# Managing Indices in Nagios Log Server 2024R2

## Purpose

This document describes how to manage your Nagios Log Server Indices for your Nagios Log Server cluster.

## Overview

Nagios Log Server is a clustered application, it consists of one or more instances of Nagios Log Server. An instance is an installation of Nagios Log Server, it participates in the cluster and acts as a location for the received log data to reside. The log data is spread across the instances using the Opensearch database, a special database used by Nagios Log Server. This documentation discusses **Indices** in the Opensearch database. In Nagios Log Server, **Indices** is the plural for an **Index**.

## Index / Indices

An index in Nagios Log Server is how the Opensearch database stores log data. Nagios Log Server creates and index for every day of the year, this makes it easy to age out old data when no longer required.

## Shards / Replicas

Each index contains **5 Shards**, a shard is a portion of the log data in that index. Shards and Replicas is how Opensearch spreads the data out for redundancy and replication.

When an index is created it contains 5 shards and is configured for 1 **Replica**. A replica means that a duplicate copy of the shards is created and need to be stored on a separate Nagios Log Server instance.

If one of your Nagios Log Server instances has a disk failure, a copy of the shards on that instance will be available on another instance and can be recovered.

In reality there are 10 shards per index, 5 are primary and 5 are replica, this is why in some areas you will see there are 10 shards per index and in other areas it says 5 shards and 1 replica.

If you have a single node cluster then there is no other instance to store the 5 replica shards on. Single node clusters do not provide you with the redundancy that the Opensearch database provides.

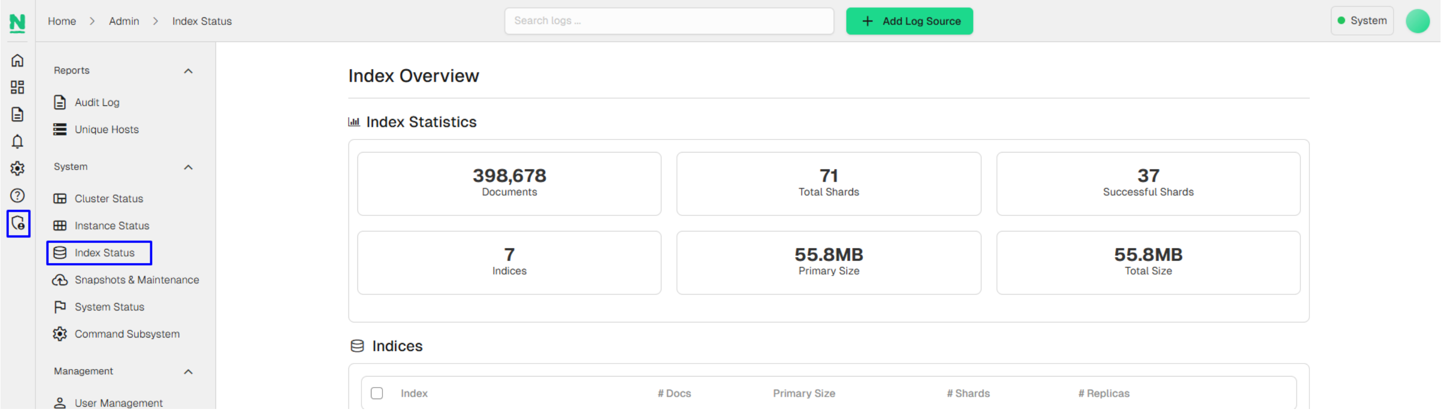
In a 2 instance cluster, for each index the 5 primary shards will exist on one instance and the 5 replica shards will exist on the other instance.

In a 3 or more instance cluster the shards are distributed across the instances as evenly as possible. A replica shard will never exist on the same instance that has the primary shard. Here is a visualization:

| Shard | Primary Shard | Replica Shard |
|---|---|---|
| 0 | Instance A | Instance C |
| 1 | Instance B | Instance C |
| 2 | Instance A | Instance C |
| 3 | Instance B | Instance C |
| 4 | Instance A | Instance B |

## Index Status

To manage your Nagios Log Server Indices navigate to **Admin > System > Index Status**



Index Overview

Index Statistics

| | | |
|---|---|---|
| 398,678<br>Documents | 71<br>Total Shards | 37<br>Successful Shards |
| 7<br>Indices | 55.8MB<br>Primary Size | 55.8MB<br>Total Size |

Indices

| ☐ Index | # Docs | Primary Size | # Shards | # Replicas |
|---|---|---|---|---|

The index status page allows administrators to see the current statistics and behavior of their Nagios Log Server indices, similar to the cluster status page.

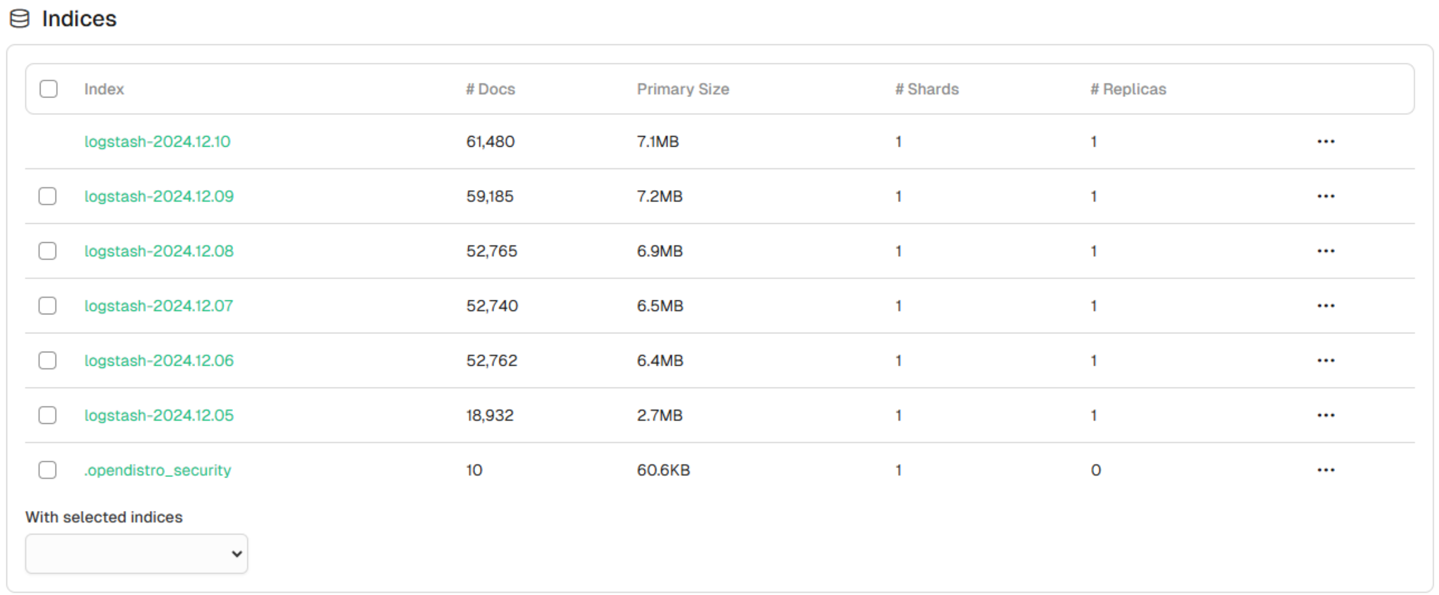
## Index Statistics

Here you can see the number of indices in your instance, the total documents over all your indices, total shards in the index, the number of shards that were successful and the primary and total size of the index.

Seeing the statistics of your index can be useful if you plan to add, remove or temporarily remove an instance. It also gives you a good idea of the number of files, shards and disk space an index is using.

## Indices

The Indices table shows you the indices that have been created.



Indices

| ☐ | Index | # Docs | Primary Size | # Shards | # Replicas | |
|---|---|---|---|---|---|---|
| | logstash-2024.12.10 | 61,480 | 7.1MB | 1 | 1 | ··· |
| ☐ | logstash-2024.12.09 | 59,185 | 7.2MB | 1 | 1 | ··· |
| ☐ | logstash-2024.12.08 | 52,765 | 6.9MB | 1 | 1 | ··· |
| ☐ | logstash-2024.12.07 | 52,740 | 6.5MB | 1 | 1 | ··· |
| ☐ | logstash-2024.12.06 | 52,762 | 6.4MB | 1 | 1 | ··· |
| ☐ | logstash-2024.12.05 | 18,932 | 2.7MB | 1 | 1 | ··· |
| ☐ | .opendistro_security | 10 | 60.6KB | 1 | 0 | ··· |

Each index has information displayed about it:

- **Index**
  - The first column is the index name
  - When the index is created the name is based on the date the logs are received
- **# Docs**
  - This show how many documents each index currently contains
- **Primary Size**
  - Actual size of the index
- **# Replicas**
  - The number of replicas assigned to the index

- **Empty (Action)** ⋯

  This column allows you to perform the following actions to an index when clicking on the Actions Icon (ellipses):

  - Close
    - Closing an index means that the log data will no longer be searched in queries and will not be replicated across instances
  - Open
    - Opening an index will allow the log data to be searched in queries
  - Delete
    - Delete the index entirely
    - Caution should be used when deleting an index, it cannot be recovered unless a snapshot has been created for the index

An index can be clicked on to see more detailed information about it such as:

- The number of documents the index is made up of, shards, indices and the total size of the index
- Search Totals
- Get Totals
- Documents
- Indexing Totals
- Operations

## Advanced Management

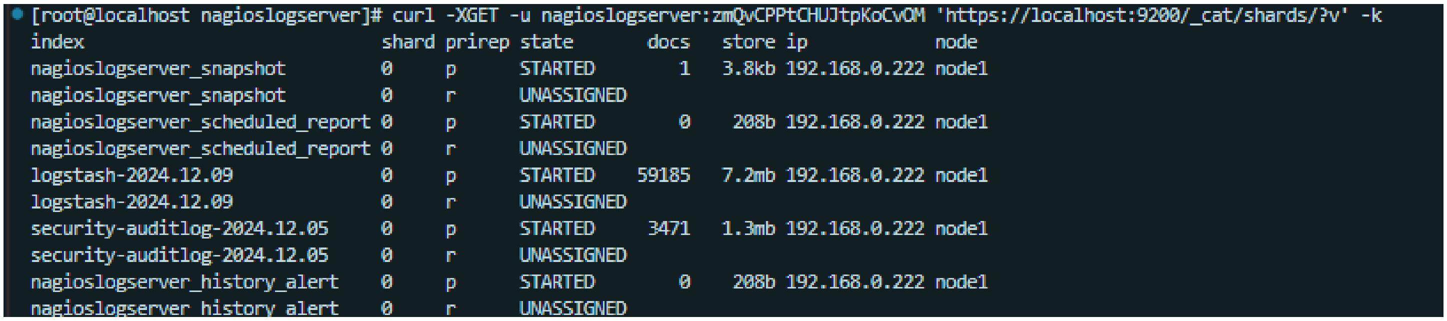
If you require more detailed information about indices you will need to execute commands in a terminal session. Information about index shard status can be executed via a *curl* command.

Establish a terminal session to one of you Nagios Log Server instances and execute the following command (note that this is a single command) :

```
curl -XGET --cacert /usr/local/nagioslogserver/opensearch/config/root-ca.pem
-u nagioslogserver:password 'https://localhost:9200/_cat/shards/logstash-
2017.10.31?v'
```

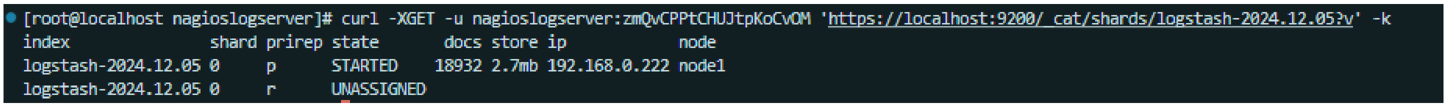
This will produce a lot of output. The password for the command above and the following command can be found in */var/www/html/nagioslogserver/application/config/config.local.php* If you are interested in a specific index you can actually specify the name of the index in the command, for example (note that this is a single command) :

```
curl -XGET --cacert /usr/local/nagioslogserver/opensearch/config/root-ca.pem
-u nagioslogserver:password  'https://localhost:9200/_cat/shards/logstash-
2017.10.31?v'
```



```
[root@localhost nagioslogserver]# curl -XGET -u nagioslogserver:zmQvCPPtCHUJtpKoCvOM 'https://localhost:9200/_cat/shards/?v' -k
index                          shard prirep state       docs   store ip            node
nagioslogserver_snapshot       0     p      STARTED        1   3.8kb 192.168.0.222 node1
nagioslogserver_snapshot       0     r      UNASSIGNED
nagioslogserver_scheduled_report 0   p      STARTED        0    208b 192.168.0.222 node1
nagioslogserver_scheduled_report 0   r      UNASSIGNED
logstash-2024.12.09            0     p      STARTED    59185   7.2mb 192.168.0.222 node1
logstash-2024.12.09            0     r      UNASSIGNED
security-auditlog-2024.12.05   0     p      STARTED     3471   1.3mb 192.168.0.222 node1
security-auditlog-2024.12.05   0     r      UNASSIGNED
nagioslogserver_history_alert  0     p      STARTED        0    208b 192.168.0.222 node1
nagioslogserver_history_alert  0     r      UNASSIGNED
```

The screenshot above shows you what instance each shard is allocated to. The screenshot below is a demonstration of when one of the Nagios Log Server instances was offline, you can see some of the shards are UNASSIGNED. These are the replica shards, indicated by the **r** in the **prirep** column.



```
[root@localhost nagioslogserver]# curl -XGET -u nagioslogserver:zmQvCPPtCHUJtpKoCvOM 'https://localhost:9200/_cat/shards/logstash-2024.12.05?v' -k
index               shard prirep state       docs store ip            node
logstash-2024.12.05 0     p      STARTED    18932 2.7mb 192.168.0.222 node1
logstash-2024.12.05 0     r      UNASSIGNED
```

## Finishing Up

This completes the documentation on Managing Indices in Nagios Log Server 2024R2. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum    Visit Nagios Knowledge Base    Visit Nagios Library