What is Nagios:

Nagios is an open-source software for continuous monitoring of system, networks and infrastructure. It runs plugins stored on a server which is connected with a host or another server on your network or the internet. In case of any failure nagios alerts about the issues & that the technical team can perform recovery process immediately.

Other tools-

Slunk, Prometheus, ELK, Sensu,Librato, Cloudwatch.

History of Nagios:

- In year 1999, ethan galstad develop it as a part of netsaind distribution
- In 2002, Ethan renames the project of "Nagios" because of trademark issues with the name "Netsaint".
- In 2009, Nagios release its first commercial version, Nagios XI,
- In 2012, Nagios again rename as Nagios Core.
- It uses port number 5666, 5667 and 5668 to monitor its client.

Why Nagios:

- It detect all type of network or server issues.
- Help us to find the root cause of the problem which allow you to get permanent solution to the problem.
- Reduce downtime
- Active monitor of entire infrastructure
- Allow us to monitor and troubleshoot server performance issues.
- Automatically fix problem.

Features of Nagios:

- Oldest and latest

- Good log and database system.
- Informative and attractive web interface.
- Automatically send alert on condition changes
- Help us to detect network errors or server crashes
- You can monitor the entire business process and IT infrastructure with a single pass.
- Monitor network service like http,smtp,snmp,ftp,ssh,pop3,DNS, LDAP, IPMI etc.

Phases of Continuous Monitoring:

- Define – develop a monitoring strategy.
- Establish – how frequently you are going to monitor it.
- Implement.
- Analyze data Report finding
- Respond.
- Review and update.

Nagios Architecture:

- Nagios is a client-server architecture.
- Usually on a network, a nagios server is running on a host and plugins are running on all remote hosts should you monitor host which should you monitor.

How does it works:

- Mention all details in configuration files.
- Daemon read those details what data to be collected
- Daemon use NRPE plug-in to collect data from nodes and store in its own database.
- Finally shows everything in dashboard.

Pre-Requisite:

1. Httpd (browser)
2. PHP (dashboard)
3. Gcc 2 dg (compiler to convert)
4. Make file (to build)
5. Perl (script)

Main configuration file:

/usr/local/nagos/etc/nagios.cfs

All monitoring things (called as a 'service)

For eg.

5 server - 4 checks each service.

You have to monitor – 5x4=20 services.

Dashboard Overview:

In dashboard, you can see ……

Host:

- o Down
- o Unreachable
- o Up
- o Recovery
- o None

Services:

- o Warning
- o Unknown
- o Critical

- Recovery
- pending