if EVERTRUST

EverTrust OCSP documentation v3.1.3 Installation Guide

EVERTRUST

Table of Contents

1. Introduction	1
1.1. Description	1
1.2. Scope	1
1.3. Out of Scope	1
2. Pre-requisites	2
2.1. Hardware pre-requisites.	2
2.2. System pre-requisites.	2
2.3. Software pre-requisites	2
3. Installation Procedure.	3
3.1. Installing NGINX	3
3.2. Installing the rngd service	3
3.3. Installing OCSPd	3
4. Configuring OCSPd	5
4.1. Configuring the NTP server(s)	5
4.2. Configuring the SMTP Relay.	7
4.3. Configuring the OCSPd Administrator's Email Address	9
4.4. Configuring the Radius Server	10
4.5. Configuring the LDAP Server.	12
4.6. Generating a new OCSPd Application Secret	15
4.7. Installing the OCSPd license	18
4.8. Installing a Server Authentication Certificate	18
4.9. Configuring the Firewall.	23
5. Running as container	25
5.1. Database considerations	25
5.2. Docker example	25
5.3. Configuration	25
6. Initial OCSPd Access	28
6.1. Starting the OCSPd services	28
6.2. Accessing the OCSPd Web Management Console	28
7. Uninstallation Procedure	30
7.1. Uninstalling OCSPd	30
7.2. Uninstalling NGINX	30

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
```

Installing the OCSPd package will install the following dependencies:

- NOTE
- java-11-openjdk-headless

• dialog

4. Configuring OCSPd

4.1. Configuring the NTP server(s)

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

/opt/ocspd/sbin/ocspd-config

<u>Step 3:</u> In the main menu, select '**NTP**':

0CS	Pd Configuration Utility
NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
Administrator	Configure OCSPd Administrator's Ema
UCSPD	Configure UCSPd
NGINA	Configure NGINA
<	OK > <cancel></cancel>

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

[NTP Server 1], [NTP Server 2]	Specify the stad conver(c) concreted by $1 + 1$	
< OK > <cancel></cancel>	[NTP Server 1], [NTP Server 2]	
< OK > <cancel></cancel>		
	< OK > <cancel></cancel>	

<u>Step 5:</u> The NTPs configuration is updated:

	ntpd Configuration Modified Please restart the ntpd service
-	

<u>Step 6:</u> Exit the configuration utility and restart the NTPd service with the following command:

/etc/init.d/ntpd restart

4.2. Configuring the SMTP Relay

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

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

<u>Step 3:</u> In the main menu, select '**SMTP**':

NTP Configure NTP server(s)	1
SMIPConfigure SMTP relayAdministratorConfigure OCSPd Administrator's EmailOCSPDConfigure OCSPdNGINXConfigure NGINX	
< <mark>OK ></mark> <cancel></cancel>	

<u>Step 4</u>: Specify IP address or the DNS name of the SMTP relay and validate:

Specify the smtp relay:	
[SMTP Relay IP or DNS Nam	me]
L	
< 0K >	<cancel></cancel>

<u>Step 5:</u> The Postfix configuration is updated:

<u>Step 6</u>: 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

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

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

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

	OCSPd Configuration Utility
NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
Administra	tor Configure OCSPd Administrator's Email
OCSPD	Configure OCSPd
NGINX	Configure NGINX
	< OK > <cancel></cancel>

<u>Step 4</u>: Specify the email address of the OCSPd Administrator and validate:

Specify O	CSPd Administrato	r's Email:	
[ADMIN EN	MAIL ADDRESS]		
	< 0% >	<cancel></cancel>	

<u>Step 5:</u> Exit the Configuration Utility;

<u>Step 6:</u> Validate the SMTP relay and Administrator Email Address with the following commands:

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

<u>Step 7:</u> Ensure that the email defined step 4 receives the test email.

4.4. Configuring the Radius Server

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

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

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

NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
OCSPD	Configure OCSPd Administrator s Emait
NGINX	Configure NGINX
L	
<	OK > <cancel></cancel>

<u>Step 4</u>: In the OCSPd menu, select '**RADIUS**':

00	SPd Configurations
JVM OCSPD_LOGLEVEL PLAY_LOGLEVEL METRICS RADIUS LDAP SECRET	Configure JVM Parameters Configure OCSPd Log Level Configure OCSPd Log Level Enable / Disable Syslog Metrics Configure Radius Settings Configure LDAP Settings Generate Application Secret
< <mark>Acce</mark>	pter> <annuler></annuler>

<u>Step 5:</u> Specify the following Radius configuration settings and validate:

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

Configure Rad	dius Settings:	ttings	
Host :[R/ Port :[R/ Secret :[R/ Protocol:[R/	ADIUS Server IP ADIUS Port] ADIUS Secret] ADIUS Protocol]	or DNS Name]	
	Accenter>	Annular	

<u>Step 6:</u> The OCSPd configuration is updated:

OCSPd Configuration Modified Please restart the OCSPd service

4.5. Configuring the LDAP Server

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

/opt/ocspd/sbin/ocspd-config

<u>Step 3:</u> In the main menu, select 'OCSPd':

0CS	Pd Configuration Utility
NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
Administrator	Configure OCSPd Administrator's Email
OCSPD	Configure OCSPd
NGINX	Configure NGINX
L	
<	OK > <cancel></cancel>

<u>Step 4:</u> In the OCSPd menu, select '**RADIUS**':

00	SPd Configurations
JVM OCSPD_LOGLEVEL PLAY_LOGLEVEL METRICS RADIUS LDAP SECRET	Configure JVM Parameters Configure OCSPd Log Level Configure OCSPd Log Level Enable / Disable Syslog Metrics Configure Radius Settings Configure LDAP Settings Generate Application Secret
< <mark>Acce</mark>	pter> <annuler></annuler>

<u>Step 5:</u> 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.

Configure LDA	P Sett	tings:
-		
Host	:	[LDAP Server IP or DNS Name]
Port	:	[LDAP Port]
SSL/TLS	:	[LDAPS enabled?]
Bind DN	:	[LDAP Bind DN]
Bind Passwor	d :	[LDAP Bind Password]
Base DN	:	[LDAP Base DN]
Filter	:	[LDAP Filter]
User Attribu	te:	[LDAP User Attribute]
L		
	<acce< td=""><td>epter> <annuter></annuter></td></acce<>	epter> <annuter></annuter>

<u>Step 6:</u> The OCSPd configuration is updated:

4.6. Generating a new OCSPd Application Secret

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

/opt/ocspd/sbin/ocspd-config

<u>Step 3:</u> In the main menu, select 'OCSPd':

0CS	Pd Configuration Utility
NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
Administrator	Configure OCSPd Administrator's Email
OCSPD	Configure OCSPd
NGINX	Configure NGINX
L	
<	OK > <cancel></cancel>

<u>Step 4:</u> In the OCSPd menu, select '**SECRET**':

00	SPd Configurations
JVM OCSPD_LOGLEVEL PLAY_LOGLEVEL METRICS RADIUS LDAP SECRET	Configure JVM Parameters Configure OCSPd Log Level Configure OCSPd Log Level Enable / Disable Syslog Metrics Configure Radius Settings Configure LDAP Settings Generate Application Secret
< <mark>Acce</mark>	pter> <annuler></annuler>

<u>Step 5:</u> Validate the new OCSPd Application Secret:

ew ucsed s Applicatio	n Secret:
Tgc!V@cT@ad5fbFdV\$1d3	rQcCt5fRRSttD\$2s51\$Z25ZevwQ2FD@F

<u>Step 6:</u> The OCSPd configuration is updated:



4.7. Installing the OCSPd license

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

<u>Step 2</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 3:</u> 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)

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Load the OCSPd Configuration Utility with the following command:

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

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

0CS	Pd Configuration Utility
NTP	Configure NTP server(s)
SMTP	Configure SMTP relay
Administrator	Configure OCSPd Administrator's Email
0CSPD	Configure OCSPd
NGINX	Configure NGINX
L	
<	OK > <cancel></cancel>

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

NGINX Configurations	1
CSR TC Generate a new Certificate Request (PKCS#10) Configure the Server Trust Chain Bundle	
< OK > <cancel></cancel>	

<u>Step 5:</u> Specify the DNS Name of the OCSPd server:

Specify the hostname:		
[OCSPd DNS Name]		
-		
< 0 < >	<cancel></cancel>	

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

New NGINX Server Certificate Request The new request is available under "/etc/nginx/ssl/ocspd.csr.new"
< 0K >

<u>Step 7:</u> Sign the certificate request using the corporate PKI.

4.8.2. Installing a Server Certificate

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

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

	NGINX Configurations
CSR CRT	Generate a new Certificate Request (PKCS#10) Import a new Server Certificate (PEM or DER)
ТС	Configure the Server Trust Chain Bundle
	< OK > <cancel></cancel>

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

<pre>Specify the path of the new server certificate: /tmp/ocspd.pem <</pre>		
< OK > <cancel></cancel>	the path of the new server	certificate:
< OK > <cancel></cancel>	_	_
	< 0K > <can< td=""><td>cel></td></can<>	cel>

<u>Step 4</u>: The server certificate is successfully installed:

NGINX Configuration Modified
Certificate Successfully imported!
Please restart the NGINX service
< 0% >

4.8.3. Installing the Server Certificate Trust Chain

<u>Step 1:</u> 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;

	NGINX Configurations
CSR	Generate a new Certificate Request (PKCS#10) Configure the Server Trust Chain Bundle
-	

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

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

Specify the path o	of the server trust o	chain:
/tmp/server.bundl	le	
< 0	<mark>) < > <cancel< mark="">></cancel<></mark>	

<u>Step 4</u>: The server bundle is successfully installed:

NGINX Configuration Modified Server Trust Chain successfully imported! Please restart the NGINX service
< 0 < >

4.9. Configuring the Firewall

4.9.1. EL6

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> 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

<u>Step 3:</u> Save the local firewall configurations with the following command:

/etc/init.d/iptables save

4.9.2. EL7

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> 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	Туре	Description	Default
LICENSE	string	A valid OCSPd license	
		string, base64-encoded.	
		Can be used if	
		LICENSE_PATH is empty.	

Variable	Туре	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	Туре	Description	Default
HTTP_PORT	port	Port of the HTTP server	9000
HTTPS_PORT	port	Port of the HTTPS server	9443
HTTPS_KEYSTORE_PAT H	string	Location where the keystore containing a server certificate is located.	
HTTPS_KEYSTORE_PAS SWORD	string	Password for the given keystore, if required by the keystore type	
HTTPS_KEYSTORE_TYP E	string	Format in which the keystore is. Can be either pkcs12, jks or pem (a base64-encoded DER certificate)	pkcs12
HTTPS_KEYSTORE_ALG ORITHM	string	The key store algorithm	Platform default algorithm

5.3.3. Mailer configuration

Variable	Туре	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	Туре	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	РАР

5.3.5. LDAP configuration

Variable	Туре	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_PASSWOR D	string	Bind password used to authenticate to LDAP	
LDAP_BASE_DN	string	LDAP base DN	
LDAP_USERNAME_ATT RIBUTE	string	LDAP username attribute	

6. Initial OCSPd Access

6.1. Starting the OCSPd services

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2</u>: Start the ocspd service with the following command:

/etc/init.d/ocspd start

<u>Step 3:</u> Start the nginx service with the following command:

/etc/init.d/nginx start

6.2. Accessing the OCSPd Web Management Console

<u>Step 1</u>: Launch a web browser;

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



Welcome to EverTrust OCSP Management Console



Reset password



The default administration credentials are:

- NOTE
- Login: 'administrator'
 - Password: 'ocspd'

<u>Step 3</u>: Specify the default administration credentials and hit the '**Login**' button:

Eoc	SP ≡			Profile About	English 🔻 Logout
Configuration Configuration Authorities		Welcome administrator,			
**	CRL Cache	OCSP Healthcheck			
الم	Signers	ОК			
~	Hardware Security Modules				
Permissions		CRL Cache	Signers	Faulty HSM	
θ	Administrators				
⊜	Roles	0	0	0	
System		Valid: 0 September 2010	Active: 0 Inactive: 0 Will expire in less than 30 days: 0		
•	Backup	HTTP Proxies			
*	Restore				
	Logs	0			
<u> </u>	HTTP Proxies				

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**!

Uninstalling OCSPd consists in uninstalling:

- The OCSPd service;
 - The NGINX service.

7.1. Uninstalling OCSPd

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> 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

<u>Step 1</u>: Access the server through SSH with an account with administrative privileges;

<u>Step 2:</u> Uninstall NGINX with the following commands:

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