Logicom Solutions | Managed Services

Author: Spyros Anemogiannis

Date: February 2021

Logicom Solutions | Managed Services

Table of Contents

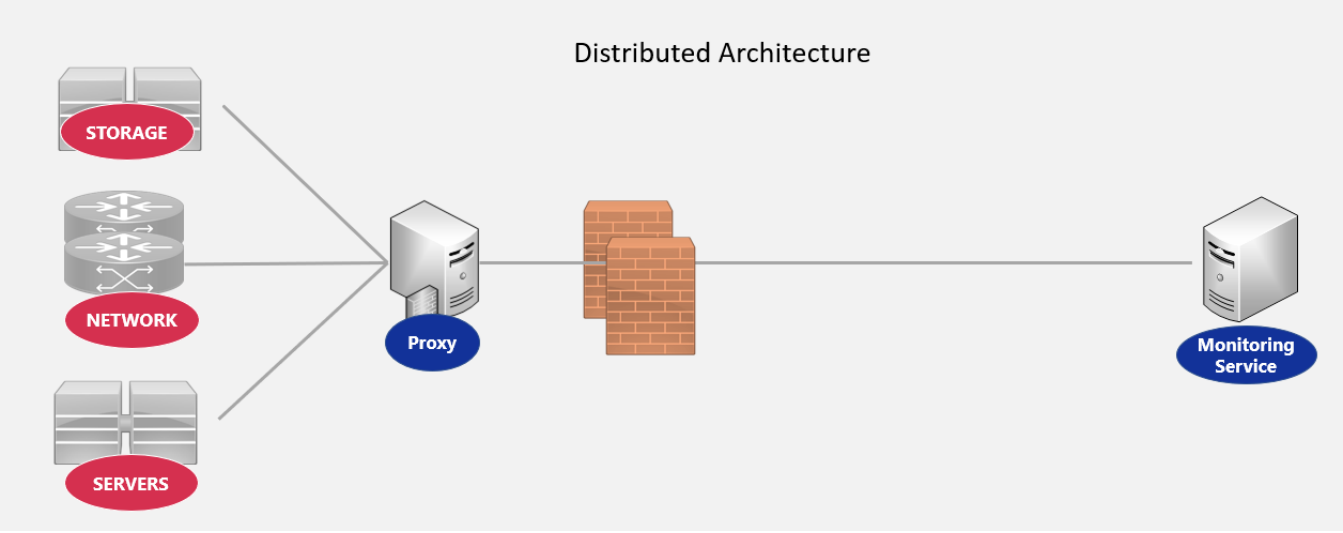
1. Proxy Architecture

The proxy is a software that will collect information about a monitored environment and sends it to the central server. This a crucial part of the solution because it provides a secure and efficient way to communicate the monitored data of your local infrastructure environment to the central server in Logicom Data center without having to open numerous firewall sessions and ports.

All monitoring is done locally via the local proxy and the agents and then the proxy opens a single outgoing session to the central server and reports the data.

In that way, there is no need to open access in the firewall for every monitored system in order to report to the central server. In a case of no communication between proxy and central server, the proxy will store locally the data and send them to central server as soon as the communication is restored.

This architecture greatly simplifies the implementation and scalability of the solution as well as increases the performance of the central server.



Distributed Architecture using local Proxy server

Data Flow

According to the distributed architecture of the solution, the data will be send from the agents to the local proxy installed on your premises and then reported from the proxy to the central server located in Logicom premises.

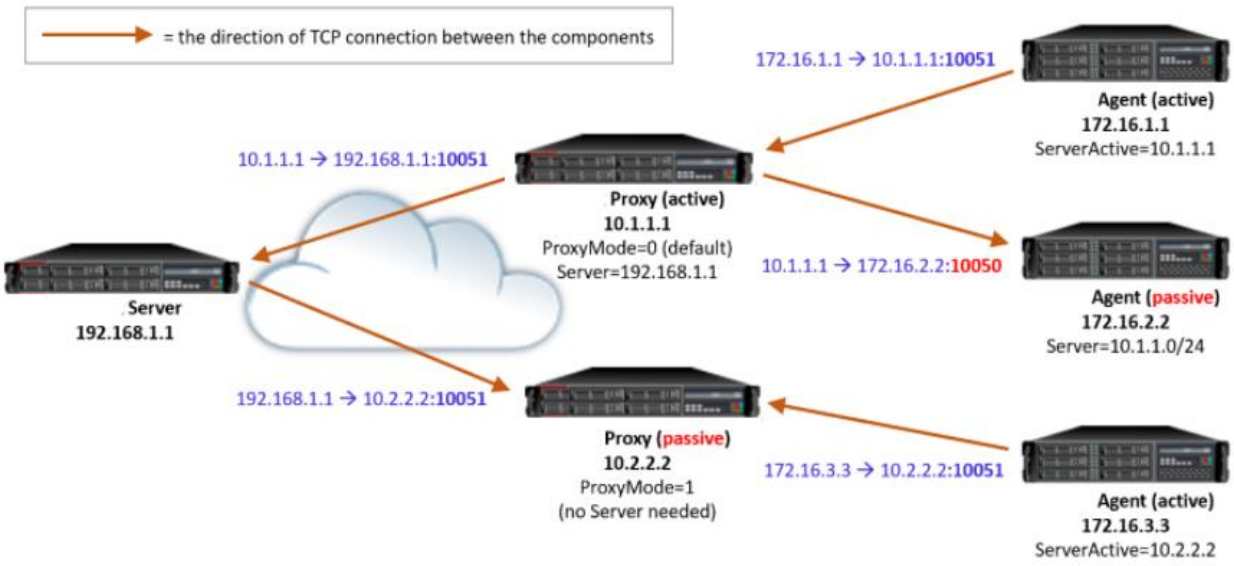
The communication between the local proxy and the central server has two options, Active and Passive mode where the **active mode is the recommended**.

Note that the active/passive mode used in proxy is not related to the active/passive mode of the agent. The proxy active/passive mode is only related to the communication between the central server and the local proxy:

Active = proxy will connect to server on port 10051

Passive = server will connect to proxy on port 10051

If a proxy is in passive mode, meaning that central server will poll local proxy for available data, an agent associated with that proxy can still be in active mode.



2. DOWNLOAD & INSTALL THE LOCAL PROXY

Step 1: Set SELinux to permissive/disable mode

```
# vi /etc/selinux/config
```

It is recommended to have SELinux in permissive mode

Step 2: Stop Local Firewall

First, disable the local firewall service in CentOS:

```
# sytemctl stop firewalld

#systemctl disable firewalld
```

Step 3: Download the Repository

This step is preparing adding the repository to CentOS so you can download and install the proxy package.

i. First, SSH to your CentOS Linux server

ii. Using the ***rpm*** command, download the proxy package. When you press Enter, your server will begin to download the package from repository. Then, you can install local proxy server direct from pre-compiled packages.

```
# rpm -Uvh https://repo.zabbix.com/zabbix/5.2/rhel/8/x86_64/zabbix-release-5.2-1.el8.noarch.rpm

# dnf clean all
```

Step 4: Install Local Proxy

There are 3 choices of package for the Local Proxy, depending which database you prefer, you run the corresponding install command: (we advise to use SQLite3 since it is simpler)

SQLite3

```
# dnf install zabbix-proxy-sqlite3 zabbix-agent
```

MySQL

```
# dnf install zabbix-proxy-mysql zabbix-agent
```

PostgreSQL

```
# dnf install zabbix-proxy-pgsql zabbix-agent
```

Step 5: Install Proxy Database

Depending on which flavor of Database you want to use, you should install the database package in CentOS server.

We recommend to use SQL Lite3 for easier setup.

For SQLite3:

```
# dnf install sqlite
```

For MySQL:

```
# dnf install mariadb-server
# systemctl start mariadb
# systemctl enable mariadb
```

Secure MySQL by changing the default password for MySQL root:

```
# mysql_secure_installation
```

```
Enter current password for root (enter for none): Press the Enter
Set root password? [Y/n]: Y
New password: <Enter root DB password>
Re-enter new password: <Repeat root DB password>
Remove anonymous users? [Y/n]: Y
Disallow root login remotely? [Y/n]: Y
Remove test database and access to it? [Y/n]:  Y
Reload privilege tables now? [Y/n]:  Y
```

Create Database with name = zabbix_db, user=zabbix, password = zabbixDBpass:

```
# mysql -uroot -p 'rootDBpass' -e "create database zabbix_db character set utf8 collate utf8_bin;"

# mysql -uroot -p 'rootDBpass' -e "grant all privileges on zabbix_db.* to zabbix@localhost identified by 'zabbixDBpass';"
```

For PostgreSQL:

```
# dnf module enable postgresql:12

# dnf install postgresql-server

# postgresql-setup –initdb

# systemctl start postgresql

# systemctl enable postgresql
```

Step 6: Import Initial DB Schema

Be aware that the Central Server schema is different from the Local Proxy schema. The Local Proxy should use it's own database and not the Zabbix Server's DB.

SQLite3

Note: You should make sure the directory you create the zabbix_db.db (e.g /etc/zabbix/) must have full access privileges (chmod 777)

Usually we use the directory: /etc/zabbix/ as the PATH for the zabbix_db.db

```
# zcat /usr/share/doc/zabbix-proxy-sqlite3*/schema.sql.gz | sqlite3 /etc/zabbix/zabbix_db.db
```

MySQL

```
# mysql -uroot -p'rootDBpass' zabbix_db -e "set global innodb_strict_mode='OFF';"
# zcat /usr/share/doc/zabbix-proxy-mysql*/schema.sql.gz | mysql -uzabbix -p zabbixDBpass zabbix_db
# mysql -uroot -p'rootDBpass' zabbix_db -e "set global innodb_strict_mode='ON';"
```

PostgreSQL

```
# zcat /usr/share/doc/zabbix-proxy-pgsql*/schema.sql.gz | sudo -u zabbix psql zabbix_db
```

3. EDIT LOCAL PROXY CONFIGURATION FILE

The Proxy Configuration file can be found in: /etc/zabbix/zabbix_proxy.conf

Key	Value	Notes
Proxymode	0	0 = Active Mode. This is the default already
Server	<central_server_ip address>	The public IP address of the central server (**not the local proxy IP address**). It will be provided to you by Logicom.
Hostname	<local_proxy_hostname>	**The hostname/IP address of the local Proxy**
DBName	<local_proxy_DB_name>	The local database name *** See Notes Below**

Note: Just use the same name as is returned from entering the command hostname on the proxy server:

```
# hostname
```

Note: Depending on the DB you are using, these are the parameters you have to edit in:

```
# vi /etc/zabbix/zabbix_proxy.conf
```

SQLite3

DBName= < Specify the path where zabbix db was created by zcat command > in Paragraph 2 – Step 6 >

MySQL/PostgreSQL

DBHost=localhost
DBName=zabbix_db
DBUser=zabbix
DBPassword= zabbixDBpass

4. START & ENABLE LOCAL PROXY PROCESS

To start a local proxy process and make it start at system boot:

```
# systemctl start zabbix-proxy

# systemctl enable zabbix-proxy
```

5. INSTALL SNMP ON LOCAL PROXY

For most of the cases, we will need to use SNMP in order to monitor local devices so we need to install snmp package on the Local Proxy Server:

```
#dnf install net-snmp net-snmp-libs net-snmp-utils

#systemctl enable --now snmpd
```

6. CONFIGURING PSK ENCRYPTION ON LOCAL PROXY (OPTIONAL)

The Monitored Service supports encrypted communications between central server and local proxy using Transport Layer Security (TLS) protocol v.1.2. You can use certificate-based and pre-shared key-based encryption (PSK), but in this tutorial we will configure the latter.

a. Generate PSK key on proxy server

Generate 256-bit (32 bytes) PSK key with openssl command:

```
# openssl rand -hex 32
```

Create and open file “zabbix_proxy.psk” with command:

```
# vi /etc/zabbix/zabbix_proxy.psk
```

and copy & paste that newly generated key into it.

Save and exit the file and set the correct file permission:

```
#chown zabbix:zabbix /etc/zabbix/zabbix_proxy.psk

#chmod 644 /etc/zabbix/zabbix_proxy.psk
```

b. Configure Local proxy to support PSK encryption

Open zabbix_proxy.conf file with command:

```
# vi /etc/zabbix/zabbix_proxy.conf
```

Now replace the variables in the proxy configuration file with the values below:

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/etc/zabbix/zabbix_proxy.psk
TLSPSKIdentity= ZBX-PSK
```

Save and exit file. Keep in mind that “TLSPSKIdentity” can be anything.

Don’t forget to restart local proxy server after changing the configuration file:

```
# vi systemctl restart zabbix-proxy
```

STEP 7: OPTIMIZING LOCAL PROXY SERVER

Open zabbix_proxy.conf file with command:

```
# vi /etc/zabbix/zabbix_proxy.conf
```

Replace the variable values in the proxy configuration file with the values below:

```
StartPollers=10
StartPollersUnreachable=5
StartPingers=10
StartTrappers=10
StartDiscoverers=15
StartHTTPPollers=5
StartVMwareCollectors=10
VMwareFrequency=60
CacheSize=128M
HistoryCacheSize=64M
HistoryIndexCacheSize=32M
ConfigFrequency=100
```

Save the config file and restart the local proxy:

```
# systemctl restart zabbix-proxy
```