# Analysis Cockpit Elasticsearch Cluster Manual

Nextron Systems

Apr 25, 2024

# CONTENTS

In this Manual we will describe how you can set up your Analysis Cockpit with an Elasticsearch Cluster. Please follow the sections thoroughly to get the desired result.

CHAPTER

ONE

# INTRODUCTION

## 1.1 Analysis Cockpit Architecture

The ASGARD Analysis Cockpit uses an Elasticsearch database to store all event data. Each day worth of incoming events uses a single Elasticsearch index.

Normally, Elasticsearch is running locally on the Analysis Cockpit Server. However, when required Elasticsearch can easily be extended to become a cluster of almost arbitrary size.

When running in Cluster mode, the Analysis Cockpit runs the underlying metadata database and acts as the cluster master, while all data is stored on the additional nodes.

## 1.2 When to consider Clustering

You should consider extending the Elasticsearch installation to become a cluster if:

- there is significant performance degradation
  - for searches that cover multiple days and/or
  - for adding events to cases.
- performance cannot be sufficiently improved by adding more CPU cores or faster disks (RAM is supported up to 32GB)
- disk size of the analysis cockpit cannot be increased but retention period requires additional storage

## 1.3 Performance

Benchmarks suggest there is a communication overhead of 10% - 20% for a cluster compared to a single node in cases where a single node would be sufficient for the given load.

As logs of one day are stored in one index and indices are distributed over cluster members the performance gain will also depend on the number of days stored in the cluster.

In a cluster configuration the former Analysis Cockpit will act a master and will hold no data. Therefore, the minimum reasonable cluster size is three. In such a minimum configuration we expect a performance gain of 60% given we have at least 60 days of logs.

CHAPTER

TWO

# ANALYSIS COCKPIT SETUP

This chapter walks you through the necessary steps to set up the Analysis Cockpit for use with a cluster of Elasticsearch nodes.

## 2.1 Prerequisites

The Elasticsearch Cluster setup requires:

- A fully functional installation of Analysis Cockpit version 4.x
- At least two additional nodes with a similar high-end spec
- High-performance low-latency networking between all nodes
- All the nodes have a FQDN and can resolve each other's FQDNs and the Analysis Cockpit's FQDN

## 2.2 Analysis Cockpit preparation

After installation, the Analysis Cockpit runs with a single local Elasticsearch instance as usual. To prepare it for use with a cluster, run `es-cluster-setup.sh`:

```
nextron@cockpit4:~$ sudo /usr/share/asgard-analysis-cockpit/scripts/es-cluster-setup.sh
```

The script will configure Elasticsearch in the following way:

- The Analysis Cockpit node continues to be the master node but data is automatically moved away from it once possible.
- SSL certificates are used for authentication of nodes.
- Any number of data nodes can be added with exactly the same configuration and certificate (as long as they are reachable).

---

**Hint:** The script will display two errors (`xpack.security.transport.ssl...`) which can be ignored. These are due to the fact that the script is setting up the configuration for the cluster node.

---

## 2.3 Resulting Elasticsearch configuration

The Elasticsearch configuration can be found in `/etc/elasticsearch/elasticsearch.yml`. It will look like the following:

```
cluster.name: elasticsearch
cluster.routing.allocation.exclude._name: elastic-test-01.nextron
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
node.roles: [ master, data, ingest ]
http.host: "_local:ipv4_"
transport.host: "_site:ipv4_"
discovery.seed_hosts: [ elastic-test-01.nextron ]
cluster.initial_master_nodes: [ elastic-test-01.nextron ]
search.default_allow_partial_results: false
xpack.security.enabled: true
xpack.security.enrollment.enabled: false
xpack.security.http.ssl.enabled: false
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  client_authentication: required
  keystore.path: /etc/elasticsearch/elastic-certificates.p12
  truststore.path: /etc/elasticsearch/elastic-certificates.p12
```

The configuration:

- Designates the Analysis Cockpit node as the (only) cluster master.
- Automatically moves existing data away from the Analysis Cockpit node, and distributes it across the other nodes.
- TLS security is enabled so that nodes authenticate by certificate.

## 2.4 Cluster Node configuration

In addition to reconfiguring the Analysis Cockpit, `es-cluster-setup.sh` will create a configuration file `clusternode.conf` which contains the required configuration for additional nodes to join the cluster. The file can be found on your Analysis Cockpit in the home directory of the nextron user (`/home/nextron`).

If you executed the script as root user, the file will be located in `/usr/share/asgard-analysis-cockpit/scripts/clusternode.conf`.

Download this configuration file for further usage in our Nextron Universal Installer (*Cluster Node Setup*).

## 2.5 Restarting Elasticsearch

Finally, restart elasticsearch so that it picks up the new configuration:

```
nextron@cockpit4:~$ sudo systemctl restart elasticsearch
```

Your Analysis Cockpit is now ready to be used in a cluster setup.

CHAPTER

THREE

# CLUSTER NODE SETUP

This chapter will guide you through the installation of the Elasticsearch Cluster Node for the ASGARD Analysis Cockpit.

## 3.1 Nextron Universal Installer

The Nextron Universal Installer is a web based installer which will guide you through the installation of our ASGARD products. The Nextron Universal Installer will install **one** of the following products on your server (this manual focuses on the `Elasticsearch Cluster Node for ASGARD Analysis Cockpit`):

- ASGARD Management Center; alternatively if your license permits:
  - ASGARD Broker
  - ASGARD Gatekeeper
  - ASGARD Lobby
- Master ASGARD
- ASGARD Analysis Cockpit; alternatively:
  - Elasticsearch Cluster Node for ASGARD Analysis Cockpit
- ASGARD Security Center, in the following variants:
  - ASGARD Security Center (Backend Only)
  - ASGARD Security Center (Frontend Only)
  - ASGARD Security Center (All-in-one, unrecommended)

---

**Note:** You can only install one product on one server, since the products are not designed to coexist on the same server. The exception being the ASGARD Security Center (All-in-one).

---

The installation takes roughly between 5-15 minutes, depending on your internet connection and the server you are installing the product on.

If you encounter problems during your installation, please see *Diagnostic Pack* for further instructions.

## 3.2 Requirements

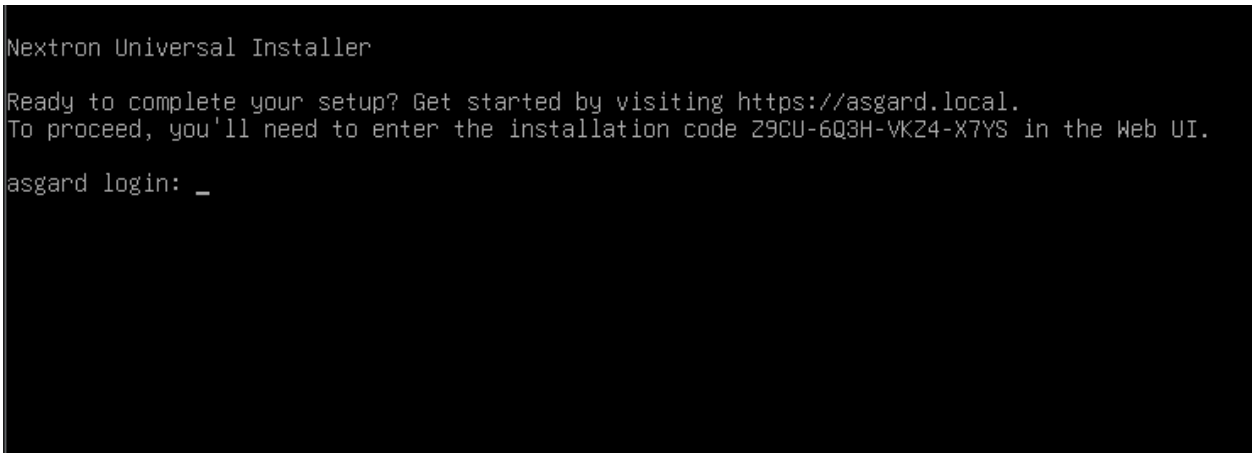
The installation of the `Elasticsearch Cluster Node for ASGARD Analysis Cockpit` requires the following:

- A valid license file for the ASGARD Analysis Cockpit
- A configured FQDN with working DNS resolution
- Internet access during installation (see *Connectivity Check*)
- All nodes must be able to reach each other by resolving the fully qualified host name.
- TCP port 9300 must be open between all nodes.
- `clusternode.conf` generated by the ASGARD Analysis Cockpit (see *Cluster Node configuration*)

## 3.3 Installation

Install the server from the Nextron ISO base image as you normally would when installing the Analysis Cockpit itself.

After the ISO installer is finished with the setup, you will be greeted at the console login prompt with the following message:




Follow the instructions and navigate to the webpage displayed on your console. You will most likely get a browser warning when you connect the first time to the page. This is due to the page using a self signed certificate, since it will only be used to install the Elasticsearch Cluster Node. You can safely ignore this warning and proceed to the page.

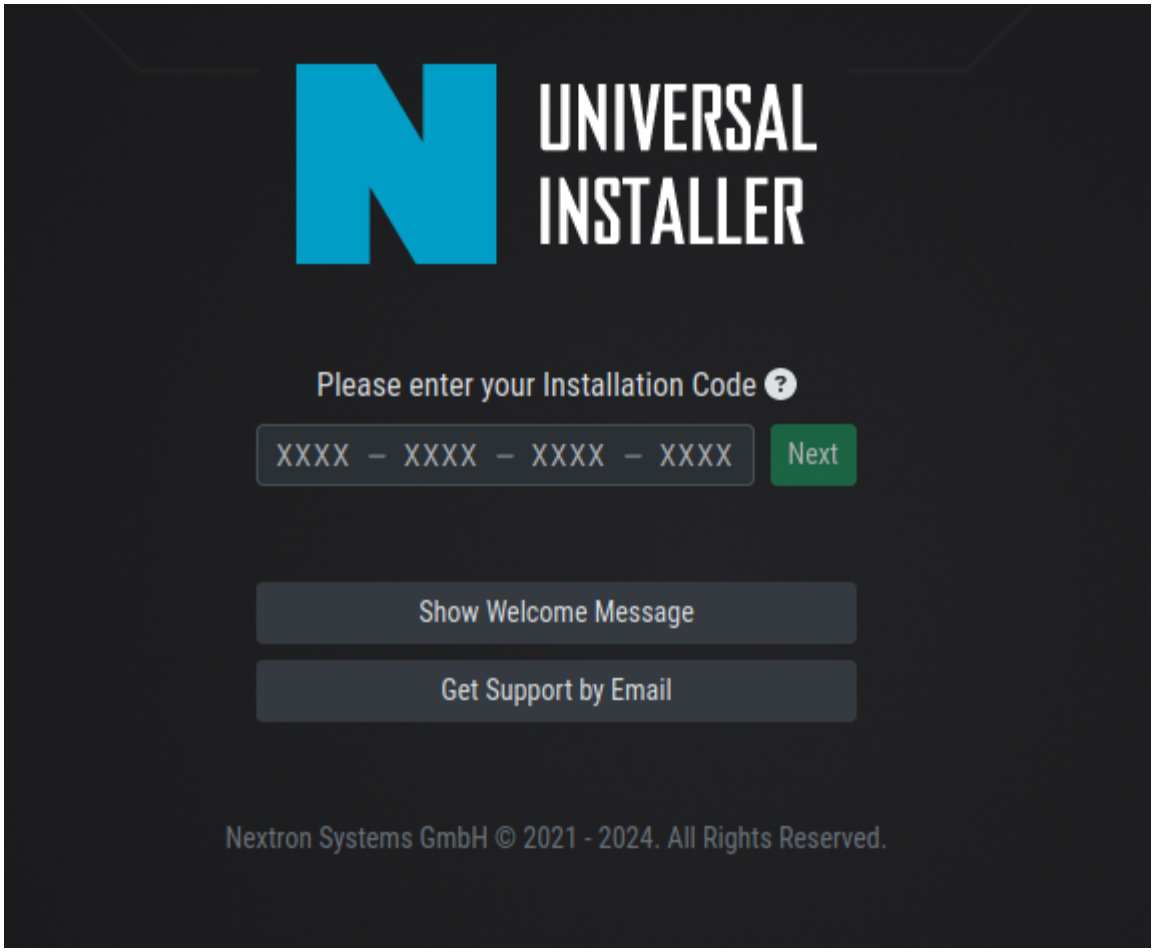
You will be greeted with a small introduction as to what the Nextron Universal Installer is and what it does. After you click `Next`, you will be presented with the landing page of the Nextron Universal Installer.

Enter the Installation Code from the terminal and click `Next`. The Installer will now guide you through the installation.

You will be prompted at one point to upload your cluster configuration file. This file is generated by the Analysis Cockpit and contains all the necessary information for the Elasticsearch Cluster Node to join the cluster.

Please see *Resulting Elasticsearch configuration* for further information on how to generate the cluster configuration file.

Once the installation is finished, your Cluster Node is a part of the Analysis Cockpit cluster and will start receiving data.


UNIVERSAL
INSTALLER
Please enter your Installation Code
XXXX – XXXX – XXXX – XXXX
Next
Show Welcome Message
Get Support by Email
Nextron Systems GmbH © 2021 - 2024. All Rights Reserved.

## 3.4 Connectivity Check

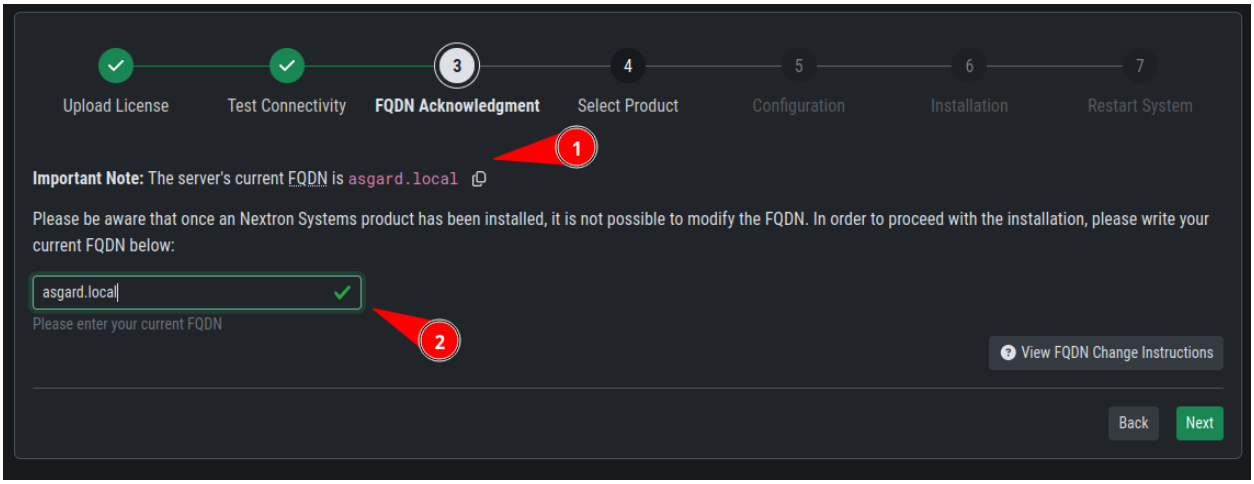
The Nextron Universal Installer will try to connect to our update server in order to download all the necessary packages once the installation starts. Make sure you can reach the update servers (TCP/443 on update-301.nextron-systems.com).

Please configure your proxy settings if you are behind a proxy (see *Proxy and NTP Settings*).

## 3.5 Valid FQDN

The Nextron Universal Installer will prompt you to verify the FQDN which you configured during the installation of the base system. This is needed in order for your server to communicate via a HTTPs connection with the Analysis Cockpit and other Cluster Nodes.

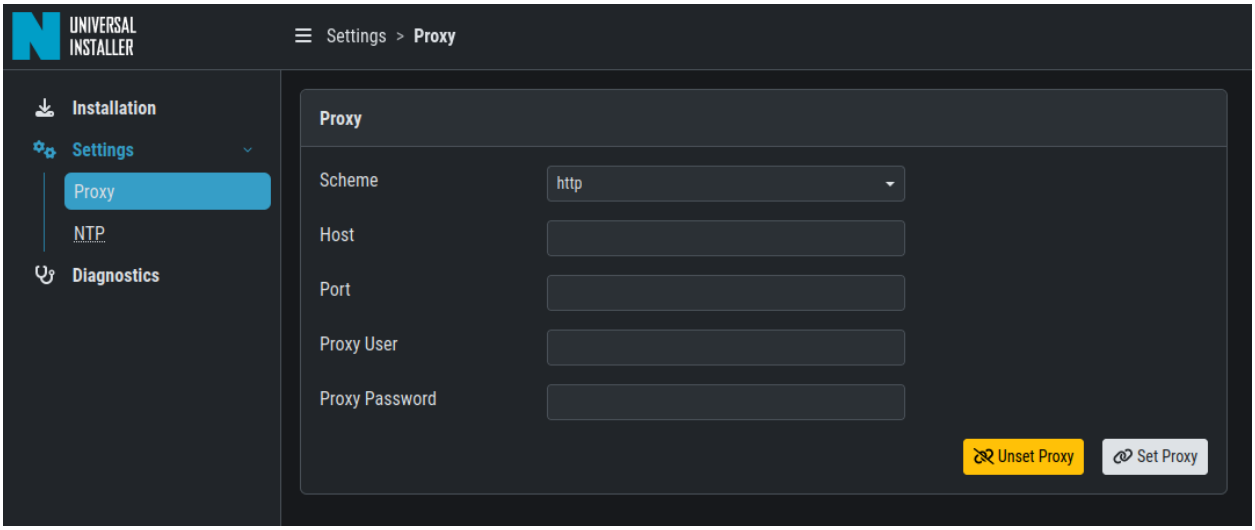
If the displayed FQDN is not correct, you can change it by clicking on the `View FQDN Change Instructions` button. This will open a dialog with instructions on how to change the FQDN of your server. Once you have changed the FQDN, you can continue with the installation.




## 3.6 Proxy and NTP Settings

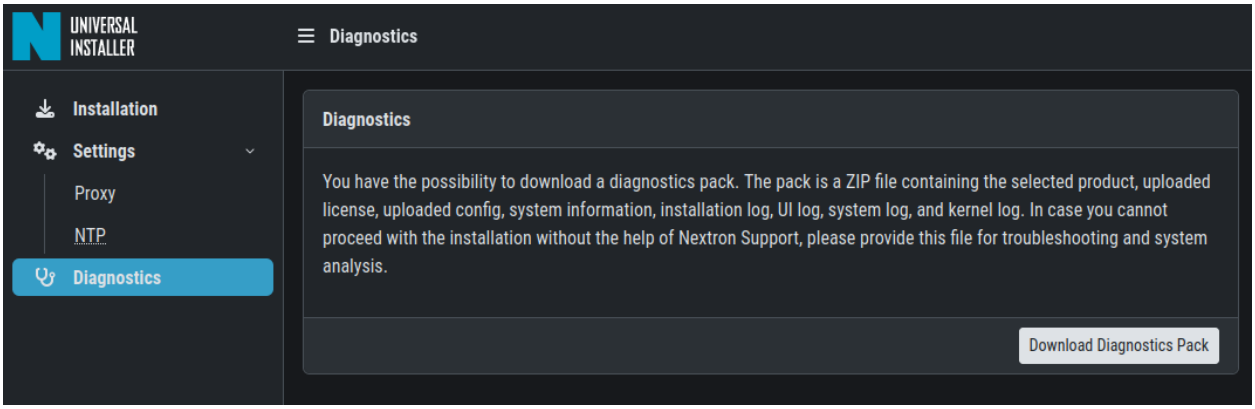
If you need to configure a proxy or change the NTP settings of your system, you can do so by clicking on the `Settings` button in the left menu of the Nextron Universal Installer.

If you configured a proxy during the ISO installation, those settings will be carried over into the Universal Installer. The settings will also be carried over into your ASGARD Management Center. The same goes for NTP.




## 3.7 Diagnostic Pack

In case of errors or problems during the installation, you can download a diagnostic pack by navigating to the `Diagnostics` tab in the left menu of the Nextron Universal Installer. Click on the `Download Diagnostic Pack` button to download the diagnostic pack. You can then send the diagnostic pack to our support team for further analysis.



CHAPTER

FOUR

# ELASTICSEARCH NODE MAINTENANCE

## 4.1 Performing Updates

When updates are applied to the Analysis Cockpit, you also need to update all additional cluster nodes by running:

```
nextron@es-node1:~$ sudo apt update
nextron@es-node1:~$ sudo apt upgrade
```

It is recommended that you update one node at a time, in particular when a reboot is required. It is not necessary to remove the node from the cluster for the update.

## 4.2 Checking Elasticsearch status

You can check elasticsearch status and index distribution on any of the nodes:

```
nextron@cockpit4:~$ sudo su -
[sudo] password for nextron:
root@cockpit4:~# curl -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password)␣
↪http://127.0.0.1:9200/_cat/health
root@cockpit4:~# curl -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password)␣
↪http://127.0.0.1:9200/_cat/nodes
root@cockpit4:~# curl -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password)␣
↪http://127.0.0.1:9200/_cat/shards
root@cockpit4:~# curl -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password)␣
↪http://127.0.0.1:9200/_cluster/health | jq
```

## 4.3 Removing Elasticsearch nodes

Before temporarily or permanently removing a node, you should reconfigure the cluster to move away any shards from that node.

You can tell Elasticsearch to remove all indexes from a node (change the placeholder value of "node_to_remove" to the actual node name):

```
nextron@cockpit4:~$ sudo su -
[sudo] password for nextron:
root@cockpit4:~$ curl -X PUT "http://127.0.0.1:9200/_cluster/settings" \
  -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password) \
```

(continues on next page)

(continued from previous page)

```
  -H "Content-Type: application/json" \
  -d '{"transient": {"cluster.routing.allocation.exclude._name": "node_to_remove"} }'
```

Then wait until the node has no shards left:

```
nextron@cockpit4:~$ curl -u elastic:$(cat /etc/asgard-analysis-cockpit/elastic.password)␣
↪http://127.0.0.1:9200/_cat/shards
```

Once no shards are assigned to the node, it is safe to shut it down. When you have replicas of each index (number_of_replicas >= 1), the cluster should automatically cope with the removal of any single node. Refer to Elasticsearch documentation!

For obvious reasons, you must not remove the Analysis Cockpit node itself from the cluster but it is ok to shut it down or restart it for maintenance.

CHAPTER

FIVE

# INDEX

- genindex

# INDEX