



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

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/us-en/vsc-vasa-provider-sra-97/deploy/reference-port-requirements-for-vsc.html> on March 21, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA. 1
 - Port requirements for VSC 1
 - Space and size requirements for the virtual appliance for VSC, VASA Provider, and SRA. 2
 - Supported storage system, licensing, and applications for the virtual appliance for VSC, VASA Provider, and SRA. 2
 - Considerations and requirements for deploying the virtual appliance for VSC, VASA Provider, and SRA . . . 3

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](#)

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	<p>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</p> <p>Deployment workflow for new users of VSC, VASA Provider, and SRA virtual appliance</p>
Upgrading from an existing deployment of VSC	<p>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</p> <p>Best practices before an upgrade:</p> <ul style="list-style-type: none"> • You should record information about the storage systems that are being used and their credentials. <p>After the upgrade, you should verify that all of the storage systems were automatically discovered and that they have the correct credentials.</p> <ul style="list-style-type: none"> • If you modified any of the standard VSC roles, you should copy those roles to save your changes. <p>VSC overwrites the standard roles with the current defaults each time you restart the VSC service.</p>

Considerations	Description
Regenerating an SSL certificate for VSC	<p>The SSL certificate is automatically generated when you deploy the virtual appliance for VSC, VASA Provider, and SRA. You might have to regenerate the SSL certificate to create a site-specific certificate.</p> <p>Regenerate an SSL certificate for</p>
Setting ESXi server values	<p>Although most of your ESXi server values are set by default, it is a good practice to check the values. These values are based on internal testing. Depending on your environment, you might have to change some of the values to improve performance.</p> <ul style="list-style-type: none"> • Configure ESXi server multipathing and timeout settings • ESXi host values set using Virtual Storage Console for VMware vSphere
Guest operating system timeout values	<p>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.</p>

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)	<p>VSC supports both vCenter Server RBAC and ONTAP RBAC. The account used to register VSC to vCenter Server (using <code>https://<appliance_ip>:8143/Register.html</code>) 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.</p> <p>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.</p> <p>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.</p> <p>If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out.</p> <ul style="list-style-type: none"> • 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	<p>To use storage capability profiles or to set up alarms, you must enable VASA Provider for ONTAP. After you enable VASA Provider, you can configure VMware Virtual Volumes (vVols) datastores, and you can create and manage storage capability profiles and alarms.</p> <p>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.</p>

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.