ΚΟΙΝΟΠΡΑΞΙΑ: ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ, ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ

Project Title:

Deployment of Generic Cross Border eHealth Services in Cyprus

Agreement number: INEA/CEF/ICT/A2015/11S1451

Action No: 2015-CY-IA-0095

Title: Annex OP 3 Zabbix Open-source monitoring Tool

Release: v4

Αρ. Αναφ. Φακέλου: ΠΚ/2018/05/14

Λευκωσία

23 Ιουλίου, 2020

Βασικές Πληροφορίες Έργου

Πληροφορίες Έργου	
Τίτλος Έργου	**NCPeH CY**
Κωδικός Έργου	***2015-CY-IA-0095***
Ιδιοκτήτης Έργου	
Στοιχεία Επικοινωνίας Συντονιστή έργου	Καθ. Κωνσταντίνος Παττίχης, Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, Λεωφόρος Πανεπιστημίου 1 Αγλαντζιά Λευκωσία 2109 ΚΥΠΡΟΣ (+357) 22892697 (+357) 22892701 pattichi@cs.ucy.ac.cy

Ιστορικό αναθεωρήσεων

Αριθμός Έκδοσης	Ημερομηνία	Συγγραφείς	Εκδότης	Σχόλια
1.0	14/5/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης	ΥΥ & ΠΚ	Πρώτο Προσχέδιο
2.0	19/6/2018	Μόνικα Καλακουτή Μάριος Νεοφύτου	ΥΥ & ΠΚ	Δεύτερο Προσχέδιο
3	18/07/2019	Ζήνωνας Αντωνίου Ιωάννης Κωνσταντίνου	ΠΚ	Τρίτο Προσχέδιο
4	23/07/20	Ζήνωνας Αντωνίου Ιωάννης Κωνσταντίνου Μάριος Νεοφύτου Ηρακλής Κυριακίδης	ΠΚ, ΥΥ, ΕΑΗΥ	Τελική

Θεώρηση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Θεώρησης
Δρ Βάσος Σκουτέλλας	Συντονιστής ελέγχου ποιότητας παραδοτέων	07/10/2020

Έγκριση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Έγκρισης
Καθ. Σχίζας Χρίστος	Πρόεδρος ΕΑΗΥ	08/10/2020

Executive Summary

Zabbix is open-source monitoring software for networks and applications. It offers real-time monitoring of thousands of metrics collected from servers, virtual machines, and any other kind of network device. These metrics can help us determine the current health of NCPeH CY and detect problems with hardware or software components before users complain. Useful information is stored in a database so we can analyze data over time and improve the quality of provided services, or plan upgrades of NCPeH CY equipment.

Zabbix is written and distributed under the GPL General Public License version 2. It means that its source code is freely distributed and available for the general public.

The University of Cyprus is in charge for installing and supporting Zabbix software. Dr Zinonas Antoniou is the manager of the system.

Table of Contents

1   Installation and monitoring

We have installed Zabbix Server to monitor the server activity as well as the activity of all active nodes of the infrastructure. The next sections describe the needed configurations that have to be done in order to support the monitoring processes.

We have installed Zabbix software version 4.2. The Zabbix's full documentation is available online[1].

---

[1] https://www.zabbix.com/documentation/4.2

2 Overview

Zabbix is open-source monitoring software for networks and applications. It offers real-time monitoring of thousands of metrics collected from servers, virtual machines, and any other kind of network device. These metrics can help you determine the current health of your IT infrastructure and detect problems with hardware or software components before customers complain. Useful information is stored in a database so you can analyze data over time and improve the quality of provided services, or plan upgrades of your equipment.

Zabbix is written and distributed under the GPL General Public License version 2. It means that its source code is freely distributed and available for the general public.

2.1 The Objective
2.1.1 Data gathering

- availability and performance checks
- support for SNMP (both trapping and polling), IPMI, JMX, VMware monitoring
- custom checks
- gathering desired data at custom intervals
- performed by server/proxy and by agents

2.1.2 Real-time graphing

- monitored items are immediately graphed using the built-in graphing functionality

2.1.3 Web monitoring capabilities

- Zabbix can follow a path of simulated mouse clicks on a web site and check for functionality and response time

2.1.4 Extensive visualisation options

- ability to create custom graphs that can combine multiple items into a single view
- network maps
- custom screens and slide shows for a dashboard-style overview
- reports
- high-level (business) view of monitored resources

2.1.5 Historical data storage

- data stored in a database
- configurable history
- built-in housekeeping procedure

3 Installation Process

We followed the step-by-step instructions of the web tutorial[2] to install Zabbix version 3.4. The system was installed in Linux Ubuntu Server 16.04 LTS locally in Famagusta Hospital. The IP of the Zabbix server is 10.227.97.63.

3.1 ZABBIX Server specs
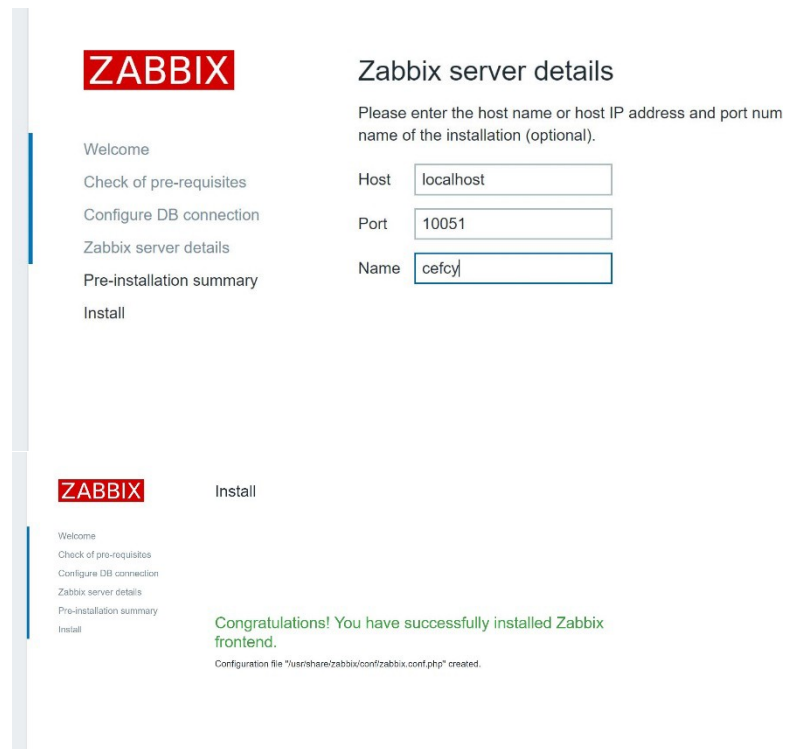
3.2 Resources

Zabbix Server was installed in Linux Ubuntu Server 16.04 LTS locally in Famagusta Hospital.

Zabbix Agent is required to install on all remote systems needs to monitor through Zabbix server. The Zabbix Agent collects resource utilization and applications data on the client system and provides such information to Zabbix server on their requests.

There are two types of checks can be configured between Zabbix Server and Client.

- Passive check – Zabbix Agent only sent data to server on their request.

- Active check – Zabbix Agent sends data periodically to Server.

Our installation is in **Active server port**:

- Host: localhost Port: 10051

- Name: cefcy

3.3 MySQL Installation

---

[2] https://www.zabbix.com/documentation/3.4/manual/installation/install

It is necessary to have an active SQL account. List of orders to setting up an account

1. sudo dpkg -i zabbix-release_4.2-1+xenial_all.deb
2. apt-get update
3. ifconfig
4. wget http://repo.zabbix.com/zabbix/4.2/ubuntu/pool/main/z/zabbix-%20release/zabbix-release_4.2-1+xenial_all.deb
5. dpkg -i zabbix-release_4.2-1+xenial_all.deb
6. sudo dpkg -i zabbix-release_4.2-1+xenial_all.deb
7. sudo apt-get update
8. apt-get install zabbix-server-mysql
9. sudo apt-get install zabbix-server-mysql
10. sudo apt-get install zabbix-proxy-mysql
11. sudo apt-get install zabbix-frontend-php
12. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
13. vi /etc/zabbix/zabbix_server.conf
14. nano /etc/zabbix/zabbix_server.conf
15. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
16. sudo nano /etc/zabbix/zabbix_server.conf
17. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
18. sudo nano /etc/zabbix/zabbix_server.conf
19. nano /etc/apache2/conf-enabled/zabbix.conf
20. sudo nano /etc/apache2/conf-enabled/zabbix.conf
21. sudo apt-get install zabbix-agent
22. service zabbix-agent start
23. /zabbix
24. sudo nano /etc/apache2/conf-enabled/zabbix.conf
25. service zabbix-agent start
26. zabbix
27. /zabbix
28. vi /etc/zabbix/zabbix_server.conf
29. service zabbix-server start
30. update-rc.d zabbix-server enable
31. service zabbix-agent start
32. service apache2 restart
33. vi /etc/zabbix/zabbix_server.conf
34. sudo nano /etc/zabbix/zabbix_server.conf
35. service zabbix-server start
36. update-rc.d zabbix-server enable
37. service apache2 restart
38. sudo nano /etc/zabbix/zabbix_server.conf
39. service apache2 restart
40. sudo nano /etc/zabbix/zabbix_server.conf
41. sudo apt-get install mysql-client mysql-server
42. service zabbix-server start
43. update-rc.d zabbix-server enable
44. service apache2 restart
45. service zabbix-agent start
46. sudo nano /etc/zabbix/zabbix_server.conf
47. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix

48. sudo apt-get install zabbix-server-mysql
49. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
50. sudo service mysql restart
51. sudo reboot
52. zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix

3.4   Zabbix Java Gateway Installation

Find below, the steps to enable apache tomcat monitoring from Zabbix server.

3.4.1   Step 1: Install Zabbix Java Gateway

```
sudo apt-get install zabbix-java-gateway
```

When installation process completed then restart your Zabbix Java Gateway

```
sudo service zabbix-java-gateway restart
```

3.4.2   Step 2: Modify Zabbix server config file

Go to Zabbix Server config file then insert Java gateway (Zabbix server IP address), Java gateway port and StartJavaPollers option.

```
sudo vim /etc/zabbix/zabbix_server.conf
```

Insert anywhere into conf file:

```
JavaGateway=10.227.97.63
JavaGatewayPort=10052
StartJavaPollers=5
```

Then restart Zabbix server:

```
sudo service zabbix-server restart
```

3.5   Technical/Project Approach

Login and configuring user

Overview. In this section you will learn how to log in and set up a system user in Zabbix. This is the Zabbix "Welcome" screen. Enter the user name Admin with password zabbix to log in as a Zabbix superuser.

When logged in, you will see 'Connected as Admin' in the lower right corner of the page. Access to Configuration and Administration menus will be granted. If you have additional servers you need to monitor, log in to each host, install the Zabbix agent, generate a PSK, configure the agent, and add the host to the web interface following the same steps you followed to add our first host.

3.5.1   Graphs

With lots of data flowing into Zabbix, it becomes much easier for the admin to look at a visual representation of what is going on rather than only numbers. This is where graphs come in. Graphs allow to grasp the data flow at a glance, correlate problems, discover when something started or make a presentation of when something might turn into a problem.

Zabbix provides admin with:

1. built-in simple graphs of one item data
2. the possibility to create more complex customised graphs
3. access to a comparison of several items quickly in ad-hoc graphs

4 Monitoring Features

Item types cover various methods of acquiring data from CEFCY system. Each item type comes with its own set of supported item keys and required parameters.
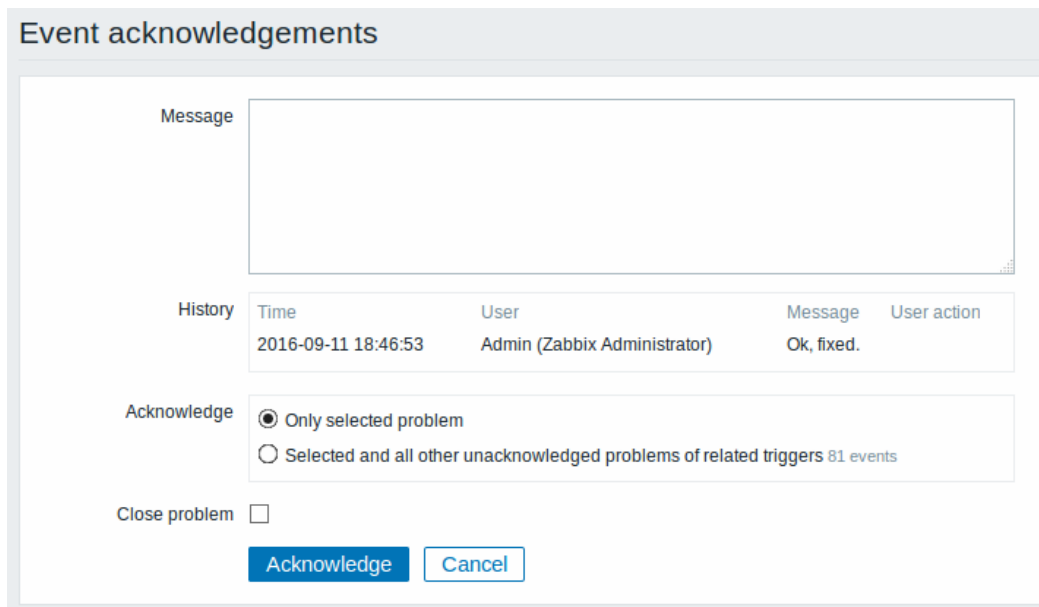
The following items types are currently offered by Zabbix:

1. Zabbix agent checks
2. SNMP agent checks
3. SNMP traps
4. IPMI checks
5. Simple checks
6. VMware monitoring
7. Log file monitoring
8. Calculated items
9. Zabbix internal checks
10. SSH checks
11. Telnet checks
12. External checks
13. Aggregate checks
14. Trapper items
15. JMX monitoring
16. ODBC checks
17. Dependent items

5   Admin alerts

The admin has to monitor the parameters of Zabbix and set manual alerts if a problem will arise. The acknowledgement status of problems is displayed in:

1. Monitoring → Dashboard (Problems and System status widgets)
2. Monitoring → Problems
3. Monitoring → Problems → Event details
4. Monitoring → Overview (with triggers selected)
5. Monitoring → Triggers
6. Monitoring → Screens (with Host group issues, Host issues, System status and Triggers overview elements)

5.1   Receiving problem notification

Zabbix offers some alerting mechanism to notify us about important events even when we are not directly looking at Zabbix frontend. This is what notifications do.

To be able to send and receive notifications from Zabbix we have to:

- Configure an email account

- Configure an action that sends a message to one of the defined media

5.1.1   Email Account Configuration

E-mail being the most popular delivery method for problem notifications. To configure e-mail as the delivery channel for messages, we need to configure e-mail as the media type and assign specific addresses to users.

To configure e-mail as the media type:

1. Go to Administration → Media types

2. Click on Create media type (or click on E-mail in the list of pre-defined media types).

The Media type tab contains general media type attributes:

Parameter	Description
Name	Name of the media type.
Type	Select *Email* as the type.
SMTP server	Set an SMTP server to handle outgoing messages.
SMTP server port	Set the SMTP server port to handle outgoing messages. This option is supported *starting with Zabbix 3.0*.
SMTP helo	Set a correct SMTP helo value, normally a domain name.
SMTP email	The address entered here will be used as the **From** address for the messages sent. Adding a sender display name (like "Zabbix-HQ" in *Zabbix-HQ <zabbix@company.com>* in the screenshot above) with the actual e-mail address is supported since Zabbix 2.2 version. There are some restrictions on display names in Zabbix emails in comparison to what is allowed by RFC 5322, as illustrated by examples: Valid examples: *zabbix@company.com* (only email address, no need to use angle brackets) *Zabbix HQ <zabbix@company.com>* (display name and email address in angle brackets) *∑Ω-monitoring <zabbix@company.com>* (UTF-8 characters in display name) Invalid examples: *Zabbix HQ zabbix@company.com* (display name present but no angle brackets around email address) *"Zabbix\@\<H(comment)Q\>" <zabbix@company.com>* (although valid by RFC 5322, quoted pairs and comments are not supported in Zabbix emails)
Connection security	Select the level of connection security: **None** - do not use the CURLOPT_USE_SSL option **STARTTLS** - use the CURLOPT_USE_SSL option with CURLUSESSL_ALL value **SSL/TLS** - use of CURLOPT_USE_SSL is optional This option is supported *starting with Zabbix 3.0*.
SSL verify peer	Mark the checkbox to verify the SSL certificate of the SMTP server. The value of "SSLCALocation" server configuration directive should be put into CURLOPT_CAPATH for certificate validation. This sets cURL option CURLOPT_SSL_VERIFYPEER. This option is supported *starting with Zabbix 3.0*.
SSL verify host	Mark the checkbox to verify that the *Common Name* field or the *Subject Alternate Name* field of the SMTP server certificate matches. This sets cURL option CURLOPT_SSL_VERIFYHOST. This option is supported *starting with Zabbix 3.0*.
Authentication	Select the level of authentication: **None** - no cURL options are set (since 3.4.2) **Username and password** - implies "AUTH=*" leaving the choice of authentication mechanism to cURL (until 3.4.2) **Normal password** - CURLOPT_LOGIN_OPTIONS is set to "AUTH=PLAIN"

Parameter	Description
	This option is supported *starting with Zabbix 3.0*.
Username	User name to use in authentication. This sets the value of CURLOPT_USERNAME. This option is supported *starting with Zabbix 3.0*.
Password	Password to use in authentication. This sets the value of CURLOPT_PASSWORD. This option is supported *starting with Zabbix 3.0*.
Enabled	Mark the checkbox to enable the media type.

The Options tab in the e-mail media type configuration contains alert processing settings. The same set of options are configurable for other media types, too.

All media types are processed in parallel. The maximum number of concurrent sessions is configurable per media type, but the total number of alerter processes on server can only be limited by the StartAlerters parameter. Alerts generated by one trigger are processed sequentially.

Parameter	Description
Concurrent sessions	Select the number of parallel alerter sessions for the media type: **One** - one session **Unlimited** - unlimited number of sessions **Custom** - select a custom number of sessions Unlimited/high values mean more parallel sessions and increased capacity for sending notifications. Unlimited/high values should be used in large environments where lots of notifications may need to be sent simultaneously.
Attempts	Number of attempts for trying to send a notification. Up to 10 attempts can be specified; default value is '3'. If '1' is specified Zabbix will send the notification only once and will not retry if the sending fails.
Retry interval	Frequency of trying to resend a notification in case the sending failed, in seconds (0-60). If '0' is specified, Zabbix will retry immediately. Time suffixes are supported, e.g. 5s, 1m.

To assign a specific address to the user:

1. Go to Administration → Users

2. Open the user properties form

In Media tab, click on Add.

User media attributes:

Parameter	Description
Type	Select *Email* as the type.
Send to	Specify the e-mail address to send the messages to. Adding a recipient display name (like "Some User" in *Some User <user@domain.tld>* in the screenshot above) with

Parameter	Description
	the actual e-mail address is supported since Zabbix 2.2 version. See examples and restrictions on display name and email address in media type attribute SMTP email description.
When active	You can limit the time when messages are sent, for example, the working days only (1-5,09:00-18:00). See the Time period specification page for description of the format. User macros are supported.
Use if severity	Mark the checkboxes of trigger severities that you want to receive notifications for. *Note* that for non-trigger events the default severity ('Not classified') is used, so leave it checked if you want to receive notifications for non-trigger events.
Status	Status of the user media. **Enabled** - is in use. **Disabled** - is not being used.

5.1.2 Action Configuration

Actions can be defined in response to events of all supported types:

- Trigger events - when trigger status changes from OK to PROBLEM and back
- Discovery events - when network discovery takes place
- Auto registration events - when new active agents auto-register
- Internal events - when items become unsupported or triggers go into an unknown state

Configuring an action
To configure an action, do the following:

- Go to Configuration → Actions
- From the Event source dropdown select the required source
- Click on Create action
- Set general action attributes
- Choose the operation to carry out, in Operations tab
- Choose the conditions upon which the operation is carried out, in Conditions tab

General action attributes:

Parameter	Description
Name	Unique action name.
Default subject	Default message subject. The subject may contain macros. It is limited to 255 characters.
Default message	Default message. The message may contain macros. It is limited to certain amount of characters depending on the type of database (see Sending message for more information).

Parameter	Description
Recovery message	Mark the checkbox to turn on a *Recovery message*. *Recovery message* is a special way of getting notified for a resolved problem. If turned on, only a **single**message with a custom subject/body is sent if trigger value changes to OK. *Note*: To receive a recovery message, "Trigger value=*Problem*" must be present in action conditions; "Trigger value=*OK*", however, must not be present. (If "Trigger value=*OK*" is set, the recovery message will not work; instead you will get a full escalation of defined messages and/or remote commands in the same way as for a problem situation). *Recovery message* will be sent only to those who received any messages regarding the problem before. A recovery message inherits acknowledgement status and history from the problem event (such as when expanding {EVENT.ACK.HISTORY} and {EVENT.ACK.STATUS} macros). If using {EVENT.*} macros in a recovery message, they will refer to the problem event (not the OK event). {EVENT.RECOVERY.*} macros will **only** expanded in a recovery message and will refer to the recovery/OK event.
Recovery subject	Recovery message subject. It may contain macros. It is limited to 255 characters
Recovery message	Recovery message. It may contain macros. It is limited to certain amount of characters depending on the type of database (see Sending message for more information).
Enabled	Mark the checkbox to enable the action. Otherwise it will be disabled.

5.1.3 CY NCP Service Desk Email Monitoring

For our project, the email notification will be sent to CY NCP Service Desk, in ncp.helpdesk@mphs.moh.gov.cy.

The NCP Service Desk Administrators have access to that email account using their credentials, through the secured Governmental Network using the following website: http://mail.intranet.gov.cy/mail/mphsncphd.nsf

Responsible to access the Zabbix notifications through email are Eleftheria Giorgitsi (Service Desk Leader), Mr. Eraclis Kyriakides, Dr. Florentia Zeitouni and Mrs. Christiana Valianti. After receiving a notification, they will inform the NCPeH System administrator to address the issues.

6   Zabbix Agents (clients) Configuration

Zabbix Agent is required to install on all remote systems needs to monitor through Zabbix server. The Zabbix Agent collects resource utilization and applications data on the client system and provides such information to the Zabbix server on their requests.

There are two types of checks can be configured between Zabbix Server and Client.

- Passive check – Zabbix Agent only sent data to server on their request.
- Active check – Zabbix Agent sends data periodically to Server.

After installing Zabbix server on 10.227.97.63, we installed zabbix agent (client) on Ubuntu 16.04 LTS systems:

- OpenNCP A Gateway: 10.227.98.83
- OpenNCP: 10.227.98.82
- MySQL cluster: 10.227.96.51 (master node)
- Application Zone: 10.227.97.61, 10.227.97.62
- Portal Zone: 10.227.105.10, 10.227.105.11

Zabbix agents listen to port 10050.

The steps followed on each of the aforementioned nodes are:

6.1.1   Step 1 – Enable Apt Repository

Zabbix apt repositories `are` available on Zabbix official website. Add the repository to install required packages for Zabbix agent using the following command.

```
wget
https://repo.zabbix.com/zabbix/4.2/ubuntu/pool/main/z/zabbix-
release/zabbix-release_4.2-1+xenial_all.deb
sudo dpkg -i zabbix-release_4.2-1+xenial_all.deb
sudo apt update
```

6.1.2   Step 2 – Install Zabbix Agent

As we have successfully added Zabbix apt repositories in your system let's use the following command to install Zabbix agent using the following command

```
sudo apt -y install zabbix-agent
```

6.1.3   Step 3 – Configure Zabbix Agent

After installation of Zabbix agent we edit Zabbix agent's configuration file /etc/zabbix/zabbix_agentd.conf and update Zabbix server IP.

```
sudo vim /etc/zabbix/zabbix_agentd.conf

#Server=[zabbix server ip]
```

```
#ServerActive=[zabbix server ip]
#Hostname=[Hostname of client system ]
Server=10.227.97.63
ServerActive=10.227.97.63
Hostname=ps_CDA
```

Here **10.227.97.63** is the IP of Zabbix server to allow for connection with this Zabbix client.

6.1.4   Step 4 – Restart Zabbix Agent

After adding Zabbix server IP in the configuration file, now restart agent service using below command.

```
sudo systemctl start zabbix-agent
```

To start and stop zabbix-agent service anytime use following commands.

```
sudo systemctl stop zabbix-agent
sudo systemctl status zabbix-agent
```

6.1.5   Zabbix Server Configuration to monitor Zabbix agents

We login to Zabbix server frontend via the interface: http://10.227.97.63/zabbix/index.php

After logging into the Zabbix server frontend, the following Dashboard is displayed:

To configure a host in Zabbix frontend, we do the following:
- Go to: *Configuration → Hosts*
- Click on *Create host* to the right (or on the host name to edit an existing host)
- Enter parameters of the host in the form

The following image shows all the aforementioned nodes that Zabbix agents are installed on.

In order to preview critical information about the nodes of the infrastructure you can do the following:

- Go to: Monitoring → Screens
- Select "Zabbix Overall System" screen

Data overview

Group: Linux servers

Hosts	CpuLoad	CpuUtil	Host name of Zabbix agent running	UpTime	Version of Zabbix agent running	Zabbix agent ping
Application A			app_A	52y 1m 28d	4.2.4	Up (1)
Application B			app_B	61y 2m 18d	4.2.4	Up (1)
MySQL Master Node			master_node	29y 11m 24d	4.2.4	Up (1)
OpenNCP			opencp	26y 5m 16d	4.2.4	Up (1)
OpenNCP A Gateway			ps_CDA	52y 1m 28d	4.2.4	Up (1)
Portal Master			master_web	52y 1m 28d	4.2.4	Up (1)
Portal Slave						

Updated: 00:50:16

System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	91	8 / 0 / 83
Number of items (enabled/disabled/not supported)	130	110 / 0 / 20
Number of triggers (enabled/disabled [problem/ok])	71	71 / 0 [1 / 70]
Number of users (online)	2	1
Required server performance, new values per second	2.14	

Updated: 00:50:16

7 Apache Tomcat Services Monitoring from Zabbix Server

7.1.1 Client Machine (Tomcat server) Configuration

In order to configure out Tomcat server, we go to our client machine then go to Tomcat folder then find bin folder now open catalina.sh file for setup Java and Tomcat remote allow.

```
sudo vim /opt/tomcat/bin/catalina.sh
```

Then setup CATALINA_OPTS config into catalina.sh file.

```
CATALINA_OPTS="$CATALINA_OPTS -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=12345 -
Dcom.sun.management.jmxremote.authenticate=false -
Dcom.sun.management.jmxremote.ssl=false -
Djava.rmi.server.hostname=CLIENT_IP_ADDR"
```

```
sudo service tomcat restart
```