Security Server Installation Guide

X-ROAD 6

Version: 2.7
23.02.2017
Doc. ID: IG-SS

Version history

Date	Version	Description	Author
01.12.2014	1.0	Initial version	
19.01.2015	1.1	License information added	
18.03.2015	1.2	Meta-package for security server added. Legacy securelog module removed	
02.04.2015	1.3	“sdsb” change to “xroad”	
27.05.2015	1.4	Some typos fixed	
30.06.2015	1.5	Minor corrections done	
06.07.2015	1.6	New repository address	
18.09.2015	1.7	Reference data in 3.2 updated	
18.09.2015	2.0	Editorial changes made	
13.10.2015	2.1	Editorial changes made	
10.12.2015	2.2	Updated the installing of the support for hardware tokens (2.7)	
17.12.2015	2.3	Added *xroad-addon-wsdlvalidator* package	

Date	Version	Description	Author
19.05.2016	2.4	Merged changes from xtee6-doc repo. Updated table 2.2 with p 1.12, added chapter 2.8 and updated 3.2.	
30.09.2016	2.5	Added chapter „Different versions of xroad-* package after successful upgrade“.	
07.12.2016	2.6	Added operational data monitoring packages. 2 GB RAM -> 3 GB RAM	
23.02.2017	2.7	Converted to Github flavoured Markdown, added license text, adjusted tables for better output in PDF	Toomas Mölder

Table of Contents

License

1 Introduction

1.1 Target Audience

The intended audience of this Installation Guide are X-Road Security server system administrators responsible for installing and using X-Road software. The daily operation and maintenance of the security server is covered by its User Guide [UG-SS].

The document is intended for readers with a moderate knowledge of Linux server management, computer networks, and the X-Road working principles.

1.2 References

1. [UG-SS] Cybernetica AS. X-Road 6. Security Server User Guide. Document ID UG-SS

2 Installation

2.1 Supported Platforms

The security server runs on the *Ubuntu Server 14.04 Long-Term Support (LTS)* operating system on a 64-bit platform. The security server software is distributed as .deb packages through the official X-Road repository at http://x-road.eu/packages/

The software can be installed both on physical and virtualized hardware (of the latter, Xen and Oracle VirtualBox have been tested).

2.2 Reference Data

Note: The information in empty cells should be determined before the server's installation, by the person performing the installation.

Caution: Data necessary for the functioning of the operating system is not included.

Ref		Explanation
1.0	Ubuntu 14.04, 64-bit 3 GB RAM, 3 GB free disk space	Minimum requirements
1.1	http://x-road.eu/packages	X-Road package repository
1.2	http://x-road.eu/packages/xroad_repo.gpg	The repository key

Ref		Explanation
1.3		Account name in the user interface
1.4	TCP 5500	Port for inbound connections (from the external network to the security server) Message exchange between security servers
	TCP 5577	Port for inbound connections (from the external network to the security server) Querying of OCSP responses between security servers
	TCP 2080	Port for inbound connections (from the external network to the security server) Message exchange between security server and operational data monitoring daemon (by default on localhost)
	TCP 9011	Port for inbound connections (from the external network to the security server) Operational data monitoring daemon JMX listening port
1.5	TCP 5500	Ports for outbound connections (from the security server to the external network) Message exchange between security servers
	TCP 5577	Ports for outbound connections (from the security server to the external network) Querying of OCSP responses between security servers
	TCP 4001	Ports for outbound connections (from the security server to the external network) Communication with the central server
	TCP 80	Ports for outbound connections (from the security server to the external network) Downloading global configuration

Ref		Explanation
	TCP 80,443	Ports for outbound connections (from the security server to the external network) Most common OCSP and time-stamping services
1.6	TCP 4000	User interface (local network)
1.7	TCP 80	Information system access points (in the local network) Connections from information systems
	TCP 443	Information system access points (in the local network) Connections from information systems
1.8		Security server internal IP address(es) and hostname(s)
1.9		Security server public IP address, NAT address
1.10	<by default, the server's IP addresses and names are added to the certificate's Distinguished Name (DN) field>	Information about the user interface TLS certificate
1.11	<by default, the server's IP addresses and names are added to the certificate's Distinguished Name (DN) field>	Information about the services TLS certificate
1.12	TCP 2552	Port for communications between `xroad-proxy` and `xroad-monitoring` processes

2.3 Requirements for the Security Server

Minimum recommended hardware parameters:

- the server's hardware (motherboard, CPU, network interface cards, storage system) must be supported by Ubuntu 14.04 in general;
- a 64-bit dual-core Intel, AMD or compatible CPU; AES instruction set support is highly recommended;

- 3 GB RAM;
- a 100 Mbps network interface card;
- if necessary, interfaces for the use of hardware tokens.

Requirements to software and settings:

- an installed and configured Ubuntu 14.04 LTS x86-64 operating system;
- if the security server is separated from other networks by a firewall and/or NAT, the necessary connections to and from the security server are allowed (**reference data: 1.4; 1.5; 1.6; 1.7**). The enabling of auxiliary services which are necessary for the functioning and management of the operating system (such as DNS, NTP, and SSH) stay outside the scope of this guide;
- if the security server has a private IP address, a corresponding NAT record must be created in the firewall (**reference data: 1.9**).

2.4 Preparing OS

- Add system user (**reference data: 1.3**) whom all roles in the user interface are granted to. Add a new user with the command

  ```
  sudo adduser username
  ```

  User roles are discussed in detail in X-Road Security Server User Guide [UG-SS].

- Set the operating system locale. Add following line to the `/etc/environment` file.

  ```
  LC_ALL=en_US.UTF-8
  ```

2.5 Installation

To install the X-Road security server software, follow these steps.

1. Add to `/etc/apt/sources.list.d/xroad.list` the address of X-Road package repository (**reference data: 1.1**) and the nginx repository:

   ```
   deb http://x-road.eu/packages trusty main
   deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main
   deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
   ```

2. Add the X-Road repository's signing key to the list of trusted keys (**reference data: 1.2**):

```
curl http://x-road.eu/packages/xroad_repo.gpg | sudo apt-key add -
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 00A6F0A3C300EE8C
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys EB9B1D8886F44E2A
```

3. Issue the following commands to install the security server packages:

```
sudo apt-get update
sudo apt-get install xroad-securityserver
```

Upon the first installation of the packages, the system asks for the following information.

- Account name for the user who will be granted the rights to perform all activities in the user interface (**reference data: 1.3**).
- The Distinguished Name of the owner of the **user interface's** self-signed TLS certificate (*Subject DN*) and its alternative names (*subjectAltName*) (**reference data: 1.8; 1.10**). The certificate is used for securing connections to the user interface. The name and IP addresses detected from the operating system are suggested as default values.
    - The *Subject DN* must be entered in the format:

      ```
      /CN=server.domain.tld
      ```

    - All IP addresses and domain names in use must be entered as alternative names in the format:

      ```
      IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld
      ```

- The Distinguished Name of the owner of the TLS certificate that is used for securing the HTTPS access point of information systems (**reference data: 1.8; 1.11**). The name and IP addresses detected from the system are suggested as default values.
    - The *Subject DN* must be entered in the format:

      ```
      /CN=server.domain.tld
      ```

    - All IP addresses and domain names in use must be entered as alternative names in the format:

      ```
      IP:1.2.3.4,IP:4.3.2.1,DNS:servername,DNS:servername2.domain.tld
      ```

The meta-package `xroad-securityserver` also installs metaservices module `xroad-addon-metaservices`, messagelog module `xroad-addon-messagelog`, operational data monitoring module `xroad-addon-opmonitoring` and WSDL validator module `xroad-addon-wsdlvalidator`.

2.6 Post-Installation Checks

The installation is successful if system services are started and the user interface is responding.

- Ensure from the command line that X-Road services are in the `start/running` state (example output follows):

```
sudo initctl list | grep "^xroad-"

xroad-jetty start/running, process 19796
xroad-confclient start/running, process 19563
xroad-signer start/running, process 19393
xroad-opmonitor start/running, process 20669
xroad-proxy start/running, process 19580
```

- Ensure that the security server user interface at https://SECURITYSERVER:4000/ (**reference data: 1.8; 1.6**) can be opened in a Web browser. To log in, use the account name chosen during the installation (**reference data: 1.3**). While the user interface is still starting up, the Web browser may display the “502 Bad Gateway” error.

2.7 Installing the Support for Hardware Tokens

To configure support for hardware security tokens (smartcard, USB token, Hardware Security Module), act as follows.

1. Install the hardware token support module using the following command:

```
sudo apt-get install xroad-addon-hwtokens
```

2. Install and configure a PKCS#11 driver for the hardware token according to the manufacturer's instructions.
3. Add the path to the PKCS#11 driver to the file `/etc/xroad/devices.ini` (as described in the example given in the file).
4. After installing and configuring the driver, the `xroad-signer` service must be restarted:

```
sudo service xroad-signer restart
```

2.8 Installing Support for Monitoring

Enabling the monitoring functionality on a security server requires installation of one additional package:

```
sudo apt-get install xroad-monitor
```

This installs and starts the `xroad-monitor` process that will gather and make available the monitoring information.

3 Security Server Initial Configuration

During the security server initial configuration, the server's X-Road membership information and the software token's PIN are set.

3.1 Prerequisites

Configuring the security server assumes that the security server owner is a member of the X-Road.

3.2 Reference Data

ATTENTION: Reference items 2.1 - 2.3 in the reference data are provided to the security server owner by the X-Road central's administrator.

The security server code and the software token's PIN will be determined during the installation at the latest, by the person performing the installation.

Ref		Explanation
2.1	http://x-road.eu/packages/<anchor file> ee-dev - development environment ee-test - test environment EE - production environment	Global configuration anchor file
2.2	GOV - government COM - commercial	Member class of the security server's owner
2.3	<security server owner register code>	Member code of the security server's owner
2.4	<choose security server identificator name>	Security server's code
2.5	<choose PIN for software token>	Software token's PIN

3.3 Configuration

To perform the initial configuration, open the address

```
https://SECURITYSERVER:4000/
```

in a Web browser (**reference data: 1.8; 1.6**). To log in, use the account name chosen during the installation (**reference data: 1.3).**

Upon first log-in, the system asks for the following information.

- The global configuration anchor file (**reference data: 2.1**).

  Please verify anchor hash value with the published value.

If the configuration is successfully downloaded, the system asks for the following information.

- The security server owner's member class (**reference data: 2.2**).
- The security server owner's member code (**reference data: 2.3**). If the member class and member code are correctly entered, the system displays the security server owner's name as registered in the X-Road center.
- Security server code (**reference data: 2.4**), which is chosen by the security server administrator and which has to be unique across all the security servers belonging to the same X-Road member.
- Software token's PIN (**reference data: 2.5**). The PIN will be used to protect the keys stored in the software token. The PIN must be stored in a secure place, because it will be no longer possible to use or recover the private keys in the token once the PIN has been lost.

4 Installation Error handling

4.1 Cannot Set LC_ALL to Default Locale

If running the locale command results in the error message

```
locale: Cannot set LC_ALL to default locale: No such file or directory,
```

then the support for this particular language has not been installed. To install it, run the command (the example uses the English language):

```
sudo apt-get install language-pack-en
```

Then, to update the system's locale files, run the following commands (the example uses the US locale):

```
sudo locale-gen en_US.UTF-8
sudo update-locale en_US.UTF-8
```

Set operating system locale. Add following line to `/etc/environment` file:

```
LC_ALL=en_US.UTF-8
```

After updating the system's locale settings, it is recommended to restart the operating system.

4.2 PostgreSQL Is Not UTF8 Compatible

If the security server installation is aborted with the error message

```
postgreSQL is not UTF8 compatible,
```

then the PostgreSQL package is installed with a wrong locale. One way to resolve it is to remove the data store created upon the PostgreSQL installation and recreate it with the correct encoding.

WARNING: All data in the database will be erased!

```
sudo pg_dropcluster --stop 9.3 main
LC_ALL="en_US.UTF-8" sudo pg_createcluster --start 9.3 main
```

To complete the interrupted installation, run the command

```
sudo apt-get -f install
```

4.3 Could Not Create Default Cluster

If the following error message is displayed during PostgreSQL installation:

```
Error: The locale requested by the environment is invalid.
Error: could not create default cluster. Please create it manually with pg_createcluster
```

use the following command to create the PostgreSQL data cluster:

```
LC_ALL="en_US.UTF-8" sudo pg_createcluster --start 9.3 main
```

The interrupted installation can be finished using

```
sudo apt-get -f install
```

4.4 Is Postgres Running On Port 5432?

If the following error message appears during installation

```
Is postgres running on port 5432 ?
Aborting installation! please fix issues and rerun with apt-get -f install,
```

check if any of the following errors occurred during the installation of PostgreSQL.

- Error installing the data cluster. Refer to section "Could not create default cluster".
- The PostgreSQL data cluster installed during the installation of the security server is not configured to listen on port 5432. To verify and configure the listening port, edit the PostgreSQL configuration file in `/etc/postgresql/9.3/main/postgresql.conf`. If you change the listening port, the postgresql service must be restarted.

The interrupted installation can be finished using

```
sudo apt-get -f install
```

4.5 Different versions of xroad-* packages after successful upgrade

Sometimes, after using `sudo apt-get upgrade` command, some of the packages are not upgraded. In the following example `xroad-securityserver` package version is still 6.8.3 although other packages are upgraded to 6.8.5:

```
# sudo dpkg -l | grep xroad-
ii xroad-addon-messagelog 6.8.5.20160929134539gitfe60f90
ii xroad-addon-metaservices 6.8.5.20160929134539gitfe60f90
ii xroad-addon-wsdlvalidator 6.8.5.20160929134539gitfe60f90
ii xroad-common 6.8.5.20160929134539gitfe60f90
ii xroad-jetty9 6.8.5.20160929134539gitfe60f90
ii xroad-proxy 6.8.5.20160929134539gitfe60f90
ii xroad-securityserver 6.8.3-3-201605131138
```

`apt-get upgrade` command doesn't install new packages - in this particular case new packages `xroad-monitor` and `xroad-addon-proxymonitor` installation is needed for upgrade of `xroad-securityserver` package.

To be sure that packages are installed correctly please use `sudo apt upgrade` or `sudo apt-get dist-upgrade` commands.

Please note that `xroad-jetty9 package` version can be different from other packages' versions.