# Table of Contents

- security certificate commands .......................................................... 1
- security certificate create ................................................................. 1
- security certificate delete ................................................................. 3
- security certificate generate-csr ......................................................... 5
- security certificate install ............................................................... 9
- security certificate print ................................................................. 12
- security certificate rename ............................................................. 15
- security certificate show-generated .................................................. 16
- security certificate show-truststore .................................................... 19
- security certificate show-user-installed ............................................. 23
- security certificate show ............................................................... 26
- security certificate sign ................................................................. 30
- security certificate ca-issued revoke .................................................. 34
- security certificate ca-issued show ..................................................... 34
- security certificate config modify ...................................................... 37
- security certificate config show ....................................................... 38
- security certificate truststore check .................................................. 38
- security certificate truststore clear ................................................... 39
- security certificate truststore load ..................................................... 40
security certificate commands

security certificate create

Create and Install a Self-Signed Digital Certificate

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

The security certificate create command creates and installs a self-signed digital certificate, which can be used for server authentication, for signing other certificates by acting as a certificate authority (CA), or for Data ONTAP as an SSL client. The certificate function is selected by the -type field. Self-signed digital certificates are not as secure as certificates signed by a CA. Therefore, they are not recommended in a production environment.

Parameters

-vserver <Vserver Name> - Name of Vserver
This specifies the name of the Vserver on which the certificate will exist.

-common-name <FQDN or Custom Common Name> - FQDN or Custom Common Name
This specifies the desired certificate name as a fully qualified domain name (FQDN) or custom common name or the name of a person. The supported characters, which are a subset of the ASCII character set, are as follows:

• Letters a through z, A through Z
• Numbers 0 through 9
• Asterisk (*), period (.), underscore (_) and hyphen (-)

The common name must not start or end with a "-" or a ".". The maximum length is 253 characters.

-type <type of certificate> - Type of Certificate
This specifies the certificate type. Valid values are the following:

• server - creates and installs a self-signed digital certificate and intermediate certificates to be used for server authentication
• root-ca - creates and installs a self-signed digital certificate to sign other certificates by acting as a certificate authority (CA)
• client - includes a self-signed digital certificate and private key to be used for Data ONTAP as an SSL client

[-subtype <kmip-cert>] - (DEPRECATED)-Certificate Subtype
This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.
This specifies a certificate subtype. This optional parameter can have an empty value (the default). The only valid value is as follows:

* `kmip-cert` - this is a Key Management Interoperability Protocol (KMIP) certificate

`[-cert-name <text>]` - Unique Certificate Name

This specifies the system's internal identifier for the certificate. It must be unique within a Vserver. If not provided, it is automatically generated by the system.

`-size <size of requested certificate in bits>` - Size of Requested Certificate in Bits

This specifies the number of bits in the private key. The larger the value, the more secure is the key. The default is 2048. Possible values include 512, 1024, 1536, 2048 and 3072 when the "FIPS Mode" in "security config" is false. When the "FIPS Mode" is true, the possible values are 2048 and 3072.

`-country <text>` - Country Name

This specifies the country where the Vserver resides. The country name is a two-letter code. The default is US. Here is the list of country codes:

Country Codes

`-state <text>` - State or Province Name

This specifies the state or province where the Vserver resides.

`-locality <text>` - Locality Name

This specifies the locality where the Vserver resides. For example, the name of a city.

`-organization <text>` - Organization Name

This specifies the organization where the Vserver resides. For example, the name of a company.

`-unit <text>` - Organization Unit

This specifies the unit where the Vserver resides. For example, the name of a section or a department within a company.

`-email-addr <mail address>` - Contact Administrator’s Email Address

This specifies the email address of the contact administrator for the Vserver.

`-expire-days <integer>` - Number of Days until Expiration

This specifies the number of days until the certificate expires. The default value is 365 days. Possible values are between 1 and 3652.

`-protocol <protocol>` - Protocol

This specifies the protocol type. This parameter currently supports only the SSL protocol type. The default is SSL.

`-hash-function <hashing function>` - Hashing Function

This specifies the cryptographic hashing function for signing the certificate. The default is SHA256. Possible values include SHA256, SHA224, SHA384 and SHA512.
Examples

This example creates a server type, self-signed digital certificate for a Vserver named vs0 at a company whose custom common name is www.example.com and whose Vserver name is vs0.

```
cluster1::> security certificate create -vserver vs0 -common-name www.example.com -type server
```

This example creates a root-ca type, self-signed digital certificate with a 2048-bit private key generated by the SHA256 hashing function that will expire in 365 days for a Vserver named vs0 for use by the Software group in IT at a company whose custom common name is www.example.com, located in Sunnyvale, California, USA. The email address of the contact administrator who manages the Vserver is web@example.com.

```
cluster1::> security certificate create -vserver vs0 -common-name www.example.com -type root-ca -size 2048 -country US -state California -locality Sunnyvale -organization IT -unit Software -email-addr web@example.com -expire-days 365 -hash-function SHA256
```

This example creates a client type of self-signed digital certificate for a Vserver named vs0 at a company that uses Data ONTAP as an SSL client. The company's custom common name is www.example.com and its Vserver name is vs0.

```
cluster1::> security certificate create -vserver vs0 -common-name www.example.com -type client -size 2048 -country US -state California -locality Sunnyvale -organization IT -unit Software -email-addr web@example.com -expire-days 365 -hash-function SHA256
```

security certificate delete

Delete an Installed Digital Certificate

**Availability:** This command is available to cluster and Vserver administrators at the admin privilege level.

**Description**

This command deletes an installed digital security certificate.

**Parameters**

- `-vserver <Vserver Name>` - Name of Vserver
  
  This specifies the Vserver that contains the certificate.

- `-common-name <FQDN or Custom Common Name>` - FQDN or Custom Common Name
  
  This specifies the desired certificate name as a fully qualified domain name (FQDN) or custom common name or the name of a person. The supported characters, which are a subset of the ASCII character set, are as follows:
- Letters a through z, A through Z
- Numbers 0 through 9
- Asterisk (*), period (.), underscore (_) and hyphen (-)

The common name must not start or end with a "-" or a ".". The maximum length is 253 characters.

[-serial <text>] - Serial Number of Certificate
This specifies the certificate serial number.

-ca <text> - Certificate Authority
This specifies the certificate authority (CA).

-type <type of certificate> - Type of Certificate
This specifies the certificate type. Valid values are the following:

- server - includes server certificates and intermediate certificates
- root-ca - includes a self-signed digital certificate to sign other certificates by acting as a certificate authority (CA)
- client-ca - includes the public key certificate for the root CA of the SSL client. If this client-ca certificate is created as part of a root-ca, it will be deleted along with the corresponding deletion of the root-ca.
- server-ca - includes the public key certificate for the root CA of the SSL server to which Data ONTAP is a client. If this server-ca certificate is created as part of a root-ca, it will be deleted along with the corresponding deletion of the root-ca.
- client - includes a public key certificate and private key to be used for Data ONTAP as an SSL client

[-subtype <kmip-cert>] - (DEPRECATED)-Certificate Subtype
This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

This specifies a certificate subtype. This optional parameter can have an empty value (the default). The only valid value is as follows:

- kmip-cert - this is a Key Management Interoperability Protocol (KMIP) certificate

[-cert-name <text>] - Unique Certificate Name
This specifies the system's internal identifier for the certificate. It is unique within a Vserver.

Examples
This example deletes a root-ca type digital certificate for a Vserver named vs0 in a company named www.example.com with serial number 4F57D3D1.
security certificate generate-csr

Generate a Digital Certificate Signing Request

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command generates a digital certificate signing request and displays it on the console. A certificate signing request (CSR or certification request) is a message sent to a certificate authority (CA) to apply for a digital identity certificate.

Parameters

[-common-name <text>] - FQDN or Custom Common Name

This specifies the desired certificate name as a fully qualified domain name (FQDN) or custom common name or the name of a person. The supported characters, which are a subset of the ASCII character set, are as follows:

- Letters a through z, A through Z
- Numbers 0 through 9
- Asterisk (*), period (.), underscore (_) and hyphen (-)

The common name must not start or end with a "-" or a ".". The maximum length is 253 characters.

{ [-size <size of requested certificate in bits>] - (DEPRECATED)-Size of Requested Certificate in Bits

This specifies the number of bits in the private key. A larger size value provides for a more secure key. The default is 2048. Possible values include 512, 1024, 1536, and 2048.

This parameter has been deprecated in ONTAP 9.8 and may be removed in future releases of Data ONTAP. Use the security-strength parameter instead.

| [-security-strength <bits of security strength>] - Security Strength in Bits |

Use this parameter to specify the minimum security strength of the certificate in bits. The security bits mapping to RSA and ECDSA key length, in bits, are as follows:

<table>
<thead>
<tr>
<th>Size</th>
<th>RSA Key Length</th>
<th>Elliptic Curve Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>4096</td>
<td>384</td>
</tr>
</tbody>
</table>
Note: FIPS supported values are restricted to 112 and 128.

[algorithm <Asymmetric key generation algorithm>] - Asymmetric Encryption Algorithm
   Use this parameter to specify the asymmetric encryption algorithm to use for generating the public/private key for the certificate signing request. Algorithm values can be RSA or EC. Default value is RSA.

[-country <text>] - Country Name
   This specifies the country where the Vserver resides. The country name is a two-letter code. The default is US. Here is the list of country codes:
   Country Codes

[-state <text>] - State or Province Name
   This specifies the state or province where the Vserver resides.

[-locality <text>] - Locality Name
   This specifies the locality where the Vserver resides. For example, the name of a city.

[-organization <text>] - Organization Name
   This specifies the organization where the Vserver resides. For example, the name of a company.

[-unit <text>] - Organization Unit
   This specifies the unit where the Vserver resides. For example, the name of a section or a department within a company.

[-email-addr <mail address>] - Contact Administrator’s Email Address
   This specifies the email address of the contact administrator for the Vserver.

[-hash-function <hashing function>] - Hashing Function
   This specifies the cryptographic hashing function for signing the certificate. The default is SHA256. Possible values include SHA224, SHA256, SHA384, and SHA512.

[-key-usage <Certificate key usage extension>,…] - Key Usage Extension
   Use this parameter to specify the key usage extension values. The default values are: digitalSignature, keyEncipherment. Possible values include:

   • digitalSignature
   • nonRepudiation
   • keyEncipherment
   • dataEncipherment
   • keyAgreement
   • keyCertSigning
   • cRLSigning
   • encipherOnly
   • decipherOnly
[-extended-key-usage <Certificate extKeyUsage extension>,...] - Extended Key Usage Extension

Use this parameter to specify the extended key usage extension values. The default values are: serverAuth, clientAuth. Possible values include:

- serverAuth
- clientAuth
- codeSigning
- emailProtection
- timeStamping
- OCSPSigning

[-rfc822-name <mail address>,...] - Email Address SAN

Use this parameter to specify the Subject Alternate Name extension - a list of rfc822-names (email addresses).

[-uri <text>,...] - URI SAN

Use this parameter to specify the Subject Alternate Name extension - a list of URIs.

[-dns-name <text>,...] - DNS Name SAN

Use this parameter to specify the Subject Alternate Name extension - a list of DNS names.

[-ipaddr <IP Address>,...] - IP Address SAN

Use this parameter to specify the Subject Alternate Name extension - a list of IP addresses.

Examples

This example creates a certificate-signing request with a 2048-bit RSA private key generated by the SHA256 hashing function for use by the Engineering group in IT at a company whose custom common name is www.example.com, located in Durham, NC, USA. The email address of the contact administrator who manages the Vserver is web@example.com. The request also specifies the subject alternative names, key-usage and extended-key-usage extensions.

```bash
cluster-1::> security certificate generate-csr -common-name www.example.com -algorithm RSA -hash-function SHA256 -security-strength 128 -key-usage critical,digitalSignature,keyEncipherment,extended-key-usage serverAuth,clientAuth -country US -state NC -locality Durham -organization IT -unit Engineering -email-addr web@example.com -rfc822-name example@example.com -dns-name shop.example.com, store.example.com

Certificate Signing Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIEWDCCAsACgAwGDAWBgNVBAoTD3d3dy5leGFtcGxlLmNvbTELMAkGA1UEBhMCVVMxDzAJBgNVBAgTAk5DMQ8wDQYDVQQIEwZEdXJoYW0xMjAyJSBEeTgMc3NhMCQwDQYDVQQGEwJlMGUxETAPBgNVBAsTQVFNREJHMjUwMwYDVQQDDBCtby50ZXN0LmNsb30sIyUzJSUwNjMuMDEwMDAwMDAwMjMwMjMwMSowMDkoMC0wNjUwMDUwMDAwMjMwMjMwMHUwNjUwMDUwMDAwMjMwMjMwMDAwMDAwNjMuMDEwMDAwMDAwMjMwMjMwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDaw...
-----BEGIN CERTIFICATE REQUEST-----

rNRn/+MqE+jQA7yAdufYxD537cDcT46ihkajISe0Ei93yf6IKmvUAvmJvQ3R7Z4E
QCOWHj56yQ+lXj36bYdwa74S8u8ipCs3Yyxw8fgvrh/v6H0rn1KDQSquF3R5u7Z2ym
tRA7EJMY62f9ALgcFNhQPuP6jpc8aP7Tv7BKXAninryDDcoMdW8UCzfTPgzCDh5z
S++eNP3s/7cGfRSQ8aXnDTVQLypsurDgVwZXXgu+2P0zUcf2AYBT/+rdq3VkgWu
QM+mGRMB5300ff4QOi+SvCsxWxq32zwicz1kWs/i9h2t2k/vd/87ESeYLqFxyh+
0nwacskMRGxOuTLgx+XH+/EntjIr4fj9/FshYCIcy8vpq10xPacPlu96ebnbiEuO
y6rvCj2eceG6oEwbRHB5fIMJ03zrdjdz/d1z4ktBuG7E4CUyEvkAgMBAAggykg
gYYGCSqGSiB3DQEDfjD5HMcwRgyDVR0RAQH/BDwwoETZXhbxBsZUBleGFtcGxl
LmNvbYlYQc2vcC51eGFtcGxlLmNvbYlYRc3RvmcuUZxhbxBsZS5je20wQyDVR0P
AQH/BAQDAgWgMB0GA1UDjQQWMBQGCCsGAQUFBQcGAo4EEF5EAA2Mw4RMA0GCSq
GSIb3DQEJDjF5MHcwRgYDVR0RAQH/BDwwOoETZXhbxBsZUBleGFtcGxl
-----END CERTIFICATE REQUEST-----

Private Key :
-----BEGIN PRIVATE KEY-----
MIIG/AIBABDgkqhkiG9w0BAQEFAAFCBuYWggbiAaEAAoIBqGQC6jzomD+zOHCz
RiIRf9Fp/+PaMcKskyh1LvnL/ig2yjBfFdufnCd/+CLAqJQI/APV7eOErdoYes
1GF/4yoT6NAdvIB259jENpftwNxpqJGrRh7QL3sfJ/qgg9QC+Ym9DdhtnqRA
I5yePnrJD4tePfpth3BrvhLy7yWkKzjdjDhx+CuH+/ofSueUoNBjC4V7hm7tlnKai
EDsQkxjrZ/OAuBwU2FA+4/qmNzxo/t/sEpCeeKevIMNyYlbxRz9N9+DMIOHnNL
7650/ez/tw92FJdpecNNAtim75knaj4/YBgfP7+t2rDWsbASa
z6YeZfQhol7c79/hA6l5JXvdJZerfbDNyU/Oqxb+IH2HPZ6PcW3/xnsRj5guOGFj7s
FbpypyQxEB65Mud5c78s205juluxM39Kfgh7Lzhy+lq7neV0E8K735p5udIJ677
pG8InZ6Bwzo55FsdYH18gnLImdt2PP93XPiOG4bsThxRiQS+8CAwEAAQKCyABW
ftqWFFIVaWi2y3dmJCbL84oAP3axTHURXvund3uk6U7incng0WqKbHnsSHaDyX
1vJqc7d1lb4w5+Tv7DGJE4E9GALKK70iIygzGtUjQUcwkF0HweOijmbDvHYyiJm
jvN2bJ71bDtpSRZAhS6mY4eZRSEDgST1PyXn7krEZ6kBSj5u85G/Bwt88Ky80s+
PIdiIldiQ5p5vA12TdpQvhyI+7sqCkZZQm5PgeBG2QDilP+PgizryWB1sMpi1CCgq
zarFQziNe7qrp6FFKvPA0Q5Lxly0xhgm86FCMJUxpxMeb08y4FRedzB42a0Z/YL0
HhpWAl42sRoa5s5fLzQ3h19wsvj2/+FRU6hWT+ma/Val35iInkygfzWUAAjNY
F6B0sBBd9bVeKDOXD/R/wCwbuaKZGMaVOenZbczmFUvSi4HZGyqVRx68lxVoD0
MZXwWlwO9Z2C6i13vp/ReAsouCndKshfervHI58x82FMTMxxz/kby7k5f7yylkC
gcEA4tiPiV1eKc/ft0sPUnMMZ/snHFxc+xohzyTygCglLRf8zjDnUT/o9D8SRe1/
crkG7ZczKvIdPz0tatyjNMsZ9TDSiAJQQR8et1+jB0Ey2qG+ab/Ub7617GBX0
O78UcmtEyx5aDeSSwjr+yGerG4e7zGzItScTe2JMa5fPl1eyfNzk1Gtba9ibM
r991o/PahSmC5iPxf4avYm/vQm2p+wIk+o6ZHJIA1LFrCv8y9y1yvQjw+tZa+A
GbD7AhBANKHqg0JB58LJnmN/5/FLkKeLhaZG+UNUngmt46dm/84/srtjCUPdthQd
HvM/skRYDverMj50Q2HzmVc8+zzs9r01VNNa+Tzcoi3eB3FpdDYDTPdLSzRfsC82
security certificate install

Install a Digital Certificate

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

The `security certificate install` command installs digital security certificates signed by a certificate authority (CA) and the public key certificate of the root CA. Digital security certificates also include the intermediate certificates to construct the chain for server certificates (the server type), client-side root CA certificates (the client-ca type), or server-side root CA certificates (the server-ca type). With FIPS enabled, the following restrictions apply to the certificate getting installed. server/client/server-ca/client-ca: Key size >= 2048, server/client: Hash function (No MD-5, No SHA-1), server-ca/client-ca: (Intermediate CA), Hash Function (No MD-5, No SHA-1), server-ca/client-ca: (Root CA), Hash Function (No MD-5)

Parameters

-vserver <Vserver Name> - Name of Vserver

This specifies the Vserver that contains the certificate.

-type <type of certificate> - Type of Certificate

This specifies the certificate type. Valid values are the following:

- server - includes server certificates and intermediate certificates.
- client-ca - includes the public key certificate for the root CA of the SSL client

Note: Please keep a copy of your certificate request and private key for future reference.
• **server-ca** - includes the public key certificate for the root CA of the SSL server to which Data ONTAP is a client

• **client** - includes a self-signed or CA-signed digital certificate and private key to be used for Data ONTAP as an SSL client

[**-subtype <kmip-cert>**] - (DEPRECATED)-Certificate Subtype

This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

This specifies a certificate subtype. This optional parameter can have an empty value (the default). The only valid value is as follows:

• **kmip-cert** - this is a Key Management Interoperability Protocol (KMIP) certificate

[**-cert-name <text>**] - Unique Certificate Name

This specifies the system’s internal identifier for the certificate. It must be unique within a Vserver. If not provided, it is automatically generated by the system.

Examples

This example installs a CA-signed certificate (along with intermediate certificates) for a Vserver named vs0.

```
cluster1::> security certificate install -vserver vs0 -type server
Please enter Certificate: Press <Enter> when done
-------BEGIN CERTIFICATE-------
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEYDVQQLDEwpZXRh
chAuY29tMQswCQYDVQQGEwJUUEJMAcGA1UEBMMMQ0MwGAYDVQQHEwJuY29tMQsw
EA0gTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNTI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEYDVQQLDEwpZXRhchAuY29tMQswCQYDVQQG
EwJUVEJMAcGA1UEBMMMQ0MwGAYDVQQHEwJuY29tMQswCQYDVQQG
-------END CERTIFICATE-------
Please enter Private Key: Press <Enter> when done
-------BEGIN RSA PRIVATE KEY-------
MIIBPAIBAAJBAAM6yrtrk8nQjB2UsWeHoET8gk0BPX+Y5MLycsUdxA7hXhumHNPvF
C61X2G32Sx8VEaith94tx+vOEzq+UaqHlt0CAwEAaQuBMZjDwlgmlm3qIr/n8VT
-------END RSA PRIVATE KEY-------
```

Do you want to continue entering root and/or intermediate certificates {y|n}: y
Please enter Intermediate Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
MIIE+zCCBGsAgIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxAwIBAIAAgxjBgNVBAYT... 

-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----
MIIC5zCCAlCAQwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVAcBGMEQwDQYJKoZIhvc... 

-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate certificates {y|n}: n

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

This example installs a CA certificate for client authentication for a Vserver named vs0.
This example installs a CA certificate for server authentication for a Vserver named vs0. In this case, Data ONTAP acts as an SSL client.

```
cluster1::> security certificate install -vserver vs0 -type server-ca

-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNhIilsXjOKUgodJfTNcJVDANBgkqhkiG9w0BAQUFADCg
zjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAAGA1UE
Qz0wU2VydGlmaWNhdGVtMRAwIzASIzIjAgIgYDVR0PAQH/BAQDQgAECAOICAQ
-----END CERTIFICATE-----
You should keep a copy of the CA-signed digital certificate for future reference.
```

security certificate print

Display the contents of a certificate

**Availability:** This command is available to `cluster` and `Vserver` administrators at the `admin` privilege level.

**Description**

This command displays the details of either an installed certificate or by reading a certificate from user input.
Parameters

-vserver <Vserver Name> - Vserver Name
   Use this parameter to specify the Vserver that has the certificate installed.

{ [-cert-name <text>] - Installed Certificate Name
   Use this parameter to specify the unique name of the installed certificate to read and display.

| [-cert-uuid <UUID>] - Installed Certificate UUID }
   Use this parameter to specify the unique UUID of the installed certificate to read and display. With no name or UUID specified, the certificate will read and display from user input.

Examples

The following example reads and prints the details of the certificate.

```bash
cluster1::> security certificate print -vserver vs0 -cert-name
AAAACertificateServices
Certificate details:
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 6271844772424770508 (0x570a119742c4e3cc)
      Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=IT, L=Milan, O=Actalis S.p.A./03358520967, CN=Actalis Authentication Root CA
      Validity
         Not Before: Sep 22 11:22:02 2011 GMT
         Not After : Sep 22 11:22:02 2030 GMT
      Subject: C=IT, L=Milan, O=Actalis S.p.A./03358520967, CN=Actalis Authentication Root CA
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
               Modulus:
                  6f:51:3b:9f:0a:5a:c9:c2:48:38:0a:c2:1c:a0:18:
                  4d:00:96:5a:6f:2f:c0:44:7e:a3:0e:e4:91:cd:58:
                  b7:8a:0c:5d:07:37:08:cb:6c:d2:7a:47:22:44:35:
```
X509v3 extensions:

X509v3 Subject Key Identifier:


X509v3 Basic Constraints: critical
CA:TRUE

X509v3 Authority Key Identifier:


X509v3 Key Usage:
Certificate Sign, CRL Sign

Signature Algorithm: sha256WithRSAEncryption
security certificate rename

Rename a certificate

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

**Description**

This command allows the user to modify the name of an installed digital certificate. This command does not alter the certificate itself.

**Parameters**

- **-vserver <Vserver Name>** - Vserver Name
  
  This specifies the name of the Vserver on which the certificate exists.

- **-cert-name <text>** - Existing Certificate Name
  
  This specifies the current name of the certificate.

- **-new-name <text>** - New Certificate Name
  
  This specifies the desired name of the certificate. It must be unique among certificates in the Vserver.

**Examples**

```
cluster1::> security certificate rename -vserver vs0 -cert-name AAACertificateServices -new-nameAAACertServ
```
security certificate show-generated

Display ONTAP generated certificates

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command displays information about the Data ONTAP generated digital digital certificates. Some details are displayed only when you use the command with the -instance parameter.

Parameters

{ [-fields <fieldname>,...] }
If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance ] }
If you specify the -instance parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Name of Vserver
Selects the Vserver whose digital certificates you want to display.

[-common-name <FQDN or Custom Common Name>] - FQDN or Custom Common Name
Selects the certificates that match this parameter value.

[-serial <text>] - Serial Number of Certificate
Selects the certificates that match this parameter value.

[-ca <text>] - Certificate Authority
Selects the certificates that match this parameter value.

[-type <type of certificate>] - Type of Certificate
Selects the certificates that match this parameter value.

[-subtype <kmip-cert>] - (DEPRECATED)-Certificate Subtype
This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

Selects the certificate subtype that matches the specified value. The valid values are as follows:

* kmip-cert - this is a Key Management Interoperability Protocol (KMIP) certificate

[-cert-name <text>] - Unique Certificate Name
This specifies the system's internal identifier for the certificate. It is unique within a Vserver.
[-size <size of requested certificate in bits>] - Size of Requested Certificate in Bits
Selects the certificates that match this parameter value.

[-start <Date>] - Certificate Start Date
Selects the certificates that match this parameter value.

[-expiration <Date>] - Certificate Expiration Date
Selects the certificates that match this parameter value.

[-public-cert <certificate>] - Public Key Certificate
Selects the certificates that match this parameter value.

[-country <text>] - Country Name
Selects the certificates that match this parameter value.

[-state <text>] - State or Province Name
Selects the certificates that match this parameter value.

[-locality <text>] - Locality Name
Selects the certificates that match this parameter value.

[-organization <text>] - Organization Name
Selects the certificates that match this parameter value.

[-unit <text>] - Organization Unit
Selects the certificates that match this parameter value.

[-email-addr <mail address>] - Contact Administrator's Email Address
Selects the certificates that match this parameter value.

[-protocol <protocol>] - Protocol
Selects the certificates that match this parameter value.

[-hash-function <hashing function>] - Hashing Function
Selects the certificates that match this parameter value.

[-self-signed {true|false}] - Self-Signed Certificate
Selects the certificates that match this parameter value.

[-is-root {true|false}] - Is Root CA Certificate?
Selects the certificates that match this parameter value.

[-authority-key-identifier <text>] - Authority Key Identifier
Selects the certificates that match this parameter value.

[-subject-key-identifier <text>] - Subject Key Identifier
Selects the certificates that match this parameter value.
Examples

The examples below display information about Data ONTAP generated digital certificates.

```
cluster1::> security certificate show-generated

Vserver  Serial Number  Certificate Name          Type
---------- -------------- -----------------------------------------
          -------------- -----------------------------------------
          4F4E4D7B         www.example.com         server

Certificate Authority: www.example.com
Expiration Date: Thu Feb 28 16:08:28 2013
```
cluster1::> security certificate show-generated -instance
Vserver: vs0
Certificate Name: www.example.com
FQDN or Custom Common Name: www.example.com
Serial Number of Certificate: 4F4E4D7B
Certificate Authority: www.example.com
Type of Certificate: server
Size of Requested Certificate(bits): 2048
Certificate Start Date: Fri Apr 30 14:14:46 2010
Certificate Expiration Date: Sat Apr 30 14:14:46 2011
Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIuYWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD
VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0G
CSqGSIb3DQEBCwUAA4IBAQBJlE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZ0M1Bhy6Q+gsE3XEnnN07AE4npjIT0eVP0nI9QIJAeBoP0uPKaCGAVBSBoM2mOwbfswI7aJoEh
+XuEoR0G0z+mltnfhgv11fT6Ms+xzd3LGZYQTworus2
-----END CERTIFICATE-----
Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (e.g. city): Sunnyvale
Organization Name (e.g. company): example
Organization Unit (e.g. section): IT
Email Address (Contact Name): web@example.com
Protocol: SSL
Hashing Function: SHA256

security certificate show-truststore

Display default truststore certificates

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command displays information about the default CA certificates that come pre-installed with Data ONTAP. Some details are displayed only when you use the command with the -instance parameter.
Parameters

{-fields <fieldname>,...}
If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use -fields '?' to display the fields to specify.

{-instance }
If you specify the -instance parameter, the command displays detailed information about all fields.

{-vserver <Vserver Name>} - Name of Vserver
Selects the Vserver whose digital certificates you want to display.

{-common-name <FQDN or Custom Common Name>} - FQDN or Custom Common Name
Selects the certificates that match this parameter value.

{-serial <text>} - Serial Number of Certificate
Selects the certificates that match this parameter value.

{-ca <text>} - Certificate Authority
Selects the certificates that match this parameter value.

{-type <type of certificate>} - Type of Certificate
Selects the certificates that match this parameter value.

{-subtype <kmip-cert>} - (DEPRECATED)-Certificate Subtype
This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

Selects the certificate subtype that matches the specified value. The valid values are as follows:

* kmip-cert - this is a Key Management Interoperability Protocol (KMIP) certificate

{-cert-name <text>} - Unique Certificate Name
This specifies the system's internal identifier for the certificate. It is unique within a Vserver.

{-size <size of requested certificate in bits>} - Size of Requested Certificate in Bits
Selects the certificates that match this parameter value.

{-start <Date>} - Certificate Start Date
Selects the certificates that match this parameter value.

{-expiration <Date>} - Certificate Expiration Date
Selects the certificates that match this parameter value.

{-public-cert <certificate>} - Public Key Certificate
Selects the certificates that match this parameter value.
[-country <text>] - Country Name
Selects the certificates that match this parameter value.

[-state <text>] - State or Province Name
Selects the certificates that match this parameter value.

[-locality <text>] - Locality Name
Selects the certificates that match this parameter value.

[-organization <text>] - Organization Name
Selects the certificates that match this parameter value.

[-unit <text>] - Organization Unit
Selects the certificates that match this parameter value.

[-email-addr <mail address>] - Contact Administrator's Email Address
Selects the certificates that match this parameter value.

[-protocol <protocol>] - Protocol
Selects the certificates that match this parameter value.

[-hash-function <hashing function>] - Hashing Function
Selects the certificates that match this parameter value.

[-self-signed {true|false}] - Self-Signed Certificate
Selects the certificates that match this parameter value.

[-is-root {true|false}] - Is Root CA Certificate?
Selects the certificates that match this parameter value.

[-authority-key-identifier <text>] - Authority Key Identifier
Selects the certificates that match this parameter value.

[-subject-key-identifier <text>] - Subject Key Identifier
Selects the certificates that match this parameter value.

### Examples

The examples below display information about the pre-installed truststore digital certificates.
cluster1::> security certificate show-truststore

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Serial Number</th>
<th>Certificate Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>4F4E4D7B</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>server-ca</td>
</tr>
</tbody>
</table>

Certificate Authority: www.example.com
Expiration Date: Thu Feb 28 16:08:28 2013

cluster1::> security certificate show-truststore -instance

Vserver: vs0
Certificate Name: www.example.com
FQDN or Custom Common Name: www.example.com
Serial Number of Certificate: 4F4E4D7B
Certificate Authority: www.example.com
Type of Certificate: server-ca
Size of Requested Certificate(bits): 2048
Certificate Start Date: Fri Apr 30 14:14:46 2010
Certificate Expiration Date: Sat Apr 30 14:14:46 2011
Public Key Certificate:

-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtssYWlu
YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQ
KEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ
8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3
DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7d

-----BEGIN CERTIFICATE-----
Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (e.g. city): Sunnyvale
Organization Name (e.g. company): example
Organization Unit (e.g. section): IT
Email Address (Contact Name): web@example.com
Protocol: SSL
Hashing Function: SHA256
security certificate show-user-installed

Display user installed certificates

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command displays information about the user installed digital certificates. Some details are displayed only when you use the command with the -instance parameter. In systems upgraded to Data ONTAP 9.4 or later, existing Data ONTAP generated certificates will also be shown as part of this command.

Parameters

{-fields <fieldname>,…}

If you specify the -fields <fieldname>, … parameter, the command output also includes the specified field or fields. You can use `-fields ?` to display the fields to specify.

{-instance }

If you specify the -instance parameter, the command displays detailed information about all fields.

-vserver <Vserver Name> - Name of Vserver

Selects the Vserver whose digital certificates you want to display.

-common-name <FQDN or Custom Common Name> - FQDN or Custom Common Name

Selects the certificates that match this parameter value.

-serial <text> - Serial Number of Certificate

Selects the certificates that match this parameter value.

-ca <text> - Certificate Authority

Selects the certificates that match this parameter value.

-type <type of certificate> - Type of Certificate

Selects the certificates that match this parameter value.

-subtype <kmip-cert> - (DEPRECATED)-Certificate Subtype

This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

Selects the certificate subtype that matches the specified value. The valid values are as follows:

* kmip-cert - this is a Key Management Interoperability Protocol (KMIP) certificate

-cert-name <text> - Unique Certificate Name

This specifies the system's internal identifier for the certificate. It is unique within a Vserver.
[-size <size of requested certificate in bits>] - Size of Requested Certificate in Bits
Selects the certificates that match this parameter value.

[-start <Date>] - Certificate Start Date
Selects the certificates that match this parameter value.

[-expiration <Date>] - Certificate Expiration Date
Selects the certificates that match this parameter value.

[-public-cert <certificate>] - Public Key Certificate
Selects the certificates that match this parameter value.

[-country <text>] - Country Name
Selects the certificates that match this parameter value.

[-state <text>] - State or Province Name
Selects the certificates that match this parameter value.

[-locality <text>] - Locality Name
Selects the certificates that match this parameter value.

[-organization <text>] - Organization Name
Selects the certificates that match this parameter value.

[-unit <text>] - Organization Unit
Selects the certificates that match this parameter value.

[-email-addr <mail address>] - Contact Administrator's Email Address
Selects the certificates that match this parameter value.

[-protocol <protocol>] - Protocol
Selects the certificates that match this parameter value.

[-hash-function <hashing function>] - Hashing Function
Selects the certificates that match this parameter value.

[-self-signed {true|false}] - Self-Signed Certificate
Selects the certificates that match this parameter value.

[-is-root {true|false}] - Is Root CA Certificate?
Selects the certificates that match this parameter value.

[-authority-key-identifier <text>] - Authority Key Identifier
Selects the certificates that match this parameter value.

[-subject-key-identifier <text>] - Subject Key Identifier
Selects the certificates that match this parameter value.
Examples
The examples below display information about user installed digital certificates.

```
cluster1::> security certificate show-user-installed

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Serial Number</th>
<th>Certificate Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>4F4E4D7B</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificate Authority: <a href="http://www.example.com">www.example.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expiration Date: Thu Feb 28 16:08:28 2013</td>
<td></td>
</tr>
</tbody>
</table>
```
cluster1::> security certificate show-user-installed -instance
    Vserver: vs0
    Certificate Name: www.example.com
    FQDN or Custom Common Name: www.example.com
    Serial Number of Certificate: 4F4E4D7B
    Certificate Authority: www.example.com
    Type of Certificate: server
    Size of Requested Certificate(bits): 2048
    Certificate Start Date: Fri Apr 30 14:14:46 2010
    Certificate Expiration Date: Sat Apr 30 14:14:46 2011
    Public Key Certificate: -----BEGIN CERTIFICATE-----
    MIIDfTCCAmWgAwIBAwIBAgkqkvhkiG9w0BAQsfADBgMRQwEgYDVQQDEwtsYWIu
    YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD
    VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0
    BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMAQG
    CsqGSiib3DQEJARYAMA0GCSqGSIb3DQEBwIEAQRoYwEHYClUyYuupQRvSLpKs/ej
    +gsE3XEtudIlp+YDCc16sKvQO0qjv3U8h8cNjyeuS8z79B867jg46Qhjnhn6Q
    +XuEoNroG0z+mltnfhgl1fT6Ms+xzd3LGZYQTworus2
    -----BEGIN CERTIFICATE-----
    Country Name (2 letter code): US
    State or Province Name (full name): California
    Locality Name (e.g. city): Sunnyvale
    Organization Name (e.g. company): example
    Organization Unit (e.g. section): IT
    Email Address (Contact Name): web@example.com
    Protocol: SSL
    Hashing Function: SHA256

security certificate show

Display Installed Digital Certificates

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command displays information about the installed digital certificates. Some details are displayed only when you use the command with the -instance parameter.
Parameters

{-fields <fieldname>,…]
If you specify the -fields <fieldname>, … parameter, the command output also includes the specified field or fields. You can use ‘-fields ?’ to display the fields to specify.

|[-instance ]}
If you specify the -instance parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Name of Vserver
Selects the Vserver whose digital certificates you want to display.

[-common-name <FQDN or Custom Common Name>] - FQDN or Custom Common Name
Selects the certificates that match this parameter value.

[-serial <text>] - Serial Number of Certificate
Selects the certificates that match this parameter value.

[-ca <text>] - Certificate Authority
Selects the certificates that match this parameter value.

[-type <type of certificate>] - Type of Certificate
Selects the certificates that match this parameter value.

[-subtype <kmip-cert>] - (DEPRECATED)-Certificate Subtype
This parameter has been deprecated in ONTAP 9.6 and may be removed in a future release of Data ONTAP.

Selects the certificate subtype that matches the specified value. The valid values are as follows:

* kmip-cert - this is a Key Management Interoperability Protocol (KMIP) certificate

[-cert-name <text>] - Unique Certificate Name
This specifies the system's internal identifier for the certificate. It is unique within a Vserver.

[-size <size of requested certificate in bits>] - Size of Requested Certificate in Bits
Selects the certificates that match this parameter value.

[-start <Date>] - Certificate Start Date
Selects the certificates that match this parameter value.

[-expiration <Date>] - Certificate Expiration Date
Selects the certificates that match this parameter value.

[-public-cert <certificate>] - Public Key Certificate
Selects the certificates that match this parameter value.
[country <text>] - Country Name
Selects the certificates that match this parameter value.

[state <text>] - State or Province Name
Selects the certificates that match this parameter value.

[locality <text>] - Locality Name
Selects the certificates that match this parameter value.

[organization <text>] - Organization Name
Selects the certificates that match this parameter value.

[unit <text>] - Organization Unit
Selects the certificates that match this parameter value.

[mailto-addr <mail address>] - Contact Administrator’s Email Address
Selects the certificates that match this parameter value.

[protocol <protocol>] - Protocol
Selects the certificates that match this parameter value.

[hash-function <hashing function>] - Hashing Function
Selects the certificates that match this parameter value.

[self-signed {true|false}] - Self-Signed Certificate
Selects the certificates that match this parameter value.

[is-root {true|false}] - Is Root CA Certificate?
Selects the certificates that match this parameter value.

[authority-key-identifier <text>] - Authority Key Identifier
Selects the certificates that match this parameter value.

[subject-key-identifier <text>] - Subject Key Identifier
Selects the certificates that match this parameter value.

Examples
The examples below display information about digital certificates.
cluster1::> security certificate show

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Serial Number</th>
<th>Certificate Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>4F4E4D7B</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Certificate Authority:  www.example.com
Expiration Date: Thu Feb 28 16:08:28 2013
cluster1::> security certificate show -instance

Vserver: vs0
Certificate Name: www.example.com
FQDN or Custom Common Name: www.example.com
Serial Number of Certificate: 4F4E4D7B
Certificate Authority: www.example.com
Type of Certificate: server
Size of Requested Certificate(bits): 2048
Certificate Start Date: Fri Apr 30 14:14:46 2010
Certificate Expiration Date: Sat Apr 30 14:14:46 2011
Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIuYWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0
-----END CERTIFICATE-----

Country Name (2 letter code): US
State or Province Name (full name): California
Locality Name (e.g. city): Sunnyvale
Organization Name (e.g. company): example
Organization Unit (e.g. section): IT
Email Address (Contact Name): web@example.com
Protocol: SSL
Hashing Function: SHA256

security certificate sign

Sign a Digital Certificate using Self-Signed Root CA

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command signs a digital certificate signing request and generates a certificate using a Self-Signed Root CA certificate in either PEM or PKCS12 format. You can use the security certificate generate-csr command to generate a digital certificate signing request.
Parameters

-vserver <Vserver Name> - Name of Vserver
This specifies the name of the Vserver on which the signed certificate will exist.

-ca <text> - Certificate Authority to Sign
This specifies the name of the Certificate Authority that will sign the certificate.

-ca-serial <text> - Serial Number of CA Certificate
This specifies the serial number of the Certificate Authority that will sign the certificate.

[--expire-days <integer>] - Number of Days until Expiration
This specifies the number of days until the signed certificate expires. The default value is 365 days.
Possible values are between 1 and 3652.

[--format <certificate format>] - Certificate Format
This specifies the format of signed certificate. The default value is PEM. Possible values include PEM and PKCS12.

[--destination {(ftp|http|https)://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Where to Send File
This specifies the destination to upload the signed certificate. This option can only be used when the format is PKCS12.

[--hash-function <hashing function>] - Hashing Function
This specifies the cryptographic hashing function for the self-signed certificate. The default value is SHA256. Possible values include SHA224, SHA256, SHA384, and SHA512.

Examples

This example signs a digital certificate for a Vserver named vs0 using a Certificate Authority certificate that has a ca of www.ca.com and a ca-serial of 4F4EB629 in PEM format using the SHA256 hashing function.
cluster1::> security certificate sign -vserver vs0 -ca www.ca.com -ca-serial 4F4EB629 -expire-days 36 -format PEM -hash-function SHA256

Please enter Certificate Signing Request(CSR): Press <Enter> when done

-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEGYDVQQDEwtleGFtcGxlGx1LmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVAgcGA1UEBxMAMQkwBwYDVQQDEwAxDzANBgkqhkiG9w0BCQEWABDCma0GCSqG
SIb3DQEBCwUA0EAMBgkqhkiG9w0DGcSghcbGkqhkjiCBxQIBAAYDAlgEBeryaszSb0b
2nnsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUA0E6EagLfsos5+4g+eiIKKTUPQO
UqOUEoKuvxhOVPC2w7b/fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ40fnKw==
-----END CERTIFICATE REQUEST-----

Signed Certificate:

-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIET1oskDANBgkqhkiG9w0BAQSFAFBDdMREwDwYDVQQDEwh2
czAuY2VydDElMAkGA1UEBhMCVVMxCTAHBgNVAgcGA1UEBxMAMQkwBwYDVQQDEwAxDzANBgkqhkiG9w0BCQEWABDCma0GCSqG
SIb3DQEBCwUA0EAMBgkqhkiG9w0DGcSghcbGkqhkjiCBxQIBAAYDAlgEBeryaszSb0b
2nnsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUA0E6EagLfsos5+4g+eiIKKTUPQO
UqOUEoKuvxhOVPC2w7b/fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ40fnKw==
-----END CERTIFICATE-----

This example signs and exports a digital certificate to destination ftp://10.98.1.1//u/sam/sign.pfx for a Vserver named vs0 using a Certificate Authority certificate that expires in 36 days and has a ca value of www.ca.com and a ca-serial value of 4F4EB629 in PKCS12 format by the SHA384 hashing function.
cluster1::> security certificate sign -vserver vs0 -ca www.ca.com -ca
-serial 4F4EB629
-expire-days 36 -format PKCS12 -destination
ftp://10.98.1.1//u/sam/sign.pfx -hash-function SHA384

Please enter Certificate Signing Request(CSR): Press <Enter> when done

-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBAgQjM5q5zSxOczji26qRy7Av/7yP8xMCdR1p+i89pFQo03e3A4
-----END CERTIFICATE REQUEST-----

Signed Certificate: 

-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIET1ot8jANBgkqhkiG9w0BAQsFADBdMREwDwYDVQQDEwzhc
2cAzYVydDELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDV
QQKEwAxCTAHBgNVBAcTADEJMAcGA1UEChMAMQkwBwYDVQQLEwAxCTAHBgNVBAMTADE
MAMTaGA1UEAxMLZXhhbXBsZS5jb20xCzAJBgNVBAYTAlVTMQkwBwYDVQQHEwAxCTA
HMA0GCSqGSIb3DQEJARYAMB4XDTEyMDMwOTEzMDAwNzowYDEUMBIGA1UEAxMEb3J0

-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done

-----BEGIN RSA PRIVATE KEY-----
MIIBoIBAAJBApXFanNoJApT1nzSxOcxJixImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsbl3wfEvQnHVNCi2ninsJ8CAwEAAcQJAw+boW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJFhYSb2O2B8eijfJvRWdTOBeav99M7cEzgPv+p5kaZTM
Cq1hApsp+j1hrUXRj979L1IJY0sNez397i77vFXWQS8x/ehAiEA+oDbOooDWLVu

-----END RSA PRIVATE KEY-----

Please enter a password for pkcs12 file:

Enter User for Destination URI: sam
Enter Password:

Related Links

• security certificate generate-csr
security certificate ca-issued revoke

Revoke a Digital Certificate

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command revokes a digital certificate signed by a Self-Signed Root CA.

Parameters

- **-vserver <Vserver Name>** - Name of Vserver
  
  This specifies the name of the Vserver on which the certificate is stored.

- **-serial <text>** - Serial Number of Certificate
  
  This specifies the serial number of the certificate.

- **-ca <text>** - Certificate Authority
  
  This specifies the name of the Certificate Authority whose certificate will be revoked.

- **-ca-serial <text>** - Serial Number of CA Certificate
  
  This specifies the serial number of Certificate Authority.

- **[-common-name <FQDN or Custom Common Name>]** - FQDN or Custom Common Name
  
  This specifies a fully qualified domain name (FQDN) or custom common name or the name of a person. This field is optional if ca-serial is specified.

Examples

This example revokes a signed digital certificate for a Vserver named vs0 with serial as 4F5A2DF2 for a Certificate Authority certificate that has a ca of **www.ca.com** and a ca-serial of 4F4EB629.

```
cluster1::> security certificate ca-issued revoke -vserver vs0 -serial 4F5A2DF2 -ca www.ca.com -ca-serial 4F4EB629
```

security certificate ca-issued show

Display CA-Issued Digital Certificates

Availability: This command is available to cluster and Vserver administrators at the admin privilege level.

Description

This command displays the following information about the digital certificates issued by the self-signed root-ca:

- Vserver
- Serial number of certificate
• FQDN or custom common name or the name of a person
• Serial number of CA certificate
• Status (active, revoked)
• Certificate Authority
• Expiration date
• Revocation date

To display more details, run the command with the `instance` parameter. This will add the following information:

• Country name
• State or province name
• Locality name
• Organization name
• Organization unit
• Contact administrator’s email address

Parameters

```
[-fields <fieldname>,...]
If you specify the -fields <fieldname>, ... parameter, the command output also includes the specified field or fields. You can use `-fields ?` to display the fields to specify.
```

```
[-instance ]
If you specify the -instance parameter, the command displays detailed information about all fields.
```

```
[-vserver <Vserver Name>] - Name of Vserver
Selects the certificates that match this parameter value.
```

```
[-serial <text>] - Serial Number of Certificate
Selects the certificates that match this parameter value.
```

```
[-ca <text>] - Certificate Authority
Selects the certificates that match this parameter value.
```

```
[-ca-serial <text>] - Serial Number of CA Certificate
Selects the certificates that match this parameter value.
```

```
[-common-name <FQDN or Custom Common Name>] - FQDN or Custom Common Name
Selects the certificates that match this parameter value.
```

```
[-status <status of certificate>] - Status of Certificate
Selects the certificates that match this parameter value. Possible values include active and revoked.
```

```
[-expiration <Date>] - Certificate Expiration Date
Selects the certificates that match this parameter value.
```
[-revocation <Date>] - Certificate Revocation Date
Selects the certificates that match this parameter value.

[-country <text>] - Country Name (2 letter code)
Selects the certificates that match this parameter value.

[-state <text>] - State or Province Name (full name)
Selects the certificates that match this parameter value.

[-locality <text>] - Locality Name (e.g. city)
Selects the certificates that match this parameter value.

[-organization <text>] - Organization Name (e.g. company)
Selects the certificates that match this parameter value.

[-unit <text>] - Organization Unit (e.g. section)
Selects the certificates that match this parameter value.

[-email-addr <mail address>] - Email Address (Contact Name)
Selects the certificates that match this parameter value.

Examples
The examples below display information about CA issued digital certificates.

```
cluster1::> security certificate ca-issued show
Serial Number of
Vserver  Serial Number  Common Name           CA's Certificate
Status
---------- --------------- --------------------------- -------------
--------
vs0       4F5A2C90      example.com             4F4EB629
active
          Certificate Authority: vs0.cert
          Expiration Date: Sat Apr 14 16:15:13 2012
          Revocation Date: -

vs0       4F5A2DF2      example.com             4F4EB629
revoked
          Certificate Authority: vs0.cert
          Expiration Date: Sat Apr 14 16:21:06 2012
          Revocation Date: Fri Mar 09 17:08:30 2012

2 entries were displayed.
```
cluster1::> security certificate ca-issued show -instance
Vserver: vs0
  Serial Number of Certificate: 4F5A2C90
  Certificate Authority: vs0.cert
  Serial Number of CA Certificate: 4F4EB629
  FQDN or Custom Common Name: example.com
  Status of Certificate: active
  Certificate Expiration Date: Sat Apr 14 16:15:13 2012
  Certificate Revocation Date: -
  Country Name (2 letter code): US
  State or Province Name (full name): California
  Locality Name (e.g. city): Sunnyvale
  Organization Name (e.g. company): example
  Organization Unit (e.g. section): IT
  Email Address (Contact Name): web@example.com

security certificate config modify

Modify the certificate management configurations

Availability: This command is available to cluster administrators at the advanced privilege level.

Description
This command modifies the certificate management configuration information for the cluster.

Parameters

[-min-security-strength <bits of security strength>] - Minimum Security Strength
Use this parameter to modify the allowed minimum security strength for certificates. The security bits mapping to RSA and ECDSA key length are as follows:

<table>
<thead>
<tr>
<th>Security Bits</th>
<th>Asymmetric Key Length</th>
<th>Elliptic Curve Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>2048</td>
<td>224</td>
</tr>
<tr>
<td>128</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>192</td>
<td>4096</td>
<td>384</td>
</tr>
</tbody>
</table>

FIPS supported values are restricted to 112 and 128.

+ NOTE: This does not affect root CA certificates.
[-expiration-warn-threshold <integer>] - Minimum Days to EMS for Expiring Certificates

Use this parameter to modify the number of days prior to certificate expiration the system sends a warning EMS event.

Examples

The following example modifies the minimum security strength allowed for certificates.

```
cluster-1:>> security certificate config modify -min-security-strength 192
```

security certificate config show

Displays the certificate management configurations

**Availability:** This command is available to `cluster` administrators at the `admin` privilege level.

**Description**

This command displays the certificate management configuration information for the cluster.

"min-security-strength" - If you specify this parameter, the command displays the minimum allowed security strength for certificates.

"expiration-warn-threshold" - If you specify this parameter, the command displays the minimum number of days before expiration date configured for event management system (EMS) notification of expiring certificates.

Examples

The following example lists minimum security strength certificate management configuration.

```
cluster-1:>> security certificate config show -fields min-security-strength
Minimum Security Strength
--------------------------
112
```

security certificate truststore check

Initiate a TLS connection and identify the root CA certificate

**Availability:** This command is available to `cluster` and `Vserver` administrators at the `advanced` privilege level.
Description

This command allows the user to check if the node can use the installed set of CA certificates to establish a secure connection with the specified server. If the connection attempt fails, the system reports which expected certificates are missing. If the attempt succeeds, the system displays details of the certificates used.

Parameters

-vserver <Vserver Name> - Vserver Name (privilege: advanced)
Use this parameter to specify the Vserver that needs the connectivity check.

-server <Hostname and Port> - Server Name (privilege: advanced)
Use this parameter to specify the server to establish a connection with and look up the required CA certificate.

Examples

The following example demonstrates a missing CA certificate:

```
cluster1::*> security certificate truststore check -vserver cluster1
-s-server example.com:443

Error: command failed: Missing certificate with subject name: "CN = ExampleRoot, C = US"
```

The following example demonstrates the required certificate being present:

```
cluster1::*> security certificate truststore check -server example.com:443

CA certificate with cert-name "ExampleRoot" is already installed in the truststore. Use "security certificate show -cert-name ExampleRoot" to see the details of the CA certificate.
```

security certificate truststore clear

Clear the default root certificates from truststore

Availability: This command is available to cluster administrators at the advanced privilege level.

Description

The security certificate truststore clear command deletes the pre-installed certificates of the type 'server-ca'. If you delete these certificates, some of the applications performing SSL communication can fail.
Examples

The following example removes the default certificate bundle:

```
cluster1::> security certificate truststore clear
```

security certificate truststore load

Load the default root certificates to truststore

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

**Description**

The `security certificate truststore load` command installs default root certificates in the certificate table of type 'server-ca'. These are the certificates required to validate any incoming server certificate during the SSL handshake process. Note: This command only installs PEM formatted certificates.

**Parameters**

```
{ [-path <text>] - File to load PEM certificates from (privilege: advanced)
   This specifies the path to the PEM formatted certificate bundle. This optional parameter can have an empty value (the default).

| [-uri <text>] - URL to download PEM certificates from (privilege: advanced) }
   This specifies the URL from which to download the PEM formatted certificate bundle.

[-ontap-version <ontap_version>] - Certificates from specific ONTAP version (privilege: advanced)
   This specifies the ONTAP version in which the certificates were introduced. Only those certificates will be loaded. This optional parameter can have an empty value (the default) which indicates that no filtering on version is done.
```

**Examples**

The following example installs the default certificate bundle:

```
cluster1::> security certificate truststore load
```