Requirements for deploying the ONTAP tools

ONTAP tools for VMware vSphere 9.13

NetApp
December 17, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-tools-vmware-vsphere/deploy/reference_port_requirements_for_vsc.html on December 17, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Requirements for deploying the ONTAP tools . . . 1
Port requirements for ONTAP tools . . . 1
Space and sizing requirements for the ONTAP tools . . . 2
Supported storage system, licensing, and applications for the ONTAP tools . . . 2
Considerations for deploying ONTAP tools . . . 3
Additional deployment considerations . . . 5

Requirements for deploying the ONTAP tools

Port requirements for ONTAP tools

By default, ONTAP tools 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 ONTAP tools 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.
```

ONTAP tools 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. This port needs to be enabled on the firewall from ESXi hosts to the ONTAP tools for VMware vSphere appliance. This port is used to download VP support bundle, access Web-CLI user interface, and control path communication from VMware to VP.
443	Depending on how you have configured your credentials, the VMware vCenter Server and the storage systems listen for secure communications on this port. The port is used in client-server communication architecture. The 443 port is enabled by default for secure connections. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data.
8143	ONTAP tools listens for secure communications on this port. The port is used in client-server communication architecture. The client, which can be any automation client that uses REST API, initiates the connection to the server and the end points exchange data. This port is enabled for ONTAP tools services and for exporting ONTAP tools server logs. The register.html page is hosted on this port. The REST swagger is exposed on this port.
8443	This port is used for ONTAP tools for VMware vSphere plugin service.

7	ONTAP tools 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 ONTAP tools.

If ICMP is disabled, then the initial configuration of ONTAP tools fails, and ONTAP tools cannot start the ONTAP tools for VMware vSphere and VASA Provider services after deployment. You must manually enable the ONTAP tools for VMware vSphere and VASA Provider services after deployment.

Space and sizing requirements for the ONTAP tools

Before deploying the ONTAP tools for VMware vSphere, 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 6.5U3 or later
  - Recommended memory: 12 GB RAM
  - Recommended CPUs: 2

Supported storage system, licensing, and applications for the ONTAP tools

You should be aware of the basic storage system requirements, application requirements, and license requirements before you begin deploying the ONTAP tools for VMware vSphere.

The Interoperability Matrix Tool (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

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.

- Troubleshooting Storage I/O Control
- vSphere Resource Management

Considerations for deploying ONTAP tools

Before you deploy ONTAP tools for VMware vSphere, it is good practice to plan your deployment and decide how you want to configure ONTAP tools in your environment.

The following table presents an overview of what you should consider before you deploy ONTAP tools.

Considerations	Description
First-time deployment of ONTAP tools	The deployment of the ONTAP tools for VMware vSphere automatically installs the ONTAP tools features. Deployment workflow for new users of ONTAP tools for VMware vSphere
Upgrading from an existing deployment of ONTAP tools	The upgrade procedure from an existing deployment of ONTAP tools to ONTAP tools depends on the version of ONTAP tools, and whether you have deployed ONTAP tools. The deployment workflows and upgrade section has more information. Deployment workflow for existing users of ONTAP tools 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 ONTAP tools roles, you should copy those roles to save your changes. ONTAP tools overwrites the standard roles with the current defaults each time you restart the ONTAP tools service.

Regenerating an SSL certificate for ONTAP tools	The SSL certificate is automatically generated when you deploy the ONTAP tools. You might have to regenerate the SSL certificate to create a site-specific certificate. Regenerate an SSL certificate for Virtual Storage Console
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 ONTAP® tools 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 ONTAP tools.

Considerations	**Description**

Requirements of role-based access control (RBAC)	ONTAP tools supports both vCenter Server RBAC and ONTAP RBAC. The account used to register ONTAP tools to vCenter Server (`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 ONTAP tools for VMware vSphere 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 ONTAP tools 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 ONTAP tools. If a user attempts to perform a task without the correct privileges and permissions, the task options are grayed out. • Standard roles packaged with ONTAP tools • Permissions for ONTAP storage systems and vSphere objects
ONTAP version	Your storage systems must be running ONTAP 9.7, 9.8P1 or later.
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.

Additional deployment considerations

You must consider few requirements while customizing the deployment ONTAP tools.

Application user password

This is the password assigned to the administrator account. For security reasons, it is recommended that the password length is eight to thirty characters long and contains a minimum of one upper, one lower, one digit, and one special character. Password expires after 90 days.

Appliance maintenance console credentials

You must access the maintenance console by using the “maint” user name. You can set the password for the “maint” user during deployment. You can use the Application Configuration menu of the maintenance console of your ONTAP tools to change the password.

vCenter Server administrator credentials

You can set the administrator credentials for the vCenter Server while deploying ONTAP tools.

If the password for the vCenter Server changes, then you can update the password for the administrator by using the following URL: `https://<IP>:8143/Register.html` where the IP address is of ONTAP tools that you provide during deployment.

Derby database password

For security reasons, it is recommended that the password length is eight to thirty characters long and contains a minimum of one upper, one lower, one digit, and one special character. Password expires after 90 days.

vCenter Server IP address

- You should provide the IP address (IPv4 or IPv6) of the vCenter Server instance to which you want to register ONTAP tools.

  The type of ONTAP tools for VMware vSphere and VASA certificates generated depends on the IP address (IPv4 or IPv6) that you have provided during deployment. While deploying ONTAP tools, if you have not entered any static IP details and your DHCP then the network provides both IPv4 and IPv6 addresses.

- The ONTAP tools IP address used to register with vCenter Server depends on the type of vCenter Server IP address (IPv4 or IPv6) entered in the deployment wizard.

  Both the ONTAP tools for VMware vSphere and VASA certificates will be generated using the same type of IP address used during vCenter Server registration.

  IPv6 is supported only with vCenter Server 6.7 and later.

Appliance network properties

If you are not using DHCP, specify a valid DNS hostname (unqualified) as well as the static IP address for the ONTAP tools for VMware vSphere and the other network parameters. All of these parameters are required for proper installation and operation.

Copyright information

Copyright © 2025 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.