Managing Web Server Certificates on iDRAC

This Dell technical white paper explains how to configure the web server certificates on iDRAC to establish secure remote connections.

Dell Engineering
November 2014

Author:
Doug Roberts

Dell | Enterprise Solutions Group

A Dell Technical White Paper

Table of contents

Executive summary 4

1 Introduction 5

2 Dell Self-Signed SSL Certificates 7

2.1 How to Trust Self-Signed Certificate on Windows Management Stations 7

2.2 How to Trust Self-Signed Certificate on Linux Management Stations 8

3 Custom Signed SSL Certificates 10

3.1 Export the signing certificate in PKCS #12 format 10

3.2 Upload the custom signing certificate to the iDRAC 10

3.3 How to Trust CA Certificate on Windows Management Stations 11

3.4 How to Trust CA Certificate on Linux Management Stations 12

4 Certificate Authority Signed SSL Certificates 14

4.1 Generate a Certificate Request 14

4.2 Submit to a CA - Windows Server 2012 Certificate Authority 14

4.3 Upload the new certificate to the iDRAC 14

4.4 Download the CA Certificate - Windows Server 2012 CA 15

4.5 How to Trust CA Certificate on Windows Management Stations 15

4.6 How to Trust CA Certificate on Linux Management Stations 16

A How to Access the Trusted Certificates Store on Windows Workstations 17

B WSMAN Command Syntax with Trusted Certificates 18

B.1 Windows Workstations (WinRM commands) 18

B.2 Linux Workstations (OpenWSMAN commands) 18

Executive summary

Dell's integrated Dell Remote Access Controller (iDRAC) uses web server certificates (also known as SSL certificates) to establish and maintain secure communications with remote clients. Web browsers and command line utilities, such as RACADM and WS-Man, use these SSL certificates for server authentication and establishing an encrypted connection.

There are several options available to secure the network connection using web server certificates. iDRAC's web server has a self-signed SSL certificate by default. The self-signed certificate can be replaced with a custom signing certificate or a certificiate signed by a well-known Certiicate Authority (CA). Which ever method is chosen, once iDRAC is configured and the SSL certificate is installed on the management stations, SSL enabled clients can access iDRAC securely and without certificate warnings.

1 Introduction

This document describes the different methods available to use a web server certificate on the iDRAC and how to configure your Windows or Linux management station to trust the certificate authority that issued the certificate. Once configured, remote connections to the iDRAC via web browsers, racadm commands, and wsman commands will be properly secured and the associated warning messages will be eliminated.

The iDRAC uses an SSL certificate to authenticate itself to web browsers and command line utilities, such as racadm and wsman, running on management stations. If the Certificate Authority that issued the certificate is not trusted by the management station, warning messages will be displayed on the management station. This document explains how to configure management stations to trust the certificate authority.

There are three types of signed web server certificates that can be employed for securing communications with iDRAC, the Dell self-signed SSL certificate, the custom signed SSL certificate and Certificate Authority (CA) signed SSL certificate. Each type has advantages and disadvantages.

Dell Self-Signed SSL Certificate - The certificate is auto generated and self-signed by the iDRAC. Starting with iDRAC7 version 2.10.10 and iDRAC8, each iDRAC has a unique self-signed certificate by default.

Advantages:

- Do not have to maintain a Certificate Authority.
- Certificates are auto generated by the iDRAC.

Disadvantage:

- The certificate for each iDRAC has to be added to the trusted certificates store on each management station. (Every iDRAC is its own Certificate Authority which must be trusted).

Custom Signed SSL Certificate - The certificate is auto generated and signed using a signing certificate uploaded from your in-house Certificate Authority.

Advantages:

- Only have to trust one Certificate Authority for all iDRAC. It's possible your in-house Certificate Authority is already trusted on your management stations.
- Certificates are auto generated by the iDRAC.

Disadvantage

- Have to maintain your own Certificate Authority.

CA Signed SSL Certificate - A certificate signing request (CSR) is generated and submitted to your in-house Certificate Authority or by a 3rd party Certificate Authority such as VeriSign, Thawte, Go Daddy, etc. for signing.

Advantages:

- Can use a commercial Certificate authority.
- Only have to trust 1 Certificate Authority for all iDRAC. If a commercial CA is used it is very likely to be already trusted on your management stations.

Disadvantage:

- Have to either purchase commercial certificates or maintain your own Certificate Authority.

- A CSR has to be generated and submitted for every iDRAC.

The SSL certificate configurations described in this document were performed using iDRAC8 but also applies to iDRAC7. For the remaining document, when referring to 'iDRAC' it applies to both iDRAC7 and iDRAC8 unless otherwise specified.

The steps describe in this document were developed using a Windows 7 Professional and Red Hat Linux 6.4 management station and a Windows Server 2012 Certificate Server The browsers on the management stations were latest available at the time this document was written. Steps will be similar, but may not be exact, on other product versions.

Remote racadm commands shown use the default user name (root) and password. Replace these with your iDRAC Administrator user name and password.

2 Dell Self-Signed SSL Certificates

Each iDRAC8 has the ability to auto-generate a unique self-signed SSL certificate good for ten years. This feature was added to iDRAC7 starting with firmware version 2.10.10.10. The certificate is generated using SHA2 algorithms and RSA 2048-bit key strength to provide a seure communication channel.

An SSL certificate is generated at boot time if one is not found or corrupt. The Fully Qualified Domain Name (FQDN) provides a unique Common Name (CN) for each iDRAC. The FQDN of iDRAC consist of the RAC name attribute and the Domain name attribute. By default, each iDRAC has a unique RAC name which includes its Service Tag number, such as "**idrac-<service tag>**".

A new self-signed SSL certificate can be generated at anytime using the RACADM command "**sslresetcfg**". This will replace the existing SSL certificate. An iDRAC reset is required to load the new certificate.

When upgrading iDRAC7 1.xx.xx.xx to iDRAC7 2.xx.xx.xx, the old certificates remain valid until sslresetcfg command is executed.

This section describe how to download iDRAC's self-signed SSL certificate and install it into the appropriate certificate store on your Windows and Linux management station.

2.1 How to Trust Self-Signed Certificate on Windows Management Stations

Download the Certificate

Web interface:

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Under **SSL Certicificate** > **Option**, select **Download SSL Certificate** > **Next.**

Where the certificate will be downloaded as <srvtag>-ssl_cert.pem. Rename the file, replacing the ".pem" extension with ".cer." For example, 1234xyz-ssl_cert.cer.

Remote RACADM:

From a command prompt, run the following command:

```
racadm -r <idrac fqdn> -u root -p ****** sslcertdownload -f <filename.cer> -t 1
```

Where *filename.cer* is a name you choose for the certificate file.

Install the Certificate in Microsoft Windows Store

- Double click on the .cer file downloaded from the iDRAC.
- Click **Install Certificate**. The Windows **Certificate Import Wizard** launches.
- Click **Next** > **Place all certificates in the following store** > **Browse** > **Trusted Root Certification Authorities > OK > Next > Finish**.
- Click **Yes** to install the certificate. **"The import was successful"** is displayed. **OK > OK.**

Internet Explorer and Google Chrome browsers, as well as racadm and WinRM (wsman) commands all use the same trusted certificate store on Windows 7 management stations. Once the certificate has been installed in the trusted store per the steps above, the certificate warning messages will no longer be received.

Browsers will need to be closed/reopened first. Be sure to use the fully qualified domain name of the iDRAC in your browser and on the command line.

Install the Certificate in Mozilla Firefox Browser Store

Firefox uses a different trusted certificate location so the certificate must be trusted separately.

- Open Firefox, go to **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates** > **Authorities**
- Click **Import**, select .cer file downloaded from iDRAC.
- Click **Open** > check **Trust this CA to identify websites** > **OK > OK > OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

2.2 How to Trust Self-Signed Certificate on Linux Management Stations

Download Certificate

Web interface:

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Under **SSL Certicificate** > **Option**, select **Download SSL Certificate** > **Next.**

Where the certificate will be downloaded as <srvtag>-ssl_cert.pem.

Remote RACADM:

From a command prompt, run the following command:

```
$racadm -r <idrac fqdn> -u root -p ****** sslcertdownload -f <filename.pem> -t 1
```

Where *filename.pem* is a name you choose for the certificate file.

Install the Certificate for Remote Racadm Commands

- Find the location of the default CA certificate bundle on the management station. For example, on RHEL6 x86_64 it is named /etc/pki/tls/cert.pem.
- Append the PEM formatted CA certificate to the management station CA certificate.

```
$cat filename.pem >> /etc/pki/tls/cert.pem
```

Remote racadm commands should now run without the certificate warning message.

Install the Certificate in Google Chrome Browser Store

- In Chrome, go to **Settings** > **Show Advanced Settings ...** > **Manage certificates ...** > **Authorities**
- Click **Import,** select .pem file downloaded from iDRAC**.**
- Click **Open,** check **"Trust this certificate for identifying websites"**. **OK** > **OK.**

Close / reopen Chrome and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

Install the Certificate for Mozilla Firefox Browser Store

- Open Firefox and go to **Edit** > **Preferences** > **Advanced** > **Encryption** > **View Certificates** > **Authorities.**
- Click **Import**, select .pem file downloaded from iDRAC.
- Click **Open**, check **Trust this CA to identify websites. OK > OK > OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

3 Custom Signed SSL Certificates

To use this method, you will need a Certificate Authority (CA) under your control since this involves uploading a certificate that includes the private key of the CA to the iDRAC. The iDRAC uses this certificate to generate a custom certificate signed by your CA. The benefit of this method is you only have to trust your CA, instead of all iDRACs individually on your management stations.

This section will provide guidance on how to export your signing certificate and upload it to iDRAC. Then describe how to install it into the appropriate certificate store on your Windows and Linux management station.

3.1 Export the signing certificate in PKCS #12 format

PKCS #12 is the format used to a store a certificate along with its private key. These files typically have the extension .pfx when exported from Windows CA's and .p12 when exported from OpenSSL CA's. The steps to do this will vary depending on the Certificate Authority you are using.

For example, on a CA running on Windows Server 2012, do the following:

Use MMC Certificate snap-in to export the signing certificate.

- Right click on the **CA certificate** > **All Tasks** > **Export** to open the Certificate Export Wizard.
- Click **Next**. Select **Yes**, export the private key > **Next**.
- Make sure Personal Information Exchange - PKCS #12 (.PFX) is selected > **Next**.
- Set a password > **Next**.
- Enter the file name > **Save** > **Next** > **Finish**.
- "The Export was successful" is displayed > **OK**.

3.2 Upload the custom signing certificate to the iDRAC

- Connect to the iDRAC in a browser, **https://<fqdn_of_idrac>**
- Go to **Overview > iDRAC Settings > Network > SSL** tab.
- Under **"Custom SSL Certificate Signing Certificate",** make sure **"Upload Custom SSL Certificate Signing Certificate"** is selected and click **Next**.
- Select **Browse >** Point to the certificate in PKCS #12 format (the .pfx file in this example) > **Open**.
- Next to **PKCS#12 Password**, enter the password **> Apply**.

It will take a few minutes to generate a new SSL certificate signed by the CA. Once complete an Informational message will indicate a reset of iDRAC is required.

Note: A new SSL certificate has been generated, signed by the CA. Now iDRAC needs to be restarted to consume the new SSL certificate. Until iDRAC has been reset the old SSL certificate is still in use.

If the management stations already trust the Certificate Authority, browsers, racadm commands, and wsman commands should all work without certificate error messages at this point. Browsers may need to be closed / reopened first.

3.3 How to Trust CA Certificate on Windows Management Stations

Note: This section can be skipped on management stations that already trust the Certificate Authority used in the steps above.

Download the CA's Certificate

Note: For security, the CA's certificate is downloaded in a format that does not contain the private key.

Web interface:

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Under **Custom SSL Certificate Signing Certificate** > **Option**, select **Download Custom SSL Certificate Signing Certificate** > **Next.**

Where the certificate will be downloaded as host-custom-signing.crt.

Remote RACADM:

From a command prompt, run the following command:

```
>racadm -r <idrac fqdn> -u root -p ****** sslcertdownload -f <filename.crt> -t 3
```

Where *filename.crt* is a name you choose for the certificate file. The -t 3 switch tells racadm to get the custom signing certificate.

Install the Certificate in Microsoft Windows Store

- Double click on the .crt file downloaded from iDRAC.
- Click **Install Certificate**. The Windows **Certificate Import Wizard** launches.
- Click **Next** > **Place all certificates in the following store** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish**.
- Click **Yes** to install the certificate. **"The import was successful"** is displayed. **OK > OK.**

Internet Explorer and Google Chrome browsers, as well as racadm and WinRM (wsman) commands all use the same trusted certificate store on Windows 7 management stations. Once the certificate has been installed in the trusted store per the steps above, the certificate warning messages will no longer be received.

Browsers will need to be closed/reopened first. Be sure to use the fully qualified domain name of the iDRAC in your browser and on the command line.

Install the Certificate for Mozilla Firefox Browser Store

Firefox uses a different trusted certificate location so the certificate must be trusted separately.

- Open Firefox, go to **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates** > **Authorities**
- Click **Import**, select .cer file downloaded from iDRAC.
- Click **Open**. check **Trust this CA to identify websites** > **OK** > **OK** > **OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

3.4 How to Trust CA Certificate on Linux Management Stations

The following steps were obtained using RHEL 6.4 x86_64 and the latest browsers available at the time of this writing. Steps will be similar, but may not be exact, on other product versions.

Download the CA's Certificate

Web interface:

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Under **Custom SSL Certificate Signing Certificate** > **Option**, select **Download Custom SSL Certificate Signing Certificate** > **Next.**

Where the certificate will be downloaded as host-custom-signing.crt.

Remote RACADM:

From a command prompt, run the following command:

```
$racadm -r <idrac fqdn> -u root -p ****** sslcertdownload -f <filename.crt> -t 3
```

Where *filename.crt* is a name you choose for the certificate file. The -t 3 switch tells racadm to get the custom signing certificate.

Install the Certificate for Remote Racadm Commands

- Convert the CA's certificate to PEM format:

```
$openssl x509 -inform pem -in <certnew.cer> -outform pem -out <filename.pem> -
text
```

- Find the location of the default CA certificate bundle on the management station. For example, on RHEL6 x86_64 it is named /etc/pki/tls/cert.pem.
- Append the PEM formatted CA certificate to the management station CA certificate.

```
$cat filename.pem >> /etc/pki/tls/cert.pem
```

Remote racadm commands should now run without the certificate warning message.

Install the Certificate in Google Chrome Browser Store

- In Chrome, go to **Settings** > **Show Advanced Settings ...** > **Manage certificates ...** > **Authorities**
- Click **Import,** select .pem file downloaded from iDRAC**.**
- Click **Open**, check **"Trust this certificate for identifying websites"**. **OK** > **OK.**

Close / reopen Chrome and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

Install the Certificate Mozilla Firefox Browser Store

- Open Firefox and go to **Edit** > **Preferences** > **Advanced** > **Encryption** > **View Certificates** > **Authorities.**
- Click **Import**, select .pem file downloaded from iDRAC.
- Click **Open**, check **Trust this CA to identify websites. OK > OK > OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

4 Certificate Authority Signed SSL Certificates

With this method, a certificate signing request (CSR) is generated and submitted to your in-house Certificate Authority or to a 3rd party Certificate Authority such as VeriSign, Thawte, Go Daddy, etc. for signing. You will only have to trust one CA, but you will need to generate a CSR for every iDRAC.

This section will provide guidance on how to generate a CSR, submit to CA and upload sign certificate to iDRAC. Then describe how to install it into the appropriate certificate store on your Windows and Linux management station.

4.1 Generate a Certificate Request

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Select **Generate Certificate Signing Request (CSR)** and click **Next**.
  1. For the **Common Name**, enter the **FQDN** of the iDRAC. For example, if the **DNS DRAC Name** entered earlier is "idrac-ST12345", and your domain name is "test.lab", you would enter "idrac-ST12345.test.lab" (no quotes) here. This field is critical.
  2. Fill out the remaining fields.
- Click **Generate**, and save the csr.txt file. (It will take a few seconds to generate the file.)

Provide the csr file to a 3rd party Certificate Authority or submit to your in-house CA.

Note: iDRAC accepts only X509 Base 64 encoded Web Server certificates.

4.2 Submit to a CA - Windows Server 2012 Certificate Authority

The following steps can be followed to generate a certificate from the CSR if you are running a CA on Windows Server 2012, configured to accept certificate requests over http:

- Browse to: **http://<IP_of _CA>/certsrv**
- Click **Request a certificate** > **advanced certificate request**
- Select **Submit a certificate request by using a base-64 encoded CMC or PKCS#10 file.**
- Copy the entire contents of the csr.txt file into the **Base-64-encoded certificate request** box.
- Under Certificate Template, select **Web Server**, click **Submit**.
- Select **Base 64 encoded**, click **Download Certificate**.

Save the file, certnew.cer, to your Desktop.

4.3 Upload the new certificate to the iDRAC

Once you have received your signed Web Server certificate (in X509 Base 64 format) from the 3rd party or in-house CA:

- Connect to the iDRAC with your browser, https://<idrac_fqdn>.
- Go to **Overview** > **iDRAC Settings** > **Network** > **SSL** tab.
- Under **SSL Certicificate** > **Option**, select **Upload Server Certificate** > **Next.**

- Browse to the path of the certificate (certnew.cer in the above example), click **Apply.**

If successful, an Informational message is displayed. Click Reset iDRAC to apply new certificate.

Note: iDRAC must be reset to apply new certificate. Until iDRAC has been reset, the old SSL certificate will be active.

If the management stations already trust the Certificate Authority, browsers, racadm commands, and wsman commands should all work without certificate error messages at this point. Browsers may need to be closed / reopened first. Remember to use the FQDN of the iDRAC when connecting.

4.4 Download the CA Certificate - Windows Server 2012 CA

The following steps can be followed to download a CA certificate if you are running a CA on Windows Server 2012, configured to accept certificate requests over http:

Note: These steps only need to be followed if your Management Stations do not already trust the CA that issued the certificate. If not already trusted on your workstations, you will need to obtain a copy of the CA's certificate and add it to the appropriate trusted store.

- Browse to: **http://<IP_of _CA>/certsrv**
- Click **Download a CA Certificate, certificate chain, or CRL**
- Under **CA certificate:** select correct CA certificate.
- Under **Encoding method:** select **Base 64**
- Click **Download CA certificate**

The certificate will be downloaded as **certnew.cer.**

4.5 How to Trust CA Certificate on Windows Management Stations

Install the Certificate in the Microsoft Windows Store

- Double click on the .crt file downloaded from iDRAC.
- Click **Install Certificate**. The Windows **Certificate Import Wizard** launches.
- Click **Next** > **Place all certificates in the following store** > **Browse** > **Trusted Root Certification Authorities** > **OK** > **Next** > **Finish**.
- Click **Yes** to install the certificate. **"The import was successful"** is displayed. **OK > OK.**

Internet Explorer and Google Chrome browsers, as well as racadm and WinRM (wsman) commands all use the same trusted certificate store on Windows 7 management stations. Once the certificate has been installed in the trusted store per the steps above, the certificate warning messages will no longer be received.

Browsers will need to be closed/reopened first. Be sure to use the fully qualified domain name of the iDRAC in your browser and on the command line.

Install the Certificate in Mozilla Firefox Browser Store

Firefox uses a different trusted certificate location so the certificate must be trusted separately.

- Open Firefox, go to **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates** > **Authorities**
- Click **Import**, select .cer file downloaded from CA.
- Click **Open**, check **Trust this CA to identify websites. OK > OK > OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

4.6 How to Trust CA Certificate on Linux Management Stations

Install the Certificate for Remote Racadm Commands

- Convert the CA's certificate to PEM format:

```
$openssl x509 -inform pem -in <certnew.cer> -outform pem -out <filename.pem> -
text
```

- Find the location of the default CA certificate bundle on the management station. For example, on RHEL6 x86_64 it is named /etc/pki/tls/cert.pem.
- Append the PEM formatted CA certificate to the management station CA certificate.

```
$cat filename.pem >> /etc/pki/tls/cert.pem
```

Remote racadm commands should now run without the certificate warning message.

Install the Certificate in Google Chrome Browser Store

- In Chrome, go to **Settings** > **Show Advanced Settings ...** > **Manage certificates ...** > **Authorities**
- Click **Import,** select .cer file downloaded from CA**.**
- Click **Open,** check **"Trust this certificate for identifying websites"**. **OK** > **OK.**

Close / reopen Chrome and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

Install the Certificate in Mozilla Firefox Browser Store

- Open Firefox and go to **Edit** > **Preferences** > **Advanced** > **Encryption** > **View Certificates** > **Authorities.**
- Click **Import**, select .cer file downloaded from CA.
- Click **Open**, check **Trust this CA to identify websites. OK > OK > OK.**

Close / reopen Firefox and connect to the iDRAC (be sure to use the FQDN of the iDRAC, not the IP address). The certificate warning message should no longer be received.

A How to Access the Trusted Certificates Store on Windows Workstations

The certificates trusted on the Windows management station can be viewed, added, and deleted with the Certificates Snap-in component of Microsoft Management Console.

To launch Microsoft Management Console, click **Start >** in the Search box type **mmc > Enter.**

To add the snap-in click **File > Add / Remove Snap-In ...** > highlight **Certificates** and click **Add**. Select **"My user account" > Finish > OK**.

To access the certificates, expand **Certificates - Current User > Trusted Root Certification Authorities > Certificates.**

B WSMAN Command Syntax with Trusted Certificates

The syntax used with wsman commands (WinRM on Windows and OpenWSMAN on Linux) will change slightly if you want to use a trusted certificate.

B.1 Windows Workstations (WinRM commands)

Without a trusted iDRAC certificate, a typical winrm command looks like this:

```
winrm e cimv2/root/dcim/DCIM_ComputerSystem -u:root -p:****** -r:https://idrac-ST12345.test.lab/wsman -encoding:utf-8 -a:basic -SkipCNCheck -SkipCACheck
```

The "-SkipCNCheck" and "-SkipCACheck" switches are required without a trusted certificate to avoid an error message. (Figure 3.)

With a trusted iDRAC certificate, the "-Skip" switches can be dropped and the certificate can properly validated by the workstation. Be sure to use the FQDN of the iDRAC in the command or the certificate name check will fail. The resulting command will look like this:

```
winrm e cimv2/root/dcim/DCIM_ComputerSystem -u:root -p:****** -r:https://idrac-ST12345.test.lab/wsman -encoding:utf-8 -a:basic
```

Reminder: For winrm certificate validation, the certificate needs to be in the Windows Trusted Root Certificates store. This can be done using the racadm, Internet Explorer, or Google Chrome options covered earlier.

B.2 Linux Workstations (OpenWSMAN commands)

Without a trusted iDRAC certificate, a typical OpenWSMAN command looks like this:

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_ComputerSystem -h idrac-ST12345.test.lab -P 443 -u root -p ****** -y basic -c dummy.cert -V -v
```

A dummy certificate file has to be used after the -c switch, and the -v and -V switches have to be included to skip the host name and CA checks.

With a trusted iDRAC certificate, the valid certificate file is used in the command after the -c switch. The -v and -V switches are dropped so the certificate will be properly validated. The resulting command will look like this:

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_ComputerSystem -h idrac-ST12345.test.lab -P 443 -u root -p ****** -y basic -c /etc/pki/tls.cert.pem
```