OpenText Centralized Certificate Management

August 2023

Digital certificates are essential for securing network-wide and intranet communications in an OES environment. The certificate can be signed and issued by an eDirectory Certificate Authority (CA), your organizational CA or a third-party CA.

Until OES 2023, some services that provide secure communication have their default settings configured to use a self-signed server certificate created by YaST. Instead of using self-signed certificates, we recommend, you use an eDirectory server certificate or a CA-signed certificate because they provide more security and trust than the former. For more information on eDirectory Certificate Server, see Understanding the Certificate Server (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/b1j4t6zc.html) in the NetIQ eDirectory Administration Server (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html)

The following issues arise because many OES services need certificates:

- Self-signed certificates offer a minimal level of security and trust.
- Certificate expiration:
  - Services are stopped.
  - The OES services are not trusted by the clients.
- When a certificate is about to expire, the administrator is not notified. As a result, certificate expiration is challenging to avoid.
- No details of 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 notifications notify 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 expired 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

The new rpm `oes-cert-mgmt.rpm` is installed on the server by default with the OES 23.4 release.

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.

Certificate of some of the services is grouped under one service. If certificate is changed for that service, then all services grouped under it will also have the updated certificate.

Table 1 *Service groups for certificate*

Certificate	Services
Apache	NURM, iManager and UMC
eDirectory	NCP

To receive alerts before 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" on page 3.

Upgrading to OES 23.4 Server

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

After upgrading to OES 23.4, it is recommended to move services using self-signed certificates to eDirectory server certificate or any other CA singed 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 2 *Certificate Management Files*

Name	Location
Binaries	`/opt/novell/oes-cert-mgmt/bin/`
Alert and Log level configuration file	`/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf`
Log file	`/var/opt/novell/log/oes-cert-mgmt/oes-cert-mgmt.log`

Usage of Commands

Listing of Certificates Used by OES Services

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

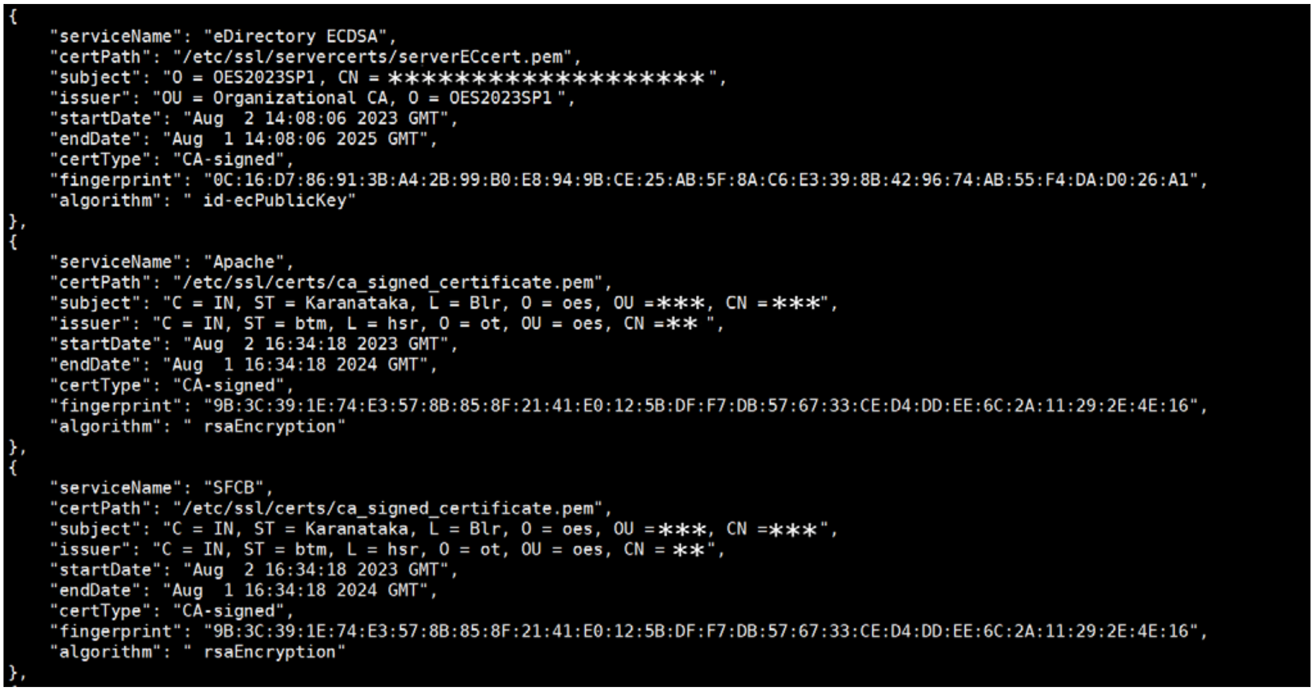
The output of the `--list` command is recorded in the `json` files – Based on services (`certlist-service.json`) and certificates (`certlist-cert.json`). These files capture all the certificate attributes such as certificate path on the OES server, and details of the certificate like subject, issuer, expiry date and whether the certificate is self-signed or CA Signed. For every certificate, details of the services are also listed. The file captures same data in different format in both the files.

Before replacing the `json` files with the output of `--list` command, it is backed up and available at the `/var/opt/novell/oes-cert-mgmt/` location.

Service-specific Format

On OES terminal, execute `/opt/novell/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.

Figure 1 *Certilist-service.json file*

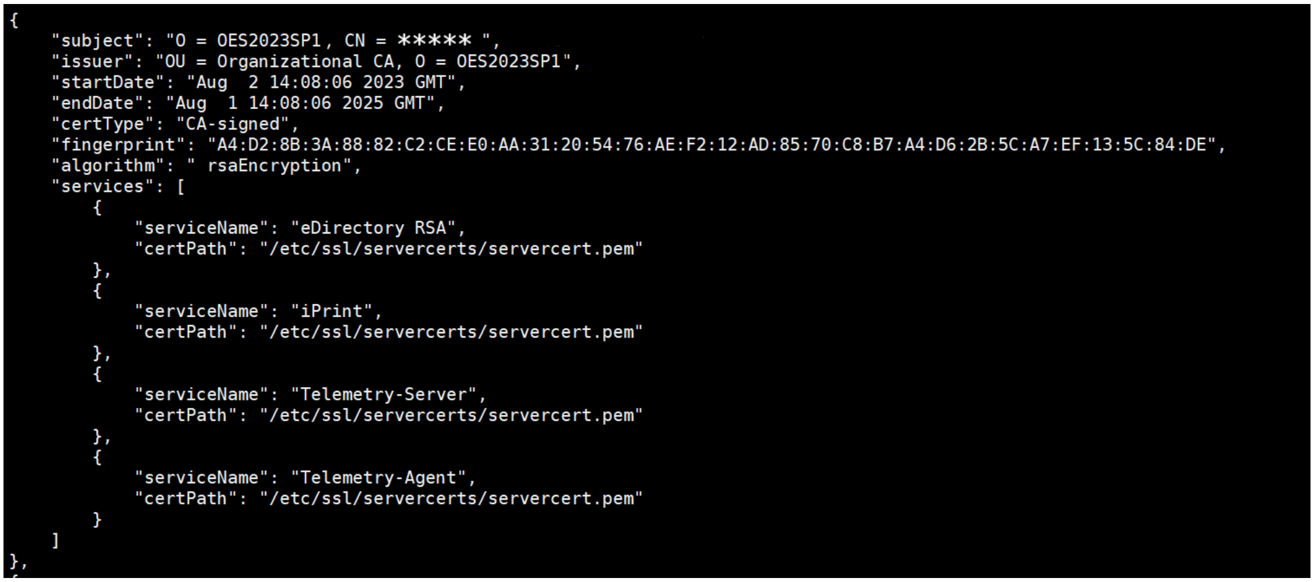


```
{
    "serviceName": "eDirectory ECDSA",
    "certPath": "/etc/ssl/servercerts/serverECcert.pem",
    "subject": "O = OES2023SP1, CN = *******************",
    "issuer": "OU = Organizational CA, O = OES2023SP1 ",
    "startDate": "Aug  2 14:08:06 2023 GMT",
    "endDate": "Aug  1 14:08:06 2025 GMT",
    "certType": "CA-signed",
    "fingerprint": "0C:16:D7:86:91:3B:A4:2B:99:B0:E8:94:9B:CE:25:AB:5F:8A:C6:E3:39:8B:42:96:74:AB:55:F4:DA:D0:26:A1",
    "algorithm": " id-ecPublicKey"
},
{
    "serviceName": "Apache",
    "certPath": "/etc/ssl/certs/ca_signed_certificate.pem",
    "subject": "C = IN, ST = Karanataka, L = Blr, O = oes, OU =***, CN =***",
    "issuer": "C = IN, ST = btm, L = hsr, O = ot, OU = oes, CN =** ",
    "startDate": "Aug  2 16:34:18 2023 GMT",
    "endDate": "Aug  1 16:34:18 2024 GMT",
    "certType": "CA-signed",
    "fingerprint": "9B:3C:39:1E:74:E3:57:8B:85:8F:21:41:E0:12:5B:DF:F7:DB:57:67:33:CE:D4:DD:EE:6C:2A:11:29:2E:4E:16",
    "algorithm": " rsaEncryption"
},
{
    "serviceName": "SFCB",
    "certPath": "/etc/ssl/certs/ca_signed_certificate.pem",
    "subject": "C = IN, ST = Karanataka, L = Blr, O = oes, OU =***, CN =***",
    "issuer": "C = IN, ST = btm, L = hsr, O = ot, OU = oes, CN = **",
    "startDate": "Aug  2 16:34:18 2023 GMT",
    "endDate": "Aug  1 16:34:18 2024 GMT",
    "certType": "CA-signed",
    "fingerprint": "9B:3C:39:1E:74:E3:57:8B:85:8F:21:41:E0:12:5B:DF:F7:DB:57:67:33:CE:D4:DD:EE:6C:2A:11:29:2E:4E:16",
    "algorithm": " rsaEncryption"
},
```

Certificate-specific Format

On OES terminal, execute `/opt/novell/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.

Figure 2 Certilist-cert.json file

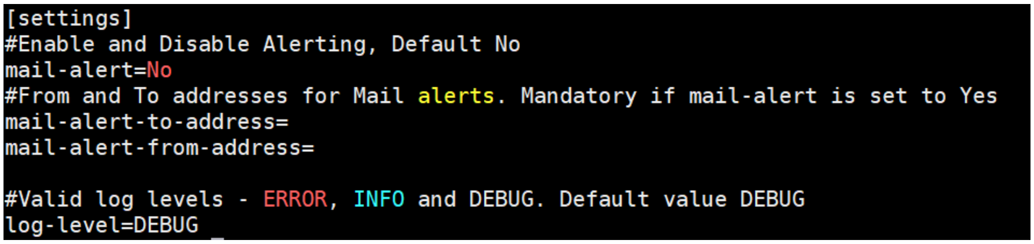


```
{
    "subject": "O = OES2023SP1, CN = ***** ",
    "issuer": "OU = Organizational CA, O = OES2023SP1",
    "startDate": "Aug  2 14:08:06 2023 GMT",
    "endDate": "Aug  1 14:08:06 2025 GMT",
    "certType": "CA-signed",
    "fingerprint": "A4:D2:8B:3A:88:82:C2:CE:E0:AA:31:20:54:76:AE:F2:12:AD:85:70:C8:B7:A4:D6:2B:5C:A7:EF:13:5C:84:DE",
    "algorithm": " rsaEncryption",
    "services": [
        {
            "serviceName": "eDirectory RSA",
            "certPath": "/etc/ssl/servercerts/servercert.pem"
        },
        {
            "serviceName": "iPrint",
            "certPath": "/etc/ssl/servercerts/servercert.pem"
        },
        {
            "serviceName": "Telemetry-Server",
            "certPath": "/etc/ssl/servercerts/servercert.pem"
        },
        {
            "serviceName": "Telemetry-Agent",
            "certPath": "/etc/ssl/servercerts/servercert.pem"
        }
    ]
},
```

Configuration file

- "Configuring Alerts For Certificate Expiry" on page 4
- "Configuring Error Logging" on page 5

Figure 3 oes-cert-mgmt.conf file



```
[settings]
#Enable and Disable Alerting, Default No
mail-alert=No
#From and To addresses for Mail alerts. Mandatory if mail-alert is set to Yes
mail-alert-to-address=
mail-alert-from-address=

#Valid log levels - ERROR, INFO and DEBUG. Default value DEBUG
log-level=DEBUG
```

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.

1a Modify the following attributes:

```
mail-alert=Yes
mail-alert-to-address=abc@gmail.com
mail-alert-from-address=abc@gmail.com
```

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

2 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 specified in the `certificate.json` file.

Configuring Error Logging

To configure the error logging setting for the certificate messages, use the `log-level` parameter in the `/etc/opt/novell/oes-cert-mgmt/oes-cert-mgmt.conf` configuration file.

The severity levels available are ERROR, INFORMATION and DEBUG.

To set the severity level, set the following:

```
log-level=severity_level (DEBUG,INFO OR ERROR)
```

For example,

```
log-level=DEBUG
```

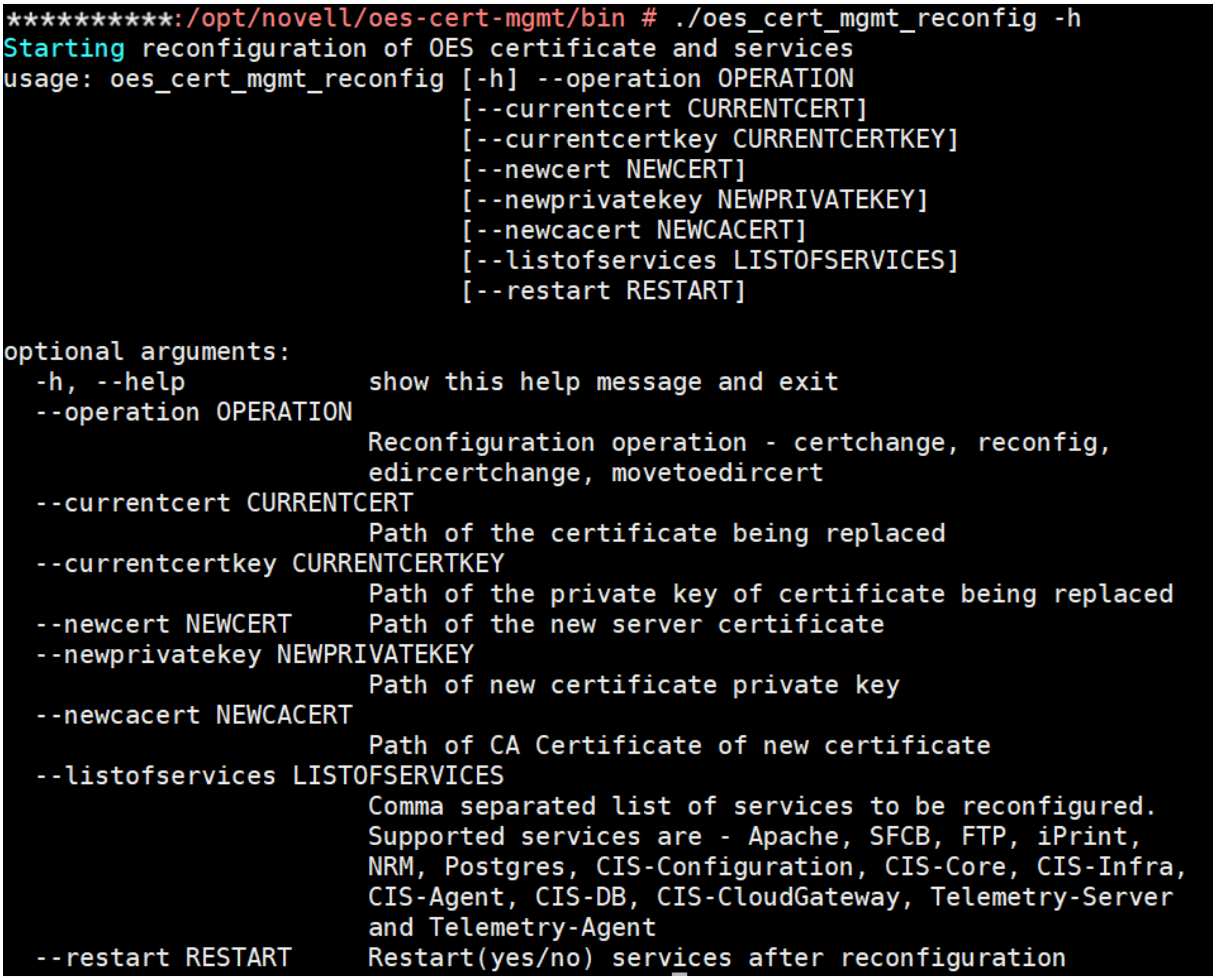
Reconfiguring Certificates

Using the command `/opt/novell/oes-cert-mgmt/bin/oes_cert_mgmt_reconfig`, an admin can reconfigure services to use any CA-signed certificate. The existing certificates are backed up with `.cert-mgmt.bak` extension before being replaced.

Listed below are the options supported for reconfiguration:

- **certchange:** Replace the existing 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.

Figure 4 Certificate Management Command Line Help



```
**********:/opt/novell/oes-cert-mgmt/bin # ./oes_cert_mgmt_reconfig -h
Starting reconfiguration of OES certificate and services
usage: oes_cert_mgmt_reconfig [-h] --operation OPERATION
                              [--currentcert CURRENTCERT]
                              [--currentcertkey CURRENTCERTKEY]
                              [--newcert NEWCERT]
                              [--newprivatekey NEWPRIVATEKEY]
                              [--newcacert NEWCACERT]
                              [--listofservices LISTOFSERVICES]
                              [--restart RESTART]

optional arguments:
  -h, --help            show this help message and exit
  --operation OPERATION
                        Reconfiguration operation - certchange, reconfig,
                        edircertchange, movetoedircert
  --currentcert CURRENTCERT
                        Path of the certificate being replaced
  --currentcertkey CURRENTCERTKEY
                        Path of the private key of certificate being replaced
  --newcert NEWCERT     Path of the new server certificate
  --newprivatekey NEWPRIVATEKEY
                        Path of new certificate private key
  --newcacert NEWCACERT
                        Path of CA Certificate of new certificate
  --listofservices LISTOFSERVICES
                        Comma separated list of services to be reconfigured.
                        Supported services are - Apache, SFCB, FTP, iPrint,
                        NRM, Postgres, CIS-Configuration, CIS-Core, CIS-Infra,
                        CIS-Agent, CIS-DB, CIS-CloudGateway, Telemetry-Server
                        and Telemetry-Agent
  --restart RESTART     Restart(yes/no) services after reconfiguration
```

Examples

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

Example - Replacing Expired or Corrupted Certificate

CA signed 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/novell/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 certificates that are getting replaced are backed up in the same location with `.cert-mgmt.bak` extension.

Example - Reconfiguring Services to Use 3rd party CA Signed Certificate

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 that can be reconfigured to use the new certificate are available with the command line parameter `--listofservices`.

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 reconfig --newcert /etc/opt/novell/certs/oesservercert.pem --newprivatekey /etc/opt/novell/certs/oesserverkey.pem --newcacert /etc/ssl/certs/CompanyCACert.pem --listofservices sfcb,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 - Replacing Expired or Corrupted eDirectory Server Certificate

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 - Moving from Self-Signed Certificates to eDirectory Server Certificate On Upgrade

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/novell/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/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":"CA-signed"` for SFCB and Postgres.

Legal Notice