



Security hardening guide for ONTAP tools for VMware vSphere

Enterprise applications

NetApp
May 09, 2024

Table of Contents

- Security hardening guide for ONTAP tools for VMware vSphere 1
 - Security hardening guide for ONTAP tools for VMware vSphere 1
 - Verifying the integrity of the ONTAP tools for VMware vSphere installation packages 1
- Ports and Protocols 3
- ONTAP tools for VMware vSphere access points (Users) 4
- Mutual TLS (Certificate-Based Authentication) 5
- ONTAP tools HTTPS Certificate 9
- Login Banner 9
- Inactivity Timeout 10
- Maximum concurrent requests per user (Network security protection :: DOS attack) 10
- Network Time Protocol (NTP) Configuration 11
- Password Policies 11

Security hardening guide for ONTAP tools for VMware vSphere

Security hardening guide for ONTAP tools for VMware vSphere

The security hardening guide for ONTAP tools for VMware vSphere provides a comprehensive set of instructions for configuring the most secure settings.

These guides apply to both the applications and the guest OS of the appliance itself.

Verifying the integrity of the ONTAP tools for VMware vSphere installation packages

There are two methods available for customers to verify the integrity of their ONTAP tools installation packages.

1. Verifying the checksums
2. Verifying the signature

Checksums are provided on the download pages of OTV install packages. Users must verify the checksums of downloaded packages against the checksum provided on the download page.

Verifying the signature of the ONTAP tools OVA

The vApp install package is delivered in the form of a tarball. This tarball contains intermediate and root certificates for the virtual appliance along with a README file and an OVA package. The README file guides users on how to verify the integrity of vApp OVA package.

Customers must also upload the provided root and Intermediate certificate on vCenter version 7.0U3E and higher. For vCenter versions between 7.0.1 and 7.0.U3E the functionality of verifying certificate is not supported from VMware. Customers need not upload any certificate for vCenter versions 6.x.

Uploading the trusted root certificate to vCenter

1. Log in with the VMware vSphere Client to the vCenter Server.
2. Specify the username and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group. If you specified a different domain during installation, log in as `administrator@mydomain`.
3. Navigate to the Certificate Management user interface: a. From the Home menu, select Administration. b. Under Certificates, click Certificate Management.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under Trusted Root Certificates, click Add.
6. Click browse and select the location of the certificate .pem file (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Click Add. The certificate is added to the store.

Refer to [Add a Trusted Root Certificate to the Certificate Store](#) for more information. While deploying a vApp (by using the OVA file), the digital signature for the vApp package can be verified on the 'Review details' page. If the downloaded vApp package is genuine, the 'Publisher' column displays 'Trusted Certificate' (As in the following screenshot).

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details
Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit https://www.netapp.com/
Download size	2.2 GB
Size on disk	3.9 GB (thin provisioned)
	53.0 GB (thick provisioned)

CANCEL
BACK
NEXT

Verifying the signature of the ONTAP tools ISO and SRA tar.gz

NetApp shares its code signing certificate with customers on the product download page, along with the product zip files for OTV-ISO and SRA.tgz.

From the code signing certificate users can extract the public key as below:

```
#> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

Then public key should be used to verify the signature for iso and tgz product zip as below :

```
#> openssl dgst -sha256 -verify <public-key> -signature <signature-file> <binary-name>
```

Example:

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK => response
```

Ports and Protocols

Listed here are the required ports and protocols that enable communication between ONTAP tools for VMware vSphere server and other entities like managed storage systems, servers, and other components.

Inbound and outbound ports required for OTV

Please note the table below which lists the inbound and outbound ports required for the proper functioning of ONTAP tools. It is important to ensure that only the ports mentioned in the table are open for connections from remote machines, while all other ports should be blocked for connections from remote machines. This will help ensure the security and safety of your system.

The following table describes the open port details.

TCP v4/v6 port #	Direction	Function
8143	inbound	HTTPS connections for REST API
8043	inbound	HTTPS connections
9060	inbound	HTTPS connections Used for SOAP over HTTPS connections This port must be opened to allow a client to connect to the ONTAP tools API server.
22	inbound	SSH (Disabled by default)
9080	inbound	HTTPS connections - VP and SRA - Internal connections from loopback only
9083	inbound	HTTPS connections - VP and SRA Used for SOAP over HTTPS connections
1162	inbound	VP SNMP trap packets
8443	inbound	Remote Plugin
1527	internal only	Derby database port, only between this computer and itself, external connections not accepted — Internal connections only
8150	internal only	Log integrity service runs on port
443	bi-directional	Used for connections to ONTAP clusters

Controlling remote access to the Derby database

Administrators can access the derby database with the following commands. It can be accessed through the ONTAP tools local VM as well as a remote server with the following steps:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;  
connect 'jdbc:derby://<OTV-  
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

Example:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;  
ij version 10.15  
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=';  
ij> show tables;  
TABLE_SCHEM | TABLE_NAME | REMARKS  
-----  
SYS | SYSALIASES |  
SYS | SYSCHECKS |  
SYS | SYSCOLPERMS |  
SYS | SYSCOLUMNS |  
SYS | SYSCONGLOMERATES |  
SYS | SYSCONSTRAINTS |  
SYS | SYSDEPENDS |  
SYS | SYSFILES |  
SYS | SYSFOREIGNKEYS |  
SYS | SYSKEYS |  
SYS | SYSPERMS |
```

ONTAP tools for VMware vSphere access points (Users)

The ONTAP Tools for VMware vSphere installation creates and uses three types of users:

1. System User: The root user account
2. Application user: The administrator user, maint user, and db user accounts
3. Support user: The diag user account

1. System User

System(root) user gets created by ONTAP tools installation on the underlying operating system(Debian).

- A default system user "root" is created on Debian by ONTAP tools installation. Its default is disabled and can be enabled on an ad-hoc basis through the 'maint' console.

2. Application User

The application user is named as a local user in ONTAP tools. These are users created in ONTAP tools application. The below table lists the types of Application users:

User	Description
Administrator User	It is created during ONTAP tools installation and user provides the credentials while deploying the ONTAP tools. Users has the option to change the 'password' in 'maint' console. Password will expire in 90 days and users are expected to change the same.

User	Description
Maintenance User	It is created during ONTAP tools installation and user provides the credentials while deploying the ONTAP tools. Users has the option to change the 'password' in 'maint' console. This is a maintenance user and is created to execute the maintenance console operations.
Database User	It is created during ONTAP tools installation and user provides the credentials while deploying the ONTAP tools. Users has the option to change the 'password' in 'maint' console. Password will expire in 90 days and users are expected to change the same.

3. Support user(diag user)

During the ONTAP tools installation, a support user is created. This user can be used to access ONTAP tools in case of any issue or outage in the server and to collect logs. By default, this user is disabled, but it can be enabled on an adhoc basis through the 'maint' console. It is important to note that this user will be automatically disabled after a certain time period.

Mutual TLS (Certificate-Based Authentication)

ONTAP versions 9.7 and later support mutual TLS communication. Beginning with ONTAP Tools for VMware and vSphere 9.12, mutual TLS is used for communication with newly added clusters (depending on ONTAP version).

ONTAP

For all previously added storage systems: During an upgrade, all added storage systems will get auto-trusted, and certificate-based authentication mechanisms will get configured.

As in the below screenshot, the Cluster setup page will show the status of Mutual TLS (Certificate-based authentication), configured for each cluster.

Name	Type	IP Address	ONTAP Release	Status	Capacity	NFS VAAI	Supported Protocols
CL_S121vsmuc5501m_1673075280	Cluster	10.224.95.142	9.12.0	Normal	20.42%		

Cluster Add

During cluster add workflow, if the cluster being added supports MTLT, MTLT will be configured by default. The user does not need to do any configuration for this. The below screen shot shows the screen presented to the user during cluster add.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.


vCenter server 10.224.58.52 ▾

Name or IP address: _____

Username: _____

Password: _____

Port: 443

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

ADD

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.


vCenter server 10.224.58.52 ▾

Name or IP address: 10.234.85.142

Username: admin

Password:

Port: 443

Advanced options 

CANCEL

ADD

Add Storage System

Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.234.85.52

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES

CANCEL

ADD

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

Certificate Information

This certificate identifies the 10.234.85.142 host.

Issued By

Name (CN or DN): C1_sti21-vsimgucs581m_1678878260

Issued To

Name (CN or DN): C1_sti21-vsimgucs581m_1678878260

Validity

Issued On: 03/15/2023 11:16:06

Expires On: 03/14/2024 11:16:06

Fingerprint Information

SHA-1 Fingerprint: 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:82:C1:A6:EE:34:53:A0:F3

SHA-256 Fingerprint: 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:52:F8:76:98:64:FA:23

Do you want to trust this certificate?

NO

YES

Cluster Edit

During cluster edit operation, there are two scenarios:

- If the ONTAP certificate expires then the user will have to get the new cert and upload it.
- If the OTV certificate expires then the user can regenerate it by checking the checkbox.
 - *Generate a new client certificate for ONTAP.*

Modify Storage System

Settings Provisioning Options

IP address or hostname: ▼

Port:

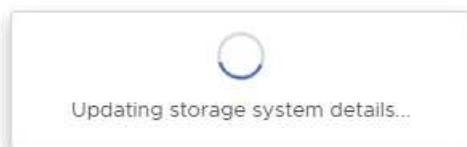
Username:

Password:

Upload Certificate (Optional) [BROWSE](#)

Skip monitoring of this storage system

Generate a new client certificate for ONTAP



ONTAP tools HTTPS Certificate

By default ONTAP tools uses a self-signed certificate automatically created during installation for securing HTTPS access to the Web UI. ONTAP tools provides the following features:

1. Regenerate HTTPS certificate

During the ONTAP tools installation, an HTTPS CA certificate gets installed and the certificate gets stored in the keystore. The user has the option to regenerate the HTTPS certificate through the maint console.

The above options can be accessed in *maint* console by navigating to '*Application Configuration*' → '*Regenerate certificates*'.

Login Banner

The following login banner is shown after the user enters a username in the login prompt. Please note that SSH is disabled by default and only allows one-time logins when enabled from the VM console.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

After the user completes login through the SSH channel, the following text is displayed:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Inactivity Timeout

To prevent unauthorized access, an inactivity timeout is set up, which automatically logs out users who are inactive for a certain period while using authorized resources. This ensures that only authorized users can access the resources and helps to maintain security.

- By default, the vSphere Client sessions close after 120 minutes of idle time, requiring the user to log in again to resume using the client. You can change the timeout value by editing the `webclient.properties` file. You can configure the timeout of the vSphere Client [Configure the vSphere Client Timeout Value](#)
- ONTAP tools has a web-cli session logout time of 30 minutes.

Maximum concurrent requests per user (Network security protection :: DOS attack)

By default, the number of maximum concurrent requests per user is 48. The root user in ONTAP tools can change this value depending on the requirements of their environment. **This value should not be set to a very high value as this provides a mechanism against denial of service (DOS) attacks.**

Users can change the number of maximum concurrent sessions and other supported parameters in the `/opt/netapp/vscserver/etc/dosfilterParams.json` file.

We can configure the filter by following parameters :

- **delayMs**: The delay in milliseconds given to all requests over the rate limit before they are considered.

Give -1 to just reject the request.

- **throttleMs**: How long to async wait for semaphore.
- **maxRequestMs**: How long to allow this request to run.
- **ipWhitelist**: A comma-separated list of IP addresses that will not be rate-limited. (This can be Vcenter, ESXi and SRA IPs)
- **maxRequestsPerSec**: The maximum number of requests from a connection per second.

Default values in the `dosfilterParams` file:

```
{ "delayMs": "-1",  
  "throttleMs": "1800000",  
  "maxRequestMs": "300000",  
  "ipWhitelist": "10.224.58.52",  
  "maxRequestsPerSec": "48" }
```

Network Time Protocol (NTP) Configuration

Sometimes, security issues can occur due to discrepancies in network time configurations. It is important to ensure that all devices within a network have accurate time settings to prevent such issues.

Virtual appliance

You can configure the NTP server(s) from the maintenance console in the virtual appliance. Users can add the NTP server details under *System Configuration* ⇒ *Add new NTP Server* option

By default, the service for NTP is `ntpd`. This is a legacy service and does not work well for virtual machines in certain cases.

Debian

On Debian, the user can access the `/etc/ntp.conf` file for ntp server details.

Password Policies

Users deploying ONTAP tools for the first time or upgrading to version 9.12 or later will need to follow the strong password policy for both the administrator and database users. During the deployment process, new users will be prompted to enter their passwords. For brownfield users upgrading to version 9.12 or later, the option to follow the strong password policy will be available in the maintenance console.

- Once the user logs into the maint console the passwords will be checked against the complex rule set and if found to be not followed then the user will be asked to reset the same.
- Password default validity is 90 days and after 75 days user will start getting the notification to change the password.

- It is required to set a new password in every cycle, the system will not take the last password as the new password.
- Whenever a user logs in to the maint console it will check for the password policies like the below screenshots before loading the Main Menu:

```
Maintenance Console : "NetApp ONTAP tools for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Validating password policies
```

- If found not following the password policy or its a upgrade setup from ONTAP tools 9.11 or before. Then user will see following screen to reset the password:

```
Your Administrator and Database password is expired or does not match password policy:
-----
1 ) Change 'administrator' user password
2 ) Change database password
x ) Exit
Enter your choice: _
```

- If user tries to set weak password or gives the last password again then user will see following error:

```
Changing password for administrator.
User: administrator
Enter new password:
Retype new password:
Password doesn't match the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.
Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
00:00:23 13:26:23 Your new password must be different
Error updating sra credential file
Press ENTER to continue...
```

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.