NAGIOS Q&A

**www.zippyops.com**

172-172, 5th floor Old Mahabalipuram Road

(Above Axis Bank-PTC Bus Stop)  
Thuraipakkam  
Chennai 600097

**🖂**[**zippyops@gmail.com**](mailto:zippyops@gmail.com)

**✆+91 7010585768**

**1.What is Nagios?**

Nagios is a open source powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes.

**2.What is Nagios monitoring tool in Linux?**

Nagios provides complete monitoring of Linux operating systems and distributions – including operating system metrics, service state, process state, file system usage, and more. When you use Nagios to monitor your Linux environment, you’re using one of the most powerful Linux monitoring tools on the planet.

What is an icinga?

Icinga is an open source computer system and network monitoring application. It was originally created as a fork of the Nagios system monitoring application in 2009. The name Icinga is a Zulu word meaning “it looks for”, “it browses” or “it examines” and is pronounced with a click consonant.

**3.What is active and passive checks in Nagios?**

Active checks can be used to “poll” a device or service for status information every so often. Nagios also supports a way to monitor hosts and services passively instead of actively. The key features of passive checks are as follows: Passive checks are initiated and performed by external applications/processes.

**4.What is OID Nagios?**

SNMP (Simple Network Management Protocol) is a network protocol designed for monitoring network-attached devices. It uses OIDs (Object IDentifiers) for defining the information, known as MIBs (Management Information Base), that can be monitored.

**5.What does Nagios use to monitor?**

Nagios is now known as Nagios Core, is a free and open source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services.

**6.What does Check\_mk do?**

Check\_MK is an extension to the Nagios monitoring system that allows creating rule-based configuration using Python and offloading work from the Nagios core to make it scale better, allowing more systems to be monitored from a single Nagios server.

**7.What is icinga2?**

 Icinga 2 is an open source monitoring system which checks the availability of your network resources, notifies users of outages, and generates performance data for reporting. Scalable and extensible, Icinga 2 can monitor large, complex environments across multiple locations.

**8.What is a plugin**in**Nagios?**

Plugins are compiled executables or scripts (Perl scripts, shell scripts, etc.) that can be run from a command line to check the status or a host or service. Nagios uses the results from plugins to determine the current status of hosts and services on your network.

**9.Can Nagios monitor Windows machine?**

To monitor Windows Machines you will need to follow several steps and they are: Install NSClient++ addon on the Windows Machine. Configure Nagios Server for monitoring Windows Machine. Add new host and service definitions for Windows machine monitoring.

**10.What is**Nrpe**in Nagios?**

NRPE allows you to remotely execute Nagios plugins on other Linux/Unix machines. This allows you to monitor remote machine metrics (disk usage, CPU load, etc.). NRPE can also communicate with some of the Windows agent addons, so you can execute scripts and check metrics on remote Windows machines as well.

**11.What is Nagios XI?**

Nagios XI provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house and external applications, services, and systems.

**12.What are the benefits of using Nagios?**

**T**here are many benefits of using Nagios:

* Plan for infrastructure upgrades before outdated systems cause failures
* Respond to issues at the first sign of a problem
* Automatically fix problems when they are detected
* Coordinate technical team responses
* Ensure your organization’s SLAs are being met
* Ensure IT infrastructure outages have a minimal effect on your organization’s bottom line
* Monitor your entire infrastructure and business processes

13. **What is Active Check?**

A check that is initiated and performed by Nagios Core or Nagios XI – usually on a pre-determined schedule. Plugins are used to perform active checks.

**14.What is Nagios Log Server?**

Nagios Log Server greatly simplifies the process of searching your log data. Set up alerts to notify you when potential threats arise, or simply query your log data to quickly audit any system. With Nagios Log Server, you get all of your log data in one location, with high availability and fail-over built right in.

**15.What is Nagios Network Analyzer?**

Nagios Network Analyzer provides an in-depth look at all network traffic sources and potential security threats allowing system admins to quickly gather high-level information regarding the health of the network as well as highly granular data for complete and thorough network analysis using netflow, sflow, jflow, etc.

**16.Explain the process of website Monitoring With Nagios?**

Nagios provides complete monitoring of websites, web applications, web transactions, and web services – including availability, URL monitoring, HTTP status, content monitoring, hijack detection, and more.

**17.What are the benefits of website monitoring with Nagios?**

 Implementing effective website monitoring with Nagios offers the following benefits:

* Increased website and web application availability
* Increased website performance
* Fast detection of outages, website defacement, and website hijacking
* Capacity planning information for future web server and application upgrades

**18.What are the benefits of HTTP monitoring with Nagios?**

Nagios provides complete monitoring of HTTP and HTTPS servers and protocols.

Benefits – Implementing effective HTTP monitoring with Nagios offers the following benefits:

* Increased server, services, and application availability
* Fast detection of network outages and protocol failures
* User experience monitoring
* Web server performance monitoring
* Web transaction monitoring
* URL monitoring

**19.What are the benefits of SSL Certificate Monitoring With Nagios?**

Nagios provides SSL Certificate monitoring to ensure that expired certificates don’t negatively impact your organization’s websites, applications, and security.

Benefits – Implementing effective SSL Certificate monitoring with Nagios offers the following benefits:

* Increased website and application availability
* Increased security

**20.What are the benefits of Database Monitoring with Nagios?**

Nagios provides complete monitoring of database servers and databases – including availability, database and table sizes, cache ratios, and other key metrics.

Benefits – Implementing effective database monitoring with Nagios offers the following benefits:

* Increased application availability
* Increased database performance
* Fast detection of database outages, failures, and table corruption
* Predictive analysis of storage requirements and index performance

**21.Which databases**supports**Nagios?**

Nagios supports following databases for monitoring.

* MySQL
* Postgres
* Oracle
* DB2 Monitoring
* Microsoft SQL Server

**22.Nagios supports which protocol monitoring?**

Nagios supports following Protocol Monitoring:

* HTTP Monitoring
* DNS Monitoring
* FTP Monitoring
* SNMP Monitoring
* SMTP Monitoring
* SSH Monitoring
* LDAP Monitoring
* IMAP Monitoring
* POP Monitoring
* ICMP Monitoring
* DHCP Monitoring
* IPMI Monitoring

**23.What are the benefits of Operating System (OS) Monitoring with Nagios?**

Nagios provides complete monitoring of desktop and server operating systems – including system metrics, service states, process states, performance counters, event logs, applications (IIS, Exchange, Apache, MySQL, etc), and services (Active Directory, DHCP, Sendmail, etc).

Implementing effective operating system monitoring with Nagios offers the following benefits:

* Increased server, services, and application availability
* Fast detection of network outages and protocol failures
* Fast detection of failed services, processes and batch jobs

**Nagios supports which OS Monitoring?**

* Windows Monitoring
* Linux Monitoring
* UNIX Monitoring
* Solaris Monitoring
* AIX Monitoring
* HP-UX Monitoring
* RHEL Monitoring
* Ubuntu Monitoring
* Debian Monitoring
* CentOS Monitoring
* Fedora Monitoring
* SuSE Monitoring

**24.What are the benefits of Cloud Computing And Cloud Monitoring With Nagios?**

Nagios provides complete monitoring of cloud computing, web, and storage services. Nagios is capable of monitoring a variety of servers and operating systems – both physical and virtual.

Benefits – Implementing effective cloud monitoring with Nagios offers the following benefits:

* Increased server, services, and application availability
* Fast detection of network outages
* Fast detection of cloud computing environment problems

**25.Explain Virtualization With Nagios?**

Nagios provides the capabilities to monitor an assortment of metrics on many different virtualization platforms. In addition, Nagios can be run from several different virtualization platforms such as VMware, Microsoft Virtual PC, Xen, Amazon EC2, etc. Nagios had pre-built VM’s for both Nagios Core and Nagios XI created for VMware, as well as Virtual PC and OFV Template for Nagios XI.

Implementing effective virtualization monitoring with Nagios offers the following benefits:

* Increased server, services, and application availability
* Fast detection of server and operating system failures
* Fast detection of service and application failures
* Reduced deployment time
* Reduced administrative overhead
* Centralized configuration
* Ability to monitor the following Metrics

CPU Usage, Memory, Networking, Input / Output, Datastore usage, VM Status, Services, More…

**25.Explain Application Server Monitoring With Nagios?**

Nagios provides complete monitoring of application servers – including JBOSS, Websphere, Weblogic, ActiveMQ, and Tomcat.

 Implementing effective application server monitoring with Nagios offers the following benefits:

* Increased server, services, and application availability
* Fast detection of network outages and protocol failures
* Fast detection of failed process, services and batch jobs

**26.Explain Storage Monitoring With Nagios?**

Nagios provides complete monitoring of storage systems – including directory size, disk usage, file count, file presence, file size, S.M.A.R.T. status, RAID array status, and more.

Implementing effective storage monitoring with Nagios offers the following benefits:

* Detection of failed batch jobs
* Advanced planning for system upgrades
* Fast detection of storage subsystem problems
* Early detection of potential future failures
* Reduced risk of unexpected downtime

**27.Explain Log Monitoring and Management with Nagios?**

Nagios provides complete monitoring and log management of application logs, log files, event logs, service logs, and system logs on Windows servers, Linux servers, and Unix servers. Nagios is capable of monitoring system logs, application logs, log files, and syslog data, and alerting you when a log pattern is detected.

Implementing effective log monitoring with Nagios offers the following benefits:

* Increased security
* Increased awareness of network infrastructure problems
* Increased server, services, and application availability
* Fast detection of network outages and protocol failures
* Fast detection of failed processes, services, cron jobs, and batch jobs
* Audit compliance and regulatory compliance

**28.How does Nagios work?**

Nagios runs on a server, usually as a daemon or service. Nagios periodically runs plugins residing on the same server, they contact hosts or servers on your network or on the internet. One can view the status information using the web interface. You can also receive email or SMS notifications if something happens.

The Nagios daemon behaves like a scheduler that runs certain scripts at certain moments. It stores the results of those scripts and will run other scripts if these results change.

**29.What are Plugins in Nagios ?**

Plugins are scripts (Perl scripts, Shell scripts, etc.) that can run from a command line to check the status of a host or service. Nagios uses the results from the plugins to determine the current status of hosts and services on your network.

Once you have defined Plugins I will suggest you to explain why we need plugins.

Nagios will execute a Plugin whenever there is a need to check the status of a host or service. The plugin will perform the check and then simply returns the result to Nagios. Nagios will process the results that it receives from the Plugin and take the necessary actions.

**30.What is NRPE (Nagios Remote Plugin Executor) in Nagios** ?

The NRPE addon is designed to allow you to execute Nagios plugins on remote Linux/Unix machines. The main reason for doing this is to allow Nagios to monitor “local” resources (like CPU load, memory usage, etc.) on remote machines. Since these public resources are not usually exposed to external machines, an agent like NRPE must be installed on the remote Linux/Unix machines.

Now I will advise you to explain the NRPE architecture on the basis of diagram shown below.

The NRPE addon consists of two pieces:

* The check\_nrpe plugin, which resides on the local monitoring machine.
* The NRPE daemon, which runs on the remote Linux/Unix machine.

**31.What is meant by Nagios backend ?(unable to find a relevant explanation) ?**

Both Configuration and Logs can be stored in a backend. Configurations are stored in backend using NagiosQL. Historical data are stored using ndoutils. In addition, you also have nagdb and opdb.

**32.What Do You Mean By Passive Check In Nagios ?**

Passive checks are useful for monitoring services that are Asynchronous in nature and cannot be monitored effectively by polling their status on a regularly scheduled basis. It can also be used for monitoring services that are Located behind a firewall and cannot be checked actively from the monitoring host.

**33.When Does Nagios Check for external commands ?**

Nagios check for external commands under the following conditions:

* At regular intervals specified by the command\_check\_interval option in the main configuration file or,
* Immediately after event handlers are executed. This is in addition to the regular cycle of external command checks and is done to provide immediate action if an event handler submits commands to Nagios.

**34.What is the difference between Active and Passive check in Nagios ?**

The major difference between Active and Passive checks is that Active checks are initiated and performed by Nagios, while passive checks are performed by external applications.

If your interviewer is looking unconvinced with the above explanation then I will suggest you to also mention some key features of both Active and Passive checks:

Passive checks are useful for monitoring services that are:

* Asynchronous in nature and cannot be monitored effectively by polling their status on a regularly scheduled basis.
* Located behind a firewall and cannot be checked actively from the monitoring host.

The main features of Actives checks are as follows:

* Active checks are initiated by the Nagios process.
* Active checks are run on a regularly scheduled basis.

**35.How does Nagios help with Distributed Monitoring ?**

With Nagios you can monitor your whole enterprise by using a distributed monitoring scheme in which local slave instances of Nagios perform monitoring tasks and report the results back to a single master. You manage all configuration, notification, and reporting from the master, while the slaves do all the work. This design takes advantage of Nagios’s ability to utilize passive checks i.e. external applications or processes that send results back to Nagios. In a distributed configuration, these external applications are other instances of Nagios.

**36.Explain Main Configuration file of Nagios and its location ?**

The main configuration file contains a number of directives that affect how the Nagios daemon operates. This config file is read by both the Nagios daemon and the CGIs (It specifies the location of your main configuration file).

Now you can tell where it is present and how it is created.

A sample main configuration file is created in the base directory of the Nagios distribution when you run the configure script. The default name of the main configuration file is nagios.cfg, it is usually placed in the etc/ subdirectory of you Nagios installation (i.e. /usr/local/nagios/etc/).

**37.Explain how Flap Detection works in Nagios ?**

Flapping occurs when a service or host changes state too frequently, this causes lot of problem and recovery notifications.

Once you have defined Flapping explain how Nagios detects Flapping.

Whenever Nagios checks the status of a host or service, it will check to see if it has started or stopped flapping. Nagios follow the below procedure to do that:

* Storing the results of the last 21 checks of the host or service analyzing the historical check results and determine where state changes/transitions occur.
* Using the state transitions to determine a percent state change value (a measure of change) for the host or service.
* Comparing the percent state change value against low and high flapping thresholds
* A host or service is determined to have started flapping when its percent state change first exceeds a high flapping threshold.
* A host or service is determined to have stopped flapping when its percent state goes below a low flapping threshold.

**38.What is meant by saying Nagios is Object Oriented ?**

One of the features of Nagios is object configuration format in that you can create object definitions that inherit properties from other object definitions and hence the name. This simplifies and clarifies relationships between various components.

**39.What is State Stalking in Nagios ?**

State Stalking is used for logging purposes. When Stalking is enabled for a particular host or service, Nagios will watch that host or service very carefully and log any changes it sees in the output of check results.  
Depending on the discussion between you and interviewer you can also add:

It can be very helpful in later analysis of the log files. Under normal circumstances, the result of a host or service check is only logged if the host or service has changed state since it was last checked.

**40.Nagios says my machine is unreachable, not down. What is the difference and how it is achieved ?**

When Nagios says a node is unreachable, a node is unreachable if Nagios is not able to find a path to the node.

Now you can mention the difference.

The node itself may be up but because Nagios is unable to connect to it, it has to mark this as unreachable. To achieve this, Nagios use parent-child relationship between components.

Finally for better understanding explain it with an example.

A router may be defined as a parent for a server.

* Now Nagios checks for server and marks it as down.
* It then checks the parent (in our example, the router)
* If parent is also down, then server is marked as unreachable.
* If Parent is up, the server is marked as really down.

**41.Explain What Is Soft And Hard States ?**

When a service or host check results are in a non-OK or non-UP state and the service check has not yet been rechecked the number of times specified by the max\_check\_attempts directives in the service or host definition. This is called Soft Error. When a service or a host recovers from Soft Error that is considered as Soft Recovery.

When a service or host check results are in a non-OK or non-UP state and the service check has been rechecked the number of times specified by the max\_check\_attempts directives in the service or host definition. This is called Hard Error. When a service or a host recovers from Hard Error that is considered as Hard Recovery.

**42.What Are Ports Numbers Nagios Will Use To Monitor Clients ?**

Port numbers are 5666, 5667 and 5668

**43.Explain Main Configuration File And Its Location ?**

**Resource File:** It is used to store sensitive information like username, passwords with out making them available to the CGIs. Default path: /usr/local/nagios/etc/resource.cfg

**Object Definition Files:** It is the location were you define all you want to monitor and how you want to monitor. It is used to define hosts, services, hostgroups, contacts, contact groups, commands, etc.. Default Path:/usr/local/nagios/etc/objects/

**CGI Configuration File:** The CGI configuration file contains a number of directives that affect the operation of the CGIs. It also contains a reference the main configuration file, so the CGIs know how you’ve configured Nagios and where your object definitions are stored. Default Path: /usr/local/nagios/sbin/

**44.How To Generate Performance Graphs ?**

 In Nagios Core there is no inbuilt option to generate the performance graphs, We have to install pnp4nagios and add hosts and services URL’s in defination files.

**45.How To Verify Nagios Configuration ?**

In order to verify your configuration, run Nagios with the -v command line option like so:

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

If you’ve forgotten to enter some critical data or misconfigured things, Nagios will spit out a warning or error message that should point you to the location of the problem. Error messages generally print out the line in the configuration file that seems to be the source of the problem. On errors, Nagios will often exit the pre-flight check and return to the command prompt after printing only the first error that it has encountered.