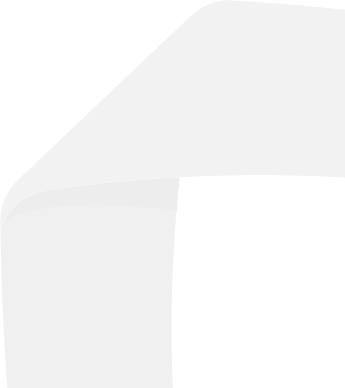


Renew or Add SSL certificate to Dynatrace Managed cluster



Auteur:



Uros DJUKIC

15/05/2024

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change |
| 2024-05-15 | Uros DJUKIC | 1.0 | Recommendations from ACE Services team |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* Introduction

There are 2 types of certificates:

**Inbound (Nginx, Dynatrace Server) and Outbound (proxy)**

***Inbound certificate:***

By default, Dynatrace Managed creates the trusted "Let's Encrypt" certificate and places it within the directory /opt/dynatrace-managed/nginx/conf/ssl.

The client can disable this certificate: Settings > Preferences in the CMC console and disable Managed domain name and SSL certificates.

The client can import their own certificate:

• Copy the /opt/dynatrace-managed/nginx/conf/ssl.

• Import it into the Dynatrace server (node): opt/dynatrace-managed/server/conf/keystore.jks.

• Also import it into the AG Embedded: opt/dynatrace-managed/security-Gateway/config/keystore.jks.

For updates, even with a cluster of multiple nodes: done only via WebUI. A general button for update, for example.

***Outbound (proxy):***

Here, the client will need to update the certificate on each node of the cluster (step-by-step). Because the certificate is configured within the installer. And will therefore use the Mission Control for downloading, otherwise manually deploy the zip.

In our case, we will go through this case 2 "Outbound".

# Outbound certificates (proxy)

**If transparent proxy or an intermediary who imposes its certificate**

Ideally authorize our Dynatrace certificate at the proxy level and thus send us a valid certificate.

Identify the proxy :

Tester *tracert -d -h* ***maximum\_hops*** *-j* ***host-list*** *-w* ***timeout target\_host (mesurer le TTL et voir où ça coince).***

Here are the commands to check as a prerequisite:

* curl -k -v [https://mcsvc.dynatrace.com](https://mcsvc.dynatrace.com/) --proxyname:port
* openssl s\_client -servername mcsvc.dynatrace.com:443 -connect proxyname:port (if installed) ==
* possibly test if the server can host several domain names behind an IP (eg: a NAT IP). The objectif is to force the correct assignment of the certificate based on the domain name
* Check the content of the certificate key CA and CRT :

*echo -n | openssl s\_client -connect proxyname:8080 \ | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >*

*/tmp/proxyCert.cert*

Or :

*openssl s\_client -proxy hostname:port -showcerts -connect "mcsvc.dynatrace.com:443" < /dev/null 2>/dev/null | sed -n -e '/BEGIN\ CERTIFICATE/,/END\ CERTIFICATE/ p' > /tmp/proxy.certchain.pem*

The other option after thoses check is to setup proxy certificat in the TrustStore (keystore):

[Add an SSL certificate to Dynatrace Managed cluster TrustStore | Dynatrace Docs](https://www.dynatrace.com/support/help/managed-cluster/configuration/how-to-add-a-certificate-to-server-trust-store#add-a-custom-certificate-to-the-cluster-node-truststore)

As a reminder of the strong recommendation when deploying the certificate (which was already done initially):

directly download the SSL certificate on the master node of the cluster and thus avoid from the browser

any interception by proxy, “ping effect”…  
*openssl s\_client -proxy hostname:port -showcerts -connect "mcsvc.dynatrace.com:443" < /dev/null 2>/dev/null | sed -n -e '/BEGIN\ CERTIFICATE/,/END\ CERTIFICATE/ p' > /tmp/proxy.certchain.pem*

[Install your own SSL certificate for a cluster node | Dynatrace Docs](https://www.dynatrace.com/support/help/managed-cluster/installation/install-your-own-ssl-certificate#install-your-trusted-certificate-on-a-dynatrace-cluster-node)

1. Conversion of the certificate to PEM format (have Openssl on the machine)   
   (if necessary explanation on the preference of formats but at Dynatrace PEM [A SSL Certificate File Extension](https://comodosslstore.com/resources/a-ssl-certificate-file-extension-explanation-pem-pkcs7-der-and-pkcs12/) [Explanation: PEM, PKCS7, DER, and PKCS#12 - Comodo SSL Resources (comodosslstore.com)](https://comodosslstore.com/resources/a-ssl-certificate-file-extension-explanation-pem-pkcs7-der-and-pkcs12/))

*openssl x509 -in certificatename.cer -outform PEM -out certificatename.pem*

*--network-proxy-cert-file*

1. Deployment and store in the keystore (trusted CA):

*/opt/dynatrace-managed/installer/reconfigure.sh --network-proxy-cert-file <path-to-customers-cer-file>*

Check the content of the CA and CRT certificate key:

echo -n | openssl s\_client -connect proxyname:8080 \ | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >

/tmp/proxyCert.cert

Last step: if several nodes make up the cluster

the command

## reconfigure.sh --network-proxy-cert-file <path-to-customers-cer-file>

allows you to put the certificate on each node, so this command is executed on each of the nodes.

**\*\*\* The encountered issue pertains to the OS Patching from Redhat 8.4 to 8.8.**

The certificates provided by SAFRAN (cacerts) are available only in the p7c format, which is not supported for conversion directly.

Therefore, the following commands were executed to convert them into the p7b format and then to the PEM format accepted by the Dynatrace cluster.

On Windows: Rename P7C to P7B, then open and convert to DER.

openssl x509 -inform der -in SAFRANInterceptorRootCA2.der.cer -out SAFRANInterceptorRootCA2.pem

openssl x509 -text -in SAFRANInterceptorRootCA2.pem | less

mv SAFRANInterceptorRootCA2.pem /etc/pki/ca-trust/source/anchors/SAFRANInterceptorRootCA2.20240515.pem

chmod 755 /etc/pki/ca-trust/source/anchors/SAFRAN\*

update-ca-trust enable

update-ca-trust extract

Then, the following command was used to test:

curl -v --cacert /etc/pki/ca-trust/source/anchors/SAFRANInterceptorRootCA2.20240515.pem --proxy vipsafr1.safran:8080 -L https://mcsvc.dynatrace.com:443/

This command utilizes the converted certificate (SAFRANInterceptorRootCA2.20240515.pem) to make a request to https://mcsvc.dynatrace.com:443/ via the specified proxy (vipsafr1.safran:8080).

# ANNEXE

<https://docs.dynatrace.com/managed/managed-cluster/configuration/how-to-add-a-certificate-to-server-trust-store>

[Convert certificate from p7c to cer - Stack Overflow](https://stackoverflow.com/questions/3192992/convert-certificate-from-p7c-to-cer)

[SSL Converter - Convert SSL Certificates to different formats (sslshopper.com)](https://www.sslshopper.com/ssl-converter.html)