

Managing Indices in Nagios Log Server 2024

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 Elasticsearch database, a special database used by Nagios Log Server. This documentation discusses Indices in the Elasticsearch database. In Nagios Log Server, Indices is the plural for an Index.

Index / Indices

An index in Nagios Log Server is how the Elasticsearch database stores log data. Nagios Log Server creates an 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 Elasticsearch 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 Elasticsearch 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.

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

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:

Index Status

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

The screenshot shows the Nagios Log Server Admin interface. The left sidebar contains a menu with sections: Reports (Audit Log), System (Cluster Status, Instance Status, Index Status, Snapshots & Maintenance, System Status, Command Subsystem), Management (User Management, LDAP/AD Integration), and General (Global Settings, Mail Settings, License Information, Proxy Configuration). The 'Index Status' link is highlighted. The main content area is titled 'Index Overview' and contains two sections: 'Index Statistics' and 'Indices'.

Index Statistics

499,706 Documents	324 Total Shards	324 Successful Shards
682 Indices	108.3MB Primary Size	216.6MB Total Size

Indices

<input type="checkbox"/>	Index	# Docs	Primary Size	# Shards	# Replicas	Action
<input type="checkbox"/>	logstash-2017.10.31	40,169	15.6MB	5	1	<input type="button" value="close"/> <input type="button" value="delete"/>
<input type="checkbox"/>	logstash-2017.10.30	39,563	7.6MB	5	1	<input type="button" value="close"/> <input type="button" value="delete"/>

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

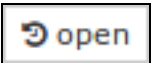

The Indices table shows you the indices that have been created.

Indices						
<input type="checkbox"/>	Index	# Docs	Primary Size	# Shards	# Replicas	Action
<input type="checkbox"/>	logstash-2017.10.31	40,430	17.2MB	5	1	<input type="button" value="close"/> <input type="button" value="delete"/>
<input type="checkbox"/>	logstash-2017.10.30	39,563	7.6MB	5	1	<input type="button" value="close"/> <input type="button" value="delete"/>
<input type="checkbox"/>	logstash-2015.10.19	-	-	5	1	<input type="button" value="open"/> <input type="button" value="delete"/>
<input type="checkbox"/>	logstash-2015.10.18	-	-	5	1	<input type="button" value="open"/> <input type="button" value="delete"/>

With selected indices:

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
- # Shards
 - The number of primary shards that have been allocated to the index
- # Replicas
 - The number of replicas assigned to the index
- Action
 - This column allows you to perform the following actions to an index:
 -

- 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 your Nagios Log Server instances and execute the following command:

```
curl -XGET 'http://localhost:9200/_cat/shards/?v'
```

This will produce a lot of output. If you are interested in a specific index you can actually specify the name of the index in the command, for example:

```
curl -XGET 'http://localhost:9200/_cat/shards/logstash-2017.10.31?v'
```

```
[root@nls-c6x-x86 ~]# curl -XGET 'http://localhost:9200/_cat/shards/logstash-2017.10.31?v'
```

index	shard	prirep	state	docs	store	ip	node
logstash-2017.10.31	4	p	STARTED	8273	1.6mb	127.0.0.1	d20fa1fa-3a37-4a6c-8722-1d453138774a
logstash-2017.10.31	4	r	STARTED	8273	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	0	p	STARTED	8356	1.6mb	127.0.0.1	d20fa1fa-3a37-4a6c-8722-1d453138774a
logstash-2017.10.31	0	r	STARTED	8356	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	3	p	STARTED	8269	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	3	r	STARTED	8269	1.5mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	1	p	STARTED	8413	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	1	r	STARTED	8413	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	2	p	STARTED	8283	1.6mb	127.0.0.1	d20fa1fa-3a37-4a6c-8722-1d453138774a
logstash-2017.10.31	2	r	STARTED	8283	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee

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@nls-c6x-x86 ~]# curl -XGET 'http://localhost:9200/_cat/shards/logstash-2017.10.31?v'
```

index	shard	prirep	state	docs	store	ip	node
logstash-2017.10.31	4	p	STARTED	8273	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	4	r	UNASSIGNED				
logstash-2017.10.31	0	p	STARTED	8356	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	0	r	UNASSIGNED				
logstash-2017.10.31	3	p	STARTED	8269	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	3	r	STARTED	8269	1.5mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	1	p	STARTED	8413	1.6mb	10.25.5.85	76e504ad-a6c9-4798-b1dd-0bba4c97c6bc
logstash-2017.10.31	1	r	STARTED	8413	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	2	p	STARTED	8283	1.6mb	10.25.5.98	edde1960-0cc2-4892-b385-b359ed6183ee
logstash-2017.10.31	2	r	UNASSIGNED				