Nagios Skills Test Upwork

**In order to run Nagios XI on your server, what is the minimum hard drive required?**

a.10 GB  
b.20 GB  
c.30 GB  
d.40 GB

**With regard to NRPE v3, what can be the maximum packet size?**

a. 1K  
b. 16K  
c. 32K  
d. 64K

**While using Auto-Discovery in Nagios XI, which of the following statements are correct about the View Job functionality?**

a. We cannot view all the hosts.  
b. We can view the new discovered hosts.  
c. Discovered services can be displayed.  
d. All of the above.

**In the NAGIOS-NOTIFY-MIB.txt file, which of the following lines send(s) the trap to Nagios?**

a. FORMAT  
b. EXEC  
c. EVENT  
d. Both b and c

**Which of the following commands can be used to start Nagios Core in Red Hat Enterprise Linux 7.x?**

a. service nagios start  
b. systemctl start nagios.service  
c. svcadm enable nagios  
d. sudo systemctl start nagios.service

**While working with the Nagios.cfg file, which of the following statements are incorrect?**  
**1. Dollar symbol "$" can be used for writing comments.**  
**2. White spaces are not allowed before a variable name.**  
**3. Variable names are case-insensitive.**

a. All 1, 2 and 3.  
b. Only 2 and 3.  
c. Only 1 and 3.  
d. Only 1 and 2.

**With regard to Host Dependency Definition, which of the following values of the notification\_failure\_criteria directive represents the criteria, "fail on an UP state"?**

a. o  
b. u  
c. p  
d. n

**While configuring the firewall, which of the following commands can be used to create a firewall rule on your Oracle Linux 7.x machine for allowing incoming traffic to NCPA on TCP port 5693?**

a. iptables -I INPUT -p tcp --destination-port 5693 -j ACCEPT  
service iptables save  
ip6tables -I INPUT -p tcp --destination-port 5693 -j ACCEPT  
service ip6tables save  
b. sudo mkdir -p /etc/ufw/applications.d  
sudo sh -c "echo '[NCPA]' > /etc/ufw/applications.d/ncpa"  
sudo sh -c "echo 'title=Nagios Cross Platorm Agent' >> /etc/ufw/applications.d/ncpa"  
sudo sh -c "echo 'description=Nagios Monitoring Agent' >> /etc/ufw/applications.d/ncpa"  
sudo sh -c "echo 'ports=5693/tcp' >> /etc/ufw/applications.d/ncpa"  
sudo ufw allow NCPA sudo ufw reload  
c. sudo /usr/sbin/SuSEfirewall2 open EXT TCP 5693  
sudo systemctl restart SuSEfirewall2.service  
d. firewall-cmd --zone=public --add-port=5693/tcp  
firewall-cmd --zone=public --add-port=5693/tcp --permanent

**While working with Nagios, the NRPE add-on consists of which of the following options?**  
**1. The NRPE agent that runs on the remote Linux/Unix server.**  
**2. The check\_nrpe plugin.**

a. Only 1.  
b. Only 2.  
c. Both 1 and 2.  
d. Neither 1 nor2.

**In order to configure hosts during the integration of Google Maps with Nagios XI, which of the following options is used to open the Host Management page?**

a. Dashboards  
b. Tools  
c. Configure  
d. Admin

**While editing the NSClient++ configuration file, the following lines should be added under which of the given sections?**  
**NRPEListener.dll**  
**NSClientListener.dll**  
**FileLogger.dll**  
**CheckSystem.dll**  
**CheckDisk.dll**  
**CheckEventLog.dll**  
**CheckHelpers.dll**  
**CheckExternalScripts.dll**

a. [modules]  
b. [NRPE]  
c. [External Script]  
d. None of the above

**With regard to Nagios frontends, which of the following options is NOT a Nagios web interface?**

a. Nagios V-Shell  
b. jNag  
c. Nagios Dashboard – PHP  
d. Birdseye

**With regard to mapping a Nagios XI user account to the Nagios Fusion user account, which of the following statements are correct?**

a. It gives surety that the multi-tenancy feature of Nagios XI flows through to Nagios Fusion.  
b. It gives the surety that the Fusion user can see all the objects in Nagios XI.  
c. Mapping is available only if a Fusekey is provided while fusing the Nagios XI server.  
d. All of the above statements are correct.

**Which of the following statements are correct about the NCPA Listener service?**  
**1. It serves and handles connections to the web graphical user interface.**  
**2. It connects and sends passive check results to the defined NRDP URL.**  
**3. It handles external API requests.**  
**4. It provides API for live graphing.**

1. All 1, 2, 3 and 4.  
   b. Only 1, 2 and 3.  
   c. Only 1, 2 and 4.  
   d. Only 1, 3 and 4.

**Which of the following is the default value of the service\_check\_timeout option in the Nagios.cfg configuration file?**

a. c  
b. u  
c. w  
d. o

**The main Nagios configuration file is usually located in which of the following directories?**

a. /usr/local/nagios/conf/  
b. /usr/path/nagios/conf/  
c. /usr/local/nagios/etc/  
d. /usr/path/nagios/etc/

**In Nagios XI, when you navigate to Home > Maps menu, which of the following options are available?**  
**1. BBmap**  
**2. Google Map**  
**3. Hyper Map**  
**4. Value Map**

a. All 1, 2, 3 and 4.  
b. Only 1, 2 and 3.  
c. Only 1, 3 and 4.  
d. Only 2, 3 and 4.

**While configuring NSClient++ during the installation of Windows agent, NSClient++, a password is mandatory for communication between the Nagios server and the Windows machine. This password is used by which of the following plugins?**

a. check\_nrpe  
b. check\_nt  
c. check\_users  
d. check\_ntp\_peer

**While configuring an auto-discovery job in the New Auto-Discovery Job form, we can enter the amount of time in the Scan Delay field in:**

a. nanoseconds.  
b. microseconds.  
c. milliseconds.  
d. seconds.

**In Nagios XI, trap definitions are defined in the /etc/snmp/snmptt.conf file. These definitions start with which of the following lines?**

a. EXEC 3  
b. EVENT 1  
c. FORMAT 2

**Nagios XI allows users to add how many customized dashboards?**

a. Only one.  
b. Only two.  
c. Only three.  
d. Multiple number of dashboards.

**While installing NCPA on Windows, which of the following tokens is used to access the web interface and agent's API?**

a. /D  
b. /NRDPTOKEN  
c. /TOKEN  
d. /S  
e. /NRDPURL

**Which of the following versions of SNMP provides community-based security?**

1. SNMP v2c  
   b. SNMP v2u  
   c. SNMP v1  
   d. SNMP v3

**While integrating SNMP traps with Nagios XI, the EXEC line executes which of the following python scripts that will submit the check result to Nagios XI, by default?**

a. /usr/local/bin/snmptraphandling.py  
b. /home/local/snmptraphandling.py  
c. /root/home/bin/snmptraphandling.py  
d. /system/local/bin/ snmptraphandling.py

**While using Auto-Discovery in Nagios XI, which of the following functionalities is NOT provided by the Action column on the Auto-Discovery Jobs page?**

1. Start Job  
   b. View job  
   c. Re-Run Job  
   d. Delete Job

**In relation to the service\_perfdata\_file\_mode option in the Nagios.cfg file, which of the following options is the correct value that can be used to open a service performance data file in the non-blocking read/write mode?**

a. a  
b. r  
c. w  
d. p

**With regard to the max\_service\_check\_spread option in the Nagios.cfg file, what is the default value?**

a. 10 minutes  
b. 20 minutes  
c. 30 minutes  
d. 60 minutes

**Which of the following tasks will be performed by the NagiosXI-SNMPTrap-setup.sh script on its execution on the Nagios XI server as the root user?**

a. In order to open UDP port 162, it adds a firewall rule to Nagios server.  
b. It modifies only the snmptt.ini file.  
c. It adds the snmptt user to the Nagios group.  
d. All of the above.

**Which of the following commands is used to carry back the value(s) or signal of actions that are directed by the SNMP Manager?**

a. SET  
b. TRAPS  
c. INFORM  
d. RESPONSE

**With regard to Host definitions in Nagios, what are the possible values of stalking\_options directive?**

a. o  
b. s  
c. d  
d. u

**SSH uses which type of cryptography for authentication?**

1. Secret key cryptography  
   b. Public key cryptography  
   c. Hash function  
   d. None of the above.

**Nagios can be stopped through which of the following ways?**  
**1. init script**  
**2. web interface**  
**3. Manually**

1. All 1, 2 and 3.  
   b. Only 1 and 2.  
   c. Only 1 and 3.  
   d. Only 2 and 3.
2. **In relation to the log\_rotation\_method in the Nagios.cfg file, what is the default value of this rotation method?**
3. a. d  
   b. w  
   c. m  
   d. n  
   e. h

**While monitoring hosts using SSH, SSH keys for the Nagios user on your Nagios XI server should be configured. Which of the following commands can be used after establishing a terminal session with your Nagios XI server as root?**  
**1. su nagios**  
**2. ssh-keygen**  
**3. ssh-agent**  
**4. ssh-add**

a. All 1, 2, 3 and 4.  
b. Only 1 and 2.  
c. Only 1 and 3.  
d. Only 1, 2 and 3.  
e. Only 1, 2 and 4.

**While configuring the Google Maps during the integration of Google Maps with Nagios XI, which of the following options will you find under the Misc Settings tab on the Host Management page?**  
**1. VRML image**  
**2. Status image**  
**3. Icon image**  
**4. Action URL**

1. All 1, 2, 3 and 4.  
   b. Only 1, 2 and 3.  
   c. Only 1 and 4.  
   d. Only 2, 3 and 4.  
   e. Only 1 and 2.

**While monitoring hosts using SSH, public and private SSH keys are saved in which of the following directories?**

1. /usr/path/nagios/.ssh  
   b. /home/path/nagios/.ssh  
   c. /root/nagios/.ssh  
   d. /home/nagios/.ssh

**Which of the following keys is used in NRPE v3 for SSL security?**

1. 256-bit key  
   b. 512-bit key  
   c. 1024-bit DH key  
   d. 2048-bit DH key

**In relation to monitoring hosts using SSH, which of the following options are mandatory to monitor the remote Linux/Unix server by using the check\_by\_ssh plugin?**  
**1. Nagios user must be created.**  
**2. Nagios plugins and/or monitoring scripts must be installed.**  
**3. SSH daemon must be installed and configured.**

a. All 1, 2 and 3.  
b. Only 1 and 2.  
c. Only 2 and 3.  
d. Only 1 and 3.

**Which of the following SNMP versions provides user-based security?**

1. SNMP v1  
   b. SNMP v2c  
   c. SNMP v2  
   d. SNMP v3
2. **In relation to the Nagios.cfg file, which of the following statements are correct?**  
   **1. The Object Cache File directive is used for specifying a file in which a cached copy of object definitions should be stored.**  
   **2. The cache file is created only once when the Nagios is started for the first time.**  
   **3. Cache file is used by the CGIs.**
3. a. All 1, 2 and 3 are correct.  
   b. Only 1 and 2 are correct.  
   c. Only 2 and 3 are correct.  
   d. Only 1 and 3 are correct.
4. **In relation to Extended Host Information Definition, the vrml\_image variable is used to define the names of which of the following types of images that should be associated with the host?**  
   **1. JPG**  
   **2. GIF**  
   **3. PNG**
5. a. All 1, 2 and 3.  
   b. Only 1 and 2.  
   c. Only 1 and 3.  
   d. Only 2 and 3.

**In relation to enabling the NRPE listener in NSClient++ 0.4.x, which of the following statements are correct about using check\_nrpe instead of check\_nt?**  
**1. The built-in memory/disk/CPU checks are more flexible and customizable.**  
**2. The CheckExternalScripts module can execute Perl, Python and PowerShell scripts.**  
**3. It uses SSL.**

a. All 1, 2 and 3.  
b. Only 1 and 2.  
c. Only 1 and 3.  
d. Only 2 and 3.

**While using Auto-Discovery in Nagios XI, a network scan is performed using which of the following commands?**  
**1. ping**  
**2. nmap**

a. Only 1.  
b. Only 2.  
c. Both 1 and 2 are used.  
d. Neither 1 nor 2 is used.

**If you want to configure the Google Maps to show a marker bubble that indicates the status of a host, then you need to add the longitude and latitude coordinates to the notes directive in the host object. Under which of the following directives will you find the Notes field to add the longitude and latitude coordinates?**

1. Common Settings  
   b. Check Settings  
   c. Alert Settings  
   d. Misc Settings

**With regard to NCPA API, which of the following are the correct options for the aggregate parameter of the cpu standard module?**

a. avg  
b. min  
c. max  
d. count

**With regard to the $NOTIFICATIONTYPE$ macro, which of the following are the valid values for the macro that can be used?**

1. PROBLEM  
   b. FLAPPINGSTOP  
   c. CRITICAL  
   d. ACKNOWLEDGEMENT
2. **Which of the following options is the default value of the check\_external\_commands option in the Nagios.cfg file?**
3. a. -1  
   b. 0  
   c. 1  
   d. None of the above.
4. **Which of the following options are the standard modules that are built directly into NCPA?**
5. a. cpu  
   b. interface  
   c. services  
   d. logs
6. **While installing the NSClient++ agent on a Windows machine, which of the following setup types are available to be installed?**
7. a. Basic  
   b. Typical  
   c. Custom  
   d. Complete

**Which of the following are the valid options that can be used to restart Nagios daemon?**

a. kill -HUP <nagios\_pid>  
b. kill <nagios\_pid>  
c. /etc/rc.d/init.d/nagios reload  
d. /etc/rc.d/init.d/nagios restart

**In order to run Nagios XI on your server, what is the minimum memory required?**

a. 2 GB  
b. 4 GB  
c. 6 GB  
d. 8 GB

**Which of the following are the required versions of the Redhat Enterprise Linux (RHEL) for running Nagios XI?**

a. RHEL 4  
b. RHEL 5  
c. RHEL 6  
d. RHEL 7

**Which of the following options are the invalid directives of Host Group Definitions in Nagios?**

a. hostgroup\_members  
b. process\_perf\_data  
c. retain\_status\_information  
d. action\_url

**In relation to Contact Definition, which of the following options are the valid values of the service\_notification\_options directive?**

a. w  
b. u  
c. c  
d. d

**While defining a service in Nagios, which of the following are the possible values of the notification\_options directive?**

a. w  
b. u  
c. c  
d. o

**While configuring an auto-discovery job in Nagios XI, which of the following options are available in the New Auto-Discovery Job form?**

a. Scan Target  
b. Include IPs  
c. Exclude IPs  
d. Scan Delay

**While defining a host in Nagios, which of the following directives are optional?**

a. check\_period  
b. notification\_interval  
c. action\_url  
d. notifications\_enabled

**While managing dashboards in Nagios XI through the Manage My Dashboards link, which of the following actions can be performed?**

a. We can create a dashboard.  
b. We can clone a dashboard.  
c. We can edit a dashboard.  
d. We can delete a dashboard.

**In relation to configuring the Nagios server to send mail notifications, which of the following are the correct options for the service\_notification\_options directive that can be used for defining the service states, for which, notifications can be sent out to a contact?**

a. w  
b. u  
c. f  
d. d

**Which of the following statements is/are correct about secure shell (SSH)?**

1. It is a network protocol through which an administrator can access a remote computer securely.  
   b. SSH uses the peer-to-peer model instead of the client-server model.  
   c. SSH does not support tunnelling.  
   d. By default, it listens on TCP port 22.

**With regard to the execute\_service\_checks option in the Nagios.cfg file, which of the following options are the valid values that can be used?**

1. TRUE  
   b. FALSE  
   c. 0  
   d. 1(default)  
   e. -1
2. **In relation to configuring the firewall on Mac OS X, which of the following statements are correct?**
3. a. The firewall is enabled by default.  
   b. The firewall is disabled by default.  
   c. Firewall allows TCP port 5693.  
   d. Firewall does not allow TCP port 5693.

**In order to receive IPv6 SNMP traps on CentOS 6.x, the following line is replaced with which of the given lines?**  
**OPTIONS="-Lsd -p /var/run/snmptrapd.pid"**

a. OPTIONS="udp:162 udp6:162"  
b. OPTIONS="-udp:162 udp6:162 -p /run/snmptrapd.pid"  
c. OPTIONS="-Lsd udp:162 udp6:162 -p /var/run/snmptrapd.pid"

**While defining a host in Nagios, which of the following directives are mandatory?**

a. host\_name  
b. address  
c. check\_interval  
d. max\_check\_attempts

**Which of the following options are the valid directives that can be used to define a host?**

1. parents  
   b. hostgroups  
   c. event\_handler\_enabled

**Nagios XI, by default, rotates through different views that are defined by a user. In order to adjust the speed of rotation, what can be the maximum speed?**

1. 20 seconds  
   b. 40 seconds  
   c. 60 seconds  
   d. 90 seconds

**With regard to Host Group Definitions in Nagios, which of the following options are the mandatory directives?**

a. hostgroup\_name  
b. alias  
c. members  
d. hostgroup\_members

**The NSClient++ agent can be downloaded from Nagios XI web interface when using the Windows Server monitoring wizard.**

a. True  
b. False

**While installing the Windows agent, NSClient++, which of the following Modules to load options are available in the NSClient++ Configuration dialog box?**

a. Enable common check plugins  
b. Enable NRPE server (check\_nrpe)  
c. Enable NSCA client  
d. Enable Apache server

**While monitoring Windows machines, which of the following tasks are a part of Active Checks?**

a. Installing the check\_ncpa.py plugin.  
b. Restarting the Nagios daemon.  
c. Adding checks to the ncpa configuration.  
d. Configuring NRDP settings.

**Which of the following is/are the correct key functions of an SNMP Manager?**

1. It is used for querying agents.  
   b. It is used for setting variables in agents.  
   c. It is used for getting response from agents.  
   d. It is used for storing and retrieving management information as defined in the MIB

**This question is based upon the figure shown below**  
**This service will generate alerts if the SSH server does not respond:**

1. within 5 seconds.  
   b. within 8 seconds.  
   c. within 10 seconds.  
   d. within 15 seconds.

**The minimal.cfg file is contained in which of the following directories?**

1. default-object/  
   b. template-object/  
   c. template-extinfo/  
   d. None of the above

**An agent is required for monitoring while implementing effective SNMP Trap management with Nagios.**

a. True  
b. False

**This question is based upon the figure shown below**  
**In Nagios XI interface, what is the function of the icon shown in the given image?**

a. It is used to upload a dashlet on the web.  
b. It is used to add a dashlet to the Nagios core.  
c. It is used to add a dashlet to any dashboard.  
d. It is used to print the dashboard elements.

**This question is based upon the figure shown below**  
**In relation to adding dashlets to dashboard in Nagios XI, what is the function of the icon shown in the given image?**

a. It is used to remove a dashlet from the dashboard.  
b. It is used to hide the dashboard.  
c. It is used to hide the title of a dashlet.  
d. It is used to hide a dashlet.

**In order to add a Google API key, we can execute the following command on a Nagios XI server as the root user, after establishing a terminal or SSH connection.**  
**vi /usr/local/nagiosxi/html/includes/components/googlemap/map.php**

a. True  
b. False

**Can more than one EVENT exist with the same OID/MIB in the snmptt.conf file?**

a. Yes  
b. No

**While working with Ubuntu 14.04, which of the following are the valid commands that can be used to create a user named nagios and a group named gpcmd, and to add the user to the group?**

a. sudo user-add nagios  
sudo group-add gpcmd  
sudo usermod -a -G gpcmd nagios  
b. sudo add-user nagios  
sudo add-group gpcmd  
sudo usermod -n -G gpcmd nagios  
c. sudo adduser nagios  
sudo addgroup gpcmd  
sudo usermod -n -G gpcmd nagios  
d. sudo useradd nagios  
sudo groupadd gpcmd  
sudo usermod -a -G gpcmd nagios

**While configuring an auto-discovery job in the New Auto-Discovery Job form, what will happen when a comma-separated list of IP addresses and/or network addresses is entered in the Exclude IPs field to exclude from the scan?**

a.The excluded addresses will never be pinged.  
b.The excluded addresses may be pinged but will not be scanned for available or open services via nmap.  
c.The excluded addresses will be pinged and scanned for available or open services via nmap.  
d.The excluded addresses will never be pinged but will be scanned for available or open services via nmap.

**Nagios Core 4.3.4 can be installed on which of the following operating systems?**  
**1. Red Hat Enterprise Linux (RHEL)**  
**2. Apple OS X**  
**3. FreeBSD**

1. All 1, 2 and 3.  
   b. Only 1 and 2.  
   c. Only 1 and 3.  
   d. Only 2 and 3.

**Nagios Interview Questions # 1) What is Nagios?**

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

**Nagios Interview Questions # 2) What is Nagios monitoring tool in Linux?**

A) 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. **Nagios Interview Questions #** 3) What is an icinga?

A) 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.

**Nagios Interview Questions # 4) What is active and passive checks in Nagios?**

A) 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.

**Nagios Interview Questions # 5) What is OID Nagios?**

A) 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.

### Nagios Basic Interview Questions

**Nagios Interview Questions # 6) What does Nagios use to monitor?**

A) 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.

**Nagios Interview Questions # 7) What does Check\_mk do?**

A) 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.

**Nagios Interview Questions # 8) What is icinga2?**

A) 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.

**Nagios Interview Questions # 9) What is a plugin**in**Nagios?**

A) 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.

**Nagios Interview Questions # 10) Can Nagios monitor Windows machine?**

A) 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.

### Nagios XI Interview Questions

**Nagios Interview Questions #** **11) What is**Nrpe**in Nagios?**

A) 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.

**Nagios Interview Questions # 12) What is Nagios XI?**

A) 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.

**Nagios Interview Questions # 13) What are the benefits of using Nagios?**

A) There 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

**Nagios Interview Questions # 14) What is Active Check?**

A) 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.

**Nagios Server Interview Questions**

**Nagios Interview Questions # 15) What is Nagios Log Server?**

A) 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.

**Nagios Interview Questions # 16) What is Nagios Network Analyzer?**

A) 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.

**Nagios Interview Questions # 17) Explain the process of website Monitoring With Nagios?**

A) 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.

**Nagios Interview Questions # 18) What are the benefits of website monitoring with Nagios?**

A) 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

**Nagios Interview Questions # 19) What are the benefits of HTTP monitoring with Nagios?**

A) 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

**Nagios Server Interview Questions**

**Nagios Interview Questions # 20) What are the benefits of SSL Certificate Monitoring With Nagios?**

A) 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

**Nagios Interview Questions # 21) What are the benefits of Database Monitoring with Nagios?**

A) 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

**Nagios Interview Questions # 22) Which databases**supports**Nagios?**

A) Nagios supports following databases for monitoring.

1. MySQL
2. Postgres
3. Oracle
4. DB2 Monitoring
5. Microsoft SQL Server

**Nagios Interview Questions # 23) Nagios supports which protocol monitoring?**

A) 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

**Nagios Interview Questions # 24) What are the benefits of Operating System (OS) Monitoring with Nagios?**

A) 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).

Benefits: 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 Interview Questions # 25) Nagios supports which OS Monitoring?**

A) Nagios supports following operating system 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

**Nagios Interview Questions # 26) What are the benefits of Cloud Computing And Cloud Monitoring With Nagios?**

A) 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

**Nagios Interview Questions # 27) Explain Virtualization With Nagios?**

A) 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.

Benefits: 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…

**Nagios Interview Questions # 28) Explain Application Server Monitoring With Nagios?**

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

Benefits: 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

**Nagios Interview Questions # 29) Explain Storage Monitoring With Nagios?**

A) 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.

Benefits: 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

**Nagios Interview Questions # 30) Explain Log Monitoring and Management with Nagios?**

A) 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.

Benefits: 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

### **Nagios Tricky Interview Question Answer**

#### **Q1). Explain Nagios or what is Nagios, explain it.**

Nagios is a monitoring tool that is used for continuous monitoring of system services, applications, and business processes. Even in case of any failure, Nagios tool can alert the technical staff about the problem. As a result, DevOps professionals or technical team members can begin the required remediation processes before the negative impact of any business processes, customers, and end-users. Here, in such cases, the team does not have to explain anyone that why an unseen infrastructure outage affects the bottom line of the organization.

Now as you know ‘what is Nagios?’ then you can also mention the things that can be achieved by the Nagios DevOps tool:

* Automatic problem fixing as and when they occur.
* Infrastructure upgrades planning even before any failure due to an outdated system.
* Technical team response coordination.
* To ensure that SLA of your organization will be met.
* To monitor the business process and the entire infrastructure.
* To respond to issues even as and when they arise.

[**Read:   Jenkins Interview Questions and Answers**](https://www.janbasktraining.com/blog/jenkins-interview-questions/)

Above-mentioned are all major factors that make Nagios a complete tool for continuous monitoring. (Here in such question you can also add some advantages of Nagios if time permits.)

#### **Q2). Explain the working of Nagios, how does it work?**

On a server, Nagios either runs as a service or daemon. Plugins that resides on the same server are being run by the Nagios; basically, they contact the hosts or servers of your network or on the internet. We can check the status by web interface; even notifications can also be received by email or SMS when something happens.

Nagios service runs certain scripts after a fix time interval, so it acts as a scheduler. It can store the script result and run other scripts when it is changed.

#### **Q3). Explain Nagios plugins.**

Plugins are basically scripts of Perl and Shell that can be run through the command line to check the service status of the host. Nagios can also use the result of the plugins that determine the present status of host or services of the network.

Now an answer to the questions that why we need plugins, you can also add here that, plugins is executed by Nagios to check the status of any service or host. A check is performed by the plugin and the result is returned to Nagios. The result is processed by Nagios to take the necessary actions.

#### **Q4). What do you understand by NRPE or Nagios Remote Plugin Executor of Nagios?**

NRPE or Nagios remote plugin executor is designed to allow execution of plugins on remote Linux or UNIX based machines. These plugins are executed to monitor the usage of CPU load and memory usage like a local resource of remote machines. It is required as this information is not usually exposed publicly to an external machine and for this purpose, NRPE agent is installed on remote machines.

NRPE add-on or plugin has two components that work together to perform the task:

* A ‘check\_nrpe’ plugin that resides on the local machine and it is used for monitoring
* The NRPE daemon that can run on remote machines

#### **Q5). What are port numbers used by Nagios for monitoring purpose?**

Usually, the port number 5666, 5667 and 5668 are used for monitoring in Nagios DevOps tool.

#### **Q6). Explain main configuration file and its location.**

Following is the description of the main configuration file:

**Resource File:** To store sensitive information like user details that may include username and passwords it is used. The information is not made available to CGI.

[**Read:   Top 20 Git Interview Questions and Answers 2018**](https://www.janbasktraining.com/blog/git-interview-questions/)

**Object Definition File:**  In this file, you can find and enlist the details of resources that you want to monitor and how you want the monitoring to be performed? Host services, host groups, contacts, contact groups, commands, etc. are defined in this file.

**CGI Configuration File:** Several directives are contained and stored in CGI file that can affect the CGI o. A reference to the main configuration file is also stored in this file, so that CGI can know the details of Nagios configuration as and when required and the location of object definition storage.

#### **Q7). What are state types of Nagios?**

Following are the state types of Nagios:

* Service or host state type
* Some states like OK, WARNING, UP, or DOWN state host or service
* Two state types that are SOFT state or HARD state

#### **Q8). What are SOFT and HARD states?**

We can define soft and hard states as:

* In case of the SOFT state, the service or host check results are not OK or not up to the mark, even in case if service check has not been rechecked the number of times that are specified for it moreover the times that is being specified by the max\_check\_attempts directive. Recovery of the component from such Soft error is called Soft Recovery.
* When a host or service check result is not ‘OK’ and it has been checked for the number of times, specified by the max\_check\_attempts directive in the host definition, then this error is known as Hard Error. Recovery of any service from this error is known as Hard Recovery.

#### **Q9). What is state stalking in Nagios?**

State stalking is used for logging purpose in Nagios. When stalking is enabled for any service or host then Nagios watch it very carefully and store any changes that if found in the check result of that resource.

Stalking can be helpful in later stages of log file analysis. Here in such scenario, any host or service check can be performed only if it has been updated for the last time.

#### **Q10). Why is it being said that Nagios is object oriented?**

Nagios has object configuration format where you can create object definitions, that can inherit the properties from other hostnames or object definitions. In this way, you can specify the component relationships easily. The components are considered as objects by the Nagios.

[**Read:   What is Docker? Docker Commands Cheat Sheet with Example for Ubuntu**](https://www.janbasktraining.com/blog/docker-commands-cheat-sheet/)

#### **Q11). Which three Nagios variables can affect recursion and inheritance in Nagios?**

The three variables that affect recursion and inheritance are:

* Name
* Use
* Register

Here, Name is just a placeholder that can be used by the other objects. Use variable can be used to define parent object, whose properties are to be used. Registers are also used for storing values that can be either 0 or 1. Register values cannot be inherited.

#### **Q12). How Does Flap detection work in Nagios?**

When a service or host changes their state frequently, then it is called flapping that may cause lots of problems and generate too many recovery notifications. Flapping is detected in the following manner:

* Store the results of last 21 checks and then analyze this historical check result to know the number of transitions that are being taken place by the host or service.
* Know the percent state change value with the help of state transition
* Compare the value of this state change against low and high flapping thresholds
* When this value exceeds then the highest specified threshold then it is called flapping
* When this percent state value goes down the specified value then it is said that flapping has been stopped.

#### **Q13). Explain main configuration file of Nagios.**

Several directives are contained in the main configuration file that can affect Nagios daemon. This file is read by both CGIs and Nagios daemons.

A Nagios file is usually created in the base Nagios directory, at the time when you run configuration script. The name of this file that is the main configuration file is ‘nagios.cfg’ and is usually placed in etc/subdirectory

#### **Q14). How is distributed monitoring being done in Nagios?**

There is a distributed monitoring scheme in Nagios with the help of which you can monitor your complete enterprise that may include local slave instances. In such environment, Nagios submit the result of reports of tasks to a single machine. All configuration, reporting, and notification can be managed at the master machine and here slaves do all the work. Here Nagios uses passive checks that are basically external applications that can send the results back to Nagios.

#### **Q15). Differentiate between active and passive check.**

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

1. What is Nagios? (Nagios Interview Questions)

**Answer:** Nagios is one of the monitoring tools. It is used for Continuous monitoring of systems, applications, services, and business processes etc. in a DevOps culture. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affects business processes, end-users, or customers. With Nagios you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line. (Nagios Interview Questions)

2. How does Nagios work?

**Answer:** 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.

3. What are Plugins in Nagios ?

**Answer:** 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.

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

**Answer:** 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.

(Nagios Interview Questions)

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

**Answer:** 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.

6. What Do You Mean By Passive Check In Nagios ?

**Answer:** Passive checks are initiated and performed by external applications/processes and the Passive check results are submitted to Nagios for processing.

7. Explain The Need For Passive Check ?

**Answer:** 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.

8. When Does Nagios Check for external commands ?

**Answer:** 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.

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

**Answer:** 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.

10. How does Nagios help with Distributed Monitoring ?

**Answer:** 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. ([Top 15 Devops SaltStack Questions and Answers Pdf](https://svrtechnologies.com/top-15-devops-saltstack-interview-questions/))

11. Explain Main Configuration file of Nagios and its location ?

**Answer:** 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/).

12. Explain how Flap Detection works in Nagios ?

**Answer:** 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](https://svrtechnologies.com/) to have stopped flapping when its percent state goes below a low flapping threshold.

13. What is meant by saying Nagios is Object Oriented ?

**Answer:** 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.

14. What is State Stalking in Nagios ?

**Answer:** 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.

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

**Answer:** 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.

16. Explain What Is Soft And Hard States ?

**Answer:** 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.

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

**Answer:** Port numbers are 5666, 5667 and 5668

18. Explain Main Configuration File And Its Location ?

**Answer:**

**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/

19. How To Generate Performance Graphs ?

**Answer:** 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.

20. How To Verify Nagios Configuration ?

**Answer:** 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.

1. **Question 1. What Are Plugins In Nagios?**

**Answer :**

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.

1. **Question 2. What Is Nagios And How It Works ?**

**Answer :**

Nagios is an open source System and Network Monitoring application. Nagios runs on a server, usually as a daemon or service. Nagios periodically run plugins to monitor clients, if it found anything warning and critical it will send an alerts via Email OR SMS as per the configuration.

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.

1. **Question 3. What Are Ports Numbers Nagios Will Use To Monitor Clients?**

**Answer :**

Port numbers are 5666, 5667 and 5668

1. **Question 4. Explain Main Configuration File And Its Location?**

**Answer :**

* 1. **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
  2. **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/
  3. **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/

1. **Question 5. Nagios Administrator Is Adding 100+ Clients In Monitoring But He Don’t Want To Add Every .cfg File Entry In Nagios.cfg File He Want To Enable A Directory Path. How Can He Configure Directory For All Configuration Files?**

**Answer :**

He can able to achieve the above scenario by adding the directory path in nagios.cfg file, in line number 54 we have to add below line.

54  cfg\_dir=/usr/local/nagios/etc/objects/monitor

1. **Question 6. What Is Nagios?**

**Answer :**

Nagios is one of the monitoring tools. It is used for Continuous monitoring of systems, applications, services, and business processes etc. in a DevOps culture. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affects business processes, end-users, or customers. With Nagios you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line.

1. **Question 7. Now, Once You Have Defined What Is Nagios, You Can Mention The Various Things That You Can Achieve Using Nagios?**

**Answer :**

By using Nagios you can:

• 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.

This overall completes the answer to this question. The further details like advantages etc. can be added as per the direction where the discussion is heading.

1. **Question 8. Explain Nagios State Types?**

**Answer :**

* 1. The status of service or host i.e. OK, WARNING, UP, DOWN etc..
  2. The type of state the service or host is in.
  3. There are two types of states SOFT states and HARD states.

1. **Question 9. Explain What Is Soft And Hard States?**

**Answer :**

* 1. 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.
  2. 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.

1. **Question 10. Nagios Says My Machine Is Unreachable, Not Down. What Is The Difference And How It Is Achieved?**

**Answer :**

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.

* 1. A router may be defined as a parent for a server.
  2. Now Nagios checks for server and marks it as down.
  3. It then checks the parent (in our example, the router)
  4. If parent is also down, then server is marked as unreachable.
  5. If Parent is up, the server is marked as really down.

1. **Question 11. What Is State Stalking In Nagios?**

**Answer :**

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.

1. **Question 12. What Is Meant By Saying Nagios Is Object Oriented?**

**Answer :**

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.

1. **Question 13. What Are The Three Main Variables That Affect Recursion And Inheritance In Nagios?**

**Answer :**

**First name the variables and then a small explanation of each of these variables:**

* 1. Name
  2. Use
  3. Register

Now I will give a small explanation for each of these variables.

Name is a placeholder that is used by other objects. Use defines the “parent” object whose properties should be used. Register can have a value of 0 (indicating its only a template) and 1 (an actual object). The register value is never inherited.

1. **Question 14. Explain How Flap Detection Works In Nagios?**

**Answer :**

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:

* 1. 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.
  2. Using the state transitions to determine a percent state change value (a measure of change) for the host or service.
  3. Comparing the percent state change value against low and high flapping thresholds
  4. A host or service is determined to have started flapping when its percent state change first exceeds a high flapping threshold.
  5. A host or service is determined to have stopped flapping when its percent state goes below a low flapping threshold.

1. **Question 15. Explain Main Configuration File Of Nagios And Its Location?**

**Answer :**

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/).

1. **Question 16. How Does Nagios Help With Distributed Monitoring?**

**Answer :**

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.

1. **Question 17. What Is The Difference Between Active And Passive Check In Nagios?**

**Answer :**

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.

**Passive checks are useful for monitoring services that are:**

* 1. Asynchronous in nature and cannot be monitored effectively by polling their status on a regularly scheduled basis.
  2. Located behind a firewall and cannot be checked actively from the monitoring host.
  3. 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.

1. **Question 18. When Does Nagios Check For External Commands?**

**Answer :**

**Nagios check for external commands under the following conditions:**

* 1. At regular intervals specified by the command\_check\_interval option in the main configuration file or,
  2. 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.

1. **Question 19. What Do You Mean By Passive Check In Nagios?**

**Answer :**

Passive checks are initiated and performed by external applications/processes and the Passive check results are submitted to Nagios for processing.

1. **Question 20. Explain The Need For Passive Check?**

**Answer :**

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.

1. **Question 21. What Is Meant By Nagios Backend?(unable To Find A Relevant Explanation)**

**Answer :**

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.

1. **Question 22. What Is Database Is Used By Nagios To Store Collected Status Data?**

**Answer :**

Nagios core will use default RRD database format to store status data

1. **Question 23. What Are The Operating Systems We Can Monitor Using Nagios..?**

**Answer :**

Any Operating System We can monitor using Nagios, OS should support to install Nagios Clinet either SNMP.

1. **Question 24. What Are The Components That Make Up The Ndo Utilities ?**

**Answer :**

**There are four main components that make up the NDO utilities:**

* 1. **NDOMOD Event Broker Module :** The NDO utilities includes a Nagios event broker module (NDOMOD.O) that exports data from the Nagios daemon.Once the module has been loaded by the Nagios daemon, itcan access all of the data and logic present in the running Nagios process.The NDOMOD module has been designed to export configuration data, as well as information about various run time events that occur in the monitoring process, from the Nagios daemon. The module can send this data to a standard file, a Unix domain socket, or a TCP socket.
  2. **LOG2NDO Utility :** The LOG2NDO utility has been designed to allow you to import historical Nagios and NetSaint log files into a database via the NDO2DB daemon (described later). The utility works by sending historical log file data to a standard file, a Unix domain socket, or a TCP socket in a format the NDO2DB daemon understands. The NDO2DB daemon can then be used to process that output and store the historical log file  information in a database.
  3. **FILE2SOCK Utility :**  The FILE2SOCK utility is quite simple. Its reads input from a standard file (or STDIN) and writes all of that data to either a Unix domain socket or TCP socket. The data that is read is not processed in any way before it is sent to the socket.
  4. **NDO2DB Daemon:** The NDO2DB utility is designed to take the data output from the NDOMOD and LOG2NDO components and store it in a MySQL or PostgreSQL database.When it starts, the NDO2DB daemon creates either a TCP or Unix domain socket and waits for clients to connect. NDO2DB can run either as a standalone, multi-process daemon or under INETD (if using a TCP socket). Multiple clients can connect to the NDO2DB daemon’s socket and transmit data simultaneously. A separate NDO2DB process is spawned to handle each new client that connects. Data is read from each client and stored in a user-specified database for later retrieval and processing.

1. **Question 25. What Is Ndoutils ?**

**Answer :**

The NDOUTILS addon is designed to store all configuration and event data from Nagios in a database. Storing information from Nagios in a database will allow for quicker retrieval and processing of that data and will help serve as a foundation for the development of a new PHP-based web interface in Nagios 4.1.

MySQL databases are currently supported by the addon and PostgreSQL support is in development.

The NDOUTILS addon was designed to work for users who have:

* 1. Single Nagios installations
  2. Multiple standalone or “vanilla” Nagios installations
  3. Multiple Nagios installations in distributed, redundant, and/or failover environments.

Each Nagios process, whether it is a standalone monitoring server or part of a distributed, redundant, or failover monitoring setup, is referred to as an “instance”. In order to maintain the integrity of stored data, each Nagios instance must be labeled with a unique identifier or name.

1. **Question 26. What Is Nrpe?**

**Answer :**

The Nagios Remote Plugin Executor 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.

**The NRPE addon consists of two pieces:**

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

**When Nagios needs to monitor a resource of service from a remote Linux/Unix machine:**

* 1. Nagios will execute the check\_nrpe plugin and tell it what service needs to be checked
  2. The check\_nrpe plugin contacts the NRPE daemon on the remote host over an (optionally) SSL-protected connection
  3. The NRPE daemon runs the appropriate Nagios plugin to check the service or resource
  4. The results from the service check are passed from the NRPE daemon back to the check\_nrpe plugin, which then returns the check results to the Nagios process.

1. **Question 27. Explain Distributed Monitoring ?**

**Answer :**

Nagios can be configured to support distributed monitoring of network services and resources.

When setting up a distributed monitoring environment with Nagios, there are differences in the way the central and distributed servers are configured.

The function of a distributed server is to actively perform checks all the services you define for a “cluster” of hosts. it basically just mean an arbitrary group of hosts on your network. Depending on your network layout, you may have several clusters at one physical location, or each cluster may be separated by a WAN, its own firewall, etc. There is one distributed server that runs Nagios and monitors the services on the hosts in each cluster. A distributed server is usually a bare-bones installation of Nagios. It doesn’t have to have the web interface installed, send out notifications, run event handler scripts, or do anything other than execute service checks if you don’t want it to.

The purpose of the central server is to simply listen for service check results from one or more distributed servers. Even though services are occasionally actively checked from the central server, the active checks are only performed in dire circumstances.

1. **Question 28. Explain How Flap Detection Works In Nagios?**

**Answer :**

Nagios supports optional detection of hosts and services that are “flapping”. Flapping occurs when a service or host changes state too frequently, resulting in a storm of problem and recovery notifications. Flapping can be indicative of configuration problems (i.e. thresholds set too low), troublesome services, or real network problems.

**Whenever Nagios checks the status of a host or service, it will check to see if it has started or stopped flapping. It does this by:**

* 1. Storing the results of the last 21 checks of the host or ser vice
  2. Analyzing the historical check results and determine where state changes/transitions occur
  3. Using the state transitions to determine a percent state change value (a measure of change) for the host or service
  4. Comparing the percent state change value against low and high flapping thresholds
  5. A host or service is determined to have started flapping when its percent state change first exceeds a high flapping threshold.
  6. A host or service is determined to have stopped flapping when its percent state goes below a low flapping threshold (assuming that is was previously flapping).
  7. The historical service check results are examined to determine where state changes/transitions occur. State changes occur when an archived state is different from the archived state that immediately precedes it chronologically. Since we keep the results of the last 21 service checks in the array, there is a possibility of having at most 20 state changes.

The flap detection logic uses the state changes to determine an overall percent state change for the service. This is a measure of volatility/change for the service. Services that never change state will have a 0% state change value, while services that change state each time they’re checked will have 100% state change. Most services will have a percent state change somewhere in between.

1. **Question 29. What Is State Stalking?**

**Answer :**

Stalking is purely 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. As you’ll see, it can be very helpful to you 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. There are a few exceptions to this, but for the most part, that’s the rule.

If you enable stalking for one or more states of a particular host or service, Nagios will log the results of the host or service check if the output from the check differs from the output from the previous check.

1. **Question 30. What Is The Difference Between Nagiosxi And Nagios Core?**

**Answer :**

NagiosXI is a Paid version and Nagios core is a free version.

NagiosXI includes lot of features which we can modify using web interface. Nagios Core default not include all the features we have to implement by installing plugins.

1. **Question 31. How To Generate Performance Graphs?**

**Answer :**

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.

1. **Question 32. How Do I Use Plugin X?**

**Answer :**

 We have to download the plugins from nagios exchange https://exchange.nagios.org/. Then check the nagios plugin by running manually.

Most all plugins will display basic usage information when you execute them using ‘-h’ or ‘–help’ on the command line.

1. **Question 33. What Are Objects?**

**Answer :**

Objects are all the elements that are involved in the monitoring and notification logic.

**Types of objects include:**

* 1. Services  are one of the central objects in the monitoring logic. Services are associated with hosts Attributes of a host (CPU load, disk usage, uptime, etc.)
  2. Service Groups :are groups of one or more services. Service groups can make it easier to (1) view the status of related services in the Nagios web interface and (2) simplify your configuration through the use of object tricks.
  3. Hosts  are one of the central objects in the monitoring logic.Hosts are usually physical devices on your network (servers, workstations, routers, switches, printers, etc).
  4. Host Groups   are groups of one or more hosts. Host groups can make it easier to (1) view the status of related hosts in the Nagios web interface and (2) simplify your configuration through the use of object tricks
  5. Contacts Conact information of  people involved in the notification process
  6. Contact Groups are groups of one or more contacts. Contact groups can make it easier to define all the people who get notified when certain host or service problems occur.
  7. Commands are used to tell Nagios what programs, scripts, etc. it should execute to perform ,Host and service checks and when Notifications should send etc.
  8. Time Periods are are used to control ,When hosts and services can be monitored
  9. Notification Escalations Use for escalating the the notification.

1. **Question 34. How To Verify Nagios Configuration?**

**Answer :**

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.

### **1.What is Nagios and how it Works ?**

**Ans:**  Nagios is an open source System and Network Monitoring application. Nagios runs on a server, usually as a daemon or service. Nagios periodically run plugins to monitor clients, if it found anything warning and critical it will send an alerts via Email OR SMS as per the configuration.

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.

### **2. what are ports numbers Nagios will use to monitor clients..?**

**Ans:** Port numbers are 5666, 5667 and 5668

### **3. Explain Main Configuration file and its location?**

**Ans:**

1. **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
2. **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/
3. **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/

### **4. Nagios administrator is adding 100+ clients in monitoring but he don’t want to add every .cfg file entry in nagios.cfg file he want to enable a directory path. How can he configure directory for all configuration files..?**

**Ans:**He can able to achieve the above scenario by adding the directory path in nagios.cfg file, in line number 54 we have to add below line.

54  cfg\_dir=/usr/local/nagios/etc/objects/monitor

### **5. Explain Nagios files and its location?**

**Ans:**

1. The main configuration file is usually named nagios.cfg and located in the /usr/local/nagios/etc/ directory default.
2. **Object Configuration File :**This directive is used to specify an object configuration file containing object definitions that Nagios should use for monitoring.  
   cfg\_file=/usr/local/nagios/etc/hosts.cfg  
   cfg\_file=/usr/local/nagios/etc/services.cfg  
   cfg\_file=/usr/local/nagios/etc/commands.cfg
3. **Object Configuration Directory :**This directive is used to specify a directory which contains object configuration files that Nagios should use for monitoring.  
   cfg\_dir=/usr/local/nagios/etc/commands  
   cfg\_dir=/usr/local/nagios/etc/services  
   cfg\_dir=/usr/local/nagios/etc/hosts
4. **Object Cache File :**This directive is used to specify a file in which a cached copy of object definitions should be stored.  
   line number 66 object\_cache\_file=/usr/local/nagios/var/objects.cache
5. **Precached Object File:** Line Number 82 precached\_object\_file=/usr/local/nagios/var/objects.precache Default  
   This is used to specify an optional resource file that can contain $USERn$ macro definitions. $USERn$ macros are useful for storing usernames, passwords, and items commonly used in command definitions.
6. **Temp File :**temp\_path=/tmp  
   This is a directory that Nagios can use as scratch space for creating temporary files used during the monitoring process. You should run tmpwatch, or a similiar utility, on this directory occasionally to delete files older than 24 hours.
7. **Status File :**  Line Number 105 status\_file=/usr/local/nagios/var/status.dat  
   This is the file that Nagios uses to store the current status, comment, and downtime information. This file is used by the CGIs so that current monitoring status can be reported via a web interface. The CGIs must have read access to this file in order to function properly. This file is deleted every time Nagios stops and recreated when it starts.
8. **Log Archive Path :**  Line Number 245 log\_archive\_path=/usr/local/nagios/var/archives/  
   This is the directory where Nagios should place log files that have been rotated. This option is ignored if you choose to not use the log rotation functionality.
9. **External Command File :**  command\_file=/usr/local/nagios/var/rw/nagios.cmd  
   This is the file that Nagios will check for external commands to process. The command CGI writes commands to this file. The external command file is implemented as a named pipe (FIFO), which is created when Nagios starts and removed when it shuts down. If the file exists when Nagios starts, the Nagios process will terminate with an error message. Always keep read only permission to submit the commands from authorized users only.
10. **Lock File :**  lock\_file=/tmp/nagios.lock  
    This option specifies the location of the lock file that Nagios should create when it runs as a daemon (when started with the -d command line argument). This file contains the process id (PID) number of the running Nagios process.
11. **State Retention File:**  state\_retention\_file=/usr/local/nagios/var/retention.dat  
    This is the file that Nagios will use for storing status, downtime, and comment information before it shuts down. When Nagios is restarted it will use the information stored in this file for setting the initial states of services and hosts before it starts monitoring anything. In order to make Nagios retain state information between program restarts, you must enable the retain\_state\_information option.
12. **Check Result Path :**    check\_result\_path=/var/spool/nagios/checkresults  
    This options determines which directory Nagios will use to temporarily store host and service check results before they are processed.
13. **Host Performance Data File :**     host\_perfdata\_file=/usr/local/nagios/var/host-perfdata.da  
    This option allows you to specify a file to which host performance data will be written after every host check. Data will be written to the performance file as specified by the host\_perfdata\_file\_template option. Performance data is only written to this file if the process\_performance\_data option is enabled globally and if the process\_perf\_data directive in the host definition is enabled.
14. **Service Performance Data File:**   service\_perfdata\_file=/usr/local/nagios/var/service-perfdata.dat  
    This option allows you to specify a file to which service performance data will be written after every service check. Data will be written to the performance file as specified by the service\_perfdata\_file\_template option. Performance data is only written to this file if the process\_performance\_data option is enabled globally and if the process\_perf\_data directive in the service definition is enabled
15. **Debug File :** debug\_file=/usr/local/nagios/var/nagios.debug  
    This option determines where Nagios should write debugging information. What (if any) information is written is determined by the debug\_level and debug\_verbosity options. You can have Nagios automatically rotate the debug file when it reaches a certain size by using the max\_debug\_file\_size option.

### **6. Explain Host and Service Check Execution Option?**

**Ans:** This option determines whether or not Nagios will execute Host/service checks when it initially (re)starts. If this option is disabled, Nagios will not actively execute any service checks and will remain in a sort of “sleep” mode. This option is most often used when configuring backup monitoring servers or when setting up a distributed monitoring environment.

**Note:** If you have state retention enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the state retention file), unless you disable the use\_retained\_program\_stateoption. If you want to change this option when state retention is active (and the use\_retained\_program\_state is enabled), you’ll have to use the appropriate external command or change it via the web interface.

**Values are as follows:**  
0 = Don’t execute host/service checks  
1 = Execute host/service checks (default)

### **7. Explain active and Passive check in Nagios?**

**Ans:**    Nagios will monitor host and services in tow ways actively and passively.Active checks are the most common method for monitoring hosts and services. The main features of actives checks as as follows:Active checks are initiated by the Nagios process

**A. Active checks:**  
1.Active checks are run on a regularly scheduled basis  
2.Active checks are initiated by the check logic in the Nagios daemon.  
When Nagios needs to check the status of a host or service it will execute a plugin and pass it information about what needs to be checked. The plugin will then check the operational state of the host or service and report the results back to the Nagios daemon. Nagios will process the results of the host or service check and take appropriate action as necessary (e.g. send notifications, run event handlers, etc).  
Active check are executed At regular intervals, as defined by the check\_interval and retry\_interval options in your host and service definitions  
On-demand as needed.Regularly scheduled checks occur at intervals equaling either the check\_interval or the retry\_interval in your host or service definitions, depending on what type of state the host or service is in. If a host or service is in a HARD state, it will be actively checked at intervals equal to the check\_interval option. If it is in a SOFT state, it will be checked at intervals equal to the retry\_interval option.  
On-demand checks are performed whenever Nagios sees a need to obtain the latest status information about a particular host or service. For example, when Nagios is determining the reach ability of a host, it will often perform on-demand checks of parent and child hosts to accurately determine the status of a particular network segment. On-demand checks also occur in the predictive dependency check logic in order to ensure Nagios has the most accurate status information.

**b.Passive checks:**  
They key features of passive checks are as follows:  
1.Passive checks are initiated and performed external applications/processes  
2.Passive check results are submitted to Nagios for processing

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.

**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

Examples of asynchronous services that lend themselves to being monitored passively include SNMP traps and security alerts. You never know how many (if any) traps or alerts you’ll receive in a given time frame, so it’s not feasible to just monitor their status every few minutes.Passive checks are also used when configuring distributed or redundant monitoring installations.

**Here’s how passive checks work in more detail…**

1. An external application checks the status of a host or service.
2. The external application writes the results of the check to the external command file.
3. The next time Nagios reads the external command file it will place the results of all passive checks into a queue for later processing. The same queue that is used for storing results from active checks is also used to store the results from passive checks.
4. Nagios will periodically execute a check result reaper event and scan the check result queue. Each service check result that is found in the queue is processed in the same manner – regardless of whether the check was active or passive. Nagios may send out notifications, log alerts, etc. depending on the check result information.

### **8. How to verify Nagios configuration ..?**

**Ans:**  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.

### **9. What Are Objects?**

**Ans:**    Objects are all the elements that are involved in the monitoring and notification logic.

**Types of objects include:**  
**Services**  are one of the central objects in the monitoring logic. Services are associated with hosts Attributes of a host (CPU load, disk usage, uptime, etc.)  
Service Groups :are groups of one or more services. Service groups can make it easier to (1) view the status of related services in the Nagios web interface and (2) simplify your configuration through the use of object tricks.

**Hosts** are one of the central objects in the monitoring logic.Hosts are usually physical devices on your network (servers, workstations, routers, switches, printers, etc).  
**Host Groups**   are groups of one or more hosts. Host groups can make it easier to (1) view the status of related hosts in the Nagios web interface and (2) simplify your configuration through the use of object tricks  
**Contacts** Conact information of  people involved in the notification process  
**Contact Groups** are groups of one or more contacts. Contact groups can make it easier to define all the people who get notified when certain host or service problems occur.  
**Commands** are used to tell Nagios what programs, scripts, etc. it should execute to perform ,Host and service checks and when Notifications should send etc.  
**Time Periods** are are used to control ,When hosts and services can be monitored  
**Notification Escalations** Use for escalating the the notification

### **10. What Are Plugins?**

**Ans:**    Plugins are compiled executable s 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.  
Nagios will execute a plugin whenever there is a need to check the status of a service or host. The plugin does something (notice the very general term) to perform the check and then simply returns the results to Nagios. Nagios will process the results that it receives from the plugin and take any necessary actions (running event handlers, sending out notifications, etc).

### **11. How Do I Use Plugin X?**

**Ans:**    We have to download the plugins from nagios exchange https://exchange.nagios.org/. Then check the nagios plugin by running manually.  
Most all plugins will display basic usage information when you execute them using ‘-h’ or ‘–help’ on the command line.

### **12. How to generate Performance graphs..?**

**Ans:** 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.

### **13. What is the difference between NagiosXI and Nagios Core ..?**

Ans:  NagiosXI is a Paid version and Nagios core is a free version.

NagiosXI includes lot of features which we can modify using web interface. Nagios Core default not include all the features we have to implement by installing plugins.

### **14. When Does Nagios Check For External Commands?**

**Ans:**     At regular intervals specified by the command\_check\_interval option in the main configuration file  
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.  
External commands that are written to the command file have the following format  
[time] command\_id;command\_arguments  
where time is the time (in time\_t format) that the external application submitted the external command to the command file. The values for the command\_id and command\_arguments arguments will depend on what command is being submitted to Nagios.

### **15. Explain Nagios State Types?**

**Ans:**   The current state of monitored services and hosts is determined by two components:  
The status of the service or host (i.e. OK, WARNING, UP, DOWN, etc.)

Tye type of state the service or host is in  
There are two state types in Nagios – SOFT states and HARD states. These state types are a crucial part of the monitoring logic, as they are used to determine when event handlers are executed and when notifications are initially sent out.

**A.Soft States:**  
When a service or host check results in a non-OK or non-UP state and the service check has not yet been (re)checked the number of times specified by the max\_check\_attempts directive in the service or host definition. This is called a soft error.  
When a service or host recovers from a soft error. This is considered a soft recovery.  
The following things occur when hosts or services experience SOFT state changes:  
The SOFT state is logged. Event handlers are executed to handle the SOFT state. SOFT states are only logged if you enabled the log\_service\_retries or log\_host\_retries options in your main configuration file.  
The only important thing that really happens during a soft state is the execution of event handlers. Using event handlers can be particularly useful if you want to try and proactively fix a problem before it turns into a HARD state. The $HOSTSTATETYPE$ or $SERVICESTATETYPE$ macros will have a value of “SOFT” when event handlers are executed, which allows your event handler scripts to know when they should take corrective action.

**B.Hard states :**

* occur for hosts and services in the following situations:
* When a host or service check results in a non-UP or non-OK state and it has been (re)checked the number of times specified by the max\_check\_attempts
* option in the host or service definition. This is a hard error state.
* When a host or service transitions from one hard error state to another error state (e.g. WARNING to CRITICAL).
* When a service check results in a non-OK state and its corresponding host is either DOWN or UNREACHABLE.
* When a host or service recovers from a hard error state. This is considered to be a hard recovery.
* When a passive host check is received. Passive host checks are treated as HARD unless the passive\_host\_checks\_are\_soft option is enabled.

The following things occur when hosts or services experience HARD state changes:  
The HARD state is logged.  
Event handlers are executed to handle the HARD state.  
Contacts are notifified of the host or service problem or recovery.  
The $HOSTSTATETYPE$ or $SERVICESTATETYPE$ macros will have a value of “HARD” when event handlers are executed, which allows your event handler scripts to know when they should take corrective action.

### **16. What is State Stalking?**

**Ans:**    Stalking is purely 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. As you’ll see, it can be very helpful to you 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. There are a few exceptions to this, but for the most part, that’s the rule.  
If you enable stalking for one or more states of a particular host or service, Nagios will log the results of the host or service check if the output from the check differs from the output from the previous check.

### **17. Explain how  Flap Detection works in Nagios?**

**Ans:**  Nagios supports optional detection of hosts and services that are “flapping”. Flapping occurs when a service or host changes state too frequently, resulting in a storm of problem and recovery notifications. Flapping can be indicative of configuration problems (i.e. thresholds set too low), troublesome services, or real network problems.

Whenever Nagios checks the status of a host or service, it will check to see if it has started or stopped flapping. It does this by:

1. Storing the results of the last 21 checks of the host or ser vice
2. Analyzing the historical check results and determine where state changes/transitions occur
3. Using the state transitions to determine a percent state change value (a measure of change) for the host or service
4. Comparing the percent state change value against low and high flapping thresholds
5. A host or service is determined to have started flapping when its percent state change first exceeds a high flapping threshold.
6. A host or service is determined to have stopped flapping when its percent state goes below a low flapping threshold (assuming that is was previously flapping).
7. The historical service check results are examined to determine where state changes/transitions occur. State changes occur when an archived state is different from the archived state that immediately precedes it chronologically. Since we keep the results of the last 21 service checks in the array, there is a possibility of having at most 20 state changes. In this example there are 7 state changes, indicated by blue arrows in the image above.

The flap detection logic uses the state changes to determine an overall percent state change for the service. This is a measure of volatility/change for the service. Services that never change state will have a 0% state change value, while services that change state each time they’re checked will have 100% state change. Most services will have a percent state change somewhere in between.

### **18. Explain Distributed Monitoring ?**

**Ans:**   Nagios can be configured to support distributed monitoring of network services and resources.  
When setting up a distributed monitoring environment with Nagios, there are differences in the way the central and distributed servers are configured.  
The function of a distributed server is to actively perform checks all the services you define for a “cluster” of hosts. it basically just mean an arbitrary group of hosts on your network. Depending on your network layout, you may have several clusters at one physical location, or each cluster may be separated by a WAN, its own firewall, etc. There is one distributed server that runs Nagios and monitors the services on the hosts in each cluster. A distributed server is usually a bare-bones installation of Nagios. It doesn’t have to have the web interface installed, send out notifications, run event handler scripts, or do anything other than execute service checks if you don’t want it to.  
The purpose of the central server is to simply listen for service check results from one or more distributed servers. Even though services are occasionally actively checked from the central server, the active checks are only performed in dire circumstances,

### **19. What is NRPE?**

**Ans:**  The Nagios Remote Plugin Executor 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.

**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

**When Nagios needs to monitor a resource of service from a remote Linux/Unix machine:**  
– Nagios will execute the check\_nrpe plugin and tell it what service needs to be checked  
– The check\_nrpe plugin contacts the NRPE daemon on the remote host over an (optionally) SSL-protected connection  
– The NRPE daemon runs the appropriate Nagios plugin to check the service or resource  
– The results from the service check are passed from the NRPE daemon back to the check\_nrpe plugin, which  
then returns the check results to the Nagios process.

### **20.What is NDOUTILS ?**

**Ans:**  The NDOUTILS addon is designed to store all configuration and event data from Nagios in a database. Storing information from Nagios in a database will allow for quicker retrieval and processing of that data and will help serve as a foundation for the development of a new PHP-based web interface in Nagios 4.1.  
MySQL databases are currently supported by the addon and PostgreSQL support is in development.

**The NDOUTILS addon was designed to work for users who have:**  
– Single Nagios installations  
– Multiple standalone or “vanilla” Nagios installations  
– Multiple Nagios installations in distributed, redundant, and/or failover environments.

Each Nagios process, whether it is a standalone monitoring server or part of a distributed, redundant, or failover monitoring setup, is referred to as an “instance”. In order to maintain the integrity of stored data, each Nagios instance must be labeled with a unique identifier or name.

### **21. What are the components that make up the NDO utilities ?**

**Ans:**

**There are four main components that make up the NDO utilities:**

1. **NDOMOD Event Broker Module :**The NDO utilities includes a Nagios event broker module (NDOMOD.O) that exports data from the Nagios daemon.Once the module has been loaded by the Nagios daemon, itcan access all of the data and logic present in the running Nagios process.The NDOMOD module has been designed to export configuration data, as well as information about various run time events that occur in the monitoring process, from the Nagios daemon. The module can send this data to a standard file, a Unix domain socket, or a TCP socket.
2. **LOG2NDO Utility :**The LOG2NDO utility has been designed to allow you to import historical Nagios and NetSaint log files into a database via the NDO2DB daemon (described later). The utility works by sending historical log file data to a standard file, a Unix domain socket, or a TCP socket in a format the NDO2DB daemon understands. The NDO2DB daemon can then be used to process that output and store the historical log file  information in a database.
3. **FILE2SOCK Utility :**  The FILE2SOCK utility is quite simple. Its reads input from a standard file (or STDIN) and writes all of that data to either a Unix domain socket or TCP socket. The data that is read is not processed in any way before it is sent to the socket.
4. **NDO2DB Daemon:**   The NDO2DB utility is designed to take the data output from the NDOMOD and LOG2NDO components and store it in a MySQL or PostgreSQL database.When it starts, the NDO2DB daemon creates either a TCP or Unix domain socket and waits for clients to connect. NDO2DB can run either as a standalone, multi-process daemon or under INETD (if using a TCP socket). Multiple clients can connect to the NDO2DB daemon’s socket and transmit data simultaneously. A separate NDO2DB process is spawned to handle each new client that connects. Data is read from each client and stored in a user-specified database for later retrieval and processing.

### **22. What are the Operating Systems we can monitor using Nagios..?**

**Ans:**  Any Operating System We can monitor using Nagios, OS should support to install Nagios Clinet either SNMP.

### **23. What is database is used by Nagios to store collected status data..?**

**Ans:** Nagios core will use default RRD database format to store status data

#### **Q1). Explain Nagios or what is Nagios, explain it.**

Nagios is a monitoring tool that is used for continuous monitoring of system services, applications, and business processes. Even in case of any failure, Nagios tool can alert the technical staff about the problem. As a result, DevOps professionals or technical team members can begin the required remediation processes before the negative impact of any business processes, customers, and end-users. Here, in such cases, the team does not have to explain anyone that why an unseen infrastructure outage affects the bottom line of the organization.

Now as you know ‘what is Nagios?’ then you can also mention the things that can be achieved by the Nagios DevOps tool:

* Automatic problem fixing as and when they occur.
* Infrastructure upgrades planning even before any failure due to an outdated system.
* Technical team response coordination.
* To ensure that SLA of your organization will be met.
* To monitor the business process and the entire infrastructure.
* To respond to issues even as and when they arise.

**[Read:   What is Chef? Chef Tutorial Guide for Beginner](https://www.janbasktraining.in/blog/chef-tutorial/" \t "_blank)**

Above-mentioned are all major factors that make Nagios a complete tool for continuous monitoring. (Here in such question you can also add some advantages of Nagios if time permits.)

#### **Q2). Explain the working of Nagios, how does it work?**

On a server, Nagios either runs as a service or daemon. Plugins that resides on the same server are being run by the Nagios; basically, they contact the hosts or servers of your network or on the internet. We can check the status by web interface; even notifications can also be received by email or SMS when something happens.

Nagios service runs certain scripts after a fix time interval, so it acts as a scheduler. It can store the script result and run other scripts when it is changed.

#### **Q3). Explain Nagios plugins.**

Plugins are basically scripts of Perl and Shell that can be run through the command line to check the service status of the host. Nagios can also use the result of the plugins that determine the present status of host or services of the network.

Now an answer to the questions that why we need plugins, you can also add here that, plugins is executed by Nagios to check the status of any service or host. A check is performed by the plugin and the result is returned to Nagios. The result is processed by Nagios to take the necessary actions.

#### **Q4). What do you understand by NRPE or Nagios Remote Plugin Executor of Nagios?**

NRPE or Nagios remote plugin executor is designed to allow execution of plugins on remote Linux or UNIX based machines. These plugins are executed to monitor the usage of CPU load and memory usage like a local resource of remote machines. It is required as this information is not usually exposed publicly to an external machine and for this purpose, NRPE agent is installed on remote machines.

NRPE add-on or plugin has two components that work together to perform the task:

* A ‘check\_nrpe’ plugin that resides on the local machine and it is used for monitoring
* The NRPE daemon that can run on remote machines

#### **Q5). What are port numbers used by Nagios for monitoring purpose?**

Usually, the port number 5666, 5667 and 5668 are used for monitoring in Nagios DevOps tool.

#### **Q6). Explain main configuration file and its location.**

Following is the description of the main configuration file:

**Resource File:** To store sensitive information like user details that may include username and passwords it is used. The information is not made available to CGI.

**[Read:   DevOps Interview Questions & Answers for Fresher & Experienced](https://www.janbasktraining.in/blog/top-devops-interview-questions-and-answers/" \t "_blank)**

**Object Definition File:**  In this file, you can find and enlist the details of resources that you want to monitor and how you want the monitoring to be performed? Host services, host groups, contacts, contact groups, commands, etc. are defined in this file.

**CGI Configuration File:** Several directives are contained and stored in CGI file that can affect the CGI o. A reference to the main configuration file is also stored in this file, so that CGI can know the details of Nagios configuration as and when required and the location of object definition storage.

#### **Q7). What are state types of Nagios?**

Following are the state types of Nagios:

* Service or host state type
* Some states like OK, WARNING, UP, or DOWN state host or service
* Two state types that are SOFT state or HARD state

#### **Q8). What are SOFT and HARD states?**

We can define soft and hard states as:

* In case of the SOFT state, the service or host check results are not OK or not up to the mark, even in case if service check has not been rechecked the number of times that are specified for it moreover the times that is being specified by the max\_check\_attempts directive. Recovery of the component from such Soft error is called Soft Recovery.
* When a host or service check result is not ‘OK’ and it has been checked for the number of times, specified by the max\_check\_attempts directive in the host definition, then this error is known as Hard Error. Recovery of any service from this error is known as Hard Recovery.

#### **Q9). What is state stalking in Nagios?**

State stalking is used for logging purpose in Nagios. When stalking is enabled for any service or host then Nagios watch it very carefully and store any changes that if found in the check result of that resource.

Stalking can be helpful in later stages of log file analysis. Here in such scenario, any host or service check can be performed only if it has been updated for the last time.

#### **Q10). Why is it being said that Nagios is object oriented?**

Nagios has object configuration format where you can create object definitions, that can inherit the properties from other hostnames or object definitions. In this way, you can specify the component relationships easily. The components are considered as objects by the Nagios.

**[Read:   How to Become a DevOps Engineer](https://www.janbasktraining.in/blog/become-a-devops-engineer/" \t "_blank)**

#### **Q11). Which three Nagios variables can affect recursion and inheritance in Nagios?**

The three variables that affect recursion and inheritance are:

* Name
* Use
* Register

Here, Name is just a placeholder that can be used by the other objects. Use variable can be used to define parent object, whose properties are to be used. Registers are also used for storing values that can be either 0 or 1. Register values cannot be inherited.

#### **Q12). How Does Flap detection work in Nagios?**

When a service or host changes their state frequently, then it is called flapping that may cause lots of problems and generate too many recovery notifications. Flapping is detected in the following manner:

* Store the results of last 21 checks and then analyze this historical check result to know the number of transitions that are being taken place by the host or service.
* Know the percent state change value with the help of state transition
* Compare the value of this state change against low and high flapping thresholds
* When this value exceeds then the highest specified threshold then it is called flapping
* When this percent state value goes down the specified value then it is said that flapping has been stopped.

#### **Q13). Explain main configuration file of Nagios.**

Several directives are contained in the main configuration file that can affect Nagios daemon. This file is read by both CGIs and Nagios daemons.

A Nagios file is usually created in the base Nagios directory, at the time when you run configuration script. The name of this file that is the main configuration file is ‘nagios.cfg’ and is usually placed in etc/subdirectory

#### **Q14). How is distributed monitoring being done in Nagios?**

There is a distributed monitoring scheme in Nagios with the help of which you can monitor your complete enterprise that may include local slave instances. In such environment, Nagios submit the result of reports of tasks to a single machine. All configuration, reporting, and notification can be managed at the master machine and here slaves do all the work. Here Nagios uses passive checks that are basically external applications that can send the results back to Nagios.

#### **Q15). Differentiate between active and passive check.**

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

**Q1. Why is Continuous monitoring necessary?**

I will suggest you to go with the below mentioned flow:  
Continuous Monitoring allows timely identification of problems or weaknesses and quick corrective action that helps reduce expenses of an organization. Continuous monitoring provides solution that addresses three operational disciplines known as:

* continuous audit
* continuous controls monitoring
* continuous transaction inspection

**Q2. What is Nagios?**

You can answer this question by first mentioning that Nagios is one of the monitoring tools. It is used for Continuous monitoring of systems, applications, services, and business processes etc in a DevOps culture. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers. With Nagios, you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line.  
Now once you have defined what is Nagios, you can mention the various things that you can achieve using Nagios.  
By using Nagios you can:

* 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.

This completes the answer to this question. Further details like advantages etc. can be added as per the direction where the discussion is headed.

**Q3. How does Nagios works?**

I will advise you to follow the below explanation for this answer:  
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.

Now expect a few questions on Nagios components like Plugins, NRPE etc..

**Q4. What are Plugins in Nagios?**

Begin this answer by defining Plugins. They 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 Plugins to determine the current status of hosts and services on your network.  
Once you have defined Plugins, explain why we need Plugins. Nagios will execute a Plugin whenever there is a need to check the status of a host or service. 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.

**Q5. What is NRPE (Nagios Remote Plugin Executor) in Nagios?**

For this answer, give a brief definition of Plugins. 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.

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.

**Q6. What do you mean by passive check in Nagios?**

According to me, the answer should start by explaining Passive checks. They are initiated and performed by external applications/processes and the Passive check results are submitted to Nagios for processing.  
Then explain the need for passive checks. They are useful for monitoring services that are Asynchronous in nature and cannot be monitored effectively by polling their status on a regularly scheduled basis. They can also be used for monitoring services that are Located behind a firewall and cannot be checked actively from the monitoring host.

**Q7.** **When Does Nagios Check for external commands?**

Make sure that you stick to the question during your explanation so I will advise you to follow the below mentioned flow. 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.

**Q8. What is the difference between Active and Passive check in Nagios?**

For this answer, first point out the basic difference Active and Passive checks. 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 you can 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.

**Q9. How does Nagios help with Distributed Monitoring?**

The interviewer will be expecting an answer related to the distributed architecture of Nagios. So, I suggest that you answer it in the below mentioned format:  
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.

**Q10. Explain Main Configuration file of Nagios and its location?**

First mention what this main configuration file contains and its function. 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/).

**Q11. Explain how Flap Detection works in Nagios?**

I will advise you to first explain Flapping first. 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 follows the below given 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.

**Q12. What are the three main variables that affect recursion and inheritance in Nagios?**

According to me the proper format for this answer should be:  
First name the variables and then a small explanation of each of these variables:

* Name
* Use
* Register

Then give a brief explanation for each of these variables. Name is a placeholder that is used by other objects. Use defines the “parent” object whose properties should be used. Register can have a value of 0 (indicating its only a template) and 1 (an actual object). The register value is never inherited.

**Q13. What is meant by saying Nagios is Object Oriented?**

Answer to this question is pretty direct. I will answer this by saying, “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.”

**Q14. What is State Stalking in Nagios?**

I will advise you to first give a small introduction on State Stalking. It 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.”

1. While defining a host in nagios

Action\_url

Notification\_enabled

2)which of the following version of snmp provides community based security

Snmp v2u

Snmpv3

3)which of the following options are the valid directives that can be used to define a host?

Parents

Hostgroups

Event\_handler\_enabled

4)In relation to monitoring hosts using ssh, which

All 1,2,3

5) with regard to host dependency definition, which of the following values of the notification\_failure\_creteira directive represents the criteria, “ fail on an UP state?

Answer: o

6)diagram : uparrow

It is used to add a dashlet to any dashboard