EVERTRUST

EverTrust OCSP documentation v3.1.3

Installation Guide

EVERTRUST

Table of Contents

1. Introduction

1.1. Description

OCSPd (OCSP daemon) is an OCSP responder compliant with the following RFCs:

- RFC 6960
- RFC 5019

This project is powered up by:

- Akka
- BouncyCastle
- EHCache
- H2 Database
- IAIK PKCS#11 Wrapper
- Kamon
- Play! Framework
- Scala
- NGINX

This document is specific to OCSPd version **3.1.3**.

1.2. Scope

This document is an installation procedure detailing how to install and bootstrap OCSPd on a server running **CentOS/RHEL 6.x/7.x/8.x x64**.

1.3. Out of Scope

This document does not describe how to configure and operate an OCSPd instance. Please refer to the administration guide for administration related tasks.

2. Pre-requisites

This section describes the system and software pre-requisites to install OCSPd.

2.1. Hardware pre-requisites

The minimum requirements for running OCSPd are:

- 2 CPU cores;
- 8 GB of RAM;
- 500 GB of free disk space.

2.2. System pre-requisites

The following elements are considered as system pre-requisites:

- A server running CentOS / RHEL [6-7-8].x x64 with the network configured;
- Access with administrative privileges (root) to the server mentioned above;
- The IP address / DNS Name of one or several NTP server(s);
- The IP address / DNS Name of an SMTP relay;
- The email address of the OCSPd server administrator.

2.3. Software pre-requisites

The following elements are considered as software pre-requisites:

- The OCSPd installation package: `ocspd-3.1.3.noarch.rpm`;
- The NGINX installation package: `nginx-latest.el8.ngx.x86_64.rpm` (latest version of the nginx web server);
- Java 11: The latest Java 11 OpenJDK package (will be installed as a dependency of OCSPd but may required when working offline);

3. Installation Procedure

3.1. Installing NGINX

1. Upload the file `nginx-latest.el8.ngx.x86_64.rpm` through SCP under `/root`;
2. Access the server through SSH with an account with administrative privileges;
3. Install the NGINX web server using the following command:

```
yum localinstall /root/nginx-latest.el8.ngx.x86_64.rpm
```

4. Enable NGINX to start at boot using the following command:

```
systemctl enable nginx
```

5. Stop the NGINX service with the following command:

```
/etc/init.d/nginx stop
```

3.2. Installing the rngd service

1. Access the server through SSH with an account with administrative privileges;
2. Install the `rng-tools` package with the following command:

```
yum install rng-tools
```

3. Configure the `rngd` service with the following command:

```
echo 'EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 10 -W 2048"' >
/etc/sysconfig/rngd
```

4. Enable and start the `rngd` service:

```
systemctl enable rngd
systemctl start rngd
```

3.3. Installing OCSPd

1. Upload the file `ocspd-3.1.3-1.noarch.rpm` through SCP under `/root`;
2. Access the server through SSH with an account with administrative privileges;

3. Install the OCSPd package with the following command:

```
yum localinstall /root/ocspd-3.1.3-1.noarch.rpm
```

NOTE

Installing the OCSPd package will install the following dependencies:

- `dialog`
- `java-11-openjdk-headless`

4. Configuring OCSPd

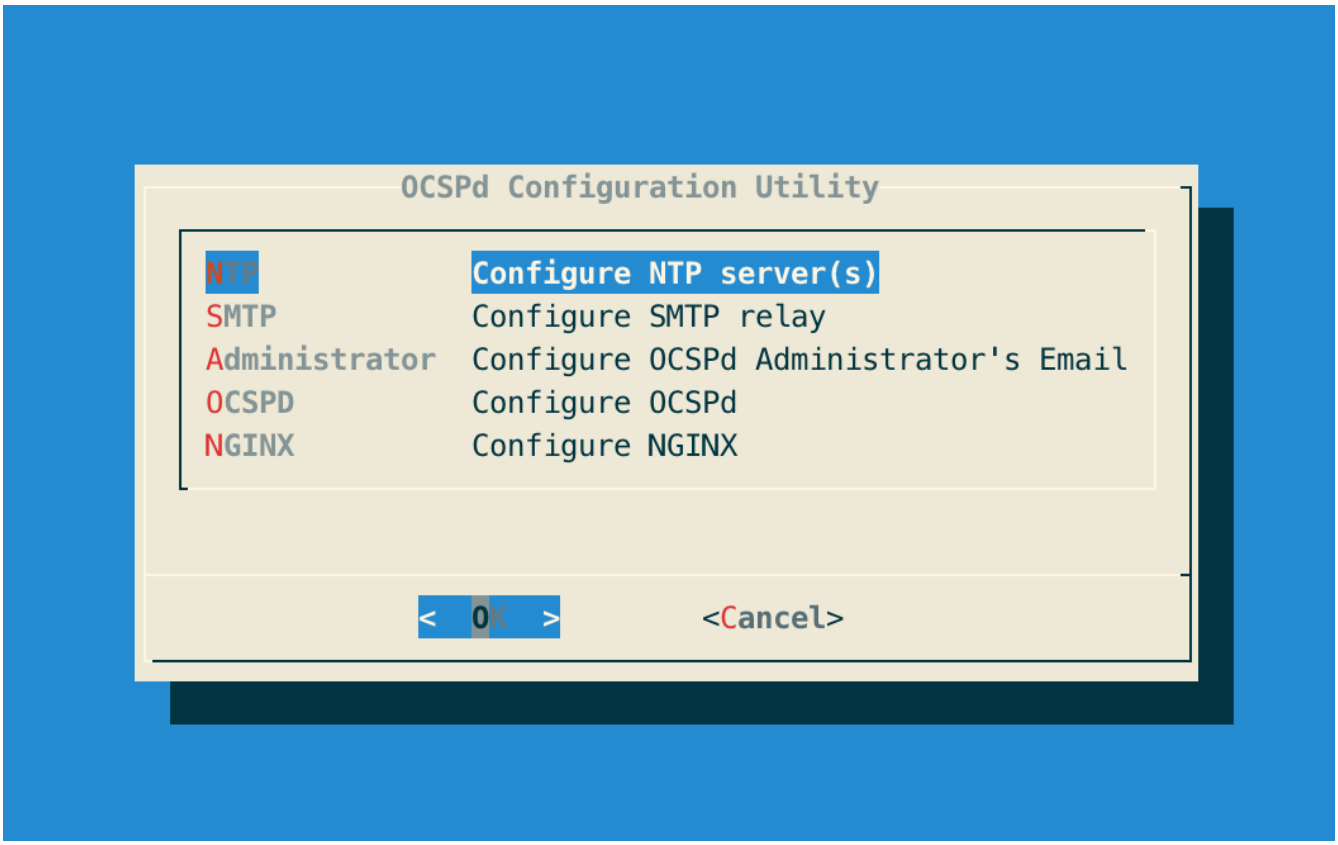
4.1. Configuring the NTP server(s)

Step 1: Access the server through SSH with an account with administrative privileges;

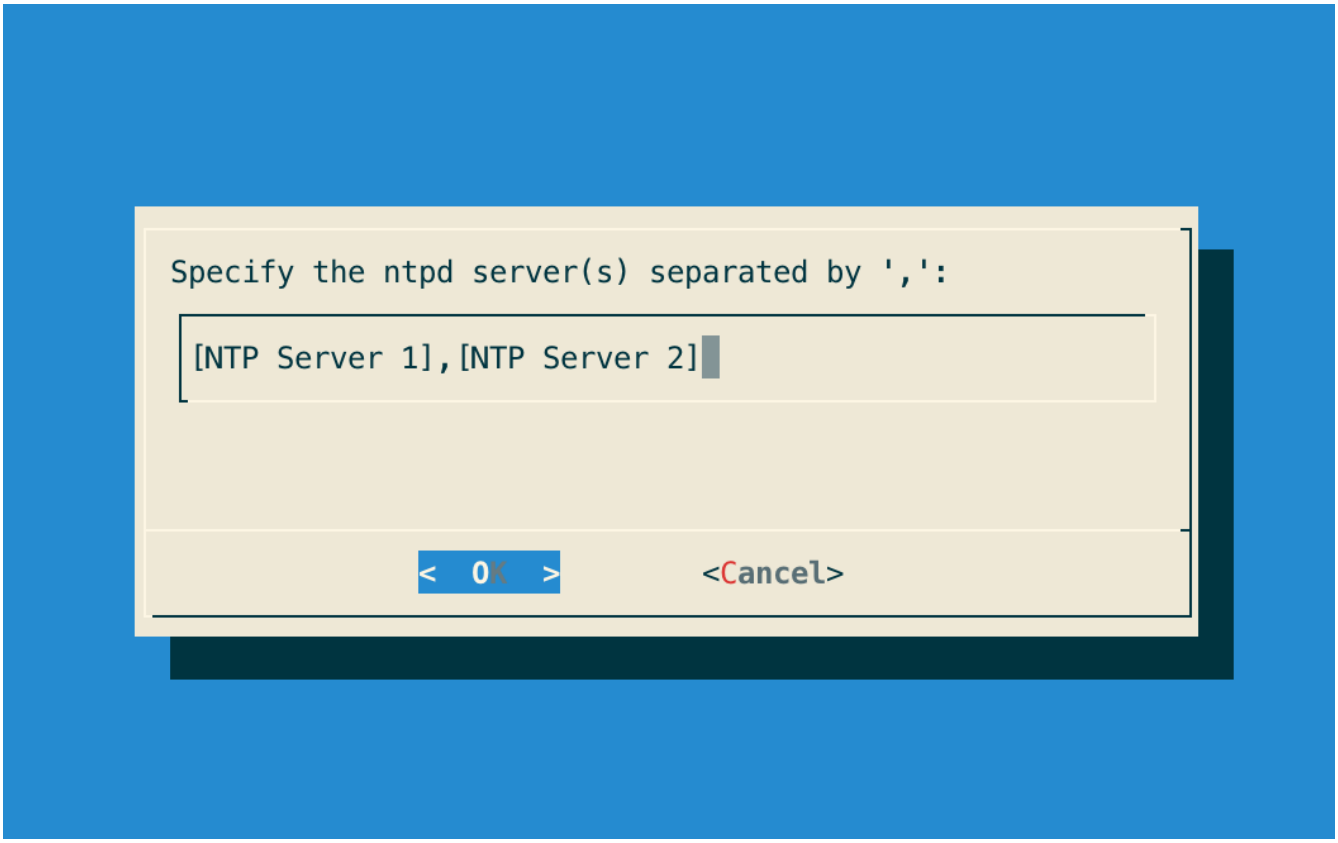
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

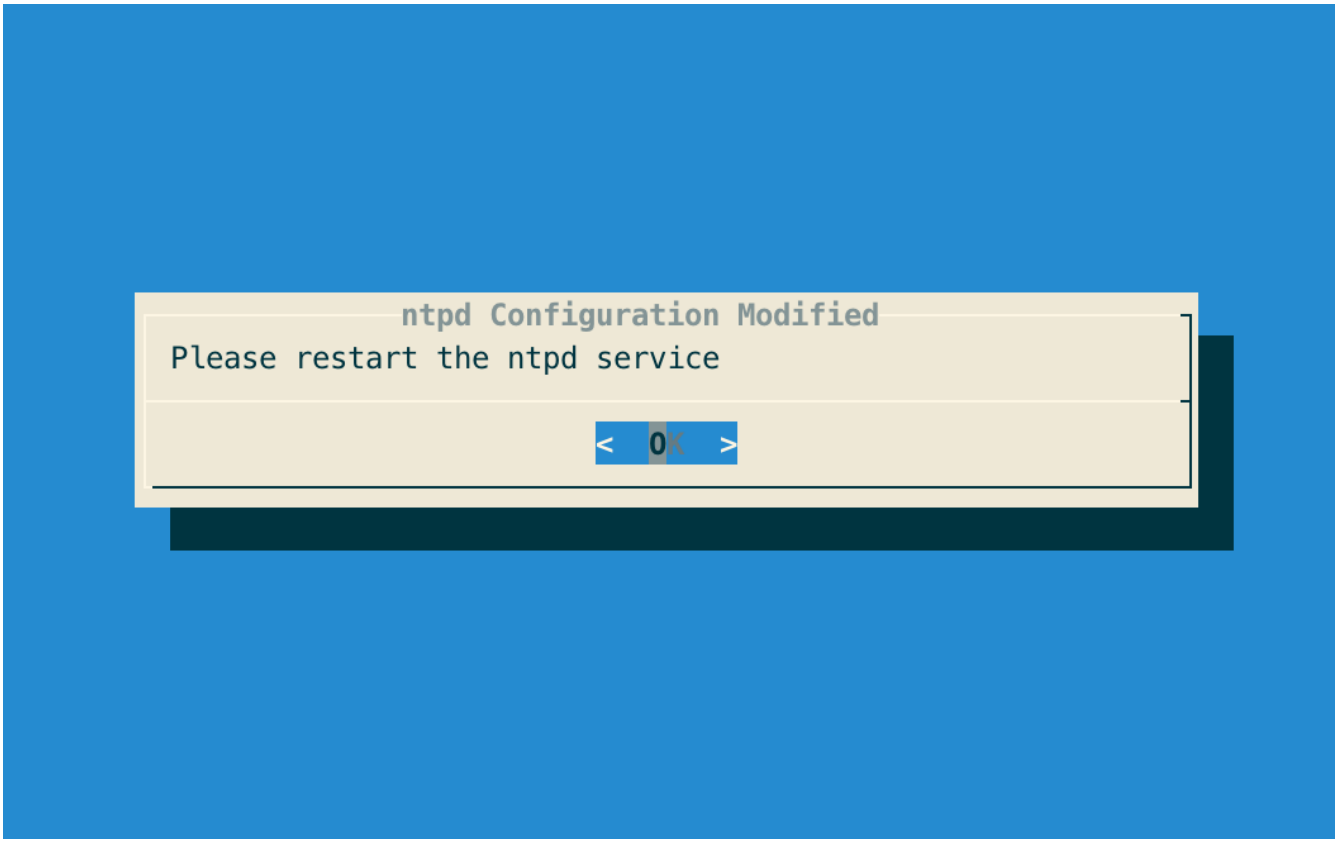
Step 3: In the main menu, select '**NTP**':



Step 4: Specify the list of NTP server(s) separated by ',' and validate:



Step 5: The NTPs configuration is updated:



Step 6: Exit the configuration utility and restart the NTPd service with the following command:

```
# /etc/init.d/ntpd restart
```

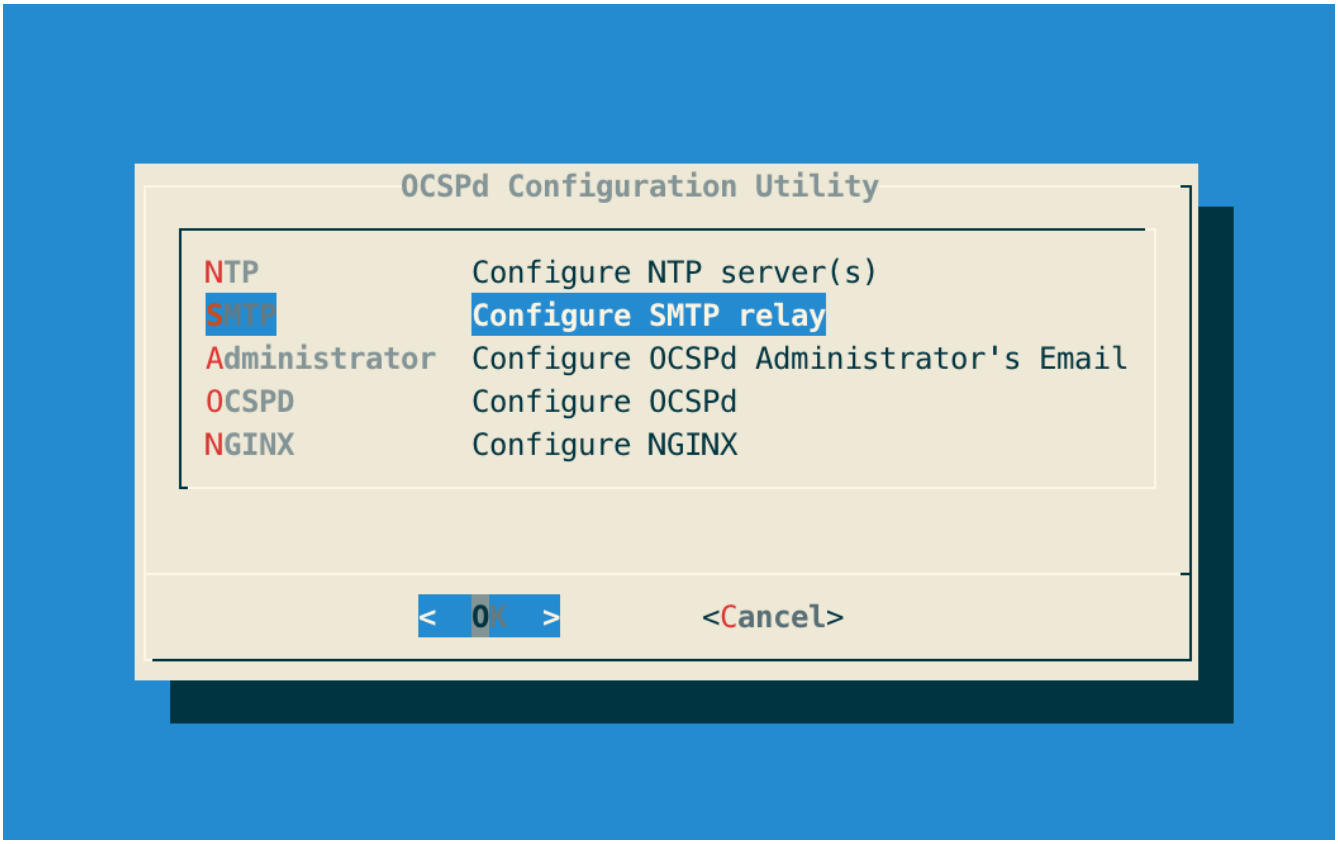
4.2. Configuring the SMTP Relay

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

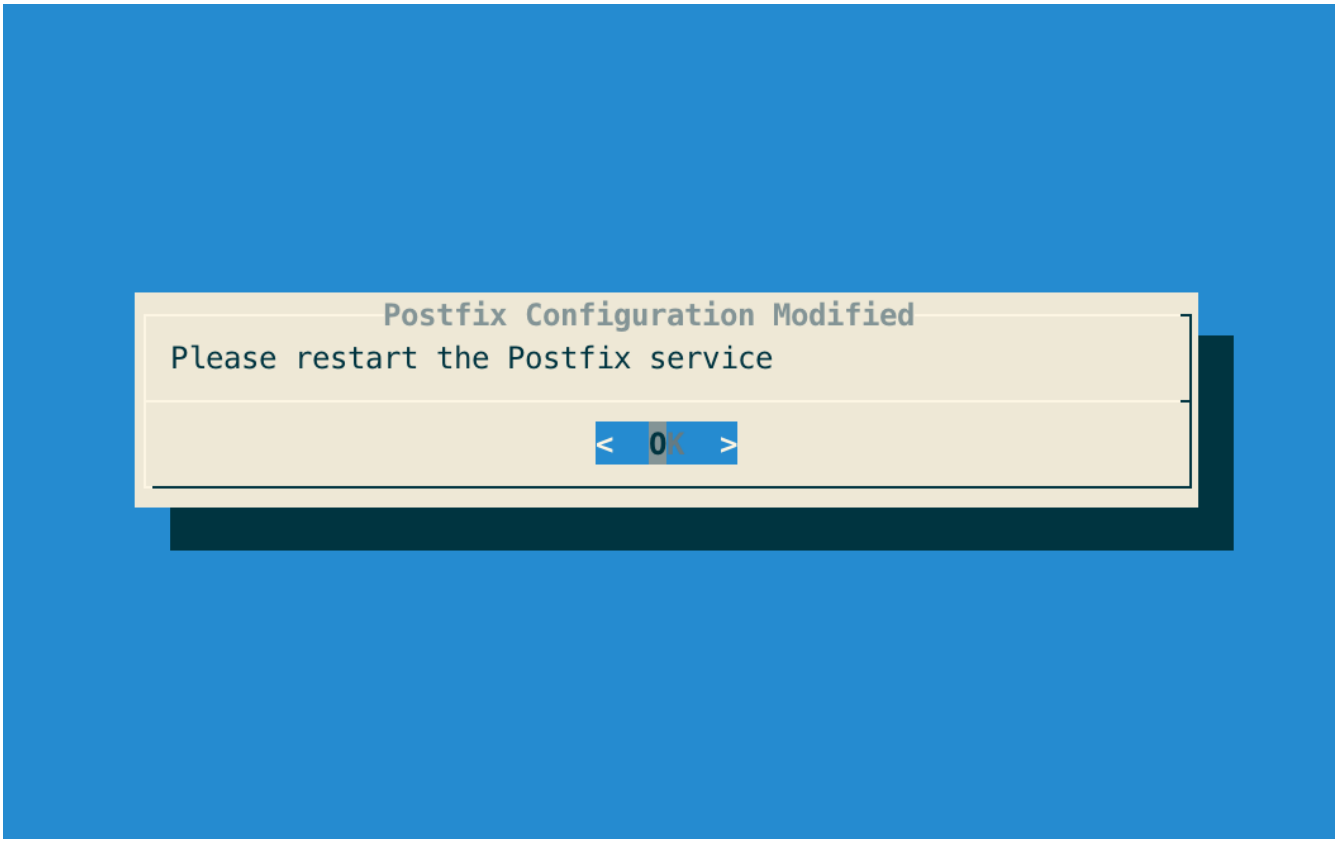
```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**SMTP**':



Step 4: Specify IP address or the DNS name of the SMTP relay and validate:

Step 5: The Postfix configuration is updated:



Step 6: Exit the configuration utility and restart the Postfix service with the following command:

```
# /etc/init.d/postfix restart
```

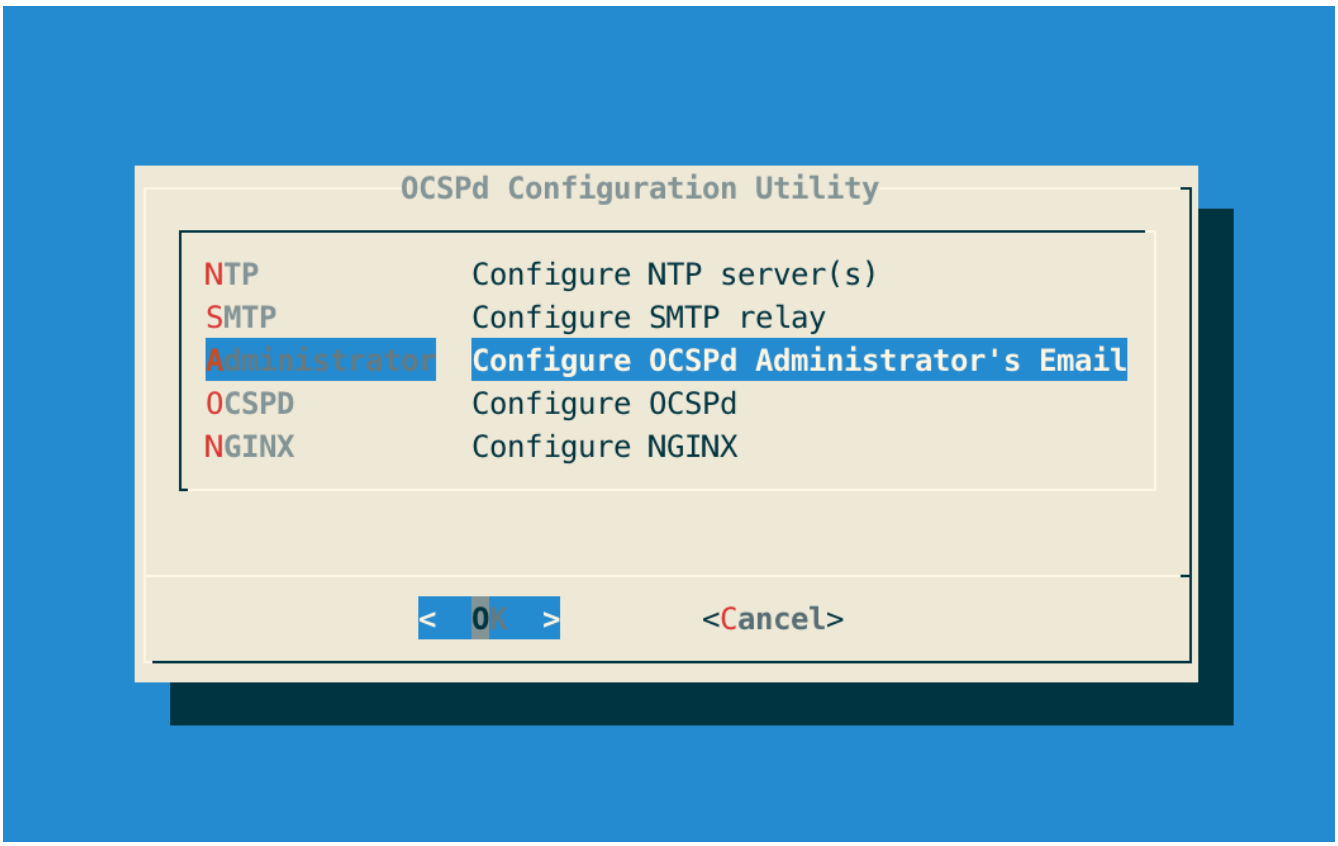
4.3. Configuring the OCSPd Administrator's Email Address

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**Administrator**':



Step 4: Specify the email address of the OCSPd Administrator and validate:

Step 5: Exit the Configuration Utility;

Step 6: Validate the SMTP relay and Administrator Email Address with the following commands:

```
# yum install mailx
# mail -s "Hello OCSPd" root
> Hello From OCSPd
.
```

Step 7: Ensure that the email defined step 4 receives the test email.

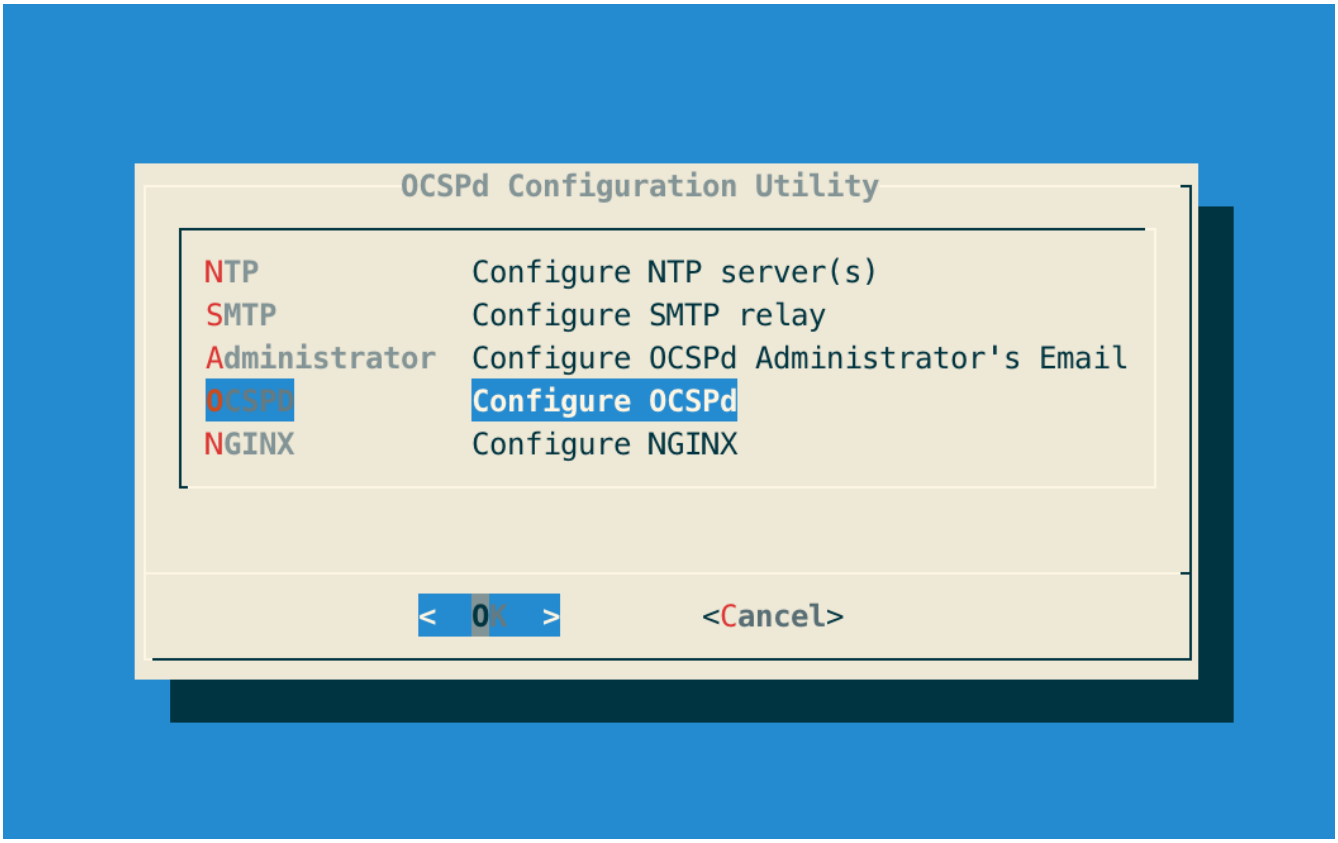
4.4. Configuring the Radius Server

Step 1: Access the server through SSH with an account with administrative privileges;

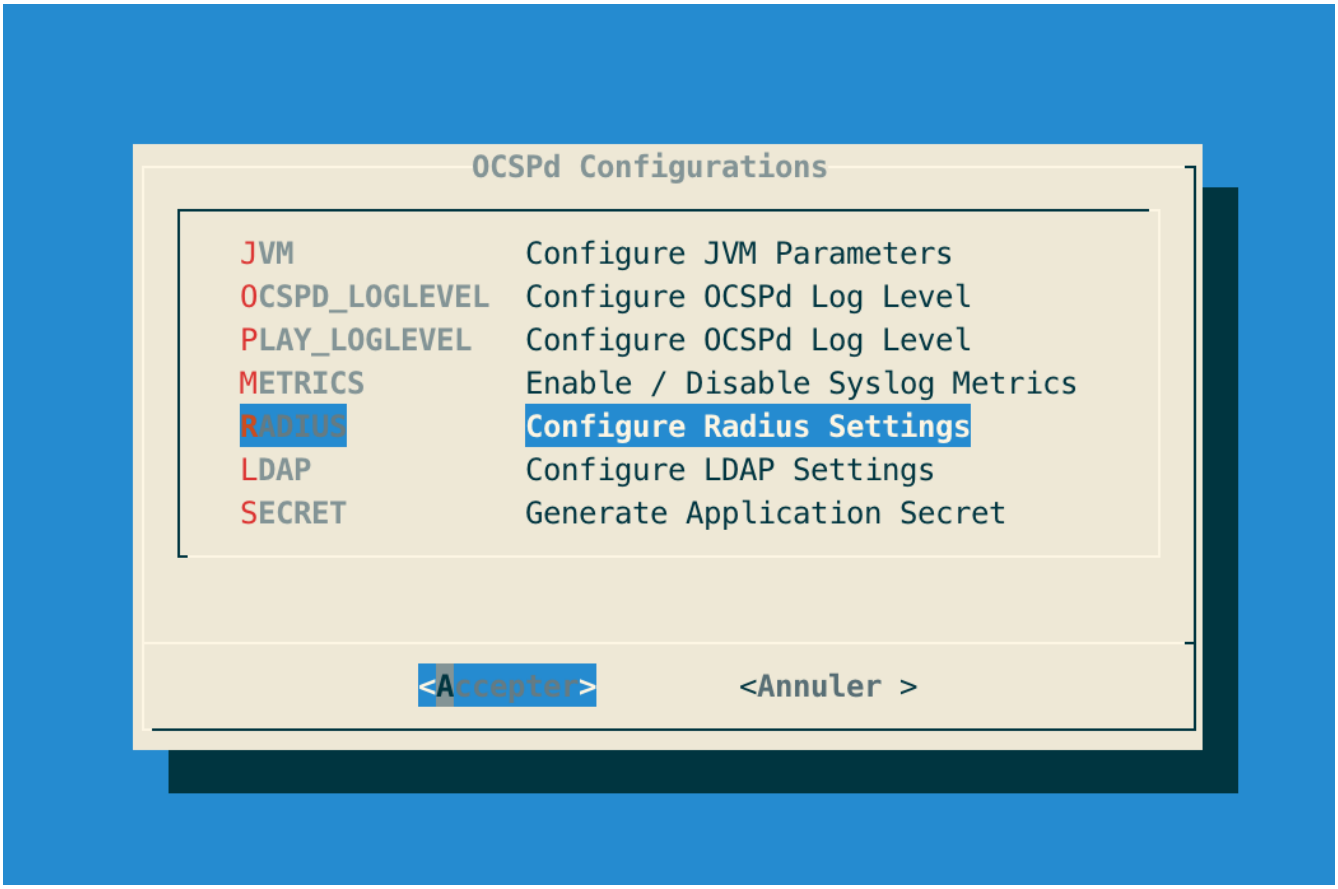
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**OCSPd**':

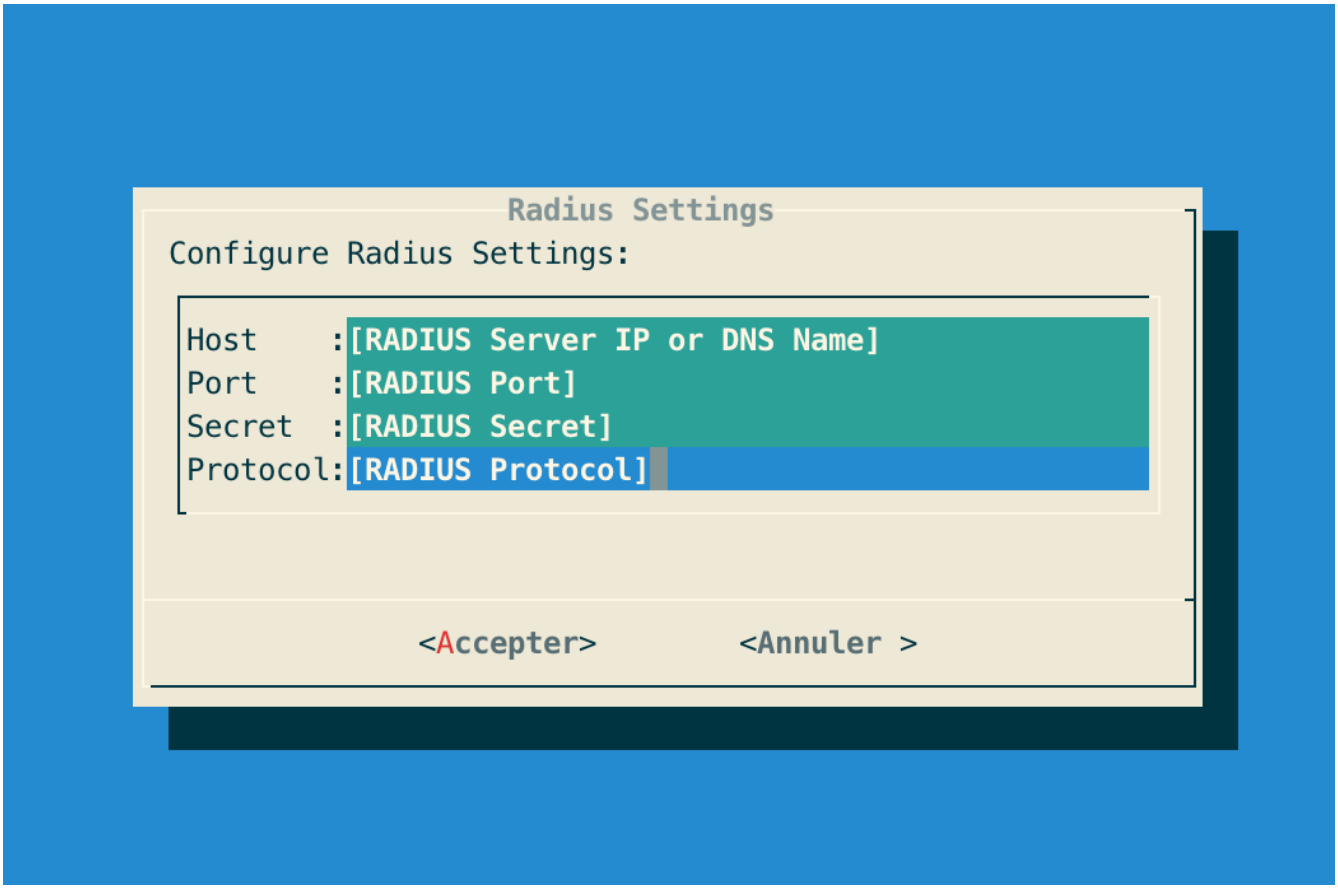


Step 4: In the OCSPd menu, select '**RADIUS**':

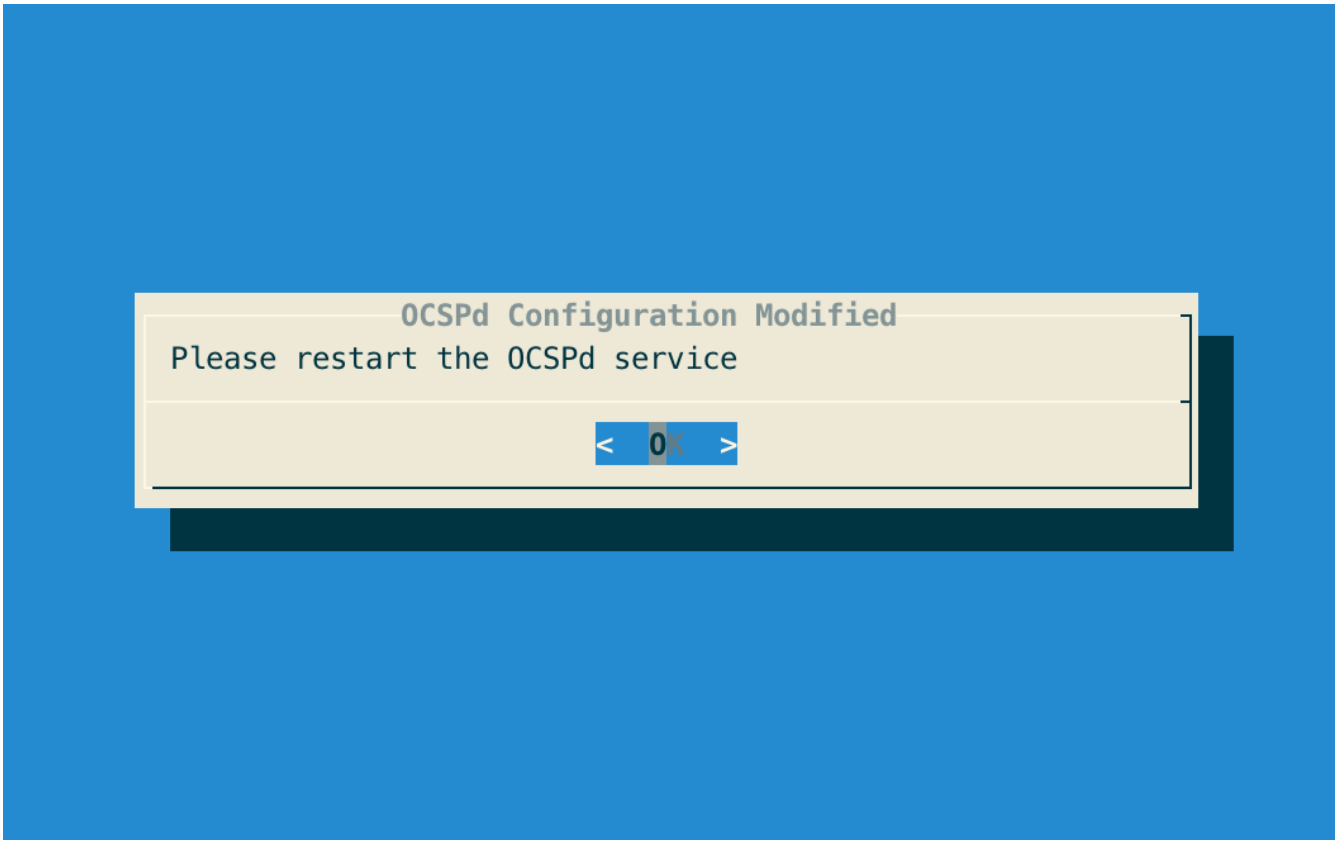


Step 5: Specify the following Radius configuration settings and validate:

NOTE	'CHAP' and 'PAP' protocols are supported by OCSPd.



Step 6: The OCSPd configuration is updated:



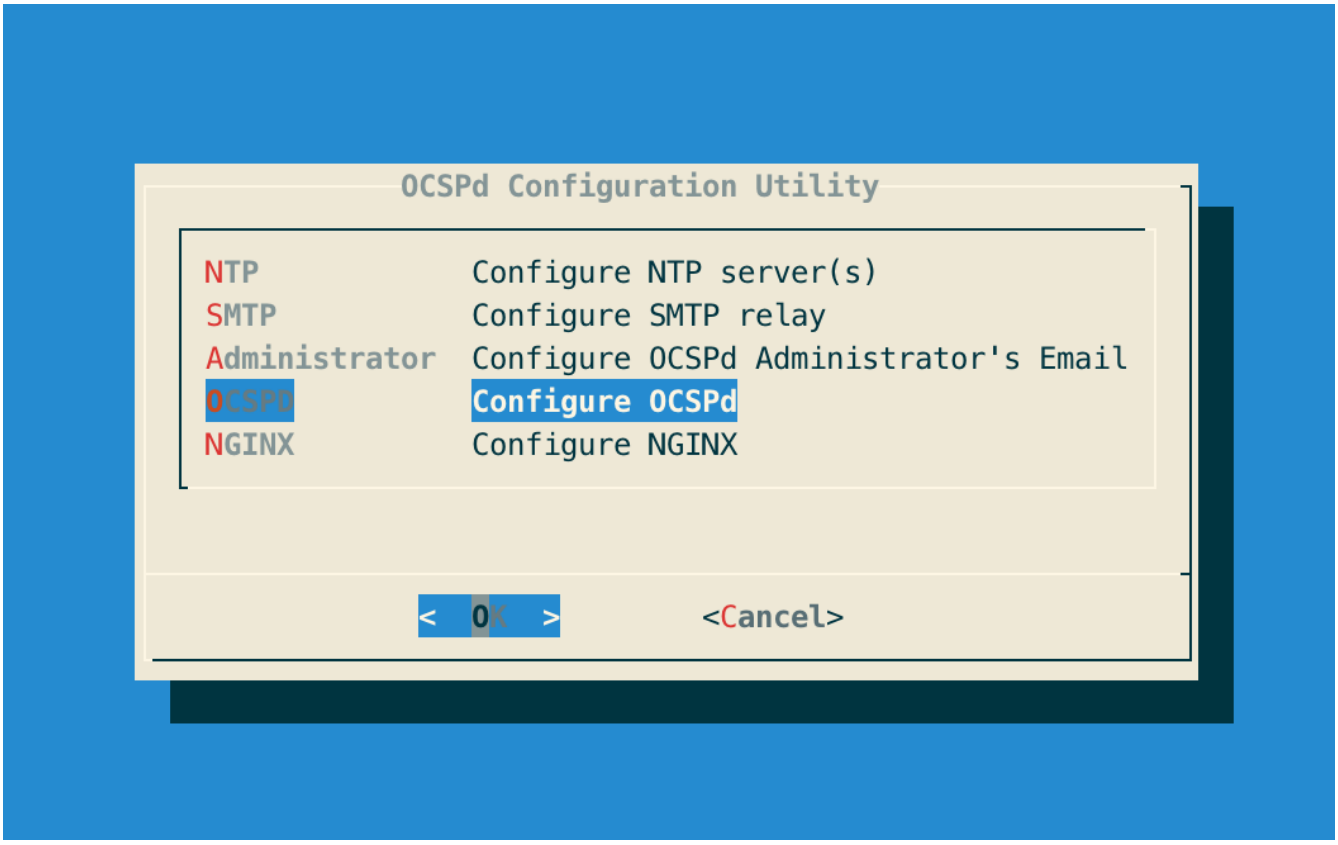
4.5. Configuring the LDAP Server

Step 1: Access the server through SSH with an account with administrative privileges;

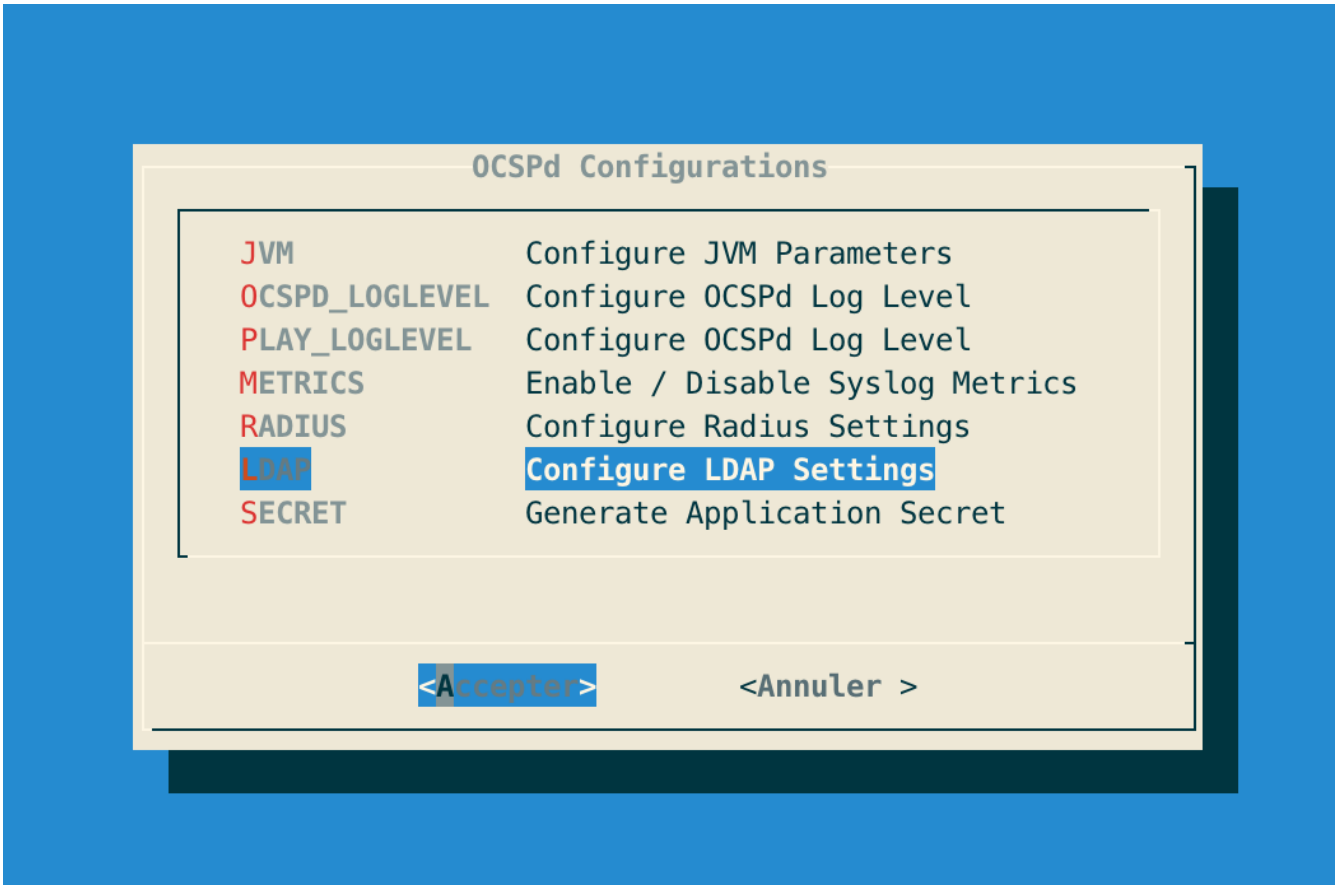
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**OCSPd**':

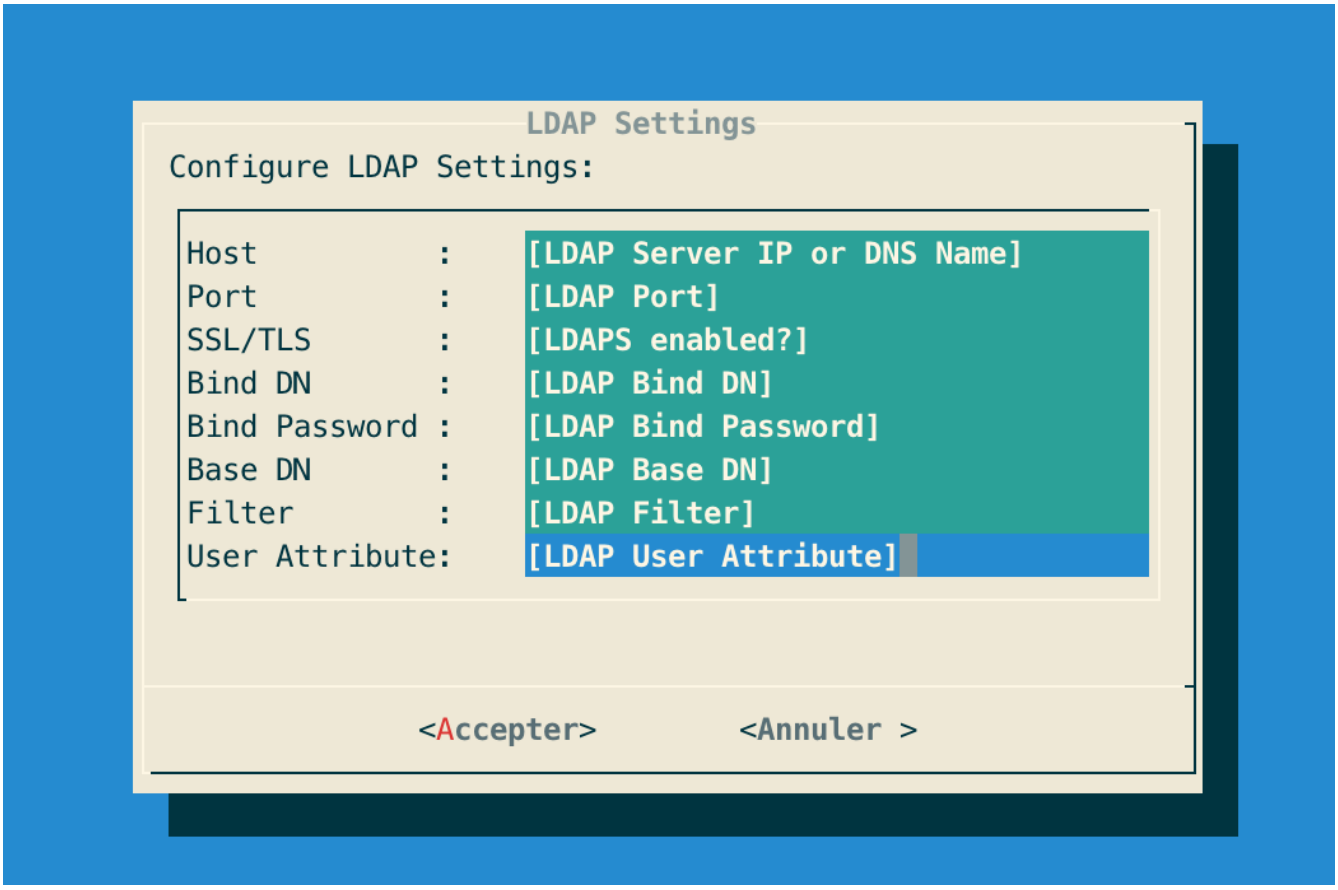


Step 4: In the OCSPd menu, select '**RADIUS**':

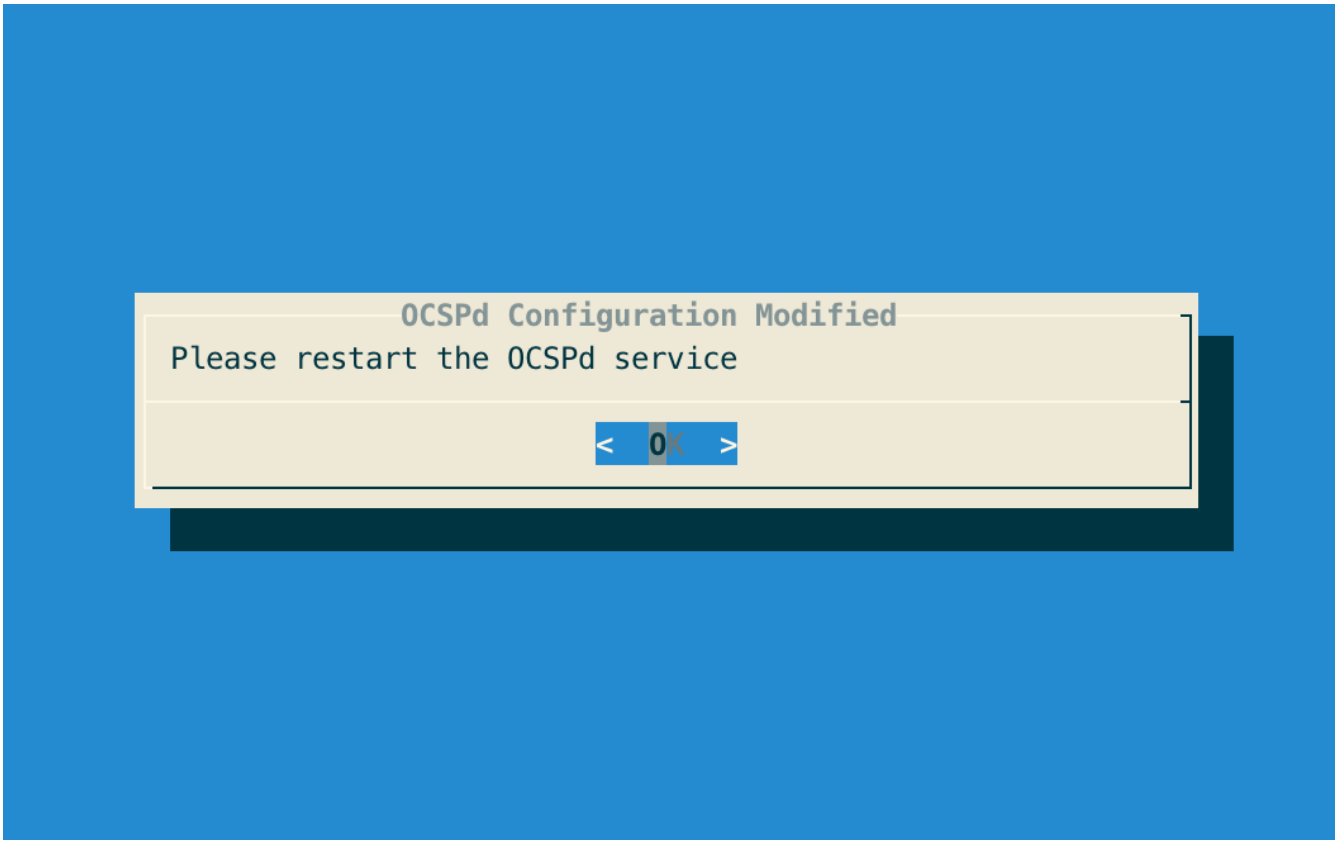


Step 5: Specify the following LDAP configuration settings and validate:

NOTE	By default the LDAP configuration will use port 389 and SSL/TLS 'false'.
NOTE	The filter settings is optionnal.



Step 6: The OCSPd configuration is updated:



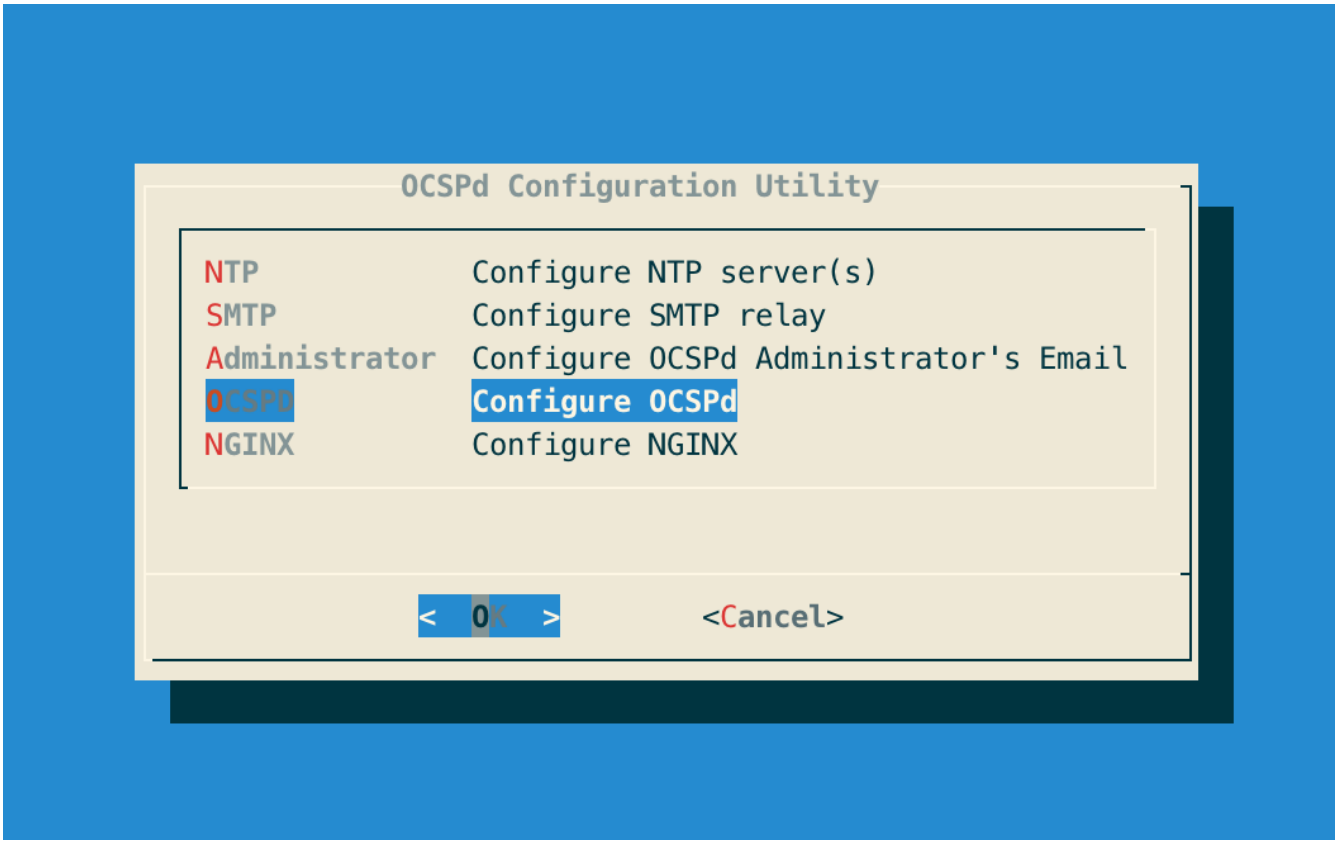
4.6. Generating a new OCSPd Application Secret

Step 1: Access the server through SSH with an account with administrative privileges;

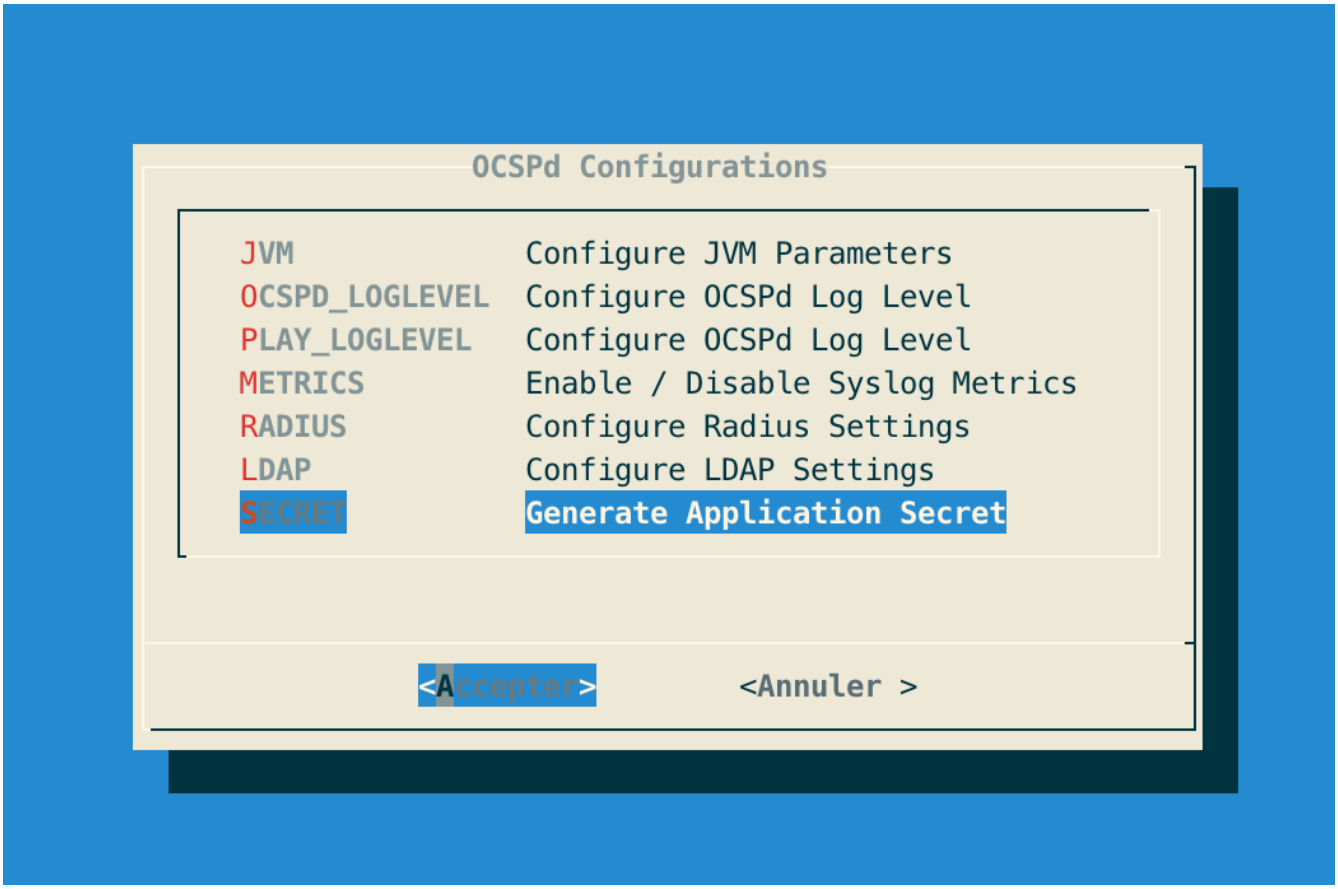
Step 2: Load the OCSPd Configuration Utility with the following command:

```
# /opt/ocspd/sbin/ocspd-config
```

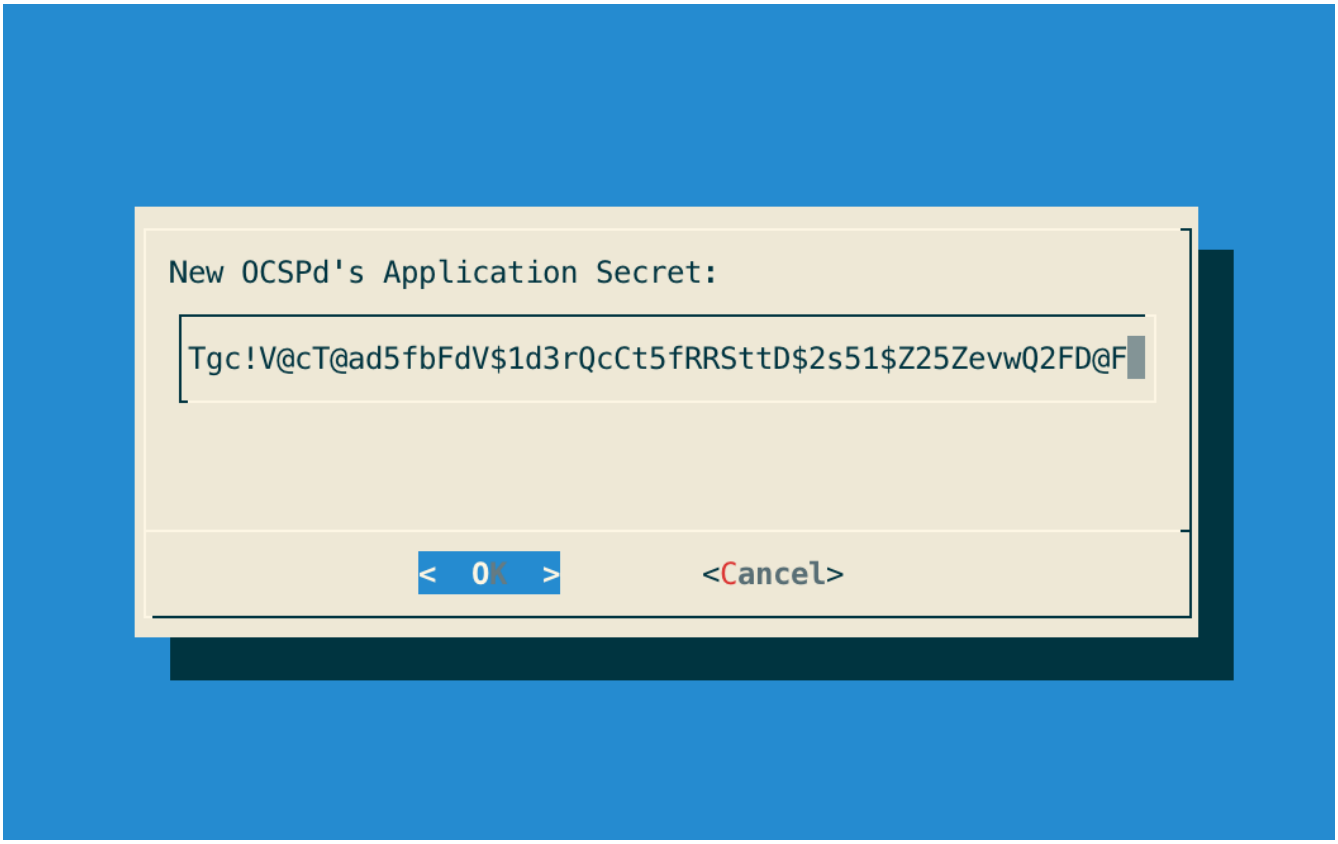
Step 3: In the main menu, select '**OCSPd**':



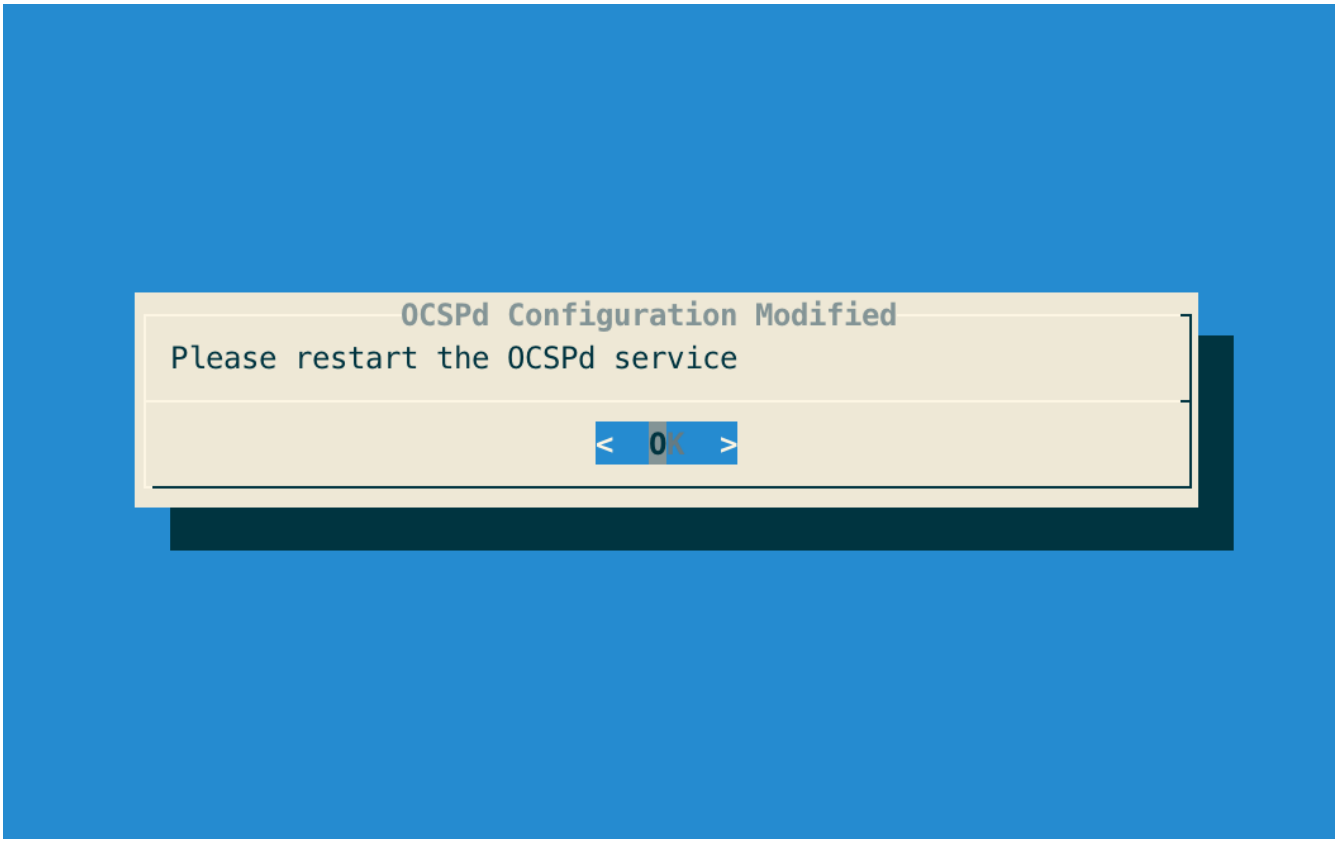
Step 4: In the OCSPd menu, select '**SECRET**':



Step 5: Validate the new OCSPd Application Secret:



Step 6: The OCSPd configuration is updated:



4.7. Installing the OCSPd license

Step 1: Upload the 'ocspd.lic' file through SCP under '/tmp/ocspd.lic':

Step 2: Access the server through SSH with an account with administrative privileges;

Step 3: Move the license file and set the permissions using the following commands:

```
# mv /tmp/ocspd.lic /opt/ocspd/etc
# chown ocspd:ocspd /opt/ocspd/etc/ocspd.lic
# chmod 640 /opt/ocspd/etc/ocspd.lic
```

4.8. Installing a Server Authentication Certificate

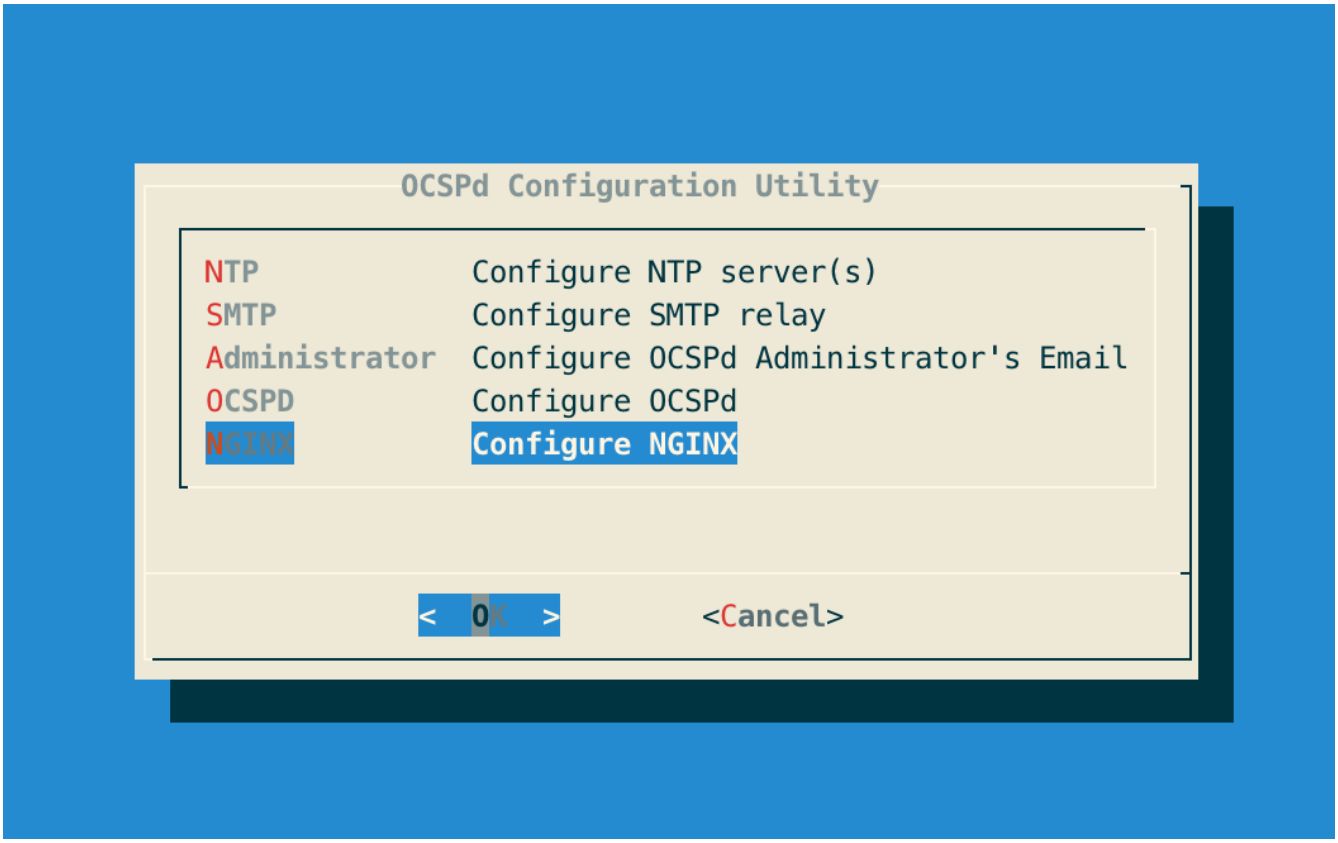
4.8.1. Issuing a Certificate Request (PKCS#10)

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Load the OCSPd Configuration Utility with the following command:

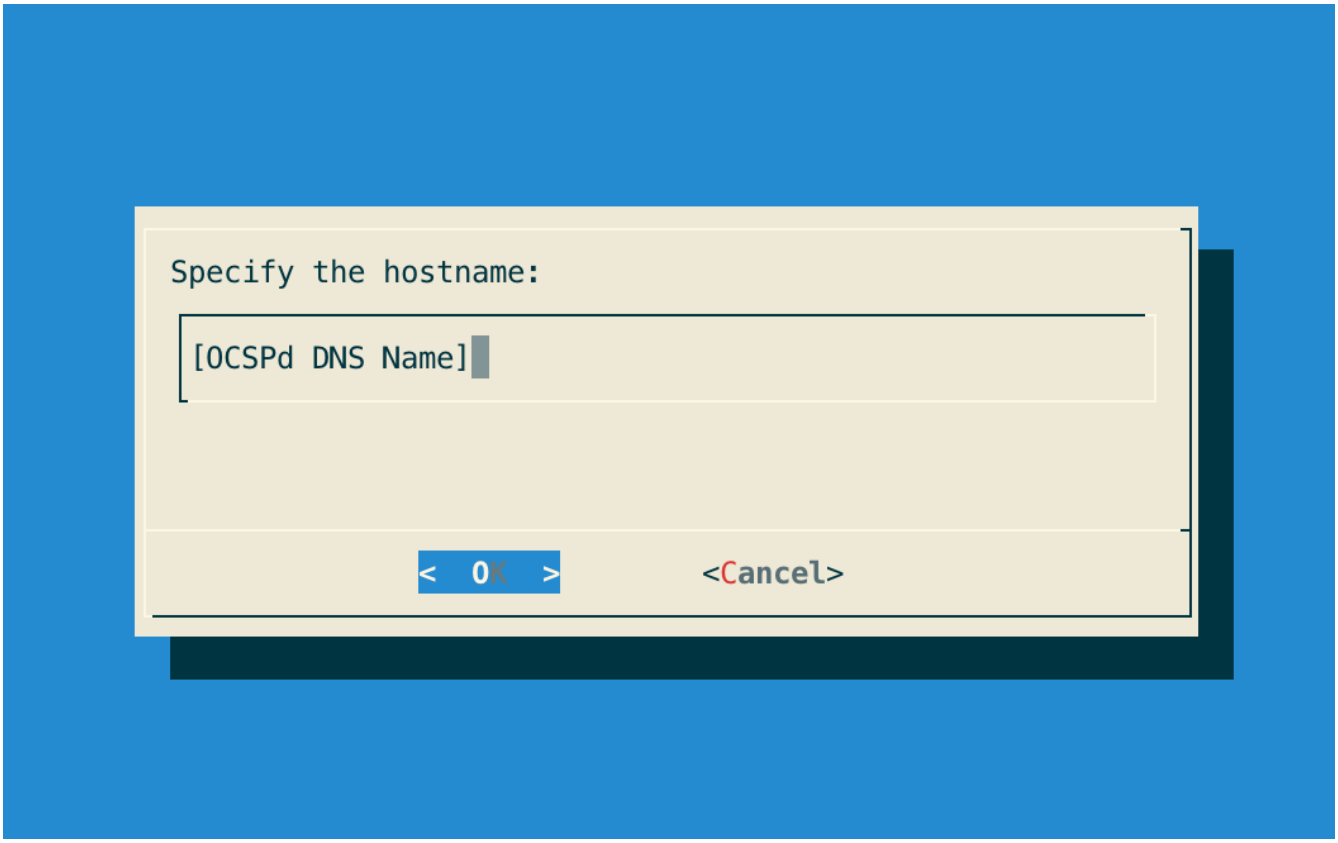
```
# /opt/ocspd/sbin/ocspd-config
```

Step 3: In the main menu, select '**NGINX**':



Step 4: In the NGINX menu, select '**CSR**':

Step 5: Specify the DNS Name of the OCSPd server:



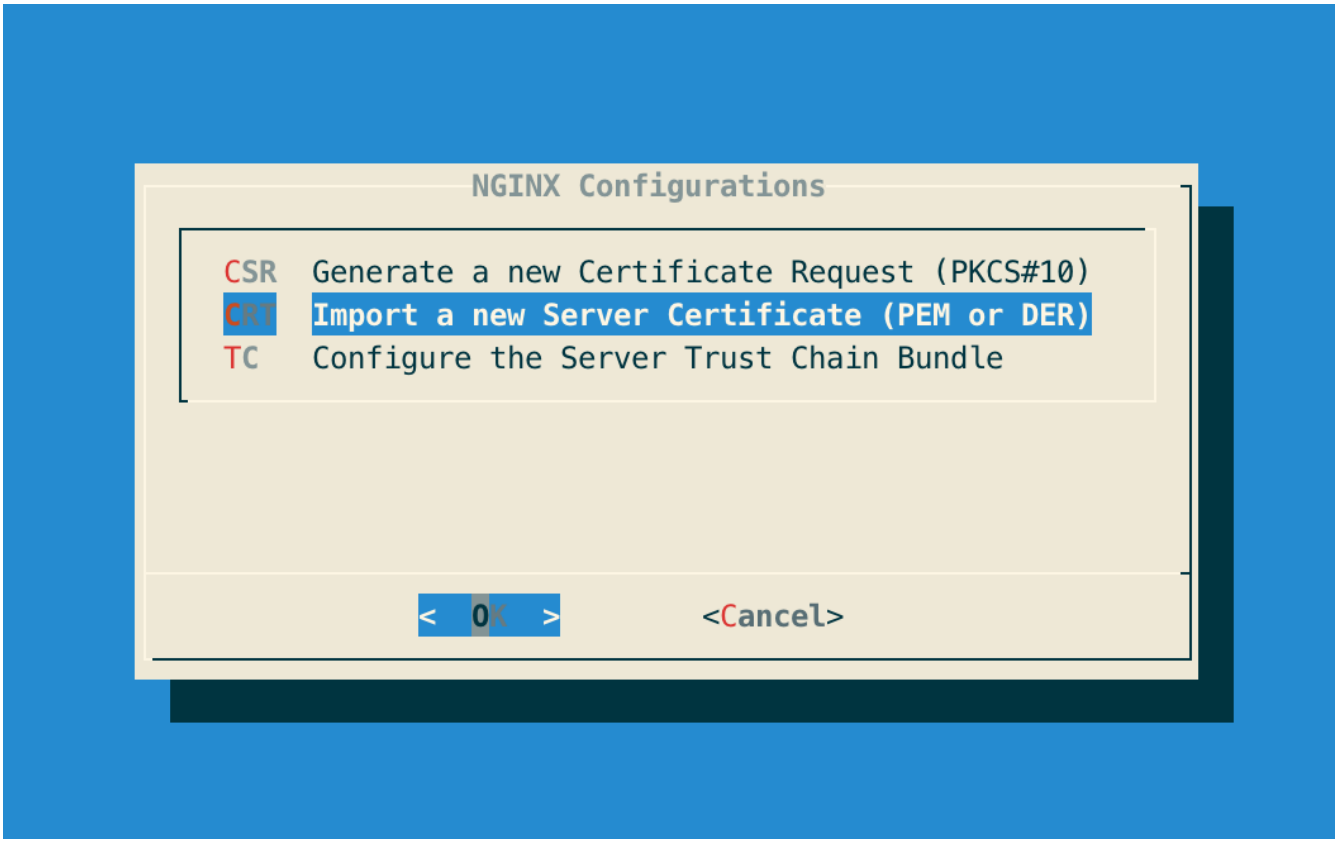
Step 6: The certificate request is generated and available under '***/etc/nginx/ssl/ocspd.csr.new***':

Step 7: Sign the certificate request using the corporate PKI.

4.8.2. Installing a Server Certificate

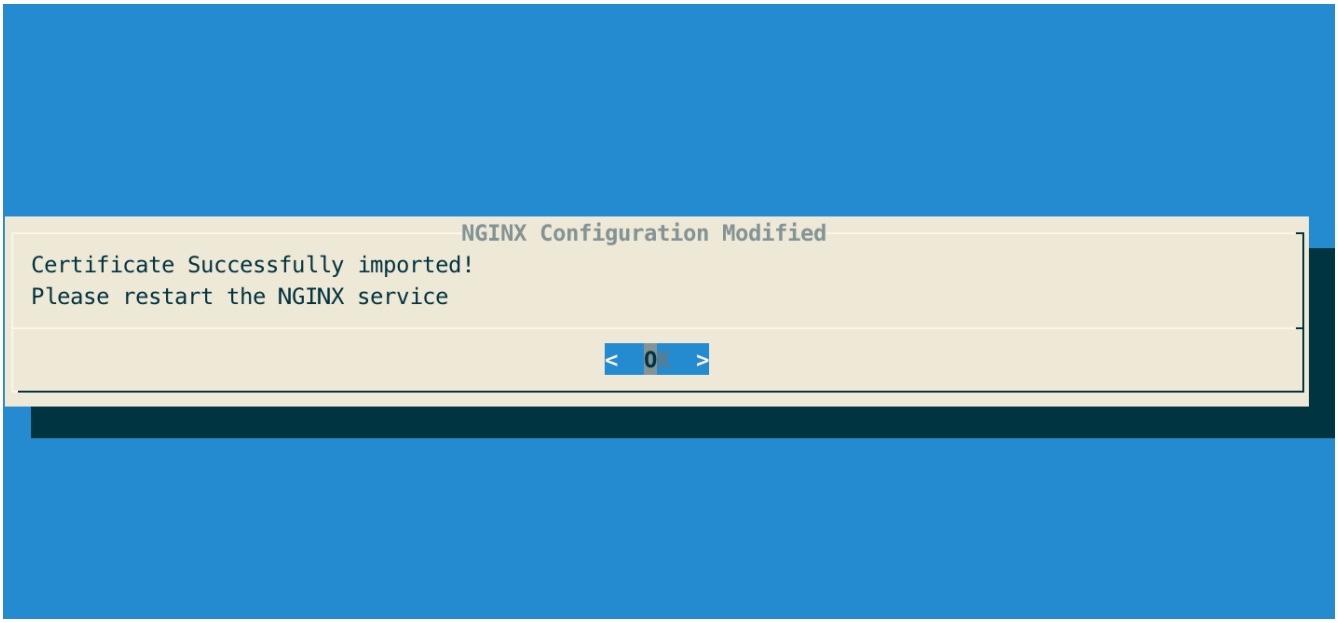
Step 1: Upload the generated server certificate on the OCSPd server under '***/tmp/ocspd.pem***' through SCP;

Step 2: In the NGINX configuration menu, select '**CRT**':



Step 3: Specify the path '***/tmp/ocspd.pem***' and validate:

Step 4: The server certificate is successfully installed:

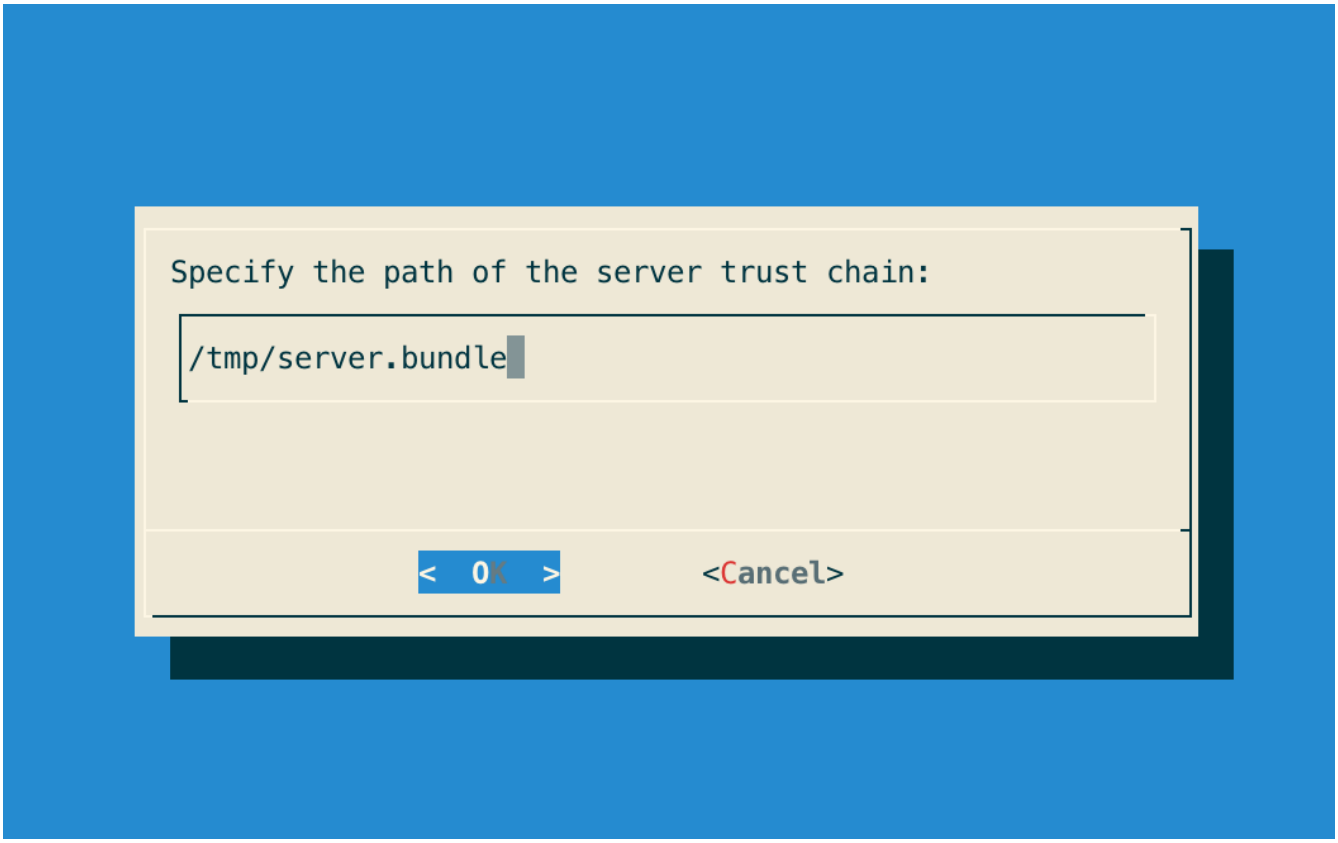


4.8.3. Installing the Server Certificate Trust Chain

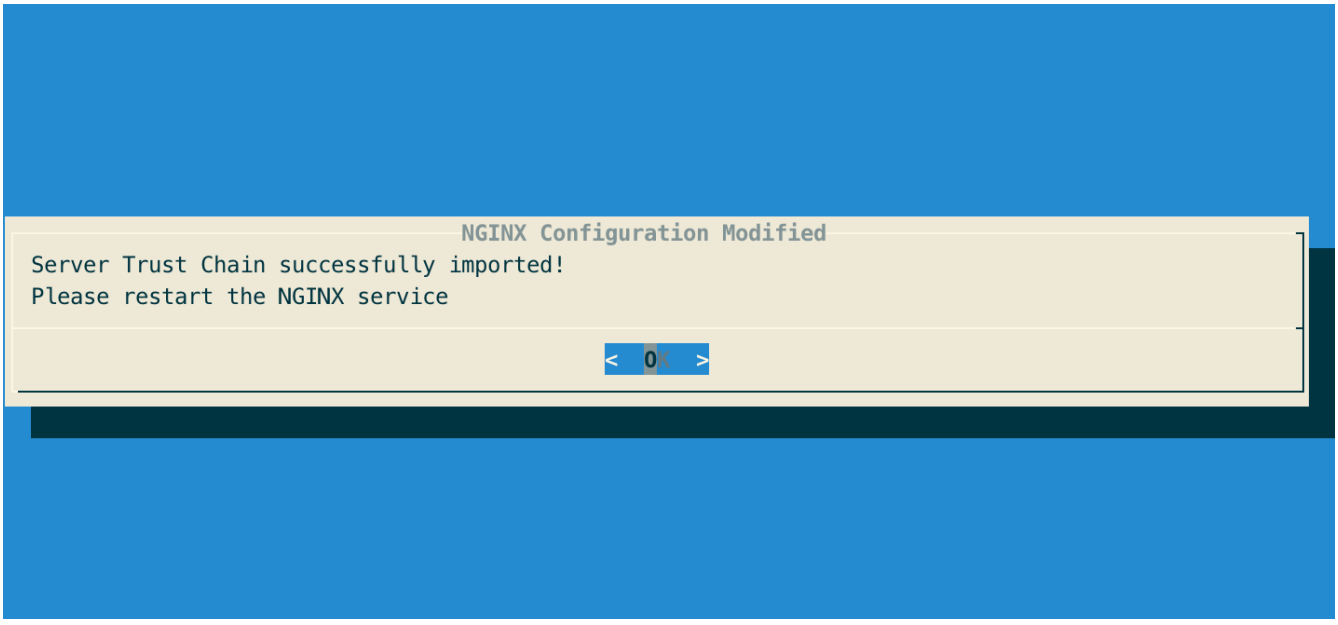
Step 1: Upload the server certificate trust chain (the concatenation of the Certificate Authority certificates in PEM format) on the OCSPd server under '***/tmp/server.bundle***' through SCP;

Step 2: In the NGINX configuration menu, select '**TS**':

Step 3: Specify the path '***/tmp/server.bundle***' and validate:



Step 4: The server bundle is successfully installed:



4.9. Configuring the Firewall

4.9.1. EL6

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Open ports TCP/80 and TCP/443 on the local firewall with the following commands:

```
# iptables -I INPUT 1 -p tcp -m tcp --dport 443 -j ACCEPT
```

```
# iptables -I INPUT 1 -p tcp -m tcp --dport 80 -j ACCEPT
```

Step 3: Save the local firewall configurations with the following command:

```
# /etc/init.d/iptables save
```

4.9.2. EL7

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Open ports TCP/80 and TCP/443 on the local firewall with the following commands:

```
# firewall-cmd --zone=public --permanent --add-service=http
# firewall-cmd --zone=public --permanent --add-service=https
```

5. Running as container

OCSPd is also packaged as a container, and can be run on container runtimes such as Docker or Kubernetes CRI-compliant runtimes.

5.1. Database considerations

OCSPd uses an embedded database to store application configuration. The database is created automatically when OCSPd is started for the first time. The database is stored in the `/ocspd/database` directory and needs to be persisted :

- On Docker, this can be done through a Docker volume or a bind mount.
- On Kubernetes, this can be done through a persistent volume claim.

5.2. Docker example

The bare minimum requirements to start an OCSPd instance is to pass through environment variables at least :

- a valid license through the `LICENSE` variable
- an application secret through the `APPLICATION_SECRET` variable

To do so, just run the following command :

```
docker run -p 9000:9000 -e LICENSE=$(cat ./ocspd.lic) -e
APPLICATION_SECRET=QA3BgXqapXaEzLbX -v ./database:/ocspd/database:rw
registry.evertrust.io/ocspd:3.1.3
```

The OCSPd server will be available at http://localhost:9000. To configure the instance, please refer to the configuration section.

5.3. Configuration

The Docker image is configured through environment variables. The following environment variables are available :

5.3.1. General configuration

Variable	Type	Description	Default
LICENSE	`string`	A valid OCSPd license string, base64-encoded. Can be used if `LICENSE_PATH` is empty.	

Variable	Type	Description	Default
LICENSE_PATH	`path`	Path where an OCSPd license file is mounted inside the container. Can be used if the license is not passed directly through `LICENSE`.	
APPLICATION_SECRET	`string`	Application secret used by OCSPd	

WARNING Your license usually contains newline characters, that you must replace by '\n' when setting it through the environment.

5.3.2. Configuring HTTPS

In production, it is strongly recommended to ensure all requests go through a layer of encryption. Configuring TLS for OCSPd will allow your reverse proxy to request OCSPd data using TLS.

NOTE If all settings are left empty, OCSPd will generate a self-signed certificate upon startup and still expose its HTTPS endpoint on

Variable	Type	Description	Default
HTTP_PORT	`port`	Port of the HTTP server	`9000`
HTTPS_PORT	`port`	Port of the HTTPS server	`9443`
HTTPS_KEYSTORE_PATH	`string`	Location where the keystore containing a server certificate is located.	
HTTPS_KEYSTORE_PASSWORD	`string`	Password for the given keystore, if required by the keystore type	
HTTPS_KEYSTORE_TYPE	`string`	Format in which the keystore is. Can be either `pkcs12`, `jks` or `pem` (a base64-encoded DER certificate)	`pkcs12`
HTTPS_KEYSTORE_ALGORITHM	`string`	The key store algorithm	Platform default algorithm

5.3.3. Mailer configuration

Variable	Type	Description	Default
SMTP_HOST	`string`	SMTP host	
SMTP_PORT	`port`	SMTP port	
SMTP_SSL	`boolean`	Whether SSL should be used	
SMTP_TLS	`boolean`	Whether TLS should be used	
SMTP_USER	`string`	SMTP user	
SMTP_PASSWORD	`string`	SMTP password	

5.3.4. Radius configuration

Variable	Type	Description	Default
RADIUS_HOST	`string`	Radius host	
RADIUS_SECRET	`string`	Radius secret	
RADIUS_PORT	`port`	Radius port	
RADIUS_PROTOCOL	`string`	Radius protocol, `PAP` or `CHAP`	`PAP`

5.3.5. LDAP configuration

Variable	Type	Description	Default
LDAP_HOST	`string`	LDAP host	
RADIUS_SECRET	`string`	Radius secret	
LDAP_PORT	`port`	LDAP port	
LDAP_SSL	`boolean`	Whether SSL should be used for LDAP	
LDAP_BIND_DN	`string`	Bind DN used to authenticate to LDAP	
LDAP_BIND_PASSWORD	`string`	Bind password used to authenticate to LDAP	
LDAP_BASE_DN	`string`	LDAP base DN	
LDAP_USERNAME_ATTRIBUTE	`string`	LDAP username attribute	

6. Initial OCSPd Access

6.1. Starting the OCSPd services

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Start the ocspd service with the following command:

```
# /etc/init.d/ocspd start
```

Step 3: Start the nginx service with the following command:

```
# /etc/init.d/nginx start
```

6.2. Accessing the OCSPd Web Management Console

Step 1: Launch a web browser;

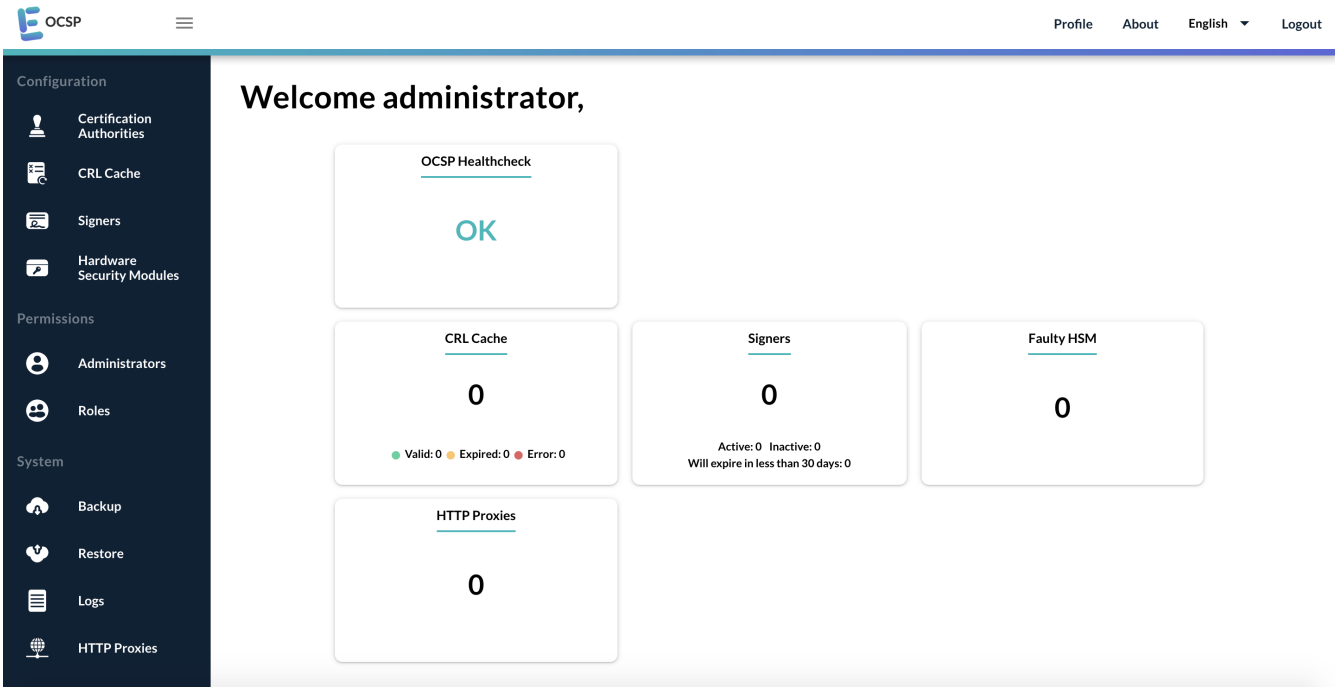
Step 2: Browse to '***https://[IP or DNS Name of the OCSPd component]***':

NOTE

The default administration credentials are:

- Login: '**administrator**'
- Password: '**ocspd**'

Step 3: Specify the default administration credentials and hit the '**Login**' button:



CAUTION

It is **highly recommended** to create a dedicated administration account and delete the default one, or at least modify the default administrator password.

7. Uninstallation Procedure

WARNING	Prior to uninstalling, please ensure that you have a **proper backup of the OCSPd component**. Once uninstalled, all the OCSPd data will be **irremediably lost**!

NOTE	Uninstalling OCSPd consists in uninstalling: • The OCSPd service; • The NGINX service.

7.1. Uninstalling OCSPd

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Uninstall OCSPd with the following commands:

```
# /etc/init.d/ocspd stop
# yum remove ocspd
# rm -rf /opt/ocspd
# rm -rf /var/log/ocspd
# rm -f /etc/default/ocspd
```

7.2. Uninstalling NGINX

Step 1: Access the server through SSH with an account with administrative privileges;

Step 2: Uninstall NGINX with the following commands:

```
# /etc/init.d/nginx stop
# yum remove nginx
# rm -rf /etc/nginx
# rm -rf /var/log/nginx
```