



Step 8: Install MapR Monitoring

To provide metrics monitoring, the MapR Control System (MCS) requires the `collectd` and `OpenTSDB` components to be installed. The logging components of MapR Monitoring are optional. MapR Monitoring components are available as part of the MapR Expansion Pack (MEP) that you selected for the cluster.

 **Note:** As of MapR 6.0, if you install MapR Monitoring on a secure cluster, you must generate the Elasticsearch keys, certifications, and trust stores on an Elasticsearch node (designated as the master) and then distribute them to the other Elasticsearch nodes in the cluster, as shown below in step 4.

Complete the steps to install MapR Monitoring as the `root` user or using `sudo`.

1. For metric monitoring, install the following packages:


Component	Requirements
collectd	Install the <code>mapr-collectd</code> package on each node in the MapR cluster.
OpenTSDB and AsyncHBase	Install the <code>mapr-opentsdb</code> on one or more nodes. To allow failover of metric storage in the event that one OpenTSDB node is unavailable, install OpenTSDB on at least three nodes in the cluster.  Note: <code>mapr-opentsdb</code> is dependent on <code>mapr-asynchbase</code> and <code>mapr-asynchbase</code> is automatically installed on the node where you install <code>mapr-opentsdb</code> .
Grafana	Install the <code>mapr-grafana</code> package on at least one node in the MapR cluster.

On a three node cluster, you could run the following commands to install metric packages:

- For CentOS/RedHat:
 - Node A: `yum install mapr-collectd mapr-grafana`
 - Node B: `yum install mapr-collectd mapr-opentsdb`
 - Node C: `yum install mapr-collectd`
- For Ubuntu:
 - Node A: `apt-get install mapr-collectd mapr-grafana`
 - Node B: `apt-get install mapr-collectd mapr-opentsdb`
 - Node C: `apt-get install mapr-collectd`
- For SUSE:
 - Node A: `zypper install mapr-collectd mapr-grafana`
 - Node B: `zypper install mapr-collectd mapr-opentsdb`
 - Node C: `zypper install mapr-collectd`

2. Optional: For log monitoring, install the following packages:

Component	Requirements
fluentd	Install the <code>mapr-fluentd</code> package on each node in the cluster.
Elasticsearch	Install the <code>mapr-elasticsearch</code> package on at least 3 nodes in the cluster to allow failover of log storage in the event that one Elasticsearch node is unavailable.
Kibana	Install the <code>mapr-kibana</code> package on at least one node in the cluster.

 **Note:** On secure Ubuntu 14.04 or 16.04 clusters, Elasticsearch can fail to generate a keystore password if the `uuid-runtime` package is not installed. `uuid-runtime` is one of the package dependencies required for installing without the MapR Installer. See the entry for SPYG-934 and `uuid-runtime` in the [MapR Monitoring Known Issues](#) (`../ReleaseNotes/c_known_issues.html#concept_qpc_pvb_tt__section_egs_rnh_5bb`).

For example, on a three node MapR cluster, you can run the following commands to install log packages:


- For CentOS/RedHat:
 - Node A: `yum install mapr-fluentd mapr-elasticsearch`
 - Node B: `yum install mapr-fluentd mapr-elasticsearch`
 - Node C: `yum install mapr-fluentd mapr-elasticsearch mapr-kibana`
- For Ubuntu:
 - Node A: `apt-get install mapr-fluentd mapr-elasticsearch`
 - Node B: `apt-get install mapr-fluentd mapr-elasticsearch`
 - Node C: `apt-get install mapr-fluentd mapr-elasticsearch mapr-kibana`
- For SUSE:
 - Node A: `zypper install mapr-fluentd mapr-elasticsearch`
 - Node B: `zypper install mapr-fluentd mapr-elasticsearch`
 - Node C: `zypper install mapr-fluentd mapr-elasticsearch mapr-kibana`


3. *For secure MapR clusters*, run `maprlogin print` to verify that you have a MapR user ticket for the `mapr` user and the `root` user. These user tickets are required for a successful installation.

If you need to generate a MapR user ticket, run `maprlogin password`. For more information, see [Generating a MapR User Ticket](#) (`../SecurityGuide/GeneratingMapRUserTicket.html#TicketsandCertificates-Ge_26281159-d3e202`)




4. *For secure MapR clusters*, complete the following steps to generate the Elasticsearch keys, certifications, and trust stores on the master Elasticsearch node and then distribute them to the other Elasticsearch nodes:
- Select one Elasticsearch node as the master, and run `configure.sh -R` on that node.
 - Run the following command on the master Elasticsearch node:

```
/opt/mapr/server/configure.sh -OT <comma-separated list of OpenTSDB nodes> -ES <comma-separated list of Elasticsearch nodes> -R -EPElasticsearch -genESKeys
```

 **Note:** The table in step 5 lists descriptions for parameters used in this command.

 **Important:** If DNS resolution on the nodes is not completely configured, running the `configure.sh -genESKeys` step will fail. For example, key creation will fail if reverse lookups do not work. Suppose that the DNS lookup for a node with `hostname node1.qa.lab` returns `192.100.1.1`. If the DNS lookup for `192.100.1.1` returns nothing (instead of `hostname node1.qa.lab`), key creation will fail.

c. Copy the specified files to the locations indicated in the table below:

File	Permissions	Copy from location (on master)	Copy to location (on other ES nodes)*
es-root-ca.pem	0600	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/ca/es-root-ca.pem	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/ca
truststore.jks	0640	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/truststore.jks	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/keystores
admin-usr-keystore.jks	0640	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/admin-usr-keystore.jks	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/keystores/admin-usr-keystore.jks
<node-fqdn>-srvr-keystore.jks	0640	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/<node-fqdn>-srvr-keystore.jks	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/keystores  Note: Only include the file that matches the nodename.
sg2.yml	0600	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/sg2.yml	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/
sg_http_<node-fqdn>.yml	0600	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/sg_http_<node-fqdn>.yml	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch  Note: Only include the file that matches the nodename.
sg_ssl_<node-fqdn>.yml	0600	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/sg_ssl_<node-fqdn>.yml	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch  Note: Only include the file that matches the nodename.
.keystore_password	0600	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/.keystore_password	/opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/.keystore_password


*The **Copy to** directories might not exist and might need to be created.




d. Copy the `es-root-ca.pem` file from the master Elasticsearch node to each Kibana node, as shown:

```
cp /opt/mapr/elasticsearch/elasticsearch-5.4.1/etc/elasticsearch/sg/ca/es-root-ca.pem /opt/mapr/kibana/kibana-5.4.1/config/ca/es-root-ca.pem
```

5. Run `configure.sh` on each node in the MapR cluster with the `-R`, `-ES`, and `-OT` parameters. Optionally, you can include the `-ESDB` parameter. You must have a warden service running during `configure.sh -R -OT`.

```
/opt/mapr/server/configure.sh -R -ES <comma-separate list of Elasticsearch nodes> -OT <comma-separate list of OpenTSDB nodes> [-ESDB <filepath>]
```

Parameter	Description
-R	After initial node configuration, specifies that configure.sh should use the previously configured ZooKeeper and CLDB nodes.
-ES	Specifies a comma-separated list of host names or IP addresses that identify the Elasticsearch nodes. The Elasticsearch nodes can be part of the current MapR cluster or part of a different MapR cluster. The list is in the following format: <ul style="list-style-type: none">hostname/IPaddress[:port_no] [,hostname/IPaddress[:port_no]...]  Note: The default Elasticsearch port is 9200. If you want to use a different port, specify the port number when you list the Elasticsearch nodes.

Parameter	Description
-OT	<p>Specifies a comma-separated list of host names or IP addresses that identify the OpenTSDB nodes. The OpenTSDB nodes can be part of the current MapR cluster or part of a different MapR cluster. The list is in the following format:</p> <ul style="list-style-type: none">hostname/IP address[:port_no] [,hostname/IP address[:port_no]...] <p> Note: The default OpenTSDB port is 4242. If you want to use a different port, specify the port number when you list the OpenTSDB nodes.</p> <p> Note: You must have a warden service running during <code>configure.sh -R -OT</code>.</p>
-ESDB	<p>Specifies a non-default location for writing index data on Elasticsearch nodes. In order to configure a index location, you only need to include this parameter on Elasticsearch nodes. By default, the Elasticsearch index is written to <code>/opt/mapr/elasticsearch/elasticsearch-<version>/var/lib/MaprMonitoring/</code>.</p> <p> Note: Elasticsearch requires a lot of disk space. Therefore, a separate file system for the index is recommend. It is not recommended to store index data under the <code>/</code> or the <code>/var</code> file system.</p>

For example, to configure MapR Monitoring components you can run one of the following commands:

- In this example, a location is specified for the Elasticsearch index directory, and default ports are used for Elasticsearch and OpenTSDB nodes.

```
/opt/mapr/server/configure.sh -R -ES NodeA,NodeB,NodeC -OT NodeB -ESDB /opt/mapr/myindexlocation
```

- In this example, non-default ports are specified for Elasticsearch and OpenTSDB nodes, and the default location is used for the Elasticsearch index directory.

```
/opt/mapr/server/configure.sh -R -ES NodeA:9595,NodeB:9595,NodeC:9595 -OT NodeB:4040
```

After you run `configure.sh -R`, if errors are displayed see [Troubleshoot MapR Monitoring Installation Errors](#) (TroubleshootMonitoringInstall.html#concept_k4r_y2h_qw).


6. To start collecting metrics for the NodeManager and ResourceManager services, restart these services on each node where they are installed.

```
maprcli node services -name nodemanager -nodes <space separated list of hostname/IPaddresses> -action restart
```

```
maprcli node services -name resourcemanager -nodes <space separated list of hostname/IPaddresses> -action restart
```

7. If you installed Kibana, perform the following steps: :

- Use one of the following methods to load the Kibana URL:
 - From the MCS, select the **Kibana** view. After you select the **Kibana** view, you may also need to select the **Pop-out page into a tab** option.
 - From a web browser, launch the following URL: `https://<IPaddressOfKibanaNode>:5601`
- When the Kibana page loads, it displays a `Configure an index pattern` screen. Provide the following values:

 **Note:** The **Index contains time-based events** option is selected by default and should remain selected.

Field	Value
Index name or pattern	mapr_monitoring-*
Time-field	@timestamp

- Click **Create**.