



# **Virtual Storage Console, VASA Provider, and Storage Replication Adapter for VMware vSphere**

Deployment and Setup Guide for 7.0 release

October 2017 | 215-12442\_DO  
doccomments@netapp.com



# Contents

<b>Overview of virtual appliance for VSC, VASA Provider, and SRA .....</b>	<b>6</b>
VSC for VMware plug-ins .....	7
Overview of the NFS plug-in for VAAI .....	7
Architecture of the virtual appliance for VSC, VASA Provider, and SRA .....	8
<b>Deployment workflows for users of the virtual appliance for VSC, VASA Provider, and SRA .....</b>	<b>9</b>
Deployment workflow for new users of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) virtual appliance .....	10
Deployment workflow for existing users of VSC, VASA Provider, and SRA .....	11
Deployment workflow for existing users of VSC .....	11
Deployment workflow for existing users of VASA Provider .....	12
Deployment workflow for existing users of SRA .....	12
<b>Deployment requirements for the virtual appliance for VSC, VASA Provider, and SRA .....</b>	<b>14</b>
Virtual Storage Console port requirements .....	14
Host requirements for the virtual appliance for VSC, VASA Provider, and SRA ....	14
Supported storage system and applications for 7.0 virtual appliance for VSC, VASA Provider, and SRA .....	15
Considerations for deploying the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA .....	15
<b>Overview of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) deployment .....</b>	<b>19</b>
Downloading the virtual appliance for VSC, VASA Provider, and SRA .....	19
Deploying the virtual appliance for VSC, VASA Provider, and SRA .....	20
Enabling extensions for the virtual appliance for VSC, VASA Provider, and SRA .....	21
Installing the NFS plug-in for VAAI .....	22
<b>Configuring your Virtual Storage Console for VMware vSphere environment .....</b>	<b>24</b>
ESXi server and guest operating system setup .....	24
Configuring ESXi server multipathing and timeout settings .....	24
Timeout values for guest operating systems .....	27
Regenerating an SSL certificate for Virtual Storage Console .....	31
Performing VSC for VMware vSphere tasks across multiple vCenter Servers .....	32
Preferences files .....	33
Enabling datastore mounting across different subnets .....	33
Accessing the maintenance console options of the virtual appliance for VSC, VASA Provider, and SRA .....	34
<b>Overview of storage system discovery and storage credentials .....</b>	<b>36</b>
Setting default credentials for storage systems .....	37
Manually adding storage systems .....	38

Discovering storage systems and hosts .....	39
Refreshing the storage system display .....	40
<b>vCenter Server role-based access control features in VSC for</b>	
<b>VMware vSphere .....</b>	<b>42</b>
Components of vCenter Server permissions .....	42
Key points about assigning and modifying permissions .....	43
Standard roles packaged with the virtual appliance for VSC, VASA Provider,	
and SRA .....	44
Guidelines for using VSC standard roles .....	45
Privileges required for VSC tasks .....	46
Product-level privilege required by VSC for VMware vSphere .....	46
ONTAP role-based access control for the virtual appliance for VSC,	
VASA Provider, and SRA .....	47
Recommended ONTAP roles when using VSC for VMware vSphere .....	48
How to configure ONTAP role-based access control for VSC for	
VMware vSphere .....	49
<b>Enabling VASA Provider for configuring virtual datastores .....</b>	<b>50</b>
VASA Provider for ONTAP overview .....	50
<b>Configuring VSC, VASA Provider, and SRA for disaster recovery .....</b>	<b>52</b>
Setting up initial configurations for Storage Replication Adapter .....	52
Configuring Storage Replication Adapter for SAN environment .....	52
Configuring Storage Replication Adapter for NAS environment .....	53
<b>Upgrade overview of Virtual Storage Console, VASA Provider, and</b>	
<b>Storage Replication Adapter .....</b>	<b>54</b>
Unregistering VSC from a Windows setup .....	54
Migrating existing VSC installation to the 7.0 version of the virtual appliance	
for VSC, VASA Provider, and SRA .....	56
Migrating existing VASA Provider installation to the 7.0 version of the virtual	
appliance for VSC, VASA Provider, and SRA .....	57
Upgrading from Storage Replication Adapter 4.0 to the 7.0 version of the	
virtual appliance for VSC, VASA Provider, and SRA .....	58
<b>Troubleshooting VSC, VASA Provider, and SRA virtual appliance .....</b>	<b>60</b>
Information at NetApp Support Site .....	60
Information available at VSC NetApp Communities Forum .....	60
Collecting the VSC, VASA Provider, and SRA virtual appliance log files .....	60
Unrecognized storage systems issue .....	60
Uninstall does not remove standard VSC roles .....	61
Error while accessing the virtual appliance Summary page .....	62
Troubleshooting information in log files .....	62
VASA Provider known issues and limitations .....	62
VASA Provider registration fails with vCenter Server 6.5 .....	62
VVOL datastore provisioning fails with vCenter Server 6.5 .....	63
Resolving VASA Provider registration issues .....	63
Unable to add storage to VVOL datastore created using the VMware	
wizard .....	65

Configuring VASA Provider to work with SSH .....	65
Configuring 7.0 virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to use SSH for remote diag access .....	65
SRA fails to perform optimally in a highly scaled environment .....	66
<b>Copyright information .....</b>	<b>67</b>
<b>Trademark information .....</b>	<b>68</b>
<b>How to send comments about documentation and receive update notifications .....</b>	<b>69</b>
<b>Index .....</b>	<b>70</b>

## Overview of virtual appliance for VSC, VASA Provider, and SRA

---

Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) for VMware vSphere is a virtual appliance and is a product suite that includes the capabilities of VSC, VASA Provider, and SRA.

The product suite includes SRA and VASA Provider as plug-ins for vCenter Server, which provide end-to-end lifecycle management for VMware virtual server environments running on NetApp storage and the VMware vSphere Web Client. The virtual appliance for VSC, VASA Provider, and SRA integrates smoothly with the VMware vSphere Web Client and enables you to use single sign-on (SSO) services. In a multiple vCenter Server environment, each vCenter Server instance has its own registered instances of VSC and VASA Provider. The VSC dashboard page enables you to quickly check the overall status of your datastores and virtual machines.

**Note:** The NetApp blue "N" icon in the screens and portlets enables you to easily distinguish the NetApp features from the VMware features.

By running the virtual appliance for VSC, VASA Provider, and SRA, you can perform the following tasks:

- **Using VSC to manage storage and configure the ESXi host**
  - You can use VSC to add, remove, and assign credentials, and to set up permissions for storage controllers within your VMware environment.  
In addition, you can manage the ESXi servers that are connected to NetApp storage. You can set values for host timeouts, NAS, and multipathing. You can also view storage details and collect diagnostic information.
  - You can add Storage Virtual Machines (SVMs) and clusters to VSC and SRA.  
VASA Provider works only with cluster credentials.
  - You can monitor the performance of the datastores and virtual machines in your vCenter Server environment by using the Summary and Reports page of the VSC GUI.  
Any issues with storage systems and host systems are displayed on the dashboard. The predefined reports provide performance details of the datastores and virtual machines that are managed by VSC.
- **Using VASA Provider to create storage capability profiles and to set alarms**  
VASA Provider for ONTAP is registered with VSC as soon as you enable the VASA Provider extension. You can create and use storage capability profiles and virtual volume (VVOL) datastores. You can also set alarms to warn you when the thresholds for volumes and aggregates are approaching full.
- **Using SRA for disaster recovery**  
You can use SRA to configure protected and recovery sites in your environment for disaster recovery in the event of a failure.

You can configure and use VSC, VASA Provider, and SRA in the following combinations:

- VSC only (default configuration)
- VSC and VASA Provider
- VSC and SRA
- VSC, VASA Provider, and SRA

The configuration that you select depends on what tasks you want to perform by using VSC, VASA Provider, and SRA.

To enable administrators to control access to the vCenter Server objects and to secure the system, VSC supports role-based access control (RBAC) at two levels:

- vSphere objects, such as virtual machines and datastores  
These objects are managed by using vCenter Server RBAC.
- ONTAP storage  
Storage systems are managed by using ONTAP RBAC.

If access control is not an issue, you can log in as an administrator and access all the features that VSC provides.

**Tip:** The View privilege is required for all users who do not have administrator privileges. Without this privilege, these users cannot see the GUI of the virtual appliance for VSC, VASA Provider, and SRA.

## VSC for VMware plug-ins

Virtual Storage Console for VMware vSphere supports optional plug-ins and virtual appliances that work with various Virtual Storage Console (VSC) features. You can enhance the capabilities of VSC by enabling the NFS Plug-in for VAAI and VASA Provider for ONTAP. You can also enable the Storage Replication Adapter (SRA) extension to configure disaster recovery for your vCenter Server instance.

VSC provisioning operations benefit from using the NFS Plug-in for VMware VAAI. The plug-in integrates with VMware Virtual Disk Libraries to provide VMware vStorage APIs for Array Integration (VAAI) features, including copy offload and space reservations.

VASA Provider is a virtual appliance that improves storage management and supports virtual volumes (VVols). It provides information to the vCenter Server instance about the NetApp storage systems that are being used in the VMware environment. Integrating VASA Provider with the vCenter Server instance enables you to make more informed decisions. For example, you can create storage capability profiles that define different storage service level objectives (SLOs) for your environment. You can then use these SLOs to select a datastore with the correct storage attributes when provisioning virtual machines. You can also set up alarms to notify you when a volume or an aggregate is nearing full capacity or when a datastore is no longer in compliance with its associated SLO.

When SRA is enabled and configured in your vCenter Server environment, you can recover the vCenter Server datastores and virtual machines in the event of a failure. VSC provides a dashboard that enables you to monitor all of the datastores and virtual machines that are managed by VSC. You can view the performance of the datastores and virtual machines in your vCenter Server environment by using the predefined VSC reports.

## Overview of the NFS plug-in for VAAI

The NetApp Plug-in for VMware vStorage APIs for Array Integration (VAAI) is a software library that integrates the VMware Virtual Disk Libraries that are installed on the ESXi host. The VMware VAAI package enables the offloading of certain tasks from the physical hosts to the storage array.

You can perform tasks such as thin provisioning and hardware acceleration at the array level to reduce the workload on the ESXi hosts. The copy offload feature and space reservation feature improve the performance of Virtual Storage Console (VSC) operations. The NetApp NFS Plug-in for VAAI is not shipped with VSC. You can download the plug-in installation package and obtain the instructions for installing the plug-in from the NetApp Support Site. You can complete your installation from the VSC **Tools > NFS VAAI** page .

[mysupport.netapp.com](http://mysupport.netapp.com)

See the NetApp Interoperability Matrix Tool (IMT) for the supported versions of ESXi, vSphere, and ONTAP.

[NetApp Interoperability Matrix Tool](#)

## Architecture of the virtual appliance for VSC, VASA Provider, and SRA

The architecture of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) involves the storage system running ONTAP, the vCenter Server, the VMware vSphere Web Client, and the ESXi hosts.

The virtual appliance for VSC, VASA Provider, and SRA uses VMware-recommended, web-based architecture. The virtual appliance consists of two major components:

- A graphical user interface (GUI) web application that is displayed as a plug-in within the vSphere Web Client to provide a single management console for virtual environments
- A server component that is controlled by the VSC service and that hosts Java servlets to handle the GUI and API calls to the storage systems and the ESXi hosts

When you run VSC, you use the VMware vSphere Web Client and the VMware vCenter Server instance. Each VSC instance and VASA Provider instance must be registered with only one vCenter Server instance. Each SRA instance is registered with Site Recovery Manager (SRM), which is registered with vCenter Server.

The vSphere Web Client and any plug-in applications that are deployed in the vCenter Server use the HTTPS protocol to communicate with each other.

The vCenter Server instance communicates with the physical servers where the ESXi hosts are running. You can have multiple virtual machines running on the ESXi hosts. Each virtual machine can run an operating system and applications. The ESXi hosts then communicate with the storage systems. You can use the virtual appliance for VSC, VASA Provider, and SRA to enable the VASA Provider extension and the SRA extension. If you want to configure virtual volumes (VVols), then you must enable the VASA Provider extension. If you want to configure disaster recovery for your vCenter Server environment, you must enable the SRA extension. While configuring the disaster recovery setup, you must install the SRA plug-in on the SRM instance that is installed in your vCenter Server. Depending on what tasks you want to perform, you can enable or disable the required extensions by using the interface of the virtual appliance for VSC, VASA Provider, and SRA .



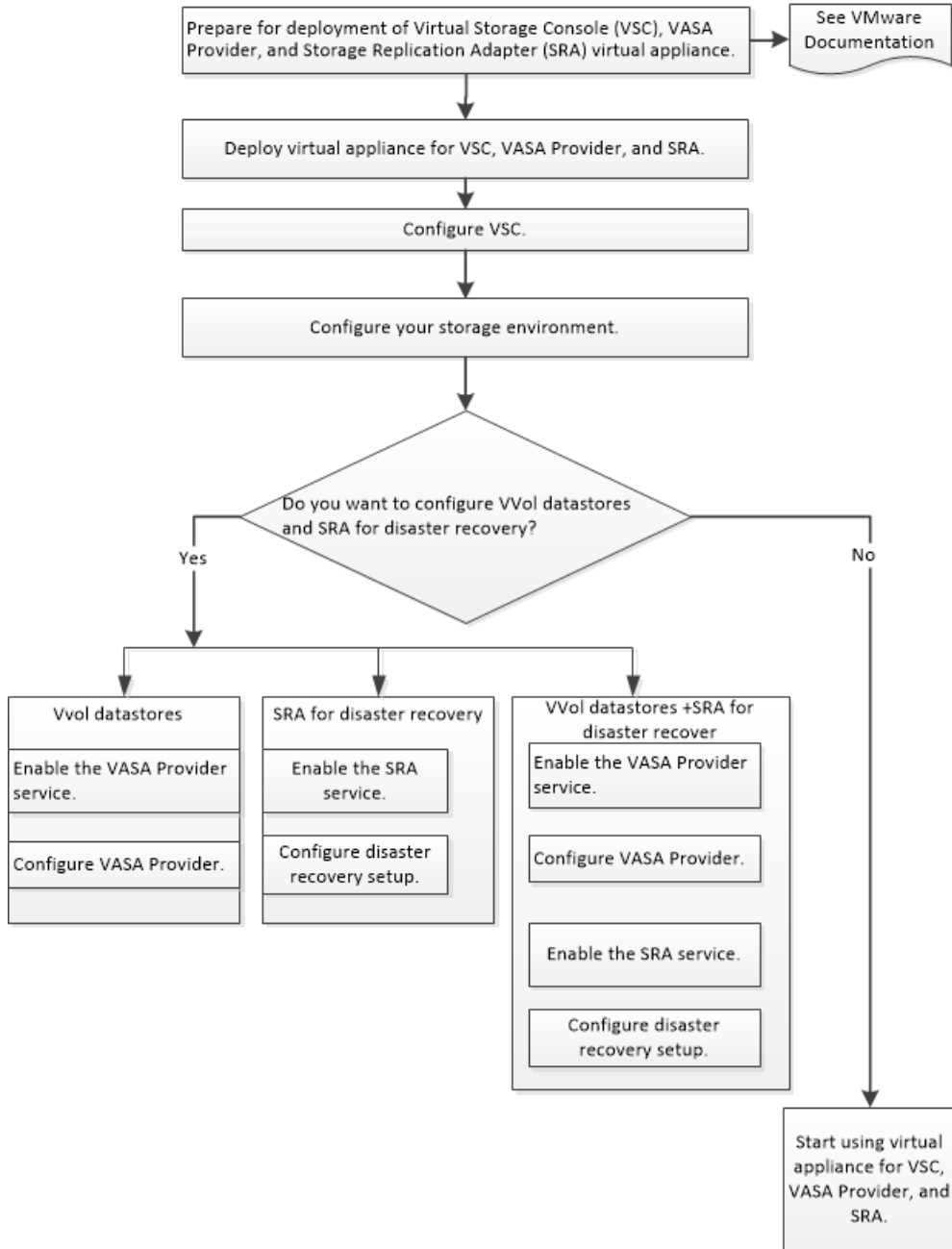
## **Deployment workflows for users of the virtual appliance for VSC, VASA Provider, and SRA**

---

If you have an existing vCenter Server setup with Virtual Storage Console (VSC) in isolation, or with VSC in combination with either VASA Provider or Storage Replication Adapter (SRA), or in combination with both, and you want to upgrade to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, then you should refer to the deployment workflows that are relevant to your deployment scenario.

## Deployment workflow for new users of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) virtual appliance

If you are new to VMware and have never used a NetApp VSC product, you need to configure your vCenter Server and setup an ESXi host, before you deploy and configure the virtual appliance for VSC, VASA Provider, and SRA.



## Deployment workflow for existing users of VSC, VASA Provider, and SRA

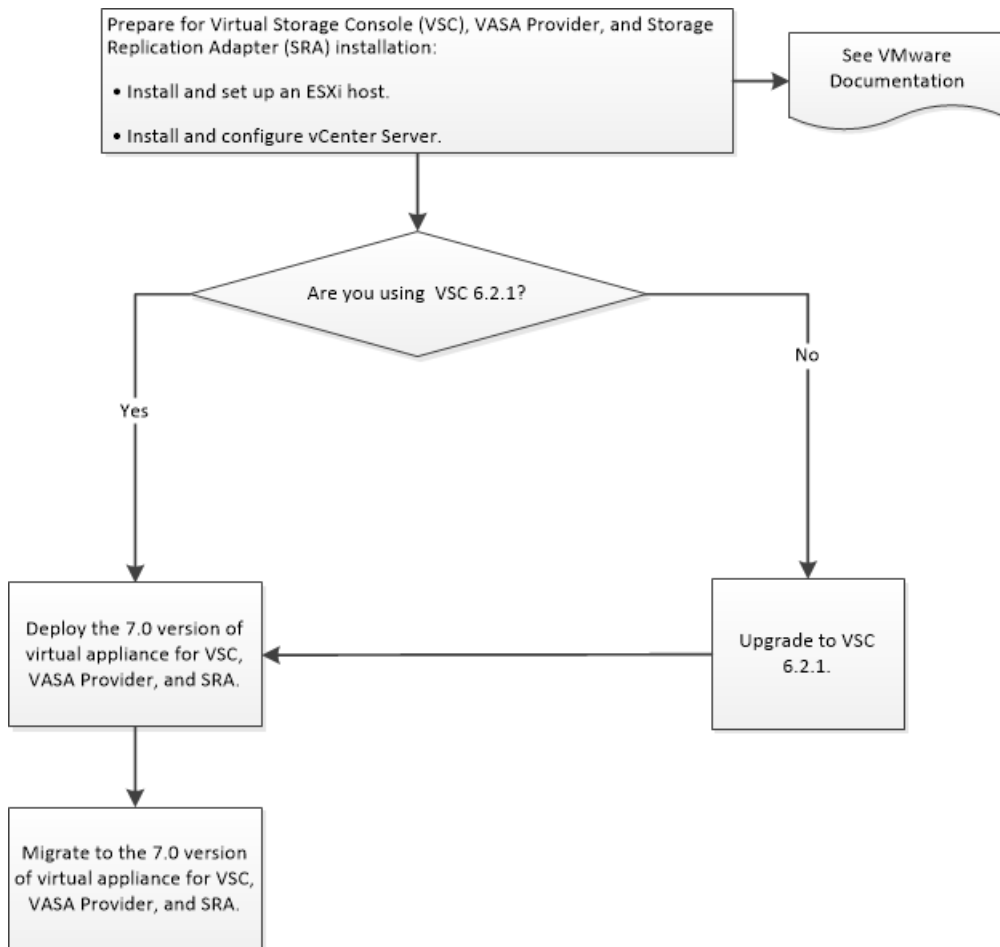
If you have installed Virtual Storage Console (VSC), VASA Provider, Storage Replication Adapter (SRA), or a combination of any of these products in your environment, then you should upgrade from your existing setup to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, and then you should migrate the data and configuration.

See the workflows for the different product configurations to understand the upgrade or migration procedure from your existing setup.

### Deployment workflow for existing users of VSC

If you have an existing setup of Virtual Storage Console (VSC) in your environment, then to upgrade to the 7.0 version of virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), you must migrate your data and configuration files.

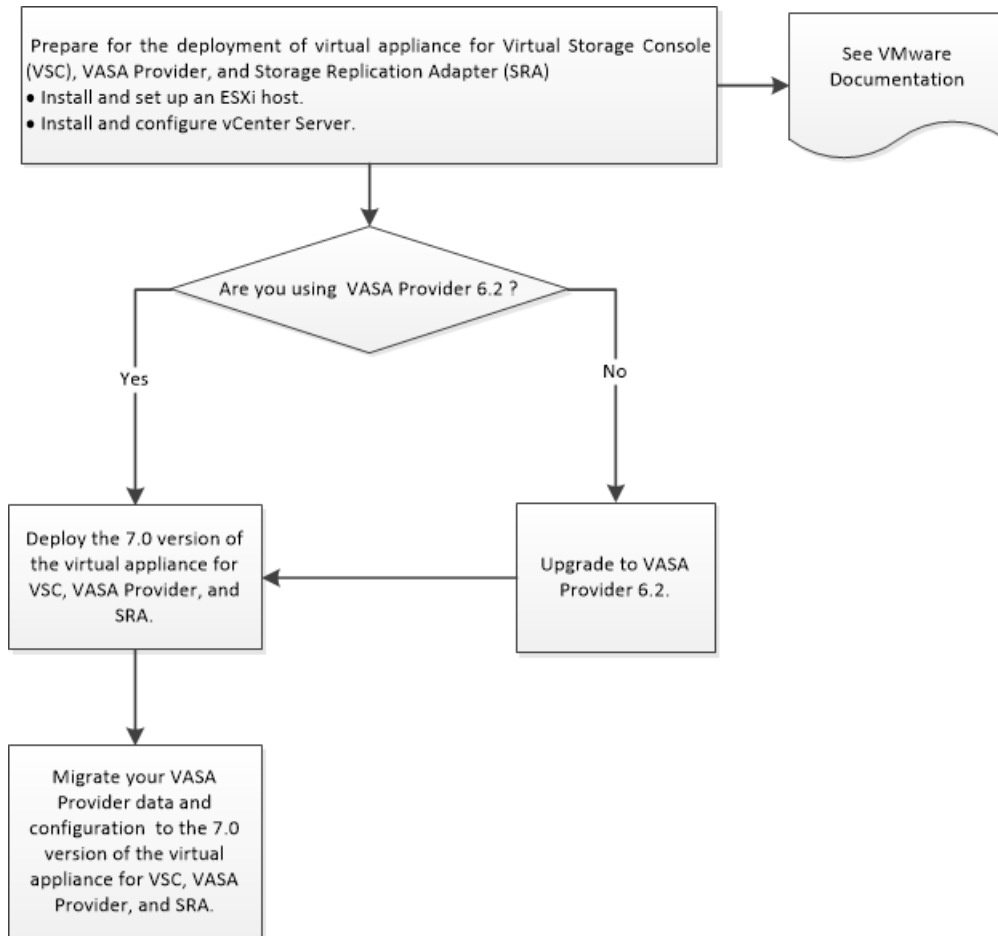
If the version of VSC is earlier than version 6.2.1, you must first upgrade to VSC 6.2.1, and then migrate to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA . If you have VSC 6.2.1 installed in your existing setup, then you must first deploy the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA , and then migrate your VSC 6.2.1 data and configuration details to the 7.0 virtual appliance.



## Deployment workflow for existing users of VASA Provider

If you have an existing setup of VASA Provider in your environment, then the process to upgrade to the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) depends on the version of VASA Provider in your setup.

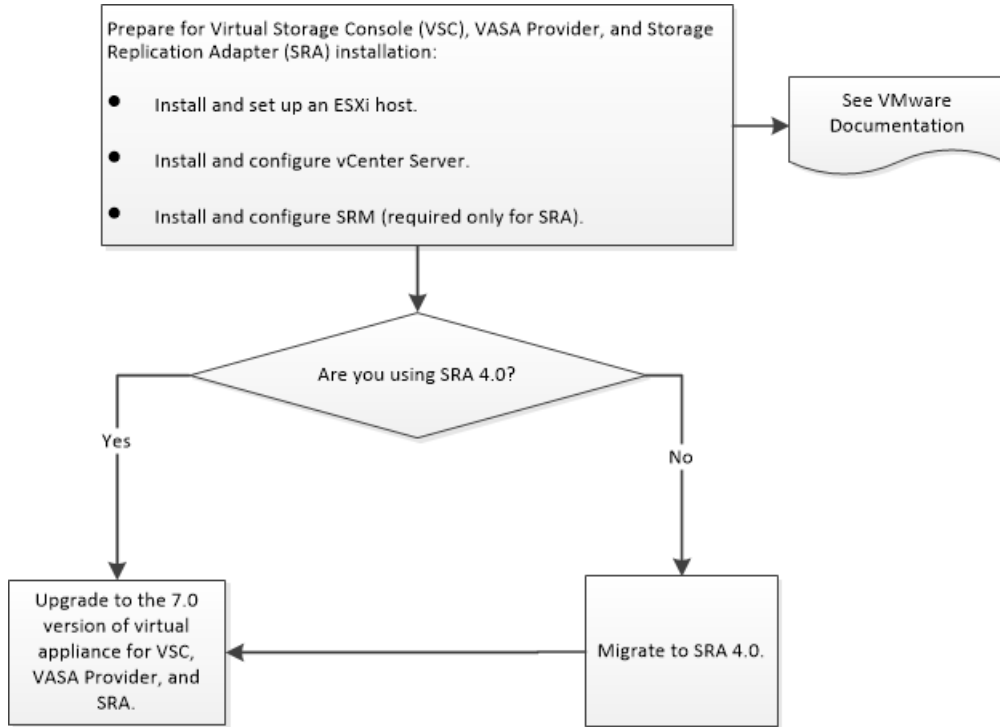
If the version of VASA Provider is earlier than version 6.2, then you must first upgrade to VASA Provider 6.2, and then deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA . You must then migrate the data after deploying the virtual appliance. If you have VASA provider 6.2 deployed in your setup, then you must deploy the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA, and then migrate data and configuration details from existing setup to the 7.0 virtual appliance.



## Deployment workflow for existing users of SRA

If you have an existing setup of Storage Replication Adapter (SRA) in your environment, then the process to upgrade to the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) depends on the version of SRA in your setup.

If the version of SRA is earlier than version 4.0, you must first migrate to SRA 4.0, and then perform an in-place upgrade from SRA 4.0 to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA . When you have SRA 4.0 installed in your existing setup, then you can perform an in-place upgrade to the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA .



## Deployment requirements for the virtual appliance for VSC, VASA Provider, and SRA

---

You should be aware of the deployment requirements before deploying the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), and you should decide the tasks that you want to perform. Based on your tasks, you can choose the deployment model for deploying the virtual appliance for VSC, VASA Provider, and SRA.

### Virtual Storage Console port requirements

By default, Virtual Storage Console (VSC) uses designated ports to enable communication between its components, which include storage systems and the VMware vCenter Server. If you have firewalls enabled, you must ensure that the firewalls are set to allow exceptions.

For firewalls other than Windows, you must manually grant access to specific ports that VSC uses. If you do not grant access to these ports, an error message such as `Unable to communicate with the server` is displayed.

VSC uses the following default ports:

Default port number	Description
9083	When enabled, both VASA Provider and SRA use this port to communicate with the vCenter Server
443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port.
8143	Plug-ins are registered to the vCenter Server using this port.

### Host requirements for the virtual appliance for VSC, VASA Provider, and SRA

Before you begin the deployment of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), you should be familiar with the space requirements for the deployment package and some basic host system requirements.

#### Installation package space requirements

- 2.1 GB for thin provisioned installations
- 54.0 GB for thick provisioned installations

#### SRM Server host system sizing requirements

- ESX 6.0 or later or ESXi 6.0 or later
- Recommended memory: 8 GB RAM
- Recommended CPUs: 4

## Supported storage system and applications for 7.0 virtual appliance for VSC, VASA Provider, and SRA

It is essential that you check the Interoperability Matrix on the NetApp Support Site for all the latest interoperability information. It is helpful to understand the basic storage system, application, and browser support before you begin your installation.

For the latest information on supported versions of ONTAP, vCenter Server, and SRM, see the Interoperability Matrix.

### License

SRA 7.0 requires the following licenses:

- SnapMirror license

**Note:** You must enable SnapMirror licenses before performing test failover and failover operations for SRA.

- FlexClone license

The FlexClone licence is required for test failover operation. So, if you enable SRA in your deployment, then you must have the FlexClone license enabled.

## Considerations for deploying the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA

Before you deploy the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), it is a good practice to plan your deployment and to decide how you want to configure VSC, VASA Provider, and SRA in your environment.

The following table presents a high-level overview of what you have to consider before you deploy and configure the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

Considerations	Description
Requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA	<p>You must deploy the virtual appliance on a 64-bit Linux server with at least 4 GB of RAM. You must not deploy it on a client computer. Additionally, the vCenter Server instance must be running a supported version of vSphere.</p> <p>Some of the VSC features use products that have additional requirements, which might require that you purchase a software license.</p>

Considerations	Description
Requirements of role-based access control (RBAC)	<p>VSC supports both vCenter Server RBAC and ONTAP RBAC.</p> <p>If you plan to run VSC as an administrator, you will have all of the required permissions and privileges for all of the tasks.</p> <p>If your company requires that you restrict access to vSphere objects, you can assign standard VSC roles to users to meet the vCenter Server requirements.</p> <p>You can create the recommended ONTAP roles by using the RBAC User Creator for ONTAP tool, which is available on the NetApp ToolChest.</p> <p>If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out.</p> <ul style="list-style-type: none"> <li>• <i>Standard roles packaged with the virtual appliance for VSC, VASA Provider, and SRA</i> on page 44</li> <li>• <i>Recommended ONTAP roles when using VSC for VMware vSphere</i> on page 48</li> </ul>



Considerations	Description
First-time deployment of the virtual appliance for VSC, VASA Provider, and SRA or upgrade scenarios	<p><b>Initial deployment:</b> The deployment of the virtual appliance for VSC, VASA Provider, and SRA automatically installs the VSC features.</p> <p><b>More information:</b></p> <p><i>Overview of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) deployment</i> on page 19</p> <p><b>Upgrade scenarios:</b> See the upgrade section for more information.</p> <p><i>Upgrade overview of Virtual Storage Console, VASA Provider, and Storage Replication Adapter</i> on page 54</p> <p>The best practices before an upgrade include the following:</p> <ul style="list-style-type: none"> <li>• <b>Important:</b></li> <li>• You should record information about the storage systems that are being used and their credentials. After the upgrade, you should verify that all of the storage systems were automatically discovered and that they have the correct credentials.</li> <li>• If you modified any of the standard VSC roles, you should copy those roles in order to save your changes. VSC overwrites the standard roles with the current defaults each time you restart the VSC service.</li> <li>• If you made any changes to the VSC preferences files, you should record those changes. Each time you upgrade VSC, VSC overwrites the current preferences files.</li> </ul> <p><b>More information:</b></p> <ul style="list-style-type: none"> <li>• <i>Deployment workflow for new users of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) virtual appliance</i> on page 10</li> <li>• <i>Overview of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) deployment</i> on page 19</li> </ul>
ONTAP version	You must have your storage systems running ONTAP 9.0, ONTAP 9.1, or ONTAP 9.2.
Regenerating an SSL certificate for VSC	<p>The SSL certificate is automatically generated when you deploy the virtual appliance for VSC, VASA Provider, and SRA. You might have to regenerate the SSL certificate to create a site-specific certificate.</p> <p><b>More information:</b></p> <p><i>Regenerating an SSL certificate for Virtual Storage Console</i> on page 31</p>

Considerations	Description
Setting ESXi server values	<p>Although most of your ESXi server values are set by default, it is a good practice to check the values. These values are based on internal testing. Depending on your environment, you might have to change some of the values to improve performance.</p> <p><b>More information:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">ESXi server and guest operating system setup</a> on page 24</li> <li>• <a href="#">Configuring ESXi server multipathing and timeout settings</a> on page 24</li> <li>• <a href="#">ESXi host values set by VSC for VMware vSphere</a> on page 25</li> </ul>
Guest operating system timeout values	<p>The guest operating system (GOS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems to provide correct failover behavior.</p> <p><b>More information:</b></p> <p><a href="#">Timeout values for guest operating systems</a> on page 27</p>
Storage capability profiles	<p>To use storage capability profiles or to set up alarms, you must enable VASA Provider for ONTAP. After you enable VASA Provider, you can configure virtual volume (VVOL) datastores, and you can create and manage storage capability profiles and alarms.</p> <p>The alarms warn you when a volume or aggregate is at nearly full capacity or when a datastore is no longer in compliance with its associated storage capability profile.</p>

# Overview of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) deployment

---

You must download and deploy the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) in your VMware vSphere, and then configure the required applications based on the tasks you want to perform using VSC, VASA Provider, and SRA.

## Downloading the virtual appliance for VSC, VASA Provider, and SRA

You can download the .ova file for the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) from the NetApp Support Site.

### About this task

The .ova file includes VSC, VASA Provider, and SRA. When the deployment is complete, all the three products are installed in your environment. By default, VSC will start working as soon as deployment is complete. You can decide on the subsequent deployment model and choose whether to enable VASA Provider and SRA based on your requirements.

You can download the virtual appliance for VSC, VASA Provider, and SRA from the NetApp Support Site by using the **Virtual Storage Console** menu, or the **NetApp VASA Provider** menu, or the **Storage Replication Adapter** menu, depending on your requirement. If you want to enable SRA in your deployment of the virtual appliance for VSC, VASA Provider, and SRA, then you must have installed the SRA 7.0 plug-in on the Site Recovery Manager (SRM) server. You can download the installation file for the SRA 7.0 plug-in from the **Storage Replication Adapter for ONTAP** menu in the Software Downloads section.

### Steps

1. Log in to the NetApp Support Site , and click the **Downloads** tab.
2. On the **Downloads** page, select **Software**.
3. From the list of products, select **Virtual Storage Console**, **NetApp VASA Provider**, or **Storage Replication Adapter**, depending on your requirement.

The virtual appliance for VSC, VASA Provider, and SRA can be downloaded by using the Virtual Storage Console menu, or the NetApp VASA Provider menu, or the Storage Replication Adapter menu.

4. Select the appropriate version of the software to download, and click **View & Download**.
5. Follow the instructions on the product description page until you reach the download page.
6. Download the .ova file:
  - Download the .ova file directly to the target system.
  - Download the .ova file to a PC host, and then copy the .ova file to the target system.

### After you finish

You should deploy the .ova file on an ESXi host.

## Deploying the virtual appliance for VSC, VASA Provider, and SRA

It is important that you understand the sequence of the steps for deploying the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) in your environment as the tasks that you can perform depend on the deployment model that you select.

### Before you begin

- You must be running a supported version of vCenter Server.
  - Note:** The virtual appliance for VSC, VASA Provider, and SRA can be deployed on either a Windows deployment of vCenter Server or a VMware vCenter Server Virtual Appliance (vCSA) deployment.
- You must have configured and set up your vCenter Server environment.
- You must have set up an ESXi host for your virtual machine.
- You must have downloaded the .ova file.
- You must have the login credentials for your vCenter Server instance.
- You must have logged out of and closed all of the browser sessions of vSphere Web Client, and deleted the browser cache to avoid any browser cache issue during the deployment of the virtual appliance for VSC, VASA Provider, and SRA.

### About this task

#### Note:

- You must not deploy the virtual appliance for VSC, VASA Provider, and SRA on the same host server on which vCenter Server is installed.
- You must not deploy the virtual appliance for VSC, VASA Provider, and SRA on a client computer.

### Steps

- Log in to the vSphere Web Client.
- Go to **Home > Host & Clusters**.
- Right-click the required datacenter, and then click **Deploy OVA template**.
- Select one of the following methods to provide the deployment file for VSC, VASA Provider, and SRA, and then click **Next**.

Location	Action
URL	Provide the URL for the .ova file for the virtual appliance for VSC, VASA Provider, and SRA.
Folder	Select the .ova file for the virtual appliance for VSC, VASA Provider, and SRA from the saved location.

- Enter the following details to customize the deployment wizard:
  - Name for your deployment

- Destination datacenter to apply permissions
- Host on which the virtual appliance for VSC, VASA Provider, and SRA is to be deployed
- Virtual disk format, VM storage policy, storage location, and network
- Administrator user name and password

**Note:** You must log in to your virtual appliance for VSC, VASA Provider, and SRA by using the administrator user name and password that you set during deployment.

The maintenance console user name is set to “maint” and the password is set to “admin123” by default.

*[Accessing the maintenance console options of the virtual appliance for VSC, VASA Provider, and SRA](#)* on page 34

- IP address of the vCenter Server instance to which you want to register the virtual appliance for VSC, VASA Provider, and SRA

You can view the progress of the deployment from the Tasks tab, and wait for deployment to complete.

6. Right-click the deployed virtual appliance for VSC, VASA Provider, and SRA, and then click **Install VMware tools**.

#### **Result**

When you log in by using the IP address that you specified during deployment, you will see the Virtual Storage Console icon.

## **Enabling extensions for the virtual appliance for VSC, VASA Provider, and SRA**

The virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) provides the option to enable the VASA Provider extension and the SRA extension to be used with VSC. This flexibility enables you to execute only the workflows that you require for your enterprise.

#### **Before you begin**

- You must have set up your vCenter Server instance and configured ESXi.
- You must have downloaded the .msi file for the SRA plug-in only if you want to configure for disaster recovery.
- You must have deployed the virtual appliance for VSC, VASA Provider, and SRA.

#### **Steps**

1. Log in to the web user interface of VMware vSphere.
2. On the home page, click the **Virtual Storage Console** icon.
3. Click **Configuration > Manage Extensions**.
4. In the **Manage Extensions** dialog box, select the extensions that you want to enable.
5. Enter the IP address of the virtual appliance for VSC, VASA Provider, and SRA and the administrator password, and then click **Apply**.

6. Double-click the downloaded .msi installer for the SRA plug-in, and follow the on-screen instructions.

You must download and install the SRA plug-in only if you want to configure for disaster recovery.

7. To complete the installation of the SRA plug-in on the Site Recovery Manager (SRM) server, enter the IP address and password of your deployed virtual appliance.

You must log out of the vCenter Server instance, and then log in again to verify that your selected extensions are available for configuration.

#### Related concepts

*Enabling VASA Provider for configuring virtual datastores* on page 50

*Configuring VSC, VASA Provider, and SRA for disaster recovery* on page 52

## Installing the NFS plug-in for VAAI

You can install the NetApp Plug-in for VMware vStorage APIs for Array Integration (VAAI) by using the GUI of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

#### Before you begin

You must have downloaded the installation package for the NetApp NFS Plug-in for VAAI from the the NetApp Support Site.

[mysupport.netapp.com](http://mysupport.netapp.com)

#### About this task

**Note:** You must set the password for the “diag” user while enabling the remote diagnostic access to be able to install the NFS VAAI plug-in with the “diag” credentials.

#### Steps

1. Enable remote diagnostic access.
  - a. Log in to the maintenance console of your virtual appliance.
  - b. Enter
    - 2
 to access the **System Configuration** menu.
  - c. In the **System Configuration** menu, enter
    - 6
 for the **Enable SSH access** option.
  - d. Navigate to the main menu, and enter
    - 4
 to access the **Support and Diagnostics** menu.
  - e. In the **Support and Diagnostics** menu, enter
    - 3
 for the **Enable Remote Diagnostic Access** option.
  - f. Click **Yes** in the **Do you want to enable remote diagnostic access** confirmation dialog box.



## Configuring your Virtual Storage Console for VMware vSphere environment

---

Virtual Storage Console (VSC) supports numerous environments. Some of the features in these environments might require additional configuration. In some cases, you might have to perform maintenance operations.

You might have to perform some of the following configuration tasks:

- Verifying your ESXi host settings, including the UNMAP settings
- Adding timeout values for guest operating systems
- Regenerating the VSC SSL certificate
- Creating storage capability profiles and threshold alarms
- Modifying the preferences file to enable the mounting of datastores across different subnets

### ESXi server and guest operating system setup

Most of the ESXi server values are set by default. It is a good practice to verify the values to ensure that the values are appropriate for your system setup. Virtual Storage Console for VMware vSphere also provides ISO files to enable you to set the correct timeout values for guest operating systems.

### Configuring ESXi server multipathing and timeout settings

Virtual Storage Console for VMware vSphere checks and sets the ESXi host multipathing settings and HBA timeout settings that work best with NetApp storage systems.

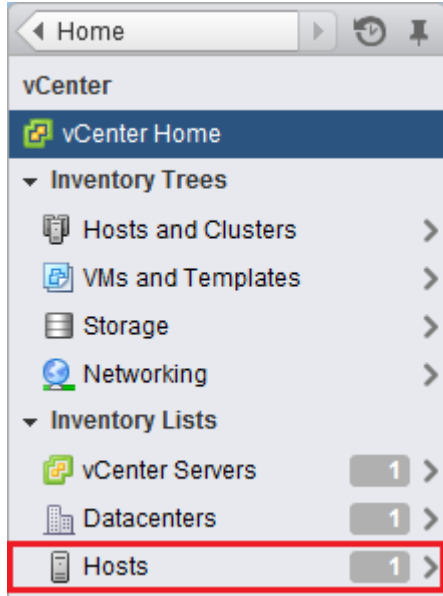
#### About this task

This process might take a long time, depending on your configuration and system load. The task progress is displayed in the **Recent Tasks** panel. As tasks are completed, the host status Alert icon is replaced by the Normal icon or the Pending Reboot icon.

#### Steps

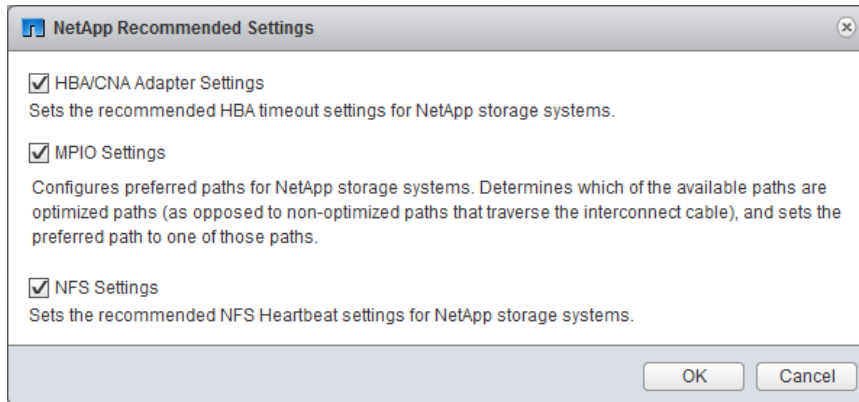
1. From the VMware vSphere Web Client **Home** page, click **vCenter > Hosts**.





2. Right-click a host, and then select **Actions > NetApp VSC > Set Recommended Values**.
3. In the **NetApp Recommended Settings** dialog box, select the values that work best with your system.

The standard, recommended values are set by default.



4. Click **OK**.

### ESXi host values set by VSC for VMware vSphere

Virtual Storage Console for VMware vSphere sets ESXi host timeouts and other values to ensure best performance and successful failover. The values that Virtual Storage Console (VSC) sets are based on internal NetApp testing.

VSC sets the following values on an ESXi host:

#### ESXi advanced configuration

##### VMFS3.HardwareAcceleratedLocking

Set to 1.

##### VMFS3.EnableBlockDelete

Set to 0.

For more information, see VMware KB article [2007427](#).

## NFS settings

### Net.TcpipHeapSize

If you are using vSphere 5.0 or later, set to 32.

For all other NFS configurations, set to 30.

### Net.TcpipHeapMax

If you are using vSphere 6.0 or later, set to 1536.

If you are using vSphere 5.5 or later, set to 512.

If you are using vSphere version 5.0 through version 5.5, set to 128.

For all other NFS configurations, set to 120.

### NFS.MaxVolumes

If you are using vSphere 5.0 or later, set to 256.

For all other NFS configurations, set to 64.

### NFS41.MaxVolumes

If you are using vSphere 6.0 or later, set to 256.

### NFS.MaxQueueDepth

If you are using vSphere 5.0 or later, set to 64.

If you are using only All Flash FAS (AFF) systems for a host cluster, set to 128 or higher to avoid queuing bottlenecks.

### NFS.HeartbeatMaxFailures

Set to 10 for all NFS configurations.

### NFS.HeartbeatFrequency

Set to 12 for all NFS configurations.

### NFS.HeartbeatTimeout

Set to 5 for all NFS configurations.

## FC/FCoE settings

### Path selection policy

Set to `RR` (round robin) for ESX 4.0, ESX 4.1, and ESXi 5.x, when FC paths with ALUA are enabled.

Set to `FIXED` for all other configurations.

Setting this value to `RR` helps to provide load balancing across all of the active/optimized paths. The value `FIXED` is used for older, non-ALUA configurations and helps to prevent proxy I/O. In other words, it helps to keep I/O from going to the other node of a high-availability (HA) pair in an environment that has Data ONTAP operating in 7-mode.

### Disk.QFullSampleSize

Set to 32 for all configurations. This setting is available with ESXi 5.x and ESX 4.x. Setting this value helps to prevent I/O errors.

**Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at [kb.netapp.com/support/index?page=content&id=1013944](http://kb.netapp.com/support/index?page=content&id=1013944).

### Disk.QFullThreshold

Set to 8 for all configurations. This setting is available with ESXi 5.0 and ESX 4.x. Setting this value helps prevent I/O errors.

**Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at [kb.netapp.com/support/index?page=content&id=1013944](http://kb.netapp.com/support/index?page=content&id=1013944).

#### **Emulex FC HBA timeouts**

For ESX 4.0, ESX 4.1, or ESXi 5.x, use the default value.

#### **QLogic FC HBA timeouts**

For ESX 4.0, ESX 4.1 or ESXi 5.x, use the default value.

### **iSCSI settings**

#### **Path selection policy**

Set to RR (round robin) for all iSCSI paths.

Setting this value to RR helps to provide load balancing across all of the active/optimized paths.

#### **Disk.QFullSampleSize**

Set to 32 for all configurations. This setting is available with ESX 4.x and ESXi 5.x. Setting this value helps to prevent I/O errors.

**Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at [kb.netapp.com/support/index?page=content&id=1013944](http://kb.netapp.com/support/index?page=content&id=1013944).

#### **Disk.QFullThreshold**

Set to 8 for all configurations. This setting is available with ESX 4.x and ESXi 5.x. Setting this value helps prevent I/O errors.

**Note:** vSphere 5.1 handles Task Set Full (QFull) conditions differently from vSphere 4.x and 5.0. For more information on QFull settings in vSphere 5.1, see knowledgebase article 1013944, which is online at [kb.netapp.com/support/index?page=content&id=1013944](http://kb.netapp.com/support/index?page=content&id=1013944).

## **Timeout values for guest operating systems**

The guest operating system (GOS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems. The timeout values help improve disk I/O behavior in a failover situation.

These scripts are provided as .ISO files. You can get a copy of the scripts by clicking **Tools > Guest OS Tools** from the Virtual Storage Console Home page. There are two scripts for each operating system:

- A 60-second script
- A 190-second script

In most cases, the recommended value is 60 seconds. Knowledge base article 3013622, which is online at [kb.netapp.com/support/index?page=content&id=3013622](http://kb.netapp.com/support/index?page=content&id=3013622), contains information you can use when deciding which timeout value to use.

You can mount and run the script from the vSphere client. The Tools panel provides URLs for the scripts.

To get the script containing the timeout values you want for your operating system, you must copy the correct URL from the Guest OS Tools page and mount it as a virtual CD-ROM in the virtual machine using the vSphere client. Make sure you install the script from a copy of Virtual Storage

Console for VMware vSphere that is registered to the vCenter Server that manages the virtual machine. After the script has been installed, you can run it from the console of the virtual machine.

### Adding the CD-ROM to a virtual machine

To enable installing the guest operating system scripts, you need to add the CD-ROM to a virtual machine if it does not exist.

#### Steps

1. In the vSphere Client, select the desired virtual machine and power it off.
2. Right-click the virtual machine and select **Manage > VM Hardware**.
3. Select **CD/DVD Drive** in the **New device** drop-down box and click **Add**.
4. Select **CD/DVD Drive** and then click **Next**.
5. Click **Use physical drive**.
6. Click **Next** several times to accept the default values.
7. Click **OK** to finish adding the CD-ROM.
8. Power on the virtual machine.

### Installing guest operating system scripts

The ISO images of the guest operating system scripts are loaded on the Virtual Storage Console for VMware vSphere server. To use them to set the storage timeouts for virtual machines, you must mount and run them from the vSphere Web Client.

#### Before you begin

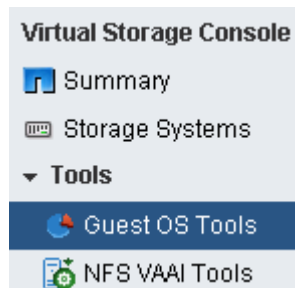
- The virtual machine must be running.
- The CD-ROM must already exist in the virtual machine, or it must have been added.
- The script must be installed from the copy of the VSC registered to the vCenter Server that manages the virtual machine.

#### About this task

If your environment includes multiple vCenter Servers, you must select the server that contains the virtual machines for which you want to set the storage timeout values.

#### Steps

1. From the Virtual Storage Console **Home** page, expand **Tools** and click **Guest OS Tools**:



2. Under **Guest OS Tools**, press Ctrl-C to copy the link to the ISO image for your guest operating system version to the clipboard.

VSC provides both 60-second timeout scripts and 190-second timeout scripts for Linux, Windows, and Solaris. Select the script for your operating system that provides the timeout value you want to use.

**Guest OS Tools**

Guest OS timeout scripts set the SCSI I/O timeout values for supported guest operating systems, which ensure correct failover behavior. Both 60-second and 190-second timeout values are supported. Select the URL for the .iso file containing the script you need and copy it using CTRL+C to the clipboard.

vCenter Server:  <https://10.0.0.00:0000/vsc/public/wr>

**Note: Before selecting an .iso file, check the Release Notes for information about the recommended timeout values.**

<p><b>60-second timeout settings:</b></p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/linux_gos_timeout-install.iso">Linux OS</a> https://10.0.0.00:0000/vsc/public/writable/linux_gos_timeout-install.iso</p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/windows_gos_timeout.iso">Window OS</a> https://10.0.0.00:0000/vsc/public/writable/windows_gos_timeout.iso</p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/solaris_gos_timeout-install.iso">Solaris OS</a> https://10.0.0.00:0000/vsc/public/writable/solaris_gos_timeout-install.iso</p>	<p><b>190-second timeout settings:</b></p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/linux_gos_timeout_190-install.iso">Linux OS</a> https://10.0.0.00:0000/vsc/public/writable/linux_gos_timeout_190-install.iso</p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/windows_gos_timeout_190.iso">Window OS</a> https://10.0.0.00:0000/vsc/public/writable/windows_gos_timeout_190.iso</p> <p><a href="https://10.0.0.00:0000/vsc/public/writable/solaris_gos_timeout_190-install.iso">Solaris OS</a> https://10.0.0.00:0000/vsc/public/writable/solaris_gos_timeout_190-install.iso</p>
--	---

3. Return to the vSphere Web Client **Home** page and select **vCenter**.
4. Select the desired virtual machine and click the **Manage > VM Hardware**.
5. Select **CD/DVD Drive 1 > Connect to ISO image on local disk**.
6. Paste the link you copied into the **File Name** field and then click **Open**.

Be sure that the link you are using is from the copy of the VSC running on the vCenter Server that manages the virtual machine.

#### After you finish

Log in to the virtual machine and run the script to set the storage timeout values.

### Running the GOS timeout scripts for Linux

The guest operating system timeout scripts set the SCSI I/O timeout settings for RHEL4, RHEL5, RHEL6, RHEL7, SLES9, SLES10, and SLES11. You can specify either a 60-second timeout or a 190-second timeout. You should always run the script each time you upgrade to a new version of Linux.

#### Before you begin

You must mount the ISO image containing the Linux script before you can run it in the virtual machine.

#### Steps

1. Open the console of the Linux virtual machine and log in to an account with root privileges.
2. Run the `linux_gos_timeout-install.sh` script.

**Result**

For RHEL4 or SLES9, a message similar to the following is displayed:

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

For RHEL5 or RHEL6, a message similar to the following is displayed:

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

For SLES10 or SLES11, a message similar to the following is displayed:

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

**After you finish**

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from filename.iso**.

**Running the GOS timeout scripts for Solaris**

The timeout scripts set the SCSI I/O timeout settings for Solaris 10. You can specify either a 60-second timeout or a 190-second timeout.

**Before you begin**

You must mount the ISO image containing the Solaris script before you can run it in the virtual machine.

**Steps**

1. Open the console of the Solaris virtual machine and log in to an account with root privileges.
2. Run the `solaris_gos_timeout-install.sh` script.

**Result**

For Solaris 10, a message similar to the following is displayed:

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

### After you finish

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from *filename.iso***.

## Running the GOS timeout script for Windows

The timeout scripts set the SCSI I/O timeout settings for Windows guest operating systems. You can specify either a 60-second timeout or a 190-second timeout. You must reboot the Windows guest OS for the settings to take effect.

### Before you begin

You must mount the ISO image containing the Windows script before you can run it in the virtual machine.

### Steps

1. Open the console of the Windows virtual machine and log in to an account with Administrator privileges.
2. If the script does not automatically start, open the CD drive and run `windows_gos_timeout.reg`.  
The Registry Editor dialog is displayed.
3. Click **Yes** to continue.  
The following message is displayed: The keys and values contained in D:\windows\_gos\_timeout.reg have been successfully added to the registry.
4. Reboot the Windows guest OS.

### After you finish

Unmount the ISO image by clicking the **CD/DVD Connections** icon in the vSphere Client and selecting **CD/DVD Drive 1 > Disconnect from *filename.iso***.

## Regenerating an SSL certificate for Virtual Storage Console

The SSL certificate is generated when you install Virtual Storage Console (VSC). The distinguished name (DN) that is generated for the SSL certificate might not be a common name (CN) that the client machines recognize. By changing the keystore and private key passwords, you can regenerate the certificate and create a site-specific certificate.

### Steps

1. Log in to the maintenance console.
2. Enter `1` to access the Application Configuration menu.
3. In the Application Configuration menu, enter `3` to stop the VSC service.
4. Enter `7` to regenerate SSL certificate.

## Performing VSC for VMware vSphere tasks across multiple vCenter Servers

If you are using Virtual Storage Console for VMware vSphere in an environment where a single VMware vSphere Web Client is managing multiple vCenter Server instances, you need to register an instance of VSC with each vCenter Server so that there is a 1:1 pairing between VSC and the vCenter Server. Doing this enables you to manage all of the servers running vCenter 5.5 or later in both linked mode and non-linked mode from a single vSphere Web Client.

**Note:** If you want to use VSC with a vCenter Server, then you must have configured the following:

- Setup or register one VSC for every vCenter Server instance.
- Each registered VSC must be of same version.

Linked mode is installed automatically during the vCenter Server deployment. It uses Microsoft Active Directory Application Mode (ADAM) to store and synchronize data across multiple vCenter Server systems.

Using the vSphere Web Client to perform VSC tasks across multiple vCenter Servers requires the following:

- You must have installed multiple instances of VSC.
- Each vCenter Server in the VMware inventory must have a single VSC server registered with it in a unique 1:1 pairing.  
For example, you can have VSC server A registered to vCenter Server A, VSC server B registered to vCenter Server B, VSC server C registered to vCenter Server C, and so on.  
You **cannot** have VSC server A registered to both vCenter Server A and vCenter Server B.  
Also, if the VMware inventory includes one vCenter Server that does not have a VSC server registered to it, you will not be able to see any instances of VSC, even though the VMware inventory has one or more vCenter Servers that are registered with VSC.

- You must have the VSC-specific View privilege for each vCenter Server that is registered to the single sign-on (SSO).  
You must also have the correct RBAC permissions.

When you are performing a task that requires you to specify a vCenter Server, the **vCenter Server** drop-down box displays the available vCenter Servers in alphanumeric order. The default vCenter Server is always the first server in the drop-down list.

If the location of the storage is known (for example, when you use the Provisioning wizard and the datastore is on a host managed by a specific vCenter Server), the vCenter Server list is displayed as a read-only option. This only happens when you use the right-click option to select an item in the vSphere Web Client.

VSC warns you when you attempt to select an object that it does not manage.

You can filter storage systems based on a specific vCenter Server from the VSC summary page. A summary page appears for every VSC instance registered with a vCenter Server. You can manage storage systems associated with a specific VSC instance and vCenter Server, but you should keep the registration information for each storage system separate if you are running multiple instances of VSC.



## Preferences files

The preferences files contain settings that control Virtual Storage Console for VMware vSphere operations. Under most circumstances, you do not have to modify the settings in these files. It is helpful to know which preference files Virtual Storage Console (VSC) uses.

VSC has several preference files. These files include entry keys and values that determine how VSC performs various operations. The following are some of the preference files that VSC uses:

```
/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml
```

```
/opt/netapp/vscserver/etc/vsc/vscPreferences.xml
```

You might have to modify the preferences files in certain situations. For example, if you use iSCSI or NFS and the subnet is different between your ESXi hosts and your storage system, you have to modify the preferences files. If you do not modify the settings in the preferences file, datastore provisioning fails because VSC cannot mount the datastore.

## Enabling datastore mounting across different subnets

If you use iSCSI or NFS and the subnet is different between your ESXi hosts and your storage system, you have to modify two settings in the Virtual Storage Console for VMware vSphere preferences files. If you do not modify these files, datastore provisioning fails because Virtual Storage Console (VSC) cannot mount the datastore.

### About this task

When datastore provisioning fails, VSC logs the following error messages:

```
Unable to continue. No ip addresses found when cross-referencing kernel ip
addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts.
```

### Steps

1. Log in to your vCenter Server instance.
2. Click **Home > Virtual Storage Console**.
3. Launch the maintenance console of your virtual machine.

*[Accessing the maintenance console options of the virtual appliance for VSC, VASA Provider, and SRA](#) on page 34*

4. Enter **4** to access the **Support and Diagnostics** option.
5. Enter **2** to access the **Access Diagnostic Shell** option.
6. Enter `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` to update the `kaminoprefs.xml` file.
7. Update the `kaminoprefs.xml` file.

If you use...	Do this...
iSCSI	Change the value of the entry key <code>default.allow.iscsi.mount.networks</code> from ALL to the value of your ESXi host subnet masks.

If you use...	Do this...
NFS	Change the value of the entry key <code>default.allow.nfs.mount.networks</code> from ALL to the value of your ESXi host subnet masks.

The preferences files include sample values for these entry keys.

**Note:** The value ALL does not mean all networks. This value means that all of the matching networks between the host and storage system can be used to mount datastores. Specifying subnet masks enables mounting across the specified subnets only.

8. Save and close the `kaminoprefs.xml` file.

## Accessing the maintenance console options of the virtual appliance for VSC, VASA Provider, and SRA

You can manage your application, system, and network configurations by using the maintenance console of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA). You can change your administrator password and maintenance password by using the maintenance console. You can also generate support bundles and start remote diagnostics by using the maintenance console.

### Before you begin

You must have installed VMware tools after deploying the virtual appliance for VSC, VASA Provider, and SRA.


### About this task

#### Note:

- You must use “maint” as the user name and “admin123” as the password to log in to the maintenance console of the virtual appliance for VSC, VASA Provider, and SRA .
- You must set a password for the “diag” user while enabling remote diagnostics.

### Steps

1. Access the **Summary** tab of your deployed virtual appliance.

2. Click  to start the maintenance console.

You can access the following maintenance console options:

#### Application Configuration

The following options are available:

- Display server status summary
- Start Virtual Storage Console service
- Stop Virtual Storage Console service
- Start VASA Provider and SRA service
- Stop VASA Provider and SRA service

- Change 'administrator' user password
- Re-generate certificates
- Hard reset keystore and certificates
- Hard reset database

### **System Configuration**

The following options are available:

- Reboot virtual machine
- Shutdown virtual machine
- Change 'maint' user password
- Change time zone
- Change NTP server
- Enable/Disable SSH Access
- Increase jail disk size (/jail)
- Upgrade
- Install VMware Tools

### **Network Configuration**

The following options are available:

- Display IP address settings
- Change IP address settings
- Display domain name search settings
- Change domain name search settings
- Display static routes
- Change static routes
- Commit changes
- Ping a host
- Restore default settings

### **Support and Diagnostics**

The following options are available:

- Generate support bundle
- Access diagnostic shell
- Enable remote diagnostic access

## Overview of storage system discovery and storage credentials

---

Virtual Storage Console for VMware vSphere provides a single mechanism to discover storage systems and to set the storage credentials. The credentials provide the ONTAP permissions that are required to enable Virtual Storage Console (VSC) users to perform tasks by using the storage systems.

Before VSC can display and manage storage resources, VSC must discover the storage systems. As part of the discovery process, you must supply ONTAP credentials for your storage systems. These are the privileges (or roles) that are associated with the user name and password pair that is assigned to each storage system. These user name and password pairs use ONTAP role-based access control (RBAC) and must be set up from within ONTAP. You cannot change these credentials from within VSC. You can define ONTAP RBAC roles by using a tool such as RBAC User Creator for ONTAP. You cannot change these credentials from within VSC.

**Note:** If you log in as an administrator, you automatically have all of the privileges for that storage system.

When you add a storage system to VSC, you must supply an IP address for the storage system and the user name and password pair that is associated with that system. You can set up default credentials that VSC will use during the storage system discovery process, or you can manually enter credentials when the storage system is discovered. The details of the storage system that is added to VSC are automatically pushed to the extensions that you enable in your deployment. So, you do not have to manually add storage to VASA Provider and Storage Replication Adapter (SRA). Both VSC and SRA support the addition of credentials at the cluster level and Storage Virtual Machine (SVM) level. VASA Provider supports only cluster-level credentials for adding storage systems.

If your environment includes multiple vCenter Server instances, when you add a storage system to VSC from the Storage Systems page, the **Add Storage System** dialog box displays a **vCenter Server** box where you can specify to which vCenter Server instance the storage system is to be added. If you add a storage system by right-clicking a datacenter name, you do not have the option to specify a vCenter Server instance because the server is already associated with that datacenter.

Discovery happens in one of the following ways. In each case, you must supply credentials for any newly discovered storage system.

- When the VSC service starts, VSC begins its automatic background discovery process.
- You can click the **Update All** icon, or select it from the Actions menu (**Actions > Netapp VSC > Update All**).

**Note:** IPv6 addresses are not supported.

All of the VSC features require specific permissions to perform tasks. You can limit what users can do based on the credentials that are associated with the ONTAP role. All of the users that have the same storage system user name and password pair share the same set of storage system credentials and can perform the same operations.

## Setting default credentials for storage systems

You can use Virtual Storage Console for VMware vSphere to set default credentials for a storage system in your vCenter Server.

### Before you begin

You must have selected the vCenter Server that you want to use for creating default credentials.

### About this task

If you set up default credentials for storage systems, Virtual Storage Console (VSC) uses these credentials to log in to a storage system that VSC has just discovered. If the default credentials do not work, you must manually log in to the storage system. VSC and SRA support addition of storage system credentials at the cluster level or SVM level. But VASA Provider will only work with cluster level credentials.

### Steps

1. From the VSC **Home** page, click **Configuration > Set Default Credentials**.
2. In the **Set Default Credentials** dialog box, enter the credentials for the storage system.

Storage system field	Description
User name and password	Storage controller credentials are assigned in ONTAP based on the user name and password pair. The storage controller can be the root account or a custom account that uses role-based access control (RBAC).  You cannot use VSC to change the roles that are associated with the user name and password pair of the storage controller. To change the storage controller credentials, you must use a tool such as RBAC User Creator for ONTAP.
Use TLS	You must select this check box if you want to enable Transport Layer Security (TLS).
Port	The default management port number is 443 if the Use TLS check box is selected and 80 if the Use TLS check box is not selected. These are the ONTAP defaults. If you toggle the Use TLS check box, the port number switches between 443 and 80. You can specify a different port number. If you specify a different port number, then toggling the Use TLS check box only changes the TLS state in the dialog box.

3. Click **OK** to save the default credentials.

### After you finish

If you updated the storage system credentials because a storage system reported “Authentication Failure” status, you must select **Update Hosts and Storage Systems**, which is available from the **Actions > NetApp VSC** menu. When you do this, VSC tries to connect to the storage system by using the new credentials.

## Manually adding storage systems

Each time you start the VSC Windows service or select **Update All**, Virtual Storage Console for VMware vSphere (VSC) automatically discovers the available storage systems. You can also manually add storage systems to VSC.

### About this task

If you have a large number of storage systems, manually adding a new storage system might be faster than using the **Update All** option to discover the storage system.

### Steps

1. Add a storage system to VSC by using either the **Add** icon or the **Add Storage System** menu option:

Starting location	Action
Virtual Storage Console Home page	<ol style="list-style-type: none"> <li>a. Click <b>Storage System</b>.</li> <li>b. Click the <b>Add</b> icon.</li> </ol>
VMware vSphere Web Client Home page	<ol style="list-style-type: none"> <li>a. Click the <b>Storage</b> icon.</li> <li>b. Select a datacenter.</li> <li>c. Click the <b>Actions &gt; NetApp VSC &gt; Add Storage System</b>.</li> </ol>

2. In the **Add Storage System** dialog box, enter the management IP address and credentials for that storage system.

You can also change the defaults for TLS and the port number in this dialog box.

When you add storage from the VSC Storage System page, you must also specify the vCenter Server instance where the storage will be located. The Add Storage System dialog box provides a drop-down list of the available vCenter Server instances. VSC does not display this option if you are adding storage to a datacenter that is already associated with a vCenter Server instance.

The screenshot shows a dialog box titled "Add Storage System". It contains the following fields and controls:

- vCenter Server:** A dropdown menu with "vcenterserver1" selected.
- Name or IP Address :** A text input field with a red asterisk indicating it is required.
- User name :** A text input field with a red asterisk indicating it is required.
- Password :** A text input field.
- Use TLS:** A checked checkbox.
- Port :** A text input field containing "443" with a red asterisk indicating it is required.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "<<Options".

3. Click **OK** after you have added all of the required information.

## Discovering storage systems and hosts

When you first run Virtual Storage Console (VSC) in a VMware vSphere Web Client, VSC discovers ESXi hosts, their LUNs and NFS exports, and the NetApp storage systems that own those LUNs and exports. After the discovery process is complete, you should provide the storage system credentials.

### Before you begin

You should ensure that all of the ESXi hosts are powered on and connected.

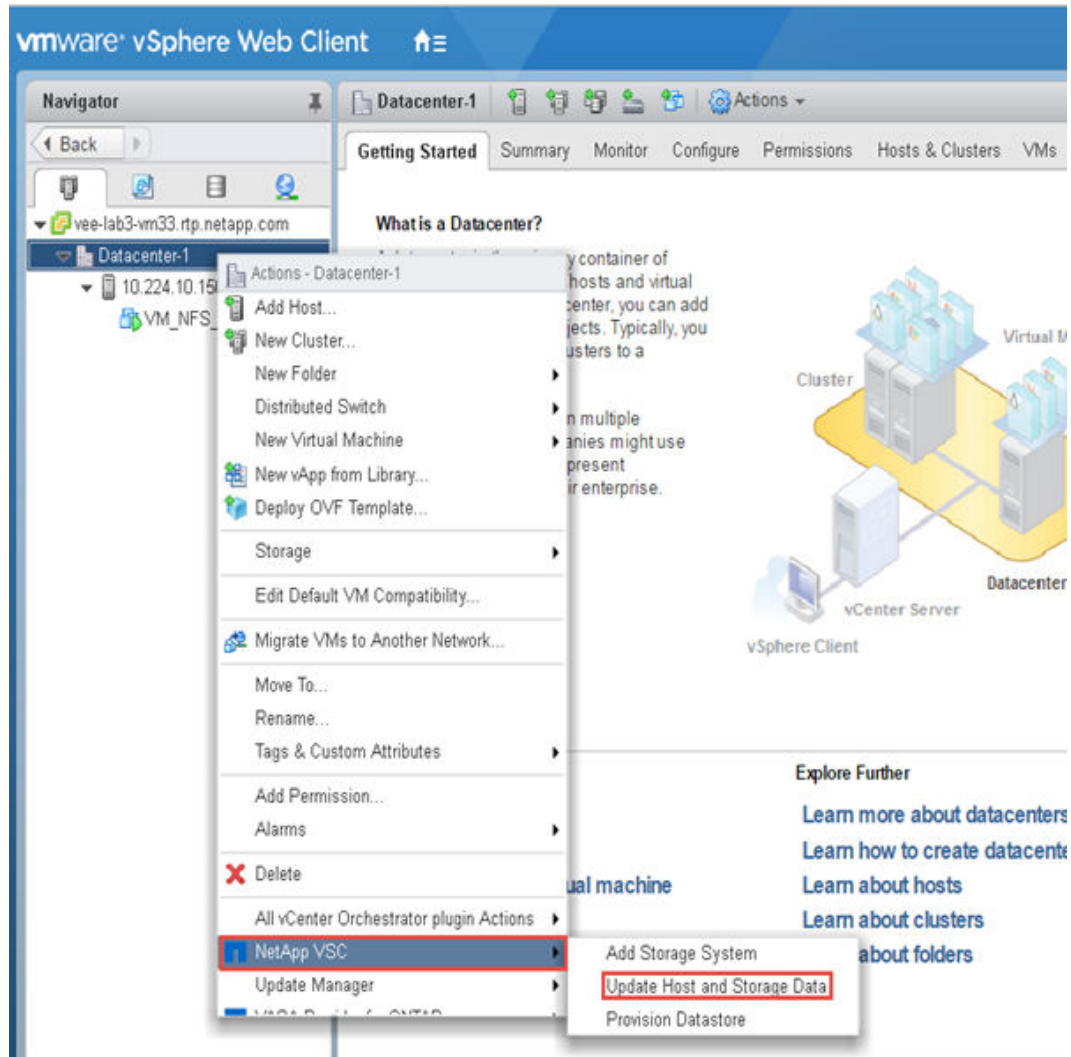
### About this task

You can discover new storage systems or update information about storage systems to obtain the latest capacity and configuration information at any time. You can also modify the credentials that VSC uses to log in to the storage systems.

The discovery process also collects information from the ESXi hosts that are managed by the vCenter Server instance.

### Steps

1. From the vSphere Web Client **Home** page, select **Hosts and Clusters**.
2. Right-click the required datacenter, and select **NetApp VSC > Update Host and Storage Data**.



VSC displays a Confirm dialog box that informs you that this operation can take a long time.

3. Click **OK**.
4. Right-click any of the discovered storage controllers that have the status “Authentication Failure”, and then select **Modify**.
5. Fill in the required information in the **Modify Storage System** dialog box.
6. Repeat steps 4 and 5 for all storage controllers with “Authentication Failure” status.

#### After you finish

After the discovery process is complete, you should use VSC to configure ESXi host settings for hosts that display the Alert icon in the Adapter Settings column, the MPIO Settings column, or the NFS Settings column.

## Refreshing the storage system display

You can use the update feature that is provided by Virtual Storage Console for VMware vSphere to refresh the information about storage systems and to force Virtual Storage Console (VSC) to discover



storage systems. This can be especially useful if you changed the default credentials for the storage systems after receiving an authentication error.

### About this task

You should always perform an update operation if you changed the storage system credentials after a storage system reported an Authentication Failure Status. During the update operation, VSC tries to connect to the storage system by using the new credentials.

Depending on your system setup, this task can take a long time to complete.

### Steps

1. Go to the **Storage** page by clicking **Storage** from either the navigation pane of the VSC **Storage** page or the icon on the VMware vSphere Web Client **Home** page.

2. Start the update:

If this location is...	Click...
Virtual Storage Console	The <b>Update All</b> icon.
Datacenter	<b>Actions &gt; NetApp VSC &gt; Update Host and Storage Data</b>

3. Click **OK** in the **Confirm** dialog box.
4. Click **OK** in the **Success Message** dialog box.

This operation works in the background.

## vCenter Server role-based access control features in VSC for VMware vSphere

vCenter Server provides role-based access control (RBAC) that enables you to control access to vSphere objects. In Virtual Storage Console for VMware vSphere, vCenter Server RBAC works with ONTAP RBAC to determine which VSC tasks a specific user can perform on objects on a specific storage system.

To successfully complete a task, you must have the appropriate vCenter Server RBAC permissions. During a task, VSC checks a user's vCenter Server permissions before checking the user's ONTAP privileges.

You can set the vCenter Server permissions on the root object (also known as the root folder). You can then refine the security by restricting child entities that do not need those permissions.

### Components of vCenter Server permissions

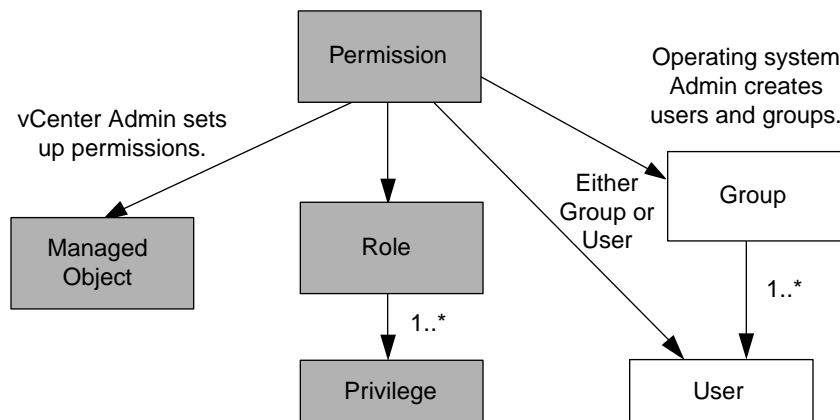
The vCenter Server recognizes permissions, not privileges. Each vCenter Server permission consists of three components.

These components are the following:

- One or more privileges (the role)  
The privileges define the tasks that a user can perform.
- A vSphere object  
The object is the target for the tasks.
- A user or group  
The user or group defines who can perform the task.

As the following diagram illustrates, you must have all three elements in order to have a permission.

**Note:** In this diagram, the gray boxes indicate components that exist in the vCenter Server, and the white boxes indicate components that exist in the operating system where the vCenter Server is running.



#### Privileges

Two kinds of privileges are associated with Virtual Storage Console for VMware vSphere:

- Native vCenter Server privileges  
These privileges come with the vCenter Server.
- VSC-specific privileges  
These privileges are defined for specific VSC tasks. They are unique to VSC.

VSC tasks require both VSC-specific privileges and vCenter Server native privileges. These privileges constitute the “role” for the user. A permission can have multiple privileges.

**Note:** To simplify working with vCenter Server RBAC, VSC provides several standard roles that contain all the VSC-specific and native privileges that are required to perform VSC tasks.

If you change the privileges within a permission, the user that is associated with that permission should **log out and then log back in** to enable the updated permission.

### vSphere objects

Permissions are associated with vSphere objects, such as the vCenter Server, ESXi hosts, virtual machines, datastores, datacenters, and folders. You can assign permissions to any vSphere object. Based on the permission that is assigned to a vSphere object, the vCenter Server determines who can perform which tasks on that object.

### Users and groups

You can use Active Directory (or the local vCenter Server machine) to set up users and groups of users. You can then use vCenter Server permissions to grant access to these users or groups to enable them to perform specific VSC tasks.

**Note:** These vCenter Server permissions apply to VSC vCenter users, not to VSC administrators. By default, VSC administrators have full access to the product and do not require permissions assigned to them.

Users and groups do not have roles assigned to them. They gain access to a role by being part of a vCenter Server permission.

You can assign only one permission to a vCenter Server user or group. However, you can set up high-level groups, and then assign a single user to multiple groups. Doing that allows the user to have all the permissions that are provided by the different groups. In addition, using groups simplifies the management of permissions by eliminating the need to set up the same permission multiple times for individual users.

## Key points about assigning and modifying permissions

There are several key points to keep in mind when you are working with vCenter Server permissions. Whether a Virtual Storage Console for VMware vSphere task succeeds can depend on where you assigned a permission or what actions a user took after a permission was modified.

You only need to set up vCenter Server permissions if you want to limit access to vSphere objects and tasks. Otherwise, you can log in as an administrator. This login automatically allows you to access all vSphere objects.

### Assigning permissions

Where you assign a permission determines the VSC tasks that a user can perform.

Sometimes, to ensure that a task completes, you must assign the permission at a higher level, such as the root object. This is the case when a task requires a privilege that does not apply to a specific vSphere object (for example, tracking the task) or when a required privilege applies to a non-vSphere object (for example, a storage system).

In these cases, you can set up a permission so that it is inherited by the child entities. You can also assign other permissions to the child entities. The permission on a child entity always overrides the permission inherited from the parent entity. This means that you can assign child entity permissions as a way to restrict the scope of a permission that was assigned to a root object and inherited by the child entity.

**Tip:** Unless your company's security policies require more restrictive permissions, it is a good practice to assign permissions on the root object (also referred to as the root folder). Then, if you need to, you can restrict those entities that you do not want to have the permission so that you have more fine-grained security.

### Permissions and non-vSphere objects

In some cases, a permission applies to a non-vSphere object. For example, a storage system is not a vSphere object. If a privilege applies to a storage system, you must assign the permission containing that privilege to the VSC root object because there is no vSphere object to which you can assign it.

For example, any permission that includes a privilege such as the VSC privilege "Add/Modify/Skip storage systems" must be assigned at the root object level.

### Modifying permissions

You can modify a permission at any time.

If you change the privileges within a permission, the user associated with that permission should **log out and then log back in** to enable the updated permission.

## Standard roles packaged with the virtual appliance for VSC, VASA Provider, and SRA

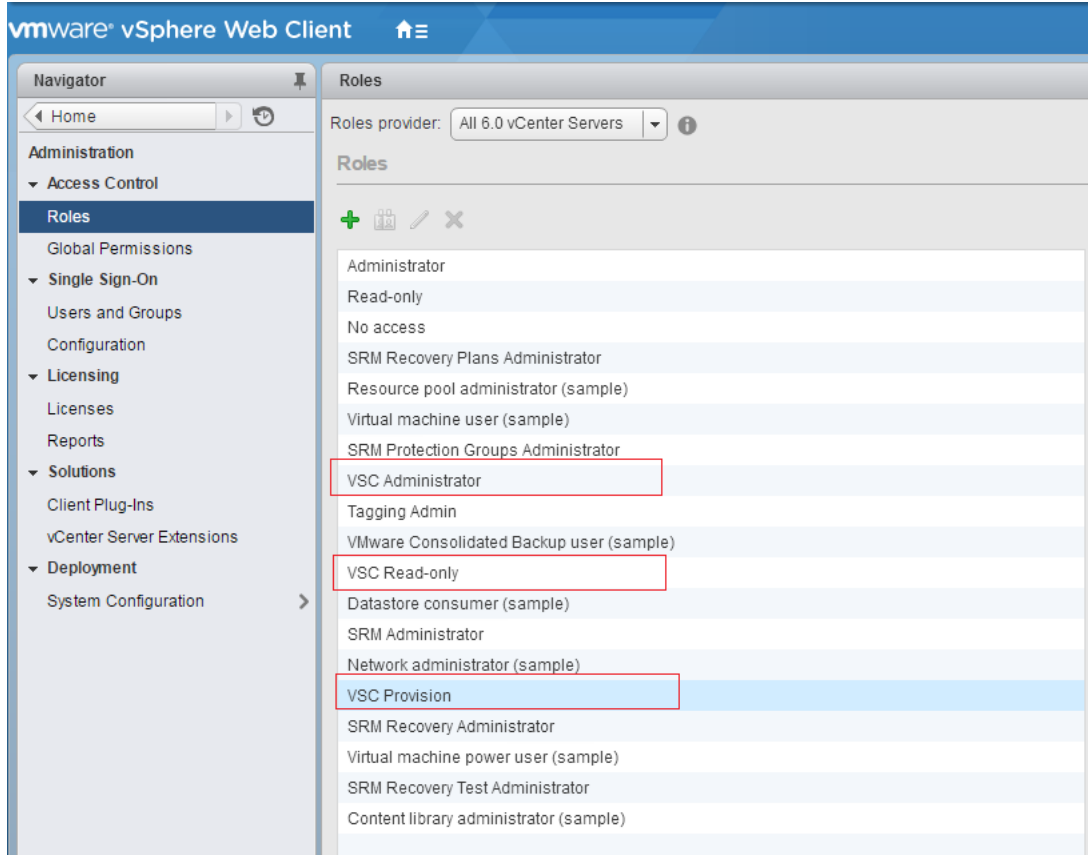
To simplify working with vCenter Server privileges and role-based access control (RBAC), Virtual Storage Console (VSC) provides standard VSC roles that enable you to perform key VSC tasks. There is also a read-only role that enables you to view VSC information, but not perform any tasks.

The standard VSC roles have both the required VSC-specific privileges and the native vCenter Server privileges that are required for users to perform VSC tasks. In addition, the roles are set up so that they have the required privileges across all supported versions of the vCenter Server.

As an administrator, you can assign these roles to users, as required.

**Note:** VSC resets these roles to their default values (the initial set of privileges) each time you restart the VSC Windows service or modify your installation. If you upgrade VSC, the standard roles are automatically upgraded to work with the new version of VSC.

You can view the VSC standard roles by clicking **Roles** on the VMware vSphere Web Client Home page.



The roles that VSC provides enable you to perform the following tasks:

Role	Description
VSC Administrator	Provides all of the native vCenter Server privileges and VSC-specific privileges that are required to perform all VSC tasks.
VSC Read-only	Provides read-only access to VSC. These users cannot perform any VSC actions that are access-controlled.
VSC Provision	Provides all of the native vCenter Server privileges and VSC-specific privileges that are required to provision storage. You can perform the following tasks: <ul style="list-style-type: none"> <li>• Create new datastores</li> <li>• Destroy datastores</li> <li>• View information about storage capability profiles</li> </ul>

## Guidelines for using VSC standard roles

When you work with standard Virtual Storage Console for VMware vSphere roles, there are certain guidelines you should follow.

You should not directly modify the standard roles. If you do, VSC will overwrite your changes each time you upgrade VSC. The installer updates the standard role definitions each time you upgrade VSC. Doing this ensures that the roles are current for your version of VSC as well as for all supported versions of the vCenter Server.

You can, however, use the standard roles to create roles that are tailored to your environment. To do this, you should copy the VSC standard role and then edit the copied role. By creating a new role, you can maintain this role even when you restart or upgrade the VSC Windows service.

Some of the ways that you might use the VSC standard roles include the following:

- Use the standard VSC roles for all VSC tasks.  
In this scenario, the standard roles provide all the privileges a user needs to perform the VSC tasks.
- Combine roles to expand the tasks a user can perform.  
If the standard VSC roles provide too much granularity for your environment, you can expand the roles by creating higher-level groups that contain multiple roles.  
If a user needs to perform other, non-VSC tasks that require additional native vCenter Server privileges, you can create a role that provides those privileges and add it to the group also.
- Create more fine-grained roles.  
If your company requires that you implement roles that are more restrictive than the standard VSC roles, you can use the VSC roles to create new roles.  
In this case, you would clone the necessary VSC roles and then edit the cloned role so that it has only the privileges your user requires.

## Privileges required for VSC tasks

Different Virtual Storage Console for VMware vSphere tasks require different combinations of VSC-specific privileges and native vCenter Server privileges.

Information about the privileges required for VSC tasks is available in Knowledgebase article 1013941 *How to configure Storage and vCenter RBAC for VSC for VMware vSphere*, which is online at [kb.netapp.com/support/index?page=content&id=1013941](https://kb.netapp.com/support/index?page=content&id=1013941).

## Product-level privilege required by VSC for VMware vSphere

To access the Virtual Storage Console for VMware vSphere GUI, you must have the product-level, VSC-specific View privilege assigned at the correct vSphere object level. If you log in without this privilege, VSC displays an error message when you click the NetApp icon and prevents you from accessing VSC.

The following information describes the VSC product-level View privilege:

Privilege	Description	Assignment level
View	<p>You can access the VSC GUI.</p> <p>This privilege does not enable you to perform tasks within VSC. To perform any VSC tasks, you must have the correct VSC-specific and native vCenter Server privileges for those tasks.</p>	<p>The assignment level determines which portions of the UI you can see.</p> <p>Assigning the View privilege at the root object (folder) enables you to enter VSC by clicking the NetApp icon.</p> <p>You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use.</p> <p>The root object is the recommended place to assign any permission containing the View privilege.</p>

## ONTAP role-based access control for the virtual appliance for VSC, VASA Provider, and SRA

ONTAP role-based access control (RBAC) enables you to control access to specific storage systems and to control the actions that a user can perform on those storage systems. In Virtual Storage Console for VMware vSphere, ONTAP RBAC works with vCenter Server RBAC to determine which Virtual Storage Console (VSC) tasks a specific user can perform on the objects on a specific storage system.

VSC uses the credentials (user name and password) that you set up within VSC to authenticate each storage system and to determine which storage operations can be performed on that storage system. VSC uses one set of credentials for each storage system. These credentials determine which VSC tasks can be performed on that storage system; in other words, the credentials are for VSC, not for an individual VSC user.

ONTAP RBAC applies only to accessing storage systems and performing VSC tasks that are related to storage, such as provisioning virtual machines. If you do not have the appropriate ONTAP RBAC privileges for a specific storage system, you cannot perform any tasks on a vSphere object that is hosted on that storage system. You can use ONTAP RBAC in conjunction with the VSC-specific privileges to control which VSC tasks a user can perform:

- Monitoring and configuring storage or vCenter Server objects residing on a storage system
- Provisioning vSphere objects residing on a storage system

Using ONTAP RBAC with the VSC-specific privileges provides a storage-oriented layer of security that the storage administrator can manage. As a result, you have more fine-grained access control than what either ONTAP RBAC alone or vCenter Server RBAC alone supports. For example, with vCenter Server RBAC, you can allow vCenterUserB to provision a datastore on NetApp storage while preventing vCenterUserA from provisioning datastores. If the storage system credentials for a specific storage system do not support the creation of storage, then neither vCenterUserB nor vCenterUserA can provision a datastore on that storage system.

When you initiate a VSC task, VSC first verifies whether you have the correct vCenter Server permission for that task. If the vCenter Server permission is not sufficient to allow you to perform the task, VSC does not have to check the ONTAP privileges for that storage system because you did not pass the initial vCenter Server security check. As a result, you cannot access the storage system.

If the vCenter Server permission is sufficient, VSC then checks the ONTAP RBAC privileges (your ONTAP role) that are associated with the storage system credentials (the user name and password) to

determine whether you have sufficient privileges to perform the storage operations that are required by that VSC task on that storage system. If you have the correct ONTAP privileges, you can access the storage system and perform the VSC task. The ONTAP roles determine the VSC tasks that you can perform on the storage system.

Each storage system has one set of ONTAP privileges associated with it.

Using both ONTAP RBAC and vCenter Server RBAC provides the following benefits:

- **Security**  
The administrator can control which users can perform which tasks at a fine-grained vCenter Server object level and at a storage system level.
- **Audit information**  
In many cases, VSC provides an audit trail on the storage system that enables you to track events back to the vCenter Server user who performed the storage modifications.
- **Usability**  
You can maintain all of the controller credentials in one place.

## Recommended ONTAP roles when using VSC for VMware vSphere

You can set up several recommended ONTAP roles for working with Virtual Storage Console for VMware vSphere and role-based access control (RBAC). These roles contain the ONTAP privileges that are required to perform the required storage operations that are executed by the Virtual Storage Console (VSC) tasks.

To create new user roles, you must log in as an administrator on storage systems running ONTAP. You can create ONTAP roles using the one of the following:

- **RBAC User Creator for ONTAP tool**  
<https://community.netapp.com/t5/Virtualization-and-Cloud-Articles-and-Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-Replication-Adapter-7-0/ta-p/133203>
- **OnCommand System Manager**, which can be downloaded for either a Windows platform or a Linux platform

Each ONTAP role has an associated user name and password pair, which constitute the credentials of the role. If you do not log in by using these credentials, you cannot access the storage operations that are associated with the role. Each ONTAP role that you create is associated with one user name. You must log in to the storage system by using the appropriate user name and password pair if you want to perform those role-based tasks on the storage system.

As a security measure, the VSC-specific ONTAP roles are ordered hierarchically. This means that the first role is the most restrictive role and has only the privileges that are associated with the most basic set of VSC storage operations. The next role includes both its own privileges and all of the privileges that are associated with the previous role. Each additional role is less restrictive with regard to the supported storage operations.

The following are some of the recommended ONTAP RBAC roles when using VSC. After you create these roles, you can assign the roles to users who have to perform tasks related to storage, such as provisioning virtual machines.

1. **Discovery**  
This role enables you to add storage systems.
2. **Create Storage**  
This role enables you to create storage. This role also includes all of the privileges that are associated with the Discovery role.
3. **Modify Storage**



This role enables you to modify storage. This role also includes all of the privileges that are associated with the Discovery role and the Create Storage role.

#### 4. Destroy Storage

This role enables you to destroy storage. This role also includes all of the privileges that are associated with the Discovery role, the Create Storage role, and the Modify Storage role.

If you are using VASA Provider for ONTAP, you should also set up a policy-based management (PBM) role. This role enables you to manage storage by using storage policies. This role requires that you also set up the Discovery role.

## How to configure ONTAP role-based access control for VSC for VMware vSphere

You must configure ONTAP role-based access control (RBAC) on the storage system if you want to use role-based access control with Virtual Storage Console for VMware vSphere. You can create one or more custom user accounts with limited access privileges with the RBAC feature of ONTAP.

You can use the administrator login credentials or root login credentials to access all of the VSC tasks. You must perform the following tasks from your ONTAP system:

- Create the required ONTAP roles

**Note:** You can use the RBAC User Creator for ONTAP tool to create these roles.

<https://community.netapp.com/t5/Virtualization-and-Cloud-Articles-and-Resources/RBAC-User-Creator-tool-for-VSC-VASA-Provider-and-Storage-Replication-Adapter-7-0/ta-p/133203>

- Create a user name and password (the storage system credentials) for each role

You require these storage system credentials to configure the storage systems for VSC. You can configure storage systems for VSC by entering the credentials in VSC. Each time you log in to a storage system by using these credentials, you are presented with the set of VSC functions that you set up in ONTAP when you created the credentials.

**Note:** You must refer to the NetApp knowledge base articles if you want to manually configure roles and privileges using ONTAP commands.

- <https://kb.netapp.com/support/s/article/ka21A0000008r19QAA/VSC-VASA-and-SRA-7-0-ONTAP-RBAC-Configuration>
- <https://kb.netapp.com/support/s/article/ka21A0000008rkk/Roll-up-of-all-commands-for-VSC-and-SRA-for-SVM-level>

VSC performs an initial privilege validation of ONTAP RBAC roles when you log in. VSC does not perform the upfront validation if the storage system is directly connected to a Storage Virtual Machine (SVM). Instead, VSC checks and enforces the privileges later in the task workflow.

## Enabling VASA Provider for configuring virtual datastores

---

If you want to configure virtual datastores in your vCenter Server environment, you must enable the VASA Provider extension that is to be used with Virtual Storage Console (VSC) after you deploy the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

### Related tasks

[Enabling extensions for the virtual appliance for VSC, VASA Provider, and SRA](#) on page 21

## VASA Provider for ONTAP overview

VASA Provider for ONTAP uses VMware vSphere APIs for Storage Awareness (VASA) to improve storage management between Virtual Storage Console for VMware vSphere and the vCenter Server. You can also use VASA Provider to manage features such as storage capability profiles, alarms, and virtual volumes (VVols).

You must have installed VASA Provider if you want to use VVol datastores. VVol datastores provide a software-defined solution for the granular management of virtual machines. You can create a VVol datastore without having detailed knowledge of the storage components that make up a VVol datastore.

In addition to enabling you to create and manage VVol datastores, VASA Provider also performs the following tasks:

- Translates VASA APIs to storage APIs and manages the APIs.
- Allows you to set up storage capability profiles that the vCenter Server can use. These profiles work with storage on both standard volumes and VVol datastores.
- Manages multiple storage systems running ONTAP.
- Checks for compliance between the datastores and the storage capability profiles.
- Allows you to set alarms for volume thresholds and aggregate thresholds.

### VASA Provider and the vCenter Server

VASA Provider sends information about storage used by VMware vSphere to the vCenter Server. Sharing this information enables you to make more informed decisions about provisioning virtual machines. It also allows the vCenter Server to warn you when certain storage conditions might affect your VMware environment.

VASA Provider communicates with the vCenter Server by using VASA APIs and communicates with ONTAP by using NetApp APIs called ZAPIs.

### VASA Provider and the VSC GUI

VASA Provider is deployed as an `.ova` virtual appliance and is managed by the VMware vSphere Web Client version of Virtual Storage Console (VSC). Because VASA Provider is integrated with VSC, you must use the VASA Provider section in the VSC GUI to perform certain VASA Provider tasks, including the following:

- Setting alarm thresholds

- Creating storage capability profiles, both by manually setting them up and by using VASA Provider's auto-generate feature
- Mapping storage to storage capability profiles
- Checking for datastore compliance with its mapped storage capability profile

#### **VASA Provider interfaces for VVol datastores and maintenance tasks**

In addition to having a section in the VSC GUI, VASA Provider also has menu options in the VMware vSphere Web Client Actions menu and a maintenance menu that you access from the console of the virtual appliance.

- To create and maintain VVol datastores, you must use the VASA Provider for ONTAP menu option in the VMware vSphere Web Client Actions menu.
- To adjust settings for VASA Provider and perform maintenance tasks, you must use the VASA Provider maintenance menus.

The Main Menu provides several options for configuring VASA Provider and for performing diagnostic operations.

If you have to create a support bundle, you should use the Vendor Provider Control Panel screen located at [https://vm\\_ip:9083](https://vm_ip:9083). The Vendor Provider Control Panel creates a more complete bundle than the bundle that the maintenance menu creates.

## Configuring VSC, VASA Provider, and SRA for disaster recovery

---

If you want to configure your vCenter server for disaster recovery, then you must enable SRA post deployment of VSC, VASA Provider, and SRA7.0. The deployment of 7.0 version of VSC, VASA Provider, and SRA installs VSC by default.

### Related tasks

[Enabling extensions for the virtual appliance for VSC, VASA Provider, and SRA](#) on page 21

## Setting up initial configurations for Storage Replication Adapter

Before you can run Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager, you must perform certain configuration tasks, such as setting up the storage systems on the sites and configuring protected and recovery sites. You can also customize SRA by using the Site Recover Manager Array Manager wizard.

### Configuring Storage Replication Adapter for SAN environment

You must set up the storage systems before running Storage Replication Adapter (SRA) for Site Recovery Manager (SRM).

#### Before you begin

You must have installed the following programs on the protected site and the recovery site:

- SRM  
Documentation about installing SRM is on the VMware site.  
[VMware Site Recovery Manager Documentation](#)
- SRA  
The adapter is installed on SRM and the SRA server.

#### Steps

1. Verify that the primary ESXi hosts are connected to the LUNs in the primary storage system on the protected site.
2. Verify that the LUNS are in igroups that have the `ostype` option set to `vmware` on the primary storage system.
3. Verify that the ESXi hosts at the recovery site have appropriate FC or iSCSI connectivity to the Storage Virtual Machine (SVM).

You can do this either by verifying that the ESXi hosts have local LUNs connected on the SVM or by using the `fc show initiators` command or the `iscsi show initiators` command on the SVMs.

## Configuring Storage Replication Adapter for NAS environment

You must set up the storage systems before running Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager (SRM).

### Before you begin

You must have installed the following programs on the protected site and the recovery site:

- SRM  
Documentation about installing SRM is on the VMware site.  
[VMware Site Recovery Manager Documentation](#)
- SRA  
The adapter is installed on SRM and the SRA server.

### Steps

1. Verify that the datastores at the protected site contain virtual machines that are registered with vCenter Server.
2. Verify that the ESXi hosts at the protected site have mounted the NFS exports volumes from the Storage Virtual Machine (SVM).
3. Verify that valid addresses such as the IP address, host name, or FQDN on which the NFS exports are present are specified in the **NFS Addresses** field when using the **Array Manager** wizard to add arrays to SRM.
4. Use the `ping` command on each ESXi host containing secondary storage to verify that the host has a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM.

### Related information

[NetApp Support Site: mysupport.netapp.com](http://mysupport.netapp.com)

## Upgrade overview of Virtual Storage Console, VASA Provider, and Storage Replication Adapter

---

If you have an existing deployment of Virtual Storage Console (VSC), VASA Provider, or Storage Replication Adapter (SRA) into your vCenter Server environment, then you can upgrade to the 7.0 version of virtual appliance for Virtual Storage Console, VASA Provider, and Storage Replication Adapter. But the process of upgrade depends on your deployment model and the software version of your products.

You may have any one of the following combination of products in your deployment:

- VSC only
- VSC and VASA Provider
- VSC and SRA
- VSC, VASA Provider, and SRA

When you have VSC in any of the deployment models, then to upgrade to the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA you must migrate your data and configuration files manually. When you have VASA Provider 6.x in any of the deployment models, then you must migrate the data and configuration files manually. When you have SRA 4.0 in any of the above deployment models, then you must always perform an in-upgrade to the 7.0 version of virtual appliance.

The support for upgrade or migrate for virtual appliance for VSC, VASA Provider, and SRA is as follows:

- In-place upgrade from SRA 4.0 to 7.0 version of virtual appliance for VSC, VASA Provider, and SRA.
- Migrating from VSC 6.2.x to 7.0 virtual appliance for VSC, VASA Provider, and SRA.
- Migrating from VP 6.2.x to 7.0 version of virtual appliance for VSC, VASA Provider, and SRA.

## Unregistering VSC from a Windows setup

Before upgrading to the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), you must unregister any earlier version of VSC from the Windows setup in your vCenter Server environment.

### Steps

1. Log in to the Windows server where VSC is installed by using the administrator credentials.
2. Stop the vSphere Web Client service.

If the version of your vCenter Server instance is...	Do this...
6.5	Enter <code>C:\Program Files\VMware\vCenter Server\vmmon&gt;. \vmmon-cli --stop vsphere-client</code> in the command-line interface (CLI).

If the version of your vCenter Server instance is...	Do this...
6.0 U3	Stop the vSphere Web Client service by using Windows services: <ol style="list-style-type: none"> <li>a. Open Server Manager on the Windows system where vCenter Server is installed.</li> <li>b. Select <b>Configuration &gt; Services</b>.</li> <li>c. Select <b>VMware vSphere Web Client</b>, and then click <b>Restart</b>.</li> </ol>
6.x and deployed as an appliance	<ol style="list-style-type: none"> <li>a. Log in to the vCenter Server using SSH as root.</li> <li>b. Stop the vSphere Web Client service:               <pre>service vsphere-client stop</pre> </li> </ol>
6.x and deployed on a Windows system	At the command prompt: <ol style="list-style-type: none"> <li>a. Enter the command               <pre>cd C:\Program Files\VMware\vCenter Server\bin</pre> </li> <li>b. Stop the vSphere Web Client service:               <pre>service-control --stop vspherewebclientsvc</pre> </li> </ol>
<b>3.</b> Go to the folder <code>C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity</code> .	
The <code>ProgramData</code> folder is a hidden folder. You must enter the complete file path in Windows Explorer to access the folder.	
<b>4.</b> Delete the directories that include the <code>com.netapp*</code> extension to delete the UI extensions.	
Deleting the directories removes both the VSC extension and the VASA Provider extension.	
<b>5.</b> Start the vSphere Web Client service.	
If the version of your vCenter Server instance is...	Do this...
6.5	Enter <code>C:\Program Files\VMware\vCenter Server\vmmon&gt;. \vmmon-cli --start vsphere-client</code> in the CLI.
6.0 U3	Stop the vSphere Web Client service by using Windows services: <ol style="list-style-type: none"> <li>a. Open Server Manager on the Windows system where vCenter Server is installed.</li> <li>b. Select <b>Configuration &gt; Services</b>.</li> <li>c. Select <b>VMware vSphere Web Client</b>, and then click <b>Restart</b>.</li> </ol>
6.x and deployed as an appliance	<ol style="list-style-type: none"> <li>a. Log in to the vCenter Server using SSH as root.</li> <li>b. Start the vSphere Web Client service:               <pre>service vsphere-client start</pre> </li> </ol>

If the version of your vCenter Server instance is...	Do this...
6.x and deployed on a Windows system	<p>At the command prompt:</p> <ol style="list-style-type: none"> <li>a. Enter the command           <pre>cd C:\Program Files\VMware\vCenter Server\bin</pre> </li> <li>b. Start the vSphere Web Client service:           <pre>service-control --start vspherewebclientsvc</pre> </li> </ol>

The vSphere Web Client service takes several minutes to restart and initialize correctly.

## Migrating existing VSC installation to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA

If you have only Virtual Storage Console (VSC) installed in your setup or if you have installed VSC with VASA Provider, then to upgrade to the 7.0 version of the virtual appliance, you must migrate your existing VSC setup to the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

### Before you begin

- You must have created a backup of your existing VSC data files and configuration files.
- You must have downloaded the .ova file for the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

### About this task

If you have installed VSC 6.2.1, VASA Provider 6.2, and SRA 4.0 in your deployment model, you must first migrate VSC and VASA Provider manually, and then perform an in-place upgrade of SRA. If you have VSC version earlier to 6.2.1, then you must first upgrade to VSC 6.2.1 and later upgrade to virtual appliance for VSC, VASA Provider, and SRA.

**Note:** Migration is supported only from VSC 6.2.1 to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

### Steps

1. Unregister the existing installation of VSC from your vCenter Server Managed Object Browser (MOB) as well as from vCenter Server.

*Unregistering VSC from a Windows setup* on page 54

2. Log in to your vCenter Server instance with administrator credentials.
3. Click **Home** > **Administration**, and then click **Roles**.
4. Delete any pre-configured VSC roles.

VSC 6.2.1 supported features such as backup, recovery, migration, and cloning, and includes roles to support these features. The 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA does not support backup, recovery, migration, and cloning. When you upgrade your existing VSC setup to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, the existing roles and privileges are available in the new deployment and might cause issues. It is a good practice to remove any stale VSC roles and privileges that are not supported by the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.



*Uninstall does not remove standard VSC roles* on page 61

5. Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.  
*Deploying the virtual appliance for VSC, VASA Provider, and SRA* on page 20
6. Manually gather the cluster details from your existing VSC 6.2.1 setup, using the **Storage Systems** page, and then add the clusters to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA .
7. Note any changes that are made to the following metadata files in the VSC 6.2.1 setup: `vscPreferences.xml`, `ehusettings.xml`, and `kaminoPreferences.xml`.
8. If there is any change to the metadata files, then manually update the files of the virtual appliance for VSC, VASA Provider, and SRA to add the collected metadata details by using the “diag” user credentials, and then restart the VSC service by using the maintenance console.
  - a. Log in to the maintenance console.
  - b. Enter **1** to access the **Application Configuration** menu.
  - c. In the **Application Configuration** menu, enter **3** to stop the VSC service.
  - d. Enter **2** to restart the VSC service.

**Note:** You must restart the VSC service for the changes in the `ehusettings.xml` file to take effect.

## Migrating existing VASA Provider installation to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA

If you have VASA Provider installed along with Virtual Storage Console (VSC) in your setup, then to upgrade to the 7.0 version of VASA Provider, you must migrate your existing VASA Provider setup to the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

### Before you begin

- You must have created a backup of your existing data files and configuration files.
- You must have downloaded the `.ova` template for the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

### About this task

If your existing setup of VASA Provider is earlier than version 6.2, you must first upgrade to VASA Provider 6.2.

*VASA Provider 6.2 for Clustered Data ONTAP® User Guide*

**Note:** Migration is supported only from VASA Provider 6.2 to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

### Steps

1. Access the web command-line interface (CLI) of VASA Provider 6.2.
2. Note down the details of the clusters in your vCenter Server environment:

**cluster list**

3. Unregister VASA Provider from the vCenter Server instance.
4. Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA on a new appliance by using the IP address and credentials of the vCenter Server instance from where VASA Provider was unregistered.

*[Deploying the virtual appliance for VSC, VASA Provider, and SRA](#) on page 20*

5. Enable the VASA Provider extension.  
*[Enabling extensions for the virtual appliance for VSC, VASA Provider, and SRA](#) on page 21*
6. Add the cluster details that you collected earlier to the virtual appliance by using the VSC GUI.
7. Log in to the web CLI of VASA Provider.
8. Recover the VASA Provider database using `vp dr_recoverfdb` command.

After the database recovery process is complete, all of the virtual volume (VVOL) datastores, storage capability profiles, and virtual machines and their VVOL datastores are restored to the virtual appliance database and are accessible from vCenter Server and ESXi hosts.

9. Register VASA Provider with your vCenter Server instance from the web CLI: `vcenter register -vcenter_ip=<vcenter_ip> -username=<vcenter-username> -password=<vcenter-password>`

You must run this command as the VASA Provider database recover would have reset the VASA Provider registration data.

**Related tasks**

*[Manually adding storage systems](#) on page 38*

## Upgrading from Storage Replication Adapter 4.0 to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA

You can deploy Storage Replication Adapter (SRA) with Virtual Storage Console (VSC) and VASA Provider, or you can deploy only SRA with VSC. In either of these deployment scenarios, you must upgrade SRA to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. You can perform an in-place upgrade from your existing setup of SRA to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

**Before you begin**

- You must have created a backup of your existing SRA data.
- You must have downloaded the `unified-virtual-appliance-for-vsc-vp-sra-7.0-upgrade.iso` file for the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA.

**About this task**

If your existing setup of SRA is earlier than version 4.0, you must upgrade to SRA 4.0.

*[Storage Replication Adapter 4.0 for ONTAP Installation and Setup Guide](#)*

### Steps

1. Power off your SRA virtual appliance.
2. Mount the downloaded ISO file to the SRA virtual appliance, and then select the **Connected** checkbox.
3. Power on the SRA virtual appliance, and then access the maintenance console.
4. At the **Main Menu** prompt, enter option 1 for **Upgrade**.

After the upgrade completes, the SRA virtual appliance restarts.

**Note:** During the upgrade, the SRA virtual appliance will not be registered to the vCenter Server instance as SRA 4.0 will not have vCenter Server configuration information.

5. Access `https://<appliance_ip>:8143/Register.html` to register the upgraded SRA virtual appliance to the required vCenter Server instance.
6. Uninstall the SRA 4.0 plug-in from the SRM server.
7. Install the SRA 7.0 plug-in on the SRM server.
8. Enter the IP address of the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, when prompted.

## Troubleshooting VSC, VASA Provider, and SRA virtual appliance

---

If you encounter unexpected behavior during the installation or configuration of VSC, VASA Provider, and SRA virtual appliance for VMware vSphere, you can follow specific troubleshooting procedures to identify and resolve the cause of such issues.

### Information at NetApp Support Site

The NetApp Virtual Storage Console for VMware vSphere support portal provides self-service troubleshooting videos and knowledge base articles in addition to other services.

The NetApp VSC support portal is online at:

<http://mysupport.netapp.com/NOW/products/vsc/>

### Information available at VSC NetApp Communities Forum

You can submit general questions related to Virtual Storage Console for VMware vSphere to the VSC NetApp Communities Forum.

The VSC NetApp Communities Forum is online at <http://community.netapp.com/t5/Virtualization-and-Cloud/ct-p/virtualization-and-cloud>. For specific VSC information, select VMware Solutions Discussions.

## Collecting the VSC, VASA Provider, and SRA virtual appliance log files

You can use the GUI of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) virtual appliance of your vCenter Server to collect the log files. Technical support might ask you to collect the log files to help troubleshoot a problem.

#### Steps

1. Open the vSphere Client and log into your vCenter Server.
2. Click **Virtual Storage Console** icon from the **Inventories** panel, and then click the **Configuration**.
3. Select **Export VSC Logs**, and then click **Submit**.
4. When prompted, save the file to your local computer.

#### After you finish

Send the .zip file to technical support.

## Unrecognized storage systems issue

The dashboard of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) displays alerts about unrecognized storage systems if

authentication fails for any storage system or if any storage system is not configured in the vCenter Server.

**About this task**

This issue may be caused if the storage system credentials or the storage system are updated in ONTAP, but are not updated in the vCenter Server. When NFS datastores are mounted over a private network or on any non-NetApp storage system in the vCenter Server, VSC discovery lists the datastores as unknown.


Storage systems with IPv6 IP addresses are also listed as unrecognized.

**Steps**

1. Access the dashboard of the virtual appliance for VSC, VASA Provider, and SRA.

2. Click  .

3. Click the link for the storage system for which an alert is displayed.

If storage system...	Do the following...
Has authentication failure	<ol style="list-style-type: none"> <li>a. Right-click the storage system with authentication failure, and click <b>Modify</b>.</li> <li>b. Enter the appropriate credentials in the Modify Storage Systems dialog box, and click <b>OK</b>.</li> </ol>
Has unknown error	<ol style="list-style-type: none"> <li>a. Right-click the storage system with unknown status and verify the error.</li> <li>b. Click  <b>Add</b> , and add the required details of the storage system in the Add Storage System dialog box.</li> <li>c. Click <b>OK</b>.</li> </ol>

When the credentials are not updated in vCenter Server, add the credentials to your vCenter Server. If the alert is due to storage system not added to your vCenter Server, then add the storage system.

## Uninstall does not remove standard VSC roles

When you uninstall Virtual Storage Console for VMware vSphere, the standard VSC roles remain intact. This is expected behavior and does not affect the performance of VSC or your ability to upgrade to a new version of VSC. You can manually delete these roles, if required.

While the uninstall program does not remove the roles, it removes the localized names for the VSC-specific privileges and appends the following prefix to them: “XXX missing privilege”. For example, if you open the vSphere Edit Role dialog box after you install VSC, you will see the VSC-specific privileges listed as `XXX missing privilege.<privilege name>.label not found XXX`.

This behavior happens because the vCenter Server does not provide an option to remove privileges.

When you reinstall VSC or upgrade to a newer version of VSC, all of the standard VSC roles and VSC-specific privileges are restored.

*Migrating existing VSC installation to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA on page 56*

## Error while accessing the virtual appliance Summary page


You may get error `/opt/netapp/vscserver/etc/vsc/performance.json` (No such file or directory) while accessing VSC Summary page post deployment.

### Description

When you try to access the VSC dashboard after the deployment of the virtual appliance for VSC, VASA Provider, and SRA, you may get errors. This is because the scheduler initialization process has not completed.

### Workaround

You must wait for few seconds post deployment of virtual appliance for the performance scheduler

initialization to complete, and then click the  button to get the latest data.

## Troubleshooting information in log files

There are several log files in the `/opt/netapp/vscserver/logs` directory and the `/opt/netapp/vpserver/logs` directory that you can check if you encounter a problem.

The following two log files can be helpful in identifying problems:

- `cxfl.log`, which contains information about API traffic into and out of VASA Provider
- `vvolvpl.log`, which contains all log information about VASA Provider

In addition, the VASA Provider web command-line interface (CLI) page contains the API calls that were made, the errors that were returned, and several performance-related counters. The web CLI page is located at `https://<IP_address_or_hostname>:9083/stats`.

## VASA Provider known issues and limitations

VASA Provider does not support vCenter Server instances in linked mode.

VASA Provider has the following issues when vCenter Server instances are in linked mode:

- While creating a virtual volume (VVol) datastore on a vCenter Server instance other than the first vCenter Server instance, VASA Provider displays the error message `Unable to create a vvol datastore due to insufficient privileges`.
- The storage capability profile that is created for one vCenter Server instance is displayed on the other vCenter Server instances in linked mode.

### VASA Provider registration fails with vCenter Server 6.5

The VASA Provider registration with vCenter Server version 6.5 fails due to VMware Profile Driven Storage Service.

The registration of VASA Provider to Virtual Storage Console (VSC) fails when VSC is running on vCenter Server version 6.5. This is a known behaviour of vCenter Server as sometimes Profile Driven Storage Service is stopped by the vCenter Server.

### Workaround

You must log out and log in to your vCenter Server to fix this issue.

## VVol datastore provisioning fails with vCenter Server 6.5

The provisioning of virtual volume (VVol) datastores might fail with the error message `Unable to complete mount VVol datastore on all hosts`. You can work around this issue to complete the VVol datastore provisioning process.

### Steps

- Restart the vCenter Server “sps” service:

If vCenter Server is deployed...	Do this...
As an appliance	<ol style="list-style-type: none"> <li>Stop the vCenter Server “sps” service:  <code>service-control --stop vmware-sps</code>                      .</li> <li>Start the vCenter Server “sps” service:  <code>service-control --start vmware-sps</code>                      .</li> </ol>
On a Windows system	<p>At the command prompt:</p> <ol style="list-style-type: none"> <li>Enter the command  <code>cd C:\Program Files\VMware\vCenter Server\bin</code>                      .</li> <li>Stop the vCenter Server “sps” service:  <code>service-control --stop vimPBSM</code>                      .</li> <li>Start the vCenter Server “sps” service:  <code>service-control --start vimPBSM</code></li> </ol>

- From the vSphere Web Client **Home** page, click **Hosts and Clusters**.
- Select the datacenter where you want to provision the datastore.
- Right-click the datastore or cluster, and then select **Storage > New Datastore**.
- Select **VVol** as the type of the datastore, and then click **Next**.
- In the **Name and container selection** field, enter a name for the datastore.  
 The new datastore is created in the Backing storage container section.
- Select the required backing storage container, and click **Next** to complete the creation of the VVol datastore.

## Resolving VASA Provider registration issues

The VASA Provider for ONTAP menu might not be displayed in the Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) GUI even after enabling VASA Provider. This issue might occur due to the improper cleanup of legacy registered instances of VASA Provider.

You must clean up legacy VASA Provider instances, register VSC with the vCenter Server instance again, and then enable VASA Provider.

### Steps

1. Access the managed access browser of your vCenter Server instance: `https://<vCenter_ip>/mob`.
2. Click **Content > Extension Manager > Unregister Extension**.
3. Unregister all of the `com.netapp.*` extensions by selecting the following extensions in the **UnregisterExtension** key dialog box:
  - `com.netapp.nvpf`
  - `com.netapp.nvpf.webclient`
  - `com.netapp.vasa.vvol.webclient`
4. Launch PuTTY, and log in to the vCenter Server instance by using the root user credentials.
5. Switch to the `vsphere-client-serenity` directory:
 

```
cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity
```
6. Stop the vSphere Web Client service:
  - For vCenter Server 5.x:
 

```
service vsphere-client stop
```
  - For vCenter Server 6.x:
 

```
service-control --stop vsphere-client
```
7. Delete the directories that have the VSC UI extensions:
 

```
rm -rf com.netapp*
```

**Note:** You must include the asterisk (\*) at the end of the command.

The command removes both the VSC extension and the VASA Provider extension.
8. Restart the vSphere Web Client service:
  - For vCenter Server 5.x:
 

```
service vsphere-client start
```
  - For vCenter Server 6.x:
 

```
service-control --start vsphere-client
```

The vSphere Web Client service takes several minutes to restart and initialize correctly.

### After you finish

After the vSphere Web Client service has restarted, you should register VSC with the vCenter Server instance, and then register VASA Provider with VSC.



## Unable to add storage to VVol datastore created using the VMware wizard

You cannot add storage to virtual volume (VVol) datastores if the datastore name is different from the name of the storage container.

### Description

When you try to add FlexVol storage to a VVol datastore, the operation fails and the following error message is displayed: Problem checking access for privilege:

```
nvpfVSC.Kamino.Datastore.com.netapp.nvpf.Provision on object:
HostSystem:undefined, occurred on the server. See VP server logs for more
details. This issue occurs because the name that is specified for the VVol
datastore is different from the name of the VASA Provider storage container.
For adding storage to a VVol datastore, the name of the VVol datastore
must be the same as the name of the storage container.
```

### Workaround

1. Right-click the VVol datastore to which you want to add storage, and then click **VASA Provider for ONTAP > Edit Properties of VVOL Datastore**.
2. Rename the datastore in the Datastore/Storage container name field, and then click **OK**.

## Configuring VASA Provider to work with SSH

You can set up VASA Provider to use SSH for secure access by configuring the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

### About this task

When you configure SSH, you must log in as the maintenance user. This is because root access to VASA Provider has been disabled. If you use other login credentials, you cannot use SSH to access VASA Provider.

### Steps

1. From the vCenter Server, open a console to the virtual appliance for VSC, VASA Provider, and SRA.
2. Log in as the maintenance user.
3. Enter **3** to select **System Configuration**.
4. Enter **6** to select **Enable SSH Access**.
5. Enter **y** in the confirmation dialog box.

## Configuring 7.0 virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to use SSH for remote diag access

You can configure VASA Provider to enable SSH access for the diag user.

### Before you begin

VASA Provider extension must be enabled for your vCenter Server.

**About this task**

Using SSH to access the diag user has the following limitations:

- You are allowed only one login per activation of SSH.
- SSH access to the diag user is disabled when one of the following happens:
  - The time expires. The login remains valid only until midnight the next day.
  - You log in as a diag user again using SSH.

**Steps**

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maint user.
3. Enter 4 to select **Support and Diagnostics**.
4. Enter 3 to select **Enable remote diagnostics access**.
5. Enter “y” on the **Confirmation** dialog box, to enable remote diagnostic access.
6. Enter a password for the remote diagnostic access.

## SRA fails to perform optimally in a highly scaled environment

If SRA is not performing optimally in a highly scaled environment and you notice issues such as timeout error or zapi ontap timeout, then you must modify the timeout intervals.

**Corrective action**

If you encounter this problem, you must modify the following settings:

**Storage Provider settings**

- Timeout interval: Increase the value of the `StorageProvider.resignatureTimeout` option from 900 seconds to 12000 seconds.
- Enable the `StorageProvider.autoResignatureMode` option.

See the VMware documentation for modifying Storage Provider settings.

[Change Storage Provider Settings](#)

**Storage settings**

Update the timeout interval (`storage.commandTimeout`) to 12000 seconds.

See the VMware documentation for modifying Storage settings.

[VMware Site Recovery Manager](#)

## Copyright information

---

Copyright © 1994–2017 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark information

---

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## How to send comments about documentation and receive update notifications

---

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

[\*doccomments@netapp.com\*](mailto:doccomments@netapp.com)

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

# Index

## A

- accessing
  - maintenance console [34](#)
- accessing storage system
  - using role-based access control [47](#)
- accounts
  - configuring with RBAC [49](#)
- application configuration
  - maintenance console options [34](#)
- architecture
  - virtual appliance for VSC, VASA Provider, and SRA [8](#)

## C

- CD-ROM
  - adding to virtual machine [28](#)
- comments
  - how to send feedback about documentation [69](#)
- communities
  - forum for VSC for VMware vSphere information [60](#)
- configuration of virtual datastores
  - enabling VASA Provider [50](#)
- configuring disaster recovery
  - enable SRA [52](#)
- credentials
  - overview [36](#)
  - setting default, for storage systems [37](#)
  - using RBAC [49](#)
- custom user accounts
  - configuring using RBAC [49](#)
- cxfl.log
  - contains API traffic information [62](#)

## D

- data collection
  - log files [60](#)
- datastores
  - enabling mounting across subnets [33](#)
- default credentials
  - setting for storage systems [37](#)
- deploying
  - virtual appliance for VSC, VASA Provider, and SRA [20](#)
- deploying 7.0 version of the virtual appliance
  - host requirements [14](#)
- deploying 7.0 virtual appliance
  - application requirements [15](#)
  - license requirements [15](#)
- deployment
  - considerations for virtual appliance deployment [15](#)
- deployment workflow
  - existing SRA users [11](#)
  - existing VASA Provider users [11](#)
  - existing VSC users [11](#)
- discovering

- hosts [39](#)
- storage systems [39](#)
- discovery
  - manually adding storage systems to VSC [38](#)
- Disk.QFullSampleSize [25](#)
- Disk.QFullThreshold [25](#)
- documentation
  - how to receive automatic notification of changes to [69](#)
  - how to send feedback about [69](#)
- downloading
  - .ova file for the virtual appliance for VSC, VASA Provider, and SRA [19](#)

## E

- Emulex FC HBA timeouts [25](#)
- enabling extension
  - Storage Replication Adapter [21](#)
  - VASA Provider [21](#)
- error
  - accessing VSC Summary page [62](#)
- ESX hosts
  - timeout values [27](#)
- ESXi hosts
  - configuring multipathing and timeout settings [24](#)
  - settings [25](#)
- ESXi server and guest operating system
  - set by default [24](#)
- existing SRA users
  - deployment workflow [12](#)
- existing VASA Provider configuration files
  - migrating to 7.0 version of the virtual appliance [57](#)
- existing VASA Provider data files
  - migrating to 7.0 version of the virtual appliance [57](#)
- existing VASA Provider installation
  - migrating to 7.0 version of the virtual appliance [57](#)
- existing VASA Provider users
  - deployment workflow [12](#)
- existing VSC configuration files
  - migrating to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA [56](#)
- existing VSC data files
  - migrating to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA [56](#)
- existing VSC installation
  - migrating to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA [56](#)
- existing VSC users
  - deployment workflow [11](#)

## F

- feedback
  - how to send comments about documentation [69](#)

**G**

- guest OS
  - installing scripts [28](#)
  - setting timeouts for Linux [29](#)
  - setting timeouts for Solaris [30](#)
  - setting timeouts for Windows [31](#)
  - timeout values [27](#)
- GUI
  - VASA Provider [50](#)

**H**

- host requirements for
  - deployment of 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA [14](#)
- hosts
  - configuring multipathing and timeout settings for ESXi [24](#)
  - discovering [39](#)

**I**

- information
  - how to send feedback about improving documentation [69](#)
- installation workflows
  - virtual appliance for VSC, VASA Provider, and SRA [9](#)
- installing
  - guest operating system (GOS) scripts [28](#)
  - NFS plug-in for VAAI [22](#)
  - VSC, VASA Provider, and SRA virtual appliance for new user [10](#)
- iSCSI
  - enabling datastore mounting across subnets [33](#)

**K**

- kaminoprefs.xml
  - modifying to enable datastore mounting across subnets [33](#)
- known issues
  - VASA Provider [62](#)

**L**

- limitations
  - VASA Provider [62](#)
- Linux
  - setting timeouts for guest OS [29](#)
- linux\_gos\_timeout-install.iso
  - guest OS tool [29](#)
- log files
  - API traffic information in cxf.log [62](#)
  - collecting [60](#)
  - VASA Provider information in vvolvp.log [62](#)
- logs
  - collecting [60](#)

**M**

- multi-vCenter environment
  - for VSC [32](#)
- multipathing
  - configuring for ESXi hosts [24](#)
- multiple vCenter Servers
  - specifying a vCenter Server in tasks [32](#)
  - using with VSC [32](#)

**N**

- NAS
  - setting up storage systems [53](#)
- Net.TcpipHeapMax [25](#)
- Net.TcpipHeapSize [25](#)
- NetApp Support Site
  - troubleshooting information [60](#)
- network configuration
  - maintenance console options [34](#)
- new user
  - VSC, VASA Provider, and SRA virtual appliance installation [10](#)
- NFS
  - enabling datastore mounting across subnets [33](#)
- NFS plug-in for VAAI
  - copy offload [7](#)
  - overview [7](#)
  - space reservations [7](#)
- NFS.HeartbeatFrequency [25](#)
- NFS.HeartbeatMaxFailures [25](#)
- NFS.HeartbeatTimeout [25](#)
- NFS.MaxVolumes [25](#)

**O**

- object
  - storage system [43](#)
  - vSphere [43](#)
- objects
  - storage systems [42](#)
  - vSphere [42](#)
- overview
  - virtual appliance [19](#)

**P**

- parameters
  - ESXi hosts [25](#)
- path selection policy [25](#)
- permission
  - vCenter Server [43](#)
- permissions
  - vCenter Server [42](#)
- plug-ins
  - supported with VSC [7](#)
- port requirements
  - for virtual appliance deployment [15](#)
- ports
  - required for VSC [14](#)
  - VSC communication ports [14](#)
- preferences files

- what they are [33](#)
- privileges
  - native vCenter Server [42, 43](#)
  - product level [46](#)
  - vCenter Server [46](#)
- Virtual Storage Console [46](#)
- VSC [46](#)
- VSC specific [42, 43](#)

## Q

QLogic

- FC HBA timeouts [25](#)
- iSCSI HBA IP\_ARP\_Redirect [25](#)
- iSCSI HBA timeouts [25](#)

## R

RBAC

- configuring [49](#)
- guidelines for standard VSC roles [45](#)
- recommended ONTAP roles [48](#)
- standard VSC roles [44](#)
- vCenter Server [42](#)

remote diag access

- configuring [65](#)

required ports

- firewall requirements [14](#)
- VSC [14](#)

requirements

- deployment of the virtual appliance for VSC, VASA Provider, and SRA [14](#)

resources

- discovering [39](#)

role-based access control

- considerations for virtual appliance deployment [15](#)

role-based access control (RBAC)

- ONTAP [47](#)

roles

- configuring with RBAC [49](#)

## S

SAN

- setting up storage systems in [52](#)

scripts, guest operating system (GOS)

- installing [28](#)

security

- configuring using RBAC [49](#)

servers, ESXi

- configuring multipathing and timeout settings [24](#)

setting up

- ESXi server and guest operating system [24](#)
- NAS storage systems [53](#)
- SAN storage systems [52](#)

settings

- ESXi hosts [25](#)

Solaris

- setting timeouts for guest OS [30](#)

solaris\_gos\_timeout-install.iso

- guest OS tool [30](#)

SRA

- enabling by using VSC GUI [8](#)
- enabling for disaster recovery setup [52](#)
- tasks performed [6](#)

SSH

- configuring [65](#)
- configuring VASA Provider to work with [65](#)

SSL certificate

- regenerating for Virtual Storage Console [31](#)

storage capability profiles

- considerations for virtual appliance deployment [15](#)
- VASA Provider [50](#)

storage credentials

- overview [36](#)

Storage Replication Adapter

- setting up [52](#)
- upgrading to 7.0 virtual appliance [54](#)

storage resources

- discovering [39](#)

storage system alerts

- resolving unrecognized storage systems issue [60](#)

storage system discovery

- overview [36](#)

storage system prerequisites

- 7.0 virtual appliance deployment [15](#)

storage systems

- adding to VSC manually [38](#)
- assigning permissions [42, 43](#)
- configuring using RBAC [49](#)
- discovering [39](#)
- discovery and credentials overview [36](#)
- setting default credentials [37](#)
- setting up NAS [53](#)
- setting up SAN [52](#)
- specifying a vCenter Server [32](#)
- updating [40](#)

suggestions

- how to send feedback about documentation [69](#)

support and diagnostics

- maintenance console options [34](#)

system configuration

- maintenance console options [34](#)

systems

- discovery and credentials overview [36](#)

## T

timeout settings

- configuring for ESXi hosts [24](#)

timeout values

- ESXi hosts [25](#)
- recommended values [27](#)
- setting for guest OS [27](#)

tools

- setting Linux guest OS timeouts [29](#)
- setting Solaris guest OS timeouts [30](#)
- setting Windows guest OS timeouts [31](#)

troubleshooting

- checking log files [62](#)
- collecting log files [60](#)
- NetApp Communities [60](#)
- NetApp Support Site [60](#)
- SRA fails to perform in a highly scaled environment [66](#)



- unrecognized storage systems [60](#)
  - VASA Provider registration [63](#)
  - VVol datastores [65](#)
  - VVol provisioning fails [63](#)
  - Twitter
    - how to receive automatic notification of documentation changes [69](#)
- ## U
- unregistering
    - VSC from a Windows setup [54](#)
  - update command
    - forces storage system discovery [36](#)
  - upgrading
    - SRA [58](#)
    - to virtual appliance 7.0 [54](#)
  - upgrading SRA
    - to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA [58](#)
  - user interfaces
    - VASA Provider [50](#)
  - user name
    - configuring custom with RBAC [49](#)
  - using VSC GUI
    - for installing NFS plug-in for VAAI [22](#)
- ## V
- VASA Provider
    - configuring to work with SSH [65](#)
    - defined [50](#)
    - enabling by using VSC GUI [8](#)
    - GUI [50](#)
    - known issues [62](#)
    - limitations [62](#)
    - registration issues [63](#)
    - supported with VSC [7](#)
    - tasks performed [6](#)
    - upgrading to 7.0 virtual appliance [54](#)
    - using to configure virtual datastores [50](#)
  - vCenter Server
    - permission [43](#)
    - permissions [42](#)
    - privileges [46](#)
    - standard VSC roles [44, 45](#)
    - using with multiple servers with VSC [32](#)
  - virtual appliance
    - considerations for deployment [15](#)
  - virtual appliance for VSC, VASA Provider, and SRA
    - architecture [8](#)
    - deploying [20](#)
    - installation workflows [9](#)
  - virtual appliances
    - supported with VSC [7](#)
  - virtual machine
    - adding CD-ROM [28](#)
  - Virtual Storage Console
    - manually adding storage systems to [38](#)
    - privileges [46](#)
    - standard roles [44, 45](#)
    - upgrading to 7.0 virtual appliance [54](#)
    - VSC NetApp Communities Forum [60](#)
  - VSC
    - configuration tasks [24](#)
    - firewall port requirements [14](#)
    - lifecycle management for VMware environments [6](#)
    - maintenance tasks [24](#)
    - manually adding storage systems to [38](#)
    - overview [6](#)
    - recommended ONTAP RBAC roles [48](#)
    - regenerating an SSL certificate [31](#)
    - required ports [14](#)
    - selecting a vCenter Server for a task [32](#)
    - support for ONTAP RBAC [47](#)
    - support for VASA Provider and SRA plug-ins [7](#)
    - support for vCenter Server RBAC [42](#)
    - supported plug-ins [7](#)
    - tasks performed [6](#)
    - unregistration from a Windows setup [54](#)
    - using multiple vCenter Servers [32](#)
    - VASA Provider for ONTAP menu unavailable [63](#)
  - VSC log files
    - troubleshooting information [62](#)
  - VSC NetApp Communities
    - See* Communities
  - VSC roles
    - guidelines [45](#)
  - vSphere
    - object [43](#)
    - objects [42](#)
  - VVol datastore issues
    - adding storage [65](#)
  - VVol provisioning fails
    - using vCenter Server 6.5 [63](#)
  - vvolvp.log
    - contains VASA Provider information [62](#)
- ## W
- Windows
    - setting timeouts for guest OS [31](#)
  - windows\_gos\_timeout.iso
    - guest OS tool [31](#)