Redfish Certificate Management

Table of contents

Certificate management actions—such as retrieving certificate information or performing atomic certificate replacement—are accessible through the `CertificateService` resource.

The `CertificateLocations` resource provides an inventory of all certificates managed by the service.

For additional details, refer to the *Redfish Certificate Management White Paper*.

Common Certificate Management Commands

Getting Certificate Locations

Inventory of all certificates the service is managing.

```
curl -k -u root:'<password>' -X GET
https://<bmc_ip>/redfish/v1/CertificateService/CertificateLocation
```

Root CA Management Commands

List Root CA

```
curl -k -u root:'<password>' -X GET
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/Truststore/Cert
```

Getting Certificate Information

```
curl -k -u root:'<password>' -X GET
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/Truststore/Cert
```

Installing Root CA Certificate

```
curl -k -u root:'<password>' -X POST
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/Truststore/Cert
-d @rootca.json
```

Replacing Existing Root CA Certificate

```
curl -k -u root:'<password>' -X PATCH
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/Truststore/Cert
-d @rootca.json
```

Root CA Certificate Creation and Replacement

1. Generate Root CA certificate:

    ```
    cat > root-ca.cnf << EOF
    [req]
    distinguished_name = req_distinguished_name
    req_extensions = v3_req
    prompt = no

    [req_distinguished_name]
    C = <country>
    ST = <state>
    L = <location>
    O = OpenBMC
    OU = bmcweb
    ```

```
CN = <common_name>

[v3_req]
basicConstraints = critical,CA:true
keyUsage = critical,keyCertSign,cRLSign
subjectKeyIdentifier = hash
EOF

# Generate root CA key
openssl genrsa -out root-ca-key.pem <key_size>

# Generate root CA certificate
openssl req -x509 -new -nodes \
    -key root-ca-key.pem \
    -sha256 -days <validity_days> \
    -out root-ca-cert.pem \
    -config root-ca.cnf \
    -extensions v3_req
```

2. Create a JSON file for the root CA certificate add

```
{
    "CertificateString": "<cert_string>",
    "CertificateType": "PEM"
}
```

3. Install the root CA certificate (can have more then 1).

```
curl -k -u root:'<password>' -X POST
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/Truststore/Certificates -d @rootca.json
```

Server Certificate Management Commands

Getting Certificate Information

```
curl -k -u root:'<password>' -X GET
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/NetworkProtocol
```

Replacing Existing Certificate

```
curl -k -u root:'<password>' -X POST
https://<bmc_ip>/redfish/v1/CertificateService/Actions/Certificate
-d @certificate.json
```

Generating CSR

Generate certificate signing request (CSR):

```
curl -k -u root:'<password>' -H "Content-Type: application/json"
-X POST
https://<bmc_ip>/redfish/v1/CertificateService/Actions/Certificate
-d @csr_file.json
```

Installing Certificate

```
curl -k -u root:'<password>' -H "Content-Type: application/octet-
stream" -X POST
```

```
https://<bmc_ip>/redfish/v1/Managers/Bluefield_BMC/NetworkProtocol/
-d @certificate.json
```

Example for CSR Generation, Certificate Creation and Replacement

1. Configure your CA to include at least the following extensions for the signed TLS server certificates:

   ```
   basicConstraints = CA:FALSE
   keyUsage = nonRepudiation, digitalSignature, keyEncipherment
   subjectAltName = IP:192.168.240.1
   ```

   > **Note**
   >
   > The extension `subjectAltName = IP:192.168.240.1` is mandatory.

2. Create a JSON containing the subject data for the BlueField BMC to use when creating the CSR. For example:

   ```
   {
       "City": "<city>",
       "CertificateCollection": {
           "@odata.id":
   "/redfish/v1/Managers/Bluefield_BMC/NetworkProtocol/HTTPS/Cert
       },
       "CommonName": "bmc0123456789.mycompany.com",
       "Country": "<country>",
   ```

```
    "Organization": "<company_name>",
    "OrganizationalUnit": "<my_org>",
    "State": "<state>",
    "KeyPairAlgorithm": "EC"
}
```

3. Generate a certificate signing request using the forth command in the table above and the JSON file created in the previous step:

Info

The BMC replies with a JSON containing the CSR.

```
curl -k -u root:'<password>' -H "Content-Type:
application/json" -X POST
https://<bmc_ip>/redfish/v1/CertificateService/Actions/Certifi
-d @csr_file.json
{
  "CSRString": "-----BEGIN CERTIFICATE REQUEST-----\
<CSR_DATA>\n-----END CERTIFICATE REQUEST-----\n",
  "CertificateCollection": {
    "@odata.id":
"/redfish/v1/Managers/Bluefield_BMC/NetworkProtocol/HTTPS/Cert
  }
}
```

4. Extract the CSR string from the JSON and sign the CSR using your CA. For example, this is how to include the required extensions to the signed TLS server certificates:

```
openssl x509 -req -in bmc.csr -CA CA-cert.pem -CAkey CA-
key.pem -CAcreateserial -out bmc.crt -days 3650 -sha384 -
extfile exfile.txt
```

Where:

- `bmc.csr` contains the CSR string from the previous step
- `CA-cert.pem` contains the CA certificate to be used to sign the CSR
- `CA-key.pem` contains the CA private key
- `extfile.txt` contains the extensions mentioned in the first step (`basicConstraints`, `keyUsage`, and `subjectAltName`)
- `bmc.crt` is the output file which will contain the BMC certificate signed by the CA

5. Create a JSON file for the BlueField BMC signed TLS server certificate data:

```
{
    "CertificateString": "-----BEGIN CERTIFICATE-----
\n<bmc.crt-data>\n-----END CERTIFICATE-----",
    "CertificateType": "PEM",
    "CertificateUri":
    {
        "@odata.id":
"/redfish/v1/Managers/Bluefield_BMC/NetworkProtocol/HTTPS/Cert
    }
}
```

6. Replace the BMC certificate using the third command in the table above and the JSON created in the previous step.

```
curl -k -u root:'<password>' -X POST
https://<bmc_ip>/redfish/v1/CertificateService/Actions/Certifi
-d @certificate.j
```

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

Trademarks