APPSYNC WITH VMAX ALL-FLASH

ABSTRACT
This white paper discusses and provides guidelines for users who are integrating to manage their Dell EMC VMAX All Flash storage system with AppSync, providing integrated application protection and repurposing.

May 2018
The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

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

Copyright © 2016 Dell Inc. or its subsidiaries. All Rights Reserved. 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 05/18 White Paper, H15713.3

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
TABLE OF CONTENTS

EXECUTIVE SUMMARY .................................................................................................................. 5
  Audience .................................................................................................................................. 5

OVERVIEW ................................................................................................................................... 5
  Using the Guidelines ................................................................................................................. 5
  Terms and Definitions .............................................................................................................. 6

VMAX ALL FLASH CONFIGURATION REQUIREMENTS .............................................................. 7
  Advanced Features Supported ............................................................................................... 7
    VMAX All Flash eNAS ........................................................................................................... 7
    VPLEX Provisioned Volumes ............................................................................................... 7
    AppSync’s “Gold” Service Plan .......................................................................................... 7
    VMAX Online Device Expansion ....................................................................................... 7

VMAX SMI-S PROVIDER .............................................................................................................. 8
  Communicating with the SMI-S provider .............................................................................. 8
  REMOVING AN SMI-S PROVIDER ...................................................................................... 8

VMAX ARRAY DISCOVERY AND CONFIGURATION ................................................................. 9
  Modifying Credentials ............................................................................................................ 11
  Provider Preference ............................................................................................................... 11
  Preventing Automatic Discovery of Arrays .......................................................................... 11
  Removing a VMAX Array from AppSync ........................................................................... 12

STORAGE MANAGEMENT ....................................................................................................... 12
  User Configured Storage Groups .......................................................................................... 12
    Configuring Storage Groups for Copy Target Devices ...................................................... 12
    Modifying Storage Groups ............................................................................................... 14
  AppSync Provisioned Devices .............................................................................................. 16
    AppSync’s Internal Storage Group .................................................................................... 16
    Dynamic Movement ......................................................................................................... 16
  Removing Copy Devices from AppSync ............................................................................. 17

ADVANCED COPY DEVICE MANAGEMENT ............................................................................. 17
  Reset Device In-Use Flag ..................................................................................................... 17
  Remove Device from AppSync ............................................................................................ 17
EXECUTIVE SUMMARY

This document provides technical information about integrating Dell EMC AppSync software with VMAX All Flash family storage systems, including the environmental caveats that should be taken into consideration when using both AppSync and VMAX All Flash. This document provides guidance while deploying the AppSync software in environments where application data resides on a VMAX All Flash (AF) array.

AUDIENCE

This white paper is intended for Dell EMC customers that are application and/or storage administrators who are currently administering AppSync in their environment and Dell EMC internal field personnel and partners who assist customers with deploying AppSync.

OVERVIEW

Dell EMC AppSync is software that enables integrated Copy Data Management (iCDM) with Dell EMC’s primary storage systems. AppSync simplifies and automates the process of generating and consuming copies of production data. By abstracting the underlying storage and replication technologies, and through deep application integration, AppSync empowers application owners to satisfy copy demand for operational recovery and data repurposing. In turn, storage administrators need only be concerned with initial setup and policy management, resulting in an agile, frictionless environment. AppSync automatically discovers applications, learns the layout structure, and maps it through the virtualization layer to the underlying storage LUN. It then orchestrates all the activities 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 operations to production.

USING THE GUIDELINES

The information and guidelines described in this document have been provided by Dell EMC AppSync Engineering and Corporate Systems Engineering teams. This information is supplemental and should be used in conjunction with other AppSync documentation, including the AppSync User and Administration Guide, the AppSync Installation and Configuration Guide, and the version specific AppSync Release Notes. Any AppSync terms seen directly within the user interface (UI) are bolded in blue. This provides a direct interpretation to what is seen within the user console, offering clearer readability. For example, within the user interface, there is a menu called Settings where you can click Storage Infrastructure which provides a wizard to add storage arrays. As seen in Figure 1 - AppSync UI Selection, the words in blue are seen verbatim.

Figure 1 - AppSync UI Selection
TERMS AND DEFINITIONS

AppSync uses terms that may also be used commonly in the industry, which may have a slightly different meaning, or perhaps a very specific versus general meaning. The following terms which are defined below, should help provide guidance.

- **Expire** – A process flow of removing copies from within the AppSync UI, and also removing the copy on the array, i.e. unlinking and expiring copies in array.

- **Mount Host** – The host where the copies are about to mount or mounted copy resides. This can be an alternate host, or the same one as the source.

- **Mount Point** – A location used by the mount operation, to which uses an existing mounted file system to attach, as a directory tree, the copied volume, appearing simply as a new directory to an existing file system structure. This is the default AppSync mount location.

- **Object** – Any database, file system, application, or datastore, to which AppSync manages. ACLs are applied to these items. Objects are either subscribed to service plans or repurposed.

- **Recover** – A process flow of extending the copy and mount operation, by also starting the application once mounted, such as bring a SQL or Oracle database online, on a mount host.

- **Repurposing Workflow** – A copy management workflow process, similar to the Service Plan workflow, providing a multi-generation copy process. Repurposing workflows are managed through Copy Management.

- **Restore** – A process flow of overwriting the source volume with the contents of a copy created previously.

- **Service Plan** – A copy management workflow process, and template, for protecting applications. Service Plans are managed in their own menu.

- **Subscribe** – The act performed on or against an object, as to how it gets associated to a service plan. Runs with the service plan, utilizing the service plan’s settings for copy management.
VMAX ALL FLASH CONFIGURATION REQUIREMENTS

AppSync supports creating and managing copies of application data on VMAX All Flash arrays using SnapVX replication technologies. AppSync also supports remote copy management for block based storage with SRDF, and when replicating file based (eNAS) environments using File Replicator.

Please refer to the following VMAX All Flash overview white paper for more information - https://www.emc.com/collateral/white-papers/h14920-intro-to-vmax-af-storage.pdf


AppSync supports SnapVX using pool based LUNs provisioned in the default Storage Resource Pool (SRP). Whilst Multiple SRPs are supported in VMAX, they are not supported by AppSync, therefore only the default SRP is used by AppSync, and cannot be changed. RecoverPoint is not supported with VMAX AF arrays as of AppSync 3.7. SRDF/S is supported for all applications for both local and remote, as well as both simultaneous copies. SRDF/A is limited to non-Microsoft applications for remote copies. eNAS and eNAS File Replicator are also supported. All standard applications are supported, such as Oracle on Linux and AIX, Microsoft Exchange, Microsoft SQL, as well as Linux and AIX file systems and VMware datastores, to name a few. Always refer to the latest support matrix for up-to-date support details - https://elabnavigator.emc.com/vault/pdf/EMC_AppSync.pdf as well as the product guides.

ADVANCED FEATURES SUPPORTED

VMAX All Flash eNAS

AppSync 3.0 and greater offers support for VMAX eNAS (embedded network attached storage). VMAX eNAS offers consolidated file storage, similar to the VNXe array. Please refer to the VMAX eNAS Deployment For Microsoft Windows And SQL Server Environments white paper: http://www.emc.com/collateral/white-papers/h14241-vmax3-enas-deployment-microsoft-sql-server-wp.pdf and also refer to the VMAX eNAS Technical Note: https://www.emc.com/collateral/technical-documentation/h13904-vmax3-embedded-nas-technical-note.pdf for more details.

VPLEX Provisioned Volumes

As of AppSync 3.5, VPLEX with VMAX AF back-end storage is supported. VMAX AF provisioned volumes are now supported behind VPLEX RAID 0, RAID 1, and Metro Distributed environments. The preferred cluster for distributed volumes and the preferred array(s) for RAID-1 volumes for each Service Plan and Repurposing workflow must be configured according to the AppSync 3.5 User and Administration Guide. Please review the AppSync User and Administration Guide for more details including limitations and restrictions on working with VMAX and VPLEX.

AppSync’s “Gold” Service Plan

As of AppSync 3.5, the Gold level service plan can be configured with VMAX AF, when utilizing existing SRDF/Synchronous replication environments. The Gold service plan provides the ability to create simultaneous local (R1) and remote (R2) copies, queiscing the application just once, providing the same point in time image for both copies. Previous to the 3.5 version of AppSync, only the bronze (local) and silver (remote) services plans were supported, which meant separate, or independent, service plans, and as a result, separate point-in-time copies. Please ensure the appropriate version, and configuration, of the SMI-S provider is utilized by referencing the latest AppSync Support Matrix. Please review the AppSync User and Administration Guide for more details including limitations and restrictions when working with Gold level service plans.

VMAX Online Device Expansion

AppSync supports VMAX's ODE (online device expansion) process. AppSync imposes no additional restriction, however, any target device pre-allocated/created, must be expanded manually. For example, depending on the array code level, snapshots must be expired before the expansion process begins. Regardless, if copies are mounted and linked, those devices will be required to be expanded manually, for AppSync to use those targets, or use those targets again. Later VMAX code levels providing support for maintaining snapshots, and R1/R2 relationships, will also be supported in AppSync, however, again, if target devices are utilized, which occur during the link operations, those must be expanded, as the source device and target device size must match.
VMAX SMI-S PROVIDER

AppSync uses SMI-S software to communicate with VMAX storage systems over port 5989. Always refer to the SMI-S Provider table, within the latest AppSync Support Matrix and refer to the AppSync Security Configuration Guide for more details on port requirements.

Multiple SMI-S providers can be configured within AppSync, one as a primary, and the other as a secondary, for redundancy purposes, as well as efficiency purposes. It is more efficient to have a local SMI-S provider when creating local copies, and a remote SMI-S provider when creating remote copies. When creating simultaneous Gold service plan copies, however, one SMI-S provider, preferably local, is required, with gatekeepers presented from both arrays - to that one SMI-S provider. It is possible to have one SMI-S provider managing both bronze (local) and silver (remote) copies. If using two different SMI-S providers, one for the local and one for the remote copies, simply ensure the preferred SMI-S provider is local to that particular array. Please also refer to the AppSync Installation and Configuration Guide for additional details.

IMPORTANT NOTE: AS OF SMI-S VERSION 8.3.0.1, AND HIGHER, SUPPORT FOR TLS 1.0 HAS BEEN REMOVED. TLS 1.0 IS REQUIRED FOR APPSYNC UP TO VERSION 3.1 TO FUNCTION, AND THE SMI-S/ECOM SERVER MUST BE CONFIGURED TO ALLOW TLS 1.0. PLEASE REFER TO DELL EMC KNOWLEDGE BASE ARTICLE NUMBER 490450 ON HOW TO CONFIGURE THIS WITHIN SMI-S. APPSYNC VERSIONS 3.1 AND LATER ARE NOT SUBJECT TO THIS CHANGE. ALWAYS REFER TO THE LATEST SUPPORT MATRIX FOR DETAILED INFORMATION.

COMMUNICATING WITH THE SMI-S PROVIDER

- Queries all required information, such as mapping, device, storage groups, pools, etc.
- Performs active management tasks, such as SnapVX sessions – creating, refreshing, terminating, restoring, LUN masking etc.

The SMI-S provider software can be installed on a Windows or Linux, virtual or physical, machine that has physical connectivity to the VMAX(s) being managed. The SMI-S provider(s) must be registered as a resource in AppSync, and the relevant VMAX arrays added. Please follow the SMI-S best practices, such as ensuring at least six dedicated gatekeepers are presented from the VMAX being managed, to the SMI-S provider host. They should be spread across two fabrics/HBAs for redundancy.

Up to five arrays using a single SMI-S instance can be supported, however, due to performance considerations, ascertained by multiple factors, caution should be used and so the recommendation is one SMI-S provider per local and its remote array. Consider other applications using the provider, total volumes and copies under management, etc., when determining how many arrays one SMI-S provider can support.

If the SMI-S provider and AppSync server share the same host, then the SMI-S provider should be installed first. If AppSync is already installed, install SMI-S provider software and then restart the AppSync server services (EMC AppSync datastore service, EMC AppSync Security Server, and EMC AppSync Service).

If the SMI-S provider host becomes unavailable, as may be the case when heavily utilized by other applications, the AppSync service plan will fail. It is for this reason, multiple SMI-S providers should be utilized or additional gatekeepers presented.

REMOVING AN SMI-S PROVIDER

Removing an SMI-S provider is accomplished by navigating to Storage Infrastructure, highlighting the VMAX array, selecting the SMI-S provider host, and clicking Remove. If any VMAX array uses this particular SMI-S provider as a preferred array, if an array is managed purely by this particular SMI-S provider and has valid copies or storage configured, the removal fails with an appropriate error message.
VMAX ARRAY DISCOVERY AND CONFIGURATION

VMAX arrays are discovered using SMI-S providers that manage the VMAX. VMAX arrays are added as seen in Figure 2 - Add VMAX, Figure 3 - SMI-S Credentials, Figure 4 - Select VMAX, and Figure 5 - Select Storage Group. AppSync requires administrative, or equivalent credentials, to the SMI-S provider. As part of the discovery phase, AppSync establishes a connection with the SMI-S provider, obtaining a list of all the arrays managed, along with detailed information about the arrays, such as the microcode information and model number. A Rediscover should be performed when changes are made to the array, such as adding additional disks to a storage group, however, as informed after the array is added, seen in Figure 6 - VMAX Auto Device Discovery, AppSync does perform a routine rediscovery, occurring twice a day. AppSync uses a secure connection to communicate with the SMI-S provider. Ensure the latest support matrix is referenced to determine which version to use with the particular environment.

Figure 2 - Add VMAX
Figure 3 - SMI-S Credentials

Figure 4 - Select VMAX
PLEASE NOTE: WHEN ADDING A VMAX ARRAY, OPTIONALLY CHOOSE A STORAGE GROUP, HOWEVER, ONLY THE DEFAULT SRP IS SUPPORTED. VMAX ARRAYS WITH MULTIPLE SRPS IS NOT SUPPORTED. WHEN A VMAX AF ARRAY IS CONFIGURED WITH A STORAGE GROUP THE DEVICE DISCOVERY WILL HAPPEN IN THE BACKGROUND.

MODIFYING CREDENTIALS
If the SMI-S provider credentials are modified by the SMI-S admin, they must also be changed within AppSync. Navigate to the Storage Infrastructure menu, highlight the VMAX, highlight the SMI-S host, and then click Edit in order to change the credentials.

PROVIDER PREFERENCE
AppSync uses the SMI-S provider that was used to initially discover the VMAX array, as the preferred provider. The preferred order, in the case of multiple SMI-S providers, can be changed within the AppSync UI by highlighting the provider and clicking Set Preferred.

PREVENTING AUTOMATIC DISCOVERY OF ARRAYS
It is best practice to limit each SMI-S host to one local, and its corresponding remote array, however, one SMI-S server may manage up to five, based on performance considerations. The performance of the SMI-S provider is critical to AppSync’s performance. The discovery of arrays on an SMI-S provider host, which is not used by AppSync, may impact the performance of AppSync jobs. If the SMI-S provider discovers arrays which do not need to managed by other products, including AppSync, please follow the SMI-S documentation for creating a symavoid file to alleviate the discovery of those other arrays.
**REMOVING A VMAX ARRAY FROM APPSYNC**

VMAX arrays can be removed from AppSync only when no active copies exist for which AppSync created - all copies AppSync created must first be expired. If storage groups are configured, they too must be de-configured. Remove the VMAX by navigating to Settings > Storage Infrastructure, highlight the array and click Remove. If anything remains configured, an error will be displayed and will prevent the VMAX from being removed.

If a VMAX array is removed from the SMI-S provider, before being removed from AppSync, AppSync removes the association between the two. If there are no AppSync created VMAX copies or storage groups, then the VMAX array itself is also removed upon rediscovery.

**STORAGE MANAGEMENT**

AppSync utilizes SnapVX technology which offers targetless copies. Target devices are only required when link operations occur. There are two link operation workflows which must be considered. SnapVX links copies in two different modes, No-Copy and Copy. In AppSync, the copies are marked as SnapVX snap (No-Copy) and SnapVX clone (Copy).

- **Service plans** do not require target devices during the copy phase, if the replication technology is SnapVX snapshots. For SnapVX clones, target devices are required during the copy phase, as SnapVX linking happens during the copy phase when using SnapVX clone technology. SnapVX snapshot copies are linked to target devices during the mount operation. SnapVX snaps are targetless copies, until mount operations occur.

- **Repurposing workflows** require target devices during the copy phase for the 1st generation snap and clone copies, but not for the 2nd generation snapshot copies. The 2nd generation snapshot is linked during the mount phase, just like when using service plans – please refer to the SnapVX Linking section for more details.

AppSync provides the following the storage configuration options to support target link operations:

**USER CONFIGURED STORAGE GROUPS**

Storage administrators can use an optional storage group for target copy devices. Using a dedicated storage group, which contains preconfigured target devices for link operations, AppSync is restricted to using just those devices, when configured. AppSync relies on there being enough storage devices available in this particular storage group, and if there is not, job linking operations fail. Storage groups are configured globally, which means that there is no way to restrict, or define, which source volumes are linked to a particular storage target, in a particular storage group. SnapVX does not offer a way to define a source-to-target pairing relationships using the AppSync UI.

- If a storage group is not defined, AppSync will use the default SRP to create target devices to link with SnapVX copies.

- Configuring a storage group prevents AppSync from provisioning target devices in the SRP – devices must be available in the configured storage group. If the storage group is not configured, AppSync will provision target device from the SRP.

- If a storage group is configured in AppSync for target devices, yet target devices are not available for the link operation, the process will fail.

- Do not configure the user storage group with a masking view or an SLO. AppSync cannot configure a storage group with a masking view, and if an SLO is configured, a warning is seen. Not configuring SLOs is the recommendation to improve the performance during mount operations. Refer to the mount section for more details.

**Configuring Storage Groups for Copy Target Devices**

Create one or more Storage Groups without host connectivity (not configured with a masking view). Please take note of the following rules when provisioning new target devices for copy processing:

- Make sure the target copy device is the same size configuration as the source device.

- All devices in the configured storage group(s) are used as copy devices, so never add production volumes into AppSync assigned storage group(s) as it will result in data loss. This is also why AppSync does not allow the storage group to have a masking view. Do not share the same storage group(s) across multiple AppSync servers.
Devices created by AppSync, perhaps prior to configuring storage groups, are not automatically added to a configured storage group, so AppSync created devices must be added to the configured storage group manually if to be used as target devices from the configured storage group.

After configuring the storage groups, AppSync updates the element name and volume identifier with AppSync's host name. This is to identify the AppSync copy devices in the array and proclaims these devices for AppSync's use. AppSync updates the device with AppSync <Hostname> Volume <volume ID>, as seen in Figure 7 - Element Name.

AppSync only discovers storage groups which are not part of any masking view. This is designed to protect devices presented to hosts, as in the case of production volumes. To configure a storage group for an AppSync target device selection, enable it by clicking on the checkbox as seen in Figure 5 - Select Storage Group. AppSync allows selecting multiple storage groups. Once selected, a warning states that the devices within in the selected storage group "will be used as target for copies created by AppSync," as seen in Figure 8 - Storage Device Warning. The data on those devices will be overwritten.

Review the storage details within AppSync, under Storage Infrastructure, by clicking on the VMAX, as seen in Figure 9 - Storage Details. When multiple storage groups are added, the Number of Devices is the sum of all storage groups.
Modifying Storage Groups

Once a storage group is modified on the array, such as through Unisphere for VMAX, the storage array within AppSync must be rediscovered. For example, run a rediscovery when adding additional target volumes to a storage group. To rediscover the VMAX storage group, navigate to Storage Infrastructure, click the VMAX array, then click Rediscover as seen in Figure 10 - Storage Rediscover. As of AppSync 3.7, AppSync runs an automatic maintenance activity every 12 hours, at 11:15 and 23:15, which includes the rediscovery process.
Configuring, or de-configuring storage groups is accomplished by clicking \textit{Manage Copy Storage} as seen in Figure 11 - Manage Copy Storage.

Once the \textit{Manage Copy Storage} dialog box appears, simply deselect the storage group, preventing AppSync from assigning target storage from it, as seen in Figure 12 - Removing a Storage Group.
APPSYNC PROVISIONED DEVICES

If storage groups are not configured, AppSync has the ability to create and link devices dynamically. This is to say, AppSync creates devices as needed during linking operations from the default SRP.

VMAX AF uses the default Storage Resource Pool (SRP) and cannot be configured differently. VMAX AF with multiple SRP is not supported in AppSync.

Devices provisioned by AppSync are named AppSync-{AppSync_Server_Name}. An example is AppSync-lrmf053, where lrm053 is the AppSync server name as seen in Figure 13 - AppSync Provisioned Name. This can be used to identify all devices which have been provisioned by AppSync.

![Figure 13 - AppSync Provisioned Name](image)

AppSync's Internal Storage Group

As of AppSync 3.7, AppSync keeps all its provisioned devices in an internal storage group on the VMAX, which is created by AppSync. The name of the internal storage group is <hostname>_INTERNAL_-AppSync-0, where hostname is the name of the AppSync server. Do not add or remove device from this internal storage group created by AppSync, as it is being managed by AppSync. The internal storage group is created without an SLO, to enhance the performance during mount operations, and it is advised to refrain from applying one.

PLEASE NOTE: IT IS BEST PRACTICE TO MANAGE A VMAX ARRAY WITH ONE APPSYNC SERVER. MULTIPLE APPSYNC SERVERS MANAGING THE SAME VMAX ARRAY IS NOT RECOMMENDED.

DYNAMIC MOVEMENT

AppSync dynamically moves the linked devices into the mount host's storage group, for presentation to that host, during mount operations. AppSync moves the device back out, and into its original storage group, during unmount operations. When using a configured storage group with preconfigured target devices, AppSync moves the devices back into that storage group after an unmount operation.

When using AppSync provisioned devices, and the internal storage group, AppSync does not pull devices out of that storage group, unless there has been an SLO policy applied. Applying an SLO policy is not recommended, nor any manual maintenance of the internally created storage group.
REMOVING COPY DEVICES FROM APPSYNC

Copy (target) devices can be provisioned by AppSync from the default SRP, or they can be provisioned by a storage administrator. Excluding the copy target device from AppSync’s management capabilities by first removing the device using the VMAX In-Use Device management feature, if using AppSync 3.7 or later (follow the guidelines in the Advanced Copy Device Management section), or remove the device from the storage group using Unisphere for VMAX, if using prior versions.

If any configuration changes on the array, an array rediscovery should be performed in AppSync to update the device properties. This is a manual process. In addition, deleting devices on the array also requires a rediscovery to remove the devices in AppSync’s device inventory.

AppSync 3.7 and greater runs a VMAX maintenance process which includes a rediscovery twice a day. This AppSync maintenance operation also deletes copies in AppSync, if the copy is deleted on the array, such as if someone deletes the copy manually outside of AppSync.

Do not delete devices on VMAX arrays used by AppSync, unless those devices are no longer managed by AppSync. AppSync does not delete devices which it has provisioned from the SRP by default, when expiring them from within AppSync. If devices provisioned by AppSync are to be deleted, first ensure to validate their in-use flag. Please refer to the following section for more details.

ADVANCED COPY DEVICE MANAGEMENT

As of AppSync 3.7, there is an option to view and manage the copy devices associated with applications; for better device management. The new wizard, VMAX In-Use Devices, provides insight into the target devices. The devices depicted are either created by an end user, who has placed them into a storage group configured within AppSync, or AppSync provisioned devices, seen in Figure 15 - User Provisioned Devices and Figure 16 - AppSync Provisioned Devices. Any device being actively used in a workflow is depicted under the In Use For Replication column, as true. If a device was used at one time, but is no longer in use, but would be a preferred device to be used once again by AppSync, then the flag would be set to false. For any device that is not being used for replication, set to false, an administrator can remove it from being managed by AppSync safely. The administrator can then remove it from the storage group if that storage group was created by the administrator. If the device had been created/provisioned by AppSync, meaning the device was created out of the SRP, then an administrator can also initiate an array device delete. Otherwise, to delete the device, an administrator must delete the device using Unisphere for VMAX, once removed from AppSync’s management.

To review the devices AppSync manages, simply navigate to Settings > Storage Infrastructure, select the array, then click the number of devices next to Number of Devices. The number is in blue and serves as a hyperlink to the menu for management.

There are two main tabs, User Provisioned and AppSync Provisioned. Both menus display the volume ID, the in-use flag, and what storage group name, or pool name, the device belongs. For each device, a user can reset the in-use flag, remove the device from AppSync management (if it is not actively being used) and find out more details of the device. If the device was provisioned by AppSync, an administrator can also delete the device on the array. More details of each feature/function are detailed below, and please refer to the following screen shots for visual representations.

APPSYNC MANAGES ALL COPY DEVICES, AND TRACKS THE ASSOCIATED ARRAY STATUS. ANY SORT OF MANUAL MANIPULATION OF THE DEVICE, WHETHER IT BE ON THE ARRAY OR HOST, IS NOT RECOMMENDED. IT IS BEST TO FIRST REMOVE THE DEVICE FROM THE LIST OF MANGED DEVICES, BEFORE USING THE DEVICES ELSEWHERE.

RESET DEVICE IN-USE FLAG

This operation resets the device’s in-use flag within AppSync. AppSync manipulates the inuse flag for the copy device. If it is not set due to server shutdown, one can reset the in-use flag manually for the device. Resetting the in-use flag is allowed only for devices that are not associated with any copies.

REMOVE DEVICE FROM APPSYNC

This operation removes a device from AppSync’s device inventory, and will remove it from the internal storage group on the array, if applicable. A confirmation message appears as seen in Figure 17 - Removing Device from AppSync.
DELETE DEVICE IN ARRAY

This operation is allowed only for AppSync provisioned devices. This operation deletes the AppSync provisioned device on the array as well as from AppSync’s inventory.

APPLICATION COPY INFO

This provides the associated copy information for the device, if a copy exists. The application type and name, server name, service plan name, and created timestamp of the copy are displayed as seen in Figure 19 - Application Copy Info.

FIGURE DEPICTIONS

Figure 14 - Number of Devices - Click the device number next to Number of Devices to launch the VMAX In-Use Devices menu.

Figure 15 - User Provisioned Devices – Displays the devices the user created and placed into a storage group managed by AppSync.

Figure 16 - AppSync Provisioned Devices – Displays the devices AppSync creates from VMAX’s default SRP.

Figure 17 - Removing Device from AppSync – Confirmation message when removing devices from AppSync.

Figure 18 - Error Removing a Device – Seen if attempting to remove a device while it is being used for replication.

Figure 19 - Application Copy Info – Displays the copy information details.
Figure 15 - User Provisioned Devices

Figure 16 - AppSync Provisioned Devices
Figure 17 - Removing Device from AppSync

Figure 18 - Error Removing a Device

Figure 19 - Application Copy Info
SNAPVX CONFIGURATION DETAILS

VMAX AF utilizes SnapVX, a new technology introduced which replaces the VMAX TimeFinder/Clone and VPSnap technologies. SnapVX eliminates the need for the traditional device management tasks, often associated with TimeFinder VPSnap, such as configuring save pools, creating target devices for pairing operations and provisioning tasks. Creating point-in-time copies now utilize VMAX’s Storage Resource Pools (SRPs), to maintain the changed tracks, which needs no configuration for AppSync to utilize, other than adding the array to AppSync. AppSync utilizes the default SRP, so offers a rapid setup. AppSync supports the default SRP only. For more details regarding the way SnapVX utilizes the SRP, please refer to the following white paper - http://www.emc.com/collateral/technical-documentation/h13697-emc-vmax3-local-replication.pdf.

AppSync provides two copy methods with TimeFinder on VMAX2, Clone and VPSnap. A clone is a 100% like-for-like copy of the source data, while the VPSnap is based on pointers, directing changed writes to a pre-configured virtualized storage pool. With SnapVX, however, this nomenclature has changed. Like-for-like target devices and pre-configured storage pools are no longer required. AppSync can utilize pre-configured devices added to a pre-configured storage group, if so desired. These devices are only utilized during the mount phase, or during the 1st generation repurposing workflow copy phase for snapshot operations.

AppSync provides support for both SnapVX Copy and NoCopy modes. Copy mode is similar to the way VMAX2 was used to create TimeFinder Clones, and the NoCopy mode is similar to TimeFinder Snaps.

When thinking about how TimeFinder works, there is a concept of create and activate, where create essentially pairs the device with a pre-configured target device, and activate creates the point-in-time copy, also reads the device to be presented to a host. SnapVX does not subscribe to create then activate nomenclature. With SnapVX, the point-in-time copy is established as a target-less device during the copy phase for SnapVX snapshots, only assigning a target device during link operations, for which AppSync initiates during the mount phases. For SnapVX clone, it links to the target device during the create-copy phase itself. The same is applicable for the repurposing workflows, however, for both snapshot and clone operations, AppSync assigns a linked target device during the copy phase, and not just during a mount operation for snapshots. This is discussed in more detail in the Repurposing Workflow section. Please also see the SnapVX Linking section for more details.

SNAPVX LINKING

Target devices are not necessary when creating copies with service plan workflows during the create copy phase for SnapVX snapshots. When creating SnapVX clones, however, target devices are required during the create copy phase. The SnapVX snap copy becomes linked to a target device only when accessed, such as when mounted. If storage groups are configured with pre-configured and available devices, AppSync uses those devices, otherwise, if storage groups are not utilized, AppSync creates new target devices from the default SRP if target devices have not already been established and paired. When devices are unmounted, they are not unlinked. Target devices are unlinked only when copies are expired from within AppSync. As of AppSync 3.7, target devices provisioned from the SRP by AppSync are tagged by AppSync and AppSync creates its own storage group on the array for better internal device management, and all the devices will be moved to that internal storage group.

Repurposing workflows behave somewhat differently than service plan workflows. Repurposing the 1st generation copy creates a snapshot of the device, also linking to a device, regardless if that device is set to mount for both snap and clone. This differs from a non-repurposing service plan as target device is required in create-copy for 1st generation copies snap and clone both. If storage groups are utilized, and no target device is available, the repurposing job fails. Refreshing the 1st generation copy will create a new snapshot and relink to the same target device. Mounting will not perform the linking as would be the case when working with service plans. Unmounting the device does not unlink the device, expiring the device does, just as a service plan. Service plans and Repurposing workflows are described in more detail, in the AppSync User and Administration Guide.

The 2nd generation copy is created from the 1st generation copy, though differs in behavior. The 2nd generation SnapVX snap copy will not link to a target during the copy phase, as does the 1st generation copy. But the 2nd generation SnapVX clone copy will link to a target during the copy phase, as same as 1st generation copy. This process is more like service plan workflows, in that target devices are linked upon the need to access the data, such as through a mount operation. Refreshing the copy will create a new snapshot and relink only if the snapshot had already been linked, such as if it had been mounted. Expiring the copy, again, will unlink the device and delete the snapshot.
### Table 1 - Workflow Comparisons

<table>
<thead>
<tr>
<th>AppSync Workflows</th>
<th>Copy Phase</th>
<th>Mount Phase</th>
<th>Unmount Phase</th>
<th>Refresh Phase</th>
<th>Expire</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Plans</strong></td>
<td><strong>Snap</strong></td>
<td><strong>Linked</strong></td>
<td>Requires Targets</td>
<td>Does not unlink</td>
<td>Relinks</td>
</tr>
<tr>
<td></td>
<td>Targetless</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Clone</strong> - Linked</td>
<td>No changes</td>
<td>Requires Targets</td>
<td>Does not unlink</td>
<td>Relinks</td>
</tr>
<tr>
<td></td>
<td>Requires Targets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Repurposing</strong></td>
<td><strong>1st Generation Snap/Clone</strong></td>
<td><strong>Linked</strong></td>
<td>Requires Targets</td>
<td>Does not unlink</td>
<td>Relinks</td>
</tr>
<tr>
<td></td>
<td>Linked - Requires Targets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>2nd Generation Snap</strong></td>
<td></td>
<td>Linked</td>
<td>Does not unlink</td>
<td>Relinks</td>
</tr>
<tr>
<td></td>
<td>Targetless</td>
<td></td>
<td>Requires Targets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>2nd Generation Clone</strong></td>
<td><strong>Linked</strong></td>
<td>Requires Targets</td>
<td>Does not unlink</td>
<td>Relinks</td>
</tr>
<tr>
<td></td>
<td><em>1st Gen must also be set to Clone</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linked - Requires Targets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SnapVX Linking FAQ**

Some frequently asked questions (FAQs) regarding SnapVX and Linking are below:

1. Q: When AppSync mounts VMAX All Flash copies, it links them to target devices. Does it unlink the target device when un-mounting?
   
   A: No, it does not unlink when un-mounting, only when expiring.

2. Q: Does it not make more sense to have AppSync unlink when un-mounting?
   
   A: This is a feature of SnapVX which AppSync utilizes to increase efficiency during the next mount operation of the same SnapVX snapshot. The device maintains the same address in the masking view settings, specifically the port group, so behaves much more efficiently.

3. Q: How is the repurposing “relink” feature utilized?
   
   A: The relink use case with the repurposing workflow provides an incremental refresh process since the device is not unlinked till expired. The refresh process is only incremental if the device remains linked, so the 1st generation refresh always links to a device, in order to allow quicker refreshing and also allows it to be the source for multiple 2nd generation copies.

4. Q: Can Appsync use the same targets for the next mount operation?
   
   A: Yes, when refreshing, AppSync does an unlink and relink internally, which is transparent to the end user.

**SNAPVX RE-LINKING**

As of AppSync 3.1, AppSync supports VMAX SnapVX Re-Linking when utilizing SnapVX Clone (set within storage preference in the service plan or through the repurposing workflow). SnapVX Re-Linking allows copies to be created more efficiently by avoiding the full copy, which reduces the amount of time consumed during consecutive mount operations, by relinking with the same target device(s).

With this enhancement, the relink occurs during the copy phase, rather than the mount phase. This provides an incremental copy, versus a full copy.

Take a case where the service plan is configured for one copy only (expiration = 1). AppSync creates two copies, due to the nature of AppSync ensuring there is always a good copy during the new copy rotation. The previous copy, however, is now expired once the new one is created. AppSync does not allow a failure during the new copy process to expose the environment, but previously consumed N+1 amount of space (if production is 500GB and copy count =1, 1TB would be consumed). Again previously, when copy mode is active, meaning full clone operations, AppSync would take an extended period of time for the second copy to complete, due to the nature of how AppSync manages linked targets - with “Clone” technology selected. As of AppSync 3.1, however, relinking is now utilized to provide incremental copies. This greatly shortens the amount of time for the second copy and reduces temporary storage (expires the rotated copy once the new copy is complete).
PROTECTING APPLICATIONS USING APPSYNC SERVICE PLANS

AppSync is an application-centric copy management solution, with the approach of protecting dynamic application environments. AppSync uses a concept of service plans, which provides a robust class of service for each of the application types supported. Each application type has three default tiered service plans:

- A **Bronze** plan for creating local copies
- A **Silver** plan for creating remote copies (remote array based copies with SRDF integration)
- A **Gold** plan for creating local and remote copies (Copies at both the local and remote site in an SRDF session).

Applications can be subscribed to different service plans based on their required SLAs, and/or recovery point objectives (RPO). Service plans are composed of several **phases** which define the copy schedule/on-demand, copy technology type, copy retention, application backup type, mount options, and any other options that may be required. The different phases are depicted in **Figure 20 - General Service Plan Phases**.

![Figure 20 - General Service Plan Phases](image)

After registering and configuring VMAX storage, and after adding application hosts, subscribe the application to a service plan to create and manage copies. **Bronze**, **Silver**, and **Gold** plans are supported for applications residing on VMAX storage systems. **Snapshot** is the default replication technology, which can be change. For instance, if a full copy/clone is desired, change the **Storage Preference** to **Clone**, either by moving it to the top of the list, or by simply deselecting the other technologies as seen in **Figure 21 - Storage Preference**. Please refer to the **AppSync User and Administration Guide** for more details on Service Plan settings.
APPLICATION DISCOVERY PHASE

Before creating the copy, AppSync must examine the application in order to account for changes, such as device expansion, addition, or removal, or if a change in status has occurred, such as whether the previous databases remain online. This phase is not configurable, nor can it be disabled.

APPLICATION MAPPING PHASE

Similar to the discovery phase, this phase always runs, and is not user configurable. During the application mapping phase, AppSync maps the application components, for example, the databases and log files, to underlying file systems and physical disk objects. AppSync then maps these file systems and disk objects through any virtualization layer, and back to the underlying storage array, i.e. LUNs. AppSync gathers all the storage system device information pertaining to these LUNs. If the underlying LUNs are on a VMAX system, the following operations are performed by AppSync:

- AppSync uses the SMI-S provider to map the world wide names (WWNs) of the source LUNs to a corresponding VMAX array to obtain their details. If a virtualization layer exists, such as LPARs, VMware, or VPLEX, etc, AppSync inventories these objects as well. These details include the type of disk, RAID type, etc. This occurs every time a service plan is run, and cannot be deselected. If there are any changes to the device on the array, AppSync is updated of those changes, such as if the size is changed.

- SMI-S providers should be kept online, otherwise delays may be experienced. If an SMI-S provider host is taken down for maintenance, for example, it should be removed from within AppSync, or the preferred list should be modified.

- For Silver and Gold service plans, AppSync also tries to find the remote device, i.e. R2, after getting the R1 details from the SMI-S Provider. For Silver plans, or remote repurposing workflows, it is preferred to use an SMI-S provider local to that remote array, and for Gold service plans, it is a requirement to utilize a single SMI-S host which has gatekeepers presented from both arrays. The local SMI-S provider is preferred.

Affinitization Rules

Once the mapping phase completes, AppSync affinitizes the applications based on certain rules allowing groups of applications to be replicated together, i.e. when multiple applications are subscribed to the same service plan. Affinitization rules are application-specific, as well as storage-specific. For example, each application has rules specific to that application, eg. SQL, Oracle, VMware, as well as rules specific to a storage system on which the application data resides. In the case where the application data resides on a VMAX storage system, the following affinitization rules apply:

- Affinitize by VMAX array ID: This rule is based on the VMAX ID (serial Number). If two databases, datastores, etc., are on the same host but are on two different VMAX systems, AppSync separates them into different PIT (point-in-time) copies.

- Affinitize by RA Group (only for plans using SRDF): All devices belonging to the same RA group are protected as one point-in-time copy.
Affinitization by Application: If an application, such as a database, is on a different host, instance, or consistency group, then AppSync breaks the copy into different PiTs.

CREATE COPY PHASE

Just like the previous two phases, the copy phase must run, though is user configurable. During the create copy phase execution, AppSync interacts with the array and application components to create application consistent (by default), point-in-time copies of the applications which were grouped together as one affinitization set. For each set of applications, one create copy phase is executed as part of a single service plan execution cycle. For example, if the affinitizer results in three sets of applications as part of an affinitization process, three create copy phases are executed during a single service plan execution cycle. Details pertaining to applications on VMAX follow:

- AppSync supports SnapVX Snap (no copy) and SnapVX Clone (copy) for VMAX All Flash as the supported copy technologies
- By default, all service plans have snapshot as the preferred storage technology type. If clones are desired, change the storage order preference, or deselect the other technologies, as seen in Figure 21 - Storage Preference.
- A specific copy rotation value in the service plan settings can be configured. The default value is seven, whereas the schedule is every 24 hours starting at midnight, by default, thus creating seven copies, or one weeks’ worth of copies by default.
- AppSync always uses the differential copy option. This is done so that AppSync does not need to perform a full synchronization in the event that a clone copy is rotated (expired from AppSync and new clone created at differential point-in-time).
- With AppSync 3.1 and greater, SnapVX relinking is utilized so when creating clones, the linking occurs during this phase. Please refer to the SnapVX Linking
- When considering creating remote copies, such as taking snaps and clones off of the R2:
  - AppSync does not manage the SRDF sessions, it simply utilizes the pre-established configuration
  - AppSync only supports SRDF/S and SRDF/A – please refer to the support matrix, as well as the AppSync User and Administration Guide’s section under Service Plan Overview, for the current list of what applications are supported for each technology, e.g. supporting SRDF/A with Microsoft applications is not supported.
  - For SRDF/A the link state should be in “Consistent” or “Synchronized“ for replications to work properly. For SRDF/S, link state should be “Synchronized”.
  - Use the Silver service plan to create copies off the R2.
  - AppSync 3.5 and greater supports Gold service plans for SRDF/S and SRDF/A.
  - Creating snapshot copies off R2 with asynchronous mode (SRDF/A), the following may apply, depending on the array code level:
    - Device level write pacing– please refer to the SRDF product guide for more details
    - All the devices which constitute a single application should belong to the same RA Group


Special Handling for Oracle Applications

AppSync splits Oracle copies into two distinct point-in-time copies. The first point-in-time copy is created for all the database files (control files, redo logs and data files), and is created while the database is in hot-backup mode, by default. The second point-in-time copy is created for the archive log volumes, including optionally the Fast Recovery Area. This archive log copy is made after Oracle has been taken out of hot-backup mode, and only when the first point-in-time copy phase is completed. Since VMAX clones can take a longer time to complete (i.e. all tracks must synchronize), after the first point in time copy is activated, a second point-in-time copy can take a significantly longer time to complete after the first point-in-time copy. To avoid this, AppSync efficiently completes one full clone synchronization cycle between the source and target devices, before triggering the first point-in-time copy. Since all tracks are completely synchronized before activating the first point-in-time copy, the second point-in-time copy doesn’t need to wait, as it is just an update of changed tracks.

Expanding Copies

Expanding copies with AppSync, on a VMAX array, does not delete the devices on the array, even if provisioned by AppSync. The AppSync expire command does not equate to symsnapvx terminate. AppSync will re-use the target devices for the next snapshot, or clone, of the same source device. This reduces the time it takes to provision devices as targets. Optionally run SYMCLI commands to validate, for example “symdev show [target ID]” or “symsnapvx list.”

MOUNT COPY PHASE

AppSync supports dynamic mounting of application copies created on VMAX for all AppSync supported platform types, i.e. Linux, AIX, and Windows. AppSync doesn’t support static mounting of VMAX copies except through using RecoverPoint. AppSync relies on VMAX’s auto provisioning capability to provision devices to mount hosts. AppSync requires the mount host to be zoned to the VMAX array and should have a masking view with the appropriate initiator, port, and storage group, in anticipation for mount operations.

To perform dynamic mounts of VMAX copies, AppSync first finds the mount hosts FC/iSCSI adapter information and then interacts with VMAX via the SMI-S provider to find an appropriate storage group. Once AppSync finds the appropriate storage group, the target copy devices are added as shown in Figure 22 - Mounting Wizard.
Mount Host Storage Group Rules

- For virtual machines, AppSync performs mounts by masking the copies to the ESX host, and then adds the devices to the virtual machine.

- In case the host is connected to VMAX via multiple masking views, and the host is not an ESX host in a cluster (for virtual or RDM mounts), AppSync gives first preference to a masking view dedicated for that host. For example, the initiator group connected to the masking view has only initiators for that host). In this scenario AppSync adds the target devices to that storage group, connected to the dedicated masking view.

- If AppSync doesn't find a dedicated storage group, it creates a list of storage groups with all storage groups attached to each of the masking devices that are connected to the host and then picks up the first storage group. If the selected storage group is dedicated for GK devices (i.e. has only gatekeeper devices), AppSync picks up the next storage group in a sorted list. If no other storage group exists except the one with only GK devices, AppSync selects that storage group.

- For an ESX host in a cluster, AppSync tries to find a masking view which has connectivity to the maximum number of nodes of the ESX cluster. If it finds such a common masking view, it uses the storage group to add the devices during the mount phase. In case any ESX nodes in cluster are not connected to this common masking view, AppSync searches for a masking view for that node as outlined in steps 2 and 3. If no storage group for any node of the cluster is found, the mount operation fails with appropriate exception.

- When the selected masking view is connected to a cascaded storage group i.e. storage group containing a list of other storage groups, AppSync sorts the storage group by its name and picks up the first storage group checking the storage group is not dedicated for GK devices. If the selected storage group is dedicated for GK devices, AppSync picks the next storage group in sorted list.

- When working with SQL cluster mounts, if the use dedicatedStorageGroup option is selected (selected by default), and if AppSync is unable to find any dedicated storage group for the mount host, an exception is displayed and the mount fails.
During **unmount**, AppSync finds the storage group using the same rules as described previously and removes the devices from the storage group as shown in Figure 23 - Unmounting Copies.

**Figure 23 - Unmounting Copies**

### Mounting with the Desired SLO

AppSync offers the ability to choose the desired Service Level Objective (SLO) when mounting target devices. AppSync will add the target devices to a storage group associated with the desired SLO, if configured within AppSync. If no storage group exists that match the SLO selection, then the devices are added to any storage group associated with the mount host selected.

VMAX AF restricts devices to one SLO associated storage group at any one point in time. Due to this restriction, AppSync 3.7 and later removes the device from the AppSync created internal storage group, if that storage group is associated with an SLO, and place the device in the mount host’s storage group. Previous versions of AppSync do not utilize the internal storage group for AppSync provisioned volumes, so this point does not apply. For storage groups that are user configured, devices are always removed and placed into the mount host's storage group.

The reverse also applies during an unmount operation, where AppSync removes the target device from the mount host's storage group, and places it back in the user configured storage group, and optionally the AppSync created internal storage group if an SLO was assigned. If the internal storage group does not have an associated SLO policy, the device movement during mount and unmount is avoided.

Refraining from associating an SLO with the AppSync created internal storage group improves the performance during the mounting and unmounting phases. VMAX AF devices can be in both, non-SLO storage groups and a SLO storage groups, such as the mount host' storage group, at a same time.
Changes to a Mounted Copy

AppSync does not support preserving changes made to target devices when they are mounted. It is not possible to create a copy, make changes to that presented copy, which is using target devices associated with the created snapshots, and then restore the copy preserving those changes. This is due to the way SnapVX manages snapshots vs. linked devices. The linked devices do not change the original snapshot, so when restoring the SnapVX snapshot, any changes made to a linked/mounted device is discarded as AppSync uses the snapshot point-in-time to restore data.

REPURPOSING WORKFLOWS

Repurposing workflows are very similar to service plan workflows, in that the same phases are followed, as seen in Figure 20 - General Service Plan Phases. There are differences, however, such as the repurposing workflow allows taking multi-generation copies. The repurposing workflow offers a 1st generation copy which can be used for restore purposes, and also serves as a source for multiple 2nd generation copies. Both generation copies can be mounted and written to, but only the 1st can be restored back to production.

- **1st Generation Copies**: Can be used for restore purposes and serves as the source for multiple 2nd generation copies. 1st generation copies integrate with the production application.

- **2nd Generation Copies**: Cannot be used for restore purposes and is created from a 1st generation copy (e.g. snap-of-snap, snap-of-clone, or clone-of-clone – creating clone-of-snap is not supported). 2nd generation copies do not integrate with any application, so it is imperative the 1st generation copy is not mounted during its creation.

PLEASE NOTE: IT IS NOT RECOMMENDED TO MOUNT THE 1ST GENERATION COPY IF CREATING 2ND GENERATION COPIES, UNLESS THE INTENTION IS TO MASK DATA, OR CHANGE THE DATA, BEFORE CREATING AND PRESENTING THE 2ND GENERATION COPIES. IN THIS CASE, IT IS ADVISED THE 1ST GENERATION COPY IS UNMOUNTED, AS NO APPLICATION INTEGRATION OCCURS WHEN CREATING THE SECOND GENERATION COPY, SO IF THE 1ST GENERATION COPY IS MOUNTED, THERE IS A CHANCE THE 2ND GENERATION COPY WOULD BE CORRUPT, OR INCONSISTENT.

When working with SnapVX snapshots and service plan workflows, devices are only required when linking. With the repurposing workflow, however, the 1st generation copy automatically links to devices, regardless if the devices are mounted. The 2nd generation copy shares the same rules as service plan copies, where linking only occurs during the mount operation. With this knowledge, ensure that there are either target devices available in the storage group AppSync is configured with, or if no storage group is configured, allow AppSync to create devices as necessary. SnapVX clone operations always require target devices during the copy phase.

SnapVX Linking Rules with Repurposing Workflows

- **1st Generation Copies**:
  - Create copy phase will create the copy of the device and link it to a target
  - Refresh will create a new copy and relink to the same target device
  - Mount will not do the linking, as the copy is already linked
  - Unmount will not unlink the target device, and only unmounts from the host (speeds up re-mounting)
  - Expire will unlink the target device and delete the copy within AppSync (device created remains on the array)

- **2nd Generation Copies**:
  - Create copy phase will create the copy, however, will not be linked to a target device (unless creating clones)
  - When the copy needs to be accessed, i.e. mounted, it is linked to a target device, then mounted
  - Refresh will create a new copy, and relinked if the original copy was already linked to a target device
  - Expire will unlink the target device, if linked, and deleted (any target device created remains on the array)
Repurposing Use Case

The following depicts a common repurposing workflow use case. A database developing group wishes to create multiple copies of production. Users require a point-in-time copy to serves as the baseline copy, the “gold” copy, for the development group’s testing. Since multiple users need the same point-in-time copy, they must use a common sourced copy, from the same PIT. This is the 1st generation copy, also commonly referred to as a “gold” copy. This copy, by default, is application consistent.

Each user has the ability to create 2nd generation copies, presenting them to different hosts. Each copy is autonomous, and can be refreshed upon demand, or schedule. The 1st generation copy can be refreshed as well, independently, thus providing a diverse work environment. The 1st generation copy, being that it is not mounted or changed, can also serve as a restorable copy.

Example 1st Generation Repurposing Workflow Process Flow

The following expert of the process log depicts a common flow for creating a 1st generation copy, for the first time, with a mounting option.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Phase</td>
<td>Beginning execution of service plan</td>
</tr>
<tr>
<td>Application discovery</td>
<td>Application discovery phase beginning</td>
</tr>
<tr>
<td>Application discovery</td>
<td>Application discovery phase completed successfully</td>
</tr>
<tr>
<td>Application mapping</td>
<td>Application mapping phase beginning</td>
</tr>
<tr>
<td>Application mapping</td>
<td>Application mapping phase completed successfully</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Create 1st gen copy phase beginning</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Skipping unmount because there were no previously mounted copies found for the applications under protection during this cycle.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Attempt number 1 to create a VSS copy of the application.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Starting backup of SQL Server databases.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>VSS application freeze succeeded on host amssqlp1.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Backup of database completed successfully.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>VSS application thaw succeeded on host amssqlp1.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>The SnapVX snapshot for the source device 003B8 on the array is EMC_SYNC_ASPECT1474905607970.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>The SnapVX snapshot for the source device 003B9 on the array is EMC_SYNC_ASPECT1474905607970.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Refreshing the SnapVX replication relationships in storage array.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>The SnapVX snapshot EMC_SYNC_ASPECT1474905607970 for the source device 003B8 on the array is linked in nocopy mode with target device 003BC.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>The SnapVX snapshot EMC_SYNC_ASPECT1474905607970 for the source device 003B9 on the array is linked in nocopy mode with target device 003BD.</td>
</tr>
<tr>
<td>Create 1st gen copy</td>
<td>Create 1st gen copy phase completed successfully</td>
</tr>
<tr>
<td>Unmount previous copy</td>
<td>Skipping unmount because there were no previously mounted copies found for the applications under protection during this cycle.</td>
</tr>
<tr>
<td>Unmount previous copy</td>
<td>Unmount previous copy phase for applications completed successfully</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Mount copy phase beginning</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Beginning mount on mount host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Mounting file systems on mount host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Making replication storage accessible to the mount host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Adding copy device 003BD,003BC in storage group on VMAX array</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Rescan HBA and datastore refresh on ESX</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Mount copy</td>
<td>All the target devices are visible on ESX</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Started to mount copy of datastore</td>
</tr>
<tr>
<td>Mount copy</td>
<td>All the target devices are visible on ESX</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Mounting the VMFS on ESX</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Cluster mount is enabled</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Rescan HBA and datastore refresh on ESX</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Copy of datastore is mounted on host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Beginning hot add of virtual disk on virtual machine</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Successfully added virtual disk on virtual machine</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Mounting file systems in read-write mode on mount host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>VSS volume import and filesystem mount succeeded on host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>SQL metadata file saved</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Saved the VSS backup components document file</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Copy mount completed successfully on mount host</td>
</tr>
<tr>
<td>Mount copy</td>
<td>Mount copy phase completed successfully</td>
</tr>
<tr>
<td>Recover copy</td>
<td>Recover copy phase beginning</td>
</tr>
<tr>
<td>Recover copy</td>
<td>Beginning recovery of databases in mode recovery.</td>
</tr>
<tr>
<td>Recover copy</td>
<td>Recover copy phase completed successfully</td>
</tr>
</tbody>
</table>
TROUBLESHOOTING TIPS

AppSync uses SMI-S provider to manage VMAX storage system and many times failure of an AppSync service plan and other operations related to VMAX arrays are due to SMI-S provider issues. In such cases, it is always recommended to collect log files related to SMI-S provider. Below is a list of log files which need to be collected from SMI-S provider host:

1. Collect all log files:
   1.1 On Windows in `C:\Program Files\EMC\SYMAPI\log` and `C:\Program Files\EMC\ECIM\ECOM\log`
   1.2 On Linux in `/var/symapi/log` and `/opt/emc/ECIM/ECOM/log`

2. Collect all dump files:
   2.1 On Windows in `C:\Program Files\EMC\ECIM\ECOM\Providers`
   2.2 On Linux in `/opt/emc/ECIM/ECOM/bin`

3. Collect the Solutions Enabler `symapi_db.bin` database file:
   3.1 On Windows in `C:\Program Files\EMC\SYMAPI\db`
   3.2 On Linux in `/var/symapi/db`

There are times when enabling debug mode with the SMI-S provider and Solutions Enabler may be required to troubleshoot. Turning the debugging mode on/off is depicted below, and should only be necessary upon request by Dell EMC support.

Steps to turn on SMI-S Provider Debugging

1. Stop ecom
   - On Windows - `C:\Program Files\emc\ECIM\ECOM\bin\sm_service stop ecom.exe`
   - On Linux stop ecom using `kill -9`

2. Stop the Solutions Enabler daemons
   - On Windows - `C:\Program Files\EMC\SYMCLI\bin\stordaemon shutdown all`
   - On Linux - `/opt/emc/usr/symcli/bin/stordaemon shutdown all`

3. Cleanup all files
   - On Windows in `C:\Program Files\EMC\SYMAPI\log` and `C:\Program Files\EMC\ECIM\ECOM\log`
   - On Linux in `/var/symapi/log` and `/opt/emc/ECIM/ECOM/log`

4. Edit the file `oslsporvider.conf` and change the following:
   - On Windows in `C:\Program Files\EMC\ECIM\ECOM\providers`
   - On Linux in `/opt/emc/ECIM/ECOM/providers`
     - Change to debug - `*/com.emc.cmp.ofl.log.Control.severity.id = INFO` to `DEBUG`

5. Start ecom
   - On Windows - `C:\program files\emc\ecim\ecom\bin\sm_service start ecom.exe`
   - On Linux - `/opt/emc/ecim/ecom/bin ./ECOM –d`

6. Wait for ecom to fully start, then verify ecom is fully started by running `- testsmiporvider dv`

7. Reproduce the issue and collect the logs, changing `DEBUG` back to `INFO` to disable debugging, by following the same process of restarting ecom and Solutions Enabler
Steps to turn on Solutions Enabler Debugging

1. Instead of launching ecom as a service on Windows or a background process on Linux, run it from the command line to collect Solutions Enabler traces. To do that, open a command prompt on Windows or Linux.
   - On Windows - `C:\Program Files\emc\ecim\ecom\bin`
   - On Linux - `/opt/emc/ECIM/ECOM/bin`

2. Set the following two environment variables
   - Windows –
     - `set SYMAPI_DEBUG=-1`
     - `set SYMAPI_DEBUG_FILENAME=C:\trace.txt`
   - Linux –
     - `export SYMAPI_DEBUG=-1`
     - `export SYMAPI_DEBUG_FILENAME=/tmp/debug.txt`

3. Re-start ecom following the steps outlined in the previous section

4. Reproduce the issue and perform collection steps

List of AppSync Error and Troubleshooting Steps

1. **Issue:** A copy fails after one of the devices provisioned by AppSync was deleted outside of AppSync
   **Troubleshooting steps:** Never delete devices which are being used by AppSync as targets.

2. **Issue:** Discovery of VMAX systems using the SMI-S Provider hangs or is very slow
   **Troubleshooting steps:** Run discovery outside of AppSync using “TestSmisProvider.exe” to determine if it is also behaving in a similar way. Check if there are arrays which the SMI-S provider is discovering, that are not correctly configured on host, do not have the necessary gatekeepers, or redundant to the SMI-S host. In such case, remove those arrays from automatic discovery using SYMAVOID file as described in Procedure to prevent Automatic Discovery of Arrays section of this whitepaper.

3. **Issue:** Replication fails if the SRDF link is not in a consistent state
   **Troubleshooting steps:** From the “symdev show” cli command, verify that the link is not in the consistent state. Per the AppSync User and Administration Guide, ensure the R1>R2 link state is “Synchronized” for SRDF/S or “Consistent” for SRDF/A.

4. **Issue:** Service Plan is configured with an expiration value of 1 but AppSync is creating two sessions
   **Troubleshooting steps:** AppSync always maintains two sessions minimum, due to the fact that AppSync ensures a copy is fully created before expiring the previous copy. This method is considered an N+1 copy count, and cannot be changed.

5. **Issue:** Copy creation fails with strange SMI-S provider errors
   **Troubleshooting steps:** Validate the SMI-S version and Enginuity/microcode level against the latest ESM - https://elabnavigator.emc.com/eln/modernHomeDataProtection

6. **Issue:** Progress appears to be HUNG, repeating the same percentage value
   **Troubleshooting steps:** Ensure the AppSync UI session is not timed out, and ensure the virtual provisioned storage pool is configured and not full.

7. **Issue:** AppSync does not delete devices which it has provisioned
   **Troubleshooting steps:** Do not delete devices provisioned by AppSync until the AppSync server is de-configured. Once the AppSync server is de-configured and uninstalled, query the VMAX to find all devices per the Device Management On The Backend VMAX section, and remove these devices. AppSync uses the naming convention while provisioning devices to make this process easy.
CONCLUSION
In conclusion, this whitepaper explains key information and concepts when protecting an application residing on VMAX All Flash storage using AppSync. It discusses the inner operations of AppSync software while protecting applications using SnapVX Snap and Clone technologies, along with deployment and troubleshooting tips.

REFERENCES
For more information on AppSync, and how to manage VMAX environments, consider the following sources:

Dell EMC AppSync Installation and Configuration Guide
Dell EMC AppSync Performance and Scalability Guidelines
Dell EMC AppSync Security Configuration Guide
Dell EMC AppSync Simple Support Matrix
Dell EMC AppSync User and Administration Guide
THE VMAX ALL FLASH STORAGE FAMILY White Paper

LIST OF FIGURES
Figure 1 - AppSync UI Selection .............................................................................................................. 5
Figure 2 - Add VMAX ............................................................................................................................... 9
Figure 3 - SMI-S Credentials .................................................................................................................. 10
Figure 4 - Select VMAX .......................................................................................................................... 10
Figure 5 - Select Storage Group ............................................................................................................. 11
Figure 6 - VMAX Auto Device Discovery .............................................................................................. 11
Figure 7 - Element Name ........................................................................................................................ 13
Figure 8 - Storage Device Warning ........................................................................................................ 13
Figure 9 - Storage Details ....................................................................................................................... 14
Figure 10 - Storage Rediscover ............................................................................................................ 14
Figure 11 - Manage Copy Storage .......................................................................................................... 15
Figure 12 - Removing a Storage Group ................................................................................................ 15
Figure 13 - AppSync Provisioned Name ............................................................................................... 16
Figure 14 - Number of Devices ............................................................................................................. 18
Figure 15 - User Provisioned Devices .................................................................................................. 19
Figure 16 - AppSync Provisioned Devices ........................................................................................... 19
Figure 17 - Removing Device from AppSync ....................................................................................... 20
Figure 18 - Error Removing a Device .................................................................................................... 20
Figure 19 - Application Copy Info ........................................................................................................ 20
Figure 20 - General Service Plan Phases ............................................................................................ 23
Figure 21 - Storage Preference ............................................................................................................. 24
Figure 22 - Mounting Wizard ................................................................................................................. 27
Figure 23 - Unmounting Copies ............................................................................................................ 28