Purpose

This document describes how to remove an instance from a Nagios Log Server cluster.

Target Audience

This document is written for administrators who are looking to remove an instance from a Nagios Log Server cluster, planned or not.

Overview

Removing an instance from a Nagios Log Server cluster is as simple as updating the `cluster_hosts` configuration file and restarting the Elasticsearch database service on each node. This applies to the following scenarios:

- Planned server removal / replacement
- Server crashed / dead / not recoverable
- Isolating a node to perform testing
  - Please refer to the Isolation Considerations section below

Isolation Considerations

You can easily isolate an instance from the cluster for testing purposes. The instance that you want to isolate simply has it's own IP address in the `cluster_hosts` configuration file and none of the other instances. This means you will have two clusters that exist with the same cluster ID but they do not talk to each other. You don't need to physically isolate this instance from the other instances on your network, the configuration file dictates who participates in the cluster. There are several points that need to be considered for isolating.

1) Snapshot Data

Snapshots are the backups of the Elasticsearch cluster log data, a cluster requires that all instance have access to the snapshot repository. When you isolate an instance from the cluster it will still be configured to use the existing snapshot repository, this can lead to two separate clusters writing to the same snapshot

repository which will lead to confusion and most likely data corruption. This is easily remedied by disabling snapshots & maintenance from the isolated cluster so that it does use it.

2) Incoming Logs

The instance that you isolate should not be receiving log data from your devices, the data they are sending will not be included in your production cluster.

3) Replicas & Shards

The data in the Elasticsearch database is stored as shards across instances. Detailed information on this topic can be found in the Managing Nagios Log Server Indices documentation. In the scenario of a two instance cluster, isolating an instance will ensure that instance has all the shards in the cluster.

However when you have three or more instances in the cluster, the instance you are isolating may not have a copy of all the shards and hence you do not have an entire copy of the cluster. Here is an example that demonstrates this. This first screenshot shows that there are four instances in this cluster:

```
[root@nls-c7x-x64 nagioslogserver]# curl -XGET 'http://localhost:9200/_cat/nodes?v'
host                    ip          heap.percent ram.percent load node.role master name
nls-c6x-x64.box293.local 10.25.5.84            5          74 0.00 d         *      23d9ebe0-0f63-479e-ba73-92a0f9d02d18
nls-c7x-x64.box293.local 10.25.5.86            2          77 0.00 d         m      16bd0c72-8ccb-438b-87c9-aa14e5fab05c
nls-r6x-x64.box293.local 10.25.5.98            5          78 0.00 d         m      bc044f3f-72e1-49b5-a937-efae12818493
nls-r7x-x64.box293.local 10.25.5.99            4          78 0.00 d         m      c6c8e668-a94c-4630-8dcb-90aed99fddb6
```

This screenshot shows the five primary and five replica shards for an index:

```
[root@nls-c7x-x64 nagioslogserver]# curl -XGET 'http://localhost:9200/_cat/shards?v'
index                shard prirep state   docs   store ip         node
logstash-2018.03.20 2     p      STARTED  121  89.9kb 10.25.5.84 23d9ebe0-0f63-479e-ba73-92a0f9d02d18
logstash-2018.03.20 2     r      STARTED  121  53.8kb 10.25.5.99 c6c8e668-a94c-4630-8dcb-90aed99fddb6
logstash-2018.03.20 0     p      STARTED  110  73.4kb 10.25.5.98 bc044f3f-72e1-49b5-a937-efae12818493
logstash-2018.03.20 0     r      STARTED  110    39kb 10.25.5.86 16bd0c72-8ccb-438b-87c9-aa14e5fab05c
logstash-2018.03.20 3     r      STARTED  126  89.4kb 10.25.5.98 bc044f3f-72e1-49b5-a937-efae12818493
logstash-2018.03.20 3     p      STARTED  126  58.6kb 10.25.5.99 c6c8e668-a94c-4630-8dcb-90aed99fddb6
logstash-2018.03.20 1     p      STARTED  121  82.8kb 10.25.5.86 16bd0c72-8ccb-438b-87c9-aa14e5fab05c
logstash-2018.03.20 1     r      STARTED  121  53.8kb 10.25.5.84 23d9ebe0-0f63-479e-ba73-92a0f9d02d18
logstash-2018.03.20 4     p      STARTED  118  55.2kb 10.25.5.98 bc044f3f-72e1-49b5-a937-efae12818493
logstash-2018.03.20 4     r      STARTED  118    40kb 10.25.5.99 c6c8e668-a94c-4630-8dcb-90aed99fddb6
```

Here is that shard data in a table:

Shard	10.25.5.84	10.25.5.86	10.25.5.98	10.25.5.99
0 Primary			X	
0 Replica		X		
1 Primary		X		
1 Replica	X			
2 Primary	X			
2 Replica				X
3 Primary				X
3 Replica			X	
4 Primary			X	
4 Replica				X

You can see from above that none of the instances have five of the required shards to make up an index. When you are trying to isolate an instance for testing this will need to be considered.

Steps

The following steps will be performed to remove an instance from a cluster:

- Stop Elasticsearch on all instances
- Update configuration file
- Start Elasticsearch on all instances
- Verify instances in cluster
- Delete removed instance
- Disable snapshots & maintenance (optional)

Stop Elasticsearch On All Instances

Establish terminal sessions to every instance in the cluster and execute the following command:

RHEL | CentOS | CentOS Stream | Oracle Linux | Debian | Ubuntu

```
systemctl stop elasticsearch.service
```

You can now proceed to the update configuration file step.

Update Configuration File

On all instances you will need to update the `/usr/local/nagioslogserver/var/cluster_hosts` configuration file. Open the file `cluster_hosts` in vi by executing the following command:

```
vi /usr/local/nagioslogserver/var/cluster_hosts
```

When using the vi editor, to make changes press ***`i`*** *on the keyboard first to enter insert mode. Press* ***`Esc`*** *to exit insert mode.*

Delete the line that has the address of the instance you are removing. **IF** you are isolating an instance then on that server delete all the addresses of the other instances.

When you have finished, save the changes in vi by typing:

```
:wq
```

and press Enter.

You can now proceed to the start elasticsearch service step.

Start Elasticsearch On All Instances

On every instance in the cluster execute the following command:

RHEL | CentOS | CentOS Stream | Oracle Linux | Debian | Ubuntu

```
systemctl start elasticsearch.service
```

If you are isolating an instance then you will also need to start the service on that server.

You can now proceed to the verify instances in cluster step.

Verify Instances In Cluster

Once you've made the changes and restarted the service you should verify that everything it OK. Execute the following commands on one of the instances:

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

```
[root@nls-c7x-x64 nagioslogserver]# curl -XGET 'http://localhost:9200/_cat/nodes?v'
host                    ip         heap.percent ram.percent load node.role master name
nls-r6x-x64.box293.local 10.25.5.98           6          77 0.09 d         m      bc044f3f-72e1-49b5-a937-efae12818493
nls-c6x-x64.box293.local 10.25.5.84           2          74 0.15 d         *      23d9ebe0-0f63-479e-ba73-92a0f9d02d18
nls-c7x-x64.box293.local 10.25.5.86           4          78 0.27 d         m      16bd0c72-8ccb-438b-87c9-aa14e5fab05c
[root@nls-c7x-x64 nagioslogserver]#
[root@nls-c7x-x64 nagioslogserver]# curl -XGET 'http://localhost:9200/_cat/health?v'
epoch      timestamp cluster                              status node.total node.data shards pri relo init unassign pending_tasks
1521515809 14:16:49  ef21c808-62c3-42c2-91b9-f488315baf2d green           3         3     42  21    0    0        0             0
```

From the screenshot above you can see that this cluster now has three nodes, the 10.25.5.99 node was removed. You can also see that it has a green status. You can confirm this by opening the Nagios Log Server web interface and navigate to **Admin** > **System** > **Cluster Status**.

The screenshot below demonstrates the health of the instance that was isolated:

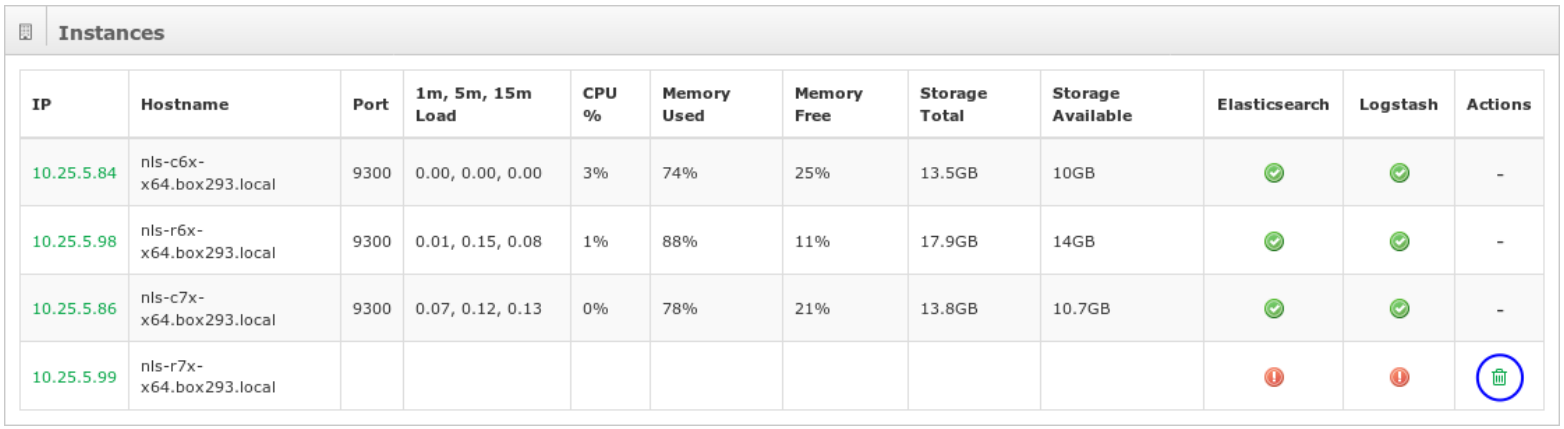
```
[root@nls-r7x-x64 nagioslogserver]#  curl -XGET 'http://localhost:9200/_cat/nodes?v'
host                    ip         heap.percent ram.percent load node.role master name
nls-r7x-x64.box293.local 10.25.5.99           4          78 0.01 d         *      c6c8e668-a94c-4630-8dcb-90aed99fddb6
[root@nls-r7x-x64 nagioslogserver]#
[root@nls-r7x-x64 nagioslogserver]# curl -XGET 'http://localhost:9200/_cat/health?v'
epoch      timestamp cluster                              status node.total node.data shards pri relo init unassign pending_tasks
1521515875 14:17:55  ef21c808-62c3-42c2-91b9-f488315baf2d red             1         1     11  11    0    0       31             0
```

As explained earlier, this instance was not able to have a copy of all the required shards and hence it is currently in a red state. More information about this can be found in the troubleshooting section.

You can now proceed to the delete removed instance step.

Delete Removed Instance

The last step is to delete the removed instance from the production cluster. Open the Nagios Log Server web interface and navigate to **Admin** > **System** > **Instance Status**.



In the **Instances** table click the **trashcan** icon to delete the removed instance.

This completes the steps required to remove an instance from a Nagios Log Server cluster. If you isolated an instance then proceed to the disable snapshots & maintenance step.

Disable Snapshots & Maintenance

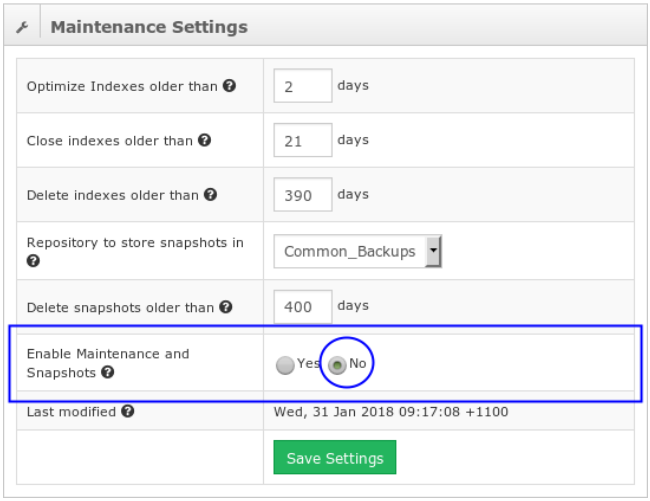
As explained in the Isolation Considerations section, you will need to disable snapshots & maintenance on the isolated instance.

Open the Nagios Log Server web interface and navigate to **Admin** > **System** > **Snapshots & Maintenance**.

For the Enable Maintenance and Snapshots option select **No** and click **Save Settings**.

This ensures the isolated instance will not use the snapshot repository and will not cause issues with production.

Snapshots & Maintenance



Troubleshooting

The following documentation will help troubleshoot issues you may encounter:

- Understanding and Troubleshooting Yellow Cluster Health
- Understanding and Troubleshooting Red Cluster Health

Finishing Up

This completes the documentation on how to remove an instance from your Nagios Log Server cluster. If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb