

Nagios XI Cluster Setup Checklist with DRBD and Pacemaker

Pre-Deployment Checklist

Ensure the environment and system prerequisites are in place before proceeding with clustering. This sets a stable foundation for DRBD and Pacemaker configuration.

Step	Task	Details
1	System Prep	Same OS (e.g., RHEL/CentOS/Ubuntu), updates applied
2	Hostnames	Unique FQDNs (e.g., `nagios-node1`, `nagios-node2`)
3	DNS or `/etc/hosts`	Proper name resolution between nodes
4	NTP	Time sync via NTP on both nodes
5	Static IPs	Two IPs (one per node) + one VIP reserved
6	Partition for DRBD	Dedicated block device (e.g., `/dev/sdb1`) on both nodes
7	Open Firewall	Ports for MySQL, HTTP(S), DRBD, Corosync

DRBD Storage Setup

Configure the Distributed Replicated Block Device (DRBD) to replicate Nagios XI data storage between nodes for high availability.

Step	Task	Details
1	Install DRBD	`yum install drbd-utils` or `apt install drbd-utils`
2	Create DRBD config	`/etc/drbd.d/nagios.res` defining resource
3	Init DRBD meta	`drbdadm create-md nagios`
4	Bring up DRBD	`drbdadm up nagios`

5	Make one primary	<code>`drbdadm -- --overwrite-data-of-peer primary nagios`</code>
6	Format DRBD	<code>`mkfs.ext4 /dev/drbd0`</code>
7	Mount DRBD	Mount at <code>`/usr/local/nagiosxi`</code> or <code>`/opt/nagios`</code>
8	Sync Nagios XI data	Install on node1, sync to DRBD volume

Nagios XI Setup on DRBD

Place Nagios XI data and configuration files on the DRBD shared storage to ensure persistence and synchronization between nodes.

Step	Task	Details
1	Move Nagios XI to DRBD	Move <code>`/usr/local/nagiosxi`</code> to DRBD mount
2	Symlink or remount	Ensure Nagios, MySQL, and logs use shared storage
3	Sync MySQL Data	Ensure MySQL data also resides on DRBD

Corosync & Pacemaker Cluster Setup

Set up the core cluster software that manages failover, monitoring, and service orchestration.

Step	Task	Details
1	Install Components	<code>`pcs`, `corosync`, `pacemaker`, `fence-agents`</code>
2	Enable pcsd	<code>`systemctl enable pcsd --now`</code>
3	Set hacluster password	<code>`echo mypass   passwd hacluster --stdin`</code>
4	Authenticate Nodes	<code>`pcs cluster auth nagios-node1 nagios-node2`</code>
5	Create Cluster	<code>`pcs cluster setup --name nagios-cluster nagios-node1 nagios-node2`</code>
6	Start & Enable Cluster	<code>`pcs cluster start --all`</code> and <code>`pcs cluster enable --all`</code>

Pacemaker Resources (in Order)

Define and order the cluster-managed resources to control DRBD, filesystem, VIP, and services in a consistent failover pattern.

Step	Task	Details
1	DRBD resource	`ocf:linbit:drbd` with master/slave configuration
2	Filesystem	`ocf:heartbeat:Filesystem` for DRBD mount
3	Virtual IP (VIP)	`ocf:heartbeat:IPaddr2` on shared subnet
4	Nagios XI service	Custom `systemd:nagiosxi` script or service group
5	MySQL/MariaDB	Optional: managed as cluster resource if HA DB
6	Colocation	Ensure filesystem and VIP before Nagios starts
7	Ordering	DRBD → Filesystem → VIP → Nagios services

Failover & Health Check

Test and verify failover functionality and ensure all services remain operational and data remains consistent.

Step	Task	Details
1	Manual Failover Test	Stop node1, ensure node2 takes over services
2	VIP Test	Ping/telnet to VIP for Nagios web, DB
3	Log Checks	`pcs status`, `journalctl -xe`, DRBD logs
4	Service State	Ensure NagiosXI, MySQL, npcd, crond running
5	External Monitoring	Verify notifications still trigger during failover

Security & Hardening

Secure your cluster environment and restrict unauthorized access to critical resources and ports.

Step	Task	Details
1	Limit DRBD port	Allow only internal IPs on port 7788
2	Secure `pcs` user	Limit `hacluster` access via firewall
3	Enable STONITH	For production environments only
4	Monitor Logs	Integrate logs with centralized syslog server

Post-Setup and Documentation

Document the setup process, ensure proper backup procedures, and integrate the cluster with monitoring and alerting systems.

Step	Task	Details
1	Update SOP	Create documentation for failover, failback
2	Monitoring Integration	Add checks for VIP, DB, DRBD status in Nagios
3	Test Restore	Test full restore from backup with DRBD volume
4	Backup Plan	Configure daily backups of Nagios DB and configs

Fallback Plan (Manual Recovery Procedures)

In the event of a complete cluster failure or unexpected behavior not handled by automatic failover, follow the steps below to restore Nagios XI operations manually.

1. Assess Cluster State

- Run ``pcs status`` and ``drbdadm status`` on both nodes.
- Check system logs: ``journalctl -xe``, ``/var/log/messages``, DRBD logs.

2. Manual DRBD Promotion

If DRBD resource fails to auto-promote:

3. Force Service Start on One Node

Manually start Nagios XI and dependencies:

Confirm that services are running and accessible.

4. Force VIP Assignment

If the virtual IP (VIP) is not assigned

5. Check Application Functionality

- Confirm Nagios web interface loads from VIP.
- Verify alerting and checks are functioning.

6. Isolate Problem Node

- If one node is unstable, isolate it:
- Avoid split-brain scenarios.

7. Plan Rejoin or Rebuild

- Once stable, re-integrate the failed node using `pcs` or rebuild from backup.

8. Log and Review

- Record issue, recovery actions, and outcomes.
- Update SOP/documentation.