Abstract
This white paper explains how to install, configure and use EMC’s implementation of VMware’s Storage API for Storage Awareness 1.0 (VASA) with vSphere 5 and 6 and VMAX storage arrays.

May 2017
# Table of Contents

Executive summary .................................................................................................................. 4

SMI-S and VASA ................................................................................................................. 4

Installation and Configuration ............................................................................................... 5
  Installation of the VASA Provider ....................................................................................... 6
  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

Using VASA 1 capabilities with vSphere 6 ....................................................................... 32
  VASA 1 capabilities in VASA 2 ....................................................................................... 32
  Storage Policies .............................................................................................................. 32
    Creating a Storage Policies ............................................................................................ 35
    Identifying Capability Sets ........................................................................................... 43

Conclusion ............................................................................................................................ 44

References ............................................................................................................................ 44

Appendix A: VASA Registration Troubleshooting in vSphere 5 ...................................... 45
  Invalid certificate .............................................................................................................. 45
  Invalid username or password .......................................................................................... 46
  Generic VASA registration error ......................................................................................... 47
  Importing a valid certificate ............................................................................................... 49

Appendix B: Extracting the Certificate from the Network .................................................. 55
  Implementation ................................................................................................................. 56
  VASA Registration .......................................................................................................... 61
  Export Certificate ............................................................................................................ 61
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.

Starting in VMware vSphere 5, VMware offers an 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 VMAX 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™1 and VMAX™ storage arrays and in VMware vSphere 6 environments with EMC VMAX3 and VMAX All Flash 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.

1 Supported with EMC Enginuity™ version 5568 or higher.
Collectively, these standards strive to ensure consistent data and eliminate inconsistencies among management tools by providing a unified interface to the 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 VMAX 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 for vSphere 5 and 8.4 for vSphere 6. 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 VMAX arrays. This paper focuses on the use of VASA with VMAX storage.

EMC's VASA Provider enables VMAX 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 VMAX 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.

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.

This section will cover the installation of the VASA 1 Provider that is delivered with Solutions Enabler 7.x and supports vSphere 5. The VASA 2 Provider which supports vSphere 6 is not part of Solutions Enabler. It is delivered as a virtual appliance and can be downloaded from support.EMC.com. The installation of that software is covered in the whitepaper *Using VMware Virtual Volumes with EMC VMAX3 and VMAX All Flash* available on EMC.com.
The SMI-S Provider in Solutions Enabler 8.x does not offer VASA 1.x capabilities. The VASA Provider 8.x is required.

**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.

![Figure 1. 64-bit Windows SMI-S installation wizard](image)

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.
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 VMAX 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.x 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, 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)
**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.

![Figure 4. Security settings XML file location](image)
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>:5989/ecomconfig

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

---

2 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.
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**

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”.
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 VMAX information, access to the desired arrays must be granted to the provider. VMAX 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 VMAX Engineering) from each respective VMAX should be presented to the provider.

---

**Figure 8. Creating a user for the VASA provider**

<table>
<thead>
<tr>
<th>Add User:</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Re-Enter Password:</td>
</tr>
<tr>
<td>Role:</td>
</tr>
<tr>
<td>Scope:</td>
</tr>
<tr>
<td>Password never expires:</td>
</tr>
</tbody>
</table>

---

**Table:**

<table>
<thead>
<tr>
<th>Role</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>security/administrator</td>
</tr>
<tr>
<td>manager</td>
<td>vmadmin</td>
</tr>
<tr>
<td>monitor</td>
<td>vmmuser</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

---

*Add User:*  

*Back to ECOM Config Page*
SMI-S Provider server\(^3\). 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.

---

\(^3\) 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.

   \[\text{https://SMI-S Provider server name or IP address}:5989/vasa/services/vasaService}\]

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

---

4 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.

![Vendor Provider Operations](image)

**Figure 12. Vendor provider operations**
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 follow two 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 VMAX 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...
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 VMAX 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

---

5 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 the VMAX. 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.

6 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.
environment is using a VMAX10K exclusively, only the storage capabilities that are specific to thin devices will be shown.

Figure 13. EMC system-defined storage capabilities

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

7 The SMI-S Provider must have access to the VMAX 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.
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.

---

8 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\(^9\) 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.

---

\(^9\) 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
Figure 17. Assigning storage capabilities to a storage profile

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.
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
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**: 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, 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 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.
Figure 23. Checking compliance for an entire storage profile

Thin-device capacity alarm

Within vSphere 5 and 6 there is an alarm definition for VASA. It is named “Thin-provisioned volume capacity threshold exceeded” and will be triggered if the thin volume on the VMAX 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.

---

10 Prior to vSphere 5.1 this alarm was named “Thin-provisioned LUN capacity exceeded.”
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” in the vSphere thick client and in Figure 26 for the vSphere Web Client.

Figure 25. Thin-provisioned volume alarm in vCenter – vSphere thick client
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 27 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 VMAX, the SMI-S Provider takes advantage of the events that are automatically recorded by the event daemon on the VMAX. 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 VMAX 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 28 where the default alert for thin device allocation (named Thin Pool Utilization) is highlighted. The default alert cannot be altered - attempts to edit it will result in the error in the dialog box of Figure 28. Users can, however, create specific alerts for particular thin pools which will supersede the default alert.

![EMC Unisphere for VMAX](image)

**Figure 28. 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. This is extremely important as more customers move to a thin on thin model for their environments. The thin volume alarm is only one of the ways that the vSphere Storage APIs for Storage Awareness can provide insight for the VMware administrator into the VMAX 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.

### Using VASA 1 capabilities with vSphere 6

**VASA 1 capabilities in VASA 2**

EMC's VASA 2 implementation (delivered through VASA Provider 8.x) includes VASA 1 capabilities. VASA 1 assigns the capability set of VMAX3/VMAX All Flash VMFS datastores according to the SLOs assigned to the storage group. Storage policies can be created with rule sets that associate it with a particular SLO/SL.

EMC's VASA Provider 8.x enables VMAX3/VMAX All Flash management software to inform vCenter of how VMFS storage is configured and protected for VASA 1 capabilities. For VASA 1 with VMAX3/VMAX All Flash, these capabilities are defined by EMC and include the SLOs available on the array. This insight allows vSphere administrators to make quick, intelligent, and informed decisions as to virtual machine placement. The VASA 1 capability offers the ability for vSphere administrators to complement their use of plugins and other tools to track how VMAX3/VMAX All Flash devices hosting VMFS volumes are configured to meet performance and availability needs.

The VASA Provider 8.x only supports VASA 1 capabilities for the VMAX3 and VMAX All Flash arrays and can only be utilized in vSphere 6.x.

There is no support for cascaded auto provisioning groups when using VASA 1 capabilities. For example, if devices backing datastores are part of a child storage group, the VASA Provider will be unable to recognize the SLO associated with the group.

### Storage Policies

Managing datastores and matching the Service Level Agreement requirements of virtual machines with the appropriate datastore can be a challenging and cumbersome task. Storage policies provide a mechanism by which VM users can ensure that the proper datastore is selected when provisioning, cloning or using Storage vMotion. Using storage policies reduce the amount of manual administration
Storage policies are built on the storage capabilities provided by the VMAX3/VMAX All Flash. The VASA Provider 8.x correlates VMAX3/VMAX All Flash devices with the capabilities designated in the provider. Currently, only one capability can be assigned to a device by VASA. The storage capabilities advertised by the EMC VASA Provider 8.x for VASA 1 are the same as those for VASA 2 and can be found listed in in Table 2 for VMAX3/VMAX All Flash and detailed in Figure 29 and Figure 30 below.

Table 2. VMAX3 storage capabilities in vSphere

<table>
<thead>
<tr>
<th>SystemLabel</th>
<th>Optimized</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
<th>Diamond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bronze+OLTP</td>
<td>Silver+OLTP</td>
<td>Gold+OLTP</td>
<td>Platinum+OLTP</td>
<td>Diamond+OLTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bronze+OLTP_REP</td>
<td>Silver+OLTP_REP</td>
<td>Gold+OLTP_REP</td>
<td>Platinum+OLTP_REP</td>
<td>Diamond+OLTP_REP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bronze+DSS</td>
<td>Silver+DSS</td>
<td>Gold+DSS</td>
<td>Platinum+DSS</td>
<td>Diamond+DSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bronze+DSS_REP</td>
<td>Silver+DSS_REP</td>
<td>Gold+DSS_REP</td>
<td>Platinum+DSS_REP</td>
<td>Diamond+DSS_REP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Service Level Objective (SLO) is a desired level of performance (response time band) required by the storage workload.

<table>
<thead>
<tr>
<th>Expected Average Response Time</th>
<th>Optimized</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
<th>Diamond</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Optimized</td>
<td>14.0 ms</td>
<td>8.0 ms</td>
<td>5.0 ms</td>
<td>3.0 ms</td>
<td>&lt; 1 ms</td>
<td></td>
</tr>
</tbody>
</table>

Small I/O
- OLTP
- OLTP + Replication
  - 14.0 ms
  - 15.5 ms
  - 8.0 ms
  - 9.5 ms
  - 5.0 ms
  - 6.5 ms
  - 3.0 ms
  - 4.4 ms
  - 0.8 ms
  - 2.3 ms

Large I/O
- DSS
- DSS + Replication
  - 15.5 ms
  - 16.9 ms
  - 9.5 ms
  - 10.9 ms
  - 6.5 ms
  - 7.9 ms
  - 4.4 ms
  - 5.9 ms
  - 2.3 ms
  - 3.7 ms

Figure 29. VMAX3 storage capabilities in Unisphere

---

11 The bolded labels in the Diamond column are those SLs available on VMAX All Flash.
Service Level is a desired level of performance (response time band) required by the storage workload.

**Expected Average Response Time**

Hide Details

<table>
<thead>
<tr>
<th>Small I/O</th>
<th>OLTP</th>
<th>OLTP + Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large I/O</td>
<td>DSS</td>
<td>DSS + Replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

< 1 ms

0.8 ms

2.3 ms

2.3 ms

3.7 ms

**Figure 30. VMAX All Flash storage capabilities in Unisphere**

After the storage provider is registered, the datastores that can be assigned capability sets, will be recognized. Note that the EMC VASA Provider 8.x only supports a single array. Therefore if there are multiple VMAX3/VMAX All Flash arrays in the VMware environment that require a storage policy capability, there must be a VASA Provider for each one. Be sure to register each provider in vCenter, demonstrated in Figure 31.
Figure 31. Registering multiple EMC VASA Providers 8.x

Creating a Storage Policies

The following section walks through the creation of a storage policy in vSphere 6.5 using the VASA 1 capabilities in the VASA Provider 8.x.

VM Storage Policy Step 1

Start by accessing the VM Storage Policies icon in the Home page of the vSphere Web Client as shown in Figure 32.
Figure 32. Creating a VM Storage Policy - step 1

VM Storage Policy Step 2

Next in step 2 in Figure 33 select the icon under the VM Storage Policies tab to create a new VM storage policy.
VM Storage Policy Step 3

Step 3 (step 1 of the wizard) formally starts the wizard. If the environment shares a Platform Service Controller then begin by selecting the appropriate vCenter. Enter a name for the policy, preferably one that reflects the capabilities that will be associated with the policy as this is the name the VMware user will see. Finally if desired enter a description. An example is shown in Figure 34.

VM Storage Policy Step 4

Step 4 is actually not a step at all as it simply describes the Policy structure. It is included here in Figure 35 for reference and continuity.
Figure 35. Creating a VM Storage Policy - step 4

There are two parts to the Policy structure. The first is the Common rules. This is where VM Encryption and/or SiOC can be configured. Figure 36 shows these options. Since this is not being used in this example, it is considered part of step 4.

Figure 36. Creating a VM Storage Policy - step 4
VM Storage Policy Step 5

Step 5 covers assigning the Rule Set. The EMC VASA Provider 8.x advertises two different data services:

- VmaxVVolProvider
- VmaxVVolVasaProvider.VASA10

The difference between the two services is straightforward – the first supports VASA 2 and VVol functionality while the second supports the older VASA 1 capabilities. As this section concerns VASA 1, the VmaxVVolVasaProvider.VASA10 is used. Therefore select the VmaxVVolVasaProvider.VASA10 as demonstrated in Figure 37.

![Figure 37. Creating a VM Storage Policy - step 5](image)

VM Storage Policy Step 6

Once the data service is selected, the advertised capabilities may be added as rules for the policy. Through the VASA Provider 8.x the VMAX3, or in this case the VMAX All Flash, presents the different Service Levels (SL) as the capabilities. It is comprised of a single rule from a VMware perspective: SystemLabel.label. Start by selecting SystemLabel.label from the drop-down box as in Figure 38.
Figure 38. Creating a VM Storage Policy - step 6

VM Storage Policy Step 7

In step 7, Figure 39, one can see all the SLs available from the provider in the drop-down list. Note that the list comprises all possible SLs from both VMAX3 and VMAX All Flash. Select an SL that is assigned to one of the storage groups presented to the vCenter. In this example Diamond+DSS is chosen.
Figure 39. Creating a VM Storage Policy - step 7

VM Storage Policy Step 8

Step 8 in Figure 40 shows the completed policy assignment.

Figure 40. Creating a VM Storage Policy - step 8
VM Storage Policy Step 9

VMware now takes the supplied parameters and compares it against the available VMFS datastores to see if any are compatible. In Figure 41 the Diamond_DSS datastore is compatible with the Diamond+DSS SL.

Figure 41. Creating a VM Storage Policy - step 9

VM Storage Policy Step 10

A summary page in Figure 42 completes the VM Storage Policy.
Figure 42. Creating a VM Storage Policy - step 10

Now each time a VM is created, this policy can be chosen to ensure the correct datastore is selected for the new VM.

Identifying Capability Sets

Regardless of whether storage policies have been created, VMware is able to display the capability set (SL) of a VMFS datastore once the VASA Provider is registered. Within the vSphere Web Client, highlight the datastore, select the Configure tab, and in the left-hand menu select Capability sets. On the right-hand side the SL associated with that device will be displayed as in Figure 43. In this case, the volume underlying the Diamond_DSS datastore has been recognized as a device in a storage group with the Diamond+DSS SL. This feature can be used to help create the storage policies if the SL has not been communicated ahead of time to the VMware administrator.

---

12 There is a known VMware bug that if the SLO of a storage group is changed, the former SLO will still show as a capability set along with the new SLO. However, VMware will not use the former SLO to determine if a datastore is compatible with a storage policy.
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 Storage API for Storage Awareness or VASA, is fully supported by the VMAX 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 and 6 environments with 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 VMAX Storage in VMware vSphere Environments  
- Release Notes: SMI-S Provider Release Notes  
  https://support.EMC.com
- VMware documentation on VMware.com  
  https://www.vmware.com/support/pubs
Appendix A: VASA Registration Troubleshooting in vSphere 5

This appendix will discuss some of the more common VASA registration errors that a user might experience and the possible resolutions in vSphere 5. 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 in vSphere 5.

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 44 is most closely associated with an expired certificate.

![Registration failure due to expired VMware certificate](image)

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 45. Note the valid dates of the certificate are boxed in red:

   ![Certificate Output](image)

   **Figure 45. 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 46 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 47 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 48.
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 49.

Figure 49. 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 50.
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 51 is an example. If an alias exists, as in this case, overwrite it.

   ![Figure 51. Converting VMware certificate into PKCS12 format](image)

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 52 has a screenshot example of this.
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 53.
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 54.
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 54. SSL Certificate Management

6. In the next window, shown in Figure 55, choose to “Import CA certificate file”.

SSL Certificate Management

Option #1: Signed Certificate

Sign a 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.

Generate a Certificate Signing Request

Import Signed Certificate

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.

Generate a Self-Signed Certificate

Option #3: Import CA certificate file

Select this option to import the CA certificate file (as PEM data).

Import CA certificate file

Figure 55. Import CA certificate file

7. Finally, paste the PEM certificate from step 3 into the box and submit the certificate shown below in Figure 56.
Submit CA Certificate

See Wikipedia for more information about PEM format.

-----BEGIN CERTIFICATE-----
MIIBizCCAUgAwIBAgIGAWEc2F5EyxxMTEuNjIyMzA5MzIzNTQxMDcwNDA2MDM4e当然，您还可以在步骤7中粘贴多个证书并再次尝试。如果这还不能解决问题，可以打开EMC支持的SR以进一步调试问题。

Appendix B: Extracting the Certificate from the Network

This appendix explains how to extract the certificate that VMware vCenter sends to the ECOM server when the ECOM server is running on Microsoft Windows. Unfortunately, this method cannot be used on the vApp. Normally the vCenter...
certificate can be obtained directly from the vCenter and converted into the proper PEM format for import into ECOM as explained in Appendix A: VASA Registration Troubleshooting; however there have been cases where the certificate being sent is in question and only through network tracing can it be obtained.

**Implementation**

In order to obtain the certificate, a third-party software is required which will allow the network to be traced or “sniffed.” In the example below, the software being used is called Wireshark™. Navigate to the URL in Figure 57 and select the 64-bit version of the software.

---

This example uses an older version of Wireshark. Though the user interface will be different in more recent versions, the functionality will be equivalent.
Install Wireshark taking all the defaults. Simply click through the install leaving all boxes checked. After installation start Wireshark. On the main page select “Start” as in Figure 58.
The main Wireshark capture screen will appear similar to Figure 59.

Figure 58. Starting Wireshark

The main Wireshark capture screen will appear similar to Figure 59.

Figure 59. Wireshark - Capture screen
From this screen stop the current capture as shown above. A two-step change will be required before capture is restarted. Go to **Edit -> Preferences** and expand **Protocols** in step 1 in Figure 60.

![Wireshark: Preferences - Profile: Default](image)

**Figure 60. Wireshark – Protocols – step 1**

Scroll down and highlight the HTTP protocol and on the right-hand screen add 5989 to the SSL/TLS Ports and click OK in step 2 in Figure 61:
Now restart the capture as in Figure 62:

Figure 62. Wireshark – Restart capture
VASA Registration

After starting the new capture, immediately try to register the VASA Provider in the vCenter. As soon as it fails, return to Wireshark and stop the capture.

Export Certificate

At this point we need to export the certificate out of the trace in a two-step process. Scroll down the capture fields and find the entry that has in the Info column “Certificate, Client Key Exchange”. The Source column should be the vCenter IP and the Destination column should be the ECOM server. Once highlighted, expand the “Secure Sockets Layer” in the bottom screen until you find the highlighted entry as shown in step 1 of Figure 63:

![Wireshark - Export certificate - step 1](image)

Figure 63. Wireshark – Export certificate – step 1

With the entry highlighted, as in step 2 in Figure 64, right-click on it and select the “Export Selected Packet Bytes…” Save the file with an extension of “.der”.

61
The certificate .der file must now be converted to PEM format so we can see what the certificate looks like. To do this we need the binary “openssl”. This binary can be downloaded to Windows however if there is a Linux environment simply SFTP the .der file over to that box and run the following:

```
openssl x509 -inform DER -in <file-name>.der -outform PEM
```

When you run the command, it will display the certificate in PEM format on the screen as in Figure 65.
Now compare this output with the certificate on the ECOM server. If they are different, then copy and paste this certificate into ECOM, as shown in the previous appendix in the section *Importing a valid certificate*, to ensure it will match when you re-register.