IMPLEMENTING VMWARE VSPHERE STORAGE API FOR STORAGE AWARENESS WITH SYMMETRIX STORAGE ARRAYS

Abstract
This white paper explains how to install, configure and use EMC’s implementation of VMware’s vStorage API for Storage Awareness 1.0 (VASA) with vSphere 5 and Symmetrix storage arrays. Topics include Storage Profiles and Virtual Provisioning out of space avoidance functionality.

September 2014
Table of Contents

Executive summary........................................................................................................... 4
SMI-S and VASA ................................................................................................................. 4

Installation and Configuration .......................................................................................... 5

Installation of the VASA Provider .................................................................................. 5
Configuration of the VASA Provider ................................................................................ 7
Port settings ....................................................................................................................... 7
Changing the external connection limit .......................................................................... 8
Configuring user authentication ...................................................................................... 10
Configuration of VMware vCenter .................................................................................. 14

Using VASA with vSphere 5 ......................................................................................... 17

Storage Profiles .................................................................................................................. 17
Creating Storage Profiles ............................................................................................... 20
Using Storage Profiles ..................................................................................................... 23
Checking storage profile compliance ............................................................................. 26
Thin-device capacity alarm .............................................................................................. 28

Conclusion ......................................................................................................................... 32

References ......................................................................................................................... 32

Appendix: VASA Registration Troubleshooting ............................................................... 33

Invalid certificate ................................................................................................................ 33
Invalid username or password ........................................................................................... 34
Generic VASA registration error ....................................................................................... 35
Importing a valid certificate ............................................................................................... 37
Executive summary

One of the challenges facing VMware administrators is relating VMware storage constructs with their array-level configuration and capabilities. It is extremely important to understand the underlying configuration of storage hosting Virtual Machine File Systems (VMFS) in order to properly place and configure virtual machines. In the past, VMware administrators had to exchange information with storage administrators in order to define the relevant storage parameters. Relating this information in an efficient and meaningful way could be a difficult task at times since these two different functional silos were not only physically separate but also logically separate.

In recent years, EMC® understood this challenge and therefore developed plugins such as the Virtual Storage Integrator which allowed for in-context storage configuration information from within the vSphere Client. This greatly simplified the process of understanding and identifying VMFS volume configuration by reducing the VMware administrators’ reliance on external tools.

With the introduction of VMware vSphere 5, VMware now offers a new application programming interface (API) for storage vendors to leverage. This allows tight and uniform integration of specific array-based information into the VMware management interface. This API, called the vSphere Storage API for Storage Awareness or VASA, is fully supported by the Symmetrix platform through the use of EMC’s SMI-S Provider.

This white paper discusses how to install, configure and use VASA in VMware vSphere 5 environments with EMC Symmetrix® DMX™ and VMAX™ storage arrays. Specific focus will be given to VMware vSphere Storage Profiles and the thin device capacity threshold alert. An understanding of the principles that are exposed here will allow the reader to deploy and utilize VMware vSphere in the most effective manner.

SMI-S and VASA

EMC’s SMI-S Provider implements industry standard services for storage and platform management that are defined and maintained by the Storage Networking Industry Association (SNIA) and the Distributed Management Task Force (DMTF) respectively. SNIA collectively publishes storage related standard interfaces in its Storage Management Initiative-Specification (SMI-S). The DMTF publishes its platform management standard interfaces separately. All of these interfaces are based on the Common Information Model (CIM) also published by DMTF and all adhere to DMTF Web Based Enterprise Management (WBEM) standards. WBEM defines standard, interoperable protocols between clients and servers in a web based environment. These include CIM XML and WS Management, both of which are XML and HTTP based.

Collectively, these standards strive to ensure consistent data and eliminate inconsistencies among management tools by providing a unified interface to the

---

1 Supported with EMC Enginuity™ version 5568 or higher.
2 Supported with EMC Enginuity™ only; not supported with HYPERMAX OS.
many storage objects that must be managed in a storage environment. This enables application developers to focus on a single, standard interface for the development of management tools.

EMC SMI-S Provider is integrated with the EMC Common Object Manager (ECOM) to provide an SMI-compliant interface for EMC Symmetrix arrays, EMC CLARiiON® arrays, and EMC VNX™ family storage systems. Included in the SMI-S Provider since version 4.3.0 is the VASA Provider—this paper will discuss version 4.6.1. The VASA Provider sits as its own protocol adapter integrated onto the top of the SMI-S provider. It uses its own protocol instead of directly using the WBEM protocol mentioned earlier. Requests are processed over the VASA protocol and translated into requests to the underlying implementation of the SMI-S and DMTF services. SMI-S and VASA are supported with CLARiiON, VNX and Symmetrix arrays. This paper focuses on the use of VASA with Symmetrix storage.

EMC’s VASA Provider enables Symmetrix management software to inform vCenter of how VMFS storage is configured and protected. These capabilities are defined by EMC and include characteristics such as disk type, thin or thick provisioning, storage tiering and remote replication status. This insight allows vSphere administrators to make quick, intelligent, and informed decisions as to virtual machine placement. VASA offers the ability for vSphere administrators to complement their use of plugins and other tools to track how Symmetrix devices hosting VMFS volumes are configured to meet performance and availability needs.

Installation and Configuration

The EMC SMI-S Provider is supported for installation on a variety of Windows and Linux platforms as detailed in the software’s release notes. Both the software and documentation can be downloaded from support.EMC.com.

VASA 1.x is not supported by the SMI-S Provider in Solutions Enabler 8.x. Only the SMI-S Provider in Solutions Enabler 7.x is supported.

Alternatively, EMC offers a simple-to-use and pre-configured Solutions Enabler Virtual Appliance that includes the VASA provider. Users can register this appliance with VMware vSphere, as instructed in the appropriate VMware vSphere 5 documentation. The Solutions Enabler Virtual Appliance is also available in versions that include Unisphere for VMAX and Performance Analyzer. For information about the deployment of these virtual appliances, see the EMC Solutions Enabler Installation Guide or the EMC Unisphere for VMAX Installation Guide.

Installation of the VASA Provider

Figure 1 shows the first screen of the 64-bit version of the Windows SMI-S provider installation wizard. For instructions on Linux installation and Virtual Appliance SMI-S deployment refer to the SMI-S release notes on support.EMC.com.
Implementing VMware's vStorage API for Storage Awareness with Symmetrix

Figure 1. 64-bit Windows SMI-S installation wizard

The VASA provider automatically installs when the Array Provider option is selected when installing the SMI-S Provider. The Windows version of the installation wizard is shown in Figure 2 with the Array Provider selected.
Implementing VMware’s vStorage API for Storage Awareness with Symmetrix

Figure 2. Installing the VASA Provider

Configuration of the VASA Provider

Before the VASA provider can be used with vCenter a few important configuration changes should be made:

1. Alter the advanced setting **ExternalConnectionLimit**
2. Change the default admin password
3. Create a new user account for VASA

Port settings

By default, the ECOM server listens on ports 5988 (for HTTP) and 5989 (for HTTPS) for CIM-XML and listens on ports 5985 (for HTTP) and 5986 (for HTTPS) for WSMAN. When running on the Symmetrix service processor, the SMI-S Provider listens on port 5989 only. If the default ports are in use by some other process (such as WMIProvider), the CIM server does not start.

When this occurs, you can either move the other process to a different network port, or specify different port values for the EMC CIM server by changing the Port0, Port1, Port2 and Port3 parameters of port_settings.xml file (located in the Solutions Enabler Windows directory C:\Program Files\emc\ECIM\ECOM\conf and UNIX directory /opt/emc/ECIM/ECOM/conf) and restarting the SMI-S Provider.

During installation the scripts attempt to determine if the default ports (5988, 5989, 5985, and 5986) are in use. If they are in use at install time, the installation attempts to use other ports until free ports are found. Once a usable port value is found, the
script automatically updates the port_settings.xml file with the ports that are used after installation.

If a firewall is enabled, it is required to have port 5989 open for TCP access on the vCenter server in order to allow access to the SMI-S provider.

Changing the external connection limit

After the SMI-S provider is installed, users must modify an ECOM setting in order for VMware vSphere 5.0 to properly use the VASA provider. The setting named ExternalConnectionLimit in the Security_settings.xml configuration file must be increased from a default value of ‘100’ to ‘1200’. This change is required because over time vCenter may open up to a maximum of 1,000 concurrent connections to a VASA provider. With the setting ExternalConnectionLimit set to a value of ‘100’, any connection after the first one hundred will be, by default, rejected by ECOM resulting in vCenter being unable to communicate with the EMC VASA Provider.

To change this setting, follow these steps:

1. Stop the ECOM service on the SMI-S Provider server if it is running. The process to do this varies with the operating system hosting the SMI-S Provider. The process for a Windows operating system is shown in Figure 3.

![Figure 3. Stopping the ECOM service](image-url)
WARNING: Stopping the ECOM service will prevent access to the SMI-S provider by all external applications. If this is a pre-existing installation, verify that no other applications are actively using the SMI-S Provider and/or require the provider to be available. If so, perform this operation during an approved maintenance window.

2. Alter the value of the `ExternalConnectionLimit` setting in the `security_settings.xml` file from ‘100’ to ‘1200’. This file is located in the folder “%root%\emc\ecim\ecom\conf\”. The precise location of the root of the folder structure varies depending on the operating system hosting the SMI-S Provider. For example this would be “C:\Program Files\” on Windows. The location of the file and the altered option are shown respectively in Figure 4 and Figure 5.

![Security settings XML file location](image)

**Figure 4. Security settings XML file location**
3. Save the configuration file.
4. Start the ECOM service.

Configuring user authentication

It is strongly recommended to change the default administrative password (if not already changed) and to create a separate user account for vCenter access to the VASA provider to secure the SMI-S Provider.

The SMI-S provider offers a web-based interface for creating and managing user accounts. The default username and password as well as the URL for access are listed below:

Username: admin
Password: #1Password
Management URL: https://<FQDN or IP of SMI-S Provider server>:59893/ecomconfig

The logon page for the web-based management interface is shown in Figure 6.

---

3 This port number may not always be 5989. If 5989 was not available during installation or manually changed later by an administrator the alternately configured port must be used. Refer to the section entitled, Port settings on page 7 for information on determining the port number that is in use.
Implementing VMware's vStorage API for Storage Awareness with Symmetrix

Figure 6. Logon page for SMI-S web-based management

If the web interface does not load, restart the ECOM service (see Figure 3) and wait a few minutes for all services to be restarted and try again.

The first thing that the user should do is to change the default admin password from #1Password to a unique and complex password to prevent unauthorized access to the SMI-S Provider. This process is shown in Figure 7.
In addition to changing the admin password, it is recommended to create a new user dedicated for VASA authentication from vCenter. Administrative access is not required for VASA provider registration with vCenter and is therefore not recommended. The role of “vmadmin” was specifically created for VASA Provider registration and has no other permissions. This role consequently allows a VMware administrator to register a VASA Provider without being provided administrative credentials to ECOM. Figure 8 shows the creation of a user account named “vasauser” with the role type of “vmadmin”.

Figure 7. Changing the default admin password
It is important to note that while the SMI-S Provider does support Windows authentication, when configured, the VASA Provider does not. Configuring SMI-S for use with Windows Authentication will block the use of VASA with that instance of SMI-S. Support for Windows authentication with the VASA provider is planned for a future release. Therefore if Windows authentication is desired for other SMI-S Provider functions, a separate instance of SMI-S should be installed and dedicated for VASA Provider user.

In order for the VASA Provider to detect and query for Symmetrix information, access to the desired arrays must be granted to the provider. Symmetrix discovery is implemented in-band and therefore requires several small devices called Gatekeepers to be presented to the SMI-S Provider. Gatekeepers can be standard (non-thin) devices or starting with Enginuity 5876 and Solutions Enabler V7.4 may be thin devices (bound or unbound); the recommended size is 3 MB. For each array that is providing storage to the target VMware environment, six gatekeepers (the minimum recommended number by Symmetrix Engineering) from each respective Symmetrix

Figure 8. Creating a user for the VASA provider
should be presented to the SMI-S Provider server. Once presented to the server, they only need to be online and ready; they should not be formatted with any type of file system.

**Configuration of VMware vCenter**

Once the VASA Provider has been installed and configured, it needs to be registered with vCenter. vCenter has to log into the VASA Provider and present a valid certificate that will be used to authenticate subsequent VASA communication.

**NOTE:** The Storage Providers icon will not be available in the vSphere Client when logging in directly to the ESXi host. The VASA Provider cannot be registered with a standalone ESXi host—it requires vCenter.

The registration process is initiated from the **Home** screen in the vSphere Client under **Administration> Storage Providers**. This can be seen in Figure 9.

![Figure 9. Storage Provider registration location](image)

The EMC VASA Provider can be added by clicking the **Add...** link on the top of the **Vendor Provider** screen as shown in Figure 10.

---

4 If the SMI-S Provider is installed in a virtual machine, the gatekeepers must be presented as Raw Device Mappings in Physical compatibility mode.
Figure 10. Initiating VASA Provider registration screen

The registration screen requires four pieces of information:

1. **A name.** A user can name the provider anything that is useful to them. This name is not verified by any process and is simply for user recognition.

2. **The VASA Provider URL.** This is the address of the VASA Provider service. The syntax is shown below. Only the server name/IP should be altered. The URL is not case sensitive.

   $$https://<SMI-S Provider server name or IP address>:5989/vasa/services/vasaService$$

3. **Login.** It is recommended to not use the default admin account but a dedicated account like described earlier in this document

4. **Password.**

   Optionally, a vendor-provided certificate can be used. By default a self-signed certificate is used for authentication. An example registration screen is shown in Figure 11.

**Figure 11. VASA Provider registration**

5 This port number may be not always be 5989. If 5989 was not available during installation or manually changed later by an administrator the alternately configured port must be used. Refer to the section entitled, Port settings on page 7 for information on determining the port number that is in use.
If no arrays are presented to the SMI-S Provider, authentication will fail. This means gatekeepers must be provisioned to the provider prior to registration in vCenter. If authentication continues to fail, verify the credentials and the URL are correct and that the VASA Provider host has IP connectivity and the ECOM service is running. Port 5989 must also be open if firewalls are in use.

Once the VASA Provider successfully registers, it will be listed in the Vendor Providers panel. The screen offers three operations in addition to adding new providers:

1. **Removing a provider.**
2. **Refreshing all listed providers.** This refreshes configuration information of the providers.
3. **Synchronizing a provider.** This synchronizes storage information from the provider.

These options can be seen in the upper right-hand corner of Figure 12.

![Figure 12. Vendor provider operations](image)
Using VASA with vSphere 5

The current implementation of EMC's VASA Provider and VMware vCenter Server offer two main features: system-defined storage capabilities and storage alert forwarding. The following sections discuss configuring and using these two features.

Storage Profiles

Managing datastores and matching the Service Level Agreement requirements of virtual machines with the appropriate datastore can be a challenging and cumbersome task. vSphere 5 introduces Profile-Driven Storage, which enables rapid and intelligent placement of virtual machines based on specific SLA, availability, performance or other requirements.

Using Profile-Driven Storage, various storage characteristics, typically defined as a tier, can be requested in a virtual machine storage profile description. These profiles are used during provisioning, cloning and Storage vMotion to ensure that only those datastores or datastore clusters that are compliant with the virtual machine storage profile are made available as valid locations to place the virtual machine. The virtual machine storage profile can also help select the same type of datastores when creating a Storage DRS datastore cluster. Profile-Driven Storage will reduce the amount of manual administration required for virtual machine placement while improving virtual machine SLA storage compliance.

Profile-Driven Storage delivers these benefits by taking advantage of the following:

- Full integration with vSphere Storage APIs – Storage Awareness, enabling usage of storage characterization supplied by storage vendors.
- Support for NFS, iSCSI and Fibre Channel (FC) storage, and all storage arrays on the HCL.
- Enabling the vSphere administrator to tag storage based on customer or business-specific descriptions.
- Using storage characterizations supplied by the VASA Provider and target storage array and/or administrator-defined descriptions to create virtual machine placement rules in the form of storage profiles.
- Providing a simple mechanism to check a virtual machine's compliance with placement rules. This ensures that a virtual machine is not deployed or migrated to an incorrect type of storage without an administrator being informed about the situation.

Storage profiles are built on the storage capabilities provided by the VASA Provider. The VASA Provider correlates Symmetrix devices with the capabilities designated in the provider. Currently, only one capability can be assigned to a device by VASA. If more capabilities are desired, an administrator can create user-defined capabilities and manually assign them to VMFS volumes to complement the system-defined capabilities assigned by VASA. VMware does not dictate how capabilities should be defined and leaves this to the discretion of the storage...
vendor. The storage capabilities offered by the EMC VASA Provider are listed and described in Table 1 and shown within vCenter in Figure 13.

Table 1. EMC system-defined storage capabilities

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS/Fibre Storage; Thin; Remote Replication</td>
<td>SAS or Fibre Channel drives; thin-provisioned; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>SAS/Fibre Storage; Thin</td>
<td>SAS or Fibre Channel drives; thin-provisioned.</td>
</tr>
<tr>
<td>SAS/Fibre Storage; Remote Replication</td>
<td>SAS or Fibre Channel drives; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>SAS/Fibre Storage</td>
<td>SAS or Fibre Channel drives.</td>
</tr>
<tr>
<td>Solid State Storage; Thin; Remote Replication</td>
<td>Solid state drives; thin-provisioned; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>Solid State Storage; Thin</td>
<td>Solid state drives; thin-provisioned.</td>
</tr>
<tr>
<td>Solid State Storage; Remote Replication</td>
<td>Solid state drives; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>Solid State Storage</td>
<td>Solid state drives.</td>
</tr>
<tr>
<td>NL-SAS/SATA Storage; Thin; Remote Replication</td>
<td>Near Line-SAS/SATA drives; thin-provisioned; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>NL-SAS/SATA Storage; Thin</td>
<td>Near Line-SAS/SATA drives; thin-provisioned.</td>
</tr>
<tr>
<td>NL-SAS/SATA Storage; Remote Replication</td>
<td>Near Line-SAS/SATA drives; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>NL-SAS/SATA Storage</td>
<td>Near Line-SAS/SATA drives.</td>
</tr>
<tr>
<td>Auto-Tier Storage; Thin; Remote Replication</td>
<td>Multiple drive tiers with FAST VP enabled; thin-provisioned; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>Auto-Tier Storage; Thin</td>
<td>Multiple drive tiers with FAST VP enabled; thin-provisioned.</td>
</tr>
<tr>
<td>Auto-Tier Storage; Remote Replication</td>
<td>Multiple drive tiers with FAST enabled; remote replication intended to provide disaster recovery.</td>
</tr>
<tr>
<td>Auto-Tier Storage</td>
<td>Multiple drive tiers with FAST enabled.</td>
</tr>
</tbody>
</table>

Depending on the Symmetrix arrays and devices that are presented to the vCenter environment, not all of the capabilities may be listed. For instance, if the vCenter environment, not all of the capabilities may be listed. For instance, if the vCenter

---

6 For the system-defined storage capabilities that include remote replication, it is important to note that EMC’s VASA provider will not recognize all replication technologies that are currently available on Symmetrix. Currently only SRDF, SRDFe, and Open Replicator for Symmetrix (ORS) are supported by the VASA Provider. Any device, for example, being remotely replicated with RecoverPoint will be treated as a non-replicated device. RecoverPoint support will be added in a future release.

7 In addition to FAST VP enabled devices (pinned or unpinned), a device that has extents in more than a single tier (technology) will also be categorized as Auto-Tier.
Implementing VMware’s vStorage API for Storage Awareness with Symmetrix

environment is using a VMAX10K exclusively, only the storage capabilities that are specific to thin devices will be shown.

EMC has released the newest platform to the VMAX family the VMAX³. This platform does not support VASA integration with the 1.x VASA Provider.

![Figure 13. EMC system-defined storage capabilities](image)

After the storage provider is registered, and the system-defined storage capabilities appear, the datastores that can be classified⁸ will be recognized. In Figure 14 the summary screen of datastore “Thin_volume_test” is displayed. Under the Storage

⁸ The SMI-S Provider must have access to the Symmetrix arrays presented to the vCenter environment. If datastores exist on volumes from arrays that the SMI-S Provider does not have access to, they cannot be assigned a capability.
Capabilities box, the volume underlying the datastore has been recognized as a NL-SAS/SATA Storage device that is thin provisioned. Note that there is a field for a User-defined Storage Capability, if one exists, for the volume.

Figure 14. Datastore system storage capability classification

Creating Storage Profiles

Once the system-defined storage capabilities have been imported by an initial synchronization of the VASA Provider, storage profiles can be enabled and created.

Before storage profiles can be assigned to virtual machines the feature must be enabled on relevant hosts/clusters first. This is achieved by clicking the Enable VM Storage Profiles button under the VM Storage Profiles screen which can be found at Home > Management within vCenter. Within the screen that pops up, all clusters/hosts are listed and licensing requirements are verified. If licensing requirements are met, storage profile functionality can be enabled on that host/cluster. This screen can be seen in Figure 15.

---

9 In addition to VMware vCenter Standard, an Enterprise Plus license is required for each ESXi host that is intended for use with storage profiles.
Regardless of whether or not storage profiles are enabled, VASA will still associate VMFS volumes with storage capabilities. Users can manually check configuration of VMFS volumes by viewing the volume properties in the vSphere Client.

Storage profiles can be created by clicking the Create New VM Storage Profile button. The wizard for creating storage profiles allows the user to name and describe the profile in a meaningful way as well as associating user-defined or system-defined storage capabilities with it.

Storage profiles can be associated with one or more storage capabilities therefore allowing virtual machines associated with a given profile the flexibility of being located on one of many heterogeneous configurations without being marked as non-compliant. Assigning only one capability restricts a virtual machine to a narrow configuration which can be recommended for critical virtual machines that require certain performance or protection.

Figure 16 and Figure 17 show the process to create a storage profile. The storage profile created in this instance includes all capabilities that indicate that the device is remotely replicated regardless of disk type and configuration. This assures that compliant virtual machines will always be protected by remote replication but may not assure performance levels.

---

10 This paper will not be discussing the creation or use of user-defined capabilities, but they are essentially used in the same way as system-defined ones. For more information on user-defined capabilities refer to VMware documentation.
Capabilities can be mixed and matched however the user sees fit. Storage capabilities can be associated with multiple storage profiles allowing for the creation of flexible and diverse storage profiles.

Figure 16. Creating a storage profile
Implementing VMware’s vStorage API for Storage Awareness with Symmetrix

Using Storage Profiles

Once a storage profile has been created, they can be associated with the virtual disks of a virtual machine. Figure 18 shows an example storage profile that requires that the virtual disk be located on a SAS or Fibre-backed thin device that is not replicated.
Implementing VMware's vStorage API for Storage Awareness with Symmetrix

Figure 18. Example of a storage profile

When creating, cloning, or migrating virtual machines, storage profiles can be used to ensure proper placement of the virtual machines' virtual disk(s). Figure 19 shows storage profile screen of the Create New Virtual Machine Wizard. This screen is very similar to the virtual machine migration or cloning wizard. A user can select a profile in the drop-down menu and the wizard will automatically sort the datastores according to their compatibility status with the selected storage profile.

If datastore clusters are configured they will be listed in place of their individual datastores. It is important to note that datastore clusters will only be assigned a storage capability by VASA if all included datastores are of the same type. If the cluster includes mixed-type datastores the cluster will be marked as incompatible. For this reason, it is highly recommended to only group datastores into clusters if they all have the same capabilities.

Furthermore, if Storage DRS is enabled on a datastore group the user will not have to specify which datastore in the cluster should be used. Storage DRS will offer
Implementing VMware's vStorage API for Storage Awareness with Symmetrix

recommendations at the end of the wizard as to which datastore would be preferred. These recommendations can be accepted or overridden.

Incompatible datastores or datastores may be chosen if desired—this is not prevented by vCenter.

Figure 19. Placing a virtual machine according to a storage profile

Once a compatible datastore or datastore cluster has been chosen, the profile will be applied to all of the virtual machine's virtual disks. If a user wishes to remove the profile association or edit which profile is associated to a virtual machine this can be achieved by choosing to edit the setting of the virtual machine.

Figure 20 displays the properties of a virtual machine. The storage profile configuration can be edited from the Profiles tab. This tab offers two options:

1. Choosing the profile for the configuration files
2. Choosing the profile for the virtual disks

The profile for the configuration files can be selected by clicking the drop-down list and choosing the appropriate storage profile. If it is desired to propagate this association to all of the virtual disks, the Propagate to disks button can be selected. If different profiles are desired for each disk, they can be individually selected and associated to a specific profile via their respective drop-down lists.

It is important to note that associating a profile here will NOT move the configuration files or virtual disks. They will simply assign the profile and check for compliancy. If the configuration files or virtual disks are located incorrectly, they will be marked as
non-compliant and will require an admin to relocate them to a proper VMFS volume with Storage vMotion.

Figure 20. Editing the storage profile associations of a virtual machine

**IMPORTANT:** It is important to note that Raw Device Mappings are not supported for use with storage profiles. Since vCenter only applies capabilities for VMFS volumes the specific capability of a RDM is unknown to vCenter even though the EMC VASA Provider does contain the information. Nevertheless RDMs will still be listed under the storage profile and can in fact be associated with one. However, importantly, vCenter will look at the capability of the VMFS where *its pointer files are*, not the RDM itself. This can lead to false positives or false negatives with RDM storage profile compliance. Therefore this should not be relied on and manual confirmation of the underlying configuration of the storage through the use of the VSI Storage Viewer is recommended.

**Checking storage profile compliance**

Once a virtual machine is associated with one or more storage profiles, the VM Storage Profiles box will be populated in the summary tab of the virtual machine. This is shown in Figure 21.
If all of the virtual disks and configuration files of the virtual machine are compliant, the Profile Compliance box will be marked with a check-marked green circle. Otherwise, if one or more virtual disks are non-compliant it will be a red diamond with an exclamation point (shown in Figure 22). Compliance checking is not real-time so reported compliance information may not always be up-to-date. It is important to click the Refresh link to ensure the correct information is displayed.

It is also possible to check the compliance of all virtual machines associated with a storage profile by navigating back to the VM Storage Profiles view shown in Figure 23.
Thin-device capacity alarm

Within vSphere 5 there is a new alarm definition for VASA. It is named “Thin-provisioned volume capacity threshold exceeded” and will be triggered if the thin volume on the Symmetrix exceeds predefined thresholds. These thresholds are as follows:

- < 65% is green
- >= 65% is yellow
- >= 80% is red

The alarm definition is seen in Figure 24.

---

Prior to vSphere 5.1 this alarm was named “Thin-provisioned LUN capacity exceeded.”
29

Implementing VMware's vStorage API for Storage Awareness with Symmetrix

Figure 24. Thin-provisioned volume capacity threshold exceeded alarm definition

A thin volume below 65% will produce no alarm; a triggered alarm is either a warning (yellow) or an alert (red). An alert is seen in Figure 25 for datastore “VASA_DS”.

<table>
<thead>
<tr>
<th>Object</th>
<th>Status</th>
<th>Name</th>
<th>Triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>VASA_DS</td>
<td>Warning</td>
<td>Datastore usage on disk.</td>
<td>9/2/2013 9:50:34 AM</td>
</tr>
<tr>
<td>VASA_DS</td>
<td>Alert</td>
<td>Thin-provisioned volume capacity threshold exceeded</td>
<td>9/2/2013 10:01:11 AM</td>
</tr>
</tbody>
</table>

Figure 25. Thin-provisioned volume alarm in vCenter

While the warning is just that, and will not prevent the user from creating other virtual machines on the datastore using that thin volume, an alert will prevent such activity. VMware takes this step to reserve the remaining space for the current virtual machines and avoid any out of space conditions for them. If the user attempts to create a virtual machine on the datastore which has this alert, the error seen in Figure 26 will result.
The user must take corrective action at this point and may choose to increase the size of the thin volume, have the system administrator perform a space reclamation on the thin volume, or use a different datastore altogether for future virtual machines. Once the thin device has enough free space to be beyond the warning and alert thresholds, the alarm will be removed.

In order for vCenter to report an exhaustion of space on the thin-provisioned volume on the Symmetrix, the SMI-S Provider takes advantage of the events that are automatically recorded by the event daemon on the Symmetrix. These events are recorded regardless of whether the user chooses to be alerted to them in Unisphere for VMAX. Therefore once the SMI-S Provider is properly installed and registered in vCenter, no additional configuration is required on the Symmetrix or within Unisphere for VMAX.

If the user wishes to see alerts for thin device allocation within Unisphere, the system administrator can configure them through the path Home > Administration > Alert Settings > Alert Thresholds. The configuration screen is shown in Figure 27 where the default alert for thin device allocation is highlighted. The default alert cannot be altered - attempts to edit it will result in the error in the dialog box of Figure 27. Users
can, however, create specific alerts for particular thin pools which will supersede the default alert.

**Figure 27. Thin device allocation alert within Unisphere for VMAX**

Such alarms and alerts allow the VMware administrator and system administrator to be aware of the state of the storage capacity presented to the VMware environment. The thin volume alarm is only one of the ways that the vSphere vStorage APIs for Storage Awareness can provide insight for the VMware administrator into the Symmetrix storage.

Managing storage tiers, provisioning, migrating, cloning virtual machines and correct virtual machine placement in vSphere deployments have become more efficient and user friendly with VASA. It removes the need for maintaining complex and tedious spreadsheets and validating compliance manually during every migration or creation of a virtual machine or virtual disk.
WARNING: When using VASA functionality, EMC does not recommend preallocating thin devices once a datastore has been created on the device. Preallocation of the device beyond the predefined thresholds will cause the vCenter alarm to be triggered. This could result in an inability to create virtual machines on the datastore. If preallocation of space within the datastore is required, EMC recommends using eagerzeroedthick virtual disks.

Conclusion

With the introduction of VMware vSphere 5, VMware offers a new standard application programming interface for storage vendors to leverage in order to tightly and uniformly integrate specific array-based information into the VMware management interface. This API, called the vStorage API for Storage Awareness or VASA, is fully supported by the Symmetrix platform through the use of EMC’s SMI-S Provider (Storage Management Initiative Specification).

Managing storage tiers, provisioning, migrating, cloning virtual machines and correct virtual machine placement in vSphere deployments have become more efficient and user friendly with VASA. It removes the need for maintaining complex and tedious spreadsheets and validating compliance manually during every migration or creation of a virtual machine or virtual disk.

This white paper discussed how to install, configure and use VASA in VMware vSphere 5.x environments with Symmetrix DMX and VMAX storage arrays. An understanding of the principles that were exposed here should allow the reader to deploy and utilize VMware vSphere in the most effective manner.

References

- TechBook: Using EMC Symmetrix Storage in VMware vSphere Environments
- Release notes: SMI-S Provider Release Notes
  [https://support.EMC.com](https://support.EMC.com)
- VMware documentation on VMware.com
Appendix: VASA Registration Troubleshooting

This appendix will discuss some of the more common VASA registration errors that a user might experience and the possible resolutions. Before reviewing these common problems, be sure that the SMI-S Provider in use is from Solutions Enabler 7.x as Solutions Enabler 8.x is not supported.

Invalid certificate

An invalid VMware certificate is a common problem in VASA registration failures. Invalid simply means the certificate is expired. When registering the Provider, the error in Figure 28 is most closely associated with an expired certificate.

![Error]

**Figure 28. Registration failure due to expired VMware certificate**

If you have this error, checking if you have an expired certificate is very straightforward. Follow these steps:

1. On your vCenter host open a command prompt
2. Change the directory to C:\Program Files\Common Files\VMware\VMware vCenter Server – Java Components\bin (vSphere 5.5 host)
3. Run the following command: `keytool -keystore "C:\ProgramData\VMware\VMware VirtualCenter\SSL\sms.keystore" -storepass testpassword -list -v` 

This will produce an entry similar to Figure 29. Note the valid dates of the certificate are boxed in red:

```
e:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components\bin>keytool -keystore "c:\ProgramData\VMware\VMware VirtualCenter\SSL\sms.keystore" -storepass testpassword -list -v
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: sms
Creation date: Oct 23, 2012
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[/]
Owner: CN=SMS-121023061517564, O=VMware
Issuer: CN=SMS-121023061517564, O=VMware
Serial number: 1600334634
Certificate fingerprints:
MD5: BD:PC6GCEI:CI+YR+V9G164G7t65W2t+vY+92:Lm:1f:1E:
Signature algorithm name: SHA1withRSA
Version: 3
```

**Figure 29. VMware certificate output**

If the certificate is invalid/expired, a new one can be generated easily as follows:

4. Stop the *VMware VirtualCenter Management Webservices* service

5. Rename the existing sms.keystore and sms.truststore files located at
   `C:\ProgramData\VMware\VMware VirtualCenter\SSL\`

6. Restart the *VMware VirtualCenter Management Webservices* service

7. Wait a couple minutes for the files to regenerate, then try to register the provider again

VMware documents this process in the following KB article:


If the vCenter Server Appliance is used, the sms.keystore and sms.truststore files are located in the following directory: `/etc/vmware-vpx/ssl`. The keytool is automatically in the path of the root user.

**Invalid username or password**

Sometimes error messages are exactly what they say they are. In this case the wrong password is supplied and the error in Figure 30 is returned.
Generic VASA registration error

Unfortunately, the previous two error messages are not the only ones that can be generated. There is a generic error message seen in Figure 31 that is also very common.

Initially, there are two things to check when this error is produced. First, it is possible to receive this when the certificate is invalid so be sure to follow the section Invalid certificate. The other potential problem is that SMI-S has not discovered any VMAX arrays. The VASA Provider cannot be registered if the SMI-S does not see any arrays. The easiest way to check this on Unix/Linux/Windows is to run the SYMCLI command in Figure 32.
On Windows there is also an executable to test SMI-S: TestSmiProvider.exe located in C:\Program Files\EMC\ECIM\ECOM\bin. When running this executable, accept all prompted defaults. Then run the command “dv” to see the arrays as in Figure 33.

Figure 33. TestSmiProvider.exe

If the vApp for Solutions Enabler is used, the Appliance Info page has an operation to display the storage arrays. The red box highlights this in Figure 34.
Figure 34. Displaying arrays in the vApp

If neither the certificate nor the lack of arrays is the cause of the registration error, it may be necessary to open an SR with EMC Support to further debug the problem.

Importing a valid certificate

As discussed in the Invalid certificate section above, an expired certificate will cause registration problems. There are times, however, when the certificate’s validity is fine, but the provider cannot be registered. While extensive debugging is possible to find out the exact reason, one workaround is to simply import the VMware certificate manually through the ECOMconfig page. The process detailed below is more involved
than the previous troubleshooting methods, but it has shown to be very effective when other solutions have not been successful.

Importing the certificate will ensure that when the comparison is done on the ECOM side, the registration will succeed. In order to import the certificate, however, it must be in PEM format. This can be done with the keytool from the vCenter (vApp or Windows) and the executable openssl (Linux or Windows). The keytool will be on the vCenter by default but openssl will only be available on the vCenter vApp. It must be installed separately on Windows. The following steps will use the vCenter vApp:

1. Execute the following on the vApp to convert the VMware certificate into the PKCS12 format:

   ```
   keytool -importkeystore -srckeystore /etc/vmware-vpx/ssl/sms.keystore -destkeystore /etc/vmware-vpx/ssl/sms.pkcs -srcstoretype JKS -deststoretype PKCS12
   ```

   This command will ask for a password. It is “testpassword”. Figure 35 is an example. If an alias exists, as in this case, overwrite it.

   ![Figure 35. Converting VMware certificate into PKCS12 format](image)

   ```
   dsib2227:/etc/vmware-vpx/ssl # keytool -importkeystore -srckeystore /etc/vmware-vpx/ssl/sms.keystore -destkeystore /etc/vmware-vpx/ssl/sms.pkcs -srcstoretype JKS -deststoretype PKCS12
   Picked up JAVA_TOOL_OPTIONS: -Xms16M -Xmx128M
   Enter destination keystore password:
   Enter source keystore password:
   Existing entry alias sms exists, overwrite? [no]: yes
   Entry for alias sms successfully imported.
   Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
   dsib2227:/etc/vmware-vpx/ssl #
   ```

2. Now that the certificate is in PKCS12 format, it can be converted again into PEM format. The command to do that uses openssl:

   ```
   openssl pkcs12 -in /etc/vmware-vpx/ssl/sms.pkcs -out /etc/vmware-vpx/ssl/sms.pem
   ```

   This command will ask for a password once and a passphrase twice. It is “testpassword” for all. Figure 36 has a screenshot example of this:

   ![Figure 36. Converting PKCS12 certificate into PEM format](image)
3. Once the PEM format is available, it can be copied and imported. To do this, simply run a “more” on the file and copy the PEM format. It is highlighted in red in Figure 37.
Figure 37. Copying the PEM formatted certificate

4. Now import the certificate. Log into the ECOM website (https://<IP>:5989/ecomconfig) as the default admin user: admin/#1Password.

5. Once in, select “SSL Certificate Management” from the menu as in Figure 38.
ECOM Administration

ECOM Version 2.7.3.0.8 (Build Date & Time: Feb 7 2014, 15:57:21)
Logged in as admin

Logging:
Display Log File
Logging Options

Security:
Add User
Modify User
Change Password
Set Password quality
Delete User
List Users
Display Security Log File
Client IP Filtering
Local IP Filtering
SSL Certificate Management
LDAP Configuration
OSLogin Configuration

Dynamic Settings
Windows Authentication Protocol Configuration

Figure 38. SSL Certificate Management

6. In the next window, shown in Figure 39, choose to “Import CA certificate file”.
SSL Certificate Management

Option #1: Signed Certificate

Sign an ECOM generated Certificate Signing Request (CSR).

2. Export the PKCS#10 formatted Certificate Signing Request.
4. Import the signed certificate as PEM data.

See Wikipedia for more information about Certificate Signing Requests.

**Figure 39. Import CA certificate file**

7. Finally, paste the PEM certificate from step 3 into the box and submit the certificate shown below in Figure 40.

Option #2: Self Signed Certificate

Select this option to auto generate a self-signed certificate. A newly generated self-signed certificate will replace the currently used one. The certificate’s Subject information will contain the defaults.

**Figure 39. Import CA certificate file**
Submit CA Certificate

See Wikipedia for more information about PEM format.

```
-----BEGIN CERTIFICATE-----
MIIBzCAUCAgIwIBAgIGAUSWTCk2nMADGCSqGSIb3DQEBAQUAA4XKCmMBoGA1UEN
8sFy2TEcHwAxAjUEAUNMTU01TLEOMQyNDEzMTMyNDU4MzAeFw0xMzAOMjQx
MTEzNjRaFw0yNDQAMjQxMTEzNjRaMC8xMzAANBgNVBAoTS1Z2d2Fy2TEcHwA
AxMTU01TLEOMQyNDEzMTMyNDU4MzCBzANBgkqhkiG9w0BQFAwDAQgYcC
qYEA1Qmk4DKK01XNWIHRQRV0ZIFnVHe1apBtFy21yJvA5TDPwPylaoUSKb
Uo8SCm9/Ac4WTL4R1cLoPchbXZ9uiFiu17rYp/mGi4FI/YvEcVnCYb9gQyqyobo
Kufq2beHDEdPtwWbSNPOOGcPHs5xG8EcEIYcaZTwtmtx2zMCIwEAATANBgkqhkiG
9w0BAQJFAQAOBgQAihw2b2CR+nH2LH0/9Du4CGQkZT8oA5P01y5eH1SB50UFShO
mUAUkw7VGCXAu4JSIqmozEMpSp4pSTOO0Uw2TnUD2Z9HW68gs9ur8id46zJBCgeT
vXcFds8bcDu8Xlrcx325FRS3xSOjxXjm4oIDeCiHU1y9BuCyDdp1DaFuSO==
-----END CERTIFICATE-----
```

Figure 40. Submit CA Certificate

8. Retry the VASA registration once complete. Note that if you are registering more than one vCenter and the second vCenter fails to register after this procedure, you can paste multiple certificates into the box in step 7 and try again.

If this fails to work, open an SR with EMC Support to further debug the problem.