CYBERNETICA

UXP

CENTRAL MONITORING AGENT MANUAL

1.1

VERSION HISTORY

Date	Version	Description
22.01.2014	0.1	Initial version
23.01.2014	0.2	Added supported Zabbix versions Added post-installation checks Added monitoring infrastructure figure Added reference data and requirements Added management of zabbix servers Added references
23.01.2014	0.3	Editorial changes, some comments.
26.01.2014	0.4	Added description of Zabbix configuration Removed nginx repository from 'Installation' Added description of automatic configuration process Updated introduction with more details Updated configuration properties table Added initial CMA configuration
27.01.2014	0.5	Minor edits More CMA management cases Added maintenance section
28.01.2014	0.6	Minor tweaks and fixes Added proper 'reload' command
28.01.2014	0.7	Editorial changes, comments
28.01.2014	0.8	Changed based on feedback
29.01.2014	0.9	Corrections, comments, modifications
13.10.2015	1.0	Editorial changes
22.10.2015	1.1	Changed port information

SISUKORD

1 INTRODUCTION

This manual describes the tasks related to installation of the central monitoring agent (CMA). In addition, it describes configuration that must be performed for it to forward monitoring information to Zabbix servers. Installation, management and use of the Zabbix servers is not in scope of this manual. Refer to corresponding section of the Zabbix documentation [Zabbix 2.4 Manual].

1.1 TARGET AUDIENCE

The intended audience of this manual is X-Road systems administrators who are responsible for monitoring the X-Road system.

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

Basic user knowledge of the Zabbix distributed monitoring solution is required. Refer to corresponding section of the Zabbix documentation [Zabbix 2.4 Manual].

1.2 MONITORING X-ROAD SERVERS

The X-Road monitoring solution allows for easy access to information such as CPU load, memory consumption and number of successful and failed requests processed by security servers. Figure 1 shows the components of the monitoring solution.

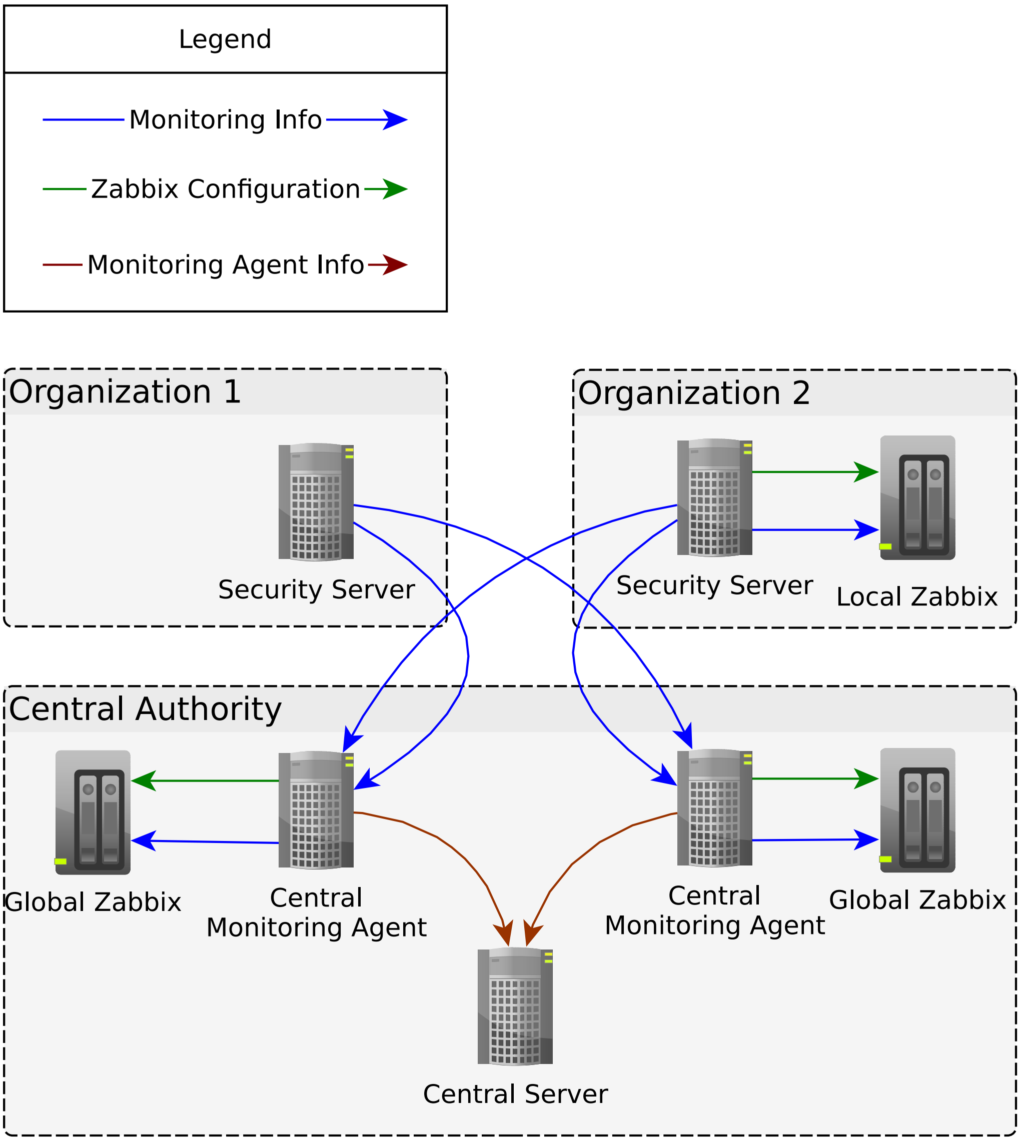

Figure 1: X-Road monitoring solution

Monitoring in the X-Road system can happen on two levels – central and organizational. On the organizational (local) level, a security server plug-in sends monitoring information to one or more locally configured Zabbix servers. On the central (global) level, the central server administrator can install one or more CMAs that collect information from security servers and send it to one or more Zabbix servers (blue arrows in the diagram). The CMA automatically sends a list of monitored servers to global Zabbix servers so that there is no need for manual configuration. Information about CMAs is entered into the central server (red arrows in the diagram) and is distributed with the global configuration to all security servers.

Communication between security servers and CMAs is protected with TLS protocol that uses certificates to authenticate both the client and the server. Security servers use authentication certificate for this purpose. CMAs use self-signed certificates that are distributed to security servers as part of the global configuration.

Both security servers and CMAs forward monitoring information to a number of Zabbix servers (see Section 3.2 on specifics of adding servers). The monitoring information comes from monitoring plug-ins in the security servers. These plug-ins send the monitoring information they gather to all CMAs that they can find from the global configuration (those that are configured at the central server as described in Section 3.1). By default the CMA will configure target Zabbix servers such that they are able to correctly interpret the information they receive (refer to Section 3.2).

This manual provides installation and configuration guides for the CMA, for information on configuring local monitoring for the security server see the corresponding manual [X-ROAD v6 Proxy Monitoring Agent Manual].

1.3 REFERENCES

1. [X-ROAD v6 Central Server User's Guide] Cybernetica AS. X-Road 6. Central Server User's Guide. Document ID Y-745-6.

2. [X-ROAD v6 Proxy Monitoring Agent Manual] Cybernetica AS. X-Road 6. Proxy Monitoring Agent Manual. Document ID Y-745-13.

3. [Zabbix 2.4 Manual] https://www.zabbix.com/documentation/2.4/manual

2 INSTALLATION

2.1 SUPPORTED PLATFORMS

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

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

The CMA has been tested and confirmed to work with Zabbix versions 2.2 through 2.4.

2.2 REFERENCE DATA FOR CENTRAL MONITORING AGENT

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

Ref			Explanation
1.0	Ubuntu 14.04, 64bit 2GB RAM, 3GB 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's key
1.3	TCP 80	global configuration download	Ports for outbound connections (from the central monitoring agent to central server)
1.4	TCP 443	monitoring data collection	Port for inbound connections from security servers
1.5	TCP 10051 TCP 80	monitoring data forwarding remote Zabbix server configuration	Ports for outbound connections to Zabbix servers
1.6	<by default, the server's IP addresses and names are added to the certificate's Distinguished Name (DN) field>		Information about the central monitoring agent's SSL certificate
1.7			Server's public IP address, NAT address (open to security servers)

2.3 REQUIREMENTS FOR THE CENTRAL MONITORING AGENT

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;
- 2 GB RAM;
- a 100 Mbps network interface card.
- Requirements to software and settings are the following.
- An installed and configured Ubuntu 14.04 LTS x86-64 operating system.

- If the CMA is separated from other networks by a firewall and/or NAT, the necessary connections to and from the security server must be allowed (reference data: 1.3; 1.4; 1.5). The enabling of auxiliary services which are necessary for the functioning and management of the operating system (such as DNS, NTP, and SSH) is outside the scope of this guide.
- If the CMA has a private IP address, a corresponding NAT record must be created in the firewall (reference data: 1.7).
- By default the CMA will attempt to connect to Zabbix servers using the default port values (reference data: 1.5), if the remote configuration differs from the default it will need to be specified in configuration (refer to Section 3.2).

If the CMA is installed to the same machine as a Zabbix server, care needs to be taken to make sure no port conflicts exist. It is up to the administrator to recognize such conflicts and resolve them by modifying the appropriate configurations.

2.4 INSTALLATION

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

1. Add the address of X-Road package repository (reference data: 1.1) and the OpenJDK Java 8 repository to '/etc/apt/sources.list':

```
deb http://x-road.eu/packages 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):

```
wget -q -O - http://x-road.eu/packages/xroad_repo.gpg | \
    sudo apt-key add -
sudo apt-key adv --keyserver keyserver.ubuntu.com \
    --recv-keys EB9B1D8886F44E2A
```

3. Issue the following commands to install the CMA packages:

```
sudo apt-get update
sudo apt-get install uxp-central-monitor
```

2.5 POST-INSTALLATION CHECKS

The installation is successful if the 'xroad-confclient' and 'xroad-central-monitor' services are started.

- Check from the command line that the 'xroad-confclient' and 'xroad-central-monitor' services are in the start/running state (example output follows):

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

xroad-confclient start/running, process 4056
uxp-central-monitor start/running, process 26808
```

- Make sure that the following commands are available from the command line:

```
generate-cma-certificate
reload-central-monitor-agent
```

2.6 INSTALLING CENTRAL SERVER ADDON

In order to add information about CMAs to the globally distributed configuration, it is necessary to install the monitoring addon to the central server. This is done by issuing the following commands in the central server.

```
sudo apt-get update
sudo apt-get install uxp-addon-central-monitor
```

3 CONFIGURATION

3.1 MANAGING CENTRAL MONITORING AGENTS

Steps needed to integrate a new CMA into the X-Road infrastructure are listed as follows.

1. Download the source anchor from the X-Road central server and save it as '/etc/xroad/configuration-anchor.xml'.
2. Generate a CMA self-signed certificate using the generate-cma-certificate command, you can enter the subject name manually using the '-s' option or use '-S' to set it to '/CN=<hostname>' (example output follows):

ATTENTION!

Certificate CN must match the IP address or the hostname of the CMA server which will be used in cma-conf file at the next step!

```
$ generate-cma-certificate -s '/CN=192.168.56.101'

Generating a 2048 bit RSA private key
...
writing new private key to '/etc/xroad/ssl/internal.key'
-----
Success! Output written to '/etc/xroad/ssl/internal.p12'.
Paste this XML segment to the Central Monitor Agent configuration:
<certHash hashAlgorithm="http://www.w3.org/2001/04/xmlenc#sha256">
    BGteBcuV+y8DCe6yh/c4UeXSt9qygMkBshqyRVuGArA=
</certHash>
```

3. Create CMA configuration file, called 'cma-conf.xml', which follows the schema available at 'http://<central>/cma-conf.xsd' (*<central>* being the address of the X-Road central server being used). The configuration file may contain multiple CMA entries, each of those may have multiple certificate hashes associated with it. Each of the entered CMAs will receive monitoring information from security servers, should it provide the matching authentication certificate. Example configuration:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:conf xmlns:tns="http://x-road.eu/xsd/xroad.xsd">
    <centralMonitorAgent>
        <address>192.168.56.101</address>
        <certHash
            hashAlgorithm="http://www.w3.org/2001/04/xmlenc#sha256">
            BGteBcuV+y8DCe6yh/c4UeXSt9qygMkBshqyRVuGArA=
        </certHash>
    </centralMonitorAgent>
</tns:conf>
```

   Notice that the *certHash* XML element generated on the previous step needs to be included inside of the *centralMonitorAgent* element, as well as the *address* (IP or hostname) that the security servers will use to send monitoring information to the CMA.

4. The 'conf-cma.xml' needs to be uploaded to the central server through the web interface (*Central Server → Configuration Management → Configuration Parts → Upload*). If 'cma-conf.xml' already exists on the central server, download it and modify it with the entry for the new CMA.

3.1.1 Changing the Central Monitoring Agent Authentication Certificate

The CMA will use the self-signed certificate from the PKCS12 keystore '/etc/xroad/ssl/internal.p12' when authenticating itself to incoming connections. Should the need arise to change the existing certificate, steps 2, 3 and 4 of the process described in Section 3.1 will need to be repeated with a couple minor alterations.

- Since the certificate already exists when the command is executed a prompt will ask the user whether the existing certificate needs to be overwritten:

  ```
  $ generate-cma-certificate -S

  Do you wish to replace the existing SSL key with the generated key?
  [Y/n]
  ```

  Should the user press 'Y' the process will continue as usual and the existing files will be replaced. Pressing any other key will result in the files being generated in the current working directory, under the names 'internal.key', 'internal.crt' and 'internal.p12'. It then will be up to the user to manually move 'internal.p12' to '/etc/xroad/ssl/'.

- The hash certificate will need to be added to 'conf-cma.xml' of the central server and the old certificate will need to be removed from there. The administrator might wish to first add the new certificate hash to the configuration and replace the certificate file after global configuration has been distributed to security servers. The old certificate hash can then be removed from 'conf-cma.xml' without interruption in the monitoring service.

3.1.2 Changing the Central Monitoring Agent Address

Should the CMA address in the network change, the configuration that the central server distributes as part of the global configuration would become outdated. In this case the user should download 'cma-conf.xml' from the central server's web interface (*Central Server → Configuration Management → Configuration Parts → Download*) and edit the *address* XML element of the relevant CMA, updating it with the new address. After the change the file should be uploaded to the central server again (as in step 5 of the process described in Section 3.1), replacing the old version.

3.2 MANAGING ZABBIX SERVERS

3.2.1 Configuring Zabbix Servers for monitoring X-Road

By default the CMA will automatically configure target Zabbix servers that are added to it's configuration file '/etc/xroad/monitor-agent.ini'. It will attempt to send configuration data to the Zabbix configuration service made available by installing the *zabbix-php-frontend* package. Connecting to the configuration service will require several additional configuration parameters (described in Section 3.2.3).

If, however, you wish to manually add security servers to the Zabbix database, an option is available to turn off automatic configuration of a target Zabbix server. Modifying the Zabbix database is not in scope of this manual. Refer to corresponding section of the Zabbix documentation [Zabbix 2.4 Manual].

3.2.2 Automatic Configuration

The CMA receives the X-Road global configuration from the central server (if step one of the configuration process described in Section 3.1 has been done). The list of security servers, that is being distributed as part of the global configuration, will be used to configure the target Zabbix servers automatically.

The CMA will create a host group on the target Zabbix server that will include all the security servers being distributed as part of the global configuration. Periodically the CMA checks the security server list of the global configuration for changes and, should new security servers be present in the list, it adds these new servers to the target Zabbix. Optionally, it is possible to let the CMA clean up any outdated servers (those that are missing from the global configuration) from the Zabbix database.

3.2.3 Adding Zabbix Servers to Central Monitoring Agent

To enable the forwarding of monitoring information to a Zabbix server one has to modify the configuration file '/etc/xroad/monitor-agent.ini', adding an entry similar to:

```
[zabbix-1]
address = 0.0.0.0
username = Admin
password = zabbix
host_group = cma
enable_cleanup = true
```

The section *[zabbix-<suffix>]* defines a Zabbix monitoring station, where the section name has a required prefix – '*zabbix*', and *<suffix>* must be some string that is unique among the other Zabbix sections. The description of the various configuration fields that can be defined within the Zabbix section follows (ones without a default value must be explicitly defined):

Field	Default Value	Explanation
address		Zabbix server host or IP address.
port	10051	Port where the Zabbix server listens for monitoring information.
enable_configurator	true	Enables/disables automatic configuration of the Zabbix monitoring station.

The following values are required if automatic configuration of the Zabbix server has been enabled:

Field	Default Value	Explanation
username		Zabbix configuration user name. Configurable during the Zabbix PHP Frontend installation.
password		Zabbix configuration user password. Configurable during the Zabbix PHP Frontend installation.
conf_api_port	80	Zabbix configuration API port. Configurable during the Zabbix PHP Frontend installation.
conf_api_path	/zabbix/api_jsonrpc.php	Zabbix configuration API path. Depends on the configuration of the apache2 web server set up for the Zabbix PHP Frontend installation.
host_group		The host group that contains security servers automatically managed by the CMA.
enable_cleanup	false	Enables/disables deletion of removed security servers from the host group if automatic configuration of the Zabbix monitoring station is enabled.

After the configuration has been updated with the correct Zabbix server information, the CMA should reload the configuration. This process is described in Section 3.3.

3.3 MAINTENANCE

There are certain scenarios where the CMA might not function as desired by the system administrator. Most of these issues can be repaired by reloading the CMA with the command:

```
reload-central-monitor-agent
```

This command causes the CMA to read its configuration from the configuration file '/etc/xroad/monitor-agent.ini' and update its components according to any changes that are detected. Any Zabbix servers present in the configuration will then be reconfigured if they have the automatic reconfiguration capability enabled in the configuration file.

3.3.1 Central Monitor Agent Configuration is Modified

If the configuration file '/etc/xroad/monitor-agent.ini' has been altered, then the configuration needs to be updated using the 'reload' command.

3.3.2 Zabbix Configuration Becomes Invalid

Should a Zabbix server configuration become lost or invalid, the reconfiguration process of Zabbix servers can be performed by force, using the 'reload' command.