security certificate commands

ONTAP 9.15.1 commands

NetApp
May 17, 2024

Table of Contents

security certificate commands

security certificate azure-install

Install a Digital Certificate from Azure Key Vault

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

Description

The `security certificate azure-install` command downloads and installs digital security certificates signed by a certificate authority (CA) and the public key certificate of the root CA stored on Azure Key Vault (AKV). 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.

`-cert-name <text>` - 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.

`-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
- *`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

`-key-vault-uri {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}` - Deployed Azure Key Vault DNS Name

The DNS name of the deployed AKV.

`-client-id <text>` - Application (Client) ID of Deployed Azure Application

The ID of the client.

`-tenant-id <text>` - Directory (Tenant) ID of Deployed Azure Application

The ID of the tenant.

`-authentication-method <AKV Authentication Method>` - AKV Authentication Method

Use this parameter to specify the authentication method.

[-oauth-host <text>] - Open Authorization Host Name
The hostname of the OAuth server.

[-proxy-type {http|https}] - Proxy Type
Proxy Type.

[-proxy-host <text>] - Proxy Host
Proxy hostname.

[-proxy-port <integer>] - Proxy Port
Proxy port.

[-proxy-username <text>] - Proxy Username
Proxy username.

[-proxy-password <text>] - Proxy Password
Proxy password.

[-timeout <integer>] - AKV Connection Timeout in Seconds
AKV Connection Timeout in Seconds.

[-verify-host {true|false}] - Verify the identity of the AKV host
Set to true to verify the identity of the AKV host name.

Examples

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

```
cluster-1::> security certificate azure-install -vserver vs0 -type client
-client-id client1 -tenant-id tenant1 -key-vault-uri
https://samplevault.vault.azure.net -cert-name certname

Enter the {0} for Azure Key Vault:
```

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.

```
cluster1::> security certificate delete -vserver vs0 -common-name
www.example.com -ca www.example.com -type root-ca -serial 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:

```
            Size      RSA Key Length       Elliptic Curve Key Length
            112       2048                 224
            128       3072                 256
            192       4096                 384
```

```
Note: FIPS supported values are restricted to 112 and 128. For ECDSA,
TLSv1.3 requires key length of 256 or greater.
```

[-algorithm <Asymmetric key generation algorithm>] - Asymmetric Encryption Algorithm

Use this parameter to specify the asymmetric encryption algoithm 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
- critical

[-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
- critical

[-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.

```
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-----
MIIEWDCCAsACAQAwgYgxGDAWBgNVBAMTD3d3dy5leGFtcGxlLmNvbTELMAkGA1UE
BhMCVVMxCzAJBgNVBAgTAk5DMQ8wDQYDVQQHEwZEdXJoYW0xCzAJBgNVBAoTAklU
MRQwEgYDVQQLEwtFbmdpbmVlcmluZzEeMBwGCSqGSIb3DQEJARYPd2ViQGV4YW1w
bGUuY29tMIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAuo86Jg/szhws
ykYiEXvRaf/j2jJArJMoZby9Z/yINsowe30Xbn5wnfvwiwICUCPwD1e3jhK3TrWH
rNRn/+MqE+jQA7yAdufYxD537cDcT46ihkajISe0Ei93yf6IKmvUAvmJvQ3R7Z4E
QCOWHj56yQ+LXj36bYdwa74S8u8lpCs3Ywx8fgrh/v6H0rnlKDQSQuFR35u7ZZym
tRA7EJMY62f9ALgcFNhQPuP6pjc8aP7Tv7BKXAninryDDcoMdW8UczfTPgzCDh5z
S++eNP3s/7cGfRSQ8aXnDTVQLYpusrdDgVwZXXgu+ZPoZuCf2AYBT+/rdq3VkgWu
QM+mGRMB53O0ff4QOi+SVcXSWXq32wzciv1KsW/iB9h2T+kVd/8Z7ESeYLqFxhY+
0nwacskMRGxOuTLgx+XH+/EntjrI4rjF9/ShYCIcy8vqp1OxFaPClu96ebnbiEOu
y6RvCJ2egcM6OeRbHWB5fIJ0ZZ3crdjz/d1z4ktBuG7E4cUYkEvvAgMBAAGggYkw
gYYGCSqGSIb3DQEJDjF5MHcwRgYDVR0RAQH/BDwwOoETZXhhbXBsZUBleGFtcGxl
LmNvbYIQc2hvcC5leGFtcGxlLmNvbYIRc3RvcmUuZXhhbXBsZS5jb20wDgYDVR0P
AQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATANBgkqhkiG
9w0BAQsFAAOCAYEAh0kOsRy5cCTnFRIWBhBrFFvQhpZIlsoeelNW6JlkE0/ULcAj
JevBx8UibY48D2Wn0nEGle9T3ZeDlg+n66xr/OUfsrENm5ORy5Ndvubkkz0t4KF5
Z2SnwPVIcX2b6ID2xhFAny2S58Adwo7uTpLytidqFj026/KcuyVZUEF9HuJcQGE8
+LMfliCkm6rI2h1ncy2sV6vtDo9GlVscTYLghisHp1aTXVPrr6Q+1OM8lTot8i71
DmZ7kRyxCDlu20XxxV+p2cm4QQVHXbw0XrKAOL2jCBBiYOSWM/BvwWIliVGD6NLg
WK7ZpyHSFjDH0pUlqJCIs079W6JDhiYvtB2xizqmg8oyABUESMUckHGeymr92mcO
```

```
JbSyeTE66Pek+Gwia6ZMG7jcznfSr31+7dShLix9kjGsKUffHTiZVySaYjny/+Aq
Seg3Fpusq25ki9D/NMnbifXraL+LbX/WNLS3nA79rp3+VcOoGBponT4i1fsxn+Bv
5RTT3nhT8BlcTe1d
-----END CERTIFICATE REQUEST-----

Private Key :
-----BEGIN PRIVATE KEY-----
MIIG/AIBADANBgkqhkiG9w0BAQEFAASCBuYwggbiAgEAAoIBgQC6jzomD+zOHCzK
RiIRe9Fp/+PaMkCskyhlvL1n/Ig2yjB7fRdufnCd+/CLAgJQI/APV7eOErdOtYes
1Gf/4yoT6NADvIB259jEPnftwNxPjqKGRqMhJ7QSL3fJ/ogqa9QC+Ym9DdHtngRA
I5YePnrJD4tePfpth3BrvhLy7yWkKzdjDHx+CuH+/ofSueUoNBJC4VHfm7tlnKa1
EDsQkxjrZ/0AuBwU2FA+4/qmNzxo/tO/sEpcCeKevIMNygx1bxRzN9M+DMIOHnNL
7540/ez/twZ9FJDxpecNNVAtim6yt0OBXBldeC75k+hm4J/YBgFP7+t2rdWSBa5A
z6YZEwHnc7R9/hA6L5JVxdJZerfbDNyK/Uqxb+IH2HZP6RV3/xnsRJ5guoXGFj7S
fBpyyQxEbE65MuDH5cf78Se2OsjiuMX39KFgIhzLy+qnU7EVo8KW73p5uduIQ67L
pG8InZ6Bwzo55FsdYHl8gnRlndyt2PP93XPiS0G4bsThxRiQS+8CAwEAAQKCAYBW
fqtWFFIVaWi2y3dmJcL840AP3PaxTHURXkVund3FkU6TIncnqoWqKbHnsSHDaDYX
1vJqc3D7lBx4W+5v7DGJE4rGALKK7olIyzGtUJqUZCwkF0Hw0EijmdBvHYyiJmYg
jvN2bJ7lDTspRZaHJS6mY4eZRSEDgST1PyXn7krEZ6kBSju58G/BWt88KyX80s+Y
pIDiLIDg5pVAI2tPDvQhyI+7sqCKZZQm5GpEgB2JDIS+PgzryUWBlSMp1ICcPcgx
rarFZQi1Ne7qrp6FfKvPAO5XLyI0xhgm8fCMJUpxmEb80XY4FeRDzB42a0Z/YL0P
HhpWAI4ZRsDyDd5S7jwLZQ3Hl9WsKvj2/FRU6hWTP+maH/Vel35iLkygfZWUAjNY
F6B0SoBBd9bVeKDODXrD/CwVbuaKZGMaVOenZbczmFUVSi4HZGyqVRxX6WIxVoD0
MZXwWUoWZ32C6II3vp/ReAsouhCnKDKhqfrvH58xF82FTMMXBZ/kDy7k5IySylkC
gcEA4tpiV1eKzC/ft0sPUNmZB/snHfXC+xohzTygCg4L1Rf8zjDnUT/o9D8SRe1/
crkG7ZcjKvIdPz0tatyjyNMsZ9TDISiAJQJ8Et1+jBP0uy2qG+ab+Ub761BR5TX0
O78UcmtEyxaaDZsESWj+qYerG4E7zGZiTscTe2Jma5fPlS1ekyfNzk1GBtya9bIM
r991o/PahSmCz5iPxf4avYM/vQm2p+wIk+o6ZhJIAUlRFrCv8y9lYivQjw+tZA+G
bdE7AoHBANKHg0Jb5BLJmN/5/PLkkELhaZG+UNUngtm46dm/84+sqtdTcUHpqdHv
M/skRYDVERmI50QZ2HmzVC8J+zzs9r01VNNA+Tzcoi3eB3FPdDYPTDtLSzRfsC82
kix8d2uVs+rfmvKwT0XucNvMQjUyYDII7IJln1iIJp2XQZaNleqgyi65kni+6FrQ
EJ9gVD4PtCkX7rKo8csMITe6n+HZIzFpOY6BX0HU/4VGa+RQHGfGIdfKDOJ5AtyG
RPYVvZ1E3QKBwE520sT7FpsBhBPV9no0iWXlTOZj9wj7RO3EJmbT7OvL3DlFWP0V
afHxTtS5DPgVX3wWZqeYDt2sv2TS5CO2Rwmy4bs6Uvh6H4g27GpvDJshdFEqNpDG
KKR/p5PsUYnI0b2xtJ26N5a1I4pwsoTY1CozTQep8h7lZKusoVhdrgMfKjMj9V+C
AtKkw0RwTUsXs4z973tXnFNJpZEKDx21o/oyvebfESh4P7LGZ/lp7o42luU6Y4rN
NNoGxiZx6EFbuQKBwGbMltJTTmXCHKzZQ6NS6gJOUR9CX/QFLAamHUIfUY3JUU59
RyNZNnv1IluyVWHYKFZgnBSLzkF2yFeDtzMDvmObZAUXh9wpG+Prs5SnqGYxSBb3
6Av14XDcY7nnOOTGn6jDcMSqRLsv99nLvlR9ea1U4C+38XvoV3rB/dvG3PpJcxAn
uxbMmWamjEdWYSxAvMcIEZ0Zk5+DF8E/loxQW7fn2pv0HhBmMjLgtRQx7fzaKXJW
Db6UOkp2IbxL11+w3QKBwDloDgwB7ukGyFHf3RKy3YX0en1WGBesXONf1m2fjwOU
nojccfaGwAUdb6m60JuZFhJ3qZ4ecoloY4GxIKV5krvBg1buow/aqDDkKmVVYNO6
FUuXp+BbTBSxjfftSaog7y5Db5aecLXU5FLE+sVlrhp17s9h8Ur+O04SytSVh9JS
SkzHYv+4GybZqmOeF2U+whib8JXD2bJkSfNI1dZZhKVqoTUQfEAE3VFY0EHkVQwk
rLHmjspsUjKc4BKfVRGWJg==
-----END PRIVATE KEY-----
```

```
Note: Keep a copy of your certificate request and private key for future
reference.
```

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
- *`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
Enter certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----
Enter private key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

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

Enter intermediate certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Enter intermediate certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----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.

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

Enter certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNhIilsXjOKUgodJfTNcJVDANBgkqhkiG9w0BAQUFADCB
zjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UE
CxMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEhMB8GA1UEAxMYVGhh
d3RlIFByZW1pdW0gU2VydmVyIENBMSgwJgYJKoZIhvcNAQkBFhlwcmVtaXVtLXNl
cnZlckB0aGF3dGUuY29tMB4XDTk2MDgwMTAwMDAwMFoXDTIxMDEwMTIzNTk1OVow
gc4xCzAJBgNVBAYTAlpBMRUwEwYDVQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcT
-----END CERTIFICATE-----
You should keep a copy of the CA-signed digital certificate for future
reference.
```

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

Enter certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNhIilsXjOKUgodJfTNcJVDANBgkqhkiG9w0BAQUFADCB
zjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UE
CxMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEhMB8GA1UEAxMYVGhh
d3RlIFByZW1pdW0gU2VydmVyIENBMSgwJgYJKoZIhvcNAQkBFhlwcmVtaXVtLXNl
cnZlckB0aGF3dGUuY29tMB4XDTk2MDgwMTAwMDAwMFoXDTIxMDEwMTIzNTk1OVow
gc4xCzAJBgNVBAYTAlpBMRUwEwYDVQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcT
-----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.

```
cluster1::> security certificate print -vserver vs0 -cert-name
AAACertificateServices
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:
                    00:a7:c6:c4:a5:29:a4:2c:ef:e5:18:c5:b0:50:a3:
                    6f:51:3b:9f:0a:5a:c9:c2:48:38:0a:c2:1c:a0:18:
                    7f:91:b5:87:b9:40:3f:dd:1d:68:1f:08:83:d5:2d:
                    1e:88:a0:f8:8f:56:8f:6d:99:02:92:90:16:d5:5f:
                    08:6c:89:d7:e1:ac:bc:20:c2:b1:e0:83:51:8a:69:
                    4d:00:96:5a:6f:2f:c0:44:7e:a3:0e:e4:91:cd:58:
                    ee:dc:fb:c7:1e:45:47:dd:27:b9:08:01:9f:a6:21:
                    1d:f5:41:2d:2f:4c:fd:28:ad:e0:8a:ad:22:b4:56:
                    65:8e:86:54:8f:93:43:29:de:39:46:78:a3:30:23:
                    ba:cd:f0:7d:13:57:c0:5d:d2:83:6b:48:4c:c4:ab:
                    9f:80:5a:5b:3a:bd:c9:a7:22:3f:80:27:33:5b:0e:
                    b7:8a:0c:5d:07:37:08:cb:6c:d2:7a:47:22:44:35:
                    c5:cc:cc:2e:8e:dd:2a:ed:b7:7d:66:0d:5f:61:51:
                    22:55:1b:e3:46:e3:e3:3d:d0:35:62:9a:db:af:14:
                    c8:5b:a1:cc:89:1b:e1:30:26:fc:a0:9b:1f:81:a7:
                    47:1f:04:eb:a3:39:92:06:9f:99:d3:bf:d3:ea:4f:
                    50:9c:19:fe:96:87:1e:3c:65:f6:a3:18:24:83:86:
                    10:e7:54:3e:a8:3a:76:24:4f:81:21:c5:e3:0f:02:
                    f8:93:94:47:20:bb:fe:d4:0e:d3:68:b9:dd:c4:7a:
                    84:82:e3:53:54:79:dd:db:9c:d2:f2:07:9b:2e:b6:
                    bc:3e:ed:85:6d:ef:25:11:f2:97:1a:42:61:f7:4a:
                    97:e8:8b:b1:10:07:fa:65:81:b2:a2:39:cf:f7:3c:
                    ff:18:fb:c6:f1:5a:8b:59:e2:02:ac:7b:92:d0:4e:
                    14:4f:59:45:f6:0c:5e:28:5f:b0:e8:3f:45:cf:cf:
                    af:9b:6f:fb:84:d3:77:5a:95:6f:ac:94:84:9e:ee:
                    bc:c0:4a:8f:4a:93:f8:44:21:e2:31:45:61:50:4e:
                    10:d8:e3:35:7c:4c:19:b4:de:05:bf:a3:06:9f:c8:
                    b5:cd:e4:1f:d7:17:06:0d:7a:95:74:55:0d:68:1a:
                    fc:10:1b:62:64:9d:6d:e0:95:a0:c3:94:07:57:0d:
                    14:e6:bd:05:fb:b8:9f:e6:df:8b:e2:c6:e7:7e:96:
                    f6:53:c5:80:34:50:28:58:f0:12:50:71:17:30:ba:
                    e6:78:63:bc:f4:b2:ad:9b:2b:b2:fe:e1:39:8c:5e:
```

```
                    ba:0b:20:94:de:7b:83:b8:ff:e3:56:8d:b7:11:e9:
                    3b:8c:f2:b1:c1:5d:9d:a4:0b:4c:2b:d9:b2:18:f5:
                    b5:9f:4b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Authority Key Identifier:

keyid:52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0
X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         0b:7b:72:87:c0:60:a6:49:4c:88:58:e6:1d:88:f7:14:64:48:
         a6:d8:58:0a:0e:4f:13:35:df:35:1d:d4:ed:06:31:c8:81:3e:
         6a:d5:dd:3b:1a:32:ee:90:3d:11:d2:2e:f4:8e:c3:63:2e:23:
         66:b0:67:be:6f:b6:c0:13:39:60:aa:a2:34:25:93:75:52:de:
         a7:9d:ad:0e:87:89:52:71:6a:16:3c:19:1d:83:f8:9a:29:65:
         be:f4:3f:9a:d9:f0:f3:5a:87:21:71:80:4d:cb:e0:38:9b:3f:
         bb:fa:e0:30:4d:cf:86:d3:65:10:19:18:d1:97:02:b1:2b:72:
         42:68:ac:a0:bd:4e:5a:da:18:bf:6b:98:81:d0:fd:9a:be:5e:
         15:48:cd:11:15:b9:c0:29:5c:b4:e8:88:f7:3e:36:ae:b7:62:
         fd:1e:62:de:70:78:10:1c:48:5b:da:bc:a4:38:ba:67:ed:55:
         3e:5e:57:df:d4:03:40:4c:81:a4:d2:4f:63:a7:09:42:09:14:
         fc:00:a9:c2:80:73:4f:2e:c0:40:d9:11:7b:48:ea:7a:02:c0:
         d3:eb:28:01:26:58:74:c1:c0:73:22:6d:93:95:fd:39:7d:bb:
         2a:e3:f6:82:e3:2c:97:5f:4e:1f:91:94:fa:fe:2c:a3:d8:76:
         1a:b8:4d:b2:38:4f:9b:fa:1d:48:60:79:26:e2:f3:fd:a9:d0:
         9a:e8:70:8f:49:7a:d6:e5:bd:0a:0e:db:2d:f3:8d:bf:eb:e3:
         a4:7d:cb:c7:95:71:e8:da:a3:7c:c5:c2:f8:74:92:04:1b:86:
         ac:a4:22:53:40:b6:ac:fe:4c:76:cf:fb:94:32:c0:35:9f:76:
         3f:6e:e5:90:6e:a0:a6:26:a2:b8:2c:be:d1:2b:85:fd:a7:68:
         c8:ba:01:2b:b1:6c:74:1d:b8:73:95:e7:ee:b7:c7:25:f0:00:
         4c:00:b2:7e:b6:0b:8b:1c:f3:c0:50:9e:25:b9:e0:08:de:36:
         66:ff:37:a5:d1:bb:54:64:2c:c9:27:b5:4b:92:7e:65:ff:d3:
         2d:e1:b9:4e:bc:7f:a4:41:21:90:41:77:a6:39:1f:ea:9e:e3:
         9f:d0:66:6f:05:ec:aa:76:7e:bf:6b:16:a0:eb:b5:c7:fc:92:
         54:2f:2b:11:27:25:37:78:4c:51:6a:b0:f3:cc:58:5d:14:f1:
         6a:48:15:ff:c2:07:b6:b1:8d:0f:8e:5c:50:46:b3:3d:bf:01:
         98:4f:b2:59:54:47:3e:34:7b:78:6d:56:93:2e:73:ea:66:28:
         78:cd:1d:14:bf:a0:8f:2f:2e:b8:2e:8e:f2:14:8a:cc:e9:b5:
         7c:fb:6c:9d:0c:a5:e1:96
```

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.

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

Selects the certificates that match this parameter value.

[-uri <text>,…] - URI SAN

Selects the certificates that match this parameter value.

[-dns-name <text>,…] - DNS Name SAN

Selects the certificates that match this parameter value.

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

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
---------- --------------- ----------------------------------------
---------
vs0        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-----

MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIu

YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD

VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0

BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0G

CSqGSIb3DQEBCwUAA4IBAQBJlE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZOM1Bhy6Q

+gsE3XEtnN07AE4npjIT0eVP0nI9QIJAbP0uPKaCGAVBSBMoM2mOwbfswI7aJoEh

+XuEoNr0GOz+mltnfhgvl1fT6Ms+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.

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

Selects the certificates that match this parameter value.

[-uri <text>,…] - URI SAN

Selects the certificates that match this parameter value.

[-dns-name <text>,…] - DNS Name SAN

Selects the certificates that match this parameter value.

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

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

Vserver    Serial Number   Certificate Name                       Type
---------- --------------- ---------------------------------------
---------
vs0        4F4E4D7B         www.example.com         server-ca
    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-----

MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIu

YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD

VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0

BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0G

CSqGSIb3DQEBCwUAA4IBAQBJlE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZOM1Bhy6Q

+gsE3XEtnN07AE4npjIT0eVP0nI9QIJAbP0uPKaCGAVBSBMoM2mOwbfswI7aJoEh

+XuEoNr0GOz+mltnfhgvl1fT6Ms+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-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.

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

Selects the certificates that match this parameter value.

[-uri <text>,…] - URI SAN

Selects the certificates that match this parameter value.

[-dns-name <text>,…] - DNS Name SAN

Selects the certificates that match this parameter value.

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

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

Vserver    Serial Number   Certificate Name                       Type
---------- --------------- ---------------------------------------
---------
vs0        4F4E4D7B         www.example.com         server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

```
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-----

MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIu

YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD

VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0

BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0G

CSqGSIb3DQEBCwUAA4IBAQBJlE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZOM1Bhy6Q

+gsE3XEtnN07AE4npjIT0eVP0nI9QIJAbP0uPKaCGAVBSBMoM2mOwbfswI7aJoEh

+XuEoNr0GOz+mltnfhgvl1fT6Ms+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

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.

[-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.

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

Selects the certificates that match this parameter value.

[-uri <text>,…] - URI SAN

Selects the certificates that match this parameter value.

[-dns-name <text>,…] - DNS Name SAN

Selects the certificates that match this parameter value.

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

Selects the certificates that match this parameter value.

Examples

The examples below display information about digital certificates.

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------- 
---------
vs0        4F4E4D7B         www.example.com
server
    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-----

MIIDfTCCAmWgAwIBAwIBADANBgkqhkiG9w0BAQsFADBgMRQwEgYDVQQDEwtsYWIu

YWJjLmNvbTELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD

VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEwMDQzMDE4MTQ0

BgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFCVG7dYGe51akE14ecaCdL+LOAxUMA0G

CSqGSIb3DQEBCwUAA4IBAQBJlE51pkDY3ZpsSrQeMOoWLteIR+1H0wKZOM1Bhy6Q

+gsE3XEtnN07AE4npjIT0eVP0nI9QIJAbP0uPKaCGAVBSBMoM2mOwbfswI7aJoEh

+XuEoNr0GOz+mltnfhgvl1fT6Ms+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 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 {scheme://(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

Enter certificate signing request (CSR): Press <Enter> when done
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Signed Certificate: :
-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIET1oskDANBgkqhkiG9w0BAQsFADBdMREwDwYDVQQDEwh2
czAuY2VydDELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD
VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEyMDMwOTE2MTUx
M1oXDTEyMDQxNDE2MTUxM1owYDEUMBIGA1UEAxMLZXhhbXBsZS5jb20xCzAJBgNV
BAYTAlVTMQkwBwYDVQQIEwAxCTAHBgNVBAcTADEJMAcGA1UEChMAMQkwBwYDVQQL
EwAxDzANBgkqhkiG9w0BCQEWADBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQD1xWpz
-----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

Enter certificate signing request (CSR): Press <Enter> when done
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Signed Certificate: :
-----BEGIN CERTIFICATE-----
MIICwDCCAaigAwIBAgIET1ot8jANBgkqhkiG9w0BAQsFADBdMREwDwYDVQQDEwh2
czAuY2VydDELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYD
VQQKEwAxCTAHBgNVBAsTADEPMA0GCSqGSIb3DQEJARYAMB4XDTEyMDMwOTE2MjEw
NloXDTEyMDQxNDE2MjEwNlowYDEUMBIGA1UEAxMLZXhhbXBsZS5jb20xCzAJBgNV
BAYTAlVTMQkwBwYDVQQIEwAxCTAHBgNVBAcTADEJMAcGA1UEChMAMQkwBwYDVQQL
EwAxDzANBgkqhkiG9w0BCQEWADBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQD1xWpz
oarXHSyDzv3T5QIxBGRJ0ACtgdjJuqtuAdmnKvKfLS1o4C90
-----END CERTIFICATE-----
Enter private key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Enter a password for pkcs12 file:
Enter it again:

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:

```
            Security Bits   Asymmetric Key Length   Elliptic Curve Key
Length
            112             2048                    224
            128             3072                    256
            192             4096                    384
```

```
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 paramter, the command displays the minimum allowed security strength for certificates.

"expiration-warn-threshold" - If you specify this paramter, 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
-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
```

Copyright information

Trademark information