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

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

Table of Contents

Requirements for deploying 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.

Port requirements for VSC

By default, (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 should manually grant access to specific ports that VSC uses. If you do not grant access to these ports, an error message such as the following is displayed.

Unable to communicate with the server

VSC uses the following default bidirectional TCP 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. This port is also required for obtaining the TCP/IP settings.
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.
7	VSC sends an echo request to ONTAP to verify reachability and is required only when adding storage system and can be disabled later.

You should have enabled Internet Control Message Protocol (ICMP) before deploying the virtual appliance for VSC, VASA Provider, and SRA.

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.

Space and size requirements for 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**
  - ESXi 6.5U2 or later
  - Recommended memory: 12 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 (IMT) contains the latest information about the supported versions of ONTAP, vCenter Server, ESXi hosts, plug-in applications, and Site Recovery Manager (SRM).

- Interoperability Matrix Tool: VSC 9.7.1
- Interoperability Matrix Tool: VASA Provider 9.7.1
- Interoperability Matrix Tool: SRA 9.7.1

You must enable the FlexClone license for performing virtual machine snapshot operations and clone operations for VMware Virtual Volumes (vVols) 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.

To view the IOPS for a datastore, you must either enable Storage I/O control or uncheck the disable Storage I/O statistics collection checkbox in the Storage I/O control configuration. You can enable the Storage I/O control only if you have the Enterprise Plus license from VMware.

- VMware KB article 1022091: Troubleshooting Storage I/O Control

- VMware vSphere Documentation: Storage I/O Control Requirements

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 good practice to plan your deployment and decide how you want to configure VSC, VASA Provider, and SRA in your environment.

The following table presents an 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. Deploying or upgrading VSC, VASA Provider, and SRA Deployment workflow for new users of VSC, VASA Provider, and SRA virtual appliance
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 VSC, VASA Provider, and SRA. The deployment workflows and upgrade section has more information. Deployment workflow for existing users of VSC, VASA Provider, and SRA 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.

Considerations	Description
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. Regenerate an SSL certificate for
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. • Configure ESXi server multipathing and timeout settings • ESXi host values set using Virtual Storage Console for VMware vSphere
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.

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

Considerations	Description
Requirements of role-based access control (RBAC)	VSC supports both vCenter Server RBAC and ONTAP RBAC. The account used to register VSC to vCenter Server (using *https*://<appliance_ip>:8143/Register.html) must be a vCenter Server administrator (assigned to the vCenter Server administrator or administrator role). 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 create and assign standard VSC roles to users to meet the vCenter Server requirements. You can create the recommended ONTAP roles by using ONTAP System Manager using the JSON file provided with the virtual appliance for VSC, VASA Provider, and SRA. 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 • Recommended ONTAP roles when using VSC for VMware vSphere
ONTAP version	Your storage systems must be running ONTAP 9.1, 9.3, 9.5, 9.6, or 9.7.
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 VMware Virtual Volumes (vVols) 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.

Copyright information

Trademark information