

Verify the identity of remote servers using certificates

ONTAP 9

NetApp December 21, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/system-admin/verify-identity-remote-servers-certificates-concept.html on December 21, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Ve	erify the identity of remote servers using certificates	•
	Verify the identity of remote servers using certificates overview	
	Verify digital certificates are valid using OCSP	
	View default certificates for TLS-based applications	
	Mutually authenticating the cluster and a KMIP server	4

Verify the identity of remote servers using certificates

Verify the identity of remote servers using certificates overview

ONTAP supports security certificate features to verify the identity of remote servers.

ONTAP software enables secure connections using these digital certificate features and protocols:

- Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections. This feature is disabled by default.
- A default set of trusted root certificates is included with ONTAP software.
- Key Management Interoperability Protocol (KMIP) certificates enable mutual authentication of a cluster and a KMIP server.

Verify digital certificates are valid using OCSP

Beginning with ONTAP 9.2, Online Certificate Status Protocol (OCSP) enables ONTAP applications that use Transport Layer Security (TLS) communications to receive digital certificate status when OCSP is enabled. You can enable or disable OCSP certificate status checks for specific applications at any time. By default, OCSP certificate status checking is disabled.

What you'll need

These commands must be performed at the advanced privilege level.

About this task

OCSP supports the following applications:

- AutoSupport
- Event Management System (EMS)
- LDAP over TLS
- Key Management Interoperability Protocol (KMIP)
- · Audit Logging
- FabricPool

Steps

- 1. Set the privilege level to advanced: set -privilege advanced.
- To enable or disable OCSP certificate status checks for specific ONTAP applications, use the appropriate command.

If you want OCSP certificate status checks for some applications to be	Use the command
Enabled	security config ocsp enable -app app name
Disabled	security config ocsp disable -app app name

The following command enables OCSP support for AutoSupport and EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

When OCSP is enabled, the application receives one of the following responses:

- Good the certificate is valid and communication proceeds.
- Revoked the certificate is permanently deemed as not trustworthy by its issuing Certificate Authority and communication fails to proceed.
- Unknown the server does not have any status information about the certificate and communication fails to proceed.
- OCSP server information is missing in the certificate the server acts as if OCSP is disabled and continues with TLS communication, but no status check occurs.
- No response from OCSP server the application fails to proceed.
- 3. To enable or disable OCSP certificate status checks for all applications using TLS communications, use the appropriate command.

If you want OCSP certificate status checks for all applications to be	Use the command
Enabled	security config ocsp enable -app all
Disabled	security config ocsp disable -app all

When enabled, all applications receive a signed response signifying that the specified certificate is good, revoked, or unknown. In the case of a revoked certificate, the application will fail to proceed. If the application fails to receive a response from the OCSP server or if the server is unreachable, the application will fail to proceed.

4. Use the security config ocsp show command to display all the applications that support OCSP and their support status.

cluster::*> security config ocsp show Application OCSP Enabled? _____ autosupport false audit log false fabricpool false ems false kmip false ldap ad true ldap nis namemap true 7 entries were displayed.

View default certificates for TLS-based applications

Beginning with ONTAP 9.2, ONTAP provides a default set of trusted root certificates for ONTAP applications using Transport Layer Security (TLS).

What you'll need

The default certificates are installed only on the admin SVM during its creation, or during an upgrade to ONTAP 9.2.

About this task

The current applications that act as a client and require certificate validation are AutoSupport, EMS, LDAP, Audit Logging, FabricPool, and KMIP.

When certificates expire, an EMS message is invoked that requests the user to delete the certificates. The default certificates can only be deleted at the advanced privilege level.



Deleting the default certificates may result in some ONTAP applications not functioning as expected (for example, AutoSupport and Audit Logging).

Step

1. You can view the default certificates that are installed on the admin SVM by using the security certificate show command:

security certificate show -vserver -type server-ca

Mutually authenticating the cluster and a KMIP server

Mutually authenticating the cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

Generate a certificate signing request for the cluster

You can use the security certificate generate-csr command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

What you'll need

You must be a cluster administrator or SVM administrator to perform this task.

Steps

1. Generate a CSR:

```
security certificate generate-csr -common-name FQDN\_or\_common\_name -size 512|1024|1536|2048 -country country -state state -locality locality -organization organization -unit unit -email-addr email_of_contact -hash -function SHA1|SHA256|MD5
```

For complete command syntax, see the man pages.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is server1.companyname.com, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is web@example.com. The system displays the CSR and the private key in the output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request:
----BEGIN CERTIFICATE REQUEST----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBqNVBAqTADEJMACGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBqNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQ0
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
----END CERTIFICATE REQUEST----
Private Key:
24 | Administrator Authentication and RBAC
----BEGIN RSA PRIVATE KEY----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
qQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQqEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
----END RSA PRIVATE KEY----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copy the certificate request from the CSR output, and then send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Install a CA-signed server certificate for the cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

What you'll need

You must have already installed the root certificate of the SSL server on the cluster or SVM with the server-ca certificate type.

Steps

1. To use a self-signed digital certificate for client authentication, use the security certificate create

command with the type client parameter.

- 2. To use a CA-signed digital certificate for client authentication, complete the following steps:
 - Generate a digital certificate signing request (CSR) by using the security certificate generate-csr command.
 - ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you to copy the output to a file for future reference.
 - b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA for signing.

You should keep a copy of the private key and the CA-signed certificate for future reference.

After processing your request, the CA sends you the signed digital certificate.

- c. Install the CA-signed certificate by using the security certificate install command with the -type client parameter.
- d. Enter the certificate and the private key when you are prompted, and then press Enter.
- e. Enter any additional root or intermediate certificates when you are prompted, and then press Enter.

You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

Provide the client-ca certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

The security certificate show command with the -instance and -type client-ca parameters displays the client-ca certificate information.

Install a CA-signed client certificate for the KMIP server

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the -subtype kmip-cert parameter), along with the client and server-ca types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

Steps

- 1. Use the security certificate install command with the -type server-ca and -subtype kmip-cert parameters to install a KMIP certificate for the KMIP server.
- 2. When you are prompted, enter the certificate, and then press Enter.

ONTAP reminds you to keep a copy of the certificate for future reference.

cluster1::> security certificate install -type server-ca -subtype kmipcert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
----BEGIN CERTIFICATE---MICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
----END CERTIFICATE----You should keep a copy of the CA-signed digital certificate for future
reference.
cluster1::>

Copyright information

Copyright © 2022 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.