security certificate commands

ONTAP 9.3 commands

NetApp
September 27, 2022

Table of Contents

security certificate commands . . . 1
- security certificate create . . . 1
- security certificate delete . . . 3
- security certificate generate-csr . . . 4
- security certificate install . . . 6
- security certificate show . . . 9
- security certificate sign . . . 12
- security certificate ca-issued revoke . . . 16
- security certificate ca-issued show . . . 16

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>]` - Certificate Subtype

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

-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 *SHA1* , *SHA256* , *MD5* , *SHA224* , *SHA384* and *SHA512* when the "FIPS Mode" in "security config" is false. When the "FIPS Mode" is true, the possible values are *SHA224* , *SHA256* , *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>] - Certificate Subtype

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

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 securely to a certificate authority (CA) via any electronic media, to apply for a digital identity certificate.

Parameters

-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.

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

This specifies the number of bits in the private key. The higher the value, the more secure is the key. The default is 2048. Possible values include *512* , *1024* , *1536* and *2048* .

[-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 *SHA1* , *SHA256* and *MD5* .

Examples

This example creates a certificate-signing request with a 2048-bit private key generated by the SHA256 hashing function 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 generate-csr `-common-
name```_www.example.com_```-size` 2048 `-country` US `-state` California
`-locality` Sunnyvale `-organization` IT `-unit` Software
`-email-addr```_web@example.com_```-hash-function` SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please 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>] - Certificate Subtype

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

[-kmip-server-ip <IP Address>] - (DEPRECATED)-IPv4 and IPv6 address

This parameter is deprecated and might be removed in the future releases of Data ONTAP.

```
This parameter is applicable only to the ``_kmip-cert_`` subtype. It
specifies the IP address of the KMIP server.
```

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-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----
Please 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

Please 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

Please 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

Please 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

Please 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 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>] - Certificate Subtype

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

[-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.

Examples

The examples below display information about digital certificates.

```
cluster1::> security certificate show

Vserver    Serial Number   Common 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
          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 {(ftp|http)://(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 *SHA1* , *SHA256* and *MD5* .

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-----
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 MD5 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` MD5

Please 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-----
Please 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-----
Please enter a password for pkcs12 file:
Please 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>` - 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>] - 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_``
```