**Purpose:**

To install on a suitable server the Elasticsearch search capability, as a service (daemon). This offers fast response to queries.

Linux versions all strongly prefer that applications be installed via a Package Manager, and this process uses the RPM package installed by DFF on RHEL8.

Elasticsearch is the distributed search and analytics engine at the heart of the Elastic Stack. Logstash and Beats facilitate collecting, aggregating, and enriching your data and storing it in Elasticsearch. Kibana enables you to interactively explore, visualize, and share insights into your data and manage and monitor the stack. Elasticsearch is where the indexing, search, and analysis magic happens.

Elasticsearch provides near real-time search and analytics for all types of data. Whether you have structured or unstructured text, numerical data, or geospatial data, Elasticsearch can efficiently store and index it in a way that supports fast searches. You can go far beyond simple data retrieval and aggregate information to discover trends and patterns in your data. And as your data and query volume grows, the distributed nature of Elasticsearch enables your deployment to grow seamlessly right along with it.

While not *every* problem is a search problem, Elasticsearch offers speed and flexibility to handle data in a wide variety of use cases:

* Add a search box to an app or website
* Store and analyze logs, metrics, and security event data
* Use machine learning to automatically model the behavior of your data in real time
* Automate business workflows using Elasticsearch as a storage engine
* Manage, integrate, and analyze spatial information using Elasticsearch as a geographic information system (GIS)
* Store and process genetic data using Elasticsearch as a bioinformatics research tool

| **Step** | **Major Activity** | **References, Forms and Details** |
| --- | --- | --- |
| 1 | Switch to superuser  sudo -i | * Need frequent higher privileges, and this saves re-entering pw. |
| 2 | Create a file called **elasticsearch.repo** in the /etc/yum.repos.d/ directory for RedHat based distributions, or in the /etc/zypp/repos.d/ directory for OpenSuSE based distributions, containing:  [elasticsearch]  name=Elasticsearch repository for 7.x packages  baseurl=https://artifacts.elastic.co/packages/7.x/yum  gpgcheck=1  gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch  enabled=0  autorefresh=1  type=rpm-md | * The configured repository is disabled by default. This eliminates the possibility of accidentally upgrading elasticsearch when upgrading the rest of the system. |
| 3 | sudo dnf install --enablerepo=elasticsearch elasticsearch | * Each install or upgrade command must explicitly enable the repository as indicated in the sample command. * Main installation at /usr/share/elasticsearch * daemon service file at /usr/lib/system/system/Elasticsearch.service * startup parameters are in /etc/Elasticsearch * log files at /var/log/elasticsearch |
| 4 | Review configuration parameters. 340-F10 | * Form 340-F10 lists normal variable locations * Defaults are normally suitable. |
| 5 | May need to add into config/elasticsearch.yml:  xpack.ml.enabled: false | * Disables the machine learning if older equipment |
| 6 | For slower computers, may need to increase startup timeout in elasticsearch.service:  TimeoutStartSec=500 | * Found in (soft link):   /etc/systemd/system/multi-user.target.wants |
| 7 | systemctl daemon-reload | * Reload all Linux daemons |
| 8 | systemctl enable elasticsearch.service | * Enable Elasticsearch daemon |
| 9 | systemctl start elasticsearch.service | * Start Elasticsearch daemon |
| 10 | systemctl status elasticsearch.service | * Ensure Elasticsearch running |
| 11 | Curl http://localhost:9200 | * Double-check Elasticsearch is running on internal port 9200 * port should **not** be public * should see:   {  "name" : "Zoo-Soggy-new",  "cluster\_name" : "elasticsearch",  "cluster\_uuid" : "IQ74\_I0gSZaALI9tq\_BPHg",  "version" : {  "number" : "7.13.3",  "build\_flavor" : "default",  "build\_type" : "rpm",  "build\_hash" : "5d21bea28db1e89ecc1f66311ebdec9dc3aa7d64",  "build\_date" : "2021-07-02T12:06:10.804015202Z",  "build\_snapshot" : false,  "lucene\_version" : "8.8.2",  "minimum\_wire\_compatibility\_version" : "6.8.0",  "minimum\_index\_compatibility\_version" : "6.0.0-beta1"  },  "tagline" : "You Know, for Search"  } |