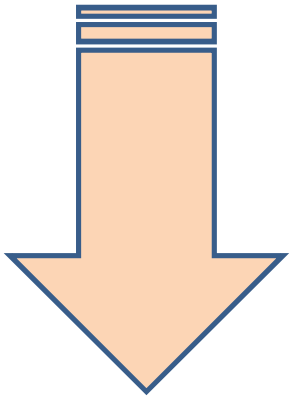
DEVOPS

DevOps



UNIT-4: Configuration Management & Continuous Monitoring:

Configuration Management with Puppet,

Configuration Management with Ansible,

Continuous Monitoring with Nagios.

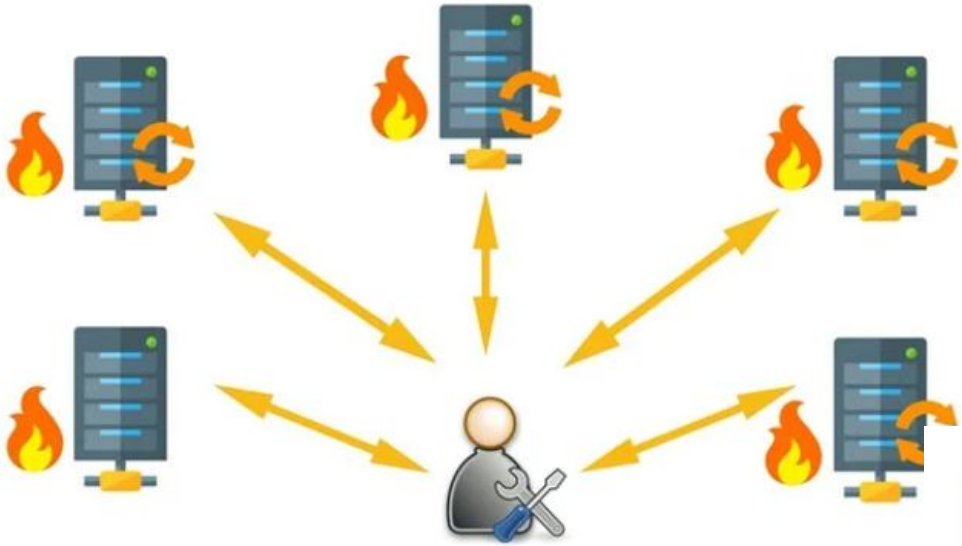
Configuration Management using Puppet

- Configuration management is the process of maintaining software and computer systems (for example servers, storage, networks) in a known, desired and consistent state.
- Puppet is a configuration management technology to manage the infrastructure on physical or virtual machines.
- Puppet is a popular open-source configuration management tool that allows IT administrators and DevOps engineers to automate the management of infrastructure configurations.
- It is an open-source software configuration management tool developed using Ruby which helps in managing complex infrastructure on the fly.
- System Administrators mostly perform repetitive tasks like installing servers, configuring those servers, etc. These professionals can automate this task, by writing scripts.
- Puppet is also used as a software deployment tool. It is an open-source configuration management software widely **used for server configuration**, **management, deployment, and orchestration of various applications and services** across the whole infrastructure of an organization.
- Puppet is **written in Ruby** and **uses its unique Domain Specific Language (DSL)** to describe system configuration.

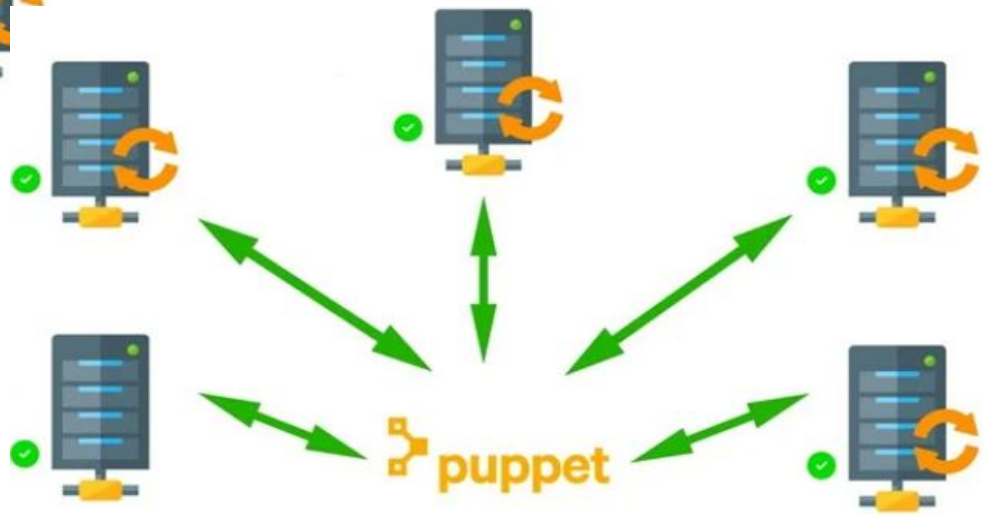
Puppet 2 versions: Open source Puppet & Puppet Enterprise

What Puppet can do?

For example, you have an infrastructure with about 100 servers. As a system admin, it's your role to ensure that all these servers are always up to date and running with full functionality.



System Admin working manually on the servers



Puppet automates Server Management

- you can use Puppet, which allows you to write a simple code which can be deployed automatically on these servers. This reduces the human effort and makes the development process fast and effective.

Puppet functions

- Puppet allows you to define distinct configurations for every host.
- The tool allows you to continuously monitor servers to confirm whether the required configuration exists or not and it is not altered. If the config is changed, Puppet tool will revert to the pre-defined configuration on the host.
- It also provides control over all the configured system, so a centralized change gets automatically effected.
- It is also used as a deployment tool as it automatically deploys software to the system. It implements the **infrastructure as a code because policies and configurations are written as code.**
- Puppet uses declarative programming model (tells logic 'what todo' not 'how to do' : example sql)

Deployment models of configuration management tools:

There are two deployment models for configuration management tools :

- Push-based deployment model: initiated by a master node.
- Pull-based deployment model: initiated by agents.

How Puppet Works?

- Puppet is based on a Pull deployment model, where the agent nodes check in regularly after every **1800** seconds with the master node to see if anything needs to be updated in the agent. If anything needs to be updated the agent pulls the necessary puppet codes from the master and performs required actions.

The Master

- A Linux based machine with Puppet master software installed on it. It is responsible for maintaining configurations in the form of puppet codes. The master node can only be Linux.

The Agents

- The target machines managed by a puppet with the puppet agent software installed on them.
- The agent can be configured on any supported operating system such as Linux or Windows or Solaris or Mac OS.
- The communication between master and agent is established through secure certificates.

How Puppet Works?

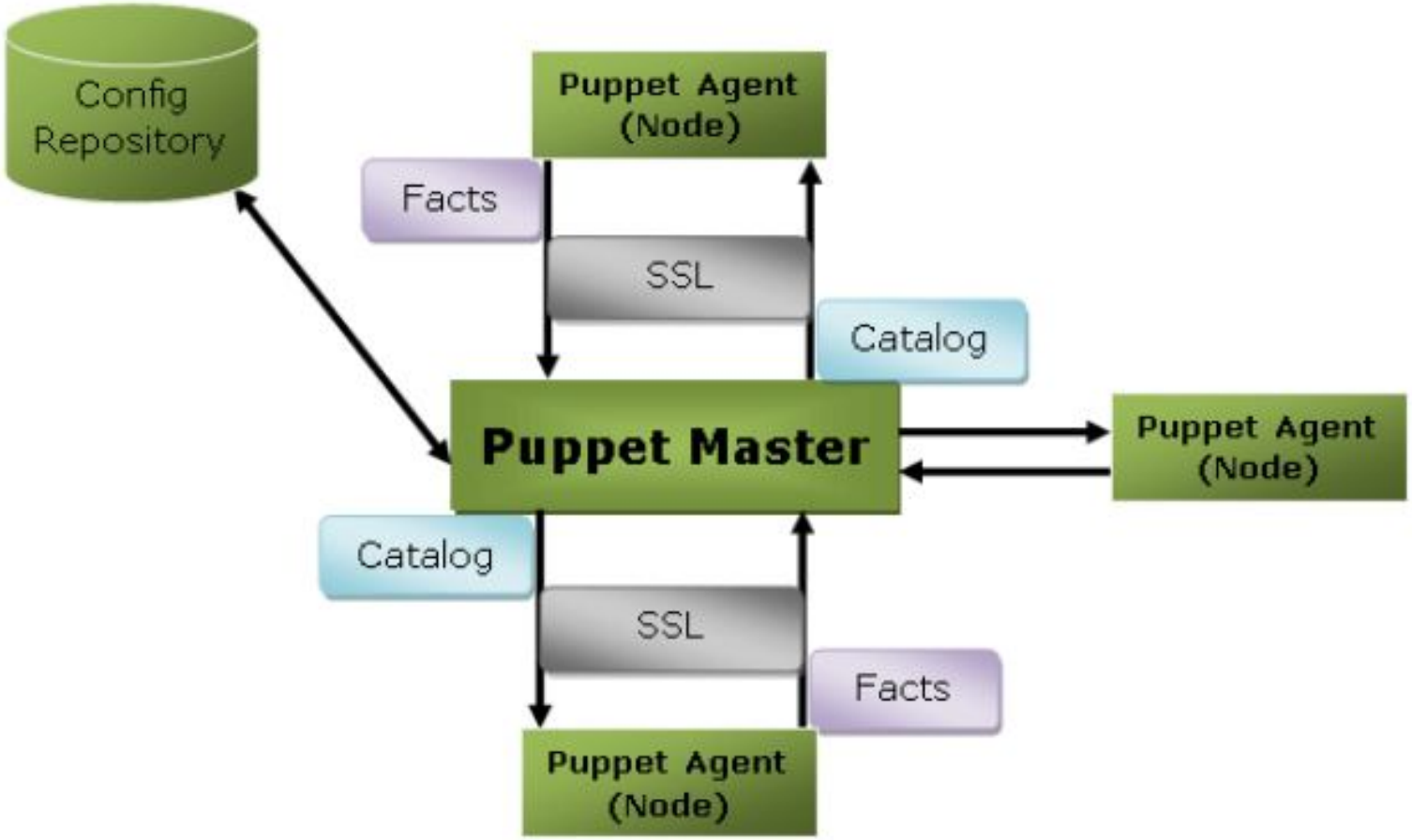
Puppet Master Agent Communication

How Puppet Works?

Communication between the Master and the Agent:

Puppet Architecture

The following is the Puppet Architecture diagram:



Puppet uses master-slave or client-server architecture. Puppet client and server interconnected by SSL, which is a secure socket layer.

Here, the client is referred to as a Puppet agent/slave/node, and the server is referred to as a Puppet master.

Puppet Architecture

- Let's see the components of Puppet architecture:

Puppet Master

- Puppet master handles all the configuration related process in the form of puppet codes. It is a Linux based system in which puppet master software is installed. The puppet master must be in Linux. It uses the puppet agent to apply the configuration to nodes.
- This is the place where SSL certificates are checked and marked.

Puppet Slave or Agent

- Puppet agents are the real working systems and used by the Client. It is installed on the client machine and maintained and managed by the puppet master. They have a puppet agent service running inside them.
- The agent machine can be configured on any operating system such as Windows, Linux, Solaris, or Mac OS.

Config Repository

- Config repository is the storage area where all the servers and nodes related configurations are stored, and we can pull these configurations as per requirements.

AWS OpsWorks

- ✓AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.
- ✓Chef and Puppet are automation platforms that allow you to use code to automate the configurations of your servers. OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.
- ✓OpsWorks has three offerings, AWS Opsworks for Chef Automate, AWS OpsWorks for Puppet Enterprise, and AWS OpsWorks Stacks.

Continuous Monitoring using Nagios

Continuous Monitoring using Nagios

Continuous monitoring is the process and technology used to detect compliance and risk issues associated with an organization's financial and operational environment. The financial and operational environment consists of people, processes, and systems working together to support efficient and effective operations

Nagios 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.

Continuous Monitoring

- It detects any network or server problems
- It determines the root cause of any issues
- It maintains the security and availability of the service
- It monitors and troubleshoot server performance issues
- It can respond to issues at the first sign of a problem
- Monitors your entire infrastructure and business processes

Continuous Monitoring Tools

Continuous Monitoring Tools

Why we need Continuous Monitoring?

- Continuous Monitoring Tools resolve any system errors (low memory, unreachable server etc.) before they have any negative impact on your business productivity.

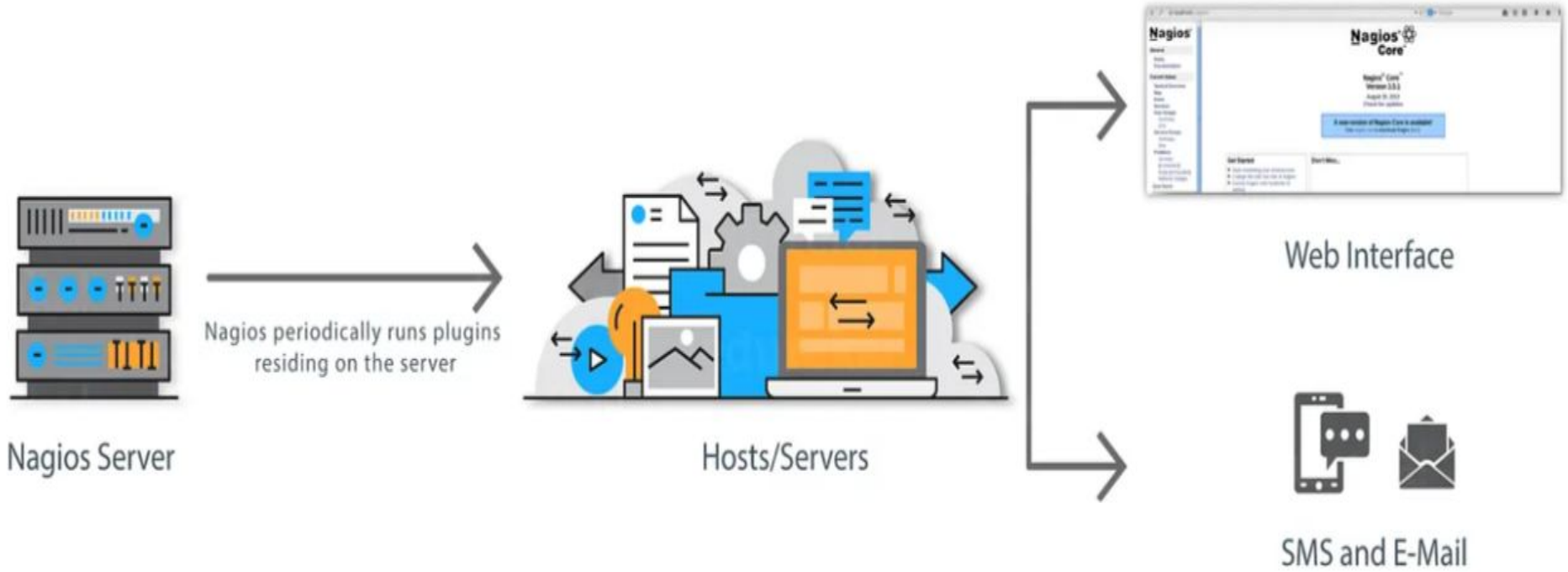
Important reasons to use a monitoring tool are:

- It detects any network or server problems
- It determines the root cause of any issues
- It maintains the security and availability of the service
- It monitors and troubleshoots server performance issues
- It allows us to plan for infrastructure upgrades before outdated systems cause failures
- It can respond to issues at the first sign of a problem
- It can be used to automatically fix problems when they are detected
- It ensures IT infrastructure outages (temporary out of service) have a minimal effect on your organization's bottom line
- It can monitor your entire infrastructure and business processes

Continuous Monitoring

- Continuous Monitoring comes into the picture, once the application is deployed on the production servers.
- Continuous Monitoring is all about the ability of an organization to detect, report, respond, contain and mitigate the attacks that occur, in its infrastructure.
- Continuous Monitoring is actually not new, it's been around for some time. For years our security professionals are performing static analysis from — system log, firewall logs, IDS logs, IPS logs (Intrusion detection systems (IDS) and intrusion prevention systems (IPS)) etc. But, it did not provide proper analysis and response. Today's Continuous Monitoring approach gives us the ability to aggregate all of the events that I discussed above, co-relate them, compare them and then estimate the organization's risk posture.

Nagios – How it works?

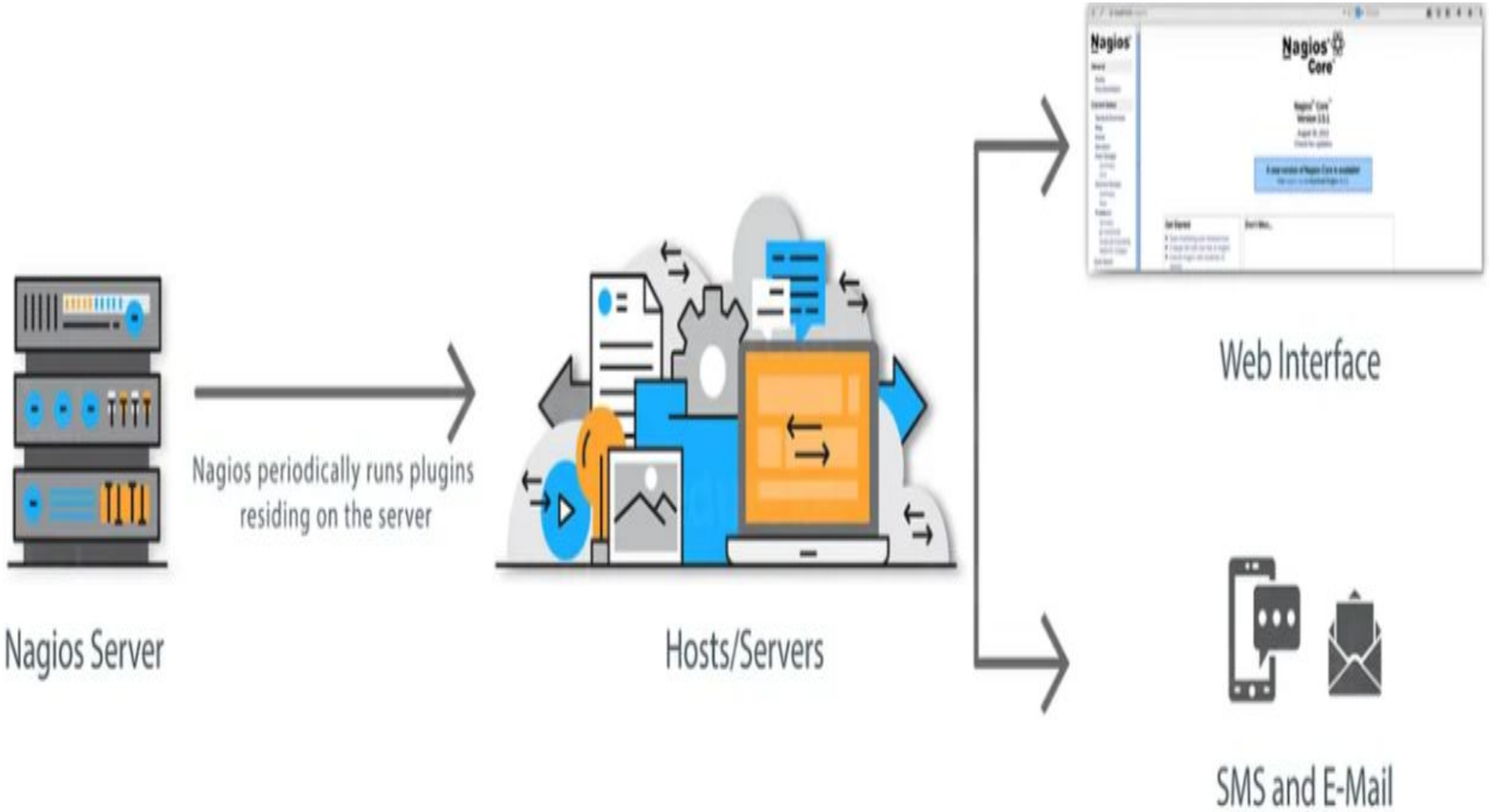


Continuous Monitoring - Nagios

Nagios runs on a server, usually as a daemon or a service.

- It 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.
- **Plugins:** These 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 the plugins to determine the current status of the hosts and services on your network.

Nagios – working



Nagios - working

- Nagios runs on a server, usually as a daemon or a service.
- It 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.
- **Plugins:** These 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 the plugins to determine the current status of the hosts and services on your network.

Nagios - Architecture

- Nagios Tutorial - Know How To Perform Continuous Monitoring With Nagios | by Saurabh Kulshrestha | Edureka | Medium

https://medium.com/edureka/nagios-tutorial-e63e2a744cc8

Nagios Tutorial: What is Nagios Tool? Architecture & Installation (guru99.com)

https://www.guru99.com/nagios-tutorial.html

How To Create A Nagios XI Instance In The Amazon EC2 Cloud

https://assets.nagios.com/downloads/nagiosxi/docs/Using-Nagios-XI-In-Amazon-EC2-Cloud.pdf

Creating a Nagios XI Instance in the Amazon EC2 Cloud

https://answerhub.nagios.com/support/s/article/Creating-a-Nagios-XI-Instance-in-the-Amazon-EC2-Cloud-7776e52a

Nagios - working

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-

Continuous Monitoring

-