Installing iDRAC Certificate Using RACADM Commands

This Dell Technical white paper provides detailed information about generation of iDRAC certificate by using RACADM CLI.

Dell Engineering
October 2013

Author

Prashanth B S

Pradeep Mulay

A Dell Technical White Paper

Revisions

Date	Description
October 2013	Initial release

Contents

Revisions 2
Executive Summary 5
Introduction 5
1 Generating Certificate Signing Request (CSR) 6
2 Submitting Certificate Request 8
3 Uploading CA Certificate to iDRAC 11
4 Installing iDRAC Certificate on Windows Systems 12
5 Installing iDRAC Certificate on Linux Systems 13
Conclusion 14

Executive Summary

This document provides details about generation of iDRAC certificate that includes signing and adding the signed certificate to the trusted store on management stations using RACADM CLI.

Running RACADM commands are the most-opted method for managing Dell servers using a command line interface (CLI). Dell is investing to continually improve and add more functionality to RACADM.

Introduction

When you try to connect to iDRAC using Remote RACADM, and if there is an invalid certificate warning before running a command, it is indicated that the iDRAC IP address being connected to might not be from a trusted source. Following are the tasks to address the certificate warning scenario.

1 Generating Certificate Signing Request (CSR)

The first task in certificate installation is to create a Certificate Signing Request (CSR) and download it by getting it signed by a Certificate Authority. Following sequence of RACADM commands are used to configure the parameters for creating a CSR. The sample values shown here are for illustration purpose only. For more information about the objects or supported values, refer to the *RACADM Command Line Reference Guide for iDRAC7 and CMC* available at dell.com/support/manuals.

1. Make sure that the DNS RAC name is same as the common name specified in the security group of iDRAC by running any of the following commands. On iDRAC6 servers, config commands are supported and on iDRAC7 servers, set commands are recommended, though config commands are also supported.

- The `set` command

```
racadm set iDRAC.NIC.DNSRacName iDRAC-SSL-Certificate
```

- The `config` command

```
racadm config –g cfgLanNetworking –o cfgDNSRacName iDRAC-SSL-Certificate
```

2. To configure a DNS domain name, under **iDRAC registration,** click **Enable** . On iDRAC6 servers, config commands are supported and on iDRAC7 servers, set commands are recommended, though config commands are also supported.

- The `set` command

```
racadm set idrac.NIC.DNSDomainName xyz.com

racadm set idrac.NIC.DNSRegister Enabled
```

- The `config` command

```
racadm config –g cfgLanNetworking –o cfgDNSDomainName xyz.com

racadm config –g cfgLanNetworking –o cfgDNSRegisterRac 1
```

3. To configure the iDRAC security group-related parameters for CSR generation, run one of the following commands:

- The `set` subcommand

```
racadm set iDRAC.Security.CsrKeySize 1024/2048

racadm set iDRAC.Security.CsrCommonName iDRAC-SSL-Certificate

racadm set iDRAC.Security.CsrOrganizationName XYZ

racadm set iDRAC.Security.CsrOrganizationUnit Unit1

racadm set iDRAC.Security.CsrLocalityName LocName
```

```
racadm set iDRAC.Security.CsrStateName StateName

racadm set iDRAC.Security.CsrCountryCode US

racadm set iDRAC.Security.CsrEmailAddr abc@xyz.com
```

- The config subcommand

```
racadm config –g cfgRacSecurity –o cfgRacSecCsrKeySize 1024/2048

racadm config –g cfgRacSecurity –o cfgRacSecCsrCommonName iDRAC-SSL-
Certificate

racadm config –g cfgRacSecurity –o cfgRacSecCsrOrganizationName XYZ

racadm config –g cfgRacSecurity –o cfgRacSecCsrOrganizationUnit Unit1

racadm config –g cfgRacSecurity –o cfgRacSecCsrLocalityName LocName

racadm config –g cfgRacSecurity –o cfgRacSecCsrStateName StateName

racadm config –g cfgRacSecurity –o cfgRacSecCsrCountryCode US

racadm config –g cfgRacSecurity –o cfgRacSecCsrEmailAddr abc@xyz.com
```

4. When all the required parameters are configured successfully, CSR is generated using the `sslcsrgen` subcommand. This subcommand uses the parameters specified under the `iDRAC.Security` group for generating a CSR. The command syntax is given here.

   racadm sslcsrgen –g –f idraccsr.txt

Note: The file option is supported only through Remote RACADM interface or Local RACADM interface.

2 Submitting Certificate Request

After the CSR file is successfully generated and downloaded to the client file system, open the CSR file in a Notepad or MS-Word application, and then copy the contents between the begin and end points as indicated in the screen shot here.

Figure 1 A Sample Certificate

1. In the **Address** bar of a browser, type `https://<IP address>/certsrv`

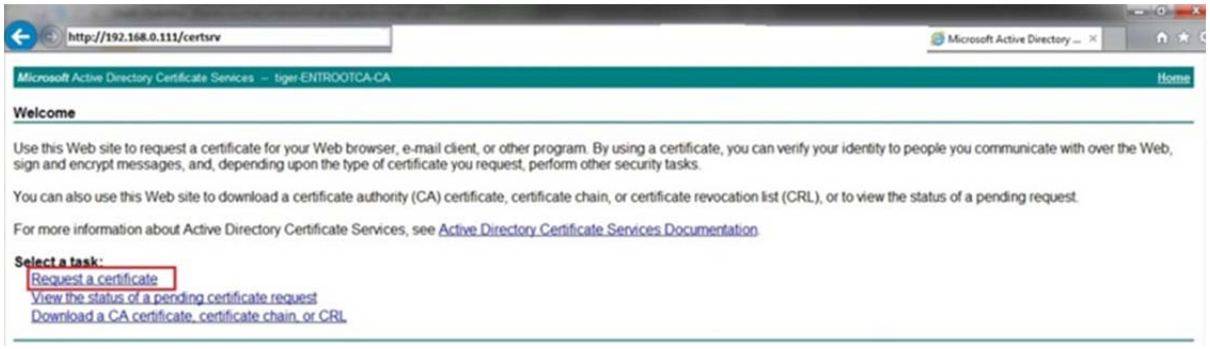

Figure 2 Certificate Authority—Home Page

2. On the **Microsoft Directory Certificate Services** page, click **Request a certificate,** and then click **advanced certificate request**.

Figure 3 Certificate Request

3. Click **Submit a certificate request by using base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base 64-encoded PKCS #7 file**

Figure 4 Advanced Certificate Request

4. In the **Saved Request** box, paste the certificate data that you copied earlier. From the **Certificate Template** drop-down menu, select **Web Server**, and then click **Submit**. An appropriate certificate is issued.

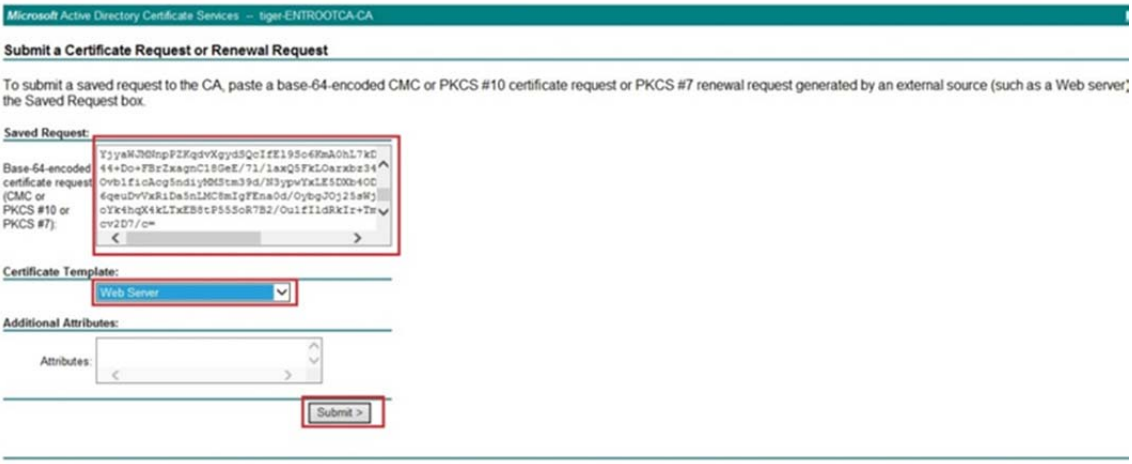

Figure 5 Submit a Certificate Signing Request

5. To issue a Signed Certificate, click **Base 64 encoded**.
6. To download the **Base-64 encoded format** certificate, click **Download Certificate**.

Figure 6 Signed Certificate Download Option

3 Uploading CA Certificate to iDRAC

1. The certificate issued by the Certificate Services has to be uploaded to iDRAC as a web server certificate for authenticating any client connection requests. To perform this operation run the following command.

   ```
   racadm sslcertupload –t 1 –f certnew.cer
   ```

2. To make sure that the certificate has been uploaded to iDRAC successfully, run the following command.

   ```
   racadm sslcertview -t 1
   ```

4 Installing iDRAC Certificate on Windows Systems

If the Windows Management Station is already part of the same domain as certificate authority, then the whole setup process is complete. There will not be any certificate warning observed during the next Remote RACADM session. Else, if MS-Windows is not part of the same domain as certificate authority, then complete the following tasks:

1. On the **Welcome** page, click **Download a CA certificate chain or CRL**.

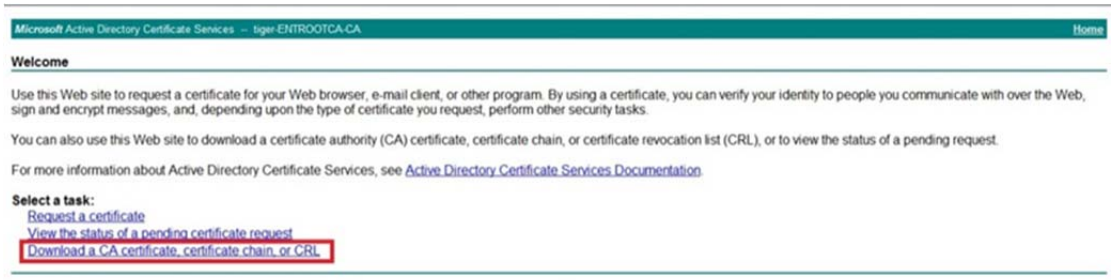

Figure 7 Welcome Page

2. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Down CA Certificate**.

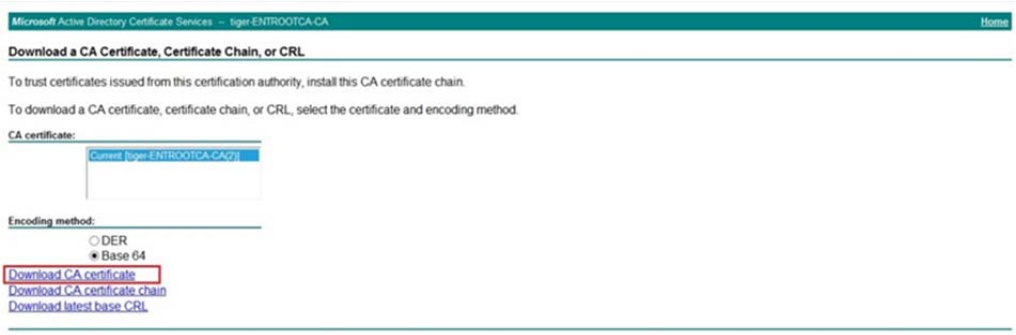

Figure 8 Download CA certificate

3. Install the certificate on the Windows management station. For more information about installing a certificate, see http://blogs.technet.com/b/sbs/archive/2007/04/10/installing-a-self-signed-certificate-as-a-trusted-root-ca-in-windows-vista.aspx
4. To point to a DNS server of the domain of the Root CA, configure the DNS settings for name resolutions in the networking,
5. To run Remote RACADM command, at the command line interface, use the iDRAC FQDN as a remote endpoint while running any remote RACADM command.

```
racadm –r iDRAC-SSL-Certificate.xyz.com –u admin –p passwd getsysinfo
```

5 Installing iDRAC Certificate on Linux Systems

1. Convert the certificate in DER format to PEM format (using openssl command line tool):

   ```
   openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] –outform pem -
   out [outcertfileinpemformat.pem] –text
   ```

2. Find the location of the default CA certificate bundle on the management station. For example, for RHEL5 64-bit, it is `/etc/pki/tls/cert.pem`.

3. Append the PEM formatted CA certificate to the management station CA certificate. For example, run the cat command: `- cat testcacert.pem >> cert.pem`

4. To point to a DNS server of the domain of the Root CA, configure the DNS settings for name resolutions in the networking,

5. To run Remote RACADM command, at the command line interface, use the iDRAC FQDN as a remote endpoint while running any remote RACADM command.
   racadm –r iDRAC-SSL-Certificate.xyz.com –u admin –p passwd getsysinfo

Conclusion

The sections covered in this document discusses about the generation and installation of iDRAC Certificate by using the RACADM commands. This helps to avoid certificate-related warnings observed while connecting to iDRAC using Remote RACADM or iDRAC GUI using a Web browser. For more information about generating and uploading a Server Certificate using iDRAC GUI, refer to the *iDRAC User's Guide* available at dell.com/support/manuals.