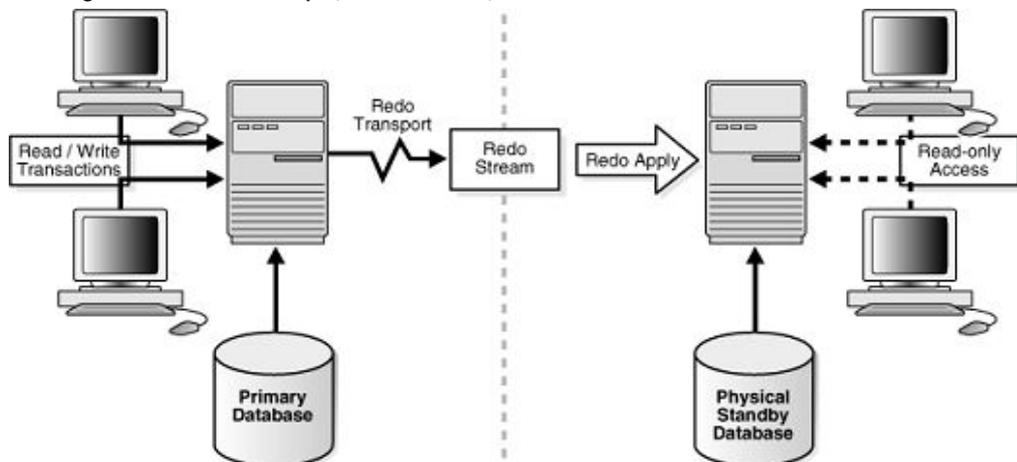
Physical standby

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 2 Physical standby environment

This figure describes the physical standby environment.



Copy Management

On the AppSync console, go to the **Copy Management > Select View > Copies > Select Application > Oracle** page. A Data Guard relationship column now displays. Click the **show/hide columns** button and select **Dataguard Relationships**. A Data guard relationship column now displays.

Note: By default, the Dataguard Relationships column is unchecked and will not appear in the page.

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.
- Mount host should have same naming scheme as that of the VCS infoscale cluster production 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: `>hagrps -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.

PowerHA (HACMP) cluster integration

AppSync can work with standalone Oracle databases that are configured to failover from node to node in an IBM® PowerHA (HACMP) cluster environment.

Introduction

AppSync protects the database on the node where the current state is active before the Service Plan run. AppSync relies on the service label IP of the Oracle database resource group.

Note:

- You must update the agent plugin to version 4.0 , if the AppSync server version is 4.0.
- Starting in AppSync 3.1, AppSync mandates the use of service label IP for Oracle database protection. The copies created using AppSync versions earlier than 3.1 can be mounted or restored even after an upgrade to AppSync 3.1. After an upgrade, scheduled service plan run fails, if the service label IP is not registered with the AppSync server.

Consider the following when protecting an application that fails over as part of a PowerHA (HACMP) cluster:

- The nodes of the PowerHA cluster must be registered with AppSync before registering the service label IP.
 - Note:** You must register the objects with AppSync in the following order:
 - Active node
 - Passive node
 - Service label IP of the Oracle database
- The service label IP/name must be configured for the Oracle database resource group.
- If the resource group has multiple service label IPs configured, register only one service label IP with the AppSync server.
- If a failover occurs while running a replication or restore process, the operation fails. Node failover must occur before running the service plan, or at the start of a restore.
- The Oratab file entry must be the same on all the cluster nodes.
- 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 PowerHA cluster.
- The AppSync host plug-in must be installed on the mount host.
- Mount to service label IP is not supported.

Restore in a PowerHA environment

Perform a restore. After a restore, the volume group is not concurrent. You must manually make them concurrent before performing a host or file system rediscovery.

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. Restore of mounted copies is not supported for applications (File System and Oracle databases), managed by AIX HACMP or PowerHA cluster.

Post restore procedure in a PowerHA environment

Learn how to perform manual steps with a restore in a PowerHA environment after a restore.

About this task

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 the file system.
2. Type the `varyoffvg` command.
3. Type the `varyonvg` command with `-c` option (to make it concurrent).

Verification:

The `lspv` command must 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
```

4. Add the file system back to the resource group.
5. Verify and synchronize the 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 application-consistent copies of Oracle databases, the data files, fast recovery area, 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.

During copy creation, if hot backup mode is not selected, AppSync creates crash consistent copies, and does not quiesce the database. You must use this method to create copies, if you have archive logs or fast recovery area sharing the same file system, volume group, ASM disk group, RP consistency group, or data store as the data files and/or control files and/or redo logs.

If all Oracle files, including archive logs are on one disk group, AppSync can protect that database without hot back mode. The copy is crash consistent.

Note: Read-only Oracle databases can only be protected in no hot backup mode.

If the archive log location is shared with other database components, use init overrides (see the Custom initialization parameters field under Mount options for details) and point to that location during mount with recovery to protect the archive log location separately. Ensure that you specify the correct path in init overrides, especially if ASM disk group rename or alternate path mount is used.

If the database is running in NOARCHIVELOG mode, do not select the hot backup mode option when creating copies.

When using VNX, ensure that all consistency groups are VNX consistency groups. Additionally, the archive log files must be on a different CG from the rest of the database files.

Note: Database files refer to data files, and/or control files, and/or redo logs. Archive log files refer to archive log destination and/or Fast Recovery Area .

Oracle ASM 4K Sectors

Oracle ASM supports 4K sectors in native mode and emulation mode. Appsync supports Oracle ASM 4K sector configurations with the following limitations.

Appsync supports:

- Linux with ASMLib.
- Dell SC, only while creating 4K sectors in emulation mode.
- XtremIO when the application hosts are physical, or are iSCSI-connected and using native mode.

Note: Appsync supports Oracle ASM 4K sector configurations for Oracle release 12cR2 or later.

Oracle Flex ASM

AppSync supports Oracle Flex ASM. AppSync detects the status of the database instance as well as the ASM instance on each RAC node and selects a node where both are online.

If either the ASM or database instance, or both instances, are offline or unavailable on one node, AppSync will check the next node of the cluster for a running ASM and database instance. If both instances are online on the next node, Appsync sets the current host to this node for further processing.

If either ASM or database or both the instances are unavailable on all RAC nodes, the job fails.

For standalone instances, ASM must be online and available on at least one node.

ASM rebalancing

AppSync switches off ASM rebalancing power factor before taking a snapshot or clone of the underlying disks and turns it back on, after the copy is created. This is to ensure that no automatic rebalancing occurs during protection. AppSync disables ASM rebalancing using the `alter system set asm_power_limit=0` command. AppSync checks for active rebalancing operations only on ASM disk groups that are involved in protection.

```
select count(group_number) from gv$asm_operation where operation='REBAL' and
group_number in <group_number of DGs in protection set>
```

The value returned must be 0 (which means that no disk group involved in protection is undergoing a rebalance operation) for AppSync to continue. If there are disk groups undergoing rebalancing, AppSync polls for the operation to terminate for a maximum of one hour, after which protection fails.

AppSync does not issue a manual rebalance operation per disk group, and it cannot disable ongoing manual rebalancing operations issued outside AppSync. Manual rebalancing operations might take a long time to complete. In order to avoid timeout failures during protection, you must ensure that no manual rebalancing operations are active prior to a Service Plan run.

AppSync also enables and disables ASM rebalancing for no hot backup copies.

Removal of Oracle deleted database

When you remove or delete a database that has copies associated with it, the database is marked for pending delete.

Note:

- For Oracle RAC, all instances of the database must be removed.
- A database can be removed only if the entry for the database is absent in the `/etc/oratab` file.
- Subscribed or protected databases are marked for pending delete only if all the instances are removed.

If the database is recreated with the same name after deletion, and rediscovery is performed after the database has been recreated, AppSync displays duplicate entries with the same database name. This is not a concern if you intend to retain the copies of the deleted database. However, if you do not intend to retain the copies of the deleted database, host or database rediscovery must be performed immediately after the removal of an Oracle database from a cluster or host.

Do the following to remove the duplicate entries:

1. Comment out the `/etc/oratab` entry for the database using a `#` at the beginning of the entry.
2. Remove all copies or subscriptions of the deleted database, and rediscover host or database in the AppSync GUI. If the created database has copies or subscriptions, it is marked pending delete. Otherwise, it does not show up after this step.
3. Uncomment the entry that was commented in step 1.
4. Rediscover host or database again in the AppSync GUI. If the database was marked pending delete in step 2, the pending delete flag is cleared. Otherwise, a single database entry for the new database is displayed in the GUI.

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 file systems on one volume group with two more file systems 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 data location and archive log location: Database 1,2,3 files on, for example, `diskgroup +data1`, and database 1,2,3 archive logs on, for example, `diskgroup +data2`.

Oracle on RecoverPoint consistency group-based storage

- Single database: Database files on LUNs in RP consistency group, for example, `DATA1CG` 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, `DATA1CG`, 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 Unity Consistency Group-based storage

The following configurations are supported:

- Single database: Database files on LUNs in Unity consistency group, for example, data files in consistency group `DATALUNGRP` and archive log files in consistency group `ARCHCG`.
- Multiple databases sharing single archive log location: Database 1 files on LUNs in Unity consistency group, for example, `DATA1LUNGRP`, then database 2 files on LUNs in Unity consistency group `DATA2LUNGRP`, and then archive log files in Unity consistency group, for example, `ARCHLUNGRP`.

- Multiple databases sharing data location and archive log locations: Database 1, 2, 3 files on LUNs in Unity consistency group, for example, DATALUNGRP, then database 1, 2, 3 archive logs on LUNs in Unity consistency 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:

- 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

i **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 VMFS and NFS 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:
 - Protection of Oracle databases across virtual machines sharing the same datastore
- Production VMWare virtual disk with multi writer option enabled is supported for Oracle RAC.
- 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](#).

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.

Oracle supported configurations

The following table describes the Oracle supported configurations.

Table 21 Oracle supported configurations

Oracle Features/ Environments	XtremIO	VVMA X V2 and VMAX 3/ Power MAX	VNX	VNX file	Unity	Unity File	VPLEX	RP	Dell SC	PowerStore
Oracle Standalone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle on file systems	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle on ASM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle ASM 4K Sector (For release 12cR2 or later)	Yes (Native Mode)	N.A	N.A	N.A	N.A	N.A	N.A	N.A	Yes (Emulation Mode)	N.A
Oracle Container Database	Yes	Yes	Yes	N.A	Yes	Yes	Yes	No	Yes	Yes
Oracle RAC with NFS (Non ASM)	No	No	No	Yes	No	Yes	No	N.A	No	No
Oracle RAC with ASM	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
Oracle Dataguard (Primary and Secondary)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Host cluster support for Oracle standalone (PowerHA - AIX and VCS/RHCS -Linux) ^a	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
Hot backup mode ^b	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No hot backup mode/ crash consistent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Oracle on physical and virtual machines (with pRDMs and Vdisks) - no	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes

Table 21 Oracle supported configurations (continued)

Oracle Features/ Environments	XtremIO	VVMA X V2 and VMAX 3/ Power MAX	VNX	VNX file	Unity	Unity File	VPLEX	RP	Dell SC	PowerStore
support for RDMS in virtual mode ^c										
Oracle databases residing on NFS file systems with VNX, Unity, or eNAS	N.A	N.A	N.A	N.A	N.A	Yes	N.A	N.A	N.A	N.A
Oracle with AIX LPARs - virtual connections and physical or NPIV connections	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	No
Repurposing of Oracle databases	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes
mknode with ASM ^d	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
UDEV with ASM ^e	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
ASMLib with ASM ^f	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
Mounting Oracle standalone to standalone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mounting standalone ASM to standalone ASM	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
Mounting RAC NFS (non ASM) to alternate RAC NFS (non ASM)	N.A	N.A	N.A	Yes	N.A	Yes	N.A	N.A	N.A	N.A
Mounting RAC ASM to alternate RAC ASM	Yes	Yes	Yes	N.A	Yes	N.A	Yes	Yes	Yes	Yes
Mounting to production RAC as a cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mounting back to production RAC as a single instance/non-clustered	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMAN with BCT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ASM RAC or standalone databases created using ASM Filter Driver (ASMFD)	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes

Table 21 Oracle supported configurations (continued)

Oracle Features/ Environments	XtremIO	VVMA X V2 and VMAX 3/ Power MAX	VNX	VNX file	Unity	Unity File	VPLEX	RP	Dell SC	PowerStore
Mixed layout of an Oracle database which has data files, control files, and redo logs on ASM disk groups and archive logs and/or FRA on file systems (such as ext4 on Linux)	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes

- a. RHCS is applicable for RHEL and VCS for both SuSE and RHEL.
- b. See the Prerequisites and supported configurations section for information on database layout.
- c. This is only applicable for LINUX.
- d. This is only applicable for AIX.
- e. This is only applicable for LINUX.
- f. This is only applicable for LINUX.

AppSync does not support the following Oracle environments:

- Oracle on any cluster file systems (such as ACFS, OCFS, GFS, GFS2, QFS, and so on)
- Cold backup
- Nested file systems on NFS
- Mounting to different OS versions and different Oracle versions
- Oracle RAC one node database
- Mix of data and archive logs on RDM and Vdisks
- Multiple databases residing on different virtual machines sharing the same datastore (for example, VM1 with DB1 and VM2 with DB2)
- ASM mounting to non-ASM
- 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
- Oracle Flex Cluster
- Oracle GoldenGate
- ASM Dynamic Volume Manager (ADVM)
- Oracle Multitenant
- Oracle RAC database on NFS 4 file system is not supported by Oracle

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 **Copy Management > SELECT VIEW > COPIES > SELECT APPLICATION > Oracle > CREATE COPY WITH PLAN** then select **Subscribe to Service Plan and Run** option when you want to protect a selected database immediately. The service plan is executed for that database alone.
- Select **Copy Management > SELECT VIEW > COPIES > SELECT APPLICATION > Oracle > CREATE COPY WITH PLAN** then select the **Subscribe to Service Plan** option 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 **Copy Management > SELECT VIEW > COPIES > SELECT APPLICATION > Oracle > CREATE COPY WITH PLAN** using a plan in the Oracle databases page.
- Select the **Run now** option from the Oracle Service Plans page to run the entire plan immediately.

For Oracle Pluggable Databases, consider the following limitations:

- There is no option to select PDBs within a CDB for protection. All PDBs are protected along with the CDB.
- All PDBs within a CDB except PDB\$SEED must be in read/write mode for hot backup. AppSync mandates this and will fail hot backup protection if any PDB is not in read/write mode.
- If certain PDBs within a CDB are not in read/write mode, then you can choose the no hot backup option while creating a copy.
- For RAC databases, all the instances of each PDB on all the RAC nodes must be in read/write mode for hot backup to succeed.
- PDB\$SEED is always protected. This is mandatory for recovering the copy later during mount and recovery.
- When you unplug and plug a pluggable database, a database rediscover or a host rediscover is required. Consider the following example:
The "CDB" database contains the PDB1, PDB2, PDB3 pluggable databases, and "CDB1" contains the PDB4 pluggable database. If you unplug PDB3 from "CDB" and plug it into "CDB1", in the same or different PDB location, a database rediscover or host rediscover becomes necessary.
- Restore is not supported for Non-CDB copies, if you are migrating from a Non-CDB to a PDB. Consider the following example:
If you migrated non-cdb copies to a PDB, then restore is not supported for the copies that were made before migration. However, you can mount these copies on a mount host.

 **Note:** The same limitations apply for repurposing copies.

Discover an Oracle database

To keep AppSync up-to-date, you must discover databases in the oracle databases page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **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 and databases that have been shut down do not appear.
4. From the **MORE** drop-down, select **Discover Databases**.
5. Under **Discover Oracle database**, select the server where the database you want to discover resides.
6. Click **OK**.

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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **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 and databases that have been shut down do not appear.
4. Select one or more Oracle databases, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select the appropriate option.

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

7. Select the service plan that you want to subscribe to.
8. Click **NEXT** to review your selection.
9. Click **FINISH**.

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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **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 and databases that have been shut down do not appear.
4. Select the database to unsubscribe from a service plan.
5. From the **MORE** drop-down, select **Unsubscribe**.
6. Select the service plan you want to unsubscribe, and click **OK**.

 **Note:** You can also unsubscribe applications from a service plans, from the Service Plan page.

Creating an Oracle database copy from the Copies page

Create a copy of a database by subscribing it to an AppSync Oracle service plan from the Databases page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **COPIES**.
3. From the **Select Application** drop-down, select **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 and databases that have been shut down do not appear.
4. Select one or more Oracle databases, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select **Subscribe to Service Plan and Run**.
7. Select the service plan that you want to subscribe to.
8. Click **NEXT** to review your selection.
9. Click **FINISH**.

Create Oracle repurpose copies

You can create first generation or second generation repurpose copies in AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Select the database and click **Create Copy With Plan**.
5. Select **Data Repurposing**.
6. Define the following properties for the copy:
 - a. The **Service Plan Name** field is defined by default.
 - b. The **Description** field provides a brief description of the copy.
 - c. The **Copy Label** field provides an autogenerated label for the copy.
 - d. The **Copy Location** list enables you to select a copy location either to **Local** or **Remote**.
 - e. Configure the **Use bookmark to copy** option.
 - f. The **Mount Copy** list enables you to select mount options for the copy. You can configure this option to either **No**, **Yes, Yes - Keep it mounted** (where the previous copy is unmounted), or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - g. The **2nd Generation Copies** list enables you to select either **Yes** or **No**.

 **Note:** Creating second generation copies is not supported in this beta release.

7. Click **Next**.
8. In the Create the Copy page, do the following:
 - a. Configure the following Oracle settings:
 - **Place the database in hot backup mode**
 - **Select archive destination for hot backup mode**
 - **Copy the Fast Recovery Area**
 - b. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. Applies to VMAX3/PowerMAX only.
 - c. In the **Array Selection** section, click **Select an Array** to choose the preferred array from the list.

 **Note:** This is applicable only for SRDF/Metro.

- d. In the **Select Storage Group for PowerMAX/VMAX3 section** option, select the preferred storage group.
- e. In the **Select Storage Pools to be used for VMAX-2 Array(s)** option to select the preferred storage pool.

- f. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
- g. Configure the **Copy Type** settings to either **Snapshot** or **Clone**.
9. Click **Next**.
10. In the **Scripts** page, select the precopy or postcopy scripts that you want to run and configure the following fields:
 - a. **Full Path to Script**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
11. Click **Next**.
12. In the **Schedule/Run** page, select one of the following scheduling options:
 - **Run Now** - Creates a copy when you click **Finish** on this wizard.
 - **Schedule** - Creates a copy that is based on the recurrence type you specify. On the first schedule, a repurposed copy is created, and on subsequent schedules, it refreshes the copy.
 - **Run Only Once At later time** - Creates a copy only once on the specified date and time.
13. Click **Next**.
14. Review the repurpose copy creation settings and click **Finish**.

Create second generation copies

Perform this procedure to create a second-generation copy from an first-generation existing copy.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Oracle** to display the databases page.
4. Click the database that contains a first-generation copy.
5. Select a first-generation copy, and then click **CREATE 2ND GEN COPY**.

The **Create 2nd-gen Copy** widget opens.

6. In the **Define the 2nd-gen Copy** page, configure the following:
 - a. `2nd-gen copies label` - Specify a label for the copy.
 - b. `Mount 2nd-gen copies` - Configure this field to one of the following options:
 - **No**
 - **Yes**
 - **Yes - Keep it mounted(Previous copy will be unmounted)**
 - **Yes - Mount the copy, but after the postmount scripts run, unmount the copy**
 - c. `2nd-gen copies type` - Configure this field to one of the following options:

- **Snap**
 - **Clone**
7. Click **NEXT** to review your selection.
 8. In the **Scripts for 2nd-gen Copy** page, select the pre-copy scripts and post-copy scripts you want to run.

 **Note:** This step also displays the post-mount scripts if you selected the mount option.
 9. Click **NEXT** to review your selection.
 10. In the **Schedule /Run** page, select one of the following options:
 - **Run now:** Creates a copy when you click **FINISH** on this wizard.
 - **Schedule:** Creates a copy that is based on the recurrence type you specify. On the first schedule, a repurposed copy is created, and on subsequent schedules, it refreshes the copy.
 - **Run Only Once At Later Time:** Creates a copy only once on the specified date and time.
 11. Click **NEXT** to review your selection.
 12. Review the configurations for the second-generation copy and click **FINISH**.

Oracle Copies page

You can view a list of copies on the Oracle Copies page.

Copy information includes:

This table describes the copy information displayed in the copies page.

Table 22 Copy Information

Column	Description
Status	Green: successful Yellow: Completed with errors Red: failed
Copy Name	Date and time when the copy was created
Service Plan	Name of the service plan that is associated with the copy. For repurposed copies, a Repurpose link displays in this column. Click this link to edit the Service Plan for 1st or 2nd generation copies.  Note: In the service plan for repurposed copies, the options to schedule and mount overrides will be disabled.
Server	Name of the server associated with the copy.
Label	Common name that is used to help identify repurposing copies
Application Consistent	Displays whether or this copy leverages hot backup to create an application consistent copy

Table 22 Copy Information (continued)

Column	Description
Mount Status	Indicates if the copy is mounted, or Not Mounted
Mount Type	If copy is mounted as part of service plan run, value for Mount Type is ServicePlan. If copy is mounted as OnDemand, value for Mount Type is OnDemand.
Recovery Status	Indicates if the copy has been recovered or not
Copy Type	It displays the type of copy that was created. The copy can be one of the following types: <ul style="list-style-type: none"> • RecoverPoint Continuous Data Protection Bookmark • RecoverPoint Continuous Remote Replication Bookmark • Unity Snap • VNX Snap, VNX File Snap • VMAX V2 Snap, VMAX V2 Clone • XtremIO snapshot • VMAX3/PowerMAX SnapVXClone, SnapVXSnap • VPLEX Snap, VPLEX Clone • DELLSC Snap • PowerStore Snapshot • PowerStore Thin Clone
Generation	The generation number of the repurposed copy
Source	The original source database for the copy, or source copy for the copy
Site	Site where the copy is located.
Storage System	Storage system where the copy resides.
Automatic Expiration	Determines whether automatic expiration is enabled or disabled for the selected copy.

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. Log in to the AppSync console and select **Copy Management**.

2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Click a database to view existing copies of the database.

You can see details of a copy in the right pane of the copies page. The list of copies can be filtered using the filter option located at the top-right corner of the table in this page.

Service plan summary and details

The service plan **Settings** tab shows the Service plan name, Description, and Enabled status of the service plan.

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Service Plan**.
3. From the **Select Application** drop-down, select **Oracle**.
4. Select the desired Service plan, and the summary of the service plan will display in the right pane of the page.

Review [Overview: Service Plan](#) for more service plan copy information.

Service plan schedule

The service plan schedule (On-demand or scheduled) 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 different times during the day.
 - Select minutes after the hour in 1 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.
 - Select **Last** to select the last day of the month.
- Server plan Recurrence Type options include:
 - **Run Now**

- **Schedule**
- **Run Only Once At later time**

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.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **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 and databases that have been shut down do not appear.
4. Select one or more Oracle databases, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select **Subscribe to Service Plan (with option to override)**.
7. Select the service plan that you want to subscribe to.
8. Click **NEXT**.
The Override Schedule page appears.
9. Select one or more databases and click **OVERRIDE SCHEDULE**.
10. Specify 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 databases.
11. Click **NEXT** to review your selection.
12. Click **FINISH**.

Storage preferences

Sets the preferred order of storage technology to use while creating copies, for example, VNX Snapshot or VMAX V2 Clone, VMAX3/PowerMAX 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 V2/VMAX3/PowerMAX block or 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 V2/VMAX3/PowerMAX block objects.

A database mix of VNX and VMAX V2/VMAX3/PowerMAX 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. AppSync executes this script once per host per service plan run on the production host.

This operation requires the Data Administrator role in AppSync.

For a successful script run ensure:

- The preferred scripts are 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 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 23 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 function creates a copy based on the replication technology that is specified in the service plan.

The create copy options specifies the backup type for the Oracle database copy that AppSync creates. It also sets the period for automatic expiration of the copies.

Automatic expiration of copies

The automatic expiration value 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.

You can run this script once per host per service plan run. If this script 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.

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 24 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 during unmount.

Pre-mount script

You can enable this script 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 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](#). You must select **Same as mount host** in the **Run on host** option so that the script runs on all mount hosts.

Table 25 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 step either mounts the copy or mounts and recovers the copy.

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 scripts, 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 VMAX3/PowerMAX array, a setting called Desired Service Level Objective (SLO) is available. The option appears in the Mount wizard and it specifies the required VMAX3/PowerMAX 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.
- **Restart databases after reboot:** This option is used to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled.

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. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Oracle**.
4. Click a service plan, and expand the right pane.
5. Click the **OVERRIDES** tab.
6. Select **Mount Overrides**.
7. Select an entry, and click **OVERRIDE MOUNT**.
8. Edit the required fields, and click **APPLY CHANGES** to save the settings.
9. To revert back to default settings for a server, click **SET TO DEFAULT**.

Post mount script

You can enable this script 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 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 26 Post-mount script field descriptions

Field in UI	Description
Full path to script	The complete path to the script location

Table 26 Post-mount script field descriptions (continued)

Field in UI	Description
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 unmount copy option in the service plan unmounts the copy.

This option is disabled if the **Unmount previous copy** option is enabled.

If you have chosen to mount with recovery options (standalone, RMAN, or cluster mount) in the Mount options, all the mounted databases are shut down as part unmount.

Mount an Oracle copy

This section describes the AppSync console mount fields and their descriptions.

Mount operations

Table 27 Console field descriptions

Field	Description
Mount on Server	The server on which to mount the copy.
Mount on path	The Default Mount Path is <code>/appsync</code> . 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, <code>/EMC</code> instead of <code>/AppSync</code> . Select Mapped Path to specify the path where you want to mount the database.
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
Copy to mount	Allows user to select if the local or remote copy has to be mounted as part of service plan run.  Note: Applies to service plans that create local and remote copies simultaneously.
Quality of Service Policy	For XtremIO only, an option called Quality of Service policy appears in the wizard. You can select the desired Quality of Service policy for mounting a copy.

Table 27 Console field descriptions (continued)

Field	Description
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> • 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 V2, 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 V2, 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 V2, and RP-XtremIO, virtual access is not supported.
Restart databases after reboot	Use this option to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired SLO appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
VPLEX Mount option	<ul style="list-style-type: none"> • Native array: Use this option if you want to mount the copy as native array volumes. • VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes.
Enable VMware cluster mount	Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled.

Table 27 Console field descriptions (continued)

Field	Description
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
Allow Unmount Of OnDemand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.
Enable VMware cluster mount	<ul style="list-style-type: none"> • Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. • If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMware SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
VMware Virtual Disk Mode	Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
Mount Operation	<p>Allows the following mount operations:</p> <ul style="list-style-type: none"> • Mount on standalone server • Mount on standalone server and create RMAN catalog entry • Mount on standalone server and recover database • Mount on standalone server and prepare scripts for manual database recovery • Mount on Grid cluster and recover as RAC database

Table 27 Console field descriptions (continued)

Field	Description
Run Filesystem Check	<p>During a mount operation, theAppSync agent checks file system data consistency by executing the <code>fsck</code> command. This operation can be time consuming. You can clear this option to skip file system check during a mount operation. By default, file system check is enabled.</p> <p>Note:</p> <ul style="list-style-type: none"> In the case of a restore operation, the Run Filesystem Check option is enabled by default. You cannot disable it. The Run Filesystem Check option is not applicable to ASM file systems.
Recovery Settings	<ul style="list-style-type: none"> Open-mode: Read-write ORACLE_HOME: Same as production host Database name: APS is the prefix, %DB% is the variable which will be replaced with the production database name during run time. SID name: APS is the prefix, %SID% is the variable which will be replaced with the production database SID during run time. ASM diskgroup name: APS is the prefix, %DG% is the variable which will be replaced with the production ASM diskgroup name during run time. <p>Note: If multiple diskgroups are involved, a prefix or suffix is mandatory.</p> <ul style="list-style-type: none"> Customize Initialization Parameters: This field will be blank. You can fill in one parameter per line, for example, <code>memory_target=629145600</code> Create TEMP Tablespace: Use this option to create the Temp Tablespace on the recovery mounted database copy. This setting is enabled when you select the following mount operations with Read/Write Open-mode: 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. When you

Table 27 Console field descriptions (continued)

Field	Description
	<p>select the Create TEMP Tablespace option, two additional options display:</p> <ul style="list-style-type: none"> • Number of Tempfiles: The number of files to be added to Temp Tablespace. The size of the files are specified in the Size of each file setting. • Use BIGFILE option: Use the BIGFILE option when creating the new temp file. If this option is selected, the number of temp files is 1. • Size of each file: The size of each temp file (in kilobytes (K), megabytes (M), gigabytes (G), or terabytes (T)). • Restart databases after reboot: Select this option to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled. <p> Note: This option is not available for RMAN and mount with generate scripts.</p> <ul style="list-style-type: none"> • Create SPFile: Select this option to create an SPFile. The SPFile is created in the default location (<code>\$ORACLE_HOME/dbs</code>), with the name <code>spfile<SID>.ora</code>. During unmount, the SPFile is removed from the <code>\$ORACLE_HOME/dbs</code> folder. • Create on ASM disk: Select this option to create the SPFile on the primary ASM diskgroup.
Advanced Recovery Options	<ul style="list-style-type: none"> • Create Control file copies: Select this option to create 0-3 additional control file copies for redundancy purposes. The default is 0. • Change Database ID: Select this option to change the database ID of the mounted database. By default, this option is disabled. • Use ADR (Automatic Diagnostic Repository) home directory for DIAGNOSTIC_DEST: Select this option to force the mounted database to use the ADR home directory instead of TEMP for diagnostic logs (default: off). By default, this option is disabled.

Table 27 Console field descriptions (continued)

Field	Description
	<ul style="list-style-type: none"> Disable archive log mode: Select this option to force the mounted database to start with archive logging disabled. By default, this option is disabled.

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.

Note: It is recommended to install Oracle 12c Patch 19404068 for reliable recovery of an Oracle database.

Additional information

- 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.
- For UNIX hosts, you can configure a command execution timeout value from the Servers page of the AppSync console. AppSync uses this value to wait for each operating system command that is executed by AppSync on a UNIX platform. The default value is 60 minutes. For example, if `fsck` during file system copy mount takes more than 60 minutes on a host, you can increase the command execution timeout value.
- AIX multiple mounts
 - Multiple copies can be mounted to the same AIX host only if the copies are created using AppSync 3.0.1 and later.
 - If copies were created using AppSync 3.0 or earlier, you cannot mount multiple copies to the same AIX host, even after you upgrade both the sever and agent to AppSync 3.0.1 and later.
 - If you have copies created using both AppSync 3.0 and 3.0.1 and later, it is recommended that you mount the copy created using AppSync 3.0.1 and later for successful concurrent mounts. If you intend to mount the AppSync 3.0 copy, only one copy can be mounted.
 - If you mount the copy created from AppSync 3.0.1 and later, the mount of AppSync 3.0 copy might fail.
 - After you upgrade the AppSync server to 3.0.1 and later, ensure that you upgrade the agent to AppSync 3.0.1 and later.

Mount 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

- On the AppSync console, go to **Copy Management**.

2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Click the name of the database you prefer in the Name column.
5. Select the copy you want to mount, then click **MOUNT COPY**.
6. Click **NEXT**.

If multiple databases were protected together, you may see the additional copies to mount option. Select the copies you prefer and click **NEXT**.

7. On the Select Mount Options page, from the Mount operation 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 database
 - Mount on standalone server and prepare scripts for manual database recovery
 - Mount on Grid cluster and recover as RAC database

If you select **Mount on standalone server and recover database**, **Mount on standalone server and prepare scripts for manual database 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 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. Use BIGFILE option: Select this option when creating the new temp file.
- c. 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.

8. Under **General Settings**, do the following:

- a. From the **Mount on Server** list, select the server on which to mount the copy.
 - b. From the **Mount on Path** list, select a mount path location either to **Default path, Same as original path**, or **Mapped Path**. The mount path is the location where the copy is mounted on the mount host.
 - c. **Mount to cluster**: This field is used to specify the cluster where you want to mount the copy. You can configure the value of this field as **Original Cluster**, to mount back to the production cluster.
 - d. Configure the **Allow unmount of On-demand mounted copy** option to allow the unmount of copies that were mounted on demand.
 - e. The **Run Filesystem Check** option is selected by default. This option is applicable for the UNIX or Linux platform only.
9. Under **Recovery Settings** configure the following options:
- a. **Open-mode**
 - b. **ORACLE_HOME**
 - c. **Database Name**
 - d. **SID Name**
 - e. **ASM Diskgroup Name**
 - f. **Customize initialization Parameters**
 - g. Select **Restart databases after reboot** to start the AppSync mounted Oracle databases automatically after a host reboot. By default, this option is disabled.
 - h. Select **Create SPFile** to create an SPFile. The SPFile is created in the default location (`$ORACLE_HOME/dbs`), with the name `spfile<SID>.ora`. During unmount, the SPFile is removed from the `$ORACLE_HOME/dbs` folder. If the **Copy SPFILE to ASM diskgroup** option is selected, the SPFile is created on the primary ASM diskgroup instead of `$ORACLE_HOME/dbs`.
-  **Note:** The **Restart databases after reboot** and **Create SPFile** options are not available for RMAN and mount with generate scripts.
10. Under **Advanced Recovery Settings**:
- a. Select **Create Control file copies** to create 0-3 additional control file copies for redundancy purposes. The default is 0.
 - b. Select **Change Database ID (DBID)** to change the database ID of the mounted database. By default, this option is disabled.
 - c. Select **Use ADR (Automatic Diagnostic Repository) home directory for DIAGNOSTIC_DEST** to force the mounted database to use the ADR home directory instead of TEMP for diagnostic logs (default: off). By default, this option is disabled.
 - d. Select **Disable archive log mode** to force the mounted database to start with archive logging disabled. By default, this option is disabled.
-  **Note:** You cannot use the advanced recovery options when restoring a RAC copy.
11. Under **Storage Settings**, configure the following options:
- a. **Image Access Mode**
 - b. **Desired SLO**

- c. **Desired FAST**
 - d. **VPLEX Mount Option**
 - e. **Unlink the SnapVX snapshots during unmount**
12. Under **VMware Settings**, do the following:
- a. **Enable VMware cluster mount** checkbox - If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. Then the target LUN is made visible only to the ESX cluster on which the mount host resides. This is applicable for both RDM and vDisk device types.
 - For VMAX3/PowerMAX arrays, select the Service Level Objective (SLO) for the mount copy.
 - For VMAX V2 arrays, select the desired FAST Policy. Each FAST Policy is associated with a storage group on the array. Select the storage group to use for the mount operation by selecting the FAST policy associated with that storage group.
 - For XtremIO 6.2 and later, click the **Quality of Service policy** option to select the desired Quality of Service policy while mounting a copy.
 - b. **Disable VMware SRM** - This option is applicable only for RP 4.1 and above.
 - c. **VMware Virtual Disk Mode** - Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
13. Click **Next**.
14. Review the mount settings and click **Finish** to complete the mount.

Results

In the **Mount Copy Status** page, you can view the progress.

Unmount an Oracle copy from the Copies page

You can unmount an Oracle copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Click the name of the database you prefer in the Name column.
5. Select the copy you want to unmount and then click **UNMOUNT COPY**.
6. Click **OK**.

Unmount an Oracle copy from the Service Plan page

You can unmount an Oracle copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > Oracle**.
4. Click the name of the service plan you prefer in the Service Plan column.
5. Select the copy you want to unmount and then click **Unmount Copy**.
6. Click **OK**.

Expire an Oracle copy

You can expire an Oracle copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Click the name of the database you prefer in the Name column.
5. Select the copy you want to expire, then click **More > Expire**.
6. Click **OK**.

Enable or disable expiry of an Oracle copy

You can enable or disable expiry of a copy during rotation using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Click the name of the database you prefer in the Name column.
5. Select the copy that you want to enable or disable and click **More**.
6. Click one of the following options depending on the action you want to perform:
 - **Enable Copy Rotation:** To enable automatic expiry of a copy during rotation.
 - **Disable Copy Rotation:** To disable automatic expiry of a copy during rotation.
7. Click **OK**.

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 28 Console field descriptions

Field in UI	Description
RMAN user	Catalog owner

Table 28 Console field descriptions (continued)

Field in UI	Description
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%
Customize initialization Parameters	This field will be blank. You can fill in one parameter per line, for example, memory_target=629145600
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 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 during copy creation.

Mount on standalone server and prepare scripts for manual database 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 on server:** This field is used to specify the host where you want to mount the Oracle copy.
- **Mount on 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%`. The length of the database name is eight characters.
- **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%`. The length of the SID name is 16 characters and the length of the RAC SID is 15 characters.
- **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 that 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 Grid Cluster and recover as RAC database

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.
- To mount to an Oracle Flex ASM cluster, ensure that all nodes are accessible and the cluster services are online. The recovery operation will fail if any node in the cluster is offline.

- **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%`. The length of the database name is eight characters.
- **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%`. The length of the SID name is 16 characters and the length of the RAC SID is 15 characters.

Note: For RAC mounts, each node in the cluster receives a unique instance name, postfixed by a 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.

Path mapping

The path mapping option mounts the copy to a host using a path mapping table set to user-defined locations. When you use a path mapping table, you have more control over where data is located.

You must specify the path where you want to mount a specific file system. You must provide a path map where the source file system and the target mount point is specified.

The following is a sample path mapping table for Windows.

The first two target paths, `G:\` and `H:\` drives must already be available on the mount host. That is, the root drive for the mount path must pre-exist before attempting a mount.

Source file system	Target mount path
D:\Test1	G:\Test1
E:\	H:\Test2
F:\Test3	I:\
L:\	N:\

Note:

- If a target path is not provided for a source path, then it is mounted to a path same as the source path on the mount host.
- Ensure that you type in the absolute mount path on the target host. If the path is invalid, mount fails.
- Mount copy overrides is unavailable, if you select the mount path as Mapped path.

- For Windows, if one of the entered path is invalid, VSS import fails. Therefore, the entire mount fails. Partial failed scenarios are not supported for Windows mount.
- For Windows and NFS file systems on Unix, nested target mount points are not supported.
- Path Mapping is not applicable to metadata paths for Microsoft Exchange and Microsoft SQL Server.

Specify path mapping settings

You can specify the path where you want to mount a specific copy.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange**.
4. Navigate to the folder that contains the copies.
5. Select the copy you want to mount, then click **MOUNT COPY**.
6. In the **Mount Copy** options, under the **Specify Mount Settings** section:
 - a. Select the mount host.
 - b. From the **Mount on Path** list, select **Mapped Path**.

The Path Mapping Settings link appears.

7. Click on the link to open the Path Mapping Settings window.
8. From the **Select Source Host** list, select a host.

All the file systems on the selected host are displayed in the source path column.

9. Specify the target path.
10. Click **Save** to save your settings.

If you want to set the target path for a file system on another source host, repeat steps 8 to 10.

11. Click **Reset**, to clear all the entered target paths for the selected source host.
12. Click **OK** to exit the Path Mapping window.

Note: If you change the path mapping settings, the earlier saved path mapping settings is not valid and the new path mapping settings takes precedence. Therefore, ensure that you save the path mapping settings for all the hosts before changing it.

Retry recovery of a mounted and recovered Oracle copy

You can retry recovery on a mounted and recovered copy without having to unmount and remount the copy.

Before you begin

This operation requires the Data Administrator role in AppSync.

About this task

Use this feature to:

- Retry a failed recovery

- Retry recovery with new recovery options such as database rename

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. Navigate to the folder that contains the copies.
5. Select a copy, and click on **Retry Recovery**.
The Retry Recovery of Mounted Oracle Copy wizard appears.
6. Select a copy, and click **NEXT**.
7. Under **Recovery Settings**, review the default settings and make the required changes.
8. Click **NEXT**.
9. Review the summary details, and click **FINISH**.

Restore an Oracle copy

You can perform a restore of an Oracle copy using the Appsync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Note:

- If a copy is mounted or recovered with database rename, it is not recommended to use this copy for restore.
- Ensure that no virtual machine snapshots are present before protecting a datastore. If virtual machine snapshots are present, protection succeeds, but AppSync fails to perform a file or virtual machine restore.
- Oracle restore fails, if the volume group where Oracle database resides has LVMs being used for other purposes, and is not protected by AppSync .

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. In the Name Column, click the desired database that contains the copy.
5. Select the copy that you want to restore and click **More > Restore**.

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.

6. In the **Select a Copy** page, select the copy you want to restore and click **NEXT**.
7. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

-  **Note:** You can perform this step only if you have multiple applications that share the same LUN or file systems.

8. Click **NEXT**.
9. Click the Restore drop-down list and select one of the following options to restore:
 - a. For Non-Container Database, select **Data, Archive logs**, or **Both Data and Archive logs**.
 - b. For Container Database (CDB), select **CDB and PDB, Archive logs, CDB, PDB and Archive logs**, or **PDB**.

If the database being restored affects any other database or file system, you might receive an affected entity warning message.

10. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.
 - ⓘ **Note:** In the case of SnapVX/XtremIO Snap/PowerStore Snap mounted copies, when you perform restore, AppSync restores the data from the snapshots created on the array to the source devices, or from linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).
 - **Restore from snapshot:** Restores copies from original snapshots.
 - **Restore from changed data:** Restores from the linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).
11. Click **NEXT**.
12. In the **Review** page, review the restore options and click **FINISH**.

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.

- ⓘ **Note:** You must manually restart the Oracle database after restore. To start the database, run the following commands:

```
Export ORACLE_SID=<SID>
Sqlplus /nolog
Connect / as sysdba
Startup
```

Restore a standalone local copy

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.

4. In the Name Column, click the desired database that contains the copy.
5. Select the copy that you want to restore and click **More > Restore**.
The Oracle Restore wizard launches.
6. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

 **Note:** You can perform this step only if you have multiple applications that share the same LUN or file systems.

7. Click **NEXT**.
8. Click the Restore drop-down list and select one of the following options to restore:
 - a. For Non-Container Database, select **Data, Archive logs, or Both Data and Archive logs**.
 - b. For Container Database (CDB), select **CDB and PDB, Archive logs, CDB, PDB and Archive logs, or PDB**.

If the database being restored affects any other database or file system, you might receive an affected entity warning message.

9. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.
10. Click **NEXT**.
11. In the **Review** page, review the restore options and click **FINISH**.

Results

After the restore (not applicable for Pluggable Database):

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
```

After Granular restore of Pluggable Database, execute below command :

```
BEGIN
DBMS_PDB.RECOVER (
pdb_descr_file => '/tmp/new_pdb1.xml',
pdb_name => 'clone_pdb1',
```

```

filenames => '/vmax_cdb_pdb/VMAXCDB/853D854C721B44C3E053DABAF70A318D_bkp/cold'
);
END;
/

```

Once above commands are executed, perform the below steps to recover the PDBs:

1. SQL> CREATE PLUGGABLE DATABASE PDB01 USING '/tmp/file.xml' NOCOPY
TEMPFILE REUSE;
2. RMAN> Recover pluggable database PDB01;
3. SQL>alter pluggable database PDB01 open;**

When PDB is not dropped, perform the below steps:

1. RMAN> Recover pluggable database PDB01;
2. SQL>alter pluggable database PDB01 open;

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 the options. This will determine the level to which affected entities are determined.

Below are the options for Non-CDB database:

- Data only
- Archive Logs only
- Data and Archive Logs

For CDB database, options are :

- CDB and PDB
- Archive Logs
- CDB, PDB, and Archive Logs
- PDB

Affected entities only display according to the restore option. If you select, **Data (CDB and PDB)**, 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 (CDB and PDB)** 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 you select PDB, then filesystems and storage for selected PDB are used for checking affected entities. AppSync does not use Oracle CDB, Archive Log, and PDBs storage (that are not selected for restore) for checking 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, if the databases are in the same consistency group they become *affected entities* when the other database is protected.
- For VNX, Unity, PowerStore, VMAX V2, VMAX3/PowerMAX, and XtremIO if the databases are on the same LUN they become *affected entities* when the other database is protected.
- For Unity, if the databases are in the same consistency 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.
- For PowerStore, while restoring from remote copy, if the databases are in the same volume group and the replication session is created for volume group, they become *affected entities* when another database in the group is protected.

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 determines affected entities (databases or file systems) for the consistency groups, volume 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, volume 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, volume 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.

Oracle Pluggable Database

- Affected entities are reported at the CDB level only if the PDBs of two CDBs overlap.
- AppSync does not support configurations where the PDB of one CDB, shares the same filesystem with the archive logs/FRA of a different CDB.

PDB Granular Restore

Affected Entities page displays the details as below:

- PDBs that are not in the restore list and that are on same FS or DG.
- Same or different CDB on PDB FS, that has to be restored on FS or DG.
- If PDB is renamed, that PDB is shown as affected entity. You must acknowledge that PDB is renamed and proceed with 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 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>`
4. Disable all impacted ASM disk groups as grid user: `grid>srvctl disable diskgroup - diskgroup <dg_name> [-node "<node_list>"]`

 **Note:** This step is applicable for release 12cR2 or later versions of Oracle Database.

On the restore node, perform the restore. Follow these steps:

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle**.
4. In the Name Column, click the desired database that contains the copy.
5. Select the copy that you want to restore and click **More > 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.

6. Under the Restore drop-down list, select one of the following options along with a specific RAC node to perform the restore:
 - a. For Non-Container Database, select **Data, Archive logs, or Both Data and Archive logs**.
 - b. For Container Database (CDB), select **CDB and PDB, Archive logs, CDB, PDB and Archive logs, or PDB**.
7. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

Note: You can perform this step only if you have multiple applications that share the same LUN or file systems.

8. Click **NEXT**.
9. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.
10. Click **NEXT**.
11. In the **Review** page, review the restore options and click **FINISH**.

Results

After the restore (not applicable for Pluggable Database) :

1. Remount the disk groups on the remote nodes as grid user: `grid> asmcmd mount <DG>`.
2. Enable the asm disk groups on the remote node as grid user: `grid>srvctl enable diskgroup -diskgroup <dg_name> [-node "<node_list>"]`
Note: This step is applicable for release 12cR2 or later versions of Oracle Database.
3. On any node, perform recovery of the restored database using redo or archive with resetlogs:
`Oracle > startup mount`
`Oracle > recover database`
4. Open the database on the recovery node:
`Oracle > alter database open`
5. Bring up the instances on the additional nodes:
`srvctl start instance -d <RACDB> -i <DbInstanceOnRemoteNodes>`
6. Repeat steps 2 and 3 to recover affected database <RACDB2>
7. Bring up affected database <RACDB2>

After Granular restore of Pluggable Database, execute the below command:

```
BEGIN
DBMS_PDB.RECOVER (
  pdb_descr_file => '/tmp/new_pdb1.xml',
  pdb_name => 'clone_pdb1',
  filenames => '/vmax_cdb_pdb/VMAXCDB/853D854C721B44C3E053DABAF70A318D_bkp/cold'
);
END;
/
```

Once above commands are executed, perform the below steps to recover the PDBs:

1. SQL> CREATE PLUGGABLE DATABASE PDB01 USING '/tmp/file.xml' NOCOPY
TEMPFILE REUSE;
2. RMAN> Recover pluggable database PDB01;
3. SQL>alter pluggable database PDB01 open;**

When PDB is not dropped, perform the below steps:

1. RMAN> Recover pluggable database PDB01;
2. SQL>alter pluggable database PDB01 open;

CHAPTER 8

Protect File Systems

This chapter includes the following topics:

• Overview of File System support	220
• File system service plan details	225
• Subscribe a File System to a service plan	229
• Unsubscribe File Systems from a service plan	230
• Create a File System copy	230
• Create File System repurpose copies	231
• Create second generation copies	233
• Overriding service plan schedules	234
• Mount a copy using the File System Mount wizard	234
• Restore a Filesystem copy	241

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

Note:

- AppSync does not support file systems on Linux operating system devices which are not full block devices (such as /dev/sdc) or primary first partition (such as /dev/sdc1).
- AppSync does not support volume groups containing both partition and non-partition devices. All devices in any volume group must be part of the same category.

Hyper-V support

In Hyper-V environments, AppSync requires the storage for File systems to be on iSCSI direct attached devices, Virtual Fiber Channel (NPIV), or SCSI pass-through devices. SCSI Command Descriptor Block (CDB) filtering must be turned off in the parent partition for SCSI pass-through. It is turned on by default.

For Hyper-V SCSI pass-through, the mount host cannot be a Hyper-V host it has to be a physical host or a virtual machine added with Virtual Fiber Channel adapter or iSCSI direct attached.

Resilient File System (ReFS) support

AppSync can discover, protect, mount, and restore ReFS file systems, and AppSync supported standalone and clustered applications residing on ReFS file systems.

Repurposing is supported for ReFS file systems and for SQL server databases on ReFS. Storage spaces are not supported.

Protect NFS file systems on VNX and Unity storage

Learn how AppSync supports protection of NFS file systems on VNX and Unity File storage.

AppSync supports protecting NFS file systems on Linux (RHEL, SUSE, and OEL) and AIX. You can use these copies for operational recovery.

 **Note:** You can protect Linux file systems located on vDisks from VMWare VMFS or NFS datastores.

In the case of service plans configured for VNX file 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 a VNX 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.

Unity file snap only supports local (Bronze) copies. AppSync can create copies for file system on an Oracle database for Bronze service plan.

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 that the array status is OK.

File System Hosts list

The list contains File System hosts that have been discovered and stored in the AppSync database.

Clicking the name of a host will display the Host File Systems within it.

Each entry shows the host name, virtual machine, virtual server, cluster, version, plug-in version, and last discovery details.

File system page

The File system page lists all the available file systems that are discovered for the selected server instance.

Click on a file system name to display copies of the file system.

File system 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 file systems can be subscribed to multiple service plans.
- Storage size in GB
- Send alerts to (if requested)

You can select one or more file systems to protect at one time. Click **SELECT ALL** to protect all the file systems on this page (except a file system C:\ which contains host system information).

File system Copies Page

In this page you can view the list of file system 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, expire, refresh or repurpose copies.

File System copies list

The list contains File System copies that have been discovered and stored in the AppSync database.

You can also see details of a copy from the Copies tab of the Service Plan.

In the File system Copies page all the copies which are protected as part of a service plan are listed. From the Copies page, you can select to mount, restore, expire, refresh or repurpose copies.

Each entry shows the protection status, name, subscribed service plans, mount status, copy type, generation, automatic expiration, label, file system consistence, source, storage system, and site details.

Column	Description
Status	Green: successful Yellow: Completed with errors Red: failed
Copy Name	Date and time when the copy was created
Service Plan	Name of the service plan that is associated with the copy. For repurposed copies, a Repurpose link displays in this column. Click this link to edit the Service Plan for 1st or 2nd generation copies.  Note: In the service plan for repurposed copies, the options to schedule and mount overrides will be disabled.
Label	Common name that is used to help identify repurposing copies
Mount Status	Hostname to which the copy is mounted, or Not Mounted
Mount Type	If copy is mounted as part of service plan run, value for Mount Type is ServicePlan. If copy is mounted as OnDemand, value for Mount Type is OnDemand.
Copy Type	Replication technology that is used to create the copy: CLR Bookmark, CDP Bookmark, CRR Bookmark, VNXSnap, VPSnap, TFClone, XtremIO Snapshot and VPLEXSnap. The copy can be one of the following types: <ul style="list-style-type: none"> RecoverPoint Continuous Data Protection Bookmark RecoverPoint Continuous Remote Replication Bookmark Unity Snap VMAX V2 Snap, VMAX V2 Clone XtremIO snapshot VMAX3/PowerMAX SnapVXClone, SnapVXSnap VPLEX Snap, VPLEX Clone DELLSC Snap PowerStore Snapshot PowerStore Thin Clone
Generation	The generation number of the repurposed copy

Column	Description
Source	The original source database for the copy, or source copy for the copy
Site	Site where the copy is located.
Storage System	Storage system where the copy resides.
Automatic Expiration	Determines whether automatic expiration is enabled or disabled for the selected copy.
File system consistence	The type of consistence configured for the copy.
<i>The following additional details are displayed in the Service Plan Copies tab:</i>	
Backup Type	Displays the type of backup selected for the copy
Servers	Displays the server information of the selected copy.

PowerHA (HACMP) cluster integration

AppSync can protect file systems residing in a PowerHA cluster environment.

AppSync protects applications on the node where the resource group is available at the time of a service plan run. AppSync relies on the service label IP (virtual IP) of the resource group to create copies or restore across failovers. All the nodes to which clustered file systems can fail over must be registered with AppSync before registering the resource group's service label IP.

Consider the following when protecting an application that fails over as part of a PowerHA cluster:

- The nodes of the PowerHA cluster must be registered with AppSync before registering the service label IP.
- The service label IP/name must be configured in the resource group for the clustered application.
- If a failover occurs while running a replication or restore process, the operation fails. Node failover must occur before running the service plan, or at the start of a restore.
- Each resource group must have a unique service label IP and that must be registered with AppSync for failover awareness.
- File systems that belong to a particular resource group can be discovered and protected only if the corresponding service label IP is registered with AppSync.
- Callout scripts must be present on both the nodes of a PowerHA cluster.
- Clustered file systems must be discovered and subscribed by using the service label IP/name and not through the physical nodes.

Mount considerations

- Mount to the original path is not supported on any of the nodes of the production PowerHA cluster.
- The AppSync host plug-in must be installed on the mount host.
- Mount is only supported in a standalone mode. Cluster mount is not supported.
- Appsync supports the Quality of Service feature for XtremIO release 6.2 and later.

Restore in a PowerHA environment

Perform a restore. After a restore, the volume group is not concurrent. You must manually make them concurrent before performing a host or file system rediscovery.

Note: Restore of mounted copies is not supported for applications (File System and Oracle databases), managed by AIX HACMP or PowerHA cluster.

Post restore procedure in a PowerHA environment

Learn how to perform manual steps with a restore in a PowerHA environment after a restore.

About this task

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 the file system.
2. Type the `varyoffvg` command.
3. Type the `varyonvg` command with `-c` option (to make it concurrent).

Verification:

The `lspv` command must 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
```

4. Add the file system back to the resource group.
5. Verify and synchronize the configuration.

Windows failover clustered file systems

AppSync can protect file systems residing in a Windows failover cluster environment.

AppSync protects applications on the node where the resource group is available at the time of a service plan run. AppSync relies on the network name resource (virtual IP) of the resource group to create copies or restore across failovers. All the nodes to which clustered file systems can fail over must be registered with AppSync before registering the resource group's network name resource (virtual IP).

Consider the following when protecting an application that fails over as part of a Windows failover cluster:

- The nodes of the Windows failover cluster must be registered with AppSync before registering the network name resource (virtual IP).
- If a failover occurs while running a replication or restore process, the operation fails. Node failover must occur before running the service plan, or at the start of a restore.
- Each role in Windows failover cluster must have a unique network name resource (virtual IP) and that must be registered with AppSync for failover awareness.

- File systems that belong to a particular role in Windows failover cluster can be discovered and protected only if the corresponding network name resource (virtual IP) is registered with AppSync.
- Callout scripts, if applicable must be present on all the nodes of a Windows failover cluster.
- Clustered file systems must be discovered and subscribed by using the network name resource (virtual IP).

For mount, AppSync mounts the clustered disk by adding it in the Cluster Resource Group associated with the virtual Server IP, but adds dependency on the disk based on the below scenarios:

- If there are no services associated with the virtual IP, then no dependency is added on to the disk.
- If there is a service associated with the virtual IP, but does not have any dependency on any clustered disk, then no dependency for that service is added on to the disk.
- If there is a service associated with the virtual IP and has a dependency on at least one disk, then the newly added disk is added as dependency to the service.
- If there are more than one service and both have dependency on the disks, then any one of them is chosen randomly and made dependent onto the disk.

 **Note:** In a Windows cluster environment, AppSync agent port must be the same across all the nodes participating in the cluster. Otherwise, AppSync operations fail.

File system service plan details

Use this table to learn file system service plan details.

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 a Copy step varies among plans. The following table summarizes the service plan details:

This table describes the File System service plan details.

Table 29 File System Service Plan details

Name	Description
Service Plan Name	Type of service plan.
Description	Describes the function of the service plan.
Service Plan State	Specifies if the service plan is enabled or disabled.
Copy Location	Specifies if the location is local, remote, or local and remote.
Mount Copy	Specifies the following options for mounting a copy: <ul style="list-style-type: none"> • No • Yes • Yes - Keep it mounted (Previous copy will be unmounted) • Yes - Mount the copy, but after the post mount scripts run, unmount the copy
Retention	Specifies the configured copy retention number.
Schedule	Specifies the recurrence type that is configured for the service plan.
Advanced plan settings	Specifies if the Enable callout script is enabled or disabled. By default, this option is enabled. Clear Enable CallOut Scripts to disable call out scripts.

Table 29 File System Service Plan details (continued)

Name	Description
	<p> Note: For repurposing, if you want to disable callout scripts during refresh, edit the repurpose plan and then clear Enable CallOut Scripts under service plan settings.</p>
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 servers are filtered out.
Mount with access	Type of access the copy should be mounted with.
Mount on path	<ul style="list-style-type: none"> • 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. • Select Mapped Path to specify the path where you want to mount the database.
Quality of Service Policy	For XtremIO only, the Quality of Service policy option appears in the wizard. You can select the desired type of Quality of Service policy while mounting a copy.
Unlink the SnapVX snapshots in unmount	Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
Desired SLO	For VMAX3/PowerMAX arrays only, a setting called Desired Service Level Objective (SLO) appears in the Mount wizard and specifies the required VMAX3/PowerMAX Service Level Objectives. SLO defines the service time operating range of a storage group.
Image access mode (during RecoverPoint mount)	<ul style="list-style-type: none"> • 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 V2, 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 V2 and RP XtremIO is not supported.
Use Dedicated Storage Group	<ul style="list-style-type: none"> • 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 V2 , VNX storage group, PowerStore host group or XtremIO initiator group for a mount. (A dedicated VMAX V2 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.

Table 29 File System Service Plan details (continued)

Name	Description
	<p>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.</p> <ul style="list-style-type: none"> If unchecked, AppSync does not enforce the use of a dedicated storage group for a mount. <p>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.</p>
Desired FAST	Select the FAST policy. This is only applicable for VMAX V2 arrays.
VPLEX Mount option	<ul style="list-style-type: none"> Native array: Use this option if you want to mount the copy as native array volumes. VPLEX virtual volume mount: Use this option if you want to mount the copy as VPLEX virtual volumes. Enable VMware cluster mount:
Enable VMware cluster mount	<ul style="list-style-type: none"> Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled. If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. This option is supported on VPLEX, XtremIO, VMAX3/PowerMAX, VMAX All Flash, PowerStore, and Unity arrays. If this option is not selected, and the mount host is part of an ESX cluster, the mount host must have a dedicated storage group, storage view, or initiator group configured according to the storage system configuration. This enables AppSync to mask LUNs only to that mount host.
Disable VMWare SRM	Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
VMware Virtual Disk Mode	<p>Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.</p> <ul style="list-style-type: none"> Enable VMWare Virtual Disk Mode and select Persistent to mount the copy in an independent persistent mode. Enable VMWare Virtual Disk Mode and select Non Persistent to mount the copy in an independent non persistent mode <p>Note: AppSync does not support:</p> <ul style="list-style-type: none"> Protection of applications created on independent non persistent virtual disk. Mounting application copies to a virtual server or shared instance (such as SQL Failover cluster and Oracle RAC) as independent non persistent disk.
Select the cluster/ arrays in preferred order for VPLEX metro configuration	In the Select the cluster and arrays in preferred order for VPLEX metro configuration section, you can drag and drop the arrays to change array preference.

Table 29 File System Service Plan details (continued)

Name	Description
Allow Unmount Of On Demand Mounted Copy	Allows you to unmount a copy that was mounted on-demand.
Pre-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on Production host before creating a copy in AppSync.
Post-copy script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after creating a copy in AppSync.
Post-mount script	Allows user to specify the name of the script and credentials with which the script has to be executed. This script is executed on selected host after the copy is mounted by the service plan run.
Run Filesystem Check	<p>During a mount operation, the AppSync agent checks file system data consistency by executing the <code>fsck</code> command. This operation can be time consuming. You can clear this option to skip file system check during a mount operation. By default, file system check is enabled.</p> <p> Note: In the case of a restore operation, the <code>Run Filesystem Check</code> option is enabled by default. You cannot disable it.</p>
Copy to mount	<p>Allows user to select if the local or remote copy has to be mounted as part of service plan run.</p> <p> Note: Applies to service plans that create local and remote copies simultaneously.</p>
Create Copy details	
Copy Priority	<ul style="list-style-type: none"> • Specifies if the Snapshot, Clone, Bookmark, or all three options are selected. • Allows you to order, select, or clear copy priority. By default, all the options are selected. You cannot clear all the preferences, at least one preference must be selected.
Unix Filesystem Consistency	<ul style="list-style-type: none"> • FS Consistent - If you select this option, the file system is frozen during copy creation. This pauses writes on the file system. You can create UNIX file system consistent copies using the UNIX <code>fsfreeze</code> utility. • Crash Consistent - This is the default option. In this case, the file system is not frozen during copy creation.
Wait for VMAX3/ PowerMAX clone sync to complete	Allows you to specify if AppSync must wait for the clone sync to complete for VMAX3/ PowerMAX Arrays.
Select Storage Groups for VMAX-3 Array(s)	Select the preferred storage groups to use if you are configuring VMAX3/PowerMAX arrays.
Select Storage Pools to be used for VMAX-2 Array(s)	Select the preferred storage pools to use if you are configuring VMAX V2 arrays.
VSS Retry Count	Specifies the number of times the VSS retry option is run. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry count.

Table 29 File System Service Plan details (continued)

Name	Description
VSS Retry Interval(In Seconds)	Specifies the timeframe (in seconds) between VSS retries. During protection, if a service plan fails because of VSS failures such as VSS timeout issue, the service plan runs the VSS freeze or thaw operation again based on the specified retry interval.

Discover File Systems

Perform this procedure to update the file systems known to AppSync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **FILE SYSTEMS**.
4. Click **Discover HOSTFILESYSTEMS**.
5. Select the desired server and click **OK**.

Subscribe a File System 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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **File Systems**, and click on a Windows or UNIX host.
4. Select the checkbox against the desired file system.
5. Select the checkbox for one or more File Systems, and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select the appropriate option.

Option	Description
Subscribe to Service Plan and Run	To subscribe the file system for protection and run the plan immediately for any selected file systems.
Subscribe to Service Plan (with option to override)	To subscribe the file system for protection. Protection for all file systems that are part of the service plan is executed at the scheduled time.

8. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold
9. Click **OK**.
10. Click **NEXT** to review your selection.
11. Click **FINISH**.

Unsubscribe File Systems 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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **FILE SYSTEMS**.
4. Click on a Windows or UNIX host.
5. Select the checkbox against the desired file system.
6. In the Name Column, click the desired file system. Select the file system you want to unsubscribe, and click **More > UNSUBSCRIBE**.
7. In the Unsubscribe dialog, select the service plan and click **OK**.

 **Note:** You can also unsubscribe applications from a service plans, from the Service Plan page.

Create a File System copy

Create a copy of a file system by subscribing it to an AppSync service plan.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **FILE SYSTEMS**.
4. Click on a Windows or UNIX host.
5. Select the checkbox against the desired file system.
6. Select one or more File Systems, and then click **CREATE COPY WITH PLAN**.
7. Select the purpose as **Data Protection**.
8. Select the appropriate option.

Option	Description
Subscribe to Service Plan and Run	To subscribe the file system for protection and run the plan immediately for any selected file systems.
Subscribe to Service Plan (with option to override)	To subscribe the file system for protection. Protection for all file systems that are part of the service plan is executed at the scheduled time.

9. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold
10. Click **OK**.
11. Click **NEXT** to review your selection.
12. Click **FINISH**.

Create File System repurpose copies

You can create first generation or second generation repurpose copies in Appsync.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. Click on a Windows or UNIX host.
5. In the Host Name Column, click the desired file system and click **Create Copy With Plan**.
6. In the Subscribe to Existing Service Plan page, select **Data Repurposing > Next**.
7. Define the following properties for the copy:
 - a. The **Service Plan Name** field is defined by default.
 - b. The **Description** field provides a brief description of the copy.
 - c. The **Copy Label** field provides an autogenerated label for the copy.
 - d. The **Copy Location** list allows you to select a copy location either to **Local** or **Remote**.
 - e. The **Mount Copy** list allows you to select mount options for the copy. You can configure this option to either **No**, **Yes**, **Yes - Keep it mounted** (where the previous copy will be unmounted), or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.
 - f. Configure the **Use bookmark to copy** option.
 - g. The **2nd Generation Copies** list allows you to select either **Yes** or **No**.
 - h. The **Advanced plan settings** option allows you to Enable CallOut Scripts. If you enable this option, you must set the value of the **Callout timeout** field in minutes.

8. Click **Next**.
9. In the Create the Copy page, to specify the storage and copy options to create the copy, do the following:
 - a. Configure the **Unix Filesystem Consistency** option to select either **Filesystem Consistent** or **Crash Consistent**.
 - b. Configure the **Retry Count** and **Retry Interval** settings under Advanced Plan Settings - VSS Retry Options.
 - c. Select the **Wait for VMAX3/PowerMAX clone sync to complete** option if you want to wait for VMAX3/PowerMAX clone sync to complete. This applies to VMAX3/PowerMAX only.
 - d. In the **Array Selection** section, click **Select an Array** to choose the preferred array from the list.

 **Note:** This is applicable only for SRDF/Metro.
 - e. In the **Select Storage Pools to be used for VMAX-2 Array(s)** section, select the preferred storage pools.
 - f. In the **Select Storage Groups to be used for VMAX-3 Array(s)** section, select the preferred storage groups.
 - g. In the **Select the cluster and arrays in preferred order for VPLEX metro configuration** section, you can drag and drop the arrays to change array preference.
 - h. Configure the Copy Type settings to either **Snapshot** or **Clone**.
10. Click **Next**.
11. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:
 - a. **File**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
12. Click **Next**.
13. In the Schedule/Run page, select one of the following scheduling options:
 - **OnDemand** - Creates a copy when you click **Finish** on this wizard.
 - **Schedule** - Creates a copy based on the specified recurrence type. On the first schedule, a repurposed copy is created, and on subsequent schedules, it refreshes the copy.
 - **Run Only Once At later time** - Creates a copy only once on the specified date and time.
14. Click **Next**.
15. In the Define the 2nd-gen Copy page, define the following properties for the 2nd-gen copies:
 - a. For the **2nd-gen Copies Label** field, enter the label of the copy.
 - b. For the **Mount 2nd-gen Copies** field, enter the label of the copy. You can configure this option to either **No**, **Yes - Keep it mounted** (where the previous copy will be unmounted), or **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**.

- c. Configure the **2nd-gen Copies Type** to either **Snapshot** or **Clone**.
16. In the **Scripts for 2nd-gen Copy** page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:
 - a. **File**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
17. Review the repurpose copy creation settings and click **FINISH**.

Create second generation copies

Perform this procedure to create a second-generation copy from a first-generation existing copy.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **File Systems**.
4. In the Name Column, click the host name.
5. Click the file system that contains a first-generation copy.
6. Select a first-generation copy, and then click **CREATE 2ND GEN COPY**.

The **Create 2nd-gen Copy** widget opens.

7. In the **Define the 2nd-gen Copy** page, configure the following:
 - a. `2nd-gen copies label` - Specify a label for the copy.
 - b. `Mount 2nd-gen copies` - Configure this field to one of the following options:
 - **No**
 - **Yes**
 - **Yes - Keep it mounted(Previous copy will be unmounted)**
 - **Yes - Mount the copy, but after the postmount scripts run, unmount the copy**
 - c. `2nd-gen copies type` - Configure this field to one of the following options:
 - **Snap**
 - **Clone**
8. Click **NEXT** to review your selection.
9. In the **Scripts for 2nd-gen Copy** page, select the pre-copy scripts and post-copy scripts you want to run.

 **Note:** This step also displays the post-mount scripts if you selected the mount option.
10. Click **NEXT** to review your selection.
11. In the **Schedule** page, select one of the following options:

- **Run now**
 - **Run Recurrently As Per Schedule**
 - **Run Only Once At Later Time**
12. Click **NEXT** to review your selection.
 13. Review the configurations for the second-generation copy and click **FINISH**.

Overriding service plan schedules

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

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **File Systems**.
4. Click on a Windows or UNIX host.
5. In the Host Name Column, click the desired host.
6. Select the checkbox for one or more File Systems, and then click **CREATE COPY WITH PLAN**.
7. Select the purpose as **Data Protection**.
8. Select **Subscribe to Service Plan (with option to override)**.
9. Select the service plan that you want to subscribe to.
10. Click **NEXT**.

The Override Schedule page appears.

11. Select one or more databases and click **OVERRIDE SCHEDULE**.
12. Specify 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 file systems.

13. Click **NEXT** to review your selection.
14. Click **FINISH**.

Mount a copy using the File System Mount wizard

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

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. In the Host Name Column, click the desired Host File System.
5. Select the copy you want to mount and click **MOUNT**.

If multiple databases were protected together, you may see the additional copies to mount option. Select the copies you prefer and click **NEXT**.

6. In the Select a Copy page, select a copy and click **Next**.
7. In the Select Mount Options page, under **General Settings**, do the following:
 - a. From the **Mount on Server** list, select the server on which to mount the copy.
 - b. From the **Mount with access** list, select the type of access the copy must be mounted with: **Read-only** or **Read-write**.
 - c. From the **Mount Location** list, select a mount path location either **To original path**, **Mount to alternate path**, or **Mapped Path**. 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.
 - d. In case the selected copy is a RecoverPoint bookmark, from the **Image access mode** list, select one of the following 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 V2, 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 V2 and RP XtremIO is not supported.
 - e. For VMAX3/PowerMAX arrays, from the **Desired SLO** list, select the desired Service Level Objective (SLO) for the mount copy.

 **Note:** The SLO values are dynamically fetched from the VMAX3/PowerMAX arrays, and only the unique values are displayed.
 - f. For XtremIO 6.2 and later, click the **Quality of Service policy** option to select the desired Quality of Service policy while mounting a copy.
 - g. For VMAX3/PowerMAX SnapVxSnap, select the **Unlink the SnapVX snapshots in unmount** option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
 - h. **Run Filesystem Check:** During a mount operation, the AppSync agent checks file system data consistency by executing the `fsck` command. This operation can be time consuming. You can clear this option to skip file system check during a mount operation. By default, file system check is enabled.

 **Note:** In the case of a restore operation, the `Run Filesystem Check` option is enabled by default. You cannot disable it.

- i. **VMware Settings:** Allows you to mount application copies on a virtual disk as independent disks. You can select this option to exclude virtual disks from snapshots created from the virtual machine. By default, this option is disabled, and copies are mounted in the persistent mode.
 - j. For VMAX V2 arrays, select the desired FAST policy for the mount copy.
 - k. Clear the **Use Dedicated Storage Group** option, if you do not want AppSync to enforce the use of a dedicated storage group for a mount. By default, this option is enabled.
 - l. From the **VPLEX Mount option**, select one of the following:
 - **Native array:** Use this option if you want to mount the copy as native array volumes.
 - **VPLEX virtual volume mount:** Use this option if you want to mount the copy as VPLEX virtual volumes.
 - **Enable VMware cluster mount:** Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled.
8. Click **Next** to review the mount options.
 9. Click **Finish**.

Changing the mount point for an affected file system

Follow this procedure to manually change the mount point for an affected file system.

About this task

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>`

Override mount settings in a service plan

If there are multiple file systems subscribed from different hosts 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.

About this task

 **Note:** Mount overrides are not supported for multiple file systems on the same host.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > File Systems**.
4. Click a service plan, and expand the right pane.
5. Click the **OVERRIDES** tab.
6. Select **Mount Overrides**.
7. Select an entry, and click **OVERRIDE MOUNT**.
8. Edit the required fields, and click **APPLY CHANGES** to save the settings.
9. To revert to default settings, select the file systems and click **Use Default Settings**.

Nested mount support for File systems

If a file system is mounted at a mount point `/a` and another file system (from the same volume group or a different volume group) is mounted at a mount point below `/a` such as `/a/b`, then `/a` and `/a/b` are considered as nested file systems because its mount point is a sub-directory of the parent file system.

You can mount and unmount nested file systems even if they are spread across volume groups.

It is recommended that you avoid creating circular nested file systems across volume groups such as the following because mount, unmount, and restore operations fail even if protection succeeds.

- `/a` in volume group 1
- `/a/b` in volume group 2
- `/a/b/c` in volume group 1

Instead, do one of the following:

- Create the file system layout in the following manner:
 - `/a` in volume group 1
 - `/a/b` in volume group 2
 - `/a/b/c` in volume group 3
- Create all nested file systems in one volume group

Note:

- Supported only on UNIX platforms.
- NFS file systems are not supported in nested layouts.
- All the file systems from a single volume group must be mounted and unmounted together. Otherwise, the second mount of a file system fails, if another file system is already mounted from that volume group. Even in the case of non-nested file systems in a volume group such as `/a` and `/b`, if `/a` is mounted, then the second mount of `/b` fails.

Mounting a UNIX file system after reboot

When an AppSync protected file system copy is mounted on to the mount host, AppSync automatically modifies the mount point related entries in the `/etc/fstab` file for Linux hosts. The AppSync agent modified entries in the `/etc/fstab` file is followed by a comment `- #` line added by AppSync Agent. The file system remains mounted even if the mount host reboots after a file system mount operation.

The following is an example of the `/etc/fstab` entry on a Linux host:

```
/dev/aps_1datavg_51fd06a41290/data1v    /appsync-mounts/oracle_mounts/
dl          ext4          rw,nofail,_netdev          0 0 # line added by AppSync Agent
```

On an AIX host, when a file system copy is unmounted, the entries are removed from the `/etc/filesystem` file.

The following is an example of the `/etc/filesystem` entry on an AIX host:

```
/appsync-mounts/symm1:
dev          = /dev/APM1v02
vfs          = jfs
log          = /dev/APMloglv27
mount       = true
check       = false
options     = nodev,rw
account     = false
```

Note: To automatically mount a file system after a production host reboot, ensure that the value of `mount` is set to `TRUE` for the production file system. For file systems created using `crfs` or `smitty`, the automatic mount option is turned to `TRUE` by default. You can check `/etc/filesystems` and verify if the `mount` flag is set to `TRUE`, which allows a reboot.

Unmount a File System copy from the Copies page

You can unmount a File System copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. In the Host Name Column, click the desired Host File System.
5. In the Name Column, click the server folder that contains the copies.
6. Select the copy you want to unmount and click **Unmount Copy**.
7. Click **OK**.

Unmount a File System copy from the Service Plan page

You can unmount a File System copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.

3. Click **Select Application > File Systems**.
4. Click the name of the service plan you prefer in the Service Plan column.
5. Select the copy you want to unmount and then click **Unmount**.
6. Click **OK**.

Enable or disable a File system copy

You can enable or disable expiry of a copy during rotation using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. In the Host Name Column, click the desired Host File System.
5. In the Name Column, click the folder that contains the copies.
6. Select the copy that you want to enable or disable and click **More**.
7. Click one of the following options depending on the action you want to perform:
 - **Enable Copy Rotation:** To enable automatic expiry of a copy during rotation.
 - **Disable Copy Rotation:** To disable automatic expiry of a copy during rotation.
8. Click **OK**.

Expire a File system copy

You can expire a File System copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. In the Host Name Column, click the desired Host File System.
5. In the Name Column, click the folder that contains the copies.
6. Select the copy that you want to expire and click **More > Expire**.
7. Click **OK**.

Path mapping

The path mapping option mounts the copy to a host using a path mapping table set to user-defined locations. When you use a path mapping table, you have more control over where data is located.

You must specify the path where you want to mount a specific file system. You must provide a path map where the source file system and the target mount point is specified.

The following is a sample path mapping table for Windows.

The first two target paths, G:\ and H:\ drives must already be available on the mount host. That is, the root drive for the mount path must pre-exist before attempting a mount.

Source file system	Target mount path
D:\Test1	G:\Test1

Source file system	Target mount path
E:\	H:\Test2
F:\Test3	I:\
L:\	N:\

Note:

- If a target path is not provided for a source path, then it is mounted to a path same as the source path on the mount host.
- Ensure that you type in the absolute mount path on the target host. If the path is invalid, mount fails.
- Mount copy overrides is unavailable, if you select the mount path as Mapped path.
- For Windows, if one of the entered path is invalid, VSS import fails. Therefore, the entire mount fails. Partial failed scenarios are not supported for Windows mount.
- For Windows and NFS file systems on Unix, nested target mount points are not supported.
- Path Mapping is not applicable to metadata paths for Microsoft Exchange and Microsoft SQL Server.

Specify path mapping settings

You can specify the path where you want to mount a specific copy.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange**.
4. Navigate to the folder that contains the copies.
5. Select the copy you want to mount, then click **MOUNT COPY**.
6. In the **Mount Copy** options, under the **Specify Mount Settings** section:
 - a. Select the mount host.
 - b. From the **Mount on Path** list, select **Mapped Path**.

The Path Mapping Settings link appears.

7. Click on the link to open the Path Mapping Settings window.
8. From the **Select Source Host** list, select a host.

All the file systems on the selected host are displayed in the source path column.
9. Specify the target path.
10. Click **Save** to save your settings.

If you want to set the target path for a file system on another source host, repeat steps 8 to 10.
11. Click **Reset**, to clear all the entered target paths for the selected source host.
12. Click **OK** to exit the Path Mapping window.

- Note:** If you change the path mapping settings, the earlier saved path mapping settings is not valid and the new path mapping settings takes precedence. Therefore, ensure that you save the path mapping settings for all the hosts before changing it.

Restore a Filesystem copy

You can perform a restore of a copy using the Appsync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > File Systems**.
4. In the Host Name Column, click the Host that contains the file system.
5. In the **Host Filesystem(s)** page, select the filesystem and click **More > Restore**.
6. In the **Select a Copy** page, select one of the following choices:
 - Select a Copy
 - Select from RecoverPoint Bookmarks
7. Click **NEXT**.
8. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

- Note:** You can perform this step only if you have multiple applications that share the same LUN or file systems.

9. Click **NEXT**.
10. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.

- Note:** In the case of SnapVX/XtremIO Snap/PowerStore Snap mounted copies, when you perform restore, AppSync restores the data from the snapshots created on the array to the source devices, or from linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

- **Restore from snapshot:** Restores copies from original snapshots.
- **Restore from changed data:** Restores from the linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

11. Click **NEXT**.
12. In the **Review** page, review the restore options and click **FINISH**.

CHAPTER 9

Protect VMware Datacenters

This chapter includes the following topics:

- [Configuration prerequisites](#) 244
- [Discover VMware Datacenters](#)..... 246
- [Considerations when mounting a VMFS copy](#)258
- [Restoring a VMware datastore from a copy](#)..... 260
- [Restoring a virtual machine from a copy](#)..... 261
- [File or folder restore with VMFS or NFS datastores](#).....264

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.
- Administrator rights and user roles and permissions must always be configured at the Datacenter level and not at the cluster level.

RecoverPoint configuration prerequisites

- Configure RecoverPoint protection (Local/Remote/Local and Remote) 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 vMotion support

- You can perform a vMotion of virtual machines with vDisks from VMFS to VMFS datastores, or from NFS to NFS datastores
- You cannot perform a vMotion of virtual machines with vDisks from VMFS to NFS datastores, or from NFS to VMFS datastores

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 privileges must be assigned to the VC role that you plan to use in AppSync:

Datastore

Folder > Create Folder

Host > CIM

Host > Configuration > Storage partition configuration

Resource > Assign virtual machine to resource pool

Resource > Migrate powered off virtual machine

Resource > Migrate powered on virtual machine

Sessions > Validate session

Virtual Machine > Configuration > Add existing disk

Virtual Machine > Configuration > Add new disk

Virtual Machine > Configuration > Add or remove device

Virtual Machine > Configuration > Advanced

Virtual Machine > Configuration > Modify device settings

Virtual Machine > Configuration > Raw device

Virtual Machine > Configuration > Reload from path

Virtual Machine > Configuration > Remove device

Virtual Machine > Configuration > Rename

Virtual Machine > Configuration > Settings

Virtual Machine > Guest Operations > Guest Operation Program Execution

Virtual Machine > Interaction > Guest operating system management by VIX API

Virtual Machine > Interaction > Power Off

Virtual Machine > Interaction > Power On

Virtual Machine > Inventory

Virtual Machine > Provisioning > Allow disk access

Virtual Machine > Provisioning > Allow read-only disk access

Virtual Machine > Provisioning > Clone virtual machine

Virtual Machine > Snapshot management

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.

Discover VMware Datacenters

Perform this procedure to discover VMware Datacenters.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **VMware Datacenters**.
4. Click **DISCOVER DATACENTERS**.
5. Select the desired server and click **OK**.

List of datacenters

The top level of the VMware Datacenters page shows all datacenters registered with AppSync.

Column	Description
Protection status of datacenter	<ul style="list-style-type: none"> • 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.

Add a VMware vCenter Server

Add a VMware vCenter Server to AppSync when you want to protect VMWare datastores or when a virtual machine is used as a mount host.

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. On the AppSync console, select **Settings > Infrastructure Resources > VCENTER SERVERS**.

2. Click **ADD SERVER**.
3. Enter the following details in the Add vCenter Server page:
 - Note:** Type the credentials for an account that has Administrator privileges on the vCenter Server.
 - a. **Name:** Enter name or IP address of the vCenter server.
 - b. **Username:** Enter the username of the user.
 - c. **Password:** Enter the password of the user.
 - Note:** The **Run Discover Now** option is selected by default.
 - Note:** AppSync allows you to mount a file system or a database (that is, the underlying storage LUN on which they reside) from a physical Windows or Linux environment to a VMware virtual environment as an RDM device. Ensure that you add the vCenter managing that virtual machine to AppSync before performing a mount.
4. Click **OK**.

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** while performing the **CREATE COPY WITH PLAN** procedure from the datastores page, when you want to protect selected datastores immediately. The service plan is executed for the datastores alone.
- Choose **Subscribe to Plan** while performing the **CREATE COPY WITH PLAN** procedure from the datastores page, 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.

Subscribe a VMware Datastore to a service plan

You can subscribe a datastore 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. On the AppSync console, select **Copy Management**.

2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **VMware Datacenters**.
4. Select one or more datastores, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select the appropriate option.

Option	Description
Subscribe to Service Plan and Run	To subscribe the datastore for protection and run the plan immediately for any selected datastores.
Subscribe to Service Plan (with option to override)	To subscribe the datastore for protection. Protection for all datastores that are part of the service plan is executed at the scheduled time.

7. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold
8. Click **OK**.
9. Click **NEXT** to review your selection.
10. Click **FINISH**.

Overriding service plan schedules

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

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

The Datastore for which you want to schedule override should be subscribed to service plan.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **VMware Datacenters**.
4. Select one or more entries from the list, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select **Subscribe to Service Plan (with option to override)**.
7. Select the service plan that you want to subscribe to.
8. Click **NEXT**.
The Override Schedule page appears.
9. Select one or more databases and click **OVERRIDE SCHEDULE**.
10. Specify 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.

11. Click **NEXT** to review your selection.
12. Click **FINISH**.

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. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **VMware Datacenters**.
4. Click a datacenter to display its datastores.
5. Select one or more datastores, and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select **Subscribe to Service Plan and Run**.

The **Subscribe to Plan and Run** dialog appears displaying the progress

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 VM**.

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.

Unsubscribe VMware Datastore from a service plan

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

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **COPIES**.
3. From the **Select Application** drop-down, select **VMware Datacenters**.
4. In the Name Column, click the datastore you want to unsubscribe.
5. In the Name Column, click the desired datastore, and click **More > UNSUBSCRIBE**.
6. In the Unsubscribe page, click **OK**.

Note: You can also unsubscribe applications from a service plans, from the Service Plan page.

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.

Note: Due to VMWare limitations, virtual machine snapshot fails for a virtual machine with shared disk using multi-writer flag. If you try to protect a datastore with such a virtual machine with VM consistency option set, service plan succeeds but virtual machine snapshot does not occur.

View Datastore copy details and its events

View the list of data store copies by browsing to **Copies > VMware Datacenter** and selecting a data center, then a data store.

Before you begin

This operation requires the Data Administrator role in AppSync.

About this task

You can also see details of a copy from the Copies tab of the Service Plan.

The list of copies can be filtered by Copy (time of creation) and by service plan. In the Service Plan Copies tab, you can filter by the vCenter Server, data center, data store, and time.

Column	Description
Status	<ul style="list-style-type: none"> 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.
VM Consistent	Shows whether the copy is VM Consistent. If No, it is Crash Consistent.
Mount Status	Shows whether the copy is mounted or not. If mounted, displays the name of the mount host.
Mount Type	If copy is mounted as part of service plan run, value for Mount Type is ServicePlan. If copy is mounted as OnDemand, value for Mount Type is OnDemand.
Copy Type	Types of copies: <ul style="list-style-type: none"> CDP/CRR Bookmark VNXSnap

Column	Description
	<ul style="list-style-type: none"> VNXFileSnap VMAX V2 Clone, VMAX V2 Snap, SnapVXSnap, SnapVXClone Click Mount or Restore to launch the respective wizard.
Storage System	Displays Remote VNX Array Serial ID for copies from Silver service plan.
<i>The following additional details are displayed in the Service Plan Copies tab.</i>	
ESX servers	The ESX server on which the data store is present.
Name	The name of the copy's data store.
Copy name	Datastore copy created is displayed along with timestamp.
VM Consistent	Shows whether the copy is VM Consistent. If No, it is Crash Consistent.
Mount Status	Shows whether the copy is mounted or not. If mounted, displays the name of the mount host
Copy Type	Copy types: <ul style="list-style-type: none"> RecoverPoint Continuous Data Protection Bookmark RecoverPoint Continuous Remote Replication Bookmark VNXSnap VNXFileSnap VMAX V2 Clone, VMAX V2 Snap, SnapVXSnap, SnapVXClone VMAX3/PowerMAX SnapVXClone, SnapVXSnap UnitySnap UnityThinClone XtremeIOSnap VPLEX Snap DellSC Snap PowerStore Snapshot PowerStore Thin Clone
Site	RecoverPoint and VNX File site information
Storage System	Displays Remote VNX Array Serial ID for copies from all VMware service plans
Automatic Expiration	Determines whether automatic expiration is enabled or disabled for the selected copy.

When a copy is selected, you can:

- Click **Mount** or **Restore** to launch the respective wizard.
- View the virtual machines that are part of the selected data store copy from the **Details > Virtual Machines** tab.

Column	Description
State	Shows the state of the virtual machine. (Powered on or Powered off)
Name	Name of the virtual machine.
Platform	The OS platform on the virtual machine.
VM Version	The version of the virtual machine
Host	IP address of the machine hosting this virtual machine
VM File Path	Path to the virtual machine file. In the path, the name of the data store that the virtual machine resides on is within the [] parentheses.

- View the virtual disks that are part of the selected data store copy from the **Details > VM disks** tab.

Column	Description
Name	Name of the virtual disk.
Size (GB)	Size of the virtual disk.
Type	Shows the type of virtual disk.
Storage	Type of storage on the virtual disk.
Mode	Mode of the disk - persistent or non-persistent.
Path	The path to the virtual disk file.
Controller	Name of the controller being used by the disk.
Mount Status	Shows whether the copy is mounted or not. If mounted, displays the name of the mount host.
Virtual Machine	Name of the virtual machine that the disk resides on.

- View the events that are associated with each copy of the virtual machine from the **Details > Events** tab.

View virtual machine copy details

View the list of virtual machine copies by navigating to **Copies > VMware Datacenter** and selecting a datacenter, then Virtual Machines tab, then a virtual machine.

Before you begin

This operation requires the Data Administrator role in AppSync.

About this task

The list of copies can be filtered by Copies (time of creation) and by service plan.

Column	Description
Status	<ul style="list-style-type: none"> Green: successful Yellow: completed with errors Red: failed
Copy Name	Name of the copy created.
Service Plan	Name of the service plan associated with the copy.

Column	Description
VM Consistent	Whether the VM snapshot was created by AppSync.
Copy Type	The type of copy to be created.

When a copy is selected, you can:

- Click **Restore** to launch the VM Restore wizard.
- View the events associated with each copy of the virtual machine from the **Details > Events** tab.

Create a VMware Datastore copy

Create a copy of a datastore by subscribing it to an AppSync service plan from the Datastores page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **COPIES**.
3. From the **Select Application** drop-down, select **VMware Datacenters** to display the VMWare datacenters.
4. In the Name Column, click the desired datacenter.
5. Select one or more datastores, and then click **CREATE COPY WITH PLAN**.
6. Select the purpose as **Data Protection**.
7. Select the appropriate option.

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

8. Click **Select** and select the service plan that you want to subscribe to from the following options:
 - Bronze
 - Silver
 - Gold
9. Click **OK**.
10. Click **NEXT** to review your selection.
11. Click **FINISH**.

Enable or disable a VMware copy

You can enable or disable expiry of a copy during rotation using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Name Column, click the desired datacenter.
5. Click the preferred datastore to go to the copies page
6. Select the copy that you want to enable or disable and click **More**.
7. Click one of the following options depending on the action you want to perform:
 - **Enable Copy Rotation:** To enable automatic expiry of a copy during rotation.
 - **Disable Copy Rotation:** To disable automatic expiry of a copy during rotation.
8. Click **OK**.

Expire a VMware copy

You can expire a VMware copy using the AppSync console.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Host Name Column, click the desired datacenter.
5. Click the preferred datastore to go to the copies page
6. Select the copy that you want to expire and click **More > Expire** .
7. Click **OK**.

Service plan schedule

The service plan scheduling options determine whether the plan is run manually, or is 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 different times during the day.
 - Minutes after the hour are set in 1 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.
 - Select **Last** to select the last day of the month.

Overriding service plan schedules

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

Before you begin

This operation requires the Service Plan Administrator role in AppSync.

The Datastore for which you want to schedule override should be subscribed to service plan.

About this task

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

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **SELECT VIEW** drop-down, select **COPIES**.
3. From the **SELECT APPLICATION** drop-down, select **VMware Datacenters**.
4. Select one or more entries from the list, and then click **CREATE COPY WITH PLAN**.
5. Select the purpose as **Data Protection**.
6. Select **Subscribe to Service Plan (with option to override)**.
7. Select the service plan that you want to subscribe to.
8. Click **NEXT**.

The Override Schedule page appears.

9. Select one or more databases and click **OVERRIDE SCHEDULE**.
10. Specify 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.

11. Click **NEXT** to review your selection.
12. Click **FINISH**.

Create copy

The create copy options specify the criteria to create a copy based on the preferred storage type specified by the user.

You can specify the type of datastore copy to make, and the storage settings for the copies. This option 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](#) 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.

`Configure VM Snapshots for VMs` link allows you to select virtual machines from the datastores added to the service plan. By default, the `Exclude VMs for Snapshot` option is enabled. This means that the selected VMs are ignored while taking VMware snapshots during the service plan run. If you select the `Include VMs for Snapshot`, only the selected VMs are considered for VMware snapshot creation 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. You can order, select, or clear storage preferences. Copies are created using the first technology preference when possible. If the first technology cannot be used, the remaining copies are processed using the next selected preference instead. For example, if the first preference was a bookmark but not all the application data in the service plan was mapped to RecoverPoint, then AppSync uses VNX snapshots instead. If you want AppSync to skip using a particular replication technology, deselect that preference from the storage ordered preference list.

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 array snapshot copies that can exist simultaneously.

Automatic expiration of array snapshot copies

The automatic expiration value 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.

Mount copy

Mount copy 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.

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 .
- **Quality of Service Policy:** Select the desired Quality of Service option. This option is applicable only for XtremIO.
- **Unlink the SnapVX snapshots in unmount:** Enable this option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.

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 VMAX3/PowerMAX 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. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.

3. Click **Select Application > VMware Datacenters**.
4. Click a service plan, and expand the right pane.
5. Click the **OVERRIDES** tab.
6. Select **Mount Overrides**.

The list of datacenters includes all vCenter datacenters whose datastores are subscribed to this plan. The mount settings display the default settings. Additionally, for VMAX3/PowerMAX Datastores, SLO Service Level Objective appears as another option.

7. Select an entry, and click **OVERRIDE MOUNT**.
8. Edit the required fields, and click **APPLY CHANGES** to save the settings.
9. To revert back to default settings, select the datastore(s) and click **SET TO DEFAULT**.

Unmount copy

The unmount copy step in the service plan unmounts the copy.

This option is disabled if the **Unmount previous copy** option is enabled.

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.

Mount a copy using the VMware Mount wizard

You can initiate an on-demand mount of a datastore copy from the datastore copies page.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Name Column, click the desired datacenter.
5. Click on any datastore to go to the copies page.
6. Select the copy you want to mount and click **MOUNT**.

If multiple datastores were protected together, you may see the additional copies to mount option. Select the copies you prefer and click **NEXT**.

7. In the Select Mount Options page, under **General Settings**, do the following:
 - a. From the **Mount on Host** list, select the server on which to mount the copy.
 - b. From the **Mount Signature** list, select the signature type.
 - c. In case the selected copy is a RecoverPoint bookmark, from the **Image access mode** list, select one of the following 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 V2, 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 V2 and RP XtremIO is not supported.
- d. For VMAX3/PowerMAX arrays, from the **Desired SLO** list, select the desired Service Level Objective (SLO) for the mount copy.
-  **Note:** The SLO values are dynamically fetched from the VMAX3/PowerMAX arrays, and only the unique values are displayed.
- e. For XtremIO 6.2 and later, click the **Quality of Service policy** option to select the desired Quality of Service policy while mounting a copy.
- f. For VMAX3/PowerMAX SnapVxSnap, select the **Unlink the SnapVX snapshots in unmount** option to unlink the SnapVX snap during unmount. This option is applicable for regular SnapVX snap and second generation repurposing SnapVX snap, for on-job and on-demand service plans.
- g. For VMAX V2 arrays, select the desired FAST policy for the mount copy.
- h. Clear the **Use Dedicated Storage Group** option, if you do not want AppSync to enforce the use of a dedicated storage group for a mount. By default, this option is enabled.
- i. From the **VPLEX Mount Option**, select one of the following:
- **Native array volume:** Use this option if you want to mount the copy as native array volumes.
 - **VPLEX virtual volume:** Use this option if you want to mount the copy as VPLEX virtual volumes.
- j. From the **VMware settings**, select one of the following:
- **Enable VMware cluster mount:** Clear this option if you do not want to perform an ESX cluster mount. By default, this option is enabled.
 - **Disable VMware SRM:** This option is only applicable for RP 4.1 and above.
8. Click **NEXT** to review the mount options.
9. Click **FINISH**.

Unmount a VMware copy from the Copies page

You can unmount a copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

About this task

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

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware datacenters**.
4. In the Name Column, click the desired datacenter.
5. Click on any datastore to go to the copies page.
6. Select the copy you want to unmount and click **Unmount Copy**.
7. Click **OK**.

Unmount a VMware copy from the Service Plan page

You can unmount a VMware copy from the Copy Management page using the AppSync console.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Service Plan**.
3. Click **Select Application > VMware Datacenters**.
4. Click the name of the service plan you prefer in the Service Plan column.
5. Select the copy you want to unmount and then click **Unmount**.
6. Click **OK**.

Restoring a VMware datastore from a copy

You can perform a restore of a VMware Datastore copy using the Appsync console.

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. On the Appsync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Name Column, click the datastore.
5. Select the datastore, and click **More > Restore**.
6. In the **Select a Copy** page, select the copy you want to restore and click **NEXT**.
7. In the **Warn affected application(s)** page, select **I have read and understand the warning above and want to continue with restore**.

If multiple applications share the same LUN or file systems (as the application for which the copy is created), those applications will be listed as affected entities.

 **Note:** You can perform this step only if you have multiple applications that share the same LUN or file systems.

8. Click **NEXT**.
9. In the **Configure Storage Options** page, configure the following:
 - **Wait for mirror rebuild to complete** - This option is applicable for VPLEX Snap copies whose production data resides on local or distributed RAID-1 volumes.
 - **Disable VMWare SRM** - Allows you to manage consistency groups, if the SRM flag is enabled on the RecoverPoint consistency group. This is only applicable for RecoverPoint 4.1 and later.
 - **Perform device restore in background** - Allows you to optimize restore of VMAX V2 and VMAX3/PowerMAX devices. If you select this option, AppSync restore operation does not wait for VMAX V2 track synchronization to complete. The production application is available instantly.

Note: In the case of SnapVX/XtremIO Snap/PowerStore Snap mounted copies, when you perform restore, AppSync restores the data from the snapshots created on the array to the source devices, or from linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).

 - **Restore from snapshot:** Restores copies from original snapshots.
 - **Restore from changed data:** Restores from the linked devices (VMAX3/PowerMAX) or read-write snapshots (XtremIO X2), or read-write clones (PowerStore).
10. Click **NEXT**.
11. In the **Review** page, review the restore options and click **FINISH**.

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, 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.

Note: AppSync checks if the underlying datastore of a virtual disk is in use or not by other virtual machines before performing a virtual disk restore. In case the underlying datastore is in use, it detects and fails the restore with the appropriate error message.

Restoring a virtual machine from a copy

You can perform a restore of a virtual machine from the **Virtual Machines** tab in the copies view.

Before you begin

- This operation requires the Data Administration 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 a copy** step.
- The virtual machine should not have any pre-existing snapshots.
- Virtual machines with RDMs cannot be restored.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Name Column, click the desired datacenter.
5. In the Datastore page, click the **VIRTUAL MACHINES** tab.
6. Select the copy that you want to restore from and click **RESTORE VM**.
7. 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
8. In the **Select Restore Location** page, make the appropriate selections.
 9. In the **Select Mount Host** page:

Note: If the mount host is part of a cluster, all cluster hosts must have access to storage.

- a. Select the mount ESX.

If production data resides on RecoverPoint storage, the target devices should be visible to the selected mount host. For VNX, the mount host should be registered to the VNX. For all other storage, the mount host should be registered to the storage array where the copy resides.

- b. For a RecoverPoint bookmark copy, select the RecoverPoint image access mode from the list - Logged Access, Virtual Access, or Virtual Access with Roll.
- c. For a VPLEX Snap copy, select the VPLEX mount option - VPLEX virtual volume or native array volume. For VPLEX virtual volumes, the mount host needs to be added to VPLEX storage view; for native array volumes, it needs to be zoned to the VPLEX backend array where the snapshot is created.
- d. 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 case of a VPLEX Snap copy, if the ESX which is selected to mount the datastore for VM restore is part of an ESX cluster, the datastore is mounted only on that ESX and not on all the ESXs of that cluster. You must select the same ESX

under **Select Restore Location** and **Select Mount host**, if you do not want VM files to be copied over the network.

- For VM Restore, across all hosts in cluster environment there must be shared storage. If not, validation fails while restoring a virtual machine from a copy.

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.
10. 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.

The Instant restore option is not available for:

- VMAX V2 and VMAX3/PowerMAX copies if the source devices are thick
 - VMAX V2 and VMAX3/PowerMAX copies
 - VPLEX snap copies
 - Dell SC snap copies
11. In the **Summary** page, review the settings that you selected in the previous pages, and then click **FINISH** to perform the restore.
12. In the **Results** page, click **View Details** to see the progress.

Virtual Machine Restore options

You can select the restore location as well as restore operations.

Table 30 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.

Table 30 Virtual machine restore options (continued)

Restore Option	Description
	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. • 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. <ul style="list-style-type: none"> 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 involves multiple steps: 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.
- If a virtual disk from a local copy is mounted; then the same virtual disk from a remote copy cannot be mounted when created using the Gold service plan.
- 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 Administration 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, Windows 2012, Windows 2016, or Windows 2019 as the operating system. The AppSync host plugin must be installed on it and it should be registered with the AppSync server.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > VMware Datacenters**.
4. In the Name Column, click the desired datacenter.
5. In the Datastore page, click the **VIRTUAL MACHINES** tab.
6. Select the copy that you want to restore from and click **RESTORE FILE**.
7. Select the virtual disks whose files or folders must be restored and click **Next**.
8. 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\ 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.
 9. In the **Summary** page, review the settings that you selected in the previous pages and click **FINISH** to start the restore of the disk.
 10. In the **Results** page, click **View Details** to see progress the steps that are part of restoring a virtual disk.
 11. Next, perform the manual step of copying the required files or folders from the mount location to a location of your choice.
 12. Optionally, you can unmount the datastore.

CHAPTER 10

Repurposing

- [Repurposing overview](#) 268
- [Creating Repurpose copies](#) 272

Repurposing overview

This topic explains how to use the AppSync repurposing feature for database and file systems.

AppSync allows you to create copies of your database and file systems for application testing and validation, test and development, reporting, data masking, and data analytics. AppSync identifies copies that are created from a repurpose action as first generation and second generation copies. The source of a second generation copy is a first generation copy. You can create multiple second generation copies from a first generation copy.

AppSync supports repurposing on File systems, SQL Server and Oracle databases.

There are two types of repurposing:

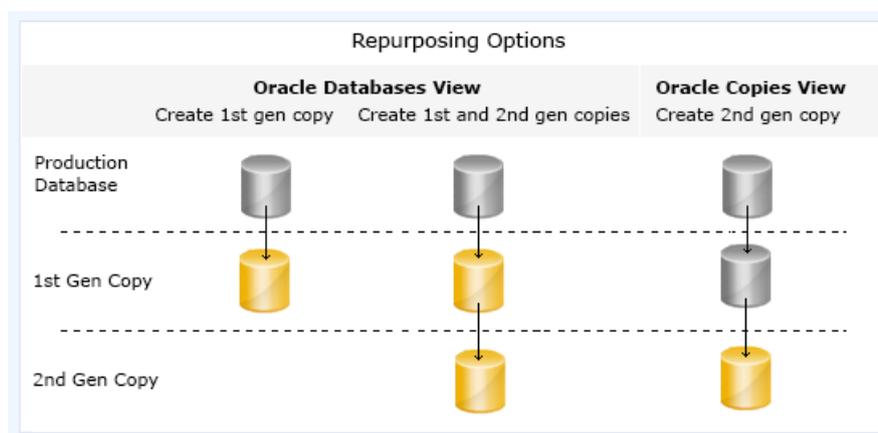
- Native array repurposing - The first generation copy is a copy of the source database. For example, in the case of an XtremIO array, snapshot of the source is the first generation copy.
- RecoverPoint bookmark repurposing - The first generation copy is a copy of the LUNs at the local or remote replication sites in the RecoverPoint consistency groups.

Note: To create a snap of a bookmark on a remote site (remote RecoverPoint repurposing), add both the local and remote native array to AppSync.

Review the following additional information about repurposing:

- A first generation copy creates a copy that can be used as source for other copies.
- Repurpose copies do not figure in RPO calculations.
- You can create first generation and second generation repurpose copies on-demand or schedule it.
- Restore is not supported for second generation copies.
- Restore of a first generation copy is not supported in the case of RecoverPoint bookmark repurposing.
- Restore from a first generation copy is not allowed in the case of VMAX V2, if it is created on the remote site.
- The first generation copy of a database creates an application consistent copy. It includes application discovery, mapping, and database freeze/thaw. For File systems, you can configure freeze/thaw operation using callout scripts.

Note: For a first generation copy of SQL, you can configure a VSS retry count and retry interval for freeze/thaw operation using the Repurpose Wizard. VSS retry options are not applicable for Crash Consistent SQL copies.
- Second generation copies are created using the first generation copy as the source without impacting the application. They do not include application discovery, mapping, and application freeze/thaw. If a first generation copy is mounted with recovery, and if the second generation copy is refreshed, the second generation copy might not be recoverable after the mount.



Additional Notes

- SQL
 - Log backup is not supported as part of repurposing.
 - Repurposing of multiple SQL databases is not supported.
- Oracle - RMAN options are not available in the Repurposing wizard.
- File system
 - Repurposing of NFS file system is not supported.
 - When repurposing multiple file systems together, failing to protect one or more file systems fails the repurpose operation completely.
 - You cannot simultaneously protect two file systems residing on two separate storage arrays.
 - File systems that are repurposed together are mounted together.
 - File systems that are protected together are repurposed together for second generation copies.

Repurpose schedule

- If you attempt to create both the first generation and second generation copies simultaneously using the Repurpose wizard from the Database page, the second generation copy is created automatically after the first generation copy is created. This is applicable for **Run Now**, **Schedule**, and the **Run Only Once At later time** options.
- If you create a schedule for the second generation copy, the second generation copy is not triggered after the first generation copy is created. The second generation copy runs according to the schedule.
- If you create a second generation copy using the Repurpose wizard from the Copies page, the second generation copy is not triggered even though the first generation copy runs according to the schedule. However, if the second generation copy is scheduled, it runs according to the schedule.
- On the first schedule, a repurposed copy is created, and on subsequent schedules, the copy is refreshed.
- Multiple file systems can be scheduled together as part of the same repurpose plan.
- If multiple file systems are scheduled to be repurposed together as part of the same schedule, selecting any of the file system and viewing the schedule displays the schedule. If you delete

the schedule, the schedule for all the file systems that were scheduled to be repurposed together are deleted.

Modifying a repurpose plan

Each copy is associated with a unique repurposing plan. To modify a repurpose plan:

1. Log in to the AppSync console and select **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters**.
4. Click the name of the database, instance, or file system that contains copies.
5. Click **MORE > Repurposed Copies** to view the repurposed copies for all the databases, or application instance.
6. Select a copy, and click on **EDIT** button in **SERVICE PLAN** tab in details pane on right to edit the repurpose plan options.

Note:

- The options that you cannot modify are disabled.
- If you modify the label, the updated label is reflected in the Copies page only when you refresh the copy.

Repurpose refresh

Refresh means to discard the current copy data and recreate the copy data using its parent. When you refresh a copy, changes from the source are reflected in the copy. This is normally done by creating a new point-in-time copy and expiring the old copy.

- First generation and second generation copies can be refreshed.
- Refreshing a first generation copy creates an application consistent copy with a new time.
- Second generation copies are not modified if you refresh the first generation copy.
- Refresh of a second generation copy recreates the second generation copy with the first generation parent. (Used for discarding changes of second generation copy and starting over.)
- The timestamp on the second generation copy is the same as first generation copy. If the first generation copy is refreshed, then the timestamp differs.
- When you refresh a mounted repurpose copy, AppSync unmounts the copy, expires the copy and creates a new copy and the refreshed copy is mounted back with the same options as previous mount operation.
- When you refresh a mounted RecoverPoint repurposed copy, AppSync unmounts the copy and refreshes the copy. It is not mounted back by the end of the refresh operation.
- When a repurposed copy is refreshed because of a scheduled repurpose service plan run, the refreshed copy is mounted with the mount options as specified in the repurpose plan.

You can refresh a repurposed copy at any time. To start the refresh:

1. Log in to the AppSync console and select **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems**.
4. Click the name of the database, instance, or file system that contains copies.
5. Click **MORE > Repurposed Copies** to view the repurposed copies for all the databases, or application instance.

6. Select the copy and click **Refresh**.

Native array refresh

When storage arrays provide copy refresh capability natively (that is, the ability to refresh the same copy instead of creating a new one), AppSync uses it instead of expiring the copy and recreating a new copy to refresh the copy data.

Native array refresh benefits

- Reduces the time required to complete a refresh workflow.
- If the copy being refreshed is mounted to a host, then the storage LUNs are not removed from the host. Only the application is stopped, the file system is unmounted, data is refreshed on the existing copy, file system is mounted back, and the application is started. In a VMWare virtual environment where application resides on virtual disks, the virtual disks are removed from the virtual machine, but LUNs are not removed from ESX.
- Eliminates the need for a rescan in a VMWare virtual environment because storage LUNs are not removed from the mount host.
- The WWN, volume, and device details of the mounted LUN remains the same because storage LUNs are not removed from the mount host. This is beneficial in the case of some backup scenarios, where external post-mount scripts depend on the copy WWN, volume, or device details for any action.

Native array refresh usage

- On Unity, first generation copies are refreshed using the native array refresh. However, for a second generation copy, native array refresh is used only if the second generation snapshot is refreshed when the first generation snapshot is ATTACHED.
 **Note:** This is only applicable for Unix based applications.
- On XtremIO, if all the LUNs to be protected are in a single XtremIO consistency group, native array refresh is used.
- In the case of VPLEX virtual devices on XtremIO storage devices, native array refresh is used, if all XtremIO LUNs belong to the same consistency group.
- For Windows based applications, the application must be fully part of a single XtremIO consistency group. For example, if a SQL database resides on LUNs from two different XtremIO consistency groups, then native array refresh is not used.
- For Oracle databases, the data, redo, and control files must reside on one consistency group and archive log, and FRA must be on a separate consistency group.

Repurpose expire

You can expire a repurposed copy when you no longer need the copy.

-  **Note:** In the case of VMAX V2 arrays, the session still persists on the array even after you expire a copy.

Data masking using scripts

You can use the AppSync repurposing feature to mask sensitive data.

To mask data using scripts:

1. Mount and recover the first generation copy of a database.

2. Apply data masking on the same copy using the post mount script and unmount the database. You can specify post mount script information in the scripts step by editing the respective repurpose plan.
3. Unmount the first generation copy.
4. Create a second generation copy from the first generation copy using the Repurpose wizard.

Creating Repurpose copies

Use the Repurpose wizard to schedule or immediately create first generation or second generation copies as required.

Before you begin

This operation requires the Data Administrator role in AppSync.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems**.
- 4.

Option	Description
To Repurpose an SQL copy:	<ol style="list-style-type: none"> a. Select Microsoft SQL Server. A list of available SQL server instances appears. b. Select an instance. c. On the Database folders page, select User databases. The list of available database appears. d. Select the database that you want to repurpose.
To Repurpose an Oracle copy:	<ol style="list-style-type: none"> a. Select Oracle. A list of available databases appears. b. Select the database that you want to repurpose.
To Repurpose a File system copy:	<ol style="list-style-type: none"> a. Select File system. A list of available hosts appears. b. Select a host. A list of available file systems appears. c. Select one or more file systems that you want to repurpose.

5. Select the database and click **Create Copy With Plan**.
6. Select **Data Repurposing** and click **NEXT**.
7. In the **Define the Copy** for Repurpose, define label for 1st gen copy to help identify the copy purpose.

 **Note:** In the case of file systems, first generation label determines the callout script names. The name of the freeze/thaw/unmount callout scripts uses the first generation label.

- a. Copy location: select **Local** or **Remote**
- b. For **Use Bookmark as an intermediate step**: This option appears only if the RecoverPoint appliance is configured in AppSync.

- c. Mount Copy: Specifies if the following options for mounting a copy:
 - **No**
 - **Yes**
 - **Yes - Keep it mounted(Previous copy will be unmounted)**
 - **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**
- d. Set the value of the **2nd gen copies** to one of the following:
 - **Yes:** To create the first generation copy and a second generation copy.
 - **No:** To create the first generation copy only.
8. Click **NEXT**.
9. In the Create the copy page, select application-specific copy options for the first generation copy only.
 - a. Configure storage options
 - b. Choose appropriate copy type
10. Click **NEXT**.
11. In the Scripts page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

i **Note:** This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

 - a. **Full Path to Script**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
12. Click **NEXT**.
13. In the Schedule/Run page, select one of the following scheduling options:
 - a. **Run Now:** Creates a service plan when you click Finish on this wizard.
 - b. **Schedule:** Creates a service plan based on the specified recurrence type. Configure the following fields to schedule the creation of a service plan
14. Configure the following fields to schedule the creation of a service plan:
 - a. In the **Recurrence Type** drop-down list: select the desired frequency of creation.
 - b. In the **Every** drop-down list: select the desired time to run the service plan.
 - c. In the **Run Only Once At Later Time** drop-down list: Creates a copy only once on the specified date and time.
15. Click **NEXT**.

i **Note:** If **2nd gen copies** was set to **Yes** in the **Define the Copy** step for Repurpose, the **Define second gen copy** page appears.
16. In the Define 2nd-gen Copy page, define label for 2nd gen copy to help identify the copy purpose.

Note: In the case of file systems, second generation label determines the callout script names. The name of the unmount callout scripts uses the second generation label.

- a. Choose appropriate copy type: **Snap** or **Clone**
 - b. **Mount Copy:** Specifies if the following options for mounting a copy:
 - **No**
 - **Yes**
 - **Yes - Keep it mounted(Previous copy will be unmounted)**
 - **Yes - Mount the copy, but after the post mount scripts run, unmount the copy**
 - c. **Run as User Name**
 - d. **Password**
17. Click **NEXT**.
 18. In the Scripts for 2nd-gen copy page select the pre-copy or post-copy scripts that you want to execute and configure the following fields:

Note: This step displays pre-mount scripts and post-mount scripts if the mount option is selected.

 - a. **Full Path to Script**
 - b. **Script Parameters**
 - c. **Run as User Name**
 - d. **Password**
 19. Click **NEXT**.
 20. Review the Repurpose Plan options and click **FINISH**.

View or delete repurpose copy schedules

You can view or delete a repurpose copy schedule.

Procedure

1. Log in to the AppSync console and go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems**.
4. Click the name of the database or filesystem.
5. click on **MORE > Repurpose Schedule** to view all the schedules for the selected application.
6. Select one or more schedules, and click **DELETE** to delete the repurpose schedule.

Note: In the case of file systems, deleting the schedule by selecting one file system also removes the schedule for other file systems.

View repurposed copies

You can view repurposed copies for File Systems, Oracle databases, and Microsoft SQL application instances.

Procedure

1. On the AppSync console, go to **Copy Management**.
2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / File Systems**.
- 4.

Option	Description
For Oracle	Click MORE > Repurposed Copies .
For Microsoft SQL Server	Click on an instance name and click Repurposed Copies .
For File Systems	Click Repurposed Copies .

The **Repurposed Copies** window appears. It lists all the first generation and second generation copies.

You can perform the following operations:

- Create second generation copy
- Mount
- Unmount
- Retry recovery
 - ⓘ **Note:** This option is applicable to Oracle only.
- Refresh
- Restore
- Expire

CHAPTER 11

Monitor AppSync

This chapter includes the following topics:

- [RPO concepts and best practices](#).....278
- [Alerts and associated events](#).....281
- [Email alerts](#).....282
- [View Jobs](#).....284
- [View Job Status progress](#).....284

RPO concepts and best practices

A recovery point objective (RPO) is one of several scheduling options that can be configured in the service plan creation options.

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.

 **Note:** RPO is an alerting mechanism only, no copies are initiated based on this setting.

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**.

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. On the AppSync console and click the **Reports** tab.

The recover point compliance reports are displayed on this page.

2. Sort and arrange columns as desired for the report.
3. Click the *Export* icon on the top-right of the table to run the export wizard.
You have the option to include table headers and export only selected rows.
4. Click **Next** and specify a filename and click **Download** to save the exported data to disk.

Results

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.

View the Service Plan Completion Report

The service plan completion report shows the service plan cycles that completed successfully, completed with errors, and failed.

About this task

You can view completed service plan cycles across all service plans for the last 24 hours, the last 3, 7 or 30 days, or for all time.

This page displays the following information for each service plan.

This table describes the details of the Service Plan Completion Report.

Table 31 Service Plan Completion Report

Column	Description
Service Plan	Name of the service plan.
Application Type	Name of the application subscribed to the service plan.
Service Plan Cycles	Number of service plan cycles run.
Completed successfully	Percentage of service plan runs completed successfully.
Completed with errors	Percentage of service plan runs completed with errors. In this case, there is a successful copy for a given database, but some other step in the service plan run failed.
Failed	Percentage of service plan runs that have failed.

Procedure

1. On the AppSync console, Click the **Reports > SERVICE PLAN COMPLETION REPORT** tab.

The service plan completion reports are displayed on this page.

2. To filter the displayed results, click the **TIME** dropdown list, and select the desired timeframe.

View the 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.

About this task

This page displays the following information for each server.

Table 32 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 at the start 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.

Procedure

1. On the AppSync console, Click **Reports > RECOVERY POINT COMPLIANCE REPORT**.

The Recovery Point compliance reports are displayed on this page.

View the Automated Log Collection Status Report

You can view reports for the status of all automated log collection activity in AppSync.

About this task

This page displays the following information for each report.

This table describes the details of the Automated Log Collection Status Report.

Table 33 Automated Log Collection Status Report

Column	Description
Log Resources	Name of the resource for log creation.
Status	Current state of the resource.
File Name	Name of the log file.
Description	Description of the log file.
Start Time	The time at which the log file was created.
Last Updated	The time at which the log file was updated last.

Procedure

1. On the AppSync console, Click **Reports > AUTOMATED LOG COLLECTION STATUS REPORT**.

The log collection reports are displayed on this page.

Alerts and associated events

AppSync generates an alert when a step in service plan run 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 step in service plan run. When an application goes out of RPO compliance, the associated alert is generated within 1 hour.

AppSync displays alerts in the console under the **Alerts** tab.

Table 34 Details of alerts

Column	Description
Alert State	Level of alert
Time	Date and time of the alert.
Server	Application server, such as the Name of Microsoft Exchange database.
Application	Replicated object, such as a Microsoft Exchange database.
Category	RPO, License, Maintenance, and Other.
Service Plan	Service plan name 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.
Acknowledged	Indicates if the alert has been acknowledged. Note that acknowledged alerts will not display in the AppSync Dashboard.

You can filter alerts by the time they were generated, by alert category, 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

The following steps show how you can acknowledge alerts.

About this task

You can choose to acknowledge alerts that are shown in the Alerts tab on the console. 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 **AppSync > 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 Datastore service plan runs

You can acknowledge an alert icon within the AppSync console for Oracle and SQL databases, File systems, and VMWare datastores.

About this task

An alert icon indicates the status of the most recent service plan run. The icon appears beside a database, file system, or datastore 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 Datastore.

The following procedure shows you how to view and acknowledge the alert.

Procedure

1. Select an alert from the database, file system, or datastore 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 Datastore table.

The alert icon changes to an information icon.

3. If required, re-run the service plan on the same database, file system, or Datastore to display the alert icon for this run.

Email alerts

You can configure AppSync to send alerts via email to a list of recipients. By default, only failure alerts are emailed.

About this task

You enable alert emails and add recipients per application instance, such as an Exchange mailbox server. To configure AppSync to also send an email after successful completion of a scheduled service plan:

Procedure

1. Select **Settings > Notification**.
2. Select **Notify Service Plan Success** to receive notifications on the successful completion of service plans.
3. Click **APPLY**.

Configure server settings for email alerts

Configure SMTP services on a machine that the AppSync server can access. Once the SMTP settings are completed, user needs to setup email notifications individually on the applications, for which he needs to receive alerts.

Before you begin

This operation requires the Resource Administrator role in AppSync.

Refer to SMTP documentation for configuration procedures.

Procedure

1. Select **Settings > Notification**.
2. Under **SMTP Settings**, enter values for SMTP Server Host Name, SMTP Server Port, Sender Email Address, and Recipient Email Address.

 **Note:** License non-compliant alerts are sent to the specified recipient address.

To validate the settings, click **SEND TEST EMAIL**, enter the recipient's email address and then click **OK**. The recipient's mailbox should receive a test email from AppSync.
3. Select **Notify Service Plan Success** to receive notifications on the successful completion of service plans.
4. Select **Notify For On Demand Success** to receive notifications on the completion or failure of on-demand jobs.
5. Click **APPLY**.

Specify 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.

Procedure

1. On the AppSync console, select **Copy Management**.
2. From the **Select View** drop-down, select **Copies**.
3. From the **Select Application** drop-down, select **Oracle / Microsoft SQL Server / File Systems / VMware Datacenters / Microsoft Exchange**.
4. Navigate to the database, datastore, or instance page, depending on the application you selected.
5. Select the desired database, datastore, or instance, and click **EMAIL NOTIFICATION**.
6. Enter one or more email recipients, separated by commas (,) and click **OK**.

A test email is sent to recipients for verification.

View Jobs

Perform this procedure to view the jobs running in AppSync.

Procedure

1. On the AppSync console, Click **Jobs**.

The **Jobs** page is displayed with the list of jobs running in AppSync.

Name	Description
Time	Shows the date and time of when the job started.
Application type	Shows the type of application.
Service plan	Shows the name of the service plan.
Label of item	Shows the label of the copy. (Only for repurpose copies).
Runs	Shows the status of the job. (Schedule or On Demand).

View Job Status progress

Perform this procedure to view the progress of jobs running in AppSync.

Procedure

1. On the AppSync console, Click **Jobs**.
2. In the Jobs page, click a job to view the details in the right pane.
3. In the right pane, click **VIEW PROGRESS**.

The **View in Progress Events** dialog displays the status of the in-progress job.

4. In the Jobs page, click a job to view the details in the right pane.
5. Expand the Details section, to view the details of the job.

The event status, date and time, host, description, and event ID details are shown for each alert. Use the **Show/Hide Columns** button to view or hide the details.

6. Click **CLOSE**.

CHAPTER 12

Storage considerations

- [VNX Block](#) 286
- [VNX file](#) 288
- [VMAX V2](#).....290
- [VMAX3/PowerMAX and VMAX All Flash](#).....294
- [XtremIO](#).....297
- [RecoverPoint](#) 300
- [Unity](#) 303
- [VPLEX](#).....306
- [Dell SC](#)..... 308
- [PowerStore](#)..... 309

VNX Block

AppSync supports the creation and management of application copies using VNX Snap copy technology. Consider best practices for VNX array setup before deploying AppSync.

Connectivity

Consider the following information for VNX connectivity with AppSync.

- AppSync supports Fibre, iSCSI, and FCoE connectivity between the host running the AppSync software and the VNX array. Network connectivity is required between the array and the AppSync server.
- Storage control occurs only on the AppSync server. No zoning is necessary from the VNX array to the AppSync server. It is not necessary to pre-expose any LUNs.
- Configurations with multiple AppSync servers per VNX array are supported.

VNX LUN support

Consider the following information for VNX LUN support.

- AppSync only supports LUNs that are in a pool. If you run VNX Snapshot replication you must use pool LUNs, not RAID LUNs. For RecoverPoint, use RAID storage.
- AppSync cannot create snapshots on LUNs with compression enabled.
- For VNX Snapshots, AppSync supports primary LUNs of any size.

VNX consistency groups

Consider the following information when using VNX consistency groups:

- All limitations that apply to VNX consistency groups also apply to AppSync.
- You can have multiple consistency groups within a single service plan.
- If you are using VNX consistency groups, all file systems that are related to an application in the snapshot set should reside in the same service plan. If not, you can encounter problems with mount and restore.

VNX mount

The following considerations apply:

- Mount hosts require SAN visibility to the VNX array.
- Changes made to a VNX Snapshot while it is mounted are persistent.
- If you accidentally delete hardware copies on the array, you cannot mount those copies with AppSync.
- Do not change the name of the storage group for the mount host when the copy is mounted. If you change the name of the storage group, ensure that you revert to the original name before unmounting the copy from AppSync.

Avoiding inadvertent overwrites

When you use AppSync to create a copy of one set of data that shares a LUN with other data, the copy contains all the data on that LUN. During restore, you may unintentionally write older data over newer data. The entities that are overwritten are called *affected entities*. Always configure data so that affected entities are reduced or eliminated.

Each LUN should contain a single file system or database file. If you are certain that the file system and/or database table residing on that LUN is always be backed up or restored as a unit, exceptions apply.

Service plan considerations for applications on VNX Block storage

After you register VNX storage, you can subscribe the application to a service plan to create and manage copies.

Bronze plans are supported. AppSync supports VNX Snapshot as the copy technology. Subscribe to the Bronze service plan to create and manage local copies for operation recovery, backup acceleration, or repurposing (create copies for test/dev). AppSync supports pooled LUNs (TLU/DLU) if the Snapshot technology supports these LUNs.

The maximum number of copies that AppSync can create and manage for VNX Block is dictated by the limits of the VNX Snap technology. The maximum number of VNX snaps per source is 256. This allows a maximum AppSync service plan rotation of 255.

Dynamic mounts

With proper zoning, AppSync automatically presents storage to the host when a copy is mounted.

Physical host

When AppSync mounts a copy, it dynamically assigns a snapshot to the host. The physical host must be zoned to the VNX array.

Virtual machine

Dynamic mounts happen as raw device mapping (RDM) or through native iSCSI on the virtual machine.

- For RDM, the ESX server where the virtual machine resides must be zoned to the VNX array.
- For RDM and virtual disks, virtual center (which manages the ESX server that the virtual machine mount host resides on) must be registered with the AppSync server.
- For native iSCSI, the virtual machine must be zoned to the VNX array.
- For virtual disks, virtual center of ESXi server (where mount host resides) must be registered with AppSync. Register the virtual machine with `disk.EnableUUID` flag enabled. AppSync installs the host plug-in on the virtual machine during registration for virtual disk and application level protection.
- For virtual disks, ESX cluster mount is not supported. While mounting application copy to a VM host on clustered ESX, the underlying snap datastore is not mounted to all the ESX hosts of ESX cluster.

Microsoft Cluster Server mounts for SQL Server

Microsoft Cluster Server (MSCS) mounts for SQL Server can be done on production or alternate clusters.

When you mount to a cluster node using VNX storage:

- The storage group configuration applies only to physical hosts or virtual machines with NPIV or iSCSI that are directly connected to the VNX. For clusters configured using virtual machines with RDM or virtual disk, the copy that is mounted is only visible to the selected node (usually passive node).
- When you mount to a cluster node for backup purposes, create a dedicated storage group for one of the nodes of the cluster, preferably the passive node.
- If PowerPath 5.7 is installed, the host IP in the VNX storage group changes to the IP that corresponds to Microsoft failover cluster virtual adapter. PowerPath 5.7 has an auto-host registration feature that intercepts host agent operation and overwrites the IP with its own

selection. This feature cannot be turned off. Upgrade to PowerPath 5.7.2 and above to correct this issue.

SAN policy on Windows Server Standard Edition

On Windows Server, the SAN policy determines whether a disk comes in online or offline when it is surfaced on the system. For Enterprise Edition systems, the default policy is offline. On Standard Edition the default policy is online. You need to set the policy to offlineshared to prevent mount failures.

To set the SAN policy to offline on a Windows Server 2008 Standard Edition host, open a command line window and run the following commands:

```
C:\>diskpart
Microsoft DiskPart version 6.0.6001
Copyright (C) 1999-2007 Microsoft
Corporation.
On computer: abcxyz
DISKPART> san policy=offlineshared
DiskPart successfully changed the SAN policy
for the current operating system.
```

VNX file

AppSync supports the creation and management of application copies using VNX File SnapSure copy technology. AppSync-managed copies can be local, remote (off the VNX Replicator target) or identical point-in-time local and remote copies.

Consider best practices for VNX file setup before deploying AppSync.

VNX SnapSure

VNX SnapSure creates a point-in-time copy of all the data on the network file system (NFS). For the initial snapshot, this method creates a full copy of the original file system, therefore requiring the same amount of space on the file system. Subsequent snapshots space usage depends on how much the data has changed since the last snapshot was taken.

SnapSure has the following characteristics:

- Storage Service — VNX File Server
- Source — VNX LUN
- Target — VNX SnapSure local snapshot
- Storage Requirements — The following storage requirements apply:
 - The source data must reside on VNX file systems.
 - Storage must include enough space for the snapshots on the VNX.
 - Storage pools cannot be defined for VNX jobs.
- Mount and Recovery — You can mount the replica on a target host and/or perform direct recovery from target to source.

VNX Replicator

VNX Replicator creates a point-in-time copy of all the data on the network file system (NFS). VNX Replicator maintains consistency between the source and target file systems that are based on the Time Out of Sync policy settings.

VNX Replicator has the following characteristics:

- Storage Service — VNX File Server
- Source — VNX NFS

- Target — Replicator remote snapshot
- Storage Requirements — The source data must reside on network file systems.
- Mount and Recovery — Can mount the copy on a target host and perform recovery from the copy if required.

VNX remote protection

Protection occurs between a local Data Mover and a Data Mover on a remote VNX system.

Both VNX for file cabinets must be configured to communicate with one another by using a common pass phrase, and both Data Movers must be configured to communicate with one another by using a Data Mover interconnect. After communication is established, a remote session can be set up to create and periodically update a source object at a remote destination site. The initial copy of the source file system can either be done over an IP network or by using the tape transport method.

Some recommendations for the session include:

- The session must be created with the Time Out of Sync update policy instead of a manual refresh.
- The Time Out of Sync value should be set to lowest value possible for the network configuration.

After the initial copy, changes made to the local source object are transferred to a remote destination object over the IP network. These transfers are automatic and are based on definable protection session properties and update policy.

One-to-many replication configurations are not supported in AppSync.

Protecting data on VNX network file systems

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.

During restore of 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.

Service plan considerations for an application on VNX File storage

Once you register VNX storage, you can subscribe the application to a service plan to create and manage copies.

Bronze, Silver, and Gold plans are supported for copies of applications (NFS data store, Oracle NFS) residing on VNX File.

The limits of VNX SnapSure technology determine the maximum number of copies that AppSync can create and manage for VNX File.

For Local SnapSure copies you can have a maximum of 96 RO (read-only) snaps. AppSync service plan rotation for VNX NFS file system is a maximum of 95.

For Remote SnapSure copies (across Remote Replicator), you can have a maximum of 95 RO snaps. AppSync service plan rotation for VNX NFS file system is a maximum of 94.

For RW (read/write) mounts, SnapSure allows for up to 16 RW snaps off existing RO snaps. A maximum of 16 snapshots for a given source can be mounted RW at any specified time. The service plans, by default, unmount the provision copy before mounting the new copy so this limit

has no consequences. However, if the implementation requires simultaneously mounting multiple copies for the same source RW, the limit of 16 must be considered.

VNX file mount

You can mount any VNX File Snapshot copy created in the service plan at any time, independent of other copies created on the same service plan.

The following considerations apply:

- ESX mount hosts must belong to a vCenter server.
- ESX mount hosts require visibility on the network.
- NFS.MaxVolumes, an advanced setting on the ESX server, should be set to the number of NFS datastores that will be mounted to each ESX on the network.
- When mounting to an ESX server, AppSync uses the lowest number interface that has connectivity.

Note: For VNX File Snapshot mount, alias of export is not used, if the source file system is NFSv4.X. Instead, in such a scenario, the checkpoints are exported and mounted using the checkpoint's full name. This is because of a limitation from VNX file storage.

VMAX V2

To create and manage copies of your applications, AppSync supports TimeFinder Clone and TimeFinder VP Snap replication technology. AppSync also supports remote copy management off of an R2 in a SRDF/S or SRDF/A configuration.

To create and manage copies in VMAX V2, it is required to register SMI-S provider for VMAX V2 in AppSync.

Review the following sections before adding your VMAX V2 storage.

Service plan considerations for applications on VMAX V2 storage

Once you register VMAX V2 storage you can subscribe your application to a service plan to create and manage copies.

Bronze and Silver plans are supported. TimeFinder VP Snap is the default replication technology used for service plans. You can change your preference to clone if TimeFinder Clone copies are desired.

The recommended maximum number of copies to keep before expiration is 6 for Timefinder Clones and up to 31 for VP Snap. The number of Timefinder Clone and VP Snap copies that can be created and managed is influenced by other copy and replication technologies used on the source LUNs. Refer to section on Copy Session Limits" for your planning. Refer to [VMAX copy session limits](#).

Bronze plan

You can subscribe to the Bronze service plan to create and manage local copies for operation recovery, backup acceleration or repurposing (create copies for test/dev).

For RAID LUNs AppSync chooses TimeFinder Clones for the Bronze plan. If the source is a RAID LUN or a mix of RAID and thin LUNs, then AppSync defaults to clone even if you select TimeFinder VP Snap as your preference.

Silver plan

For copies across SRDF/S or SRDF/A subscribe applications to the Silver service plan.

Note: Creation of remote copies in an SRDF/A configuration is not supported with Microsoft applications.

SRDF/A caveats: Creating a TimeFinder VP Snap or TimeFinder Clone of the R2 device is not allowed if either of the following is true:

- SRDF/A device-level write pacing is not activated and supported on the SRDF/A session.
- The SRDF pair is the R21-> R2 of a cascaded configuration, and any of the following apply:
 - The R21 Symmetrix array is running an Enginuity level lower than 5876.159.102
 - The R2 Symmetrix array is running an Enginuity level lower than 5875.
 - The R21 device is not pace-capable.
- Restore from SRDF/A is not supported

Source storage LUNs can be traditional RAID LUNs or thin LUNs (TDEVs). TimeFinder VP Snap support is only for thin LUNs. Consider the following recommendations:

- R1 > R2 should be in Synchronized state (for SRDF/S) and Consistent state (for SRDF/A)
- For Silver plan Create copy: Affinitizer splits the applications based on the RDF Group (RA Group) to which the source devices belong.
- Put all application LUNs in the same RDF group.

Note:

- If you are creating local bronze level copies, it is best to provide a local SMI-S provider, and also make it the preferred provider for that local array.
- If you are creating remote silver copies, it is best to provide a remote SMI-S provider for the remote array, and also make it the preferred provider for that remote array.

Copy session limits

Symmetrix VMAX V2 series arrays support up to 16 differential sessions per source device, which can be used for TimeFinder/Clone, TimeFinder/Snap, TimeFinder VP Snap, SRDF/Star, Solutions Enabler Open Replicator (ORS), or Symmetrix Differential Data Facility (SDDF) operations.

This limits the number of available copies that can be created.

TimeFinder VP Snap allows an additional 32 sessions per Symmetrix device which includes availability of one session of the traditional 16 sessions available. If you want to perform a restore, an additional session is required from the 16.

For example, if you use VP Snap for a source LUN and then desire a restore operation, this action leaves 14 sessions available for other copy technologies (TF Clone, ORS, Timefinder/Snap, SRDF/Star, on so on).

Additionally, if you want to create and manage TF Clone copies for the same source, you can create no more than 7 TF Clone copies using AppSync. (AppSync creates differential TimeFinder Clone copies which take up 2 differential sessions per copy $14/2 = 7$.) Since AppSync does not delete or expire a copy prior to creating a new one, the source of the AppSync rotation for the TimeFinder Clone copies can be no more than 6. This allows for an additional copy to be created prior to delete/expire of the oldest copy.

Note: For additional TimeFinder session limits, refer to *Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide*.

Mount and unmount VMAX V2 copies

Mount/unmount operations on VMAX V2 involve masking/unmasking LUNs or set of LUNs to a host.

AppSync relies on the VMAX V2 Auto-Provisioning capability. AppSync requires the mount host to be zoned to the VMAX V2 array. You should create a masking view with the appropriate initiator group, port group and storage group.

When AppSync performs a mount operation on VMAX V2, it discovers the host initiator for the mount host first. Based on the host initiator, it maps to the appropriate masking view to determine the Storage Group to or from which the target LUNs are masked/unmasked to perform a mount/unmount operation.

You can select the desired FAST policy for the target LUN in the mount step of the service plan. If there is a storage group for the mount host with the desired FAST policy, 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.

Note:

- When you select FAST policy, ensure that the storage pool of the storage group (FAST policy's storage group) and the storage pool of the copy devices are of the same storage pool type (that is, they must be on the same storage tiers). If the copy devices and FAST policy storage pools are on different storage tiers, the copy devices cannot be moved between different storage tiers and mount operation fails. For example, if a VMAX V2 source device is created on a Flash Drive Pool and a TimeFinder Snap is also created from the same pool in AppSync, to mount the copy to a desired FAST policy, ensure that you select a FAST policy associated with the Flash Drive Pool because LUNs cannot be moved from one tier to another having pools with mismatched disk drives.
- To use the FAST policy feature after an upgrade from AppSync 2.2.3 or earlier versions to 3.0, rediscover the array.
- Do not change the name of the storage group for the mount host when the copy is mounted. If you change the name of the storage group, ensure that you revert to the original name before unmounting the copy from AppSync.
- Multiple AppSync servers must never use or share the same storage group from a given VMAX V2 array.

For RDM or Vdisk mount/unmounts, AppSync identifies the Masking view based on the host initiator for the ESX server.

Note: All the AppSync provisioned storage pool devices created by AppSync is moved to an AppSync created internal storage group. This internal storage group is not visible to the user. It is created to handle the AppSync provisioned devices efficiently.

Microsoft Cluster Server mounts for SQL Server

Microsoft Cluster Server (MSCS) mounts for SQL Server can be done on production or alternate clusters.

When you mount to a cluster node using VMAX V2 storage:

- The storage group configuration applies only to physical hosts or virtual machines with iSCSI that are directly connected to the VMAX V2. For clusters configured using virtual machines with RDM or virtual disk, the copy mounted is only visible to the selected node (usually the passive node).
- When you mount to a cluster node for backup purposes, create a dedicated storage group for one of the nodes of the cluster, preferably the passive node.
- AppSync does not support mount to a cluster as a clustered resource. To mount to a cluster as a clustered resource (in a physical/iSCSI environment), deselect the default setting **Use dedicated storage group** on the AppSync mount dialog . During mount AppSync will make the copy visible to multiple nodes in the cluster by using a Storage Group with multiple assigned nodes. AppSync also mounts the filesystems to the selected mount host. After the completion of AppSync mount, manually add the mounted devices under cluster management to avoid the possibility of any data corruption.

Repurpose copies on VMAX V2

Consider this information when repurposing Oracle and SQL Server database copies residing on a VMAX V2.

You can repurpose a VMAX V2 source copy where the database resides or the source can be the target device in an SRDF session.

You can only repurpose a 1st Gen copy from the source, or a 2nd Gen copy (copy of the copy).

You can repurpose a RecoverPoint bookmark copy of a File System, Oracle, or SQL Server database.

When considering repurposing, review the following information:

- VMAX does not support a mix of thick and thin devices in cascading.
- A first generation copy must be a clone. The second generation copy can be a clone or a TimeFinder VP Snap.
- If the source device is thick, then the first and second generation targets are thick. If the source device is thin, AppSync only supports a clone of a clone for the source device.
- If the source is thin, AppSync supports both a TimeFinder VPSnap of clone and a clone of a clone.
- The first generation copy can be a remote copy or local copy in an SRDF session. But the second generation is local only.
- If you have thick source devices, configure the storage group with thick devices, otherwise the first generation copy creation fails.

VMAX V2 restore

VMAX V2 restricts the maximum number of hops in cascading to two.

If source A has the following sessions such as A > D and A > B > C (when created by a service plan or using Repurposing workflow), then during the restore from D the number of hops changes to 3 as the restore session leads to D > A > B > C. Therefore, Appsync provides an option to terminate the session B > C if it is a clone.

During consecutive runs if AppSync chooses C as a target for B, then it will be a full sync instead of a resync since the session B > C will be terminated during restore.

For example:

A > B > C

A > D > E

Restore from B will terminate D > E. Restore from D will terminate B > C. Necessary sessions will be terminated only if you select the option.

If the second generation copy is a TimeFinder VP Snap, you must expire second generation snaps manually. The restore fails if a snap of clone exists for source and displays all the copies that need to be expired in the progress window.

Note: Refer to the *AppSync VMAX Array Support Guide* on support.dell.com for additional information.

VMAX3/PowerMAX and VMAX All Flash

VMAX3/PowerMAX and VMAX All Flash arrays are supported with AppSync. This section describes supported features, and service plan considerations including mount/unmount and restore of VMAX3/PowerMAX and VMAX All Flash copies.

To create and manage copies in VMAX3/PowerMAX, it is required to register U4P(Unisphere for PowerMAX) in AppSync. AppSync supports SRDF/M, SRDF/S, and SRDF/A environment for VMAX3/PowerMAX.

Note:

- In this document, all mentions of VMAX3 includes information and instructions for VMAX All Flash and PowerMax arrays.
- SRDF/Metro is supported only for Repurposing service plans with site selection.

To create and manage copies of applications, AppSync supports SnapVX snapshot replication technology in VMAX3/PowerMAX and VMAX All Flash arrays.

Service plan considerations for applications on VMAX All Flash and VMAX3/PowerMAX storage

Review these considerations for service plan support with VMAX3/PowerMAX and VMAX All Flash.

Overview

After you register (add) VMAX3/PowerMAX, and VMAX All Flash, storage, subscribe an application to a service plan to create and manage copies.

Bronze, Silver, and Gold service plans are supported with VMAX3/PowerMAX, and VMAX All Flash. Snap in a service plan with VMAX3/PowerMAX and VMAX All Flash is equivalent to a SnapVX snapshot linked in *no copy* mode. Clone in a service plan is equivalent to SnapVX snapshot linked in *copy* mode. The default preference for a service plan is Snap.

If the source device is expanded online in a VMAX3/PowerMAX and VMAX All Flash array, expand the target devices in the storage group configured in the AppSync server, or add new devices with the same geometry as the source device.

If the target storage being used is provisioned by AppSync from SRP, it must be expanded online to match the geometry of the source device.

Note:

- In the case of Gold service plans (simultaneous local and remote copies), AppSync requires U4P (Unisphere for PowerMAX) that has gatekeepers presented from both the local and remote array.
- In the case of remote SRDF copies (on R2 devices) for Silver and Gold service plans, AppSync requires U4P (Unisphere for PowerMAX) that has access to both the local and

remote array. See the *AppSync VMAX Array Support Guide* on <https://support.dell.com> for additional information.

SnapVXClone optimization

AppSync supports both storage group level and volume group level snapvx snapshots based on application volume storage group layout in array.

The SnapVX clone is created and linked with the target device during copy creation. AppSync optimizes the SnapVX clone linking using the relinking strategy. While linking the SnapVX clone with the target device, AppSync attempts to find a suitable target device, which is already linked with a previous SnapVX of the same source device, and can be used for relinking. If you relink the new SnapVX with the same target device, it only synchronizes the delta data, that is the data that changed from the earlier SnapVX to the new SnapVX. This minimizes the linking time for larger devices. The non-repurposing service plan employs the relinking feature during copy creation. The repurposing service plans can refresh the repurposed copies and use the relink feature.

i Note:

- To support clone relinking, n+1 set of target devices are required for n copies. For example, if there are seven copies, then eight target devices are required for each source device. This is applicable for VMAX3/PowerMAX, VMAX All Flash, and SnapVXClone. In the absence of the extra set of target devices, the SnapVX clone creation might fail with an error.
- For storage group level copies, the storage group should be intact to mount and restore existing copies. Due to array-related restrictions, adding devices to the storage group or renaming the storage group (after a copy is created) would cause link failure during mount and restore of copies.

Restore VMAX3/PowerMAX and VMAX All Flash copies

When you restore SnapVX copies in AppSync, it restores the data from the SnapVX snapshots created on the array for the source devices, or from linked devices (in the case of mounted copies).

- Restore from snapshot — Restores copies from unmodified SnapVX snapshots.
- Restore from changed data — Restores from the SnapVX snapshot linked device, which retains the changes in the mounted copies.

i Note: Restore from remote copies is not supported for VMAX V2, VMAX3/PowerMAX, and VMAX All Flash arrays in an SRDF environment.

i Note: In SRDF Metro, restore is supported for R1 copies, restore is not allowed for R2 copies.

Mount/unmount VMAX3/PowerMAX and VMAX All Flash copies

Mount/unmount operations on VMAX3/PowerMAX and VMAX All Flash include masking/unmasking LUNs or a set of LUNs to a host. AppSync relies on the VMAX3/PowerMAX and VMAX All Flash Auto-Provisioning capability.

The mount host must be zoned to the VMAX3/PowerMAX and VMAX All Flash array. Next, you can create a masking view with the initiator group, port group, and storage group.

When AppSync performs a mount operation on VMAX3/PowerMAX and VMAX All Flash, 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 required Service Level Objective (SLO) for the target LUN in the mount step of the service plan run. If there is a storage group for the mount host with the required 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.

If the selected storage group does not have any SLO, the devices are not removed from the AppSync configured storage group.

Do not use the AppSync created internal storage group for any other operation. Also, ensure that you do not configure an SLO for this storage group. The format of the AppSync internal storage group is <hostname>+"__INTERNAL-AppSync"+number format. For example, the AppSync internal storage groups created for the AppSync server lmp253 are lmp253__INTERNAL-AppSync-0, lmp253__INTERNAL-AppSync-1, lmp253__INTERNAL-AppSync-2, and so on.

If multiple storage groups exist on the array for the same mount host with the same SLO, AppSync sorts the storage groups alphabetically and selects the first one from the list. If you want AppSync to use a specific storage group, rename the storage group in such a way that it appears on top of the list when sorted. The service plan must be recreated for this change to take effect.

Note:

- Do not change the name of the storage group for the mount host when the copy is mounted. If you change the name of the storage group, ensure that you revert to the original name before unmounting the copy from AppSync.
- All the AppSync provisioned storage pool devices created by AppSync is moved to an AppSync created internal storage group. This internal storage group is not visible to the user. It is created to handle the AppSync provisioned devices efficiently.
- Multiple AppSync servers must never use or share the same storage group from a given VMAX3/PowerMAX array.

VMAX3/PowerMAX and VMAX All Flash repurpose overview

Review VMAX3/PowerMAX and VMAX All Flash support for Repurposing.

AppSync supports local and remote repurposing of VMAX3/PowerMAX and VMAX All Flash SnapVX copies. Refresh of an existing copy will create a new snapshot of the source LUN and link it to the original target of the copy in the required mode. The old snapshot is then expired.

AppSync supports SRDF Metro for local repurposing. The following SRDF Metro options can be configured in the **Create the Copy** step, during copy creation for data repurposing:

- **Wait for VMAX3/PowerMAX clone sync to complete**
- **Array Selection (Applicable only for SRDF/Metro)**
- **Select Storage Groups to be used for VMAX-3 array(s)**

Use the Repurpose wizard to create a local or remote repurposed copy with VMAX3/PowerMAX and VMAX All Flash.

Note: Refer to the *AppSync VMAX Array Support Guide* on support.dell.com for additional information.

XtremIO

Review the supported applications, replication technology, configuration requirements, and restrictions for XtremIO arrays with AppSync before you begin the installation.

AppSync creates write-consistent snapshots on the XtremIO array for each application you add to a service plan. AppSync XtremIO supports the following applications:

- Oracle databases
- SQL Server databases
- Exchange databases and DAG
- File systems
- VMware data stores

After you register XtremIO storage, you can subscribe to the Bronze or Silver service plan to create and manage local or remote copies for operation recovery and backup acceleration. After you register XtremIO storage, AppSync selects snap for the selected service plan by default.

Note: Remote replication is supported only on XtremIO 6.1 and later.

For remote protection (using the Silver service plan), both the source and the target devices must be in a consistency group. AppSync creates a local bookmark which, based on the XtremIO policy, gets shipped to the target XtremIO array, after which, the local bookmark gets deleted.

In the case of remote repurposing, the first generation copy is the linked consistency group repurposed from the shipped bookmark. The second generation copy is the linked consistency group repurposed from the linked consistency group of the first generation copy.

In remote repurposing, refreshing the linked consistency group of a first generation copy creates a new bookmark to refresh the existing linked consistency group.

Note:

- For remote protection and repurposing of XtremIO VSS applications, a maximum of four consistency groups are supported.
- Static mount is supported for remote copies. However, it is not supported for repurposing.

AppSync supports the use of XtremIO consistency group APIs to create and refresh snapshots, allowing for the fastest possible operation time. However, support is limited to the repurposing workflow. The minimum XtremIO version required is 4.0.2.

For XtremIO release 6.2 and later, consider the following:

- For protection local copies, the Quality of Service (QoS) policy is applied to the read/write snapshots that are created during mount.
- For repurposing local copies, the QoS policy is applied to the read/write snapshot volumes, and are not linked to consistency groups (CG).
- During protection for remote copies, the QoS policy is applied on the target CG volumes of remote replication sessions.
- For repurposing remote copies, the QoS policy is applied on the read/write snapshot volumes on the target array, and not on the linked CG.

Note:

- XtremIO QoS policy is not supported along with AppSync mount overrides.
- XtremIO QoS policy is not supported for RecoverPoint bookmark copies.

- XtremIO QoS policy is not supported for second generation copies created before the AppSync 3.9 release.

For XtremIO release 6.1 and later, consider the following:

- During protection, AppSync creates a snapshot-set with read-only immutable copies using the source volume list or source consistency group depending on the application volume layout. When mounting these copies, AppSync creates an additional snapshot-set of read-write volumes from the read-only copy.
- For repurposing, AppSync creates a linked consistency group, if all the repurposed production volumes belong to a single consistency group. Otherwise, a snapshot-set with read-write copies are created.

(For releases earlier than XtremIO 6.1) To use XtremIO consistency group APIs, the following conditions must be met:

- All source LUNs must have the same consistency group
- All source LUNs must be part of only one consistency group
- All snapshots must be part of a single Snapshot-set (consistency group level refresh or restore)

Note: A single source LUN in a consistency group is also supported.

For Windows based applications, all the LUNs must be in one consistency group.

For Oracle, all archive log LUNs must be part of one consistency group and the database LUNs must be part of a different consistency group.

If applications span across consistency group and non-consistency group volumes, repurpose the applications on consistency group and non-consistency group volumes separately.

Note: If a single application entity is on both consistency group and non-consistency group volumes, AppSync treats the volumes as non-consistency group volumes during affinization.

Restrictions

Consider the following restrictions for XtremIO with AppSync:

- XtremIO Initiator Groups must be defined in XtremIO for all mount hosts to which AppSync mounts XtremIO copies.
- AppSync does not support XtremIO with iSCSI connectivity for AIX hosts.
- XtremIO remote protection and repurposing use cases are not supported, if:
 - The source and target arrays are managed by the same XMS
 - The source array has a replication session with more than one target array
- Do not change the name of the initiator group for the mount host when the copy is mounted. If you change the name of the initiator group, ensure that you revert to the original name before unmounting the copy from AppSync.

Configuration considerations

- The XtremIO Management Server (XMS) should be configured on a SAN with at least one XtremIO array.
- Zone XtremIO arrays to production and mount hosts (physical) or ESX servers (virtual).
- For mount and unmount of copies:
 - Ensure that you configure Oracle or SQL Server databases on XtremIO arrays for data and logs.
 - Fibre Channel and iSCSI are supported.

Considerations before adding an array:

To add and configure an XtremIO array to work with AppSync, you need at least one XtremIO Management Server (XMS) configured for that XtremIO array. Review the following considerations before adding an array:

- Administrator privileges are required to add the XtremIO array.
- Ensure XtremIO storage is zoned to production hosts (physical) or ESX servers (virtual). RDM and virtual disk are supported on VMware virtual machines. iSCSI is supported for Windows and Linux hosts, allowing you to see XtremIO storage over an iSCSI LAN. iSCSI is supported for physical or virtual hosts, and also ESX servers.
- Oracle, file systems and VMFS data stores on Linux/AIX are supported. File systems and virtual disks are supported on Windows.
- You need the XMS name/IP address and credentials.

Note: If you change the array credentials, ensure that you update the same in AppSync before attempting any operation.

The *AppSync Installation and Configuration Guide* provides instructions to add an XtremIO array.

Restore options with XtremIO storage

Learn about restore options for application copies on XtremIO arrays when planning the installation.

AppSync 2.2.2 and later supports automated restore of XtremIO 4.0 and later copies. The following applications are supported:

- SQL Server databases
- Exchange standalone databases and Exchange Data Availability Groups (DAG)
- VMware data stores
- File systems
- RecoverPoint

AppSync uses the Restore wizard for automated restore on XtremIO storage. Click the Restore button to launch Restore wizard for respective applications. During restore, AppSync creates another XtremIO-generated snapshot, stored under the tag `/volumes/AppSyncSnapshots/RestoredSnapshots`. An Administrator must clean up these snapshots manually.

XtremIO remote restore considerations

When restoring a remote XtremIO Snapshot copy, AppSync:

- Fails over the local array replication session using Appsync-created remote bookmark.
- Refreshes the remote CG using linked CG, if the restore is from remote repurpose copy.
- Starts the replication session in the reverse direction.
- Fails over the remote array using the sync-and-failover option, and resumes the replication session on the local array.

Note: Appsync does not create rollback snapshots for XtremIO remote restore.

If there are other applications sharing the same storage device or the same CG, with the application that is being restored, then ensure that they are stopped before attempting a restore from AppSync. AppSync can only quiesce the application that is being restored.

RecoverPoint

Consider best practices for RecoverPoint setup before deploying AppSync. For example, be sure to observe RecoverPoint consistency group granularity best practices.

Service plan considerations for applications with RecoverPoint protection

AppSync supports different RecoverPoint replication options.

Three types of replication options:

Local (Continuous Data Protection)

In Local protection, RecoverPoint replicates to a storage array at the same site. In a RecoverPoint installation that is used exclusively for local protection, you install RPAs at only one site and do not specify a WAN interface. The Bronze service plan protects application replication.

Remote (Continuous Remote Replication)

In Remote replication, RecoverPoint replicates over a WAN to a remote site. There is no limit to the replication distance. The Silver service plan protects application replication.

Local and Remote (Concurrent Local and Remote)

In Local and Remote replication, RecoverPoint protects production LUNs locally using local protection and remotely using remote replication. Both copies have different protection windows and RPO policies. The Gold service plan protects application replication. RecoverPoint multi-site (multiple remote sites) is not supported at this time.

Note: For RecoverPoint bookmarks:

- Source VNX volume, target VMAX V2 volume—virtual and virtual with roll access modes are not supported.
- Source VMAX V2 volume, target VNX volume—virtual and virtual with roll access modes are supported.

RecoverPoint prerequisites

Verify that the RecoverPoint configuration meets the prerequisites necessary for use with AppSync.

- Install and configure RecoverPoint according to the RecoverPoint documentation.
- Use RecoverPoint to create consistency groups.
- Ensure that the splitters for all mount hosts are attached to the RecoverPoint target volumes they are going to use.
- Synchronize time on all systems. Follow the steps in the operating system documentation to configure the AppSync server and all production and mount hosts to be synchronized with a time server. This includes all hosts, VNX, Unity storage, and RecoverPoint appliances.
- For failover preparation, keep in mind that AppSync requires that RecoverPoint Local and Remote consistency groups have both local and remote copies, even in a failover situation. This may require RecoverPoint administrator configuration steps after failover to configure a local copy on the remote site.
- During AppSync configuration, the RecoverPoint site is added as a resource. In a Local and Remote configuration, AppSync discovers all sites in the RecoverPoint system configuration.

Credentials for an account that has RecoverPoint admin privileges is required when adding the site.

Dynamic or static mounts

RecoverPoint copies can be mounted in two ways, statically or dynamically.

AppSync supported static mounts of RecoverPoint targets. Using static mounts, the RecoverPoint target LUNs (Local or Remote) had to be pre-exposed (masked) to the mount host before you could mount the RecoverPoint copies. If you are using static mounts in a virtual machine environment, the RecoverPoint target LUNs must be masked to the ESX server, and added as RDMs to the virtual machines prior to mounting the copy.

RecoverPoint targets may also be dynamically mounted. RecoverPoint target LUNs are mapped at mount time to identify the LUNs, and the LUNs are masked (moved to the mount host storage group) and surfaced prior to mounting. When the target LUNs for dynamic mount are on VNX storage, the VNX must be registered with AppSync. This is also applicable for Unity storage.

AppSync does not have a prerequisite that replica devices must be made visible to the mount host. AppSync can dynamically expose devices across all storage technologies. For VMAX V2 and VMAX3/PowerMAX, AppSync does not support static mounts. This is also applicable for RecoverPoint environments involving VMAX V2 and VMAX3/PowerMAX.

For VMAX V2 dynamic mounts, follow the VMAX V2 auto provisioning instructions so that masking succeeds.

If you are using dynamic mounts in a virtual environment, do not mask the target LUNs to the ESX server. AppSync will mask the LUN to the ESX server, and then add the LUN as an RDM to the mount host. Refer to [Mount and unmount VMAX copies](#).

When unmounting:

- LUNs which were dynamically mounted are dynamically unmounted, that is, the LUNs are removed from the storage group.
- LUNs which were statically mounted remain in the storage group after the unmount completes.
- For application copies with LUNs that are mixed (both statically and dynamically mounted), the LUNs will be dynamically unmounted. All mounted LUNs are removed from the storage group.

Given proper zoning, AppSync presents storage to the host automatically when a copy is mounted.

Physical host

AppSync dynamically assigns a snapshot to the host when the copy is mounted. The physical host must be zoned to the VNX or the Unity array of the RecoverPoint target LUNs (Local or Remote).

Virtual machine

Dynamic mounts happen as a raw device mapping (RDM) or through native iSCSI on the VM.

- For RDM, the ESX server where the VM resides must be zoned to the VNX or the Unity array of the RecoverPoint target LUNs (Local or Remote).
- For RDM and virtual disks, virtual center (which manages the ESX server where the VM mount host resides) must be registered with the AppSync server.
- For native iSCSI, the virtual machine must be logged into the array (VNX or Unity) initiators of the RecoverPoint target LUNs (Local or Remote). The VNX must have a storage group defined for the host.

Repurpose RecoverPoint Bookmark copies of Oracle or SQL Server databases

AppSync supports the ability to repurpose RecoverPoint Bookmark copies for Oracle or SQL Server databases.

Use AppSync to repurpose a RecoverPoint Bookmark on a VMAX V2 target (VMAX3/PowerMAX is not supported) and create a first generation (1st Gen) copy, which leverages TimeFinder Clone or TimeFinder VPSnap replication technology. You can repurpose the clone copy further (not for VPSnap) to create a 2nd Gen copy that leverages TimeFinder Clone or TimeFinder Clone VPSnap.

- **Bookmark (hidden) > Clone**
- **Bookmark (hidden) > Clone > Snap**
- **Bookmark (hidden) > VPSnap**
- **Bookmark (hidden) > Clone > Clone**

To copy Bookmarks, use the RecoverPoint repurpose wizard. The RecoverPoint Appliance and SMI-S provider or VNX must be registered in AppSync.

Supported configurations include:

- Application: Oracle and SQL Server
- Storage: VNX and VMAX V2 (1st Gen copy is a VMAX V2 copy)
- Bookmark: The 2nd Gen copy is a copy of the 1st Gen copy).

In the repurpose wizard, select **Use Bookmark as an intermediate step** to perform RecoverPoint repurposing. If you do not select this option, AppSync begins native repurposing. The drop-down list lists **create a 1st Gen copy from site**. This option determines if the system uses RecoverPoint Continuous Data Protection or RecoverPoint Continuous Remote Replication Bookmark repurposing.

Considerations

- If you refresh the 1st Gen copy, AppSync takes a new copy of the database.
- 1st Gen and 2nd Gen copies are always local.
- Manual expire of 1st Gen the Bookmark copy.
- Refresh a 2nd Gen to create a copy of the 2nd Gen from the 1st Gen.
- If the 1st Gen copy is a VMAX V2 clone, the same LUN is used during refresh (instead of rotation).

Repurpose (create) a 1st Gen copy of a RecoverPoint Bookmark

Learn to repurpose a RecoverPoint Bookmark on a VMAX V2 target and create a 1st Gen (clone) copy of an Oracle or SQL Server database, which leverages TimeFinder Clone or TimeFinder VPSnap replication technology. You can repurpose the clone copy further (not for VPSnap) to create a second generation copy that leverages TimeFinder Clone or TimeFinder Clone VPSnap.

Before you begin

The RecoverPoint Appliance and the underlying storage array (VNX, SMI-S, Unity, or XtremIO) must be registered in the AppSync Server.

About this task

To copy Bookmarks, use the RecoverPoint repurpose wizard.

Procedure

1. Log in to the AppSync console and select **Copy Management**.

2. Click **Select View > Copies**.
3. Click **Select Application > Oracle / Microsoft SQL Server / VMware Datacenters / File Systems / Microsoft Exchange**.
4. Click the name of the database, instance, or file system that contains copies.
5. Click **MORE > Repurposed Copies** to view the repurposed copies for all the databases, or application instance.
The **Repurposed Copies** window appears. copies.
6. Click **Create second generation copy**.
7. In the repurpose wizard, select **Use Bookmark as an intermediate step** to perform RecoverPoint repurposing.

Unity

This section describes Unity support with AppSync. It includes information on configuration considerations, supported service plan and application details.

Unity arrays support all applications within AppSync.

AppSync does not support the following configuration with Unity:

- Unity File storage on Windows platform

Unity copy management

This section describes a typical AppSync workflow where you can create and manage application-consistent copies on Unity storage. AppSync manages Unity arrays with the Management Interface instead of the Service Processor interface.

Perform resource registration for Unity when you start AppSync after installation. Register hosts as well as vCenter and storage systems so that AppSync can perform various operations that are required to create and manage copies of applications. Typically, registration of an entity includes identifying the system using name/IP address and providing the necessary credentials (username/password) for AppSync to discover and operate on the registered system.

Note: AppSync rediscovers file systems, interfaces, and file shares every hour. Therefore, any new file, file system, or file share added on the array is not identified by AppSync until the next refresh cycle.

Protecting Unity Block storage (Silver and Gold plans)

AppSync supports asynchronous and synchronous replication types.

Note: Manual replication is not supported.

- Asynchronous replication — During remote protection (using Gold or Silver service plan), AppSync first creates a Unity snapshot on the local array, and then using the Unity Snapshot shipping technology, remote snapshots are created on the remote array.
Note: In the case of a Silver service plan, snapshots created on the local array are removed.
- Synchronous replication - During remote protection, AppSync creates the copy directly on the remote array, in the case of a Silver service plan.
Note: AppSync does not support remote protection, if the replication session is configured between pools within the same array.

Storage and replication type

AppSync supports Unified Snapshot replication technology to create and manage:

- Local copies of applications that reside on Unity block or file storage.
- Remote copies of applications that reside on Unity Block storage. Supported only on Unity 4.2 and later.

Source block storage LUNs can be pool LUNs that are either thick or thin. You can provision the required source block devices using the Unity LUN or VMware data store wizards within the Unisphere UI. When creating basic LUNs using the LUN wizard select one of the following options:

- Create a LUN - Creates an individual LUN from a desired storage pool.
- Create a Consistency group - Creates a grouping of LUNs from a desired storage pool. The advantage of using a consistency group is that all LUNs within the group are snapped together guaranteeing consistency on the array.

Best practice states that in Microsoft environments you must use consistency groups in their storage layout to help the application consistent creation of Unity snapshots within the Microsoft VSS Service time window.

You can provision the required source file devices using the Unity file system or VMware data stores wizard. When provisioning from the file system wizard, only NFS share file systems are supported.

Service plan considerations with Unity

Before you add a service plan to create Unity copies, review these considerations.

After you register Unity storage, you can subscribe to the Bronze, Silver, or Gold service plan to create and manage local or remote copies for operation recovery and backup acceleration. After you register Unity storage, AppSync selects snap for the selected service plan by default.

For copies across RecoverPoint Remote replication or Local and Remote replication, subscribe to Silver or Gold service plan respectively. You can change snap to Bookmark for RecoverPoint copies.

Mounting and unmounting Unity NFS datastore copies

Review the following information for NFS datastore mount/unmount.

AppSync creates a share based on the Unity file snap that you want to mount. The share is visible to the mount host. During unmount, the share created during the mount is deleted. The share name appears in the following format:

```
AS-Share-  
lastFourDigitOfUnitySerialNum-ProductionFilesystemId-  
TimeOfShareCreated
```

AppSync creates a list of export IP interfaces from the Unity array. Production export IP is a priority.

Mounting and unmounting Unity copies

Review this information before you mount and unmount Unity copies with AppSync.

Mount and unmount operations on Unity arrays involve attaching and detaching snapshots to SMPs, and granting and removing (masking/unmasking) snapshot access to SMP LUNs or a set of SMPs to a host. Unity OE versions prior to 4.1 only allow attaching one snapshot at a time for a set of LUNs or consistency groups to SMP LUNs. This restriction does not apply for OE versions 4.1 and later. LUNs contained in a consistency group are attached and detached together, there is no partial attach or detach.

Before performing a mount or unmount, zone the mount host to the Unity array, and register the host name with its initiators.

The first step AppSync performs when mounting a snapshot on Unity, is host initiator discovery for the mount host. Based on the snapshot information, AppSync maps to the appropriate source LUN/consistency group(s) to determine host access for the mount host.

AppSync verifies that no other snapshots are attached to the SMP LUNs. Next AppSync modifies host access to either grant snapshot access to perform a mount, or remove host access to unmount.

For RDM or vDISK mount/unmount, AppSync identifies host access based on the host initiator for the ESX server.

Mounting and unmounting Unity NFS File system copies

Review the following information for NFS File system mount and unmount.

AppSync creates a share based on the Unity unified snapshot for file that you want to mount. The share is made visible to the mount host by exporting the NFS file system's unified snapshots, and the file system is created on that NFS exports. During unmount, the file system is unmounted and the NFS share created during mount is deleted. The share name appears in the following format:

```
AS-SharelastFourDigitOfUnitySerialNum-ProductionFilesystemId-
TimeOfShareCreated
```

AppSync creates a list of export IP interfaces from the Unity array. Production export IP is a priority.

Oracle database on Unity NFS file system is supported. The unified snapshots for file is created for Oracle data and logs. During mount of an Oracle database, use one of the following options:

- Mount and Recovery - This option mounts the file system on the mount host and recovers the database.
- Mount the file system - This option only mounts the file system on the mount host.

Unity restore considerations

Consider the following when restoring data from Unity copies.

- When restoring a local Unity Snapshot copy (if synchronous replication is configured), AppSync pauses the synchronous replication session and resumes the session after the copy is restored.
- When restoring a remote Unity Snapshot copy, AppSync:
 - Fails over the local array replication session.
 - Resumes the remote array replication session.
 - Restores and waits for data synchronization to complete.
 - Fails over the remote array, and resumes the replication session on the local array.
- If there are other applications sharing the same storage device with the application that is being restored, ensure that they are stopped before attempting a restore from AppSync. This is because AppSync can only quiesce the application being restored.
- For any application restore on Unity arrays, ensure that all IO's on the LUN is stopped.

Repurposing copies on Unity

AppSync supports repurposing application copies on Unity arrays. Both snapshot and thin clone copy technologies of Unity are supported. The minimum Unity version required is 4.2.

[Repurposing overview](#) provides additional information on repurposing.

- The first generation copy is always a snapshot.
- The second generation copy can either be a snapshot or a thin clone. By default, the second generation copy is a snapshot. You can change the default option.
- First generation snapshots must not be mounted when creating or refreshing a second generation thin clone.

For additional information on Unity snapshot and thin clone copy technologies, see Unity documentation.

VPLEX

AppSync can create application consistent and crash consistent Snapshot (VPLEX Snap and VPLEX Clone) copies on the underlying managed array hosting VPLEX virtual volumes. AppSync supports the following applications on VPLEX storage:

- Oracle databases
- SQL Server databases
- File systems
- Microsoft Exchange
- VMware data stores

The following VPLEX device configurations are supported:

- VPLEX Local
 - RAID 0
 - RAID 1
- VPLEX Metro
 - Distributed devices

Note:

- VPLEX virtual volumes must be mapped 1:1 to an array volume.
- Concatenated devices (RAID-C) are not supported.
- Nested devices are not supported.
- Remote volumes (local device with global visibility by setting remote access) is not supported.
- If there is a mobility job in progress, the device cannot be protected until the mobility job completes.

Service plan considerations for applications on VPLEX storage

After you register VPLEX storage, you can subscribe your application to a service plan to create and manage copies.

- AppSync supports the Bronze service plan for applications on VPLEX storage. This means that you can only create application specific local copies.
- When you select the storage preference as Snapshot in a service plan, AppSync creates a snapshot on the back-end storage array.
- During mapping, AppSync queries VPLEX about the virtual volume details such as device components, extents, and storage volume. It then communicates to the back-end storage array and maps the corresponding storage LUN to be protected.

- If applications on the same hosts are from different VPLEX clusters, the applications are grouped separately during protection.
- If applications are on the same host and on the same VPLEX virtual volumes, they are grouped together during protection.
- If the underlying VPLEX storage device is a RAID1, or a distributed device, you must configure storage options in the create copy options under service plans.
- A VPLEX virtual volume on a RAID 1 device has two legs. The two legs can be from two different back-end storage arrays. The leg to be protected is determined by the array that is selected in configure storage options. A VPLEX distributed virtual volume has storage devices on both the clusters. The leg to be protected is determined by the cluster that is selected in configure storage options.
- In the case of RAID 0 devices, the VPLEX back-end array's storage LUN which maps to the VPLEX virtual volume is protected.
- In the case of RAID-1 devices, the VPLEX back-end array's storage LUN which maps to the selected leg of the RAID-1 device is protected.

Mount and unmount VPLEX copies

Review this information before you mount and unmount VPLEX copies with AppSync.

AppSync provides two mount options:

- Mount as VPLEX virtual volumes
- Mount as native array volumes

Mount as VPLEX virtual volumes

When you select this option, the snapshot on the back-end array is made visible to VPLEX. AppSync creates VPLEX virtual volumes on the underlying native array snapshots and provisions these virtual volumes to the mount host. The provisioned virtual volumes are added to the storage view of the mount host. During unmount, the virtual volumes are removed from the storage view of the mount host, and it tears down the created VPLEX virtual volume on the underlying native array snapshots. The snapshot on the back-end array is de-provisioned from VPLEX.

Consider the following:

- The mount host must be zoned to the VPLEX cluster where the production copy is created.
- The mount host must be zoned to VPLEX, but does not have to be zoned to the native array where the snapshot is created.
- Copy of production volumes on VPLEX RAID 0 devices are mounted as local RAID 0 volumes on the same cluster.
- Copy of production volumes on VPLEX RAID 1 devices are mounted as local RAID 1 devices with a single leg on the same cluster. If you manually add a mirror leg, ensure that you manually remove that leg before unmount.
- Copy of production volumes on VPLEX distributed RAID 0 devices are mounted as local RAID 0 volumes on the same cluster.
- Copy of production volumes on VPLEX distributed RAID 1 devices are mounted as local RAID 1 volumes on the same cluster. If you manually add a mirror leg, ensure that you manually remove that leg before unmount.

Mount as native array volumes

When you select this option, AppSync provisions the native array snapshots to the mount host. The mount host must be zoned to the native array where the snapshot is created. All other mount considerations of the native array are applicable.

Enable VMware cluster mount

If the mount host is a VMware virtual machine residing on an ESX cluster, the target LUN is made visible to all the nodes of the ESX cluster during mount. By default, this is enabled. If you do not want to perform an ESX cluster mount, you can clear this option. Then the target LUN is made visible only to the ESX cluster on which the mount host resides. This is applicable for both RDM and vDisk device types.

VPLEX restore considerations

Consider the following when restoring data from VPLEX Snap copies:

- The VPLEX production virtual volume layout must be the same as it was when the copy was created. If there is any change in the production virtual volume layout, AppSync detects it and the restore fails.
- In the case of a RAID 1 and distributed devices, AppSync restores one leg of the mirror for which the copy was created. The other leg is rebuilt and synchronized after restore is complete from the native array snapshots. If you do not want to wait for mirror synchronization, ensure that you clear the **Wait for mirror rebuild to complete** option in the Restore wizard.
- During restore, AppSync removes VPLEX virtual volumes from the consistency group, restores from native array snapshot, and adds the virtual volumes back to the consistency group. It also invalidates cache of all the VPLEX virtual volumes.
- AppSync does not support restore of VPLEX production virtual volumes, which are protected by RecoverPoint.
- When restoring from VPLEX Snap copies, ensure that no other operation is performed on the device being restored.

Dell SC

AppSync can create and manage application consistent copies on Dell SC storage, including mounting and recovering a copy of the application instance to the original or an alternate host.

AppSync supports the following applications on Dell SC storage:

- Oracle databases
- SQL Server databases
- File systems
- Microsoft Exchange
- VMware data stores

AppSync does not support the following configuration with Dell SC storage:

- Repurposing copies on Dell SC arrays
- Restoring copies on Dell SC arrays, except Granular File and VM restore
- File storage
- Live volume replication
- When number of volumes protected together exceeds the maximum limit of volumes in a snapshot profile, for that version of array.

Service plan considerations for applications on Dell SC storage

After you register Dell SC storage, you can subscribe applications to a service plan to create and manage copies.

AppSync supports the Bronze service plan for applications on Dell SC storage. This means that you can only create and recover application specific local copies on the local Dell SC storage array. AppSync supports the Dell SC Series Snapshot replication technology to manage local copies that reside on Dell SC storage.

Note: The name of the service plan that is used to protect the application on the Dell SC array, must not contain the <, >, or & symbols. If the service plan name contains these symbols, protection fails, as the snapshot profile name on the Dell SC array cannot contain these symbols.

Mount and unmount Dell copies

Mount or unmount operations on Dell SC arrays involve adding or removing snapshots to ViewVolumes, and granting or removing (masking or unmasking) snapshot access to ViewVolumes or a set of ViewVolumes to a host.

Before performing a mount or unmount, zone the mount host to the Dell SC array, and register the host name with its initiators (HBA WWN or IQN).

If the mount host is a virtual machine, the following is supported:

- Direct iSCSI connectivity to the virtual machine
- FC or iSCSI connectivity to the ESX hosting the virtual machine

PowerStore

This section describes PowerStore support with AppSync. It includes information about configuration considerations, supported service plan, and application details.

AppSync supports the following applications on PowerStore storage:

- Oracle Databases
- SQL Server Databases
- File Systems
- Microsoft Exchange Databases and DAG
- VMware data stores

Add a PowerStore appliance to AppSync

Perform this procedure to add a PowerStore appliance to AppSync.

Before you begin

Supply the credentials for an account that has the role of Administrator or Storage Administrator.

Note: This operation requires the Resource Administrator role in AppSync.

Procedure

1. On the AppSync console, select **Settings > Infrastructure Resources > STORAGE SYSTEMS**.
2. Click **ADD SYSTEMS**.

3. In the Select System Type page, select **PowerStore> Next**
4. Type credentials for the appliance in the following fields:
 - a. Management Interface: Type the fully qualified Name or IP Address of the Management Interface.
 - b. Username: Type the username.
 - c. Password: Type the password.
5. Click **Next**.
6. Select the PowerStore appliance that you want to add to AppSync, and then click **NEXT**.
7. Review the configurations in the Summary page, and click **FINISH**.

AppSync discovers and operates on the registered system.

Note: A single PowerStore management provider can manage a single or multiple appliances, and AppSync supports both the configurations.

AppSync manages PowerStore appliances with the Management Interface using REST APIs.

Service plan considerations with PowerStore

Before you add a service plan to create PowerStore copies, review these considerations.

AppSync supports Snapshot or Thin clone replication technology to create and manage:

- Local copies of applications that reside on PowerStore block storage using Bronze or Local Repurpose service plans.
- Remote copies of applications that reside on PowerStore block storage using Silver, Gold, or remote Repurpose service plans.

Note: AppSync supports PowerStore asynchronous replication type. When using remote protection service plans, AppSync first creates a PowerStore snapshot on the local array. It then uses the PowerStore Snapshot shipping technology and creates remote snapshots on the remote array.

For Gold service plans only, snapshots are retained on both local and remote arrays. For Silver or remote repurpose service plans, the intermediate snaps on local array are deleted.

Source block storage volumes can be individual or in groups (Volume group).

- Create a volume - Creates an individual volume.
- Create a Volume Group - Creates a grouping of volumes. The advantage of using a volume group is that all volumes within the group are snapped together. To guarantee consistency across volumes in a volume group, you must choose "Write order consistency" flag in the volume group settings on the array.

In Microsoft environments, you must use volume groups with "Write order consistency" in their storage layout. It helps to create application consistent PowerStore snapshots within the Microsoft VSS Service time window.

AppSync does not support the following configuration with PowerStore:

- PowerStore File storage.
- PowerStore Virtual Volumes.
- Remote replication from a source PowerStore appliance to multiple target PowerStore appliance.

Mount and Unmount PowerStore copies

Review this information before you mount and unmount PowerStore copies with AppSync.

Mount and unmount operations on PowerStore appliances for snapshots have an intermediate step of creating mountable objects or Thin clones. The clones are attached and detached to host or host-groups on PowerStore appliance. Volumes that are contained in a volume group are attached and detached separately one after the other.

Before a mount or unmount, zone the mount host to the PowerStore appliance, and register the hostname with its initiators.

 **Note:** Hosts must be zoned to all the PowerStore appliances in a multi-appliance cluster setup.

The first step AppSync performs when mounting a snapshot on PowerStore is host initiator discovery for the mount host. Based on the snapshot information, AppSync maps to the appropriate volume to determine host access for the mount host.

Next, AppSync attaches or detaches clone volumes to either grant host access to perform a mount, or remove host access to unmount.

For mount or unmount of RDM or vDISK, AppSync identifies host access based on the host initiator for the ESX server.

In a multi-appliance cluster setup, to migrate the volume whose copy is mounted, the copy should be unmounted first, before migrating the volume on the appliance. If not, the AppSync operations might fail. Also, rediscover the appliance in AppSync after migrating any resource on the appliance that AppSync is managing.

PowerStore restore considerations

Consider the following when restoring data from PowerStore copies.

- When restoring a remote PowerStore Snapshot or Thin clone copy, AppSync:
 - Syncs and Fails over the local array replication session
 - Resumes the remote array replication session
 - Restores and waits for data synchronization to complete
 - Syncs and Fails over the remote array session and resumes the replication session on the local array
 - Restores a copy either from snapshot or from changed data if the copy was created as a snapshot and was previously mounted from all the service plans and for all applications
- If there are other applications sharing the same storage device (or same volume group, if the replication session is created on volume group) with the application that is being restored, ensure that they are stopped before attempting a restore from AppSync. This is because AppSync can only quiesce the application being restored.
- For any application restore on PowerStore appliances, ensure that all IO's on the volume are stopped.

Repurposing copies on PowerStore

AppSync supports repurposing application copies on PowerStore arrays. Both snapshot and thin clone copy technologies of PowerStore are supported.

[Repurposing overview](#) provides additional information about repurposing.

- The first generation copy is a snapshot or a thin clone. By default, the first generation copy is a snapshot. You can change the default option.

Storage considerations

- The second generation copy is always a thin clone.

For additional information about PowerStore snapshot and thin clone copy technologies, see PowerStore documentation.

CHAPTER 13

Troubleshooting AppSync

This section provides information on the common problems encountered while using AppSync.

- [Automated log collection](#).....314
- [Dell EMC SupportAssist](#)..... 317
- [AppSync issues](#)..... 319
- [Error handling](#).....335
- [Event logging](#).....337

Automated log collection

AppSync provides an automated option to collect logs from the AppSync server, the AppSync agent hosts, vCenter servers, UNIVMAX and SMI-S providers.

The logs are collected and saved in a Zip file at the location that is specified during log collection. In the case of a failure, no logs are collected. You can use the collected logs to report issues that you might encounter when using AppSync.

The final log file includes:

- AppSync CAS logs
- AppSync server logs
- AppSync agent logs
- Vpxd logs from the selected Vcenter servers
- SMI-S logs from the selected SMI-S providers
- Consolidated agent logs from UNIX agent hosts
- U4P RESTAPI logs from selected UNIVMAX providers

The following items are packaged with AppSync:

- EMCGrab for Linux - Is packaged along with the agent_plugin_bundles (C:\EMC\AppSync\agent\agent_plugin_bundles\linux\current_appsnc_version) and is deployed on the agent host when log collection is initiated.
- EMCGrab for AIX - Is packaged along with the agent_plugin_bundles (C:\EMC\AppSync\agent\agent_plugin_bundles\aix\current_appsnc_version) and is deployed on the agent host when log collection is initiated.
- EMCRTPT for Windows agent - Is packaged with the Windows agent and is deployed on the agent host during the installation of the agent.

Note:

- AppSync server logs are collected by default.
- For log collection, you require Server Message Block (SMB) access (TCP port 135 and TCP port 445) from the AppSync server to the AppSync Windows host plug-in.

Collect Logs

AppSync provides an automated option to collect logs from the AppSync server, the AppSync agent hosts, vCenter servers, UNIVMAX and SMI-S providers.

Before you begin

This operation requires the Resource Administrator role in AppSync.

About this task

The logs are collected and saved in a Zip file at the location that is specified during log collection. You can use the collected logs to report issues that you might encounter when using AppSync.

The final log file includes:

- AppSync CAS logs
- AppSync server logs
- AppSync agent logs

- Vpxd logs from the selected Vcenter servers ,
- U4P RESTAPI logs from selected UNIVMAX,
- SMI-S logs from the selected SMI-S providers
- Consolidated agent logs from UNIX agent hosts

Procedure

1. On the AppSync console, select **Settings > Logs and Data Expiration**.
2. Click **COLLECT LOGS**.
3. Specify the location to store logs in the **Location to store logs** field.

The default location for this field is `C:\EMC\AppSync\jboss\advanced-logs`.

Note:

By default, the logs are retained for 20 days. To modify the default value:

- Go to **Settings > Logs and Data Expiration > Collect logs from registered hosts > Log retention**.
- Configure the **Update Log Retention (in days)** option, and click **APPLY**.

By default, log collection has a default timeout of 90 minutes. To modify the default value:

- Go to **Settings > Logs and Data Expiration > Collect logs from registered hosts**.
- Configure the **Update Timeout for log collection (in minutes)** option, and click **APPLY**.

4. Click **NEXT**.
5. Select one or more hosts from which logs must be collected. :

Note: AppSync server logs are collected by default.

- **Appsync host**
- **VMWare vCenter Server**
- **SMI-S Provider**
- **UNIVMAX**

6. (Optional) Select **Collect EMC Grab/EMCRPT** to collect the logs that are generated using the EMCGrab tool from the AppSync server and the agent hosts. This includes system logs, event logs, and so on, besides the AppSync logs. By default, this option is disabled, and only AppSync logs are collected from the agent hosts.

The following items are packaged with AppSync:

- **EMCGrab for Linux** - Is packaged along with the agent_plugin_bundles (`C:\EMC\AppSync\agent\agent_plugin_bundles\linux\current_appsync_version`) and is deployed on the agent host when log collection is initiated.
- **EMCGrab for AIX** - Is packaged along with the agent_plugin_bundles (`C:\EMC\AppSync\agent\agent_plugin_bundles\aix\current_appsync_version`) and is deployed on the agent host when log collection is initiated.
- **EMCRPT for Windows agent** - Is packaged with the Windows agent and is deployed on the agent host during the installation of the agent.

Note: AppSync server logs are collected by default. For log collection, you require Server Message Block (SMB) access (TCP port 135 and TCP port 445) from the AppSync server to the AppSync Windows host plug-in. For Unix agents, the `emcgrab` utility is installed under the `appsync` agent install directory. The default location is `/opt/emc/appsync/emcgrab`.

Note:

- For Unix agents, the `emcgrab` utility is installed under the `appsync` agent install directory. The default location is `/opt/emc/appsync/emcgrab`. If the `emcgrab` directory is deleted or corrupted accidentally, download the latest version of `emcgrab` from [Dell EMC Support](#) and install it under the installation directory of the AppSync agent.
- AppSync does not support log collection for SMI-S providers or UNIVMAX that are running inside arrays (embedded guests).
- For SUDO users, ensure that you create a folder under `/opt/emc/appsync/logcollection` with read, write, and run permissions. Also, add the following in the Sudoers file to grant permission to run the script (`/opt/emc/appsync/logcollection/get_smis_log.sh`) without any password:

```
<sudo_user_name> ALL = (root) NOPASSWD: /opt/emc/appsync/logcollection/get_smis_log.sh
```

7. (Optional) Select **Collect consolidated Log** to collect only consolidated agent logs. This option is only applicable for UNIX AppSync Host plug-ins.
8. (Optional) Select the vCenter servers to collect Vpxd logs. You can select multiple vCenter servers.

The vpxd logs include information about vSphere client and web service connections, internal tasks, events, and communication with the vCenter Server Agent (vpxa) on managed ESXi or ESX hosts. The vpxd files are zipped along with the AppSync server files, agent logs, U4P REST API logs and the SMI-S provider logs, if selected.

9. (Optional) Select the SMI-S providers to collect SMI-S logs for SMI-S providers on Linux and Windows hosts, and click **Next**.

Enter the username and the password of the host.

For a Windows SMI-S host, add the domain name before the username: `domain_name \user_name`

Note: Select **Save SMI-S/UNIVMAX Host Credentials** to save specified host credentials.

The SMI-S logs are zipped with the final logs. The format of the SMI-S logs is:

- Linux hosts: `SMIS_Log_<smis_host_name>_timestamp.tar`
- Windows hosts: `SMIS_Log_<smis_host_name>_timestamp.zip`

10. (Optional) Select the UNIVMAX server to collect U4P Rest API logs and enter the username and the password of the host.

Select **Save SMI-S/UNIVMAX Host Credentials** to save specified host credentials.

Note: Port 22 must be enabled for Linux hosts, to collect SMI-S logs or U4P REST API logs.

11. Click **Next**.

The Review screen appears.

12. Review the log collection summary, and click **Finish**.

The Log collection progress screen displays the progress of log collection.

13. Click **Close**.
14. Verify if the logs are collected.

The logs are located in a folder that is named with the current timestamp at the specified path. The log file format is `yyyy-mm-dd_hh.mm.ss` (for example, `2019-12-27_08.47.13`).

Dell EMC SupportAssist

Dell EMC SupportAssist is a software-based, secure access point for remote support activities between Dell EMC and your Dell EMC information infrastructure.

Dell EMC SupportAssist

Dell EMC SupportAssist is a software-based, secure access point for remote support activities between Dell EMC and your Dell EMC information infrastructure.

Before you begin

You can configure AppSync to communicate with SupportAssist and provide system configuration information to Dell EMC.

- This operation requires the Resource Administrator role in AppSync.
- You connect to Secure Remote Services (SRS)v.3.24 or connect through SupportAssist Enterprise 4.0+. SRS V3 (Virtual Edition) or SAE 4.0+ must be running in a supported VMware ESX or Microsoft HyperV environment.
- You require valid Dell EMC Online Support credentials.

Procedure

1. On the AppSync console, select **Settings > Dell EMC SupportAssist**.
2. Click **REGISTER**.

The **SupportAssist Enterprise Registration** page opens.

3. Type the **Active GateWay Name, User Name, Password**, and the **AppSync Server IP**.
4. Click **OK**.

Note: You can only register one SAE (SupportAssist Enterprise) gateway. If you want to register a different SAE gateway, remove the existing SAE gateway and add a new one. SAE cluster nodes are not supported.

Configuration information sent to Dell EMC through SupportAssist: AppSync sends a configuration file to Dell EMC daily, which contains resource usage data about your environment.

Configuration information sent to Dell EMC via Dell EMC SupportAssist

AppSync sends a configuration file to Dell EMC every day that contains internal data about your environment.

Table 35 Configuration information

Category	Details
Agent configuration	<ul style="list-style-type: none"> • Number of Linux hosts • Number of Windows hosts • Number of AIX hosts • Average number of File systems per hosts • Clustered agent usage • LDAP configuration usage
Storage configuration	<ul style="list-style-type: none"> • Number of arrays • Number of XtremIO arrays • Number of VPLEX arrays • Number of VNX arrays • Number of VMAX3/PowerMAX arrays • Number of VMAX V2 arrays • Number of Unity arrays • Number of VNX arrays • License type: Array based license, Starter Pack, VSL and DPS
Application configuration	<ul style="list-style-type: none"> • VMware usage • Number of Virtual Centers • Number of SQL databases • Number of Exchange databases • Number of Oracle databases • Number of Data stores • Oracle RAC usage • Exchange DAG usage
Copy usage	<ul style="list-style-type: none"> • Repurposing usage • Number of copies currently mounted • Number of SQL copies • Number of Data store copies • Number of Exchange copies • Number of Oracle copies • Number of File System copies

Table 35 Configuration information (continued)

Category	Details
	<ul style="list-style-type: none"> • Number of SQL repurposing copies • Number of Oracle repurposing copies • Number of File system repurposing copies

AppSync issues

User account does not have the correct permissions

Problem

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.

Resolution

To grant the user account the correct permissions, and manually register the EMC AppSync Exchange Interface 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 Plugin 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 /appsyncechuser /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 appsyncechexchangeinterface`.
11. Use the AppSync console to rediscover the server. Go to **Settings > Servers**, select the server, and then click **Rediscover**.

- Discover the Exchange mailbox databases. Go to **Copy Management > Exchange** and click on the Exchange server. You may have to re-enter the credentials.

AppSync Exchange Interface service is partially registered

Problem

If the rights and permissions are not granted properly to the user account, or if conflicting software is installed, the AppSync Exchange Interface service does not register correctly. You might have to perform a manual cleanup.

Resolution

Do the following:

- Open a command prompt and navigate to the directory where the AppSync host plugin is installed. The default location is `C:\Program Files\EMC\AppSync Host Plug-in`.
- Run the following command to remove the service and delete the DCOM component:
`awExchangeInterface /unregserver`
- Using the Services console (`service.msc`), verify that the EMC AppSync Exchange Interface service is removed. If it persists, run: `sc delete AppSyncExchangeInterface`
- 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**.
- If the component persists, click **DCOM Config**, then in the center pane, click **EMC AppSync Exchange Interface**, and then click **Delete**.
- Using **REGEDIT**, verify that all the stale entries related to AppSync Exchange Interface are deleted.

VSS timeout issue

Problem

During protection of applications which reside on Unity, XtremIO, or VPLEX on XtremIO, protection fails with the VSS timeout error.

Resolution

Add the IP address and the FQDN of the XMS in the AppSync server host file located at `C:\Windows\System32\drivers\etc\hosts`. For example, `10.247.169.71 lrmb071`.

Note: You can configure VSS retry settings during copy creation in the service plan for Windows applications such as File system, Microsoft SQL, and Microsoft Exchange. For SQL Server databases, you can consider taking Crash Consistent backup. The Protect SQL Server chapter provides more information on the Crash Consistent backup type.

Host installation and deployment issue

Problem

When installing the agent plug-in, SUDO user installation might fail.

Resolution

Ensure the following:

- SSH service is configured on the Unix/Linux systems.
- BZip2, OpenSSH, and OpenSSL packages are available for AIX.

3. The sg3_utils package is available for Linux.
4. SSH port 22 is unblocked.
5. There is sufficient space available at the install location.
6. The home/install directory of the SUDO user has the "write" privilege.

The *AppSync Installation and Configuration Guide* provides additional information on installing the SUDO user.

Oracle ASM disk groups cannot be mounted after a host reboot

Problem

Production Oracle ASM disk groups cannot be mounted after a host reboot because of conflicting ASMLIB disks. The udev rules that mask the devices of an AppSync mounted copy does not get loaded after a reboot leading to conflict between the production ASMLIB devices and the mounted copy's devices. If udev rules are not loaded, then the mounted copy's devices are exposed through their ASMLIB header because that information is present on the replicated device and it is not hidden by the udev rules. Therefore, the ASM instance sees two ASMLIB disks with the same name and gets confused.

Resolution

Do one of the following:

- Unmount the copy in AppSync.
- Manually reload the udev rules according to the Linux platform version.

Mount of ASM disk groups fail on RHEL 6.x and 7.x MPIO configurations

Problem

If you set the disk string to `/dev/mapper/*` on the mount host, it can lead to a conflict because AppSync attempts to mask devices using the disk string `/dev/emc-appsync-*`. The `/dev/emc-appsync-*` paths are UDEV rules based NAME parameter (in the case of RHEL 6.x) or UDEV rules based SYMLINK+ parameter (in the case of RHEL 7.x), and it is like an alias over the `/dev/mapper/*` devices. The conflict occurs because the same target device is masked using two paths - `/dev/mapper/*` path and `/dev/emc-appsync-*` path, and ASM does not accept duplicate paths for candidate disks.

Resolution

Remove `/dev/mapper/*` from the `asm_diskstring` parameter using the following command:

```
alter system set asm_diskstring= '<paths without /dev/mapper/*>' scope=both
```

For example, if existing ASM disks have paths with MPIO aliases such as `/dev/mapper/asm_disk<n>`, change `/dev/mapper/*` to `/dev/mapper/asm_disk*`.

AppSync fails to mount Oracle ASM disk groups (Event - ORCL_000043)

Problem

AppSync fails to mount Oracle ASM disk groups.

Resolution

1. Check the previous agent log for `mountASMFilesystems` operation to confirm if all the related devices have surfaced correctly.
2. If MPIO on Linux 6.x and 7.x is used, ensure that no duplicate paths are presented to ASM through the existing `asm_diskstring` parameter. [Mount of ASM disk groups fail on RHEL 6.x and 7.x MPIO configurations](#) provides more information.
3. This issue might occur if the `asm_diskstring` parameter is empty or if it is set to nested paths such as `/dev/*`, `/dev/asm-disk*`. Ensure that a proper value is assigned to the `asm_diskstring` parameter.
4. For Linux flavors, this issue might occur if there is any spurious udev rules file present under `/etc/udev/rules.d/` directory masking the same target devices with some other `NAME/SYMLINK` parameter. Ensure that no such file exists and remove the files, if any.
5. Ensure that there is enough space in `/tmp`.

AppSync fails to unmount Oracle ASM disk groups (Event - ORCL_000044)

Problem

AppSync fails to unmount Oracle ASM disk groups during a restore operation.

Resolution

1. Check if there are any affected databases that must be shutdown manually before restore. AppSync reports unprotected affected databases before restore and you must shut them down manually.
2. If the failure occurs during unmount of a mounted copy, connect to the ASM instance on the mount host and manually dismount the mounted disk group using the sqlplus `alter diskgroup <diskgroup name> dismount` command . Before executing this command, ensure that the mounted and recovered database is shutdown.

Oracle database discovery failure

Problem

If a symbolic link is used for `ORACLE_HOME` in `/etc/oratab` for a database, AppSync fails to discover the database, if you start the database with the actual path.

Resolution

Ensure that you start the database with the `ORACLE_HOME` variable set to the same symbolic link path.

Oracle database discovery failure - / file system full

Problem

Oracle database discovery fails with the following error:

```
No valid instance available when / file system is full
```

Resolution

Ensure that either disk space or inode usage in root (`/`) file system is not full.

Oracle database fails to start after a reboot

Problem

The AppSync mounted Oracle databases does not start after a host reboot.

Resolution

If the mounted and recovered databases do not come up post a reboot, then the most common reasons can be:

- The file systems cannot be mounted before the database restart is triggered. AppSync waits for a maximum of 1 minute for the file systems to be mounted.
- The ASM instance cannot be started (if database resides on ASM disk groups). AppSync waits for a maximum of 2 minutes for the ASM instance to start.
- After reconnecting to the rebooted host, if you notice that the ASM disk groups and/or the file systems on which the mounted and recovered database resides are mounted, do the following:
 1. Navigate to the AppSync agent install path (usually `/opt/emc/appsync`).
 2. If root is the owner of AppSync installation, run `./acp -b .`
 3. If a SUDO user is the owner of AppSync installation, then run `su - <sudouser>` and `sudo ./acp -b.`
 4. Check whether all the databases that were mounted and recovered using AppSync are opened in the desired open mode using sqlplus.

When you run `acp -b`, check for the events.

To check logs after a host reboot, refer to the following locations:

On Linux:

- Check `/var/log/messages`.
- Check `/var/log/boot.log`.

On AIX:

1. Add a line in `/etc/inittab` to direct the logs to boot log and console logs.

```
asdbora:2:once:/etc/asdbora 2>&1 | alog -tboot > /dev/console #oracle
restart
```

2. Enable syslog, if it is not enabled, and check for errors.
3. Check the boot log and the console log.

Restore of Oracle database causing server service to crash

Problem

AppSync server crashes while protecting Oracle database with large number of data files. When you try to protect a database with several thousands of data files, AppSync server may crash with an out of memory exception.

Resolution

Increase the heap size by changing the below parameters in `C:\EMC\AppSync\jboss\executive\application-service.conf` file. The default installation path may vary based on the installation location.

`wrapper.java.additional.2=-Xms2048m` (previous value - 1024m or 1GB)

`wrapper.java.additional.3=-Xmx5120m` (previous value - 2048m or 2GB)

Oracle restart script not removed for UNIX hosts registered using a SUDO user on agent uninstallation

Problem

The Oracle restart script created by AppSync, that is, `/etc/asdbora` for AIX and `/etc/init.d/asdbora` for Linux might not be removed, if a SUDO user is used for registering the host. There is no impact on functionality, it is only a cleanup issue.

Resolution

After the host agent is removed and uninstalled from the AppSync server:

1. Manually remove the script.
2. Remove the symlinks pointing to the `asdbora` file, if they are not removed from `/etc/rc.d/[rc0.d,rc2.d, rc3.d, rc5.d]`.

AppSync requires higher ulimit settings for the root user than the Oracle user.

Problem

If you are using the root user to install an AppSync Linux client plug-in. AppSync requires that the ulimit settings for the root user be equal to or higher than the ulimit settings for the Oracle User. If not, AppSync inherits the root user profile with the lower ulimit settings.

Workaround

If the ulimit settings for the root user are lower than the ulimit settings for the Oracle User, you must manually alter the system to match ulimits between the root and oracle users. You can add the root ulimits to the `/etc/security/limits.conf` file.

Resolution

It is recommended to use a SUDO user, to install an AppSync Linux Oracle client . This allows you to set the ulimits to the SUDO user to match those of the Oracle user.

AppSync fails to create symlinks

Problem

AppSync fails to create symlinks to the `asdbora` file when you select the restart database post reboot option.

Resolution

On Linux, run the following commands:

- `ln -s /etc/init.d/asdbora /etc/rc.d/rc0.d/K01asdbora`
- `ln -s /etc/init.d/asdbora /etc/rc.d/rc3.d/S99asdbora`
- `ln -s /etc/init.d/asdbora /etc/rc.d/rc5.d/S99asdbora`

On AIX, run the following commands:

- `ln -s /etc/asdbora /etc/rc.d/rc0.d/K01asdbora`
- `ln -s /etc/asdbora /etc/rc.d/rc3.d/S99asdbora`

Checking system logs for Oracle restart

To check system logs for Oracle restart:

On Linux, see:

- `/var/log/messages`
- `/var/log/boot.log`

On AIX:

1. Enable `syslog` (Note: Be careful while editing `/etc/syslog.conf`)
2. Create an empty file such as `touch /tmp/syslog.out`
3. Copy the following lines and paste it in `/etc/syslog.conf`

```
*.debug          /tmp/syslog.out    rotate size 100k files 4
*.crit           /tmp/syslog.out    rotate time 1d
*.info          /tmp/syslog.out    rotate time 1d
*.*             /tmp/syslog.out    rotate size 100k files 4
```

4. Type the following command to restart the syslog service:

```
refresh -s syslogd
```

5. Check whether `syslog.out` is populated with the logs.
6. Confirm that an entry in `/etc/inittab` exists for: `asdbora:2:once:/etc/asdbora 2>&1 | alog -tboot > /dev/console #oracle restart`
7. Type the following command to view the boot log:

```
alog -o -t boot
```

8. Type the following command to view the console log:

```
alog -o -t console
```

Database fails to start with the created SPFile

Problem

When you mount a copy, the database does not start with the created SPFile.

Resolution

To start the database with the created SPFile, connect to the database and run the following commands:

- `shutdown immediate`
- `startup mount`

Oracle recovery failure

Problem

Oracle database recovery might fail during mount, if the database name starts with a numeric character.

Resolution

Ensure that the database name does not start with a numeric character because Oracle does not allow an `ORACLE_SID` to begin with a numeric character.

Oracle 12.2 RAC database discovery failure

Problem

Oracle 12.2 RAC database discovery might fail, if you do not add the database name or SID in the `/etc/oratab` file when creating the database using DBCA.

Resolution

Ensure that you add the database name or SID in the `/etc/oratab` file when creating the database using DBCA.

Oracle database recovery failure during `prerecoverdb` operation

Problem

Oracle database recovery fails during the `prerecoverdb` operation because two archive destinations point to the same location on the mount host.

Reason

This is an edge scenario where the production database has two archive destinations pointing to the Fast Recovery Area. This is possible when the first destination points to `use_db_recovery_file_dest` and the second destination points to the actual Fast Recovery Area location (for example, `/ora_fra/db`).

`log_archive_dest_1 - location=use_db_recovery_file_dest`

`log_archive_dest_2 - location=/ora_fra/bct_db`

In this case, if you do not protect the Fast Recovery Area, but select 1 and 2 archive destinations, AppSync resolves the first destination to the actual path because Fast Recovery Area is not protected. Therefore, the `use_db_recovery_file_dest` parameter cannot be specified for an archive destination during mount. This causes the problem because both destinations 1 and 2 resolve to the same path.

Resolution

Protect the Fast Recovery Area when any selected archive log destination points to the `use_db_recovery_file_dest` parameter.

AppSync fails to freeze the SQL Server database in a timely manner (Event - SQL_000018)

Problem

AppSync might fail to freeze the SQL Server database in a timely manner, if there is heavy IOPs on the database or due to other database performance issues.

Resolution

1. Add a registry key `CC_AGENT_THREAD_WAIT_TIME` of type `REG_DWORD` with value of 1200 (See step 3 to determine the actual time taken during a Microsoft VDI backup). Also, add another key of type `REG_DWORD` with the same value for VDI timeout as `CC_SQL_VDI_TIMEOUT`.
2. Consider taking a non-VDI backup. Refer the SQL server mount and restore considerations for limitations with non-VDI backups.
3. Contact the SQL Server database administrator to address the performance issues. Microsoft also provides VDI backup diagnostic tools that can be leveraged to check the time taken by Microsoft VDI backups for a database. Contact Microsoft or Dell EMC support for more information.

4. You can consider taking Crash Consistent backup. The Protect SQL Server chapter provides more information on Crash Consistent backup.

Note: For Crash Consistent SQL backup, AppSync does not use VSS or VDI framework. Therefore, there is no VSS timeout or Freeze/Thaw failure issues.

Note: This does not address the VSS timeout issues that occur due to 10 second limitation from Microsoft. This resolution is applicable only if AppSync fails to quiesce the SQL Server database before VSS comes into the picture.

SQL Cluster - second generation copy mount failure

Problem

When you mount both the first generation and the second generation copies sequentially under the same mount drive in a mount cluster, the mount of the second generation copy fails.

Resolution

Ensure that you place the existing mounted drives in maintenance mode. After all the clustered mount points are placed in the maintenance mode, the second generation mount succeeds.

AppSync places only the root of the mount point in maintenance mode. You must place the other clustered drives mounted within the same root drive in maintenance mode. Before unmounting the copies, you must take out all such drives out of the maintenance mode.

Timeout error during SQL database discovery

Problem

During SQL database discovery, you might receive a request timed out message even after configuring the SQL server settings with the appropriate credentials.

Resolution

On the SQL Server, navigate to **Control Panel > Administrative Tools > ODBC application** to start the ODBC application and ensure that the application is functioning.

Alternatively, you can consider running the `sfc` or the `scannow` command in DOS as Administrator to resolve possible issues with the ODBC application. However, check with your SQL or Windows administrator before running the command, or work with the owner of the ODBC application to resolve issues.

SQL recovery failure

Problem

SQL recovery might fail, if:

- There is a version mismatch in the minor number of SQL instance version
- The mount host-plugin version is earlier than 3.7 and the production host-plugin version is 3.7

Resolution

Update mount host-plugin version to 3.7 and re-discover the host.

SQL database protection failure

Problem

For Microsoft SQL server, if TLS 1.0 is disabled on the Windows host, you might get the following error during discovery or protection of a SQL database:

Unable to connect to database xxxx\xxxx.master. This can happen if either SQL database is not in online state or ODBC driver is not properly installed. Check the AppSync host plug-in log for more details.

Resolution

- Install ODBC drivers on the Windows host, if not present already.
- If you want Appsync to use a specific version of the ODBC driver, you can specify the preferred ODBC driver for connecting to the SQL instance using the following registry key:
`[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\AppSync] "CC_SQL_SERVER_ODBC_DRIVER"="ODBC Driver xx for SQL Server"`

<AppSync>\jboss\standalone\tmp\vfs\ folder disk usage

Problem

The files in <AppSync>\jboss\standalone\tmp\vfs\ directory are temporary files. If the files accumulate in the folder, disk usage can be very high.

Resolution

To free up disk space:

1. Stop the AppSync server service.
2. Stop the AppSync datasource service.
3. Delete all the files from the C:\EMC\AppSync\jboss\standalone\tmp\vfs directory. This cleans up the old tmp\vfs files that can impact swapping.
4. Start the AppSync datasource service.
5. Start the AppSync server service.

XtremIO copy creation takes time

Problem

Snapshot creation on XtremIO takes significant time (more than 2 seconds) irrespective of the host (Windows or UNIX).

Resolution

Add the IP address and the FQDN of the XMS in the host file located at C:\Windows\System32\drivers\etc\hosts. For example, 10.247.169.71 lrm071.

Changing an XMS IP

Problem

Changing an XMS IP when a mount operation is in progress can lead to unmount failure because AppSync looks for the old XMS IP.

Resolution

Before you change your XMS IP address, ensure that you unmount all the XtremIO copies mounted in AppSync.

Error during datastore or virtual disk mount

Problem

If copy target LUNs are exposed to ESX, but they are not mounted (unmounted state) as datastores to ESX, you might encounter the following error:

Host Platform Config fault

Resolution

Ensure that more than one copy of the same datastore is not left in an unmounted state on ESX.

Virtual disk mapping failure

Problem

Virtual disk mapping fails even after VMware vCenter Server and appropriate storage array is added.

Resolution

You must set the `disk.EnableUUID` value to true.

1. Power off the virtual machine.
2. Log into vCenter Server or the ESXi/ESX host through the vSphere Client.
3. Right-click the virtual machine, and click **Edit settings**.
4. Click the **Options** tab.
5. Go to **Advanced > General > Configuration Parameters**.
6. Add or modify the row `disk.EnableUUID` with the value TRUE.
7. Click **OK** to save
8. Click **OK** to exit.
9. Right-click the virtual machine and click **Remove from Inventory** to unregister the virtual machine from the vCenter Server inventory.

 **Note:** If you perform this change using the command line, use the `vim-cmd` command to reload the vmx file. For more information, see the relevant VMware knowledge base article.
10. Power on the virtual machine.

Protection of File systems or Oracle applications on MPIO devices fail during mapping

Problem

The protection of File systems or Oracle applications on MPIO devices on RHEL fails during mapping with the following error: `disk.EnableUUID=TRUE` is not enabled for the virtual device.

The reason might be one of the following:

- File systems are created on `/dev/mpath/` MPIO devices. AppSync does not support devices starting with `/dev/mpath/*` for MPIO.
- The `lvm.conf` file might read `preferred_names = ["^/dev/mpath/", "^/dev/mapper/mapper/mapper", "^/dev/[hs]d"]`.

Resolution

- AppSync supports devices created only on `/dev/mapper/` devices, because they are persistent and created early during boot.
- The `lvm.conf` file must be modified to read `preferred_names = ["^/dev/mapper/mapper/mapper", "^/dev/[hs]d"]`.

Mount of a File system or an Oracle database on RHEL 7.x fails

Problem

Mount of a File system or an Oracle database on RHEL 7.x might fail, if target devices are not under MPIO control during mount.

Resolution

Ensure that you comment the parameter `find_multipaths` in the `/etc/multipath.conf` file.

Repurposing file systems on multiple LUNs fail

Problem

Repurposing file systems on multiple LUNs might fail, if the file systems being repurposed are from different storage types.

Resolution

Ensure that you repurpose file systems on the same array together.

Problem

Repurposing file systems on multiple LUNs might fail, if the number of LUNs to be protected exceeds the number of storage units allowed by the AppSync server.

Resolution

- Try repurposing fewer file systems.
- By default, the number of storage units allowed is 12. If you want to repurpose additional file systems, configure the server settings in the following manner:
 - For VMAX V2 and VMAX3/PowerMAX arrays - `max.vmax.block.affinity.storage.units`
 - For VNX arrays - `max.vnx.block.affinity.storage.units`
 - For VPLEX and XtremIO arrays - `max.common.block.affinity.storage.units`

For more information on configuring the server settings, contact Dell EMC Support.

Problem

Repurposing file systems on multiple LUNs might fail, if the subset of file systems to be repurposed does not exist on the host.

Resolution

Create repurpose copies and schedules again.

Changed file system type not updated after host discovery

Problem

AppSync does not automatically update the Windows file system type when a file system is changed from NTFS to ReFS or ReFS to NTFS.

Resolution

Do the following:

1. Remove the file system on the host.

2. Rediscover file systems in AppSync.
3. Add the new file system with the changed type on the host.
4. Rediscover file systems in AppSync again.

Mount of a file system snapshot to RHEL7 fails

Problem

Mount of a file system snapshot to RHEL 7 fails.

Resolution

Ensure that you set the `auto_activation_volume_list` parameter in the `lvm.conf` file to read the following: `auto_activation_volume_list = ["vplexvg1", "vplexvg2", "ol"]`

CST lockbox restore failure

Problem

Login to AppSync fails with a lockbox issue. Check logs at `C:\EMC\AppSync\apache-tomcat\logs` to verify failure.

Resolution

1. Stop all the three AppSync services, that is EMC APPSYNC Datastore Service, EMC AppSync Security Server Service, and the EMC AppSync Server Service.
2. Delete all the files under `C:\EMC\AppSync\cst\xml`.
3. Copy the files from `C:\EMC\cstBackup\<timestamp>\xml` to `C:\EMC\AppSync\cst\xml`. Ensure that you copy the files with the latest working timestamp.
4. Start all the three AppSync services.
5. Login to AppSync.

Protection and repurposing failure on VMAX V2

Problem

When you protect or repurpose applications on VMAX V2, it fails with the following error:

```
the device is already in requested state
```

Resolution

Protection or repurposing must have failed before activating the clone session, which AppSync had placed in the PreCopy state. To verify, fetch the state of the clone session for each of the source devices. Do the following:

1. Login to the host that has SMI-S installed.
2. Open a command prompt window. Type the following commands:

```
cd "\Program Files\EMC\SYMCLI\bin"
symclone -sid <symmetrix_id> list
```

3. If the clone sessions of the source are in the PreCopy state, add the source and target device information in a file (each line of the file must be in the <SOURCE DEVICE> <TARGET DEVICE> format) and activate the clone session using the `symcli` command.
4. Type the following command to activate the session and change the clone session from the PreCopy state to CopyInProgress state:

```
symclone -sid <symmetrix_id> -file <full_path_to_filename> activate -
noprompt
```

AppSync services do not start after reboot

Problem

If AppSync Server is installed on a Windows host, the AppSync security server and the AppSync server services do not start after a reboot.

Resolution

Run a repair of the AppSync server on the host to resolve this issue.

Windows server configuration issue

Problem

When configuring Windows server, it fails with the following error: Host plug-in registered to another AppSync server

Resolution

Do the following:

1. Select **Start > Run**.
2. Type `regedit` and click **OK**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > EMC > AppSync**.
4. Delete the following registry key entries:
 - CC_AUTH_PEER_CERT
 - CC_AUTH_SELF_CERT
 - CC_AUTH_SELF_KEY
5. Restart the AppSync host plug-in service before attempting to add the Windows agent to another AppSync server.

Scheduled service plan fails

Problem

If you have scheduled a recurring service plan for a database, for example, everyday at 3 PM, and a backup tool is also scheduled to run at the same time on a particular day (for example, Friday at 3PM), AppSync protection might fail because of resource conflicts.

Resolution

To schedule a service plan to run every day, excluding a particular day (for example, Friday at 3PM), you must create two schedules:

- Set a schedule to run “Every day at...” at > 12 AM, 3 AM, 6 AM, 9 AM, 12 PM, 6PM, 9PM

- Set a schedule to run "On selected days..." at > 3PM on Sunday, Monday, Tuesday, Wednesday, Thursday, Saturday

AppSync fails to launch on Google Chrome

Problem

By default, Google Chrome blocks some ports for security reasons (for example, port 123). If you use this port for Appsync protocols such as http, https, CAS, or tomcat, Appsync might fail to launch on a Chrome browser with the following error:

```
ERR_UNSAFE_PORT
```

Resolution

Do one of the following:

- Use a different browser to launch AppSync.
- Enable the port number used during Appsync installation. For example, to enable ports 123, 80, and 84 for Chrome, type the following command:

```
C:\Program Files (x86)\Google\Chrome\Application>chrome.exe --explicitly-allowed-ports=123,80,84
```

AppSync upgrade failure

Problem

During upgrade, AppSync might fail with the following Xcopy error:

```
Invalid drive specification
```

Resolution

Ensure that you have the required permissions to the drive root folder.

For example, if AppSync is installed on E drive, you must have explicit read, write, and modify permissions to E drive.

AppSync server database failure

Problem

The AppSync server database might get corrupted, if the server host (AppSync services) shuts down abruptly.

Resolution

Do the following:

1. Uninstall and re-install AppSync.
2. Import the latest PG backup taken by AppSync.

The section `Schedule automated backup of the AppSync server database` in the *AppSync Installation and Configuration Guide* provides additional information on scheduling backups.

Mount failure on RHEL 7.4

Problem

Mount might fail on a RHEL 7.4 host with the `vgimportclone` exception.

Resolution

This is a RHEL 7.4 bug. A possible workaround is to edit the `/etc/lvm/lvm.conf` file on the mount host and enable the `auto_activation_volume_list` variable. Set its value to volume groups that must be activated by default. Also, set the `use_lvmetad` flag to 0. For more information, see RHEL documentation.

Mount host fails to respond during an unmount operation

Problem

The mount host stops responding during an unmount operation, if the operating system is SUSE 11 Service Pack 4. This is because of an issue in the `rescan-scsi-bus.sh` script. This command removes all devices, if used with `-w`, `-r` switches.

Resolution

Reboot the system and modify the `/usr/bin/rescan-scsi-bus.sh` script.

1. Disable the `-r` switch in the following places:

```
opt=${opt#-}
case "$opt" in
  a) existing_targets=;; #Scan ALL targets when specified
  d) debug=1 ;;
  f) flush=1 ;;
  l) lunsearch=`seq 0 7` ;;
  L) lunsearch=`seq 0 $2`; shift ;;
  m) mp_enable=1 ;;
  w) opt_idsearch=`seq 0 15` ;;
  c) opt_channelsearch="0 1" ;;
  r) remove=0 ;; ----->Before change remove=1
  s) resize=1 ;;
  i) lipreset=0 ;;
  I) shift; lipreset=$opt ;;
```

```
opt="$1"
while test ! -z "$opt" -a -z "${opt##*-}"; do
  opt=${opt#-}
  case "$opt" in
    a) existing_targets=;; #Scan ALL targets when specified
    d) debug=1 ;;
    f) flush=1 ;;
    l) lunsearch=`seq 0 7` ;;
    L) lunsearch=`seq 0 $2`; shift ;;
    m) mp_enable=1 ;;
    w) opt_idsearch=`seq 0 15` ;;
    c) opt_channelsearch="0 1" ;;
    r) remove=0 ;; ----->Before change
remove=1
    s) resize=1 ;;
    i) lipreset=0 ;;
    I) shift; lipreset=$opt ;;
```

2. Change line 59 from

```
hosts=`find /sys/class/scsi_host/host* -maxdepth 4 -type d -o -type l
2> /dev/null | awk -F '/' '{print $5}' | sed -e 's~host~~' | sort -nu`
```

to

```
hosts=`find /sys/class/scsi_host/host* -maxdepth 4 -type d -o -type l
2> /dev/null | grep -v host0 | awk -F '/' '{print $5}' | sed -e 's~host~~' |
sort -nu`
```

Recovery of 2nd-gen copy fails if the SQL backup type of the 1st-gen service plan is altered

Problem

Creating a first generation full copy of a SQL database and then creating a second generation copy of the same database is successful. However, editing the first generation service plan and setting the backup type to **Non-VDI**, and then creating a second generation copy, and choosing to run mount with recovery causes recovery to fail.

Resolution

To resolve the issue, create a new second generation copy by navigating to the SQL Copies page. See [Create second generation copies](#) for detailed information.

Unmount does not remove used devices from storage groups

Problem

Unmount does not remove used devices from the storage group if the storage group is renamed after mount.

Resolution

To resolve this issue you must unmount the copy manually and perform the following steps:

1. Unmount the database manually at OS level. (Shutdown the database, unmount the filesystems, and so on).
2. Clean up the devices at the VC level (RDM/VDisk removal at ESX level).
3. Remove the devices from all the affected storage groups.
4. Choose the force unmount option under server settings at the AppSync level, and mark it as unmounted.

 **Note:** Once done, revert the server settings in AppSync.

Datastore mount fails when ATS locking is enabled

Problem

Datastore mount using virtual access mode fails when ATS locking is enabled.

Resolution

If your vDisk resides on ESX 5.0 or later, disable the `VMFS3hardwareaccelerated` locking flag on the ESX that is hosting the VMs hosting the databases on vDisks.

Disable ATS locking as AppSync datastore mount fails if ATS locking is enabled for VMFS3/5 datastore.

Error handling

The AppSync logging format is fixed and any log monitoring tool can be tuned to match the appropriate expression to raise an alert in service desk. You can check the metadata part of a logged event to determine if an event is an error event or not. If you see a TYPE-ERROR, then it is an error event, the ID appears after the EVENT in [], and the text that appears (excluding the metadata information) after the event ID is the event message. Other details such as the time of

error, from which AppSync server, from which Appsync user, and so on can also be tracked. The category of events are indicated in the EVENT ID (for example, ORCL, DPL, HST, SPP, and so on).

The following are some examples of AppSync generated events:

- 07-09-2016 14:06:57.489 INFO [Thread-58 (HornetQ-client-global-threads-2113097824)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [ORCL_000104]: During discovery, AppSync detected that the following database(s) were offline: SymASM. As a result, they will not be available for protection.(METADATA: TYPE=ERROR, TIME-2016-07-09 14:06:57.469-0400NATIVETIME-2016-07-09 14:06:57.469-0400, HOST-lrmk096, PHASE-, THREAD=Thread-58 (HornetQ-client-global-threads-2113097824), USER-admin, CATEGORY=GENERIC, SESSIONID-5br0S4+nz3-n6SzORPWYGAcn.undefined)
- 07-21-2016 05:07:45.076 INFO [Thread-156 (HornetQ-client-global-threads-436170702)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [SPP_000001]: Mount copy phase for RPdbl beginning(METADATA: TYPE=INFO, TIME-2016-07-21 05:07:45.076-0400NATIVETIME-2016-07-21 05:07:45.076-0400, HOST-lrmk096, PHASE=Mount copy, THREAD=Thread-156 (HornetQ-client-global-threads-436170702), USER-admin, CATEGORY=GENERIC, SESSIONID-FPO4yGMevayAeRzNPJC8AAF0.undefined)
- 07-21-2016 05:04:26.027 INFO [Thread-158 (HornetQ-client-global-threads-436170702)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [UNM_000001]: Skipping unmount phase. There were no previously mounted copies found for the applications under protection during this cycle.(METADATA: TYPE=INFO, TIME-2016-07-21 05:04:26.027-0400NATIVETIME-2016-07-21 05:04:26.027-0400, HOST-lrmk096, PHASE=Create CRR bookmark copy, THREAD=Thread-158 (HornetQ-client-global-threads-436170702), USER-admin, CATEGORY=GENERIC, SESSIONID-)
- 07-21-2016 05:04:10.178 INFO [Thread-158 (HornetQ-client-global-threads-436170702)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [SPP_000001]: Application mapping phase for RPdbl beginning(METADATA: TYPE=INFO, TIME-2016-07-21 05:04:10.178-0400NATIVETIME-2016-07-21 05:04:10.178-0400, HOST-lrmk096, PHASE=Application mapping, THREAD=Thread-158 (HornetQ-client-global-threads-436170702), USER-admin, CATEGORY=GENERIC, SESSIONID-)
- 07-21-2016 05:04:09.398 INFO [Thread-162 (HornetQ-client-global-threads-436170702)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [MILE_000006]: Application discovery phase for RPdbl completed successfully(METADATA: TYPE=INFO, TIME-2016-07-21 05:04:09.398-0400NATIVETIME-2016-07-21 05:04:09.398-0400, HOST-lrmk096, PHASE=Application discovery, THREAD=Thread-162 (HornetQ-client-global-threads-436170702), USER-admin, CATEGORY=MILESTONE, SESSIONID-)
- 07-21-2016 05:03:11.102 INFO [Thread-89 (HornetQ-client-global-threads-436170702)]
 [com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [VNX_000052]: Successfully created repurpose VNX snapshot copy

```
AppSyncSnap-20160721_050227:80-545e3dbf-d238-4c8e-bd2e-883666512bb8-
APPSYNC_TMP_CG_20160721_050228:484_400_0_488.CopySnap.oracle.autol_re
purpose.2.1.20160721_050310:946 of source VNX snapshot
AppSyncSnap-20160721_050227:80-545e3dbf-d238-4c8e-bd2e-883666512bb8-
APPSYNC_TMP_CG_20160721_050228:484_400_0_488.(METADATA: TYPE-INFO,
TIME-2016-07-21 05:03:11.102-0400NATIVETIME-2016-07-21
05:03:11.102-0400, HOST-lrmk096, PHASE-Create 2nd gen archLogs copy,
THREAD=Thread-89 (HornetQ-client-global-threads-436170702), USER-
admin, CATEGORY-GENERIC, SESSIONID-Hgg-ZRqpCV0ixTrPp-tXbJ
+C.undefined)
```

- 07-21-2016 05:00:28.724 INFO [Thread-158 (HornetQ-client-global-threads-436170702)]
[com.emc.archway.service.eventservice.EventServiceBean] [] [] EVENT [LIC_000004]: Storage array APM00140431583 is not licensed for use with AppSync, but is within the 90 day trial period.(METADATA: TYPE-WARNING, TIME-2016-07-21 05:00:28.724-0400NATIVETIME-2016-07-21 05:00:28.724-0400, HOST-lrmk096, PHASE-Create CRR bookmark copy, THREAD=Thread-158 (HornetQ-client-global-threads-436170702), USER-admin, CATEGORY-GENERIC, SESSIONID-Hgg-ZRqpCV0ixTrPp-tXbJ +C.undefined)

Event logging

- The `events.log` file captures the generated events for every run of a service plan. It is located in the same place as the `server.log` file. It also captures the details of the resources during different stages.
For example,

```
Resource involved at discovery phase are:
Production host Name lrmq020. Version :Microsoft(R) Windows(R) Server
2008 R2 Enterprise Edition 64-bit Service Pack 1 (build 7601)
Host : lrmq020 belongs to Virtual Center : lrma093 and Virtual Center
version : 5.5.0
SQLServerInstance LRMQ020, Version : 10.50.1600.1 , Clustered : false
```

- The rotation count of the log file and the size of log file is dependent on **Settings > Logs >Trace Logs**.

GLOSSARY

A

alternate path An user defined alternate path that AppSync uses while mounting a copy.

array A collection of disk drives where user data and parity data may be stored. Devices can consist of some or all of the drives within an array.

ASM (Automated Storage Management) A disk volume manager used for storing Oracle files, ASM allows administrators to add and remove disks while the database is available. Data is automatically striped across all disks in a disk group.

C

command line interface (CLI) Method of operating system or application software by typing commands to perform specific tasks.

continuous data protection The method of data protection in which all changes to data are continuously captured and tracked, allowing for data recovery to any point in time.

copy - SQL backup SQL Server backup type that is used to protect the database and active part of the transaction logs without affecting the sequence of backups. The copy backup type allows you to take a backup without affecting other backup tools that might be creating full copies of the database.

D

default path AppSync's predefined alternate path used while mounting a copy. The format is %SystemDrive%\AppSyncMounts\%%ProdServerName%\.

distributed device A RAID 1 device whose mirrors are in different VPLEX clusters.

E

event A log message that results from a significant action initiated by a user or the system.

F

failover Automatically switching to a redundant or standby device, system, or data path upon the failure or abnormal termination of the currently active device, system, or data path.

full - SQL backup SQL Server backup type that is used to protect the database and active part of the transaction logs. The full backup type allows you to restore transaction logs, so that you can restore the database to a point-in-time that is newer than the copy.

H

host-plugin An AppSync agent software that is installed and used on production and mount hosts to perform certain functions in order to facilitate protection and recovery of applications.

L

logical unit number (LUN) Virtual storage to which a given server with a physical connection to the underlying storage device may be granted or denied access. LUNs are used to identify SCSI devices, such as external hard drives, connected to a computer. Each device is assigned a LUN number which serves as the device's unique address.

M

metadata Information about data, such as data quality, content, and condition.

mount host The system that AppSync uses to mount a copy. This can be different from the production system.

N

network System of computers, terminals, and databases connected by communication lines.

network name resource A logical server name that is managed as a cluster resource. A network name resource must be used with an IP address resource.

O

original path The mount path AppSync uses to mount copies. The same path as on the production host.

P

production host The production computer that contains the information system that manages the production data: a database server, Web server, application server, or file server.

R

RAC Real Application Clusters. Allows multiple Oracle instances on different nodes of a cluster to access a shared database on the cluster to facilitate load balancing.

RAID The use of two or more storage volumes to provide better performance, error recovery, and fault tolerance.

- RAID 0** A performance-orientated striped or dispersed data mapping technique. Uniformly sized blocks of storage are assigned in regular sequence to all of the arrays disks. Provides high I/O performance at low inherent cost. No additional disks are required. The advantages of RAID 0 are a very simple design and an ease of implementation.
- RAID 1** Also called mirroring, this has been used longer than any other form of RAID. It remains popular because of simplicity and a high level of data availability. A mirrored array consists of two or more disks. Each disk in a mirrored array holds an identical image of the user data. RAID 1 has no striping. Read performance is improved since either disk can be read at the same time. Write performance is lower than single disk storage. Writes must be performed on all disks, or mirrors, in the RAID 1. RAID 1 provides very good data reliability for read-intensive applications.
- recover** The additional operation performed on a protected application to bring the application online and running, after the copy has been mounted or restored.
- RecoverPoint Appliance (RPA)** Hardware that manages all aspects of data protection for a storage group, including capturing changes, maintaining the images in the journal volumes, and performing image recovery.
- RecoverPoint site** All RecoverPoint entities on one side of the replication.
- resource group** A collection of cluster resources managed as a single cluster object. Typically a resource group contains all of the cluster resources that are required to run a specific application or service. Failover and failback always act on resource groups.
- restore** The process performed on a copy of a protected application to bring the production data of the application to contain consistent data up to a point in time that is earlier than the current time.
- S**
- service plan** Defines the attributes of a copy that AppSync creates and manages.
- SRDF** A technology that allows two or more Symmetrix systems to maintain a remote mirror of data in more than one location. The systems can be located within the same facility, in a campus, or hundreds of miles apart using fibre or dedicated high-speed circuits. The SRDF family of replication software offers various levels of high-availability configurations, such as SRDF/Synchronous (SRDF/S) and SRDF/Asynchronous (SRDF/A).
- storage area network (SAN)** A high-speed special purpose network or subnetwork that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.
- storage volume** A Logical Unit Number (LUN) or unit of storage presented by the back end array.
- T**
- TimeFinder** Symmetrix TimeFinder is a business continuance solution that allows you to use special Symmetrix devices called business continuance volumes (BCVs) to create mirrors of Symmetrix data.

TimeFinder Clone Copies of a source device on multiple target devices. The source and target devices can be either standard devices or BCV devices as long as they are all of the same size and emulation type. Clone copies of striped or concatenated meta devices can also be created, but the source and target meta devices must be completely identical in stripe count, stripe size, and capacity. Once activated, the copy can be instantly accessed by a target's host, even before the data is fully copied to the target device.

TimeFinder Snap A host-accessible device containing track-level location information (pointers), that indicates where the copy session data is located in the physical storage. TimeFinder Snap operations provide instant snapshot device copies, using virtual devices (VDEVs).

U

universal unique identifier (UUID) A 64-bit number used to uniquely identify an AppSync copy.

V

VDI Virtual Device Interface. SQL Server provides an API called Virtual Device Interface (VDI) that helps AppSync agent in providing support for backup and restore operations. These APIs provide maximum reliability and performance, and support the full range of SQL Server backup and restore functionality, including the full range of snapshot backup capabilities.

virtual volume Unit of storage presented by the VPLEX front end ports to hosts. A virtual volume looks like a contiguous volume, but can be distributed over two or more storage volumes.

VSS Volume Shadow Copy Service. A Windows service and architecture that coordinate various components to create consistent point-in-time copies of data called shadow copies.

INDEX

A

- agent, See AppSync host plug-in , See AppSync host plug-in
- alert 281–283
 - associated events 281
 - email 283
 - filtering 281
 - when generated 281
 - where displayed 281
- alerts 282
- Alerts 20
- AlwaysOn Availability Groups 125
- AppSync
 - architecture 16
 - console 17
 - host plug-in 16
 - overview 14
 - REST interface 17
 - server 16
 - summary of deployment steps 95
 - user interface 17
- AppSync host plug-in
 - installation 246
- assqlrestore 166, 167
- assqlrestore commands 165
- audience 11

C

- CLI actions 25
- cli utility 24
- cluster mount 287, 292
- comments 11
- console
 - effect of user role on 20
 - overview 20
 - times shown 22
- conventions for publication 11
- copyDetails 36
- CST lockbox 331

D

- data masking 271
- datastore
 - affected entities 261
- datastore, vmware 247
- datastores 243
- definition 52
- Dell SC 308, 309
- disableSP 28
- discover 132
- dynamic and statis mounts 301
- dynamic mount 287

E

- email 282
- email alerts 283
- enableSP 27
- ESRS 317, 318
- event
 - alert-related 281
- event logging 337
- exchange 96
- Exchange 93, 94, 96, 97, 102, 103, 106–108, 113, 115, 116, 278
 - backup type 102
 - consistency check 106, 107
 - DAG 96
 - database and log layout 103
 - deleted database restore 116
 - event log errors 102
 - interaction with VSS 102, 108
 - mount 108
 - overview of support 94
 - protect 97
 - protect immediately 97
 - remove mailbox server 96
 - requirements for partial restore 115
 - restore 108, 113
 - subscribe database to a service plan 278
 - VSS 102
- exchange interface service 320
- expire 30

F

- file system 237, 330
- File system 329
- filesystem 220
- Filesystem 219
- Filesystem copoies page 221
- Filesystem page 221
- Filesystem, change mount point 236

H

- HACMP cluster integration 175
- HACMP Restore 176, 224

I

- installation 320

J

- Job Status 21

L

- listCopies 34
- log collection 314

login 25
logout 26

M

Microsoft Exchange, See Exchange , See Exchange
monitor 281
Monitor 277
mount 36, 106, 108, 110, 287, 304, 307, 311
 by server 106
 copy by server 106
 dynamic 287
 host override 106
 locations 108
 minimize log option 110
 override 106
 throttle option 110
 validation options 110
 virtual machine 287
Mount dopy 195
mount on cluster 208
mount override
 VMware datastore 236, 257
mount phase
 datastore copy 257
Mount VMFS copy 258
MSCS 287, 292

N

NFS filesystems 220

O

on virtual disks 121
Oracel, Veritas Cluster Services 174
oracle 191
Oracle 74, 170, 196, 206, 207, 214, 321, 322, 324, 325
 affected entities in restore 214
 override mount settings 196
 summary of service plan settings 74
Oracle Data Guard 171
Oracle on VMware virtual disks 180
Oracle pre-mount script 195
Oracle support 181
oracle, copy expiration 193
Oracle, mount 202
oracle, post-copy script 194
Oracle, pre-copy script 193
oracle, prerequisites and supported configurations 176
oracle, protecting 184
oracle, restoring RAC copy for affected entities 216
oracle, storage preferences 192
oracle, unmount copy 197
oracle, unmount previous copy 194

P

path mapping 112, 155, 156, 209, 210, 239, 240
post mount script 196
PowerHA cluster 223
PowerMax 294
PowerStore 309, 311
preface 11

protect 247
push install 246

R

RecoverPoint 113, 115, 161, 300, 301
 affected entities in restore 113
 affected entities in SQL restore 161
 consistency groups 300
 prerequisites 300
 replication options 300
 restore granularity 115
 setup 300
recovery point objective
 compliance report 278
 concepts 278
 setting 100, 139, 254
refresh 26
related documentation 11
report 29
reports
 overview 16
 recovery point compliance 278
 save to CSV 278
repurpose 270, 293, 302
Repurpose
 bookmark) 302
repurpose expire 271
repurpose refresh 270
repurpose schedule 269
repurpose, view 274
repurposing 157, 187, 268, 272, 305, 311, 330
REST interface 17
restore 113, 115, 116, 161, 214, 308
 affected entities 113, 214
 deleted database 116
 Exchange 113
 manual option 115
 partial 115
 SQL affected entities 161
Restore VMFS or NFS datastores 264
RHEL 7 331
role
 definition 15
 effect on console 20
rotation 102, 142, 256
runSP 27

S

SAN policy
 prerequisite 288
script
 post-copy 104, 143
 post-mount 107, 148
 pre-copy 101, 140
server
 adding 246
service plan 15, 55, 64, 72, 100, 101, 104, 106, 107, 139, 140, 143, 148, 149, 254, 257, 258, 304, 306, 310
 create copy phase 101
 create new 55
 definition 15

- delete 64
- disable 64
- enable 64
- mount copy phase 104, 106
- phase details 100
- post-copy script phase 104, 143
- post-mount script phase 107, 148
- pre-copy script phase 101, 140
- run on demand 64
- save copy as 55
- schedule 100, 139, 254
- start 100, 139, 254
- unmount copy phase 107, 149, 258
- unmount previous copy phase 257
- validate copy phase 106, 107
- service plan schedule 191
- service plan summary and details 191
- service plans 52
- sql 127
- SQL 327
- SQL database
 - copies page 136
- SQL Database 132
- SQL restore 161
- SQL server
 - mount copy 152
- SQL Server 78, 119–122, 124, 130–132, 143, 149, 163
 - considerations in a cluster 130
 - database discovery 131
 - included plans 78
 - mount phase of service plan 143
 - permissions 122
 - restore damaged database 163
 - rights 122
 - user databases folder 131
 - user privileges 123, 124
- SQL server backup 141
- sql server log backup expiration 128
- SQL Server service plan
 - table of default settings 78
- sql server transaction log 125
- SQL Server:user privileges 123, 124
- SQL, expire 139, 160
- SQL, mount 151
- SQL, restore 163
- SQL, unmount 157
- Storage System
 - PowerStore 309
- subscribe 31
- Subscribe 132
- support information 11

T

- transaction log
 - configure 126

U

- Unity 303–305
- unmount 48, 257
 - as part of service plan 257
- unmount a copy

- as part of service plan 107, 149, 258
- unsubscribe 32
- Unsubscribe 135

V

- Vdisk restore 216
- VIO vSCSI 180
- vm consistency 250
- VMAX 290, 292, 293, 331
 - restore 293
- VMAX All Flash 294
- vmax service plans 193
- VMAX service plans 290
- VMAX, Symmetrix copy session arrays 291
- VMAX3 294–296
 - mount, unmount 295
- vmfs requirements 244
- vmware snapshots 250
- VNX
 - setup 286
- VNX array
 - dynamic mount 287
- VNX file service plan 289
- VNX file setup 288
- VNX File Snapshot copy mount 290
- VNX remote protection 288
- VNX Replicator 288
- VNX service plan 287
- VNX Snapshot
 - affected entities in restore 113, 214
 - affected entities in SQL restore 161
 - expiration 102, 142, 256
 - partial restore 115
- VNX Snapshot, RP bookmarks
 - control replication storage utilization 100
- VNX SnapSure' 288
- VPLEX 306
- VSS failure 103, 142
- VSS timeout 320

W

- Windows server 332

X

- XtremIO 297, 299
 - restore 299

