

OpenText Centralized Certificate Management

August 2023

In an OES environment, digital certificates play a crucial role in securing communications within and across the network. The certificate can be signed and issued by eDirectory CA, your own organizational CA or a third-party CA.

The self-signed server certificate produced by YaST is the default configuration for a few of the services that offer secure communication. Consider adopting eDirectory server certificate or a CA-signed certificate in place of self-signed certificates because they offer greater security and trust than the former.

With many services on OES using certificates, following are the problems that are faced:

- ♦ Self-signed certificates offer a minimal level of security and trust.
- ♦ Certificate expiration:
 - ♦ Services are suspended.
 - ♦ The OES services are not trusted by the clients.
- ♦ The administrator is not notified prior to expiration. Therefore, difficult to prevent certificate expiration.
- ♦ No details of the services using the certificates, their path and format.
- ♦ Insufficient documentation.

We have implemented the following to address all certificate-related issues:

- ♦ By default, all services on OES 23.4 are configured to use eDirectory server certificates.
- ♦ New component help in certificate management on OES

Centralized certificate management helps administrators in managing the certificate lifecycle. The features are:

- ♦ Mail alerts informs the administrator of the certificates' impending expiration.
- ♦ Indicates where each service's certificates can be found.
- ♦ Indicates the certificate's type, such as whether it is self-signed or CA-signed.
- ♦ Indicates whether the certificates are still valid.
- ♦ Replaces invalid or out-of-date certificates.
- ♦ A browser-based tool (Unified Management Console, or UMC) that enables remote management of certificates across servers will be available in the upcoming releases.

Installing Centralized Certificate Management Binaries

Beginning with OES 23.4 release, the `oes-cert-mgmt.rpm` will be installed on the OES server by default.

At `/opt/novell/oes-cert-mgmt/bin`, you will find all the executables that you need to list the certificates, replace certificates and configure services to use new certificates.

To receive alerts for expiry of certificates, modify the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` file.

Detailed information is provided in the Usage of Commands section.

Upgrading to OES 23.4 Server

On upgrading to OES 23.4 server, `oes-cert-mgmt.rpm` is installed with the base rpms.

At `/opt/novell/oes-cert-mgmt/bin`, you will find all the executables that you need to list the certificates, replace certificates and configure services to use new certificates.

To receive alerts before expiry of certificates, modify the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` file.

After upgrading to OES23.4 version, it is recommended to move services using self-signed certificates to eDirectory server certificate or any other CA signed certificate.

If services continue using self-signed certificate, you will not be able to take the full advantage of the tool. As the tool does not support self-signed certificates, on expiry, you will not be able to reconfigure the services to use a new self-signed certificate.

Path to Important Certificate Management Files

Table 1 *Certificate Management Files*

Name	Location
Binaries	<code>/opt/novel/oes-cert-mgmt/bin/</code>
Alert and Log level configuration file	<code>/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf</code>
Log file	<code>/opt/novel/oes-cert-mgmt/bin/</code>

Usage of Commands

- ♦ [“Listing of Certificates Used by OES Services” on page 3](#)
- ♦ [“Configuring Alerts For Certificate Expiry” on page 3](#)
- ♦ [“Reconfiguring Certificates” on page 3](#)

Listing of Certificates Used by OES Services

View certificate details of all the OES services configured on the server where the script is executed.

Two json format files record the information – Based on services (`certlist-service.json`) and other based on certificates (`certlist-cert.json`). These files capture all the certificate attributes such as certificate path on the OES server, and details of the certificate like subject, issuer, expiry date and whether the certificate is self-signed or CA Signed. For every certificate, details of the services are also listed.

Service-specific Format

On OES terminal, execute `/opt/novel/oes-cert-mgmt/bin/oes_cert_mgmt_list --list service`. The output of this command is written to the `/var/opt/novell/oes-cert-mgmt/certlist-service.json` file.

Certificate-specific Format

On OES terminal, execute `/opt/novel/oes-cert-mgmt/bin/oes_cert_mgmt_list --list certificate`. The output of this command is written to the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file.

Configuring Alerts For Certificate Expiry

The administrator receives an alert about the expiry of the certificates on 15th of every month through an email 90 days in advance. The system date is considered for identifying expiry status of the certificates. Details of expired certificates or certificates getting expired within 90 days are available in json format.

To receive an alert, do the following:

- 1 On the OES terminal, modify the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` file.
- 2 Modify the following attributes:

```
Mail-alert=Yes
Mail-alert-to-address=abc@gmail.com
Mail-alert-from-address=abc@gmail.com
Log-level=DEBUG or INFO or ERROR
```

It is recommended to mention your email address in the from attribute too, else specifying server name might be treated as spam by the mailbox.

- 3 An email is sent to the mailbox of the address specified in the "Mail-alert-to-address" attribute. The email is sent only when one or more certificates are expiring within 90 days. The details are attached in the `certificate.json` file.

Reconfiguring Certificates

Using the command `/opt/novel/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig`, an admin can reconfigure services to use any CA-signed certificate. Listed below are the options supported for reconfiguration.

- ♦ **certchange**: Replace the certificate of all services with a new certificate.
- ♦ **reconfig**: Reconfigure selected services to use a new certificate.
- ♦ **edircertchange**: Replace eDirectory server certificate used by all the services with a new certificate.

- ♦ **movetoedircert:** Reconfigure services to use eDirectory Server Certificate. On upgrade, all the services that are using self-signed certificate will use eDirectory server certificate by using this command.

Examples

The path and certificate names specified are for example purpose and might not be the actual names or path of the certificates.

Example 1

Third party CA certificate is expired or corrupted and needs to be replaced with a new certificate.

The location of the expired certificate could be `/etc/ssl/servercerts/` that includes both the `.pem` files for server certificate and private key of the certificate. Admin copies the new certificate to a temporary location `/etc/opt/novell/oescerts` that includes both the `.pem` files for the new server certificate and private key. The location of the CA certificate `/etc/ssl/certs/` that includes the `.pem` file.

To reconfigure all the services with a new certificate, do the following:

- 1 On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig --operation certchange --currentcert etc/ssl/servercerts/ oescert.pem --currentcertkey etc/ssl/servercerts/oescertserverkey.pem --newcert /etc/opt/novell/oescerts/oesnewservercert.pem --newprivatekey /etc/opt/novell/oescerts/oesnewcertkey.pem --newcacert /etc/ssl/certs/CACert.pem --restart yes`

Success message is displayed. For more details, refer to the `/var/opt/novel/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

All the services will be restarted and the services on this server will start using the new certificate. To restart the services later, you can specify `--restart no`. To apply the new certificate, you must restart the services.

The `/etc/ssl/servercerts/oescert.pem` and `/etc/ssl/servercerts/oescertkey.pem` content is replaced with `oesnewservercert.pem` and `oesnewcertkey.pem`. The existing certificates that are getting replaced are backedup with `.cert-mgmt.bak` extension.

Example 2

The OES services are using eDirectory certificate. The organization policy has changed and a few of the services (SFCB and Apache) need to consume the new certificates provided by the third-party CA.

The supported list of services for `--listofservices` attribute is Apache, SFCB, FTP, iPrint, NRM, Postgres, CIS-Configuration, CIS-Core, CIS-Infra, CIS-Agent, CIS-DB, CIS-CloudGateway, Telemetry-Server and Telemetry-Agent.

The location of the new certificate is `/etc/opt/novell/certs` that includes both the `.pem` files for server and key. The location of the CA certificate `/etc/ssl/certs/` that includes the `.pem` file.

To forcibly make the existing services to use a new certificate, do the following:

- 1 On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig --operation reconfigure --newcert /etc/opt/novell/certs/oesservercert.pem --newprivatekey /etc/opt/novell/certs/oesserverkey.pem --newcacert /etc/ssl/certs/CompanyCACert.pem --listofservices sfc,apache --restart yes`

SFCB and Apache services will be reconfigured to use the new certificate signed by the 3rd party CA and the services will be restarted automatically. To restart the services later, you can specify `--restart no`. To apply the new certificate, you must restart the services.

Success message is displayed. For more details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

Example 3

eDirectory certificate is expired or corrupted. To reconfigure all the services using eDirectory certificate with a new eDirectory server certificate, do the following:

- 1 Delete existing eDirectory server certificate files from `/etc/ssl/servercerts` location.
- 2 Admin generates a new eDirectory server certificate.
- 3 Restarts eDirectory service so the new certificates are copied to the `/etc/ssl/servercerts` location.
- 4 On the OES terminal, execute the command `/opt/novell/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig --operation edircertchange --restart yes`

All the services will be restarted and the services on this server will start using the new eDirectory server certificates from `/etc/ssl/servercerts` location.

To restart the services later, you can specify `--restart no`. To apply the new certificate, you must restart the services.

Success message is displayed. For more details, refer to the `/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log` file.

Example 4

On upgrading services from OES 2023 to OES 23.4 server, it is recommended for services to use eDirectory server certificate or any CA signed certificate instead of self-signed certificate.

On OES 2023 server, SFCB and Postgres services are using self-signed certificate. Perform the following steps, so the services can use eDirectory server certificate.

- 1 Upgrade OES 2023 server to OES 23.4 server.
- 2 Verify the services that use self-signed certificate.
 - 2a On the OES terminal, execute the `/opt/novell/oes-cert-mgmt/bin/oes_cert_mgmt_list -list certificate`

In the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file, the `"certType": "self-signed"` for SFCB and Postgres.

3 Modify the certificates to use eDirectory server certificate.

- 3a** On the OES terminal, execute the command `/opt/novel/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig --operation movetoedircert --listofservices sfcb,Postgres --restart yes`

Success message is displayed for restarting the SFCB and Postgres services. Also, a message stating that selected services are moved to eDirectory server certificate is displayed.

4 Verify SFCB and Postgres are using eDirectory server certificate.

- 4a** On the OES terminal, execute the `/opt/novel/oes-cert-mgmt/bin/oes_cert_mgmt_list --list certificate`

In the `/var/opt/novell/oes-cert-mgmt/certlist-cert.json` file, the `"certType": "CA-signed"` for SFCB and Postgres.

Legal Notice

Copyright 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.