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

Deployment and Setup Guide for 7.2 release

July 2018 | 215-13168_B0
doccomments@netapp.com

NetApp®

Contents

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

The virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) is a product suite that includes the capabilities of VSC, VASA Provider, and SRA. You can deploy this product suite as a virtual appliance, which reduces your effort of installing and registering each product separately with the vCenter Server.

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 an environment with multiple vCenter Server instances, each vCenter Server instance that you want to manage must have its own registered instance of VSC. 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 to configure the ESXi host**
  - You can add storage controllers to VSC that both SRA and VASA Provider can leverage.

    Note: For VASA Provider, you can add storage only as clusters.

    You can add, remove, and assign credentials, and 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 monitor the performance of the datastores and virtual machines in your vCenter Server environment by using the Summary page 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 about the datastores and virtual machines that are managed by VSC.
- **Using VASA Provider to create storage capability profiles and virtual datastores, and to set alarms**

  VASA Provider for ONTAP is registered with vCenter Server as soon as you enable the VASA Provider extension. You can create and use storage capability profiles and virtual datastores. You can also set alarms to warn you when volumes and aggregates are approaching the threshold limits. You can monitor the performance of virtual machines disks (VMDKs) and the virtual machines that are created on virtual datastores.
- **Using SRA for disaster recovery**

  You can use SRA with VMware Site Recovery Manager (SRM) to configure protected sites 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 which 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
  The 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 of the features that VSC provides.

Tip: VSC has a "View" privilege that is available after the virtual appliance for VSC, VASA Provider, and SRA is installed. You can add the "View" privilege to the vCenter Server roles. The "View" privilege is required if you want to view VSC in the VMware vSphere Web Client.

Supported plug-ins for VSC

Virtual Storage Console for VMware vSphere (VSC) supports optional plug-ins to enhance the capabilities such as 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 used in conjunction with VMware Site Recovery Manager (SRM), 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.

mysupport.netapp.com

You can complete your installation from the VSC **Tools > NFS VAAI** page .

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

You can use the VMware vSphere Web Client to access VSC. Each VSC instance and VASA Provider instance must be registered with only one vCenter Server instance. Each SRA instance must be registered with Site Recovery Manager (SRM), which must be 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.

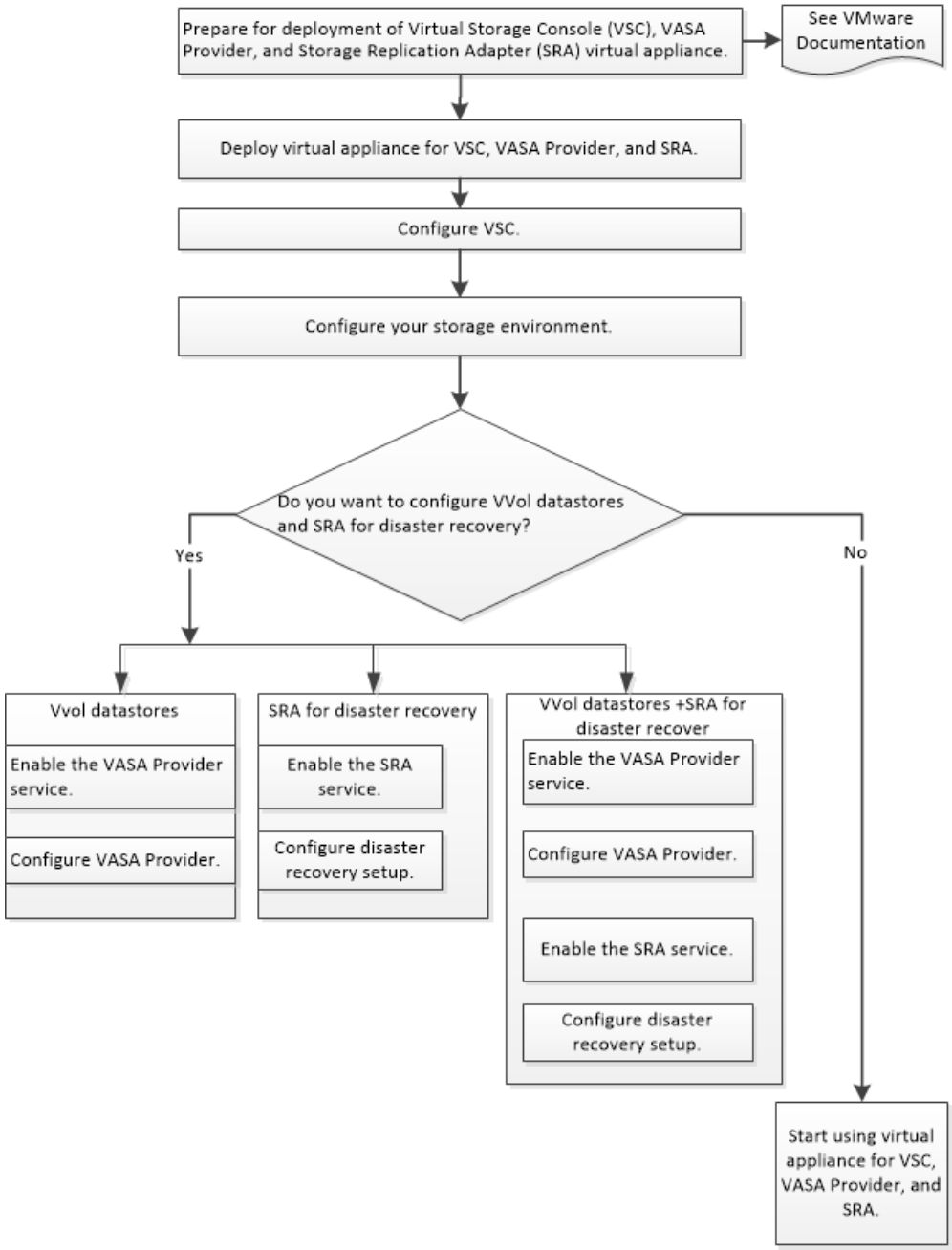
The vCenter Server instance communicates with the physical servers where the ESXi hosts are running. You can have multiple virtual machines running on the ESXi hosts. Each virtual machine can run an operating system and applications. The ESXi hosts then communicate with the storage systems. You can use 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, with VSC in combination with either VASA Provider or Storage Replication Adapter (SRA), or with VSC in combination with both VASA Provider and SRA, and you want to upgrade to the virtual appliance for VSC, VASA Provider, and SRA, you should see 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 for ONTAP, Storage Replication Adapter (SRA), or a combination of any of these products in your environment, then you must upgrade and then migrate from your existing setup to the virtual appliance for VSC, VASA Provider, and SRA or you must migrate from your existing setup to the virtual appliance for VSC, VASA Provider, and SRA.

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

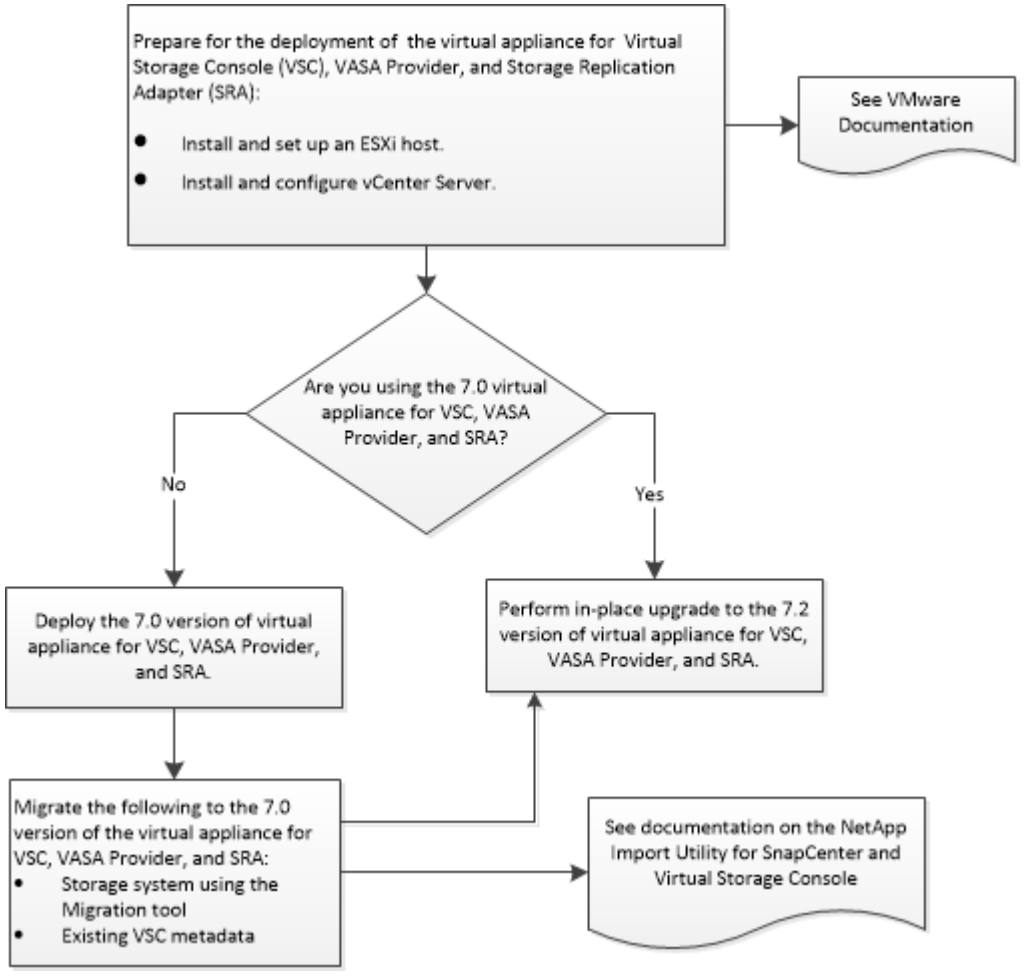
Related information

NetApp ToolChest: NetApp Import Utility for SnapCenter and Virtual Storage Console
Installing and setting up SnapCenter

Deployment workflow for existing users of VSC

If you have the 7.0 version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), then you can perform an in-place upgrade to the 7.2 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 the virtual appliance for VSC, VASA Provider, and SRA, and then migrate your VSC 6.2.1 metadata to the 7.0 version of the virtual appliance. You can then perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA .

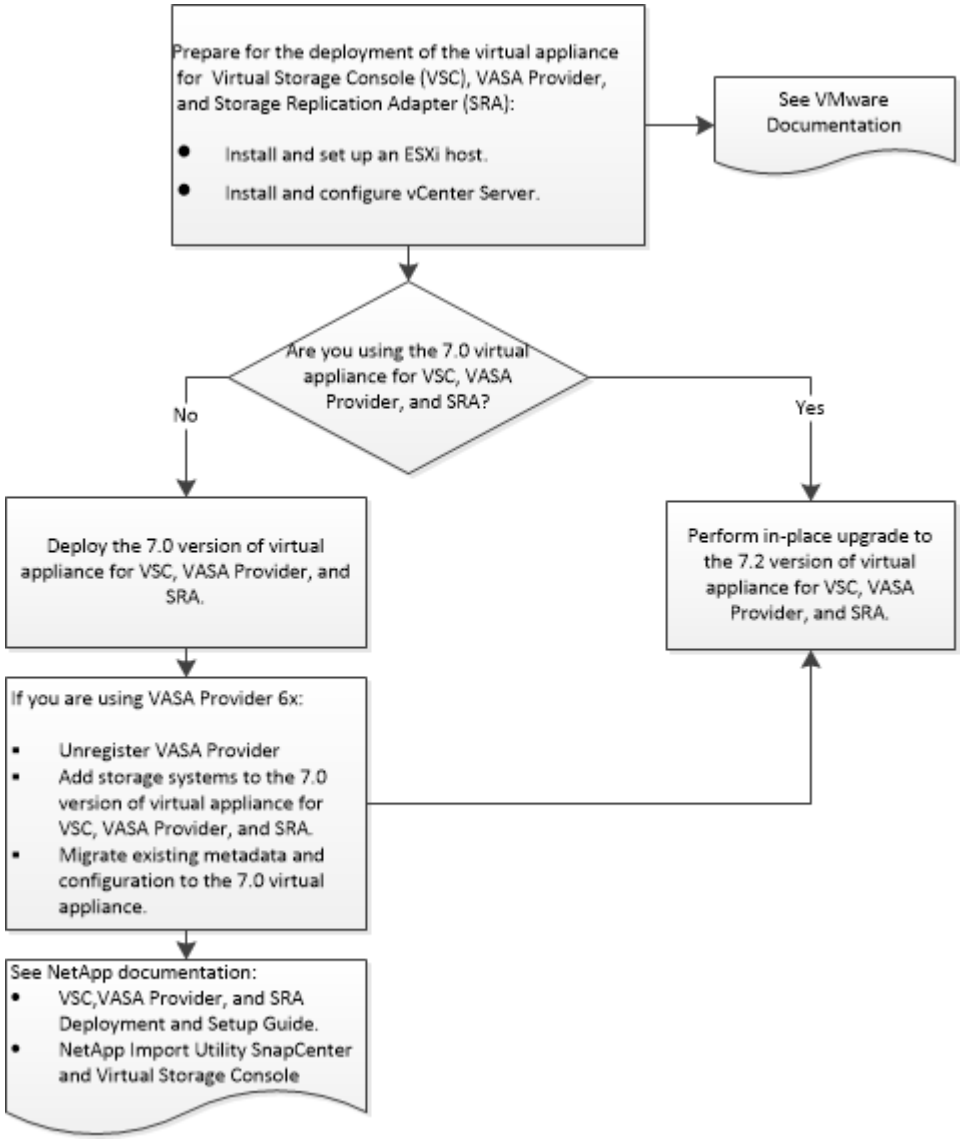


Deployment workflow for existing users of VASA Provider

If you have an existing setup of VASA Provider in your environment, then the process to upgrade to the latest 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 your version of VASA Provider is 6.2, you must deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, and migrate the metadata from your existing setup to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. You can then perform an in-place upgrade to the latest version of the virtual appliance for VSC, VASA Provider, and SRA.

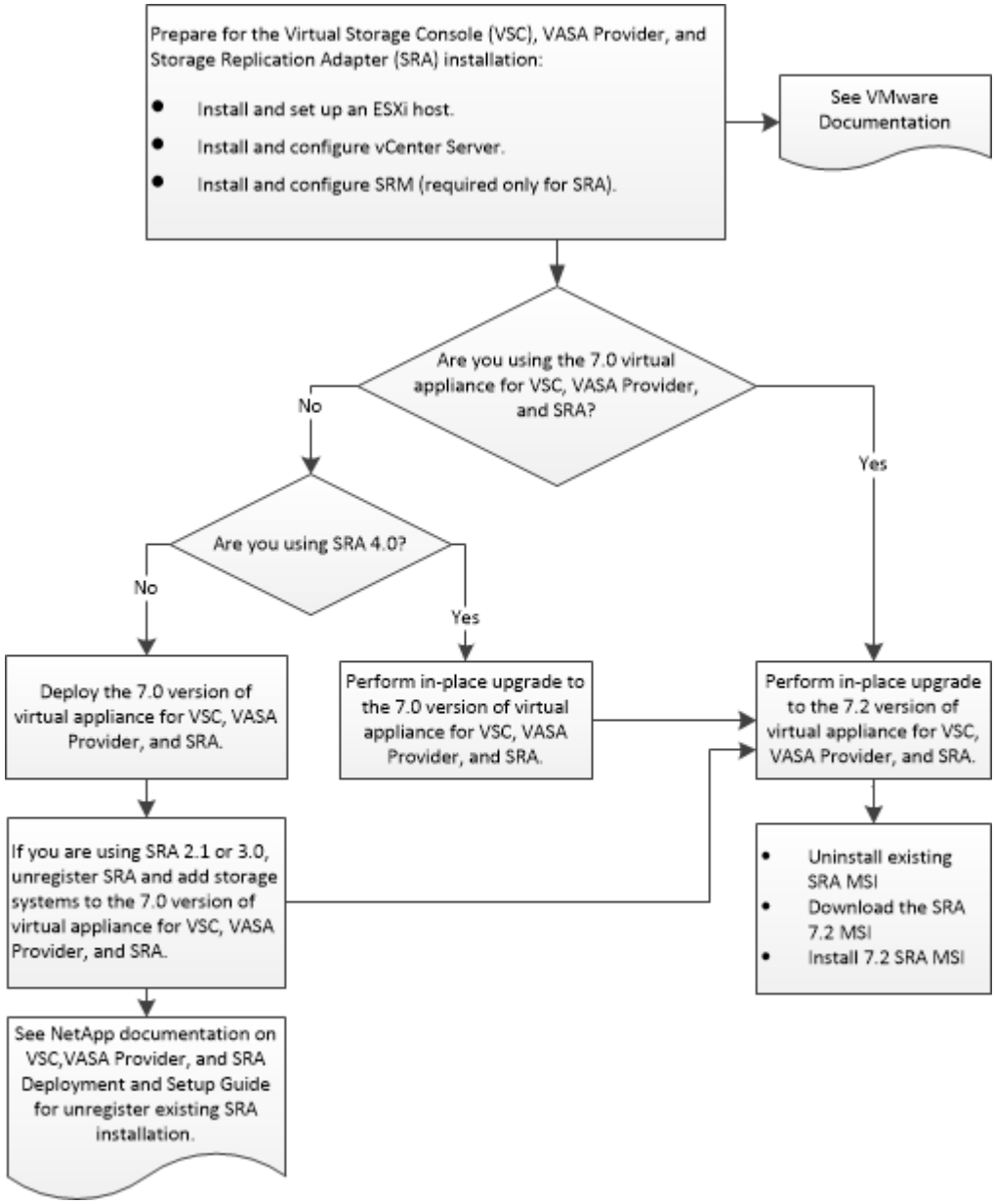
If your version of VASA Provider is earlier than version 6.2, then you must first upgrade your existing setup to VASA Provider 6.2, and then follow the upgrade procedure for the 6.2 version of VASA Provider.



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


Prepare for the Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) installation:
Install and set up an ESXi host.
Install and configure vCenter Server.
Install and configure SRM (required only for SRA).
See VMware Documentation
Are you using the 7.0 virtual appliance for VSC, VASA Provider, and SRA?
No
Yes
Are you using SRA 4.0?
No
Yes
Deploy the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA.
Perform in-place upgrade to the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA.
Perform in-place upgrade to the 7.2 version of virtual appliance for VSC, VASA Provider, and SRA.
If you are using SRA 2.1 or 3.0, unregister SRA and add storage systems to the 7.0 version of virtual appliance for VSC, VASA Provider, and SRA.
Uninstall existing SRA MSI
Download the SRA 7.2 MSI
Install 7.2 SRA MSI
See NetApp documentation on VSC,VASA Provider, and SRA Deployment and Setup Guide for unregister existing SRA installation.

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 Storage Replication Adapter (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	VSC listens for secure communications on this port.

Requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA

Before deploying 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

Host system sizing requirements

- ESX 6.0 or later, or ESXi 6.0 or later
- Recommended memory: 8 GB RAM
- Recommended CPUs: 2

Supported storage system, licensing, and applications for the virtual appliance for VSC, VASA Provider, and SRA

You should be aware of the basic storage system requirements, application requirements, and license requirements before you begin deploying the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA).

The Interoperability Matrix Tool (IMT) contains the latest information about supported versions of ONTAP, vCenter Server, and Site Recovery Manager (SRM).

You must enable the FlexClone license for performing virtual machine snapshot operations and clone operations for virtual volume (VVol) datastores.

Storage Replication Adapter (SRA) requires the following licenses:

- SnapMirror license
  You must enable the SnapMirror license for performing failover operations for SRA.
- FlexClone license
  You must enable the FlexClone license for performing test failover operations for SRA.

You must enable storage I/O to view IOPS for a datastore. You can enable the storage I/O options only if you have the Enterprise Plus license from VMware.

- *https://kb.vmware.com/s/article/1022091*
- *https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.resmgmt.doc/GUID-37CC0E44-7BC7-479C-81DC-FFFC21C1C4E3.html*

Considerations and requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA

Before you deploy 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 should consider before you deploy the virtual appliance for VSC, VASA Provider, and SRA.

Considerations	Description
First-time deployment of the virtual appliance for VSC, VASA Provider, and SRA	The deployment of the virtual appliance for VSC, VASA Provider, and SRA automatically installs the VSC features. *Overview of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) deployment* on page 19 *Deployment workflow for new users of Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) virtual appliance* on page 10

Considerations	Description
Upgrading from an existing deployment of VSC	The upgrade procedure from an existing deployment of VSC to the virtual appliance for VSC, VASA Provider, and SRA depends on the version of VSC and whether you have deployed VASA Provider and SRA. See the deployment workflows and upgrade section for more information. • *Deployment workflow for existing users of VSC, VASA Provider, and SRA* on page 11 • *Considerations for upgrading the virtual appliance for VSC, VASA Provider, and SRA* on page 59 Best practices before an upgrade: • 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. • If you modified any of the standard VSC roles, you should copy those roles to save your changes. VSC overwrites the standard roles with the current defaults each time you restart the VSC service. • 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.
Regenerating an SSL certificate for VSC	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. *Regenerating an SSL certificate for Virtual Storage Console* on page 31
Setting ESXi server values	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. • *ESXi server and guest operating system setup* on page 24 • *Configuring ESXi server multipathing and timeout settings* on page 24 • *ESXi host values set by VSC for VMware vSphere* on page 25
Guest operating system timeout values	The guest operating system (guest OS) timeout scripts set the SCSI I/O timeout values for supported Linux, Solaris, and Windows guest operating systems to provide correct failover behavior. *Timeout values for guest operating systems* on page 27

The following table presents a high-level overview of what you require to configure the virtual appliance for VSC, VASA Provider, and SRA.

Considerations	Description
Requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA	You must deploy the virtual appliance on a 64-bit Linux server with at least 4 GB of RAM. You must not deploy the virtual appliance on a client computer. Additionally, the vCenter Server instance must be running a supported version of vSphere. Some of the VSC features use products that have additional requirements, which might require that you purchase a software license.
Requirements of role-based access control (RBAC)	VSC supports both vCenter Server RBAC and ONTAP RBAC. If you plan to run VSC as an administrator, you must have all of the required permissions and privileges for all of the tasks. 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. You can create the recommended ONTAP roles by using the RBAC User Creator for ONTAP tool, which is available from the NetApp ToolChest. If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out. • *Standard roles packaged with the virtual appliance for VSC, VASA Provider, and SRA* on page 46 • *Recommended ONTAP roles when using VSC for VMware vSphere* on page 50
ONTAP version	Your storage systems must be running ONTAP 9.3 or ONTAP 9.4.
Storage capability profiles	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. The alarms warn you when a volume or an aggregate is at nearly full capacity or when a datastore is no longer in compliance with the associated storage capability profile.

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 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 starts 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 any of the following software download links depending on your requirement:

- **Virtual Storage Console**
- **NetApp VASA Provider**
- **Storage Replication Adapter**

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 plug-in on the Site Recovery Manager (SRM) server. You can download the installation file for the SRA adapter 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.
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.

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.
- You must have enabled ICMP.
  If ICMP is disabled, then the initial configuration of the virtual appliance for VSC, VASA Provider, and SRA fails, and VSC cannot start the VSC and VASA Provider services after deployment. You must manually enable the VSC and VASA Provider services after deployment.

About this task

- 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

1. Log in to the vSphere Web Client.
2. Select **Home > Host & Clusters**.
3. Right-click the required datacenter, and then click **Deploy OVA template**.
4. You can 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.

5. 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 Policies, storage location, and network
   - Administrator user name and password

     Note:

     - You must log in to the web command-line interface (CLI) by using the administrator user name and password that you set during deployment.
       If you want to change the administrator password, you must create a password with minimum length eight characters and maximum length 63 characters.
     - You should use `https://<UA_APPLIANCE_IP>:9083` to access the web CLI.
     - You must access the maintenance console by using the “maint” user name.
       The password is set to “admin123” by default.
     - While configuring the static IP address for the virtual appliance for VSC, VASA Provider, and SRA, you must provide a host name that includes only the following characters: “-”, English uppercase characters (A through Z), English lowercase characters (a through z), or base digits (0 through 9).
     - You must not use any spaces in the administrator password.

     Accessing the maintenance console options of the virtual appliance for VSC, VASA Provider, and SRA on page 33
   - The 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**.

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

After you finish

You must use `https://<appliance_ip>:8143/Register.html` to register the VSC instance after deployment only if the virtual appliance for VSC, VASA Provider, and SRA is not registered with any vCenter Server.

Note: If you want to view the VASA Provider for ONTAP dashboard, then you must download and install OnCommand API Services.

VASA Provider for ONTAP overview on page 53

Enabling the VASA Provider and SRA extensions

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

   You must log out of the vSphere Web Client, 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 53
Configuring VSC, VASA Provider, and SRA for disaster recovery on page 56

Installing the NFS plug-in for VAAI

You can install the NetApp NFS 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 NFS Plug-in for VAAI (`.vib`) from the NetApp Support Site.
  mysupport.netapp.com
- You must have installed ESXi host 6.0 or later and ONTAP 9.1 or later.
- You must have powered on the ESXi host and mounted an NFS datastore.
- You must have set the value of the `DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`, and `VMFS3.HardwareAcceleratedLocking` host settings to 1.

- You must have enabled the vstorage option on the storage virtual machine (SVM) by using the `vserver nfs modify -vserver vserver_name -vstorage enabled` command.

Steps

1. Rename the `.vib` file that you downloaded from the NetApp Support Site to `NetAppNasPlugin.vib` to match the predefined name that VSC uses.
2. Click the **NFS VAAI Tools** section of the VSC home page, and then click **Select File**.
3. Browse and select the renamed `.vib` file, and then click **Upload** to upload the file to the virtual appliance.
4. Click **Install on Host** to select the ESXi host on which you want to install the NFS VAAI plug-in.

   You should follow the on-screen instructions to complete the installation. You can monitor the installation progress in the Tasks section of vSphere Web Client.
5. Reboot the ESXi host after the installation finishes.

   When you reboot the ESXi host, VSC automatically detects the NFS VAAI plug-in. You do not have to perform additional steps to enable the plug-in.

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.

You might have to perform some of the following tasks to configure your ESXi hosts, guest operating systems, and VSC:

- 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

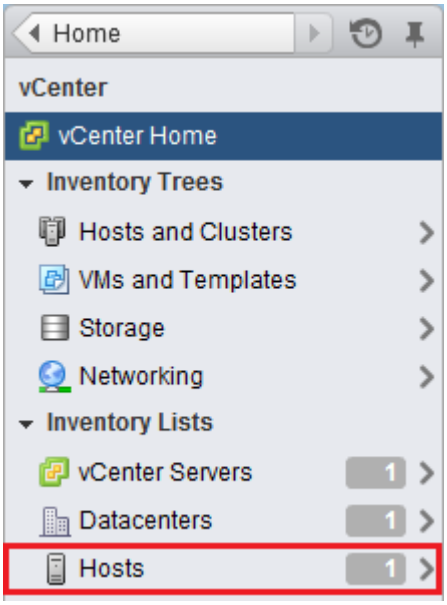
Virtual Storage Console for VMware vSphere checks and sets the ESXi host multipathing settings and HBA timeout settings that work best with NetApp storage systems.

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.

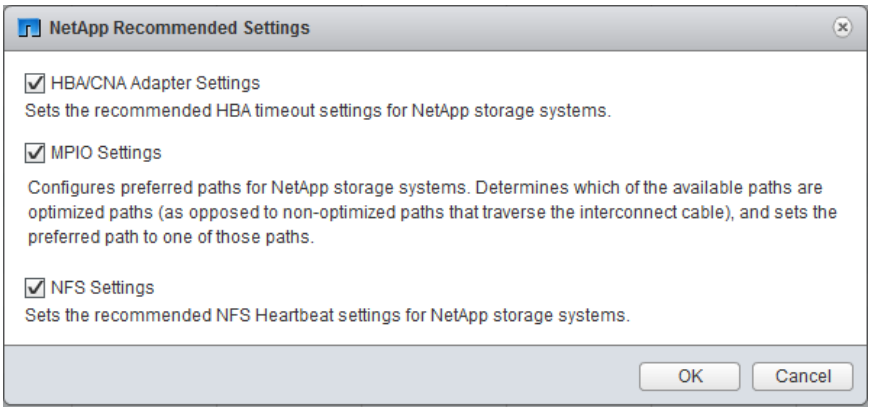
Steps

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

You should set this value to 1.

VMFS3.EnableBlockDelete

You should set this value to to 0.

2007427.

NFS settings

Net.TcpipHeapSize

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

For all other NFS configurations, you should set this value to 30.

Net.TcpipHeapMax

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

If you are using vSphere 5.5, you should set this value to 512.

If you are using vSphere 5.0 or 5.1, you should set this value to 128

If you are using vSphere 5.0 or earlier, you should set this value to 120.

NFS.MaxVolumes

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

For all other NFS configurations, you should set this value to 64.

NFS41.MaxVolumes

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

NFS.MaxQueueDepth

If you are using the vSphere 6.0 or later version of ESXi host, then you should set this value to 128 or higher to avoid queuing bottlenecks.

For vSphere versions prior to 6.0, you should set this value to 64.

NFS.HeartbeatMaxFailures

You should set this value to 10 for all NFS configurations.

NFS.HeartbeatFrequency

You should set this value to 12 for all NFS configurations.

NFS.HeartbeatTimeout

You should set this value to 5 for all NFS configurations.

FC/FCoE settings

Path selection policy

You should set this value to `RR` (round robin) when FC paths with ALUA are used.

You should set this value 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

You should set this value to 32 for all configurations. 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.

NetApp Knowledgebase Answer 1030581: How to manually configure Task Set Full (QFull) Tunables for LUNs in vSphere 5.1

Disk.QFullThreshold

Set to 8 for all configurations. 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.

NetApp Knowledgebase Answer 1030581: How to manually configure Task Set Full (QFull) Tunables for LUNs in vSphere 5.1

Emulex FC HBA timeouts

Use the default value.

QLogic FC HBA timeouts

Use the default value.

iSCSI settings

Path selection policy

You should set this value 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

You should set this value to 32 for all configurations. 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.

NetApp Knowledgebase Answer 1030581: How to manually configure Task Set Full (QFull) Tunables for LUNs in vSphere 5.1

Disk.QFullThreshold

You should set this value to 8 for all configurations. 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.

NetApp Knowledgebase Answer 1030581: How to manually configure Task Set Full (QFull) Tunables for LUNs in vSphere 5.1

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 obtain 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. See the knowledgebase article to decide which timeout value to use.

NetApp Knowledgebase Answer 1001979: What are the guest OS tunings needed for a VMware vSphere deployment?

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

To obtain the script containing the timeout values that you want for your operating system, you must copy the correct URL from the Guest OS Tools page and mount the script as a virtual CD-ROM in the virtual machine using the vSphere client. You must 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 the script from the console of the virtual machine.

See the *vSphere Virtual Machine Administration* guide for your version of vSphere for details on adding a CD-ROM to a virtual machine.

https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-C58B93A7-52CF-456D-95C1-8B5A906C9619.html

Installing guest operating system scripts

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

Before you begin

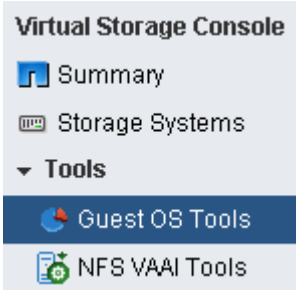
- The virtual machine must be running.
- The CD-ROM must already exist in the virtual machine.
  You must have been added a CD-ROM to the virtual machine.

About this task

You must have installed the script from the copy of the VSC instance that is registered to the vCenter Server that manages the virtual machine. 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.

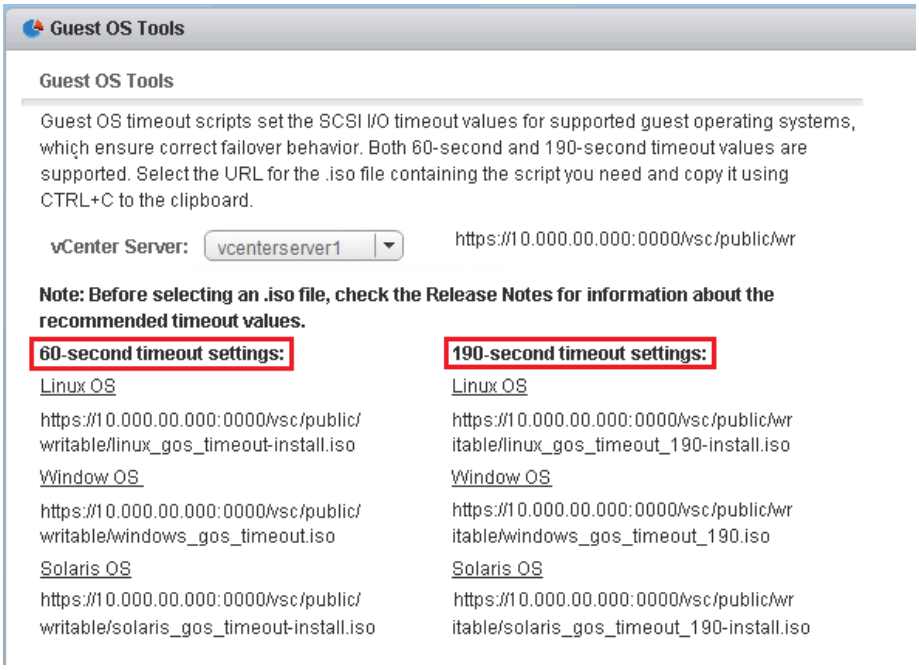
Steps

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



2. From the **Guest OS Tools** menu, press Ctrl-C to copy the link to the ISO image for your guest OS 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 that you want to use.



3. Mount the copied ISO link to the CD-ROM.

After you finish

You should log in to the virtual machine, and then run the script to set the storage timeout values.

Setting timeout values for Linux guest operating systems

The guest operating system (OS) timeout scripts set the SCSI I/O timeout settings for versions 4, 5, 6, and 7 of Red Hat Enterprise Linux and versions 9, 10, and 11 of SUSE Linux Enterprise Server. You can specify either a 60-second timeout or a 190-second timeout. You must run the script each time you upgrade to a new version of Linux.

Before you begin

You must have mounted the ISO image containing the Linux script.

Steps

1. Access 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.

   For Red Hat Enterprise Linux 4 or SUSE Linux Enterprise Server 9, 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 Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and Red Hat Enterprise Linux 7 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 SUSE Linux Enterprise Server 10 or SUSE Linux Enterprise Server 11, 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
```

3. Unmount the ISO image.

Setting timeout values for Solaris guest operating systems

The guest operating system (OS) 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 have mounted the ISO image containing the Solaris script.

Steps

1. Access 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.

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

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

3. Unmount the ISO image.

Setting timeout values for Windows guest operating systems

The guest operating system (OS) 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 have mounted the ISO image containing the Windows script.

Steps

1. Access 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 then run the `windows_gos_timeout.reg` script.

   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.
5. Unmount the ISO image.

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.

Virtual Storage Console performance in multiple vCenter Servers environment

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 must 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 6.0 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 set up or registered one VSC instance for every vCenter Server instance that you want to manage. Each registered VSC instance must be of the same version.

Linked mode is installed automatically during the vCenter Server deployment. Linked mode 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:

- Each vCenter Server in the VMware inventory that you want to manage 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 happens only 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 that is registered with a vCenter Server. You can manage the storage systems that are 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 the Virtual Storage Console for VMware vSphere preferences files. If you do not modify the preferences file, then 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 33
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 `default.allow.iscsi.mount.networks` from ALL to the value of your ESXi host networks.
NFS	Change the value of the entry key `default.allow.nfs.mount.networks` from ALL to the value of your ESXi host networks.

   The preferences file includes sample values for these entry keys.

   Note: The value “ALL” does not mean all networks. “ALL” value enables all of the matching networks, between the host and the storage system, to be used for mounting datastores. When you specify host networks, then you can enable mounting only across the specified subnets.
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, set different log levels, 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
   - Change LOG level for Virtual Storage Console service
   - Change LOG level for VASA Provider and SRA service

   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

Related concepts

Virtual Storage Console and VASA Provider log files on page 64

Configuring high availability for virtual appliance for VSC, VASA Provider, and SRA

The virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) provides a high-availability (HA) solution to help provide uninterrupted functionality of VSC, VASA Provider, and SRA.

The virtual appliance for VSC, VASA Provider, and SRA relies on the VMware vCenter Server vSphere high-availability (HA) feature and vSphere fault tolerance (FT) feature to provide high availability. The high-availability (HA) solution must be used for recovery in the following scenarios:

- Host failure
- Network failure
- Virtual machine failure (Guest OS failure)
- Application (VSC, VASA Provider, and SRA) crash

No additional configuration is required on the virtual appliance to provide high availability. Only the vCenter Server and the ESXi hosts must be configured with the VMware vSphere HA feature or the vSphere FT feature based on their requirements. You must enable vSphere FT on virtual machines that reside in a cluster that meets the specific requirements for the virtual appliance to be fault-tolerant.

Virtual machines that are deployed only on a traditional datastore can be configured for high availability. You must have datastores configured on shared ESXi hosts for high availability to work.

In addition to the VMware vSphere HA solution and vSphere FT solution, the virtual appliance also helps keep the VSC, VASA Provider, and SRA services running at all times. The virtual appliance watchdog process periodically monitors all three services, and restarts them automatically when any kind of failure is detected. This helps to prevent application failures.

VMware vSphere HA for vCenter Server

You can configure your vCenter Server where the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) is deployed for high availability (HA).The VMware vSphere HA feature provides failover protection from hardware failures and operating system failures in virtual environments.

The vSphere HA feature monitors virtual machines to detect operating system failures and hardware failures. When a failure is detected, the vSphere HA feature restarts the virtual machines on the other physical servers in the resource pool. Manual intervention is not required when a server failure is detected.

With the vSphere HA feature, you can reduce the planned downtime that is required to carry out maintenance operations, and you can prevent unplanned outages. If you have multiple ESXi hosts configured as a cluster, then you can configure vSphere HA. When one host fails, vSphere HA restarts the virtual machines on another host in the cluster. Thus, vSphere HA provides rapid recovery from outages and a cost-effective high-availability (HA) solution for applications that are running on virtual machines. You can manually enable vSphere HA for the virtual appliance by configuring an ESXi host in an HA cluster.

The procedure to configure HA depend on the version of your vCenter Server. For example, to configure HA for vCenter Server 6.0 and vCenter Server 6.5, you can use the following reference links.

- *https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html*
- *https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-E90B8A4A-BAE1-4094-8D92-8C5570FE5D8C.html*

VMware vSphere Fault Tolerance for vCenter Server

The VMware vSphere Fault Tolerance (FT) feature provides high availability (HA) at a higher level and enables you to protect virtual machines without any loss of data or connections. You must enable or disable vSphere FT for the virtual appliance for VSC, VASA Provider, and SRA from your vCenter Server.

After you enable vSphere FT, you will not notice any delays in the operations, and you do not need to plan for downtime. You can use vSphere FT in mission-critical scenarios. Your virtual appliance deployment must have a minimum of two vCPUs and a standard license to support the vSphere FT feature.

vSphere FT enables virtual machines to operate continuously even during server failures. When vSphere FT is enabled on a virtual machine, a copy of the primary virtual machine is automatically created on another host (the secondary virtual machine) that is selected by Distributed Resource Scheduler (DRS). If DRS is not enabled, the target host is selected from the available hosts. vSphere FT operates the primary virtual machine and secondary virtual machine in lockstep mode, with each mirroring the execution state of the primary virtual machine to the secondary virtual machine.

When there is a hardware failure that causes the primary virtual machine to fail, the secondary virtual machine immediately picks up where the primary virtual machine stopped. The secondary virtual machine continues to run without any loss of network connections, transactions, or data.

Your system must meet the CPU requirements, virtual machine limit requirements, and licensing requirements for configuring vSphere FT for your vCenter Server instance.

The procedure to configure HA depend on the version of your vCenter Server. For example, to configure HA for vCenter Server 6.0 and vCenter Server 6.5, you can use the following reference links.

- *https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.avail.doc/GUID-57929CF0-DA9B-407A-BF2E-E7B72708D825.html*
- *https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.avail.doc/GUID-57929CF0-DA9B-407A-BF2E-E7B72708D825.html*

MetroCluster configurations supported by the virtual appliance for VSC, VASA Provider, and SRA

The virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) supports environments that use MetroCluster configurations for ONTAP. Most of this support is automatic; however, you might notice a few differences when you use a MetroCluster environment with VSC and VASA Provider.

MetroCluster configurations and VSC

You must ensure that VSC discovers the storage system controllers at the primary site and the secondary site. Normally, VSC automatically discovers storage controllers. If you are using a cluster management LIF, it is a good practice to verify that VSC discovered the clusters at both sites. Otherwise, you can manually add the storage controllers to VSC. You can also modify the user name and password pairs that VSC uses to connect to the storage controllers.

When a switchover occurs, the SVMs on the secondary site take over. These SVMs have the “-mc” suffix appended to their names. If you are performing certain operations such as provisioning, when a switchover operation occurs, the name of the SVM where the datastore resides is changed to include the “-mc” suffix. This suffix is dropped when the switchback occurs, and the SVMs on the primary site resume control.

Note: If you have added direct SVMs with MetroCluster configuration to VSC, then after switchover, the change in the SVM name (the addition of the "-mc" suffix) is not reflected. All other switchover operations continue to execute normally.

When a switchover or switchback occurs, VSC might take a few minutes to automatically detect and discover the clusters. If this happens while you are performing a VSC operation such as provisioning a datastore, you might experience a delay.

MetroCluster configurations and VASA Provider

VASA Provider automatically supports environments that use MetroCluster configurations. The switchover is transparent in VASA Provider environments. You cannot add direct SVMs to VASA Provider.

Note: VASA Provider does not append the “-mc” suffix to the names of the SVMs on the secondary site after a switchover.

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 the **Update All** option, 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.

Note:

- You must not add storage systems that have infinite volumes to VSC because VSC does not support storage systems that have infinite volumes.
- Storage Replication Adapter (SRA) does not support fan-out SnapMirror configuration.

Steps

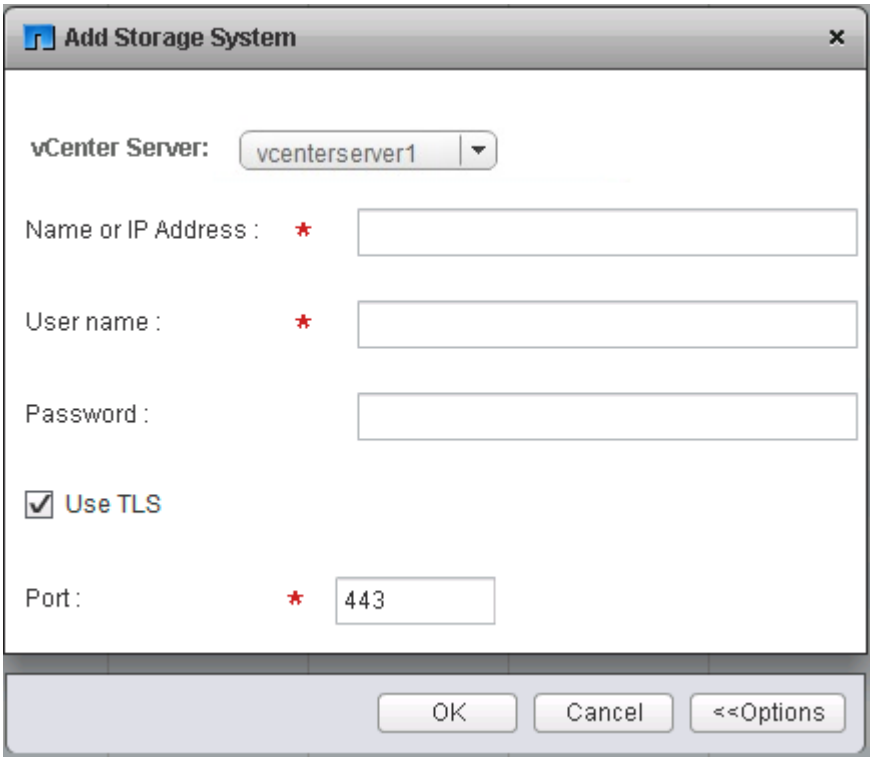
1. Add a storage system to VSC by using either the **Add** icon or the **Add Storage System** menu option:

Starting location	Action
Virtual Storage Console Home page	**a.** Click **Storage System**. **b.** Click the **Add** icon.
VMware vSphere Web Client Home page	**a.** Click the **Storage** icon. **b.** Select a datacenter. **c.** Select **Actions > NetApp VSC > Add Storage System**.

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.



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.

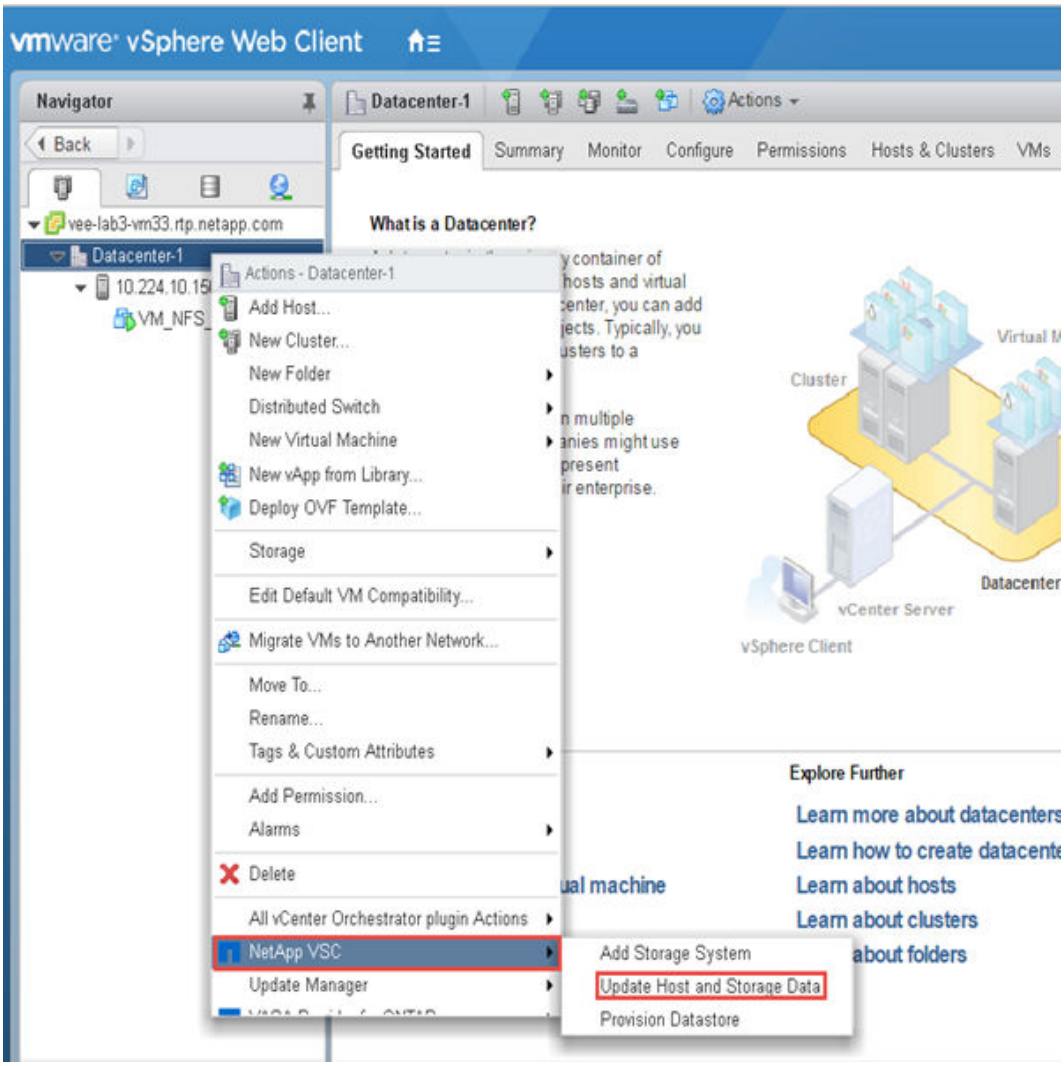
About this task

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 **Update All** icon.
Datacenter	**Actions > NetApp VSC > Update Host and Storage Data**

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

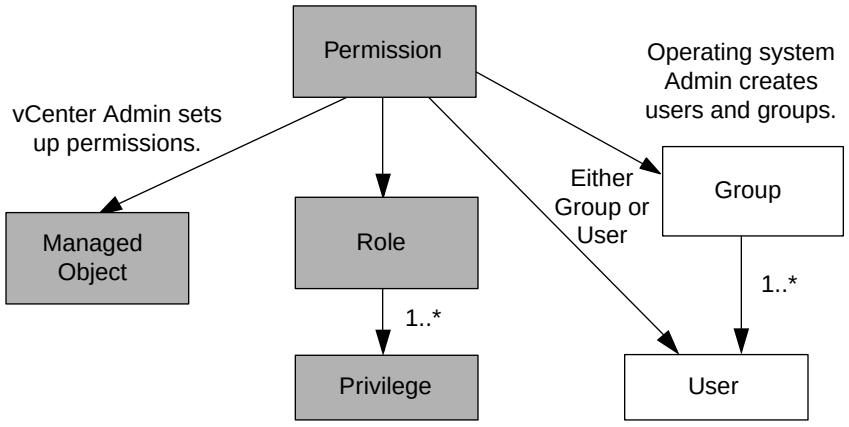
The vCenter Server recognizes permissions, not privileges. Each vCenter Server permission consists of three components.

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

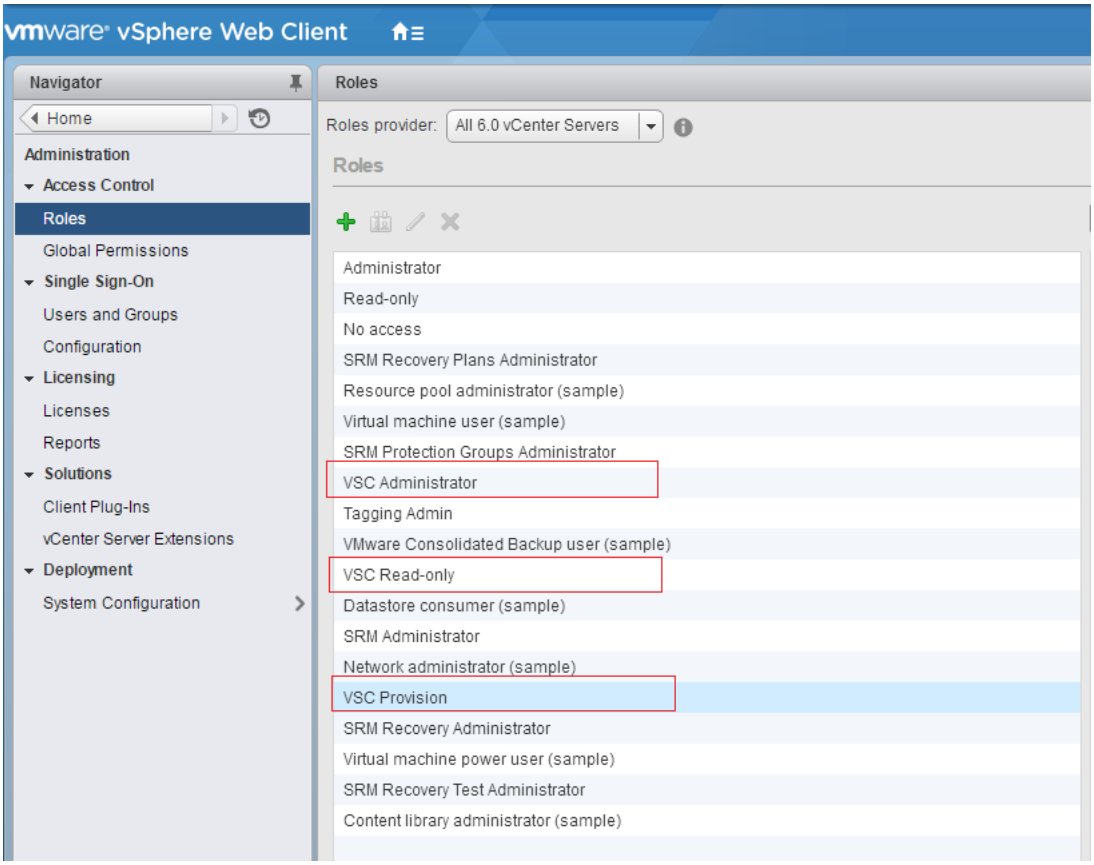
To simplify working with vCenter Server privileges and role-based access control (RBAC), Virtual Storage Console (VSC) provides standard VSC roles that enable you to perform key VSC tasks. There is also a read-only role that enables you to view VSC information, but not perform any tasks.

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: • Create new datastores • Destroy datastores • View information about storage capability profiles

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 privileges specific to Virtual Storage Console (VSC) and native vCenter Server privileges.

Information about the privileges required for VSC tasks is available in the NetApp Knowledgebase article 1032542.

NetApp Knowledgebase Answer 1032542: How to configure RBAC for Virtual Storage Console

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	You can access the VSC GUI. 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.	The assignment level determines which portions of the UI you can see. Assigning the View privilege at the root object (folder) enables you to enter VSC by clicking the NetApp icon. You can assign the View privilege to another vSphere object level; however, doing that limits the VSC menus that you can see and use. The root object is the recommended place to assign any permission containing the View privilege.

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 (VSC). You can create one or more custom user accounts with limited access privileges with the ONTAP RBAC feature.

VSC and SRA can access storage systems at either the cluster level or the SVM level. If you are adding storage systems at the cluster level, then you must provide the credentials of the admin user to provide all of the required capabilities. If you are adding storage systems by directly adding SVM details, you must be aware that the “vsadmin” user does not have all of the required roles and capabilities to perform certain tasks.

VASA Provider can access storage systems only at the cluster level. If VASA Provider is required for a particular storage controller, then the storage system must be added to VSC at the cluster level even if you are using VSC or SRA.

To create a new user and to connect a cluster or SVM to VSC, VASA, and SRA, you should perform the following:

- Create a cluster administrator or SVM administrator role using ONTAP

  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 users with the role assigned and the appropriate application set using ONTAP
  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 with these credentials, you will have permissions to the VSC functions that you had set up in ONTAP while creating the credentials.
- Add the storage system to VSC and provide the credentials of the user that you just created

VSC roles

VSC classifies the ONTAP privileges into the following set of VSC roles :

- Discovery
  Enables the discovery of all of the connected storage controllers.
- Create Storage
  Enables the creation of volumes and logical unit number (LUNs).
- Modify Storage
  Enables the resizing and deduplication of storage systems.
- Destroy Storage
  Enables the destruction of volumes and LUNs.

VASA Provider roles

You can create only Policy Based Management at the cluster level. This role enables policy-based management of storage using storage capabilities profiles.

SRA roles

SRA classifies the ONTAP privileges into a SAN or NAS role at either the cluster level or the SVM level. This enables users to run SRM operations.

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/ka21A0000008rl9QAA/VSC-VASA-and-SRA-7-0-ONTAP-RBAC-Configuration*
- *NetApp Knowledgebase Answer 1001056: FAQ: Roll up of all commands for VSC and SRA for SVM level*

VSC performs an initial privilege validation of ONTAP RBAC roles when you add the cluster to VSC. If you have added a direct SVM storage IP, then VSC does not perform the initial validation. 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 the VASA Provider and SRA extensions 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 use VASA Provider to manage features such as storage capability profiles, alarms, and virtual volumes (VVols). You can use the VASA Provider dashboard to monitor performance of your VVol and virtual machines.

You must have enabled 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:

- Enables you to set up storage capability profiles that the vCenter Server can use.
  These profiles work with storage on both standard datastores and VVol datastores.
- Manages multiple storage systems running ONTAP.
- Checks for compliance between the datastores and the storage capability profiles.
- Enables 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. If you want to view the VASA Provider dashboard, then you must have installed and registered OnCommand API Services with your vCenter Server.

Note: VASA Provider requires a dedicated instance of OnCommand API Services. One instance of OnCommand API Services cannot be shared with multiple VASA Provider instances.

You must follow the installation instructions that are provided in the *OnCommand API Services Installation and Setup guide* after downloading and installing OnCommand API Services from the NetApp Support Site. You must not configure OnCommand API Services after installation, as the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) handles the configuration of OnCommand API Services.

https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62040

VASA Provider and the VSC GUI

VASA Provider is integrated with VSC. You must use the VASA Provider section in the VSC GUI to perform the following VASA Provider tasks:

- Setting alarm thresholds
- Creating storage capability profiles, both by manually setting them up and by using the auto-generate feature of VASA Provider
- 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*. The Vendor Provider Control Panel creates a more complete bundle than the bundle that the maintenance menu creates.

VASA Provider dashboard for monitoring VVol datastores and virtual machines

You can view the performance of VVol datastores and virtual machines configured using VASA Provider dashboard on a single page. The VASA Provider dashboard provides an overview of the VVol datastores and performance metrics such as IOPS, latency, space savings, and so on.

Registering OnCommand API Services with the virtual appliance for VSC, VASA Provider, and SRA

The dashboard of VASA Provider for ONTAP can display the details of virtual volume (VVol) datastores and virtual machines only if you have registered OnCommand API Services for VASA Provider.

Before you begin

You must have downloaded OnCommand API Services 2.1 or later from the NetApp Support Site.

Note: The VASA Provider for ONTAP dashboard displays performance metrics only when the VVol datastores and virtual machines are configured by using ONTAP 9.3 or later.

Steps

1. From the Virtual Storage Console (VSC) **Home** page, click **VASA Provider for ONTAP** to navigate to the VASA Provider section.

   A message with the status of the OnCommand API Services registration process for VASA Provider is displayed.

2. Enable OnCommand API Services by using one of the following methods:
   - Use the Configuration tab:
     a. Click **Configuration**.
     b. Select the vCenter Server for which you want to register OnCommand API Services.
     c. Click Manage VASA Provider Extensions.
   - Click the link in the warning message.
3. Register OnCommand API Services by using the **Manage VASA Provider Extensions** dialog box:
   a. Select the **Register OnCommand API Services** checkbox.
   b. Enter the IP address, service port, and credentials for OnCommand API Services.

      You can also use the Manage VASA Provider Extensions dialog box for the following modifications:
      - To update OnCommand API Services registration when there is any change to the credentials.
      - To unregister OnCommand API Services when you no longer require the VASA Provider dashboard.
        You must clear the Register OnCommand API Services checkbox to remove the OnCommand API Services registration for VASA Provider.

   c. Click **Apply**.

   The VASA Provider dashboard displays the metrics only after the registration of OnCommand API Services is complete.

Related information

NetApp Support

Configuring VSC, VASA Provider, and SRA for disaster recovery

If you want to configure your vCenter Server for disaster recovery, you must enable Storage Replication Adapter (SRA) after you deploy the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA). The deployment of the virtual appliance installs VSC by default. You must enable SRA for your vCenter Server after the deployment of the virtual appliance.

Related tasks

Enabling the VASA Provider and SRA extensions 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 `fcp 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

Configuring SRA for highly scaled environments

You must configure the storage timeout intervals per the recommended settings for Storage Replication Adapter (SRA) to perform optimally in highly scaled environments.

Storage Provider settings

- You must increase the value of the `StorageProvider.resignatureTimeout` setting from 900 seconds to 12000 seconds.
- You must enable the `StorageProvider.autoResignatureMode` option.

See VMware documentation for more information on modifying Storage Provider settings.

https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-E4060824-E3C2-4869-BC39-76E88E2FF9A0.html

Storage settings

You must set the value of the `storage.commandTimeout` timeout interval for highly scaled environments to 12,000 seconds.

Note: The timeout interval specified is the maximum value. You do not need to wait for the maximum timeout to be reached. Most commands finish within the set maximum timeout interval.

NetApp Knowledgebase Answer 1001111: NetApp Storage Replication Adapter 4.0/7.X for ONTAP Sizing Guide

See VMware documentation for more information on modifying SAN Provider settings.

https://docs.vmware.com/en/Site-Recovery-Manager/6.5/com.vmware.srm.admin.doc/GUID-711FD223-50DB-414C-A2A7-3BEB8FAFDBD9.html

Considerations for upgrading the virtual appliance for VSC, VASA Provider, and SRA

If you have an existing deployment of Virtual Storage Console (VSC), VASA Provider, or Storage Replication Adapter (SRA) in your vCenter Server environment, then you can upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA. The upgrade process depends on your deployment model and the software version of your products.

You can have any one of the following combinations of products in your deployment:

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

If you have VSC 6.2.x or VASA Provider 6.2.x in any of the deployment models, then to upgrade to the latest version of the virtual appliance for VSC, VASA Provider, and SRA, you must migrate your data and configuration files manually. If you have SRA 4.0 in any of the deployment models, then you must perform an in-place upgrade to the 7.0 version of the virtual appliance, and then upgrade to the 7.2 version of the virtual appliance.

The following operations for upgrading or migrating to the latest version of the virtual appliance for VSC, VASA Provider, and SRA are supported:

- In-place upgrade from SRA 4.0 to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA
- Migrating from VSC 6.2.x to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, and then performing an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA
- Migrating from VASA Provider 6.2.x to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA, and then performing an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA

You can perform an in-place upgrade from the 7.x version of the virtual appliance to the latest version of the virtual appliance for VSC, VASA Provider, and SRA after upgrading from your existing deployment to the 7.x version of the virtual appliance.

If your existing deployment has…	Do this…
Version 7.0 or 7.1 of the virtual appliance for VSC, VASA Provider, and SRA	Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.

If your existing deployment has…	Do this…
Virtual Storage Console 6.2.x	• Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing metadata to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.
VASA Provider 6.2.x	• Unregister VASA Provider. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing metadata to the 7.0 version of the virtual appliance. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.
SRA 2.1 or 3.0	• Unregister SRA. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing data and configurations to the 7.0 version of the virtual appliance • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA
SRA 4.0	• Perform an in-place upgrade to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.

If your existing deployment has…	Do this…
Virtual Storage Console 6.2.x and VASA Provider 6.x	• Unregister VASA Provider. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing metadata to the 7.0 version of the virtual appliance. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.
Virtual Storage Console 6.2.x and SRA 2.1 or 3.0	• Unregister SRA. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your metadata to the 7.0 version of the virtual appliance. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.
Virtual Storage Console 6.2.x, VASA Provider 6.x, and SRA 2.1 or 3.0	• Unregister VASA Provider and SRA. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing metadata to the 7.0 version of the virtual appliance. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.

If your existing deployment has…	Do this…
Virtual Storage Console 6.2.x, VASA Provider 6.x, and SRA 4.0	• Unregister VASA Provider. • Deploy the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Add storage systems to the 7.0 version of the virtual appliance for VSC, VASA Provider, and SRA. • Migrate your existing metadata to the 7.0 version of the virtual appliance. • Perform an in-place upgrade to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.

Related information

Installing and setting up SnapCenter
NetApp ToolChest: NetApp Import Utility for SnapCenter and Virtual Storage Console

Upgrading to the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA

You can perform an in-place upgrade from the 7.x version of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to the 7.2 version of the virtual appliance. If you have an existing deployment earlier than the 7.x version of the virtual appliance for VSC, VASA Provider, and SRA, then you must first upgrade or migrate to the 7.x version of the virtual appliance.

Before you begin

- You must have downloaded the `iso` file for the 7.2 version of the virtual appliance for VSC, VASA Provider, and SRA.
- You must have reserved 8 GB of RAM for the virtual appliance for VSC, VASA Provider, and SRA to work optimally after the upgrade.

Steps

1. Mount the downloaded `.iso` file to the virtual appliance:
   a. Click **Edit Settings** > **DVD/CD-ROM Drive**.
   b. Select **Datastore ISO** file from the drop-down list.
   c. Browse and select the downloaded `.iso` file, and then select the **Connect at power on** checkbox.
2. Access the **Summary** tab of your deployed virtual appliance.
3. Click to start the maintenance console.

4. At the Main Menu prompt, enter option **2** for **System Configuration**, and then enter option **8** for **Upgrade**.

   After the upgrade finishes, the virtual appliance restarts.

Troubleshooting issues with the virtual appliance for VSC, VASA Provider, and SRA

If you encounter unexpected behavior during the installation or configuration of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA), then 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.

Uninstall does not remove standard VSC roles

When you uninstall Virtual Storage Console for VMware vSphere (VSC), 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 operation does not remove the VSC roles, the uninstall operation 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.

Virtual Storage Console and VASA Provider log files

You can check the log files in the `/opt/netapp/vscserver/logs` directory and the `/opt/netapp/vpserver/logs` directory when you encounter errors.

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

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

The maintenance menu of the virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) enables you to set different log levels for your requirement. The following log levels are available:

- Info
- Debug
- Error
- Trace

When you set the log levels, the following files are updated:

- VSC server: `kamino.log` and `vvolvp.log`
- VASA Provider server: `vvolvp.log`, `error.log`, and `netapp.log`

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`.

Out of memory exception for virtual appliance for VSC, VASA Provider, and SRA

You might receive an out of memory exception while accessing the vSphere Web Client or the vSphere Web Client may be slow.

Description

This issue occurs due to the sudden increase in the periodic heap consumption of vSphere Web Client. The vCenter Server services may run out of memory when the heap increases beyond a specific limit.

Workaround

You may perform one of the following:

- You must wait for some time for the heap to be cleared.
- You must restart your vCenter Server by using the `start` and `stop` commands.

See the procedure for stopping and starting vCenter Server services in the “Resolving VASA Provider registration issues” topic.

Resolving VASA Provider registration issues on page 66

VASA Provider extension unavailable when vSphere Web Client service is restarted

If the VASA Provider extension is enabled for your vCenter Server and the vSphere Web Client service restarts, then VASA Provider for ONTAP menu is unavailable in the navigation pane of

Virtual Storage Console. However, the status of VASA Provider registration for your vCenter Server remains unchanged.

Description

You can verify that the VASA Provider extension is available by using the command line interface (CLI) and performing VASA Provider actions. However, you cannot access VASA Provider in your vCenter Server and you cannot access the VASA Provider services.

Workaround

You must unregister both VSC and the VASA Provider extension, delete the plug-in folders located at `/etc/vmware/vsphere-client/vc-packages` from your vCenter Server, and then restart and register VSC and VASA Provider.

Resolving VASA Provider registration issues on page 66

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 Clientservice:
   - 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.nvpf.webclient* com.netapp.vasa*`

   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.

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.

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 the virtual appliance for VSC, VASA Provider, and SRA to use SSH for remote diag access

You can configure virtual appliance for Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) to enable SSH access for the diag user.

Before you begin

The VASA Provider extension must be enabled for your vCenter Server instance.

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 session 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** in the **Confirmation** dialog box to enable remote diagnostic access.
6. Enter a password for remote diagnostic access.

SRA fails to perform optimally in a highly scaled environment

Issue

SRA fails to perform optimally in a highly scaled environment, and you notice issues such as a timeout error or a ONTAP timeout.

Corrective action

You must modify the timeout intervals.

Configuring SRA for highly scaled environments on page 57

Unable to install the SRA plug-in

Issue

During the installation of the Storage Replication Adapter (SRA) plug-in, the system stops at the server IP address and password screen with the following error message: “The credentials you entered are not valid. Please enter a valid hostname and password.”

Cause

The error might occur due to one of the following reasons:

- You entered incorrect administrator credentials.
- The WinHTTP proxy settings are incorrect.

Corrective action

- Verify your administrator credentials.
- See the NetApp knowledgebase article for resolving issues with WinHTTP proxy settings. *https://kb.netapp.com/app/answers/answer_view/a_id/1005074*

Copyright information

Trademark information

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

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

S

T

U

V

W