Table of Contents

* [Zabbix Installion Lab](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_zabbix_installion_lab)
* [1. Set Up Zabbix Server](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_set_up_zabbix_server)
  + [1.1. Install Zabbix Server](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_install_zabbix_server)
  + [1.2. Start Zabbix Server and Configure HTTP](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_start_zabbix_server_and_configure_http)
* [2. Configure Zabbix Server Front End](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_configure_zabbix_server_front_end)
* [3. Configure Monitoring Templates](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_configure_monitoring_templates)
* [4. Prepare Zabbix Server for Auto Registration of Zabbix Agents](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_prepare_zabbix_server_for_auto_registration_of_zabbix_agents)
* [5. Install Zabbix Agents on Nodes](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_install_zabbix_agents_on_nodes)
* [6. Explore Zabbix Dashboard](https://www.opentlc.com/labs/ocp_operations/03_03_Zabbix_Monitoring_Lab.html#_explore_zabbix_dashboard)

Zabbix Installion Lab

1. Set Up Zabbix Server

In this section, you install the Zabbix Server. In this environment, you use the **Bastion** VM to run the Zabbix Server. Zabbix is located on **bastion.${GUID}.example.opentlc.com**.

|  |  |
| --- | --- |
|  | You can find detailed installation instructions for Zabbix Server at [Zabbix Server Installation with MySQL](https://www.zabbix.com/documentation/3.2/manual/installation/install_from_packages/server_installation_with_mysql" \t "_blank). |

1.1. Install Zabbix Server

1. Make sure you are logged in to your Bastion VM as **root**.
2. Add the repository for Zabbix:

rpm -ivh http://repo.zabbix.com/zabbix/3.2/rhel/7/x86\_64/zabbix-release-3.2-1.el7.noarch.rpm

1. Install MariaDB Server, MariaDB Client, Apache HTTP Server, and Zabbix Server:
2. yum repolist
3. yum -y install mariadb-server mariadb zabbix-server-mysql zabbix-web-mysql httpd
4. systemctl enable mariadb

systemctl start mariadb

1. Run **mysql\_secure\_installation** to set up your MariaDB instance with recommended security settings:

mysql\_secure\_installation

* + This also allows you to set a root password for your database. You may replace **MariaDB-Root** with a root password of your choice—just make sure you use the same password whenever the database root password is required.

1. Once the script runs and you are prompted for input, enter the following values:
   * **Enter current password for root (enter for none)**: **Enter**
   * **Set root password? [Y/n]** **Y**
   * **New password**: **MariaDB-Root**
   * **Re-enter new password**: **MariaDB-Root**
2. Type **Enter** to accept the defaults on all of the other prompts.
3. Create the Zabbix database, replacing **Zabbix-Root** with the password you chose:
4. mysql -uroot -pMariaDB-Root
5. mysql> create database zabbix character set utf8 collate utf8\_bin;
6. mysql> grant all privileges on zabbix.\* to zabbix@localhost identified by 'Zabbix-Root';

mysql> quit;

1. Populate the newly created database with Zabbix tables:

zcat /usr/share/doc/zabbix-server-mysql-3.2.\*/create.sql.gz | mysql -Dzabbix -uzabbix -pZabbix-Root

1. Edit **/etc/zabbix/zabbix\_server.conf** and update the following values, removing **#** when necessary:
2. DBHost=localhost
3. DBName=zabbix
4. DBUser=zabbix

DBPassword=Zabbix-Root

* + Be sure to use your chosen value for **DBPassword**.

1. Edit **/etc/selinux/config** and set **SELINUX=permissive** to disable SELinux.
   * Zabbix requires SELinux to be turned off.
2. At the command line, turn off SELinux for the current session:

setenforce Permissive

1. Update the Zabbix web front-end configuration by editing **/etc/httpd/conf.d/zabbix.conf** and updating the following values if necessary:
2. php\_value max\_execution\_time 300
3. php\_value memory\_limit 128M
4. php\_value post\_max\_size 16M
5. php\_value upload\_max\_filesize 2M
6. php\_value max\_input\_time 300
7. php\_value always\_populate\_raw\_post\_data -1

php\_value date.timezone America/New\_York

* + Most likely this includes removing the comment and setting the correct time zone.

1.2. Start Zabbix Server and Configure HTTP

1. Enable and start the Zabbix server:
2. systemctl enable zabbix-server

systemctl start zabbix-server

1. Make sure your Zabbix server is running:

systemctl status zabbix-server

1. Update the Apache HTTP server configuration to redirect **/** to **/zabbix** by opening **/etc/httpd/conf/httpd.conf** for editing, searching for "Redirect", and adding the following line to the **alias\_module** section:

RedirectMatch ^/$ /zabbix

1. Set SELinux rules for Zabbix to connect to the HTTP server, and enable and start the server:
2. setsebool -P httpd\_can\_connect\_zabbix on
3. systemctl enable httpd

systemctl start httpd

1. Make sure your Apache server is running:

systemctl status httpd

2. Configure Zabbix Server Front End

In this section, you access the Zabbix server, which starts the front-end configuration process.

1. Open your web browser and navigate to **http://bastion.$GUID.example.opentlc.com**:

|  |  |
| --- | --- |
|  | The documentation to install the Zabbix front end is located at [Zabbix Documentation 3.2](https://www.zabbix.com/documentation/3.2/manual/quickstart/login" \t "_blank). |

1. Follow the prompts of the configuration wizard by clicking **Next step**.
   * Make sure your Zabbix database password is the same one you set when configuring the Zabbix database earlier—for example, **Zabbix-Root**).
2. Accept the default values for everything else and click **Next step** until you see the success page.
3. Click **Finish**.
   * Expect to see the Zabbix login page.
4. Log in with the **Admin** username and **zabbix** as the password to see the Zabbix dashboard.
   * Note that the username and password are case-sensitive.

3. Configure Monitoring Templates

1. Download the OpenShift host templates from GitHub to your local workstation:

curl -o zabbix\_ocp\_templates.xml https://raw.githubusercontent.com/wkulhanek/openshift-zabbix/3.6/zabbix\_ocp\_templates.xml

1. Click **Configuration → Templates** to bring up the templates screen.
2. At the top right corner of the page, click **Import** to import the OpenShift host templates.
3. Click **Browse** and select the templates file you just downloaded.
4. Click **Import** to import the templates.

|  |  |
| --- | --- |
|  | * + By default the template to monitor the master API uses port **443** to check the OpenShift master public API. So if you need to change this to port **8443**:     1. Navigate to **Configuration → Templates → Template OS Linux - OCP Host - Master**.     2. Click **Macros**.     3. Change the effective value of your port from **443** to the desired value.     4. Click **Update**. |

4. Prepare Zabbix Server for Auto Registration of Zabbix Agents

1. Switch to **Configuration → Actions**.
2. From the **Event Source** list in the top right corner, select **Auto registration**.
3. Create three actions by clicking **Create action** and adding the following properties:

|  |  |  |
| --- | --- | --- |
| Name | Conditions | Operations |
| **Auto-register OCP Host** | **Host Metadata like OCP Host** | **Add Host**; **Add host to host groups**: OCP host; **Link to templates**: Template OS Linux—OCP Host |
| **Auto-register OCP Master** | **Host Metadata like OCP Master** | **Add Host**; **Add host to host groups**: OCP host; **Link to templates**: Template OS Linux—OCP Host, Templates OS Linux—OCP Node, Templates OS Linux—OCP Master |
| **Auto-register OCP Node** | **Host Metadata like OCP Node** | **Add Host**; **Add host to host groups**: OCP host; **Link to templates**: Template OS Linux—OCP Host, Templates OS Linux - OCP Node |

|  |  |
| --- | --- |
|  | Be careful when creating these Actions. The Zabbix User Interface is not very intuitive and it is very easy to miss a step. |

* 1. After you click the blue **Create action** button you will see a screen to add the Action. This screen has two tabs: **Action** and **Operations**. On the **Actions** specify the Condition and click the *underlined* **Add** link to save the action. It should be listed in the **Conditions** box like shown below.
  2. Then you need to switch to the **Operations** tab to add the three operations. On the Operations screen you have to click the *underlined* **New** link to create a new operation. Select the operation (e.g. **Add host to host groups**) and then specify any optional parameters to the operation again before clicking the *underlined* **Add** link.

|  |  |
| --- | --- |
|  | If you accidentally click the blue **Add** button before you are finished, simply open the item again and resume editing. |

* + - Expect your final configuration to look like this:
    - Your Zabbix server is now ready to be discovered by Zabbix agents.

1. Switch back to the main dashboard by clicking **Monitoring → Dashboard**.

5. Install Zabbix Agents on Nodes

1. On your **bastion** host as **root**, clone the **openshift-zabbix** project. This project contains the playbooks and configuration files to set up all of the Zabbix agents on all of the OpenShift nodes:
2. cd /root
3. git clone https://github.com/wkulhanek/openshift-zabbix
4. cd openshift-zabbix

git checkout 3.6

1. Edit the file **zabbix\_vars.yml** and make sure that **zabbix\_host** points to the Zabbix server you previously installed.
   * You will need to change the GUID from **mon** to match your environment.
2. Run the playbook to install the agents on all of the nodes:

ansible-playbook install-zabbix-agents.yml

* + The playbook picks up all of the hosts to install the Zabbix agent to from the OpenShift Ansible **/etc/ansible/hosts**configuration file. If your Ansible hosts file is in a different location, include **-i /path/to/your/hosts\_file** as a parameter.

1. Run the playbook to configure the agents on all of the nodes:

ansible-playbook configure-zabbix-agents.yml

* + This includes everything necessary to deploy and configure the Zabbix agent along with associated scripts to OpenShift nodes. Because you set up automatic discovery of Zabbix agents on the Zabbix server, no other steps are necessary.

1. Log in to your Zabbix server and verify that all of the nodes were discovered automatically and added to the list of monitored nodes.
   * This may take a few minutes.
2. Examine the dashboard and expect it to show all discovered hosts as green—without problems—and that they are part of the **OCP host** group.:
3. Switch to **Configuration → Hosts** to see details about the automatically registered OpenShift nodes:
   * Note how there is a green **ZBX** status indicating that the Zabbix server can communicate with the agent. Also note that there are a number of applications and triggers set up for each host.

Your Zabbix Environment is now fully configured to monitor your environment.

6. Explore Zabbix Dashboard

1. Explore the Zabbix dashboard further.
2. Investigate some of the templates.

In a real-world environment, your next step is to set up alerting to make sure that any abnormality is reported immediately. This can be done via email, Slack, Pager, SMS or other means. In the lab environment, you do not have any of those available, so skip this step. Should something go wrong, an alert is raised but not sent to any recipients. Instead it is displayed on the dashboard.

Build Version: be32934b41da1e34c27e21e79bdf57d30c732a3e : Last updated 2018-01-19 05:59:04 EST