Dell EMC AppSync 4.x with PowerMax, VMAX All Flash, and VMAX3

Abstract

This document provides best-practices guidelines for managing Dell EMC™ PowerMax™, VMAX™ All Flash, and VMAX3™ storage systems for copy management with Dell EMC AppSync™. AppSync 4.0 and later versions use the Unisphere™ for PowerMax REST API with these systems.

June 2020

H18341

Revisions

Date	Description
June 2020	Initial release

Acknowledgments

DELLTechnologies

Table of contents

DЗLLTechnologies

Executive summary

This document provides best practices for integrating Dell EMC™ AppSync™ versions 4.0 and later with Dell EMC PowerMax™, VMAX™ All Flash, and VMAX3™ storage systems. It includes many environmental caveats that should be considered during implementation.

Audience

This white paper is intended for Dell EMC customers who plan to use AppSync for copy management. It is also intended for Dell EMC internal field personnel and partners who assist customers with AppSync deployment.

D⊘LL Technologies

1 Introduction

Dell EMC AppSync is software that enables integrated Copy Data Management (iCDM) with Dell EMC primary storage systems. It simplifies and automates the process of generating copies of production data, abstracting the underlying storage and replication technologies. AppSync discovers applications, understands their layout structure, and maps them to the underlying storage device. It fully orchestrates all activities required, including copy creation and validation, mounting, recovering, and bringing the application online. Application owners now have the means to satisfy their own copy management needs. AppSync provides an end-to-end copy management workflow solution.

1.1 Using this document

The best-practices guidelines in this document result from the combined efforts of AppSync technical marketing, engineering, and development groups. This information is supplemental to the primary AppSync documentation on Dell Support. These documents include the *AppSync User and Administration Guide*, the *AppSync Installation and Configuration Guide*, the *AppSync Security and Configuration Guide*, and the *AppSync Release Notes*.
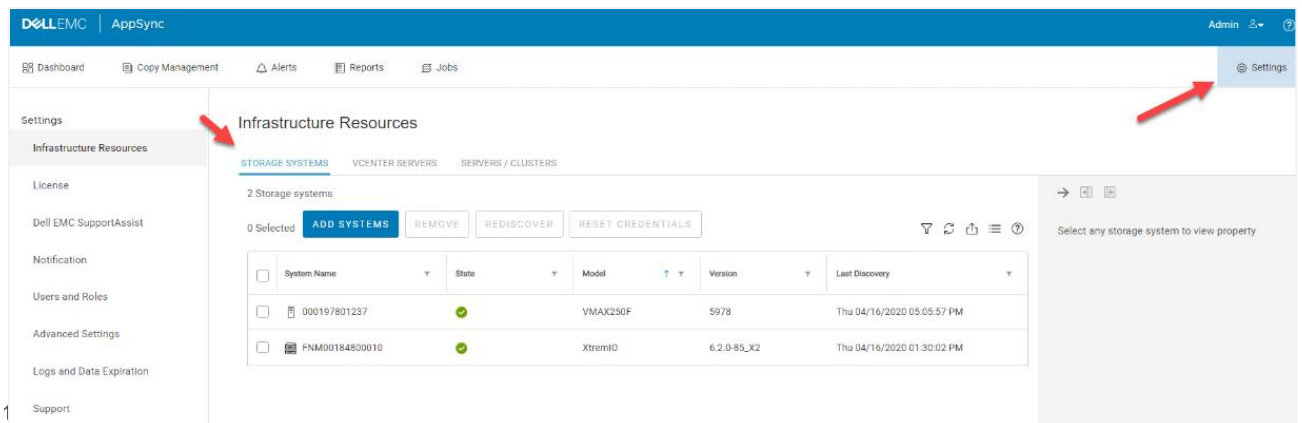
Figure 1   AppSync console UI

1.2 Terminology

The following terms are used in this document:

Expire: A process flow of removing copies from within the AppSync UI and on the array, such as unlinking and expiring copies.

Mount host: The host where the copies are mounted. This can be an alternate host or the same host as the source.

Mount point: A location used by the mount operation that uses an existing mounted file system to attach, as a directory tree, the copied volume. The mount point appears as a new directory to an existing file system structure. This is the default AppSync mount location.

Object: A database, filesystem, application, or VMware® datastore that AppSync manages. Objects are subscribed to service plans or repurposed.

Recover: The process of extending the copy and mount operation by starting the application when it is mounted. Example: Bringing a copy of a Microsoft® SQL Server® or Oracle® database online on a mount host.

Repurposing workflow: A copy-management workflow process, similar to a service plan, that provides a multigeneration copy process.

Restore: The process of overwriting a source volume with the contents of a previously created copy.

Service plan: A copy-management workflow process for protecting applications.

Subscribe: Associating an object with a service plan.

Unsubscribe: Disassociating an object from a service plan.

D&LL Technologies

2 Storage considerations

AppSync supports creating and managing copies of application data on PowerMax and similar arrays using SnapVX replication technology. AppSync also supports remote copy management for block-based storage with SRDF, and replicating file-based (eNAS) environments using File Replicator.

AppSync supports SnapVX using the default storage resource pool.

- **AppSync does not support Multiple SRPs.**
- AppSync can create both local and remote copies (Gold Service Plan) while using SRDF/S.
- SRDF/A and Metro are limited to **either** local **or** remote copies.
- AppSync is not able to create remote SRDF/A copies for Microsoft applications (local copies only).
- AppSync does not support RecoverPoint with PowerMax.
- AppSync does not support restoring remote copies over SRDF.
- Only the **local repurposing** workflow is supported for SRDF/Metro. AppSync provides the option to select the leg to create the copy on in the local repurposing workflow. Other SRDF/Metro functionality is expected in future releases. Check the AppSync support matrix for the latest supported use cases.

2.1 Advanced features

2.1.1 U4P REST API

A minimum version of Unisphere for PowerMax (U4P) is required. Review the latest AppSync Support Matrix for details. **SMI-S is no longer supported for VMAX3 and newer arrays on AppSync 4.0+**. **VMAX2** arrays are still supported with SMI-S.

2.1.2 SRDF/Metro

AppSync 4.0+ supports SRDF/Metro using the U4P REST API protocol. The following points outline AppSync support and limitations. Other SRDF/Metro support is expected in future releases as mentioned above. Check the support matrix for the latest information.

- Each leg of an SRDF/Metro environment can be selected individually but not simultaneously; AppSync is not able to create a copy on both legs of a metro environment at the same time.
- Repurposing of workflows by AppSync is supported; **service plan workflows are not supported.**
- Copies are mounted as non-metro devices.
- Restores are supported for the local copies only.
- **VMware datastores and Microsoft Exchange environments are not supported.**
- Due to the nature of repurposing workflows, only one database application can be managed at any one time; however, multiple file systems are supported.

2.1.3 Storage-group-level snapshots

AppSync 4.0+ supports storage group (SG) level snapshots. SG-level snapshots are taken whenever applications are mapped to unique storage groups. If an application is not mapped to a unique storage group, volume level snapshots will be taken. This is reported in the status logging as the service plan runs.

2.1.4 Storage group specification per service plan

AppSync 4.0+ supports configuring a specific storage group for AppSync to use for target devices. Previously, storage groups were global. With the AppSync 4.0 release, each service plan can be configured to use its own storage group, providing a more granular and controlled use of target devices.

2.1.5 AppSync Gold service plan

When using existing SRDF/S replication environments, Gold service plans can be configured with the storage arrays. The Gold service plan enables creating simultaneous local (R1) and remote (R2) copies, quiescing the application once. This provides the same point-in-time image for both local and remote copies. Review the *AppSync User and Administration Guide* for more details including the limitations and restrictions when working with **Gold** level service plans.

- Gold service plans require both SRDF legs to be registered with the same Unisphere for PowerMax (REST API) server.
- Gold service plans are not supported when using the embedded U4P REST server. It is a best practice to not use the embedded U4P server for upgrade and performance reasons.

2.1.6 VPLEX

Volumes or devices provisioned from the arrays are supported behind VPLEX RAID 0, RAID 1, and Metro Distributed environments. The preferred cluster for distributed volumes and the preferred arrays for RAID-1 volumes for each service plan and repurposing workflow must be configured according to the *AppSync User and Administration Guide.* Review this guide for more details, including limitations and restrictions when working with these arrays and VPLEX.

2.1.7 eNAS

AppSync offers support for VMAX eNAS (embedded network attached storage). VMAX eNAS offers consolidated file storage, similar to the Dell EMC VNXe™ array. For more information, see the eNAS documentation.

eNAS and eNAS file replicator are also supported. All standard applications are supported, such as Oracle® on Linux® and AIX, Microsoft® Exchange, Microsoft SQL Server®, Linux and AIX file systems, VMware® datastores, and others. See the AppSync Simple Support Matrix for up-to-date support details.

2.1.8 Online device expansion

AppSync fully supports the online device expansion process. However, any target device that is preallocated or created must be expanded manually for AppSync to use or reuse it as a target device—source and target devices must match.

D≪LL Technologies

3 Array discovery and configuration

PowerMax and similar arrays are discovered with AppSync 4.0+ using U4P and the REST API. As part of the discovery process, AppSync obtains a list of all arrays managed by the Unisphere for PowerMax (U4P) server, along with detailed information such as the microcode version, model number, and the last discovery time. A **Rediscover** should be performed when changes are made to the array, such as adding additional disks or updating microcode.

To discover a new storage array or arrays, in the interface click **Settings** (Figure 1) and click the **Add Systems** button (Figure 2) . Under the **Infrastructure Resources** section, **Storage Systems** are selected by default. Select **PowerMax/VMAX3** (Figure 3) and click **Next**. Enter the credentials (Figure 4) for Unisphere for PowerMax (U4P) and click **Next**. Select the array or arrays (Figure 5) to discover and click **Next**. Select the Storage Group, SRP, or both (Figure 6) to use and click **Next**. Validate all selected options on the last summary screen and click **Finish** to complete the discovery.
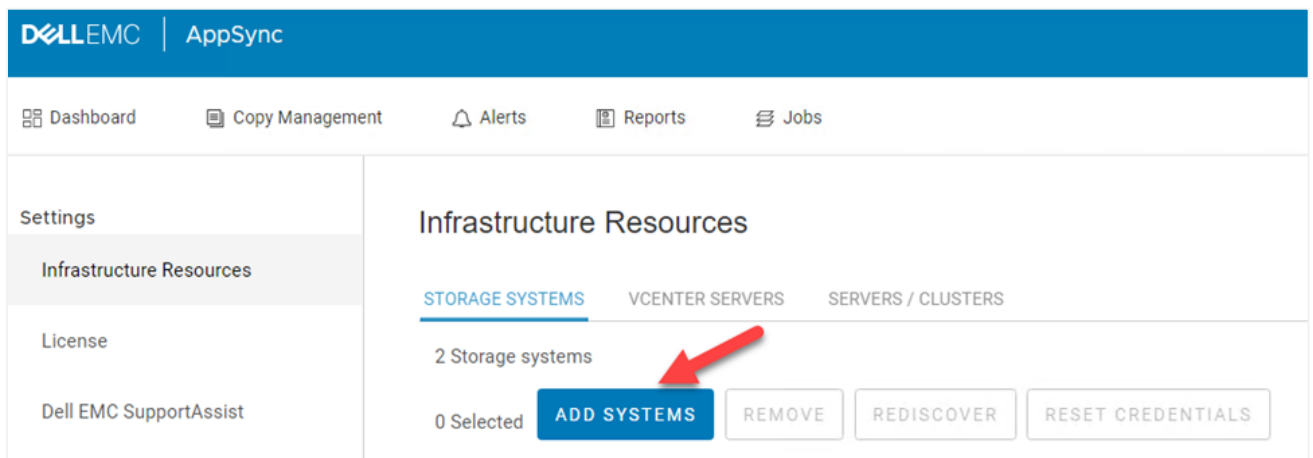
Figure 2   Add systems
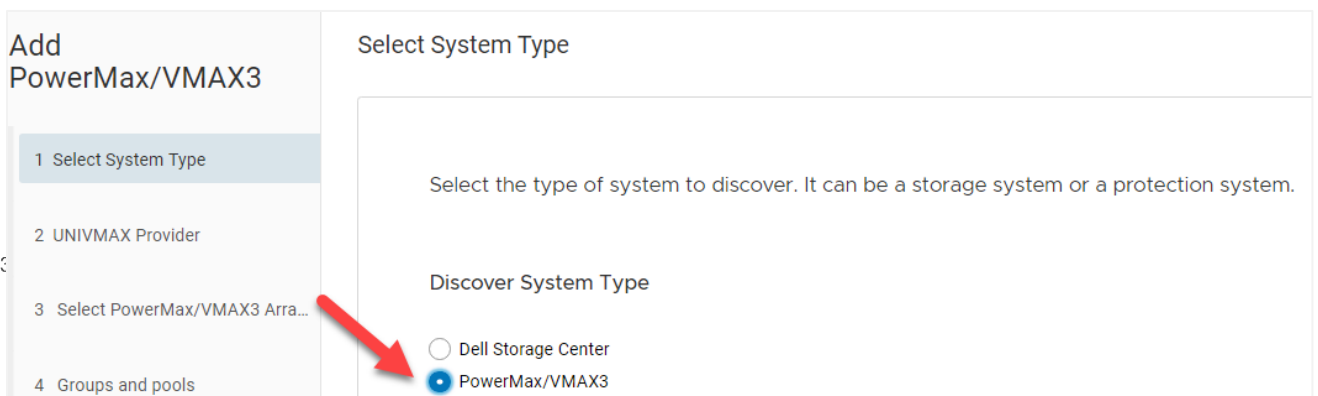
Figure 3   Select PowerMax/VMAX3

U4P credentials

Figure 4

Figure 5

Select storage array or arrays

Figure 6

Configure storage groups/SRP

3.1　Modifying credentials

If the Unisphere for PowerMax > U4P credentials are modified by the administrator, they must also be changed in AppSync. Go to the **Storage Systems** menu, select the array, select the U4P host, and click **Edit** to change the credentials. See Figure 7.

Figure 7　　　　　　　Modify U4P credentials

3.2　Provider reference

As the preferred provider, AppSync uses the U4P management server that was used to initially discover the array or arrays. To change the preferred order with multiple U4P servers, in the AppSync UI select the server, and click **Set Preferred**.

3.3　Preventing automatic display of arrays

It is best practice to limit each U4P host to one local host and its corresponding remote array. However, one U4P server may manage up to five hosts, based on performance considerations. The performance of the U4P server is critical to AppSync performance. The discovery of arrays on a U4P host, which are not used by AppSync, may impact the performance of AppSync jobs. If the U4P server discovers arrays which do not need to be managed by other products, including AppSync, follow the U4P documentation for creating a **symavoid** file to alleviate the discovery of those other arrays.

3.4　Removing arrays from AppSync

No arrays can be removed from AppSync until all copies are expired. If storage groups are configured, they too must be removed from AppSync. To remove arrays, go to **Settings** > **Infrastructure Resources** > **Storage Systems**, check the array, and click **Remove**. If anything remains configured, an error is displayed and prevents the array from being removed.

If an array is removed from the U4P server, before being removed from AppSync, AppSync removes the association between the two. If there are no array copies or storage groups created by AppSync, the array itself is also removed upon rediscovery.

4 Storage management

AppSync uses 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 snap. For SnapVX clone, target devices are required during the copy phase since SnapVX linking occurs during the copy phase when using SnapVX copy 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 first-generation snap and clone copies, but not for the second-generation snapshot copies. The second-generation snapshot is linked during the mount phase, like when using service plans. See the section 7.1 for more details.

The following subsections detail the AppSync storage-configuration options that support target-link operations.

4.1 User-configured storage groups

Storage administrators can use an optional storage group or groups for target copy devices. Using a dedicated storage group, which contains preconfigured target devices for **link** operations, AppSync is restricted to using only those devices, when configured. These storage groups can be configured on a per-service-plan basis with AppSync 4.0+. AppSync relies on there being enough storage devices available in this particular storage group; if there are not enough devices, job-linking operations fail if SRP is not configured. If an SRP is configured in addition to a storage group, AppSync creates devices as needed. The following points outline the caveats.

- If one or more storage groups are not defined, AppSync uses the default SRP to create **target** devices to link with SnapVX copies.
- Configuring a storage groups manually prevents AppSync from provisioning target devices automatically if an SRP is not also configured. Target devices must be created in the storage groups beforehand.
- Devices are created from the SRP (if configured) for storage groups configured if there are not enough available devices created ahead of time in the storage groups.
- Do not configure the user storage groups with a masking view or an SLO. AppSync cannot use a storage group with a masking view, and if an SLO is configured, a warning is shown. Not configuring SLOs is the recommendation to improve performance during mount operations.

4.1.1 Configuring storage groups for copy target devices

Create one or more storage groups without host connectivity (not configured with a masking view). Note the following rules when provisioning new target devices for copy processing:

- Ensure the target copy device is the same size configuration as the source device.
- All devices in the configured storage groups are used as copy devices, so never add production volumes into AppSync assigned storage groups 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 groups across multiple AppSync servers.
- Devices created by AppSync, such as devices that are created before storage groups are configured, are not automatically added to a configured storage group. Devices that are created by AppSync 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 the AppSync host name. This is to identify the AppSync copy devices in the array and proclaims these devices for AppSync use. AppSync updates the device names with **AppSync - <Hostname>,** as shown in Figure 8**.**
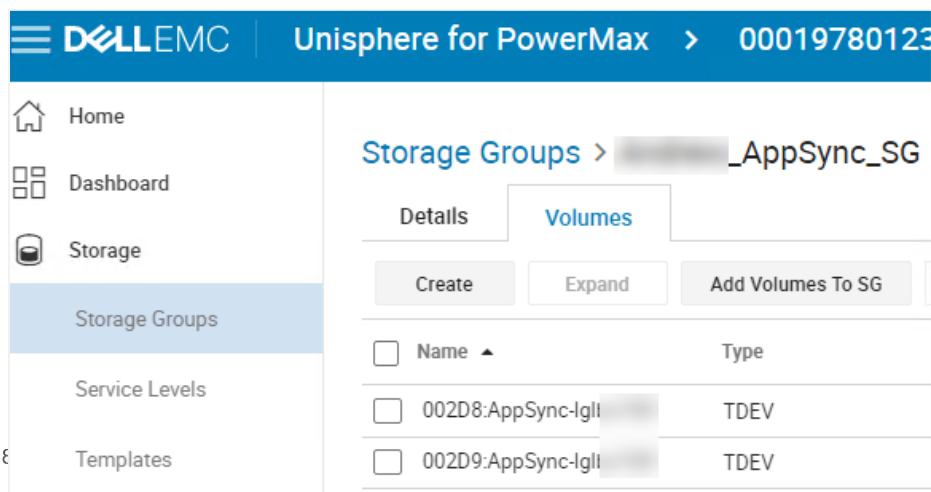
Figure 8   Volume name

AppSync only discovers storage groups which are not part of any masking view. This is designed to protect devices presented to hosts, such as with production volumes. To configure a storage group for an AppSync target device selection, enable it by clicking the checkbox as seen in Figure 5. 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 9. The data on the devices is overwritten by this process.
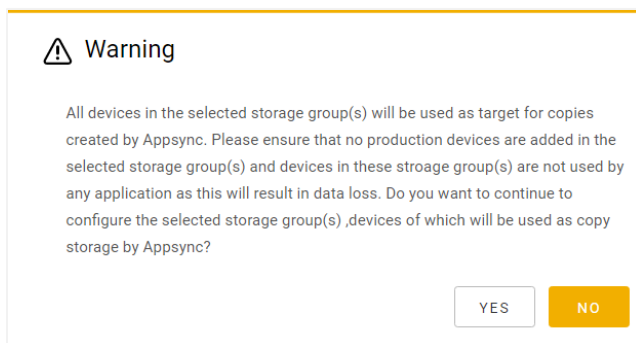
Storage device warning

Review the storage details within AppSync. Under **Storage Systems**, click the array as seen in Figure 10. When multiple storage groups are added, the **Number of devices** is the sum of all storage groups.
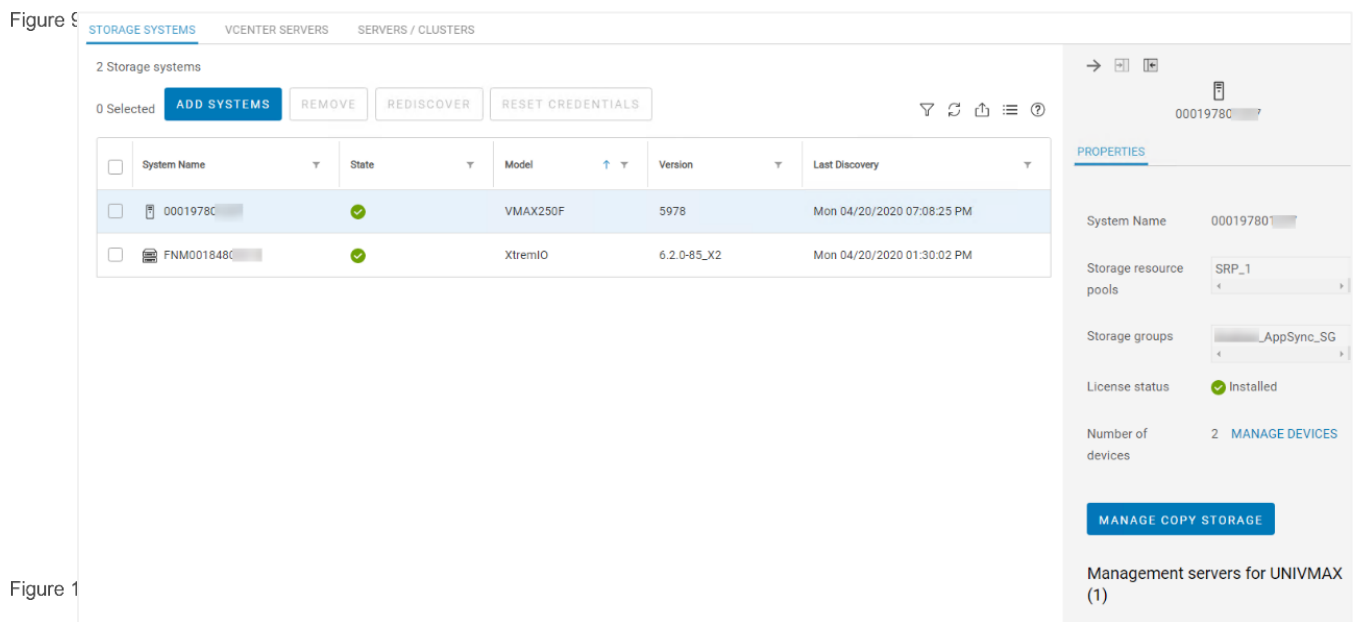
Figure 9

Figure 10

Storage details

4.1.2 Modifying storage groups

Once a storage group is modified on the array (possibly with U4P or CLI), 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 storage group, go to **Storage Systems**, click the array, and click **Rediscover** as seen in Figure 1. 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.
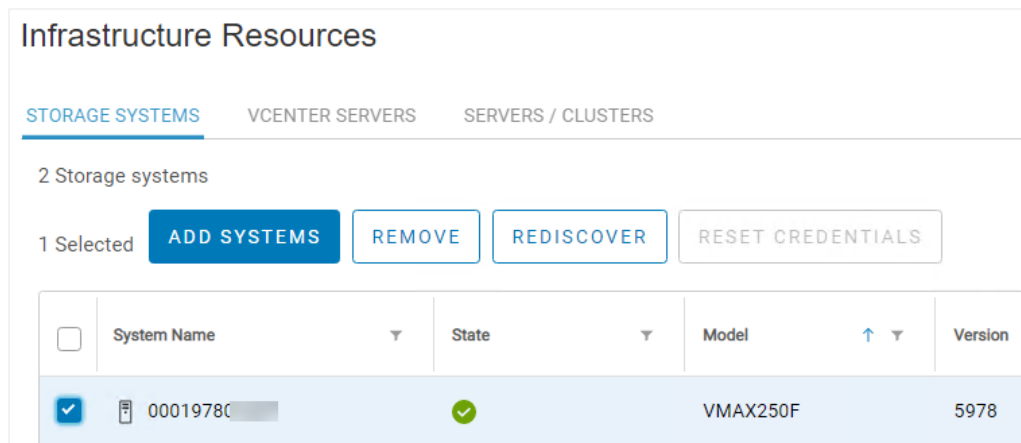
Storage rediscover

To configure or unconfigure storage groups, click the **Manage Copy Storage** button as shown in Figure 10. This displays the **Configure target storage** details as shown in Figure 12.

Figure 11
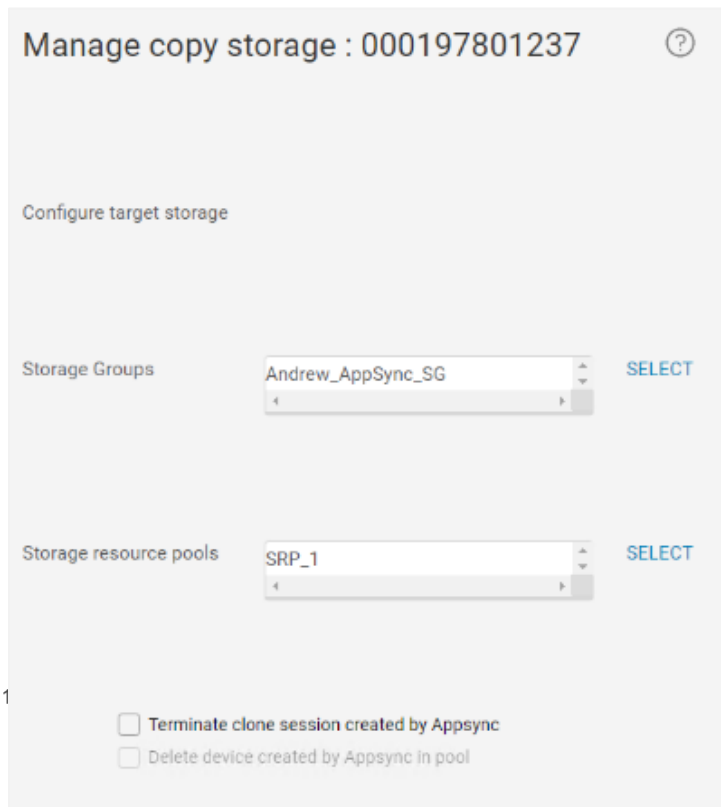
Figure 1

Configure target storage

Once the **Manage Copy Storage** dialog box appears, click the select button next to storage groups, check the storage group or groups on the right that you want to remove, and click the left arrow button. This prevents AppSync from assigning target storage from it, as seen in Figure 13. You can also add storage groups by selecting them from the left pane and clicking the right arrow button.
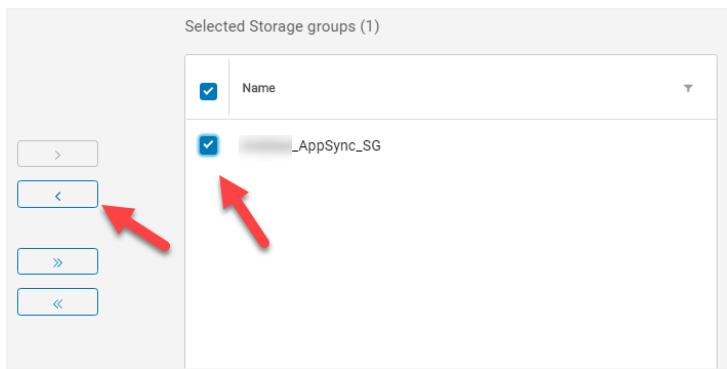
Removing a storage group

4.2 AppSync provisioned devices

Figure 16 If storage groups are not configured, AppSync has the ability to create and link devices dynamically. This means AppSync creates the devices as needed during linking operations from the default SRP.

AppSync uses any storage resource pool (SRP) you configure, but using multiple SRPs at once is not supported in AppSync.

Devices provisioned by AppSync are named **Device#:AppSync-{AppSync_Server_Name}.** An example is shown in Figure 14. This can be used to easily identify all devices which have been provisioned by AppSync.
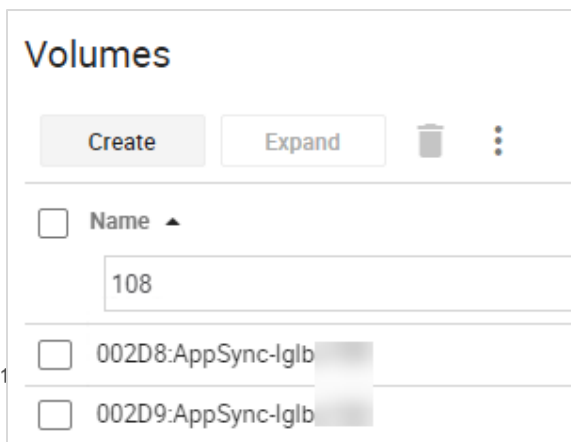
AppSync provisioned name

4.2.1 AppSync internal storage group

As of AppSync 3.7, AppSync keeps all its provisioned devices in an internal storage group on the array, 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 a device from this internal storage group created by AppSync because it is managed by AppSync. The internal storage group is created without an SLO to enhance the performance during mount operations, and we do not recommend applying one.

Note: It is best practice to manage an array with one AppSync server. Multiple AppSync servers managing the same VMAX array is not recommended. Contact Dell Support if you have questions regarding this best practice.

4.3 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.

D¢LL Technologies

5 Advanced copy device management

AppSync allows viewing and managing the copy devices that are associated with applications, for better device management. The wizard under **Manage Devices**, provides insight into the target devices. Click **Manage Devices** to launch the Manage Devices menu. See Figure 15 below.
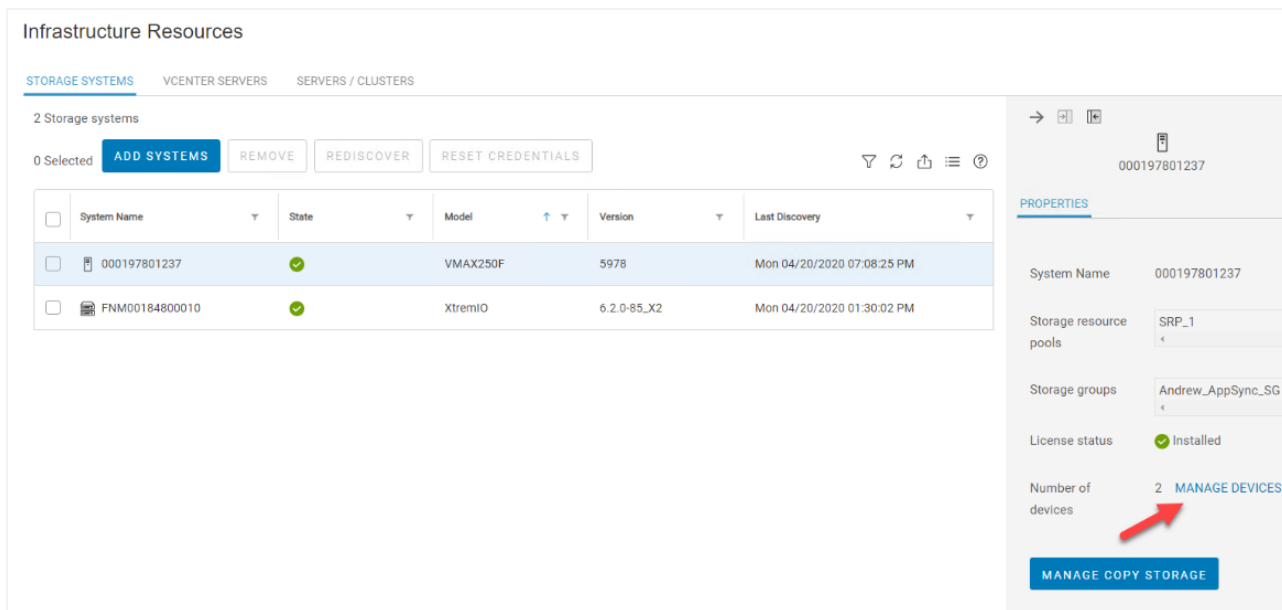
Figure 15   Manage devices

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 16 and Figure 17.
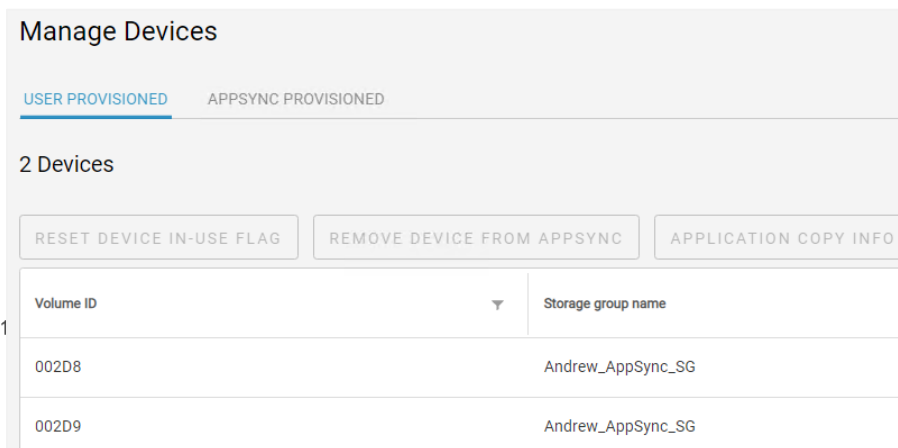
Figure 1

User provisioned devices

AppSync provisioned devices

Figure 17

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 it would be a preferred device to be used once again by AppSync, 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 or 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 PowerMax, once removed from AppSync management.

To review the devices that AppSync manages, go to **Settings** > **Infrastructure Resources** > **Storage Systems**, select the array line, and click **Manage Devices**.

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 or function are detailed below. See the following screenshots for visual representations.

Note: 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 managed devices, before using the devices elsewhere.

5.1   Reset device In-Use flag

This operation resets the device's in-use flag within AppSync. AppSync manipulates the **in-use** flag for the copy device. If it is not set due to server shutdown, you 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.

5.2   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 18.

⚠Remove device from AppSync

Removing the device 002D8 from AppSync will not delete the device from Array, but will make it unavailable to AppSync to be used as a target device for further protections. Click Yes to remove the device from AppSync.

OK   CANCEL

Removing device from AppSync
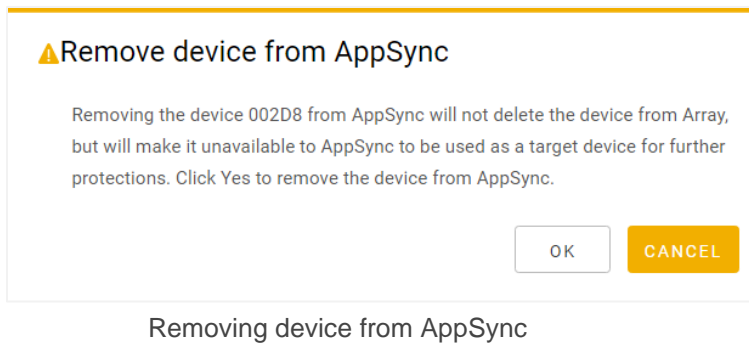
Figure 18

6 Delete device in array

This operation is allowed only for AppSync provisioned devices. This operation deletes the AppSync provisioned device from the array and from the AppSync inventory. An error message will appear if attempting to remove a device while it is being used for replication. The copy would need to be expired prior to deleting the device. See Figure 19.
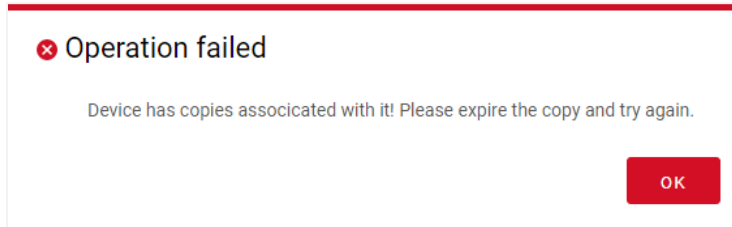
Error removing a device

6.1 Application copy info

Figure 19

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 20.
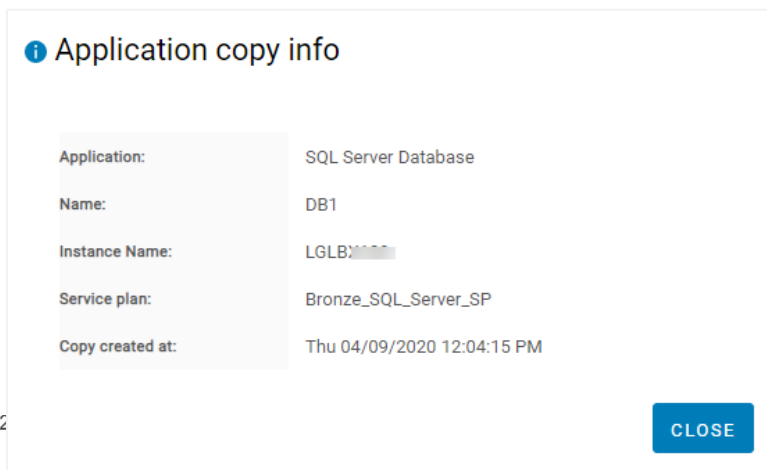
Figure 2

Application copy info

7 SnapVX configuration details

The arrays mentioned in this document use SnapVX technology for the copy management process in AppSync. Creating point-in-time copies uses the array SRPs to maintain the changed tracks, which requires no configuration for AppSync to use other than adding the array to AppSync. AppSync uses the SRP that is configured by the end user. **AppSync supports only using one SRP per array**. For more details regarding the way SnapVX uses the SRP, see the document Dell EMC PowerMax and VMAX All Flash: TimeFinder SNAPVX Local Replication.

SnapVX does not require like-for-like target devices and preconfigured storage pools as in the past with previous technologies. AppSync can use preconfigured devices added to preconfigured storage groups if required. These devices are only used during the mount phase, or during the first-generation repurposing workflow copy phase for snapshot operations.

AppSync provides support for both SnapVX copy and no copy modes. **Copy** mode is similar to the way VMAX2 was used to create TimeFinder Clones, and the **no copy** mode is similar to TimeFinder Snaps.

When thinking about how TimeFinder works, there is a concept of **create** and **activate**, where create pairs the device with a preconfigured target device, and activate creates the point-in-time copy and also readies the device to be presented to a host. SnapVX does not follow the 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 only during a mount operation for snapshots. This is discussed in more detail in section 7.1 and section 9.1.

7.1 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 it is mounted. If storage groups are configured with preconfigured and available devices, AppSync uses those devices, otherwise, if storage groups are not used, 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 by default, you can enable the unlink option during unmount in the service plan options for SnapVX snapshots, not clones. SnapVX snapshot target devices are unlinked only when copies are expired from within AppSync by default. 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 differs from service plan workflows. Repurposing the first-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 first-generation copies snap and clone both. If storage groups are used, and no target device is available, the repurposing job fails. Refreshing **the** first-generation copy creates a new snapshot and relink to the same target device. Mounting does not perform the linking as would be the case when working with service plans. Unmounting the device does not unlink the device by default like mentioned above, but expiring the device does, like the service plan. Service plans and repurposing workflows are described in more detail in the *AppSync User and Administration Guide*.

The second-generation copy is created from the first-generation copy, though it differs in behavior. The second-generation SnapVX snap copy does not link to a target during the copy phase, as the first-generation copy does. The second-generation SnapVX clone copy links to a target during the copy phase, which is the same as first-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 creates a new snapshot and relinks only if the snapshot had already been linked, such as if it had been mounted. Expiring the copy unlinks the device and deletes the snapshot.

Workflow comparisons

Table 1

AppSync workflows	Copy phase	Mount phase	Unmount phase	Refresh phase	Expire
Service plans	**Snap** Targetless	Linked Requires targets	Does not unlink by default (can change to unlink for Snap)	Relinks	Unlinks (only for the SnapVXSnap that it unlinks)
	Clone - linked Requires targets	No changes Already linked			For SnapVXClone, it is **not** unlinked and deleted in array. The link is kept in array for relinking. When creating the next clone, it relinks to the same target device and creates a new SnapVX snapshot. The previous SnapVX snapshot is then deleted.
Repurposing	**First-generation snap/clone** Linked - requires targets	No changes Already linked	Does not unlink	Relinks	Unlinks
	Second-generation snap Targetless	Linked Requires targets			

D‍ELL Technologies

AppSync workflows	Copy phase	Mount phase	Unmount phase	Refresh phase	Expire
	Second-generation clone **Note:** First-generation must also be set to clone**)** Linked - requires targets	No changes Already linked			

7.1.1   SnapVX linking FAQ

The following list includes frequently asked questions (FAQs) regarding SnapVX and linking:

Q: When AppSync mounts copies for PowerMax or similar arrays, it links them to target devices. Does it unlink the target device when unmounting?

A: No, it does not unlink when unmounting by default, only when expiring. This can be modified in the service plan options (**Mount** section > **Storage Settings**).

Q: Does it not make more sense to have AppSync unlink when unmounting?

A: This is a feature of SnapVX which AppSync uses 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 it behaves more efficiently. This can be changed as mentioned above if needed. One more reason is the link is unlinked in unmount phase is that for restore from modified copy. Once copy mounted to the host, all the changes are in link devices. If wanting to restore from modified copy, select the option to restore from modified copy. The link is not unlinked to support restore from modified copy.

Q: How is the repurposing relink feature used?

A: The relink use case with the repurposing workflow provides an incremental refresh process since the device is not unlinked until it has expired. The refresh process is only incremental if the device remains linked, so the first-generation refresh always links to a device to allow quicker refreshing and also allows it to be the source for multiple second-generation copies. Relinking is used in SnapVX clone, when expiring the SnapVX clone in AppSync would remove the copy in AppSync, but the SnapVX is not unlinked and expired in array. In the next clone-copy creation, AppSync relinks with same target device for the source volume SnapVX, and it reduces the linking time in SnapVX Clone. Once te relink completes, AppSync cleans up the previous SnapVX in the array.

Q: Can AppSync use the same targets for the next mount operation?

A: Yes, when refreshing, AppSync performs an unlink and relink internally, which is transparent to the end user.

7.2   SnapVX relinking

AppSync supports VMAX SnapVX relinking when using 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 same target devices.

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

In this example, 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 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 500 GB and copy count =1, 1 TB would be consumed). When copy mode is active (full clone operations), AppSync takes 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. Relinking is now used 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).

8 Protecting applications using AppSync service plans

AppSync is an application-centric copy management solution that is designed to protect 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:

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

Applications can be subscribed to different service plans based on their required SLAs or recovery point objectives (RPOs). 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. Some of the different phases are depicted in Figure 21.
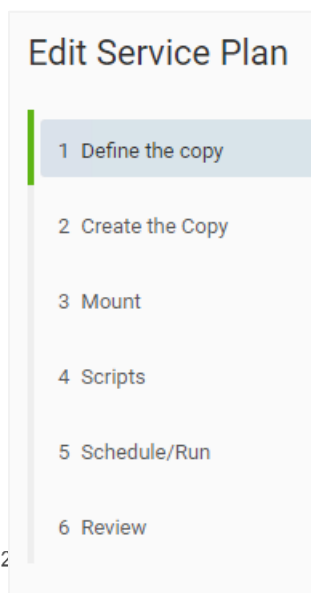
Figure 2

General service plan phases

After registering and configuring PowerMax or similar storage, and 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 storage systems discussed in this document. **Snapshot** is the default replication technology, which can be changed. For instance, if a full copy/clone is needed, change the **Copy Priority** to **Clone**, either by moving it to the top of the list, or by clearing the other technologies. Clone has been moved to the top of the priority list and the other options have been cleared in Figure 22**.** See the *AppSync User and Administration Guide* for more details about service plan settings.
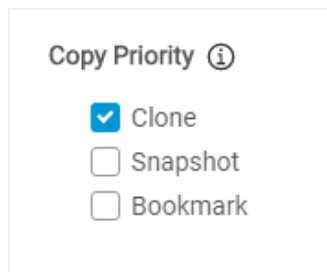
Copy priority

8.1 Application discovery phase

Figure 22
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.

8.2 Application-mapping phase

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, that is LUNs. AppSync gathers all the storage system device information pertaining to these LUNs. In certain circumstances the mapping phase can be disabled but a support case should be opened to discuss the details and any repercussions. If the underlying LUNs are on a PowerMax or similar array, the following operations are performed by AppSync:

- AppSync uses the U4P server to map the world wide names (WWNs) of the source LUNs to a corresponding array to obtain their details. If a virtualization layer exists, such as LPARs, VMware, VPLEX, or other layers, AppSync inventories these objects as well. These details include the type of disk, RAID type, or other details. If there are any changes to the device on the array, AppSync is updated of those changes, such as if the size is changed.
- U4P servers should be kept online, otherwise delays may be experienced. If a U4P server is taken down for maintenance, for example, it should be removed from within AppSync, or the preferred list should be modified. AppSync cannot communicate with the arrays if all U4P servers are down.
- For silver and gold service plans, AppSync also tries to find the remote device, such as R2, after getting the R1 details from the U4P server. For silver plans, or remote repurposing workflows, it is preferred to use an U4P server local to that remote array. For gold service plans, it is a requirement to use a single U4P host which has gatekeepers presented from both arrays. The local U4P server is preferred.

8.2.1 Affinitization rules

Once the mapping phase completes, AppSync **affintizes** the applications based on certain rules allowing groups of applications to be replicated together, such as when multiple applications are subscribed to the same service plan. Affinitization rules are application-specific and storage-specific. For example, each application has rules that are specific to that application (such as SQL, Oracle, VMware) and rules that are specific to a storage system on which the application data resides.

In the case where the application data resides on a PowerMax storage system, the following affintization rules apply:

- **Affinitize by PowerMax array ID**: This rule is based on the PowerMax ID (serial number). If two databases or datastores are on the same host but are on two different PowerMax systems, AppSync separates them into different 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, AppSync breaks the copy into different PiTs.

8.3 Create copy phase

The copy phase 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 as one affinitization set. For each set of applications, one create copy phase is performed 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 performed during a single service plan execution cycle. Details pertaining to applications on VMAX are as follows:

- AppSync supports SnapVX Snap (no copy) and SnapVX Clone (copy) for PowerMax and similar arrays as the supported copy technology.
- By default, all service plans have **snapshot** as the preferred storage technology type. If clones are desired, change the storage order preference, or clear the other technologies, as seen in Figure 22.
- 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 if a clone copy is rotated (expired from AppSync and new clone created at differential point-in-time).
- SnapVX relinking is used so when creating clones, the linking occurs during this phase. See section 7.1
- When considering creating remote copies, such as taking snaps and clones from the R2 note the following:

  – AppSync does not manage the SRDF sessions, it uses the preestablished configuration.
  – AppSync only supports SRDF/S and SRDF/A. See 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. For example, 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+ 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: See the SRDF product guide for more details.
    > All the devices which constitute a single application should belong to the same RA group.

8.3.1 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. AppSync does not wait for PowerMax clones to sync by default, this can be changed in the Create the Copy > Storage Preferences section of the service plan. This is because it can take a longer time to complete (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 does not need to wait, as it is only an update of changed tracks.

8.3.2 Expiring copies

Expiring copies with AppSync, on a PowerMax or similar 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 reuses 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**.

8.3.3 Mount copy phase

AppSync supports dynamic mounting of application copies created on PowerMax or similar arrays for all AppSync supported platform types, such as Linux, AIX, and Windows. AppSync does not support static mounting of array copies except through using RecoverPoint. AppSync relies on the arrays auto provisioning capability to provision devices to mount hosts. AppSync requires the mount host to be zoned to the 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 array copies, AppSync first finds the mount hosts FC/iSCSI adapter information and then interacts with the array through the U4P provider to find an appropriate storage group. Once AppSync finds the appropriate storage group, the target copy devices are added as shown in Figure 23**.**
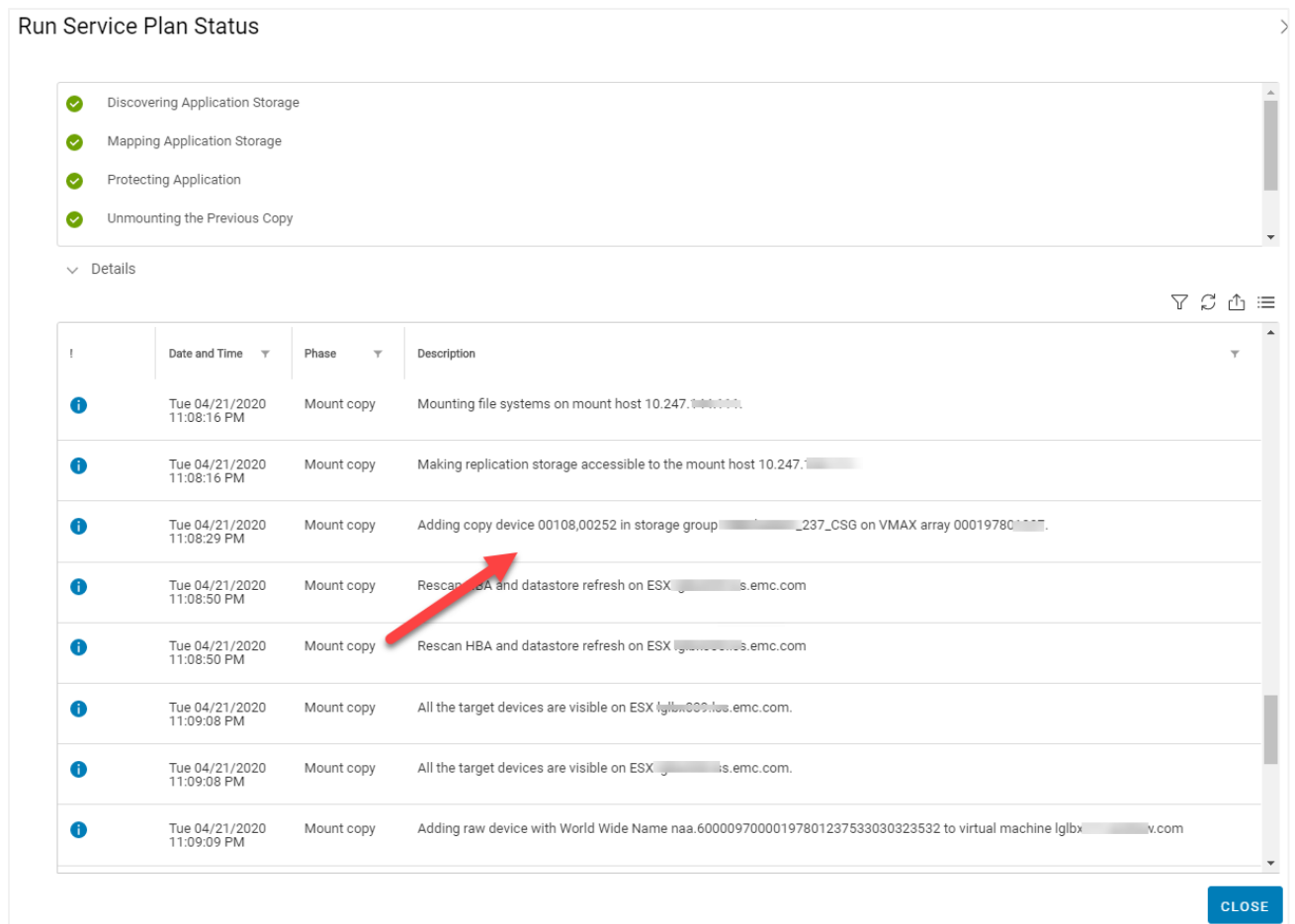
Figure 23   Mounting wizard

8.3.4   Mount host storage group rules

- For virtual machines, AppSync performs mounts by masking the copies to the ESXi host, and then adds the devices to the virtual machine.
- In case the host is connected to a PowerMax or similar array by multiple masking views, and the host is not an ESXi 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 does not 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 (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 ESXi host in a cluster, AppSync tries to find a masking view which has connectivity to the maximum number of nodes of the ESXi 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 ESXi 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 (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 **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 24.
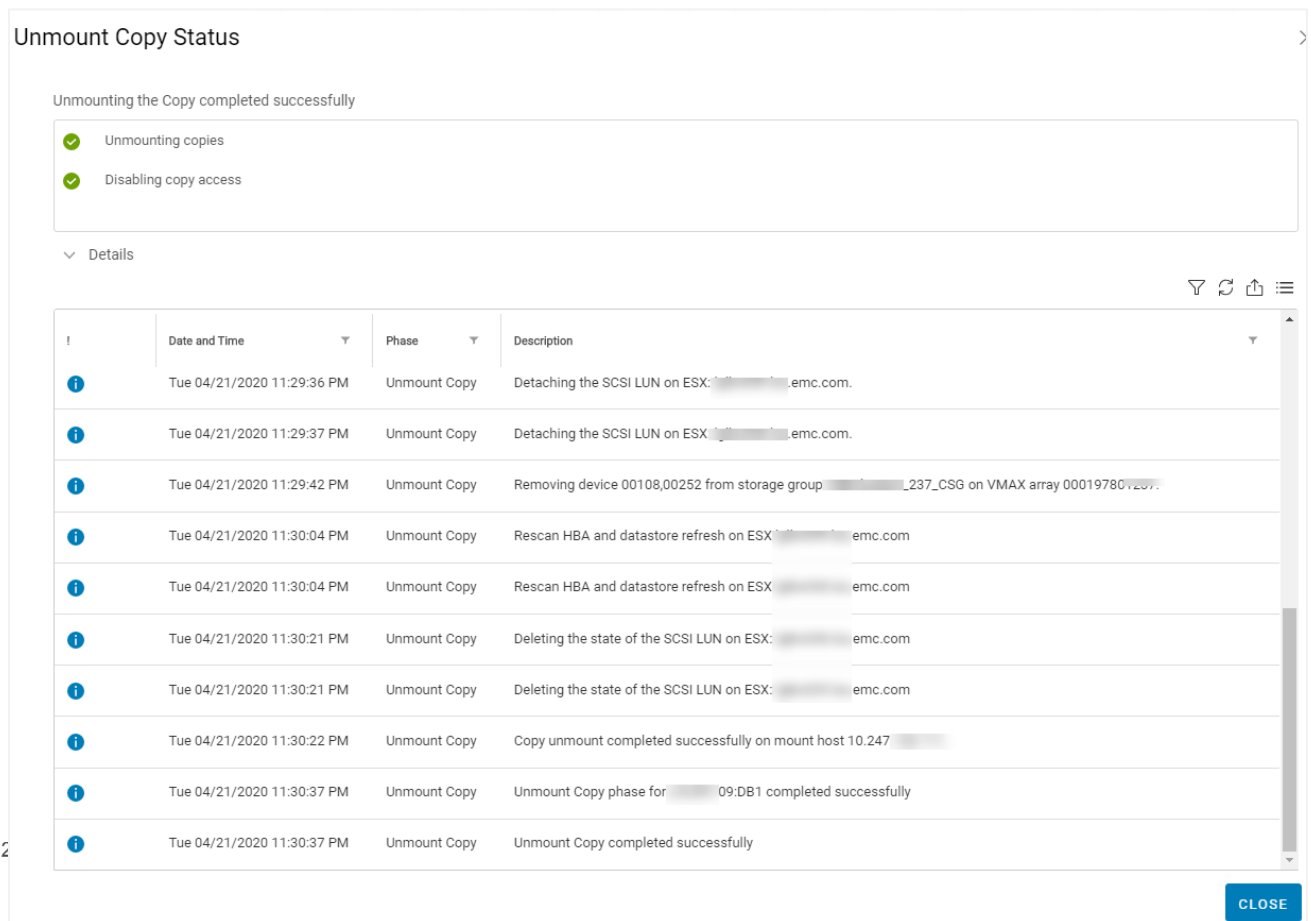

Unmount Copy Status

Unmounting the Copy completed successfully

- ✅ Unmounting copies
- ✅ Disabling copy access

⌄ Details

!	Date and Time	Phase	Description
ℹ	Tue 04/21/2020 11:29:36 PM	Unmount Copy	Detaching the SCSI LUN on ESX: ████████.emc.com.
ℹ	Tue 04/21/2020 11:29:37 PM	Unmount Copy	Detaching the SCSI LUN on ESX: ████████.emc.com.
ℹ	Tue 04/21/2020 11:29:42 PM	Unmount Copy	Removing device 00108,00252 from storage group ████████_237_CSG on VMAX array 00019780████.
ℹ	Tue 04/21/2020 11:30:04 PM	Unmount Copy	Rescan HBA and datastore refresh on ESX ████████emc.com
ℹ	Tue 04/21/2020 11:30:04 PM	Unmount Copy	Rescan HBA and datastore refresh on ESX ████████emc.com
ℹ	Tue 04/21/2020 11:30:21 PM	Unmount Copy	Deleting the state of the SCSI LUN on ESX: ████████emc.com
ℹ	Tue 04/21/2020 11:30:21 PM	Unmount Copy	Deleting the state of the SCSI LUN on ESX: ████████emc.com
ℹ	Tue 04/21/2020 11:30:22 PM	Unmount Copy	Copy unmount completed successfully on mount host 10.247 ████
ℹ	Tue 04/21/2020 11:30:37 PM	Unmount Copy	Unmount Copy phase for ████████ 09:DB1 completed successfully
ℹ	Tue 04/21/2020 11:30:37 PM	Unmount Copy	Unmount Copy completed successfully

CLOSE

Figure 2

Unmounting copies

8.3.5 Mounting with the required SLO

AppSync offers the ability to choose the required service level objective (SLO) when mounting target devices. AppSync will add the target devices to a storage group associated with the required 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.

PowerMax and the other arrays mentioned in this document restrict devices to one SLO associated storage group at any one point in time. Due to this restriction, AppSync 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. 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.

8.3.6   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.

D&LL Technologies

9 Repurposing workflows

Repurposing workflows are very similar to service plan workflows, in that the same phases are followed, as seen in Figure 21. There are differences, however, such as the repurposing workflow allows taking multi-generation copies. The repurposing workflow offers a first-generation copy which can be used for restore purposes, and also serves as a source for multiple second-generation copies. Both generation copies can be mounted and written to, but only the first can be restored back to production.

- **First-generation copies**: These can be used for restore purposes and serves as the source for multiple second-generation copies. First-generation copies integrate with the production application.
- **Second-generation copies**: These cannot be used for restore purposes and are created from a first-generation copy (for example, snap-of-snap, snap-of-clone, or clone-of-clone; creating clone-of-snap is not supported). Second-generation copies do not integrate with any application, so it is imperative the first-generation copy is not mounted during its creation.

Note: It is not recommended to mount the first-generation copy if creating second-generation copies, unless the intention is to mask data, or change the data, before creating and presenting the second-generation copies. In this case, it is advised the first-generation copy is unmounted, as no application integration occurs when creating the second-generation copy, so if the first-generation copy is mounted, there is a chance the second-generation copy would be corrupt, or inconsistent.

When working with SnapVX snapshots and service plan workflows, devices are only required when linking. Conversely, with the repurposing workflow, the first-generation copy automatically links to devices, regardless if the devices are mounted. The second-generation copy shares the same rules as service plan copies, where linking only occurs during the mount operation. Ensure that there are either target devices available in the storage groups AppSync is configured with, or if no storage groups are configured, allow AppSync to create devices as necessary. SnapVX clone operations always require target devices during the copy phase.

9.1 SnapVX linking rules with repurposing workflows

- First-generation copies**:**

  - Create copy phase will create the copy of the device and link it to a target
  - Refresh creates 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 remounting)
  - Expire will unlink the target device and delete the copy within AppSync (device created remains on the array)

- Second-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 (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)

9.2 Repurposing use case

The following depicts a common repurposing workflow use case. For example a database developing group needs to create multiple copies of production, and users require a point-in-time copy to serve as the baseline copy (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 point-in-time copy. This is the first-generation copy, also commonly referred to as a gold copy. This copy, by default, is application consistent.

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

9.2.1 Example first-generation repurposing workflow process flow

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

Phase	Message
Master phase	Beginning execution of service plan
Application discovery	Application discovery phase beginning
	Application discovery phase completed successfully
Application mapping	Application mapping phase beginning
	Application mapping phase completed successfully
Create first-generation copy	Create first-generation copy phase beginning
	Skipping unmount because there were no previously mounted copies found for the applications under protection during this cycle.
	Attempt number 1 to create a VSS copy of the application.
	Starting backup of SQL Server databases.
	VSS application freeze succeeded on host amssqlp1.
	Backup of database completed successfully.
	VSS application thaw succeeded on host amssqlp1.
	The SnapVX snapshot for the source device 003B8 on the array is EMC_SYNC_ASPECT1474905607970.
	The SnapVX snapshot for the source device 003B9 on the array is EMC_SYNC_ASPECT1474905607970.
	Refreshing the SnapVX replication relationships in storage array.
	The SnapVX snapshot EMC_SYNC_ASPECT1474905607970 for the source device 003B8 on the array is linked in nocopy mode with target device 003BC.

Phase	Message
	The SnapVX snapshot EMC_SYNC_ASPECT1474905607970 for the source device 003B9 on the array is linked in nocopy mode with target device 003BD.
	Create first-generation copy phase completed successfully
Unmount previous copy	Skipping unmount because there were no previously mounted copies found for the applications under protection during this cycle
	Unmount previous copy phase for applications completed successfully
Mount previous copy	Mount copy phase beginning
	Beginning mount on mount host
	Mounting file systems on mount host
	Making replication storage accessible to the mount host
	Adding copy device 003BD,003BC in storage group on VMAX array
	Rescan HBA and datastore refresh on ESXi
	All the target devices are visible on ESXi
	Started to mount copy of datastore
	All the target devices are visible on ESXi
	Mounting the VMFS on ESXi
	Cluster mount is enabled
	Rescan HBA and datastore refresh on ESXi
	Copy of datastore is mounted a on host
	Beginning hot add of virtual disk on virtual machine
	Successfully added virtual disk on virtual machine
	Mounting file systems in read-write mode on mount host
	VSS volume import and filesystem mount succeeded on host
	SQL metadata file saved
	Saved the VSS backup components document file
	Copy mount completed successfully on mount host
	Mount copy phase completed successfully
Recover copy	Recover copy phase beginning
	Beginning recovery of databases in mode recovery
	Recover copy phase completed successfully

DELLTechnologies

10 Troubleshooting tips

AppSync 4.0+ uses the U4P server to manage PowerMax and similar storage systems. Sometimes an error in an AppSync service plan or other operation related to the storage arrays are due to U4P issues. In such cases, it is always recommended to collect log files related to the U4P server.

If a Windows or Linux version of U4P is being used, implement the AppSync Server log collection utility to gather the necessary log files. Sometimes support will ask you to enable debug mode and duplicate the error message so enhanced logs messages are captured. You can see how this can be done in the Unisphere GUI in the following steps. If running the U4P appliance, follow the brief steps described below to collect the U4P logs. Below are directions for both circumstances.

In the AppSync UI, go to **Settings**, click **Logs and Data Expiration,** and click **Collect Logs** as shown in Figure 25.
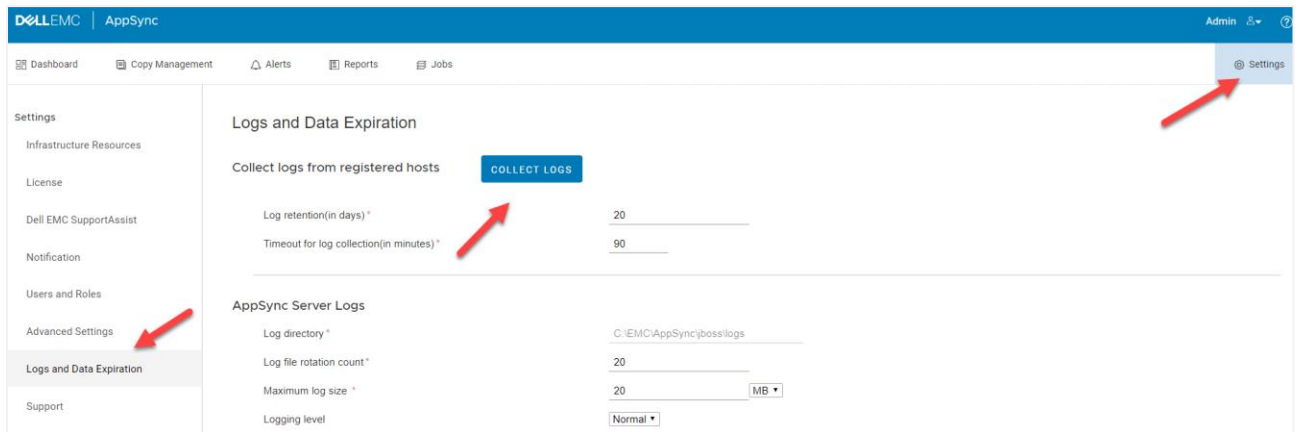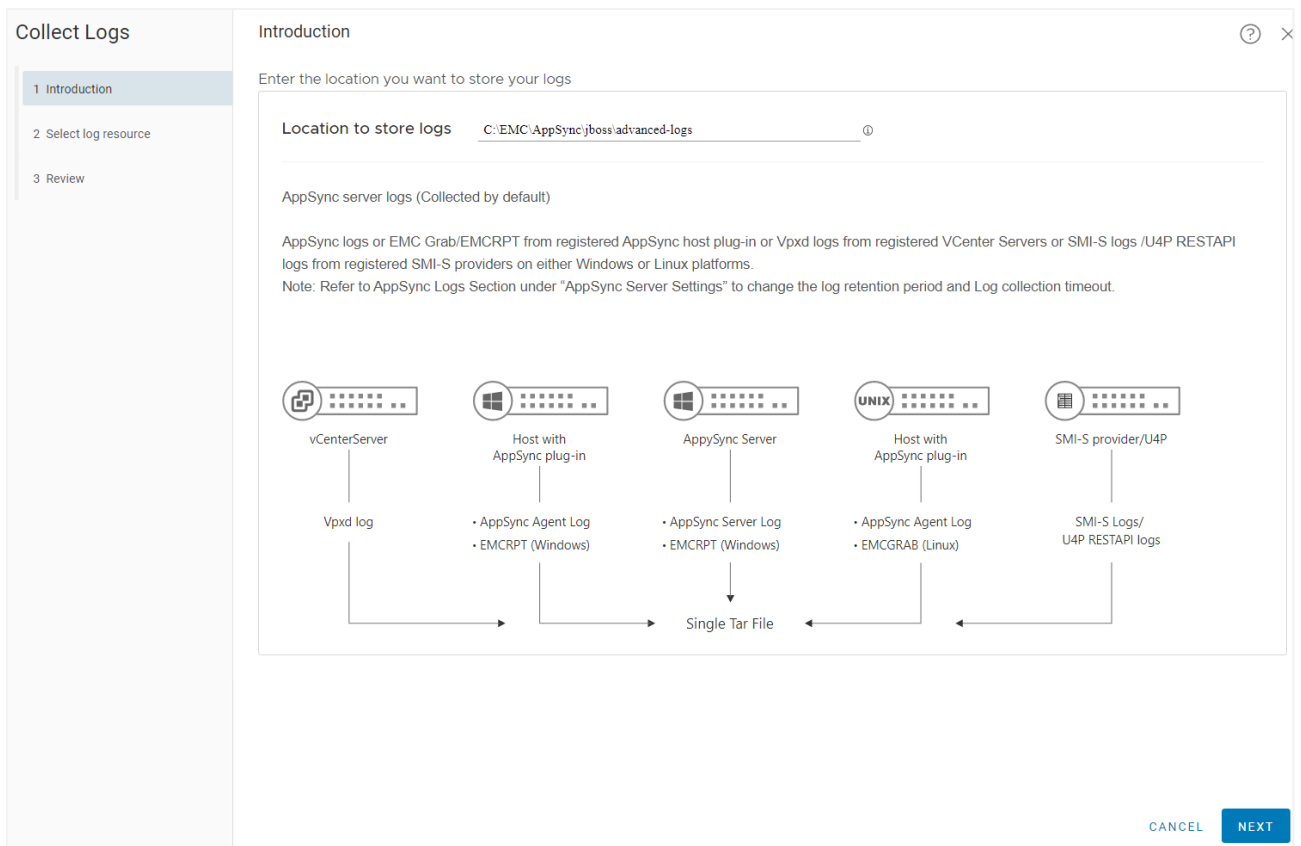

Figure 25   Collecting logs

Figure 26　　　　　Log paths

Click **Next** to accept the default log path as shown in Figure 26. On the next screen, scroll down until you see UNIVMAX and check the box next to your U4P server or servers to make sure the logs are collected from these hosts running on Windows or Linux as shown in Figure 27. You can select the appropriate option of Windows or Linux next to your U4P host and choose to save the credentials for future log collection. Once finished making your log collection choices, click **Next,** and click **Finish** on the review screen. The tooltip next to UNIVMAX states that **U4P REST API logs will be collect from selected UNIVMAX. Log collection is supported for UNIVMAX on Windows/Linux platforms only**. Figure 28 shows the log collection running.
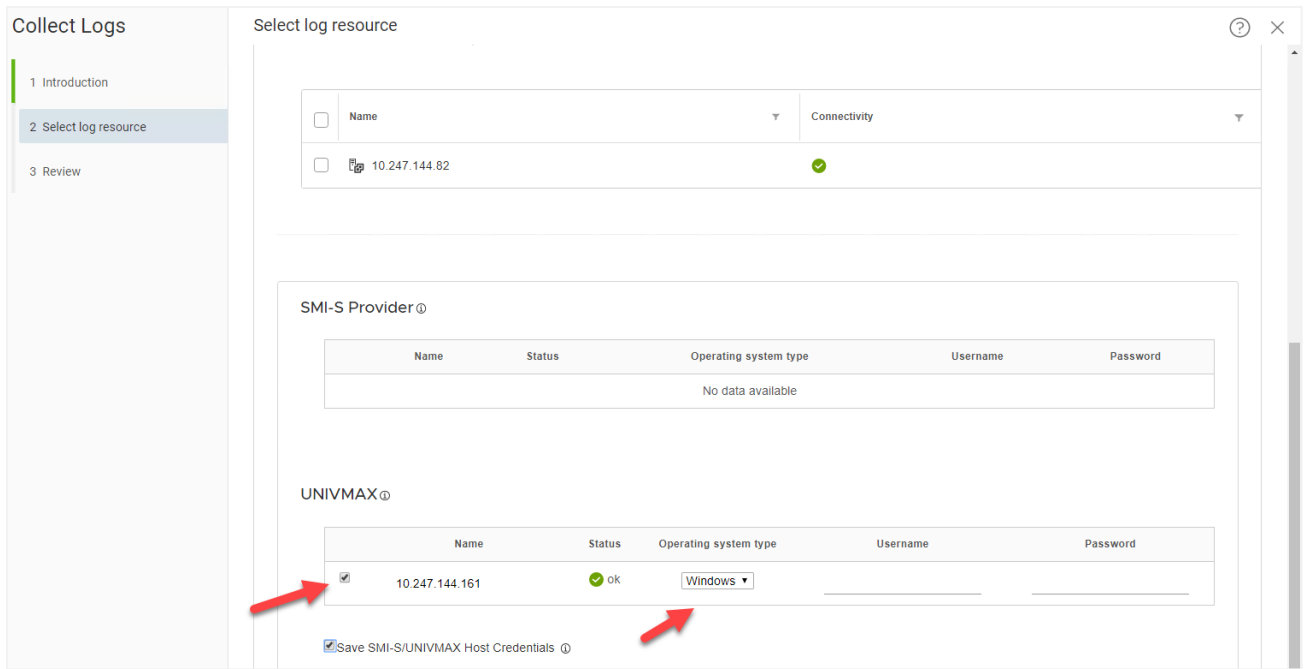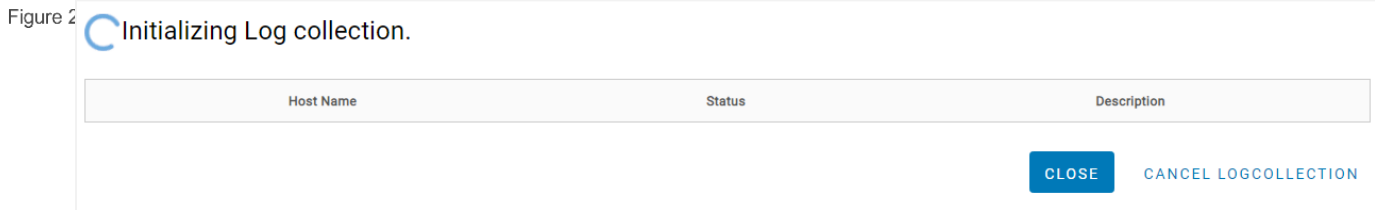
Collect U4P logs

Figure 2

Figure 28

Log collection running

Once the log collection process is done, you can upload the logs to your support case or review them as needed. The wizard provides a link to the support site upon completion.

This next procedure describes how to collect Dell EMC Grab Reports and other logs from a **Dell EMC Unisphere for PowerMax appliance**. This helps troubleshoot AppSync related problems when using PowerMax, VMAX All Flash, and VMAX3 arrays. AppSync does not do this automatically for the U4P virtual appliance because it lacks the APIs for the latter. AppSync can collect these logs automatically from the U4P versions running on Windows and Linux/Unix as noted above.

The best method is to log in to the U4P GUI and enable debug logging. Log in to the U4P instance at https://12.123.123.123:8443 with the smc/smc credentials.

Click the **Support** menu and set **Server Logging** to **DEBUG** from the **Modify Server Logging** link on the right. Check the box that says **Enable REST API Logging**. At this point, reproduce the issue in AppSync if this mode was not already set previously. This will ensure that we capture all the necessary logs to help support troubleshoot the issue. See Figure 29 below.
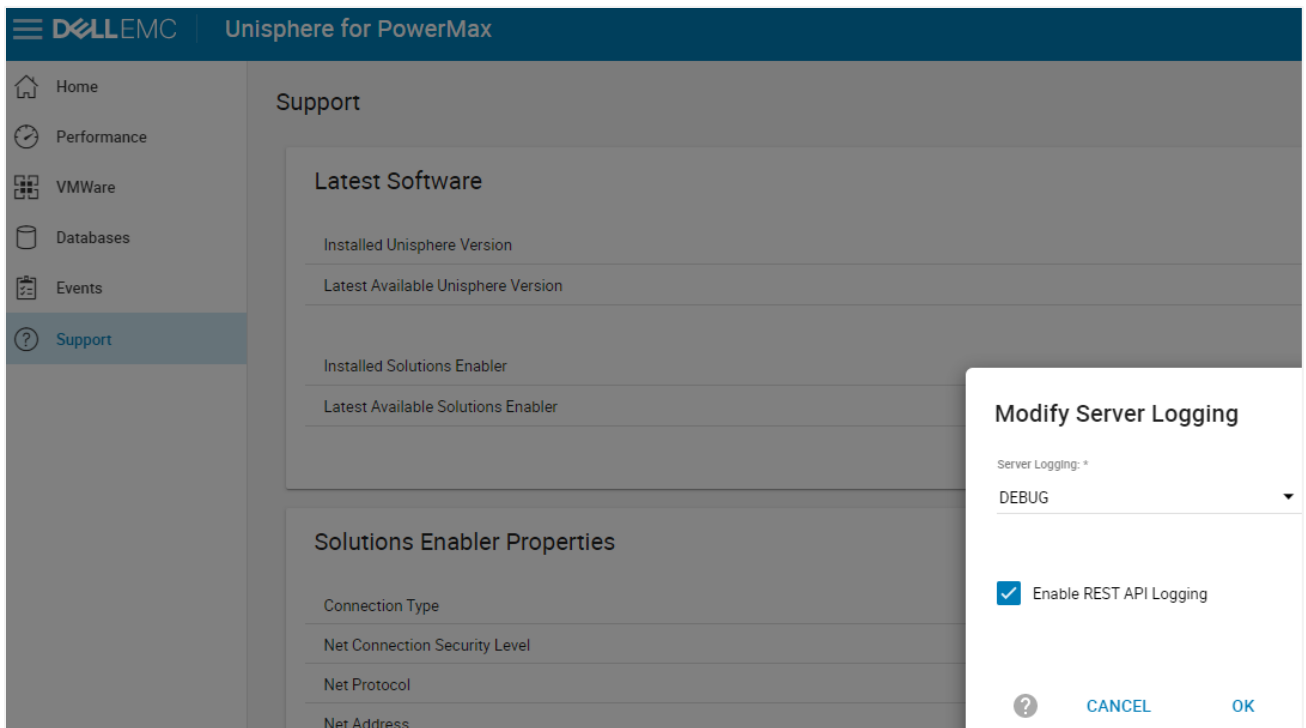
Modify server logging

Figure 29

Log in to the vApp Manager for Unisphere for PowerMax using the seconfig user. The first time you log in, use the username for the password, but after that, you can change it as needed. Notice the port is different.

http://12.123.123.123:5480/

seconfig/yourpassword

From the main screen, click the **Download** button, and select the **DELL EMC Grab Files** link. This downloads the grab files to the desktop. From there, you can upload them to the support ticket or FTP site. See Figure 30.
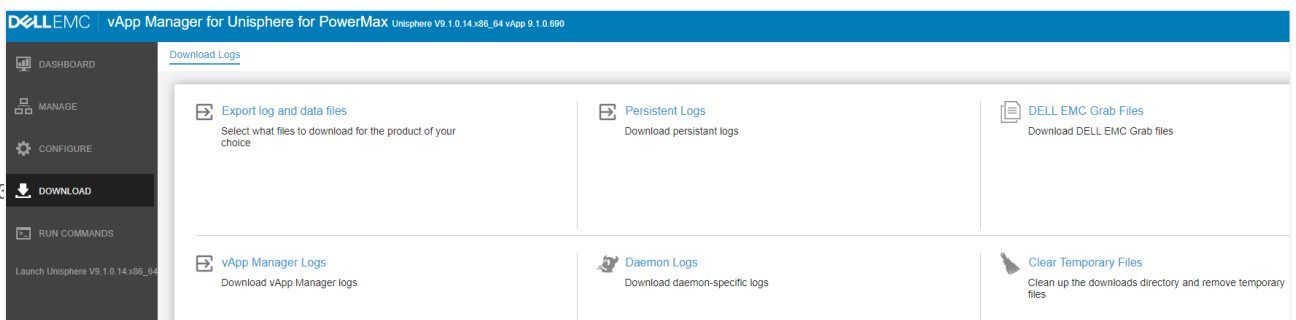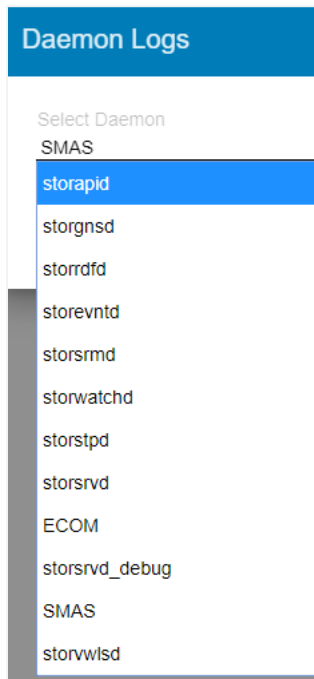

Figure 3

Download Dell EMC Grab Files

If you need additional log files, for example, click the **Daemon Logs** link and download the SMAS logs. See Figure 31.

Download daemon logs

Figure 31

11 Conclusion

This document explains key information and concepts when protecting an application residing on PowerMax or similar storage using AppSync. It discusses the inner operations of AppSync software while protecting applications using SnapVX technologies, along with deployment and troubleshooting tips.

A   Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

A.1   Related resources

For more information about AppSync and how to manage array environments, see the following sources at
https://www.dell.com/support/home/en-us/product-support/product/appsync/docs:

- AppSync Installation and Configuration Guide
- AppSync Performance and Scalability Guidelines
- AppSync Security Configuration Guide
- AppSync Simple Support Matrix
- AppSync User and Administration Guide