



Access ONTAP tools for VMware vSphere maintenance console

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Table of Contents

- Access ONTAP tools for VMware vSphere maintenance console 1
 - Learn about the ONTAP tools maintenance console 1
 - Configure remote diagnostic access for ONTAP tools 2
 - Start SSH on other ONTAP tools nodes. 2
 - Update vCenter Server credentials in ONTAP tools 3
 - Change certificate validation flag in ONTAP tools 3
 - Verify SAN-based certificates for storage backends 4

Access ONTAP tools for VMware vSphere maintenance console

Learn about the ONTAP tools maintenance console

The maintenance console for ONTAP tools for VMware vSphere enables you to manage application, system, and network settings. You can update administrator and maintenance passwords, generate support bundles, configure log levels, manage TLS settings, and enable remote diagnostics.

After deploying ONTAP tools for VMware vSphere, if the maintenance console is not accessible, install the VMware tools from the vCenter Server. Log in using the `maint` username and the password set during deployment. Use `nano` to edit files in the maintenance or root login console.



You should set a password for the `diag` user while enabling remote diagnostics.

You should use the **Summary** tab of your deployed ONTAP tools for VMware vSphere to access the maintenance console. When you select , the maintenance console starts.

Console Menu	Options
Application Configuration	1. Display server status summary 2. Change LOG level for ONTAP tools services 3. Change cert validation flag
System Configuration	1. Reboot virtual machine 2. Shutdown virtual machine 3. Change 'maint' user password 4. Change time zone 5. Increase jail disk size (/jail) 6. Upgrade 7. Install VMware Tools
Network Configuration	1. Display IP address settings 2. Display domain name search settings 3. Change domain name search settings 4. Display static routes 5. Change static routes 6. Commit changes 7. Ping a host 8. Restore default settings

Support and Diagnostics	1. Access diagnostic shell 2. Enable remote diagnostic access 3. Provide vCenter credentials for backup 4. Take backup
-------------------------	---

Configure remote diagnostic access for ONTAP tools

You can configure ONTAP tools for VMware vSphere to enable SSH access for the diag user.

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

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

- you're allowed only one login account per activation of SSH.
- SSH access to the diag user account is disabled when one of the following happens:
 - The time expires.

The login session expires at 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 maintenance user.
3. Enter 4 to select **Support and Diagnostics**.
4. Enter 2 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.

Start SSH on other ONTAP tools nodes

You need to start SSH on other nodes before you upgrade.

Before you begin

Enable the VASA Provider extension for your vCenter Server instance.

About this task

Repeat this procedure on each node before upgrading.

Steps

1. From the vCenter Server, open a console to VASA Provider.

2. Log in as the maintenance user.
3. Enter 4 to select Support and Diagnostics.
4. Enter 1 to select Access diagnostic shell.
5. Enter *y* to proceed.
6. Run the command *sudo systemctl restart ssh*.

Update vCenter Server credentials in ONTAP tools

You can update the vCenter Server instance credentials using the maintenance console.

Before you begin

You need to have maintenance user login credentials.

About this task

If you changed vCenter Server credentials after deployment, update them using this procedure.

Steps

1. From the vCenter Server, open a console to VASA Provider.
2. Log in as the maintenance user.
3. Enter 2 to select System Configuration Menu.
4. Enter 8 to change vCenter credentials.

Change certificate validation flag in ONTAP tools

By default, the certificate validation flag is enabled (set to true). You can set the ONTAP storage backend certificate validation flag to false if you need to bypass SAN certificate checks. This setting is not applicable to vCenter Server certificates.

Before you begin

You need to have maintenance user login credentials.

Steps

1. From the vCenter Server, open a console to ONTAP tools.
2. Log in as the maintenance user.
3. Enter 1 to select **Application Configuration** menu.
4. Enter 3 to change cert validation flag.

The maintenance console shows the certificate validation flag status and prompts you to change it.

5. Enter 'y' to toggle the flag or 'n' to cancel.

When you enable the certificate validation flag (set to true), ONTAP tools checks that all storage backends use certificates with a Subject Alternative Name (SAN). If any backend uses a certificate without a SAN, you cannot enable certificate validation. Before enabling this flag, verify that all storage backends use SAN-based certificates. If you disable the certificate validation flag (set to false), ONTAP tools bypasses certificate validation for all configured storage backends.

Verify SAN-based certificates for storage backends

To ensure secure communication and proper validation, verify that all storage backends use SAN-based certificates:

1. Check that the ONTAP management certificate includes a Subject Alternative Name (SAN) entry.
2. Confirm that the SAN entries match the ONTAP management IP address or DNS name, or both.
3. Ensure the details used to onboard ONTAP match the IP address or DNS name in the SAN entry of the certificate.

Following these steps helps prevent certificate validation issues and ensures that the ONTAP system is securely integrated.

The following sample certificate shows the decoded information:

```
HG8u6GK r2JJonWe/kjoKTUnkjwt7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMAvdecTeU1X/1X3qMxiL+tU4p9SbKVpQw6hjM/zi0LNC784EYI0S7qVob
6f21mfP0JHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgI9z
dGkyMjAtdnNpbS1zcjA1MWUtY20uY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kbxQZbfryy68itKGF4LeAid0hgyxc3y9iv4zK1x85fLNgITnVqAe8'KYNoyD6
IEwppDUE0eVNIZIQjrz9QjUAAF9ifjq8+SKrLphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwqx9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMs0MSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

Copyright information

Copyright © 2026 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.