How To Back Up And Restore Nagios Log Server 2024R2 and 2026

Purpose

This document describes how to backup and restore your Nagios Log Server cluster.

Trying to Migrate?

See Migrating Nagios Log Server to a different server for steps on migrating without using the backup and restore method.

Before migrating, see the OS compatibility matrix.

Backup Overview

Nagios Log Server has several backup methods:

- Snapshots
    - Snapshots are backups of your OpenSearch Log Data.
- Config Snapshots
    - These are backups of the Inputs, Filters and Outputs for Logstash.
- System Backups
    - This is a backup of the entire system (excluding the OpenSearch log data).

Backups in Nagios Log Server (NLS) are slightly different than regular backup methods. This has to do with NLS being a cluster-oriented application. The backup methodology in NLS ensures that backups are held on all instances in the NLS cluster. This means that if an instance is lost you would not lose any data because the backup data is held on other NLS instances.

However, If you have a single instance cluster, then you will need to take additional manual steps to ensure that the config snapshots and system backups are stored on an external server. This will ensure you will be able to restore your single instance Nagios Log Server in the event of a disaster.

Snapshots

Backing up and restoring Nagios Log Server Snapshots are point in time backups of your log data that exist in the OpenSearch database.

- Snapshots are stored in a Snapshot Repository.
- The repository needs to be accessible by all instances in your Nagios Log Server cluster.
    - Usually, a NFS or CIFS network share mounted to a path like `/snapshot_repository`.
    - The mounted path needs to be identical on all instances.

The snapshot is performed on the entire cluster. During the snapshot and maintenance job, a node will run the commands to create a new snapshot. Because the snapshot is of indices that have shards allocated to different instances, you need an NFS or CIFS share so that those instances can store their data in the snapshot being created.

For more information on Snapshots, please refer to the following documentation: Managing Snapshots And Maintenance.

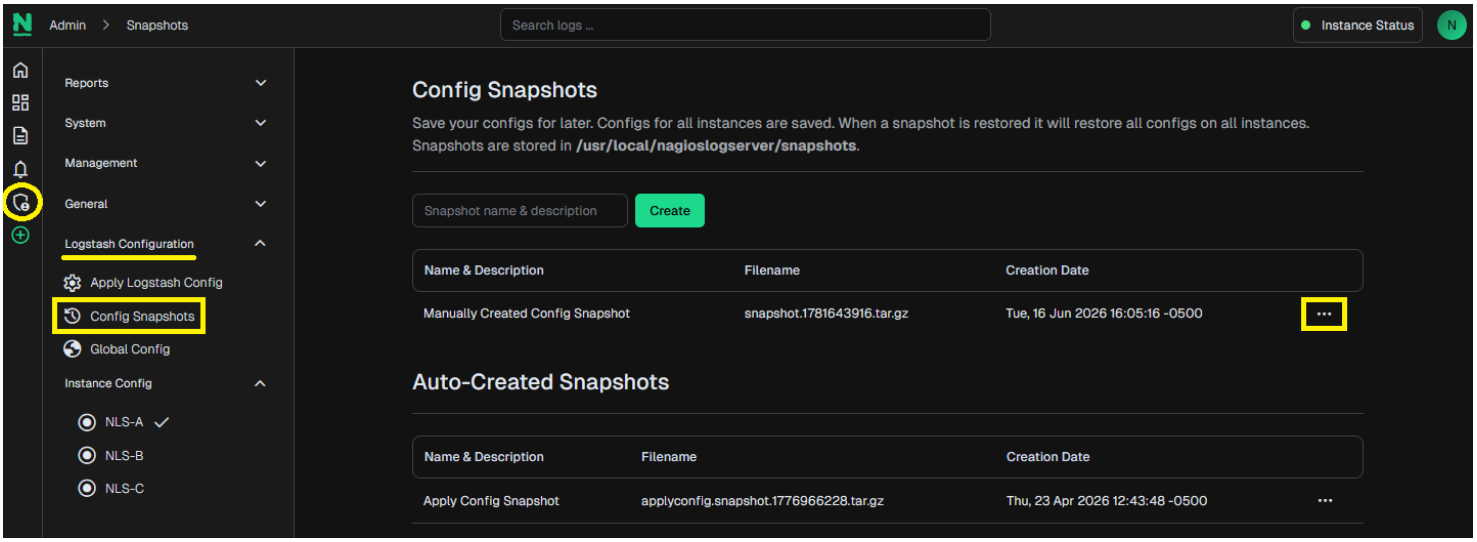
Again, if you have a single instance Nagios Log Server cluster, it is important that your snapshot repository is on another server. In this case, if your instance was to be completely destroyed you would lose everything if it was all on the same server.

Config Snapshots

- Config Snapshots are backups of the Inputs, Filters, and Outputs for Logstash. These are created automatically whenever you apply configuration, or you can create manual config snapshots.
- Config snapshots are stored in the `/usr/local/nagioslogserver/snapshots/` location on every instance in the cluster. Every instance in the cluster will have a copy of the config snapshots in this location ensuring that if an instance goes down the others have a copy of it.
- Config snapshots allow you to roll back to a point in time in the scenarios where you did not like the changes previously made. Manual snapshots will remain until you choose to delete them.

Config snapshots can be found by navigating to **Admin > Logstash Configuration > Config Snapshots**.

Here you can see the existing snapshots.



Both Manual and Auto-Created snapshots have these actions available, access by clicking the **Actions** icon to the right of any entry:

- **Download the .tar.gz file to your computer**
- **Restore instance to this configuration**: restores the snapshot to all instances in the cluster.

Manually Created/Archived snapshots have this action available:

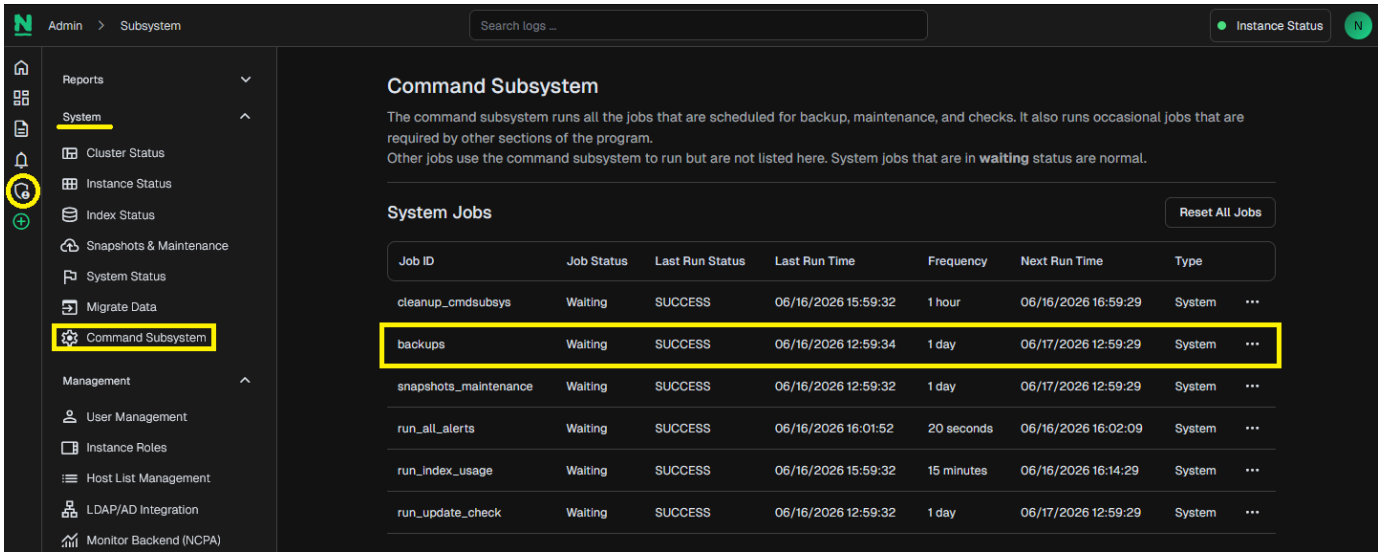
- **Remove**: This allows you to permanently delete the snapshot.

Auto-created snapshots have this action available:

- **Archive this snapshot in the regular shapshots section**: This allows you to archive the Auto-Created snapshot to the Manual snapshots section above.

System Backups

- System backups contain configuration settings, dashboards, users, internal logs, and alerts. Also included are the Inputs, Filters and Outputs for Logstash.
- They are stored in the location `/store/backups/nagioslogserver/` and are named based on the current current date and epoch value, for example `nagioslogserver.2026-06-16.1781643916.tar.gz`.
- These backups are stored on every instance in your log server cluster. Whenever the backup job is scheduled to run, each instance will create a local copy of the backup. This means that if you were to lose an instance in your cluster, another instance will have a copy of this backup. This however does not protect you if all of your instances were to be lost in a disaster. You should periodically take a copy of the system backup to an external location to ensure you can restore Nagios Log Server.
- System backups are configured to run once a day as a system job. By default, the time they are run is based on when you installed the first instance in your Nagios Log Server cluster. Navigate to **Admin > System > Command Subsystem** and you will find the **backups** system job. From here you can change the frequency of the snapshot and also initiate one to run now.



- There is no location in the Nagios Log Server GUI to view the system backups, you will need to establish a terminal session to a Nagios Log Server instance and check the directory to ensure the backups exist in this location.

What Happens In A Disaster

Multiple Instance Cluster - Losing One Instance

When you have multiple instances in your Nagios Log Server cluster and you lose one of those instances, generally the impact is minimal.

- The cluster will continue to function as the OpenSearch data is spread across the instances.
- Any log data that is being sent to the down instance will not be received.
    - If the log data is sent to a load balancer then it will be diverted to another instance (not a part of Nagios Log Server).

To return the cluster back to a healthy state you can attempt to repair the problem that caused the instance to fail in the first place (in the case of a physical hardware failure). Once the instance reconnects to the cluster OpenSearch will automatically become updated with the rest of the data in the cluster.

If you have devices sending log data to this instance:

- If you expect the instance to be down for an extended period of time, you should reconfigure the devices to send their data to another instance.
- If updating every device to send data to another instance is too time-consuming then you can instead run up a fresh install of Nagios Log Server that uses the existing IP address of the old instance and add it to the existing cluster.

It's worth mentioning that any one instance in the cluster is no more important than another. If you lose an instance due to problems that require a substantial amount of time to repair, it can be simpler and quicker to run up a fresh install of Nagios Log Server that uses the existing IP address of the old instance and add it to the existing cluster.

Multiple Instance Cluster - Losing Multiple Instances

The impact is very similar to just losing one instance. This has to do with how the OpenSearch data is spread across the instances. Follow the same principles outlined in the previous section.

Single Instance Cluster OR Multiple Instance Cluster - Losing ALL Instances

This scenario is more likely going to occur when you have a single instance cluster. It is possible to lose all instances in a multi-instance cluster and in that scenario the recover steps are the same for the single instance cluster.

- Run up a fresh install of Nagios Log Server on a new instance.
- Restore the System Backup.
- Mount the Snapshot Repository.
- Restore the indices to recover the log data.

In a multi-instance scenario, once you have the first instance running then it is a simple matter of running up additional instances and adding them to the cluster.

Restoring A System Backup or Migrating to a different Server

If you need to follow these steps it is assumed that you have lost all instances in your cluster, (single instance or multiple instance). You should not follow these steps if you have lost an instance in a multi-instance cluster and need to repair it, these steps do not apply.

You can also follow these steps if you want to test restoring a system backup. You do not need to perform this action in an isolated network as the restored cluster has a different ID and won't affect your production cluster.

Fresh Install of Nagios Log Server

The first step is to run up a fresh install of Nagios Log Server. This can be on the existing hardware of an instance that died; however, it is recommended that you perform a clean install of the RHEL or CentOS operating system.

Perform the steps in the following documentation:

Nagios Log Server - Manual Installation Instructions

Once the install is complete, DO NOT navigate to the user interface to complete the final installation steps. Leave the terminal open as you will use it in the following steps.

Restore The System Backup

Next you will need to transfer your system backup to the `/store/backups/nagioslogserver/` directory on this instance. You can use a program like WinSCP to do the transfer or use another method like scp.

To restore the system backup, execute the following commands in the terminal session:

```
cd /usr/local/nagioslogserver/scripts/
./restore_backup.sh /store/backups/nagioslogserver/nagioslogserver.2026-06-16.1781643916.tar.gz
```

You can see that the backup file used in this example is `nagioslogserver.2026-06-16.1781643916.tar.gz`, you will need to change this to match the name of your system backup.

You will see the message `Restore Complete!` when it has finished. At this point you should open the web GUI to this instance and log in to check that it is `OK`. Dashboards, inputs, filters, users, and other settings should exist, however, there will not be any log data available to query against, this will be covered next.

Mount The Snapshot Repository

Now mount the snapshot repository that contains your existing snapshots. In this example it will be mounted to `/snapshot_repository`.

Once the repository is mounted, open the web GUI and navigate to **Admin > System > Snapshots & Maintenance**.

- Click the **Create Repository** button and populate the fields for the new repository.
- The **Location** field will be `/snapshot_repository` in this example.
- Click the **Add Repository** button to create the repository.

Now that the repository has been created, the **Snapshots** list will be populated with the existing snapshots that can be restored.

Restore Indices

To restore the existing log data, you need to restore the indices from your snapshot repository.

- Click the **Restore** icon to restore the required snapshot.
- Select the indices that you want to restore and then click the **Restore Indexes** button.
- The restore process will run in the background.
- To confirm they have been restored navigate to **Admin > System > Index Status**.

This completes the process of restoring Nagios Log Server from a system backup. At this point you can add more instances to the cluster if required.

Finishing Up

This completes the documentation on Backing Up and Restoring Nagios Log Server 2026. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

Visit Nagios Support Forum Visit Documentation Hub Visit Nagios Library