DevOps Certification Training

Continuous Monitoring

Learning Objectives

By the end of this lesson, you will be able to:

- Explain continuous monitoring tools in DevOps
- Demonstrate Nagios
- Describe ELK Stack
- Demonstrate continuous monitoring on Docker with ELK Stack

TECHNOLOGY

Introduction to Continuous Monitoring

What Is Continuous Monitoring ?

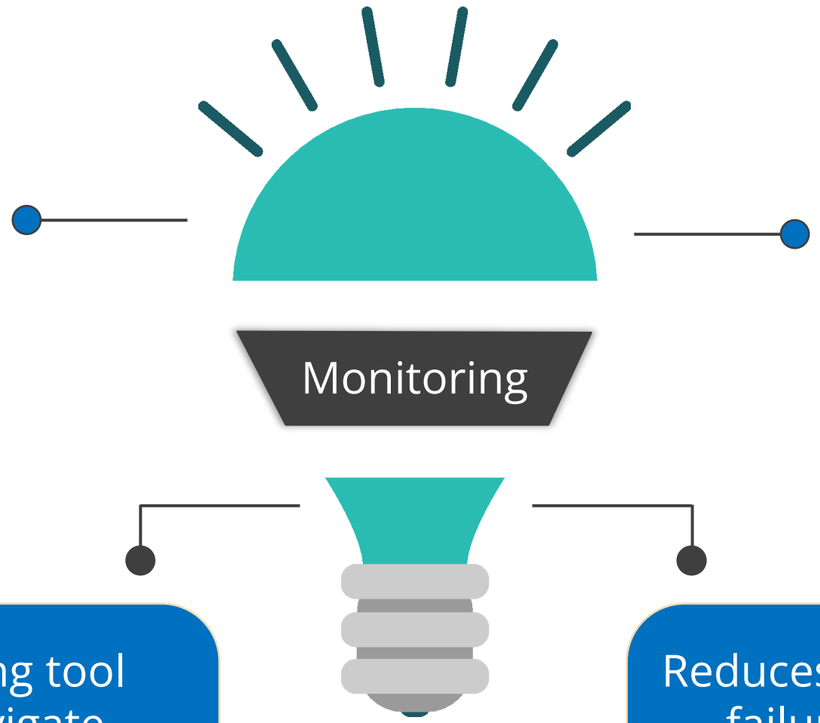
Continuous monitoring involves monitoring and identifying compliance issues and security risks in each phase of the DevOps lifecycle.

It is the ability to:

- Detects
- Reports
- Responds
- Contains
- Mitigates attacks to the IT infrastructure

What Is Continuous Monitoring ?

Helps Detect risk, compliance, and security issues in an operational environment

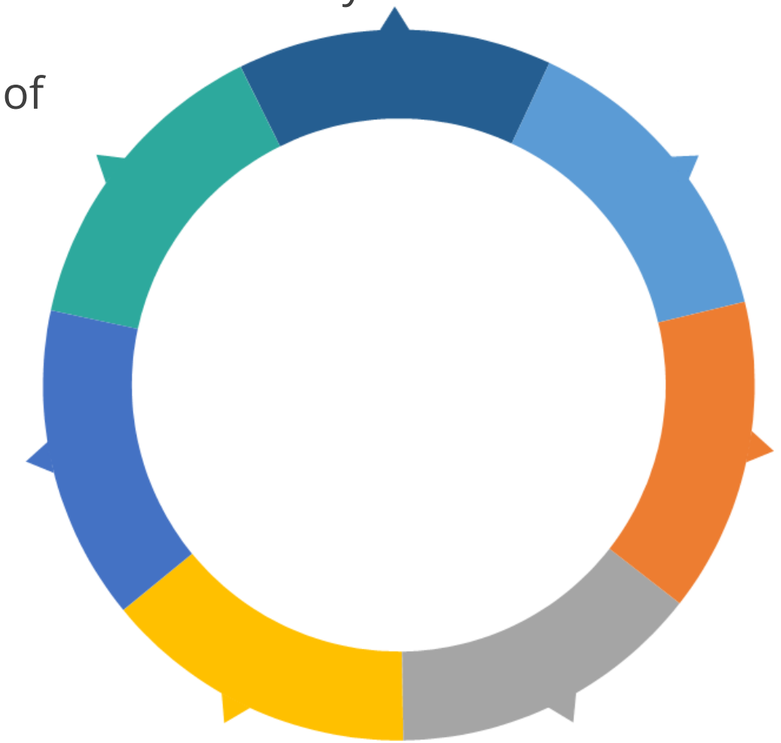


Takes precautions to maintain a stable operational environment

Acts as an auditing tool where it can navigate through old monitoring data to analyze and improve performance of system

Reduces the probability of failure and provides assurance to business with regard to security and reliability

Role of Monitoring Systems



Helps to design and sustain a stable and reliable system

Reduces cost by accumulating detailed knowledge on duplication of software assets

Alerts any issue in infrastructure or application service

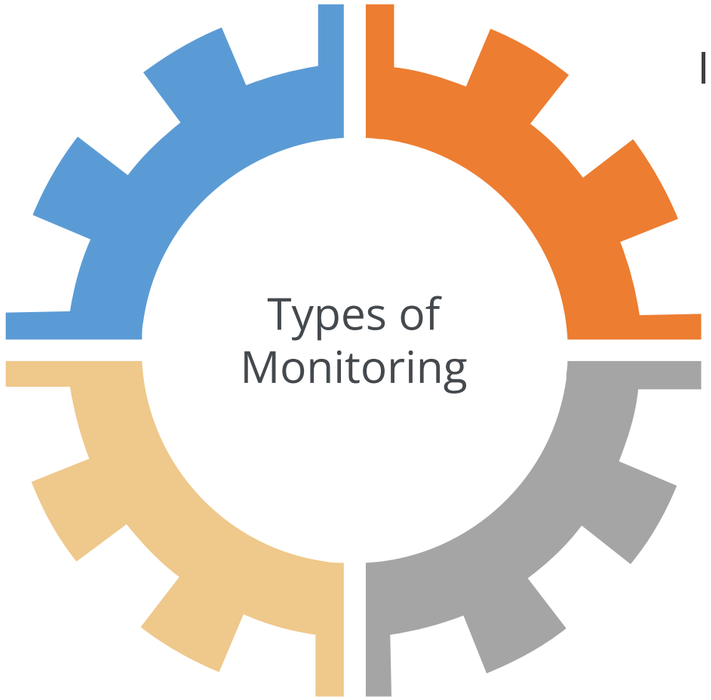
Monitors the production environment for risks and failures

Retrieves historical data for analysis

Displays application behavior during peak business hours

Reduces the risk of application downtime

Types of Monitoring Systems



Types of Monitoring Systems

Real-time Monitoring

Deals with Monitoring of:

- Server CPU statistics
- Disk usage and memory stats
- Spikes in CPU performance
- I/O count on server

Infrastructure Monitoring

Deals with Monitoring of:

- CPU and memory
- Network and routers
- App servers, web servers, and DB servers
- Data-centers, storage
- IT hardware, software

Types of Monitoring

Network Monitoring

Deals with Monitoring of:

- Network
- Routers, firewalls
- Switches, servers
- Virtual machines

Application Monitoring

Deals with Monitoring of:

- API success/failure
- count
- API accessibility
- API HTTP error codes

Continuous Monitoring Tools

Some of the most popular tools used for continuous monitoring are:

Continuous Monitoring Tools

- Nagios Core is a free, open-source, network monitoring application.
- It was launched in 2002 and is one of the popular monitoring tools.
- It can monitor applications, networks, routers, switches, and servers.
- It needs Nagios NRPE agents to be deployed on respective servers to collect stats from node machines.

Continuous Monitoring Tools

- ELK Stack is a log monitoring and open-source tool.
- It is a combination of three open-source tools: Elasticsearch, Logstash, and Kibana.
- Elasticsearch is the heart of the stack as it acts as the data engine, stores applications, server logs, and retrieves the data for analysis.
- Logstash acts as data pipeline which processes logs and helps in saving the data to Elasticsearch.
- Kibana is a front-end application used to visualize and display the data retrieved from the data engine.

Continuous Monitoring Tools

- Zabbix is open-source tool launched in 2001 that provides features similar to Nagios.
- It needs agents to be installed on the nodes in order to monitor the data.

- Sensu is a powerful next-generation monitoring tool which is more popular than traditional monitoring tools.
- It was launched in 2011 as open-source under MIT license.
- Sensu enterprise version provides additional features and plugins.
- It uses RabbitMQ to exchange data between nodes and the master server.
- It uses Redis as the database to store all the monitoring data.

Continuous Monitoring Tools

- New Relic was launched in 2008 as SAAS(Software A As Service) software offering.
- It helps to monitor applications, and servers in real-time.
- New Relic's collectors installation in the nodes is necessary instead of New Relic software in the infrastructure.
- All monitoring data is transferred to New Relic and its dashboards are used to visualize monitoring data.

Continuous Monitoring Tools

splunk>

- Splunk is interpreted as an application and security analytics tool.
- It collects data from each application and server and can be further analyzed to predict the future behavior for necessary precautions.
- Monitoring application failures and warning exceptions are possible.
- It is implemented in financial and product-based organizations to monitor the applications.

Continuous Monitoring Tools

- Datadog is a cloud-based monitoring service.
- Datadog agent should be installed on the servers to monitor other servers within the infrastructure.
- All monitoring data is pushed to Datadog web application to visualize it.

- AppDynamics tool is used to monitor the server and application performance which results in improved efficiency of the source code.
- It helps in making a suitable business decision while monitoring application, as it monitors both mobile and web.

Continuous Monitoring Tools

- AWS CloudWatch is one of the core services of AWS cloud.
- By default, all the services in AWS are monitored by CloudWatch.
- It can store logs from various serverless components in AWS.
- It retains and stores monitored data, which is helpful to validate the stats anytime.
- It helps to create and generate alerts to users in case of issues.

TECHNOLOGY

Introduction to Nagios

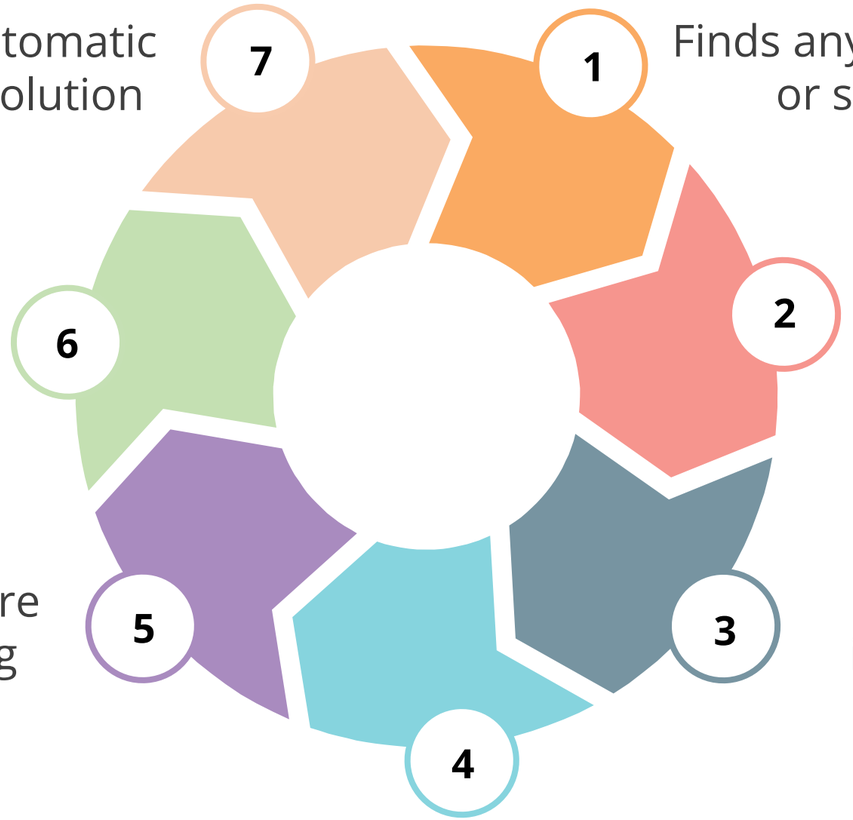
simplilearn

What Is Nagios ?

Nagios is an open-source continuous monitoring tool used to monitor the system, network, and IT infrastructure.

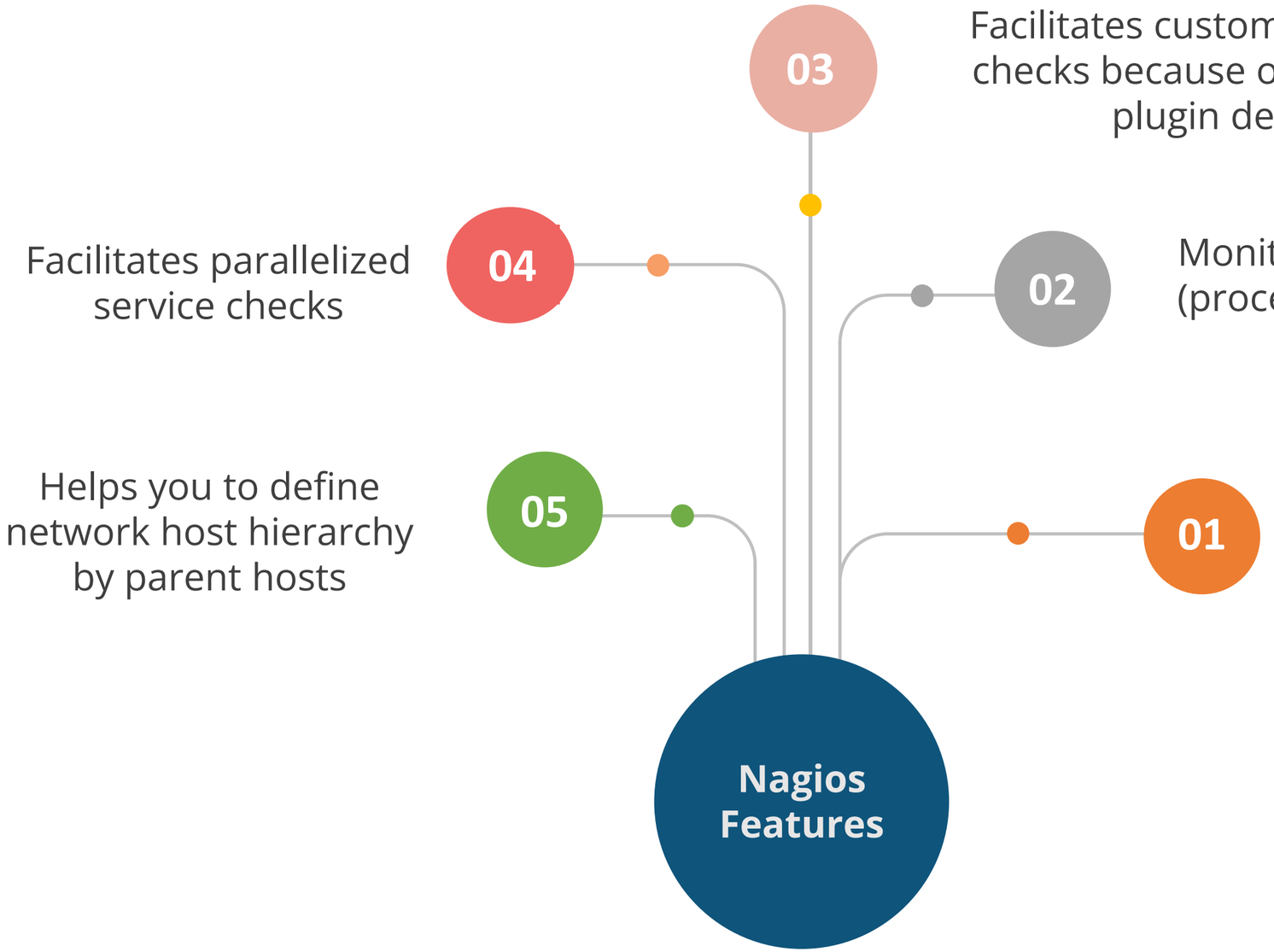
- It monitors the specified hosts and services that are specified and alerts you when things go bad and when they get better.
- Nagios is available in two variants - namely Nagios Core and Nagios XI.
- Nagios Core is an open source product whereas Nagios XI is a licensed version.

Why Nagios?

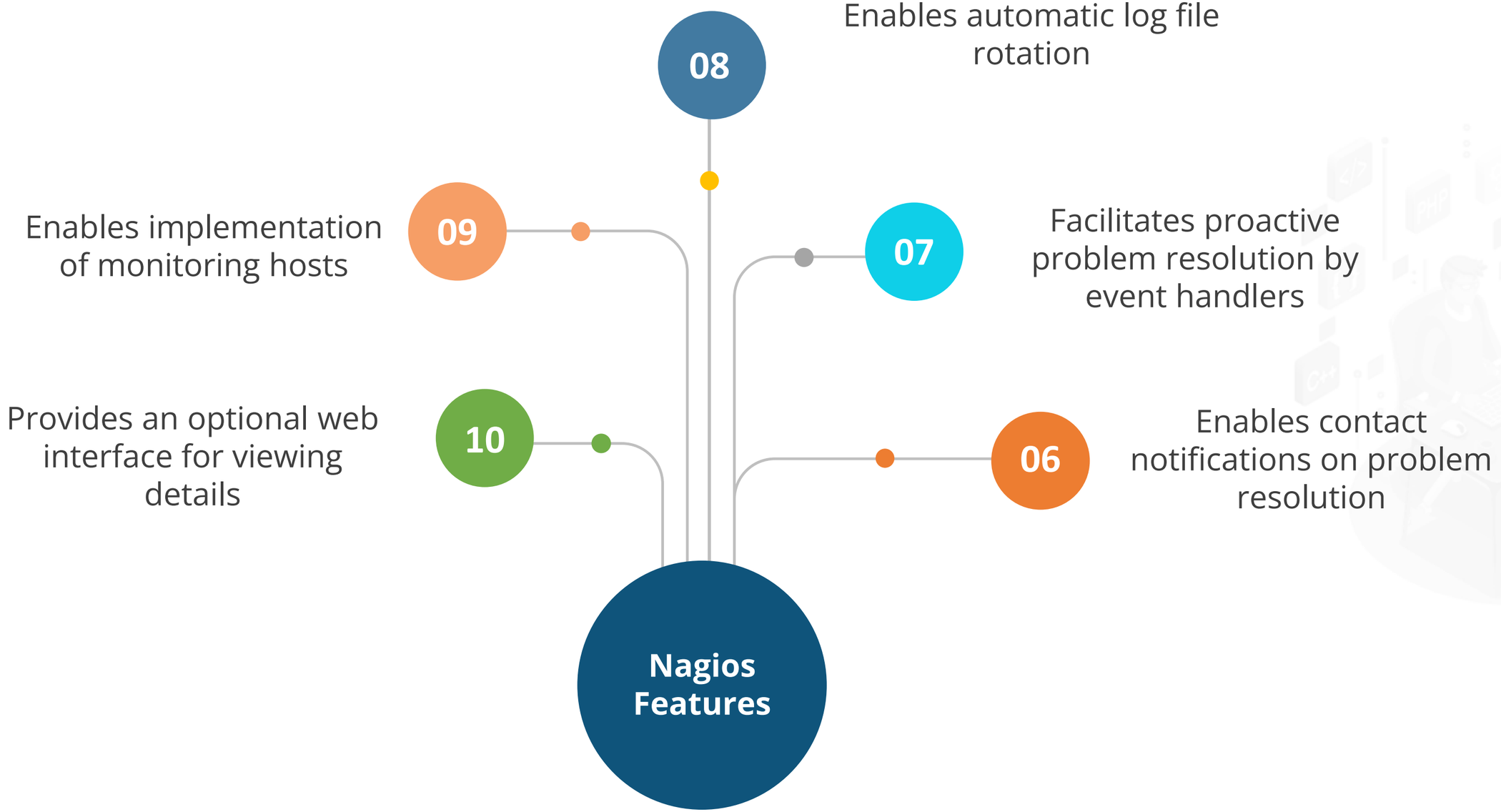


1. Finds any type of network or server issues
2. Identifies the root cause of the problem
3. Monitors the infrastructure actively
4. Troubleshoots server performance issues
5. Facilitates infrastructure upgrade and planning
6. Ensures security maintenance and service availability
7. Facilitates automatic problem resolution

Features of Nagios



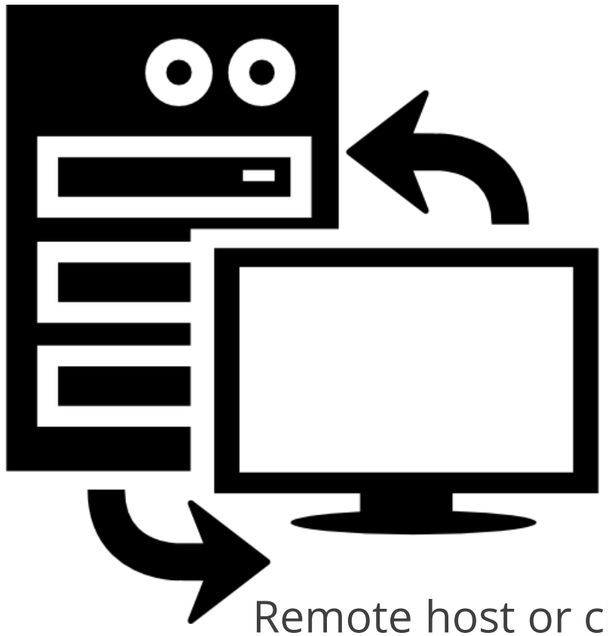
Features of Nagios



Nagios Architecture

Nagios uses a client/server architecture.

Nagios Server

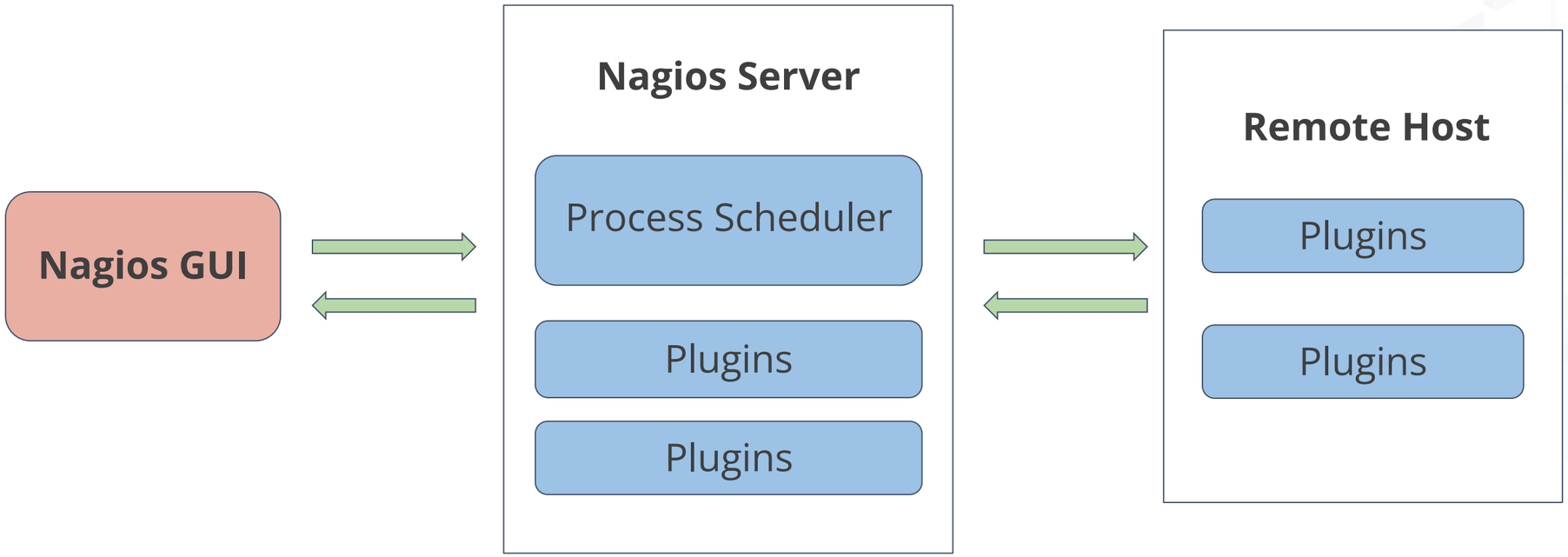


Remote host or client

The Nagios server usually runs on a host and the plugins run on remote hosts which are specified for monitored.

Nagios Architecture

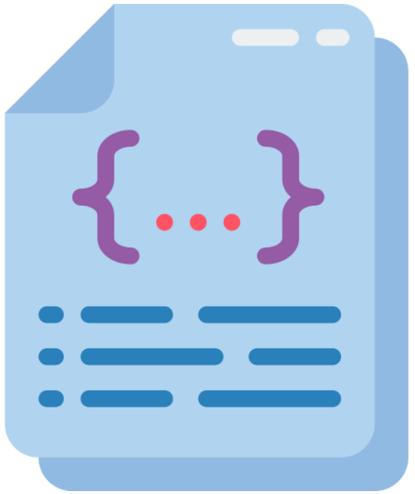
Nagios architecture is comprised of three main components namely - the process scheduler (running on the Nagios server), the plugins, and the user interface.



Nagios Plugins

Nagios Plugins

Plugins are compiled executables or scripts (Perl scripts and shell scripts) that can be run from the command line to check the status of a host or service.



- Plugins allow the user to monitor databases, operating systems, applications, network equipment, and protocols.
- They are standalone extensions to Nagios Core.

Types of Nagios Plugins

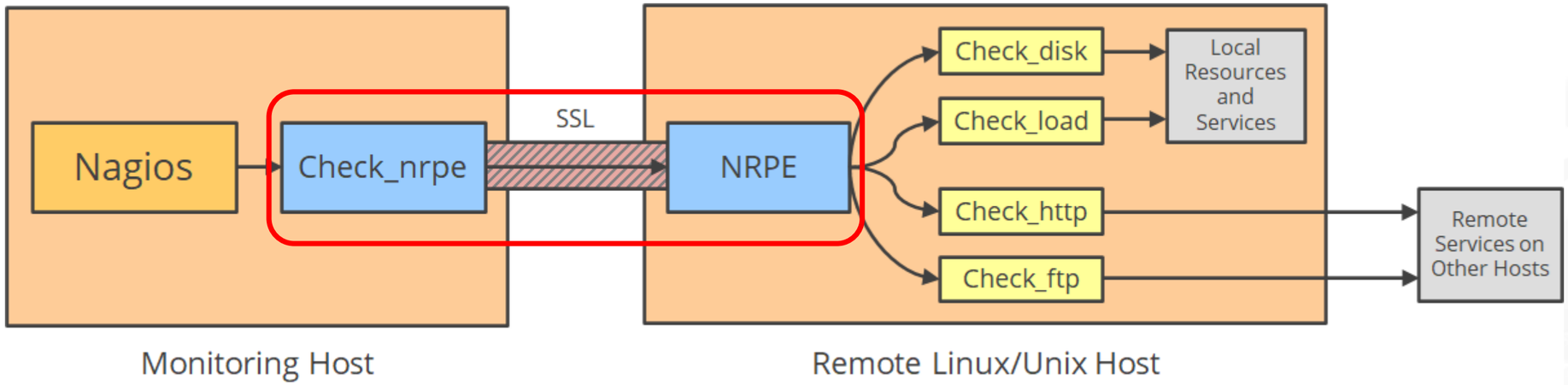
Official Nagios Plugins
Developed and maintained by official Nagios plugin team.

Community Plugins
Developed by hundreds of Nagios community members.

Custom Plugins
Developed by users in order to suit their requirements.

Nagios Remote Plugin Executor (NRPE)

NRPE is an addon that allows you to run Nagios plugins on remote machines to monitor remote machine metrics (disk usage, and CPU load).



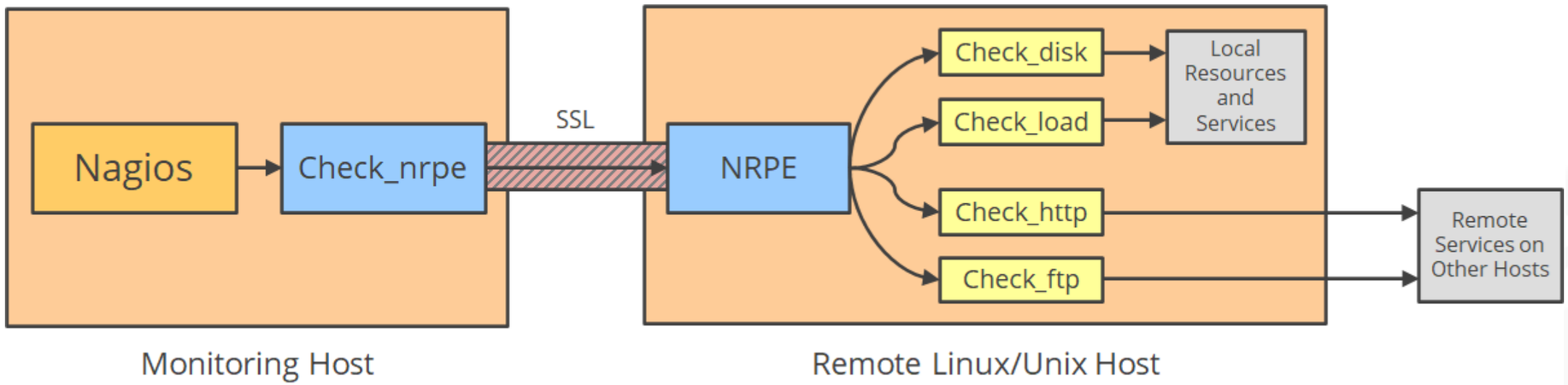
NRPE addon consists of:

- The check_nrpe plugin, which resides on the local monitoring host.
- The NRPE daemon, which runs on the remote Linux or Unix host.

Source: https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details

Nagios Remote Plugin Executor (NRPE)

To monitor a resource of a service from a remote Linux or Unix machine:



- Nagios executes the check_nrpe plugin and identifies which service needs to be checked.
- The check_nrpe plugin contacts the NRPE daemon on the remote host over SSL protected connection.
- The NRPE daemon runs the required Nagios plugin to check the service or resource.
- The results from the service check are sent by the NRPE daemon to the check_nrpe plugin, which then returns the transfers to the Nagios process.

How to Configure Plugins on Remote Nodes?

Nagios plugins monitor hosts, devices, services, protocols, and applications with Nagios and sends reports the report to NRPE.

NRPE sends those reports to Nagios server based on the Nagios server request.

Nagios and NRPE can perform all the processes only with Nagios plugins.

How to Configure Plugins on Remote Nodes ?

To monitor the remote host in the Nagios server, two installations are required:

- **Remote Host:** NRPE plugin and Nagios plugins
- **Nagios Server:** NRPE plugin

Nagios Installation

Nagios Installation

System Requirements for Nagios Core:

- A Linux machine (or UNIX variant) that has network access.
- A C compiler installed (In case you are installing from source code).

- It is optional to use the CGIs included with Nagios Core. However, if you plan to use them, you should have the software listed below:

1. Apache web server
2. Thomas Boutell's gd library - version 1.6.3 or higher

Installing and Configuring Nagios Monitoring Tool

Duration: 25 Min.

Problem Statement:

You are given a project to install and setup Nagios monitoring tool.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install and setup Nagios monitoring tool on Linux:

1. Install and configure Nagios Core

2. Verify and enable Nagios

3. Upgrade to the latest version of Nagios

TECHNOLOGY

Monitoring with Nagios

simplilearn

Using the Default Plugins

There are some default plugins available to monitor devices and services, including:

- HTTP, POP3, IMAP, FTP, SSH, and DHCP
- CPU Load, Disk Usage, Memory Usage, and Current Users
- Unix and Linux, Windows, and Netware Servers
- Routers and switches

The Nagios Exchange website offers a number of additional plugins developed by users, that can be used as per your requirement.

Using the Default Plugins

- ***check_http:*** Plugin used for monitoring web servers
- ***check_ftp:*** Plugin used for monitoring FTP servers
- ***check_ssh:*** Plugin used for monitoring SSH servers
- ***check_smtp:*** Plugin used for monitoring your email servers
- ***check_pop:*** Plugin used for monitoring the POP3 service on your email servers
- ***check_imap:*** Plugin used for monitoring IMAP4 service on your email servers

Adding Hosts to the Nagios Monitoring Tool

Duration: 25 Min.

Problem Statement:

You are given a project to add a Linux node to the Nagios server for monitoring.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to add a Linux node to the Nagios server for monitoring :

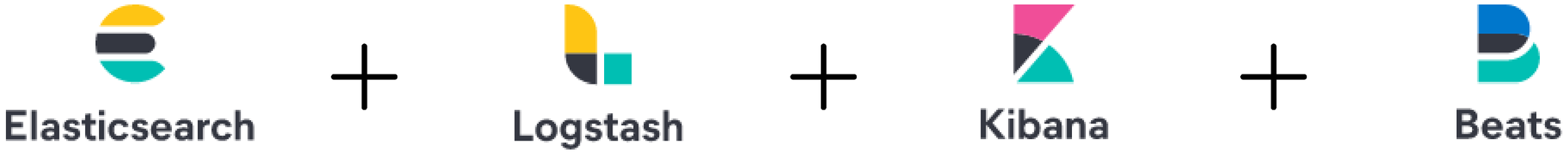
1. Login to the Nagios XI dashboard

2. Add a host using the Core Config Manager

ELK Stack

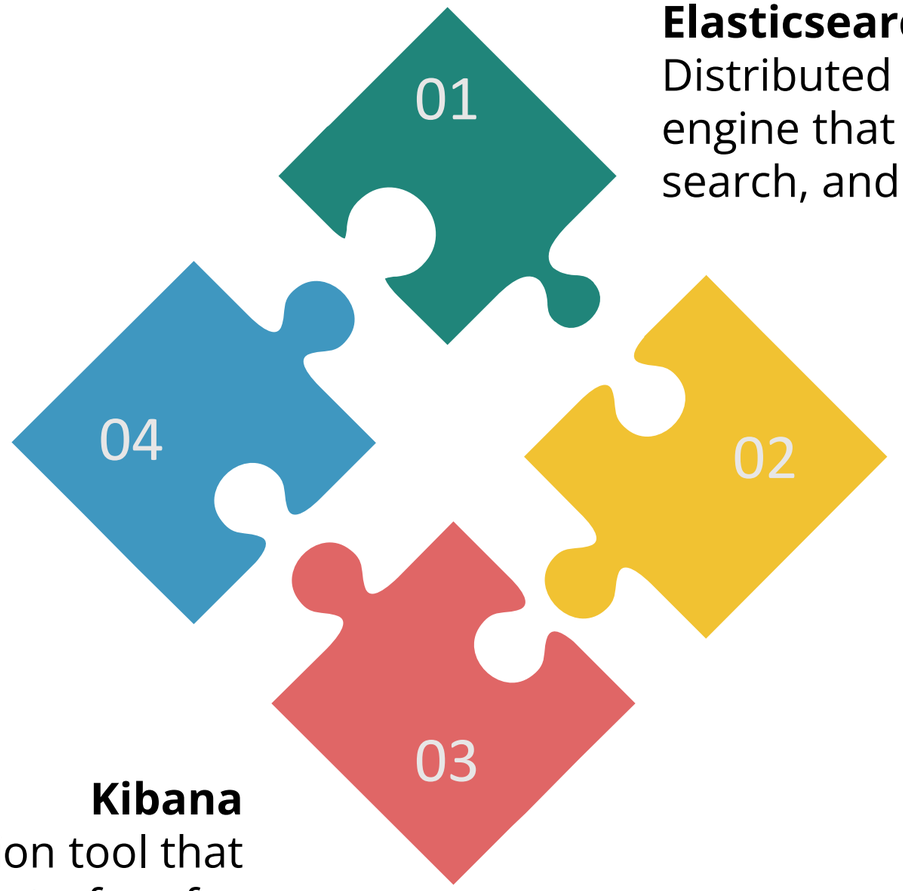
ELK Stack

ELK Stack is an open-source, distributed monitoring solution with centralized logging, metric, and application performance monitoring, suitable for almost any structured and unstructured data source.



ELK is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana. Recently a new component called Beats was included in the ELK Stack.

Main Components of ELK Stack



Elasticsearch
Distributed search and analytics engine that can store, index, search, and analyze data.

Logstash
Data collection pipeline tool that collects data inputs and feeds the Elasticsearch.

Kibana
Data visualization tool that provides a web interface for searching and visualizing logs.

Beats
Lightweight data collectors that fetch metrics, data logs, and send it to Logstash or Elasticsearch.

Elasticsearch

Elasticsearch is a distributed search and analytics engine that provides the real-time search and analytics for data (structured and unstructured).

Elasticsearch

Functions

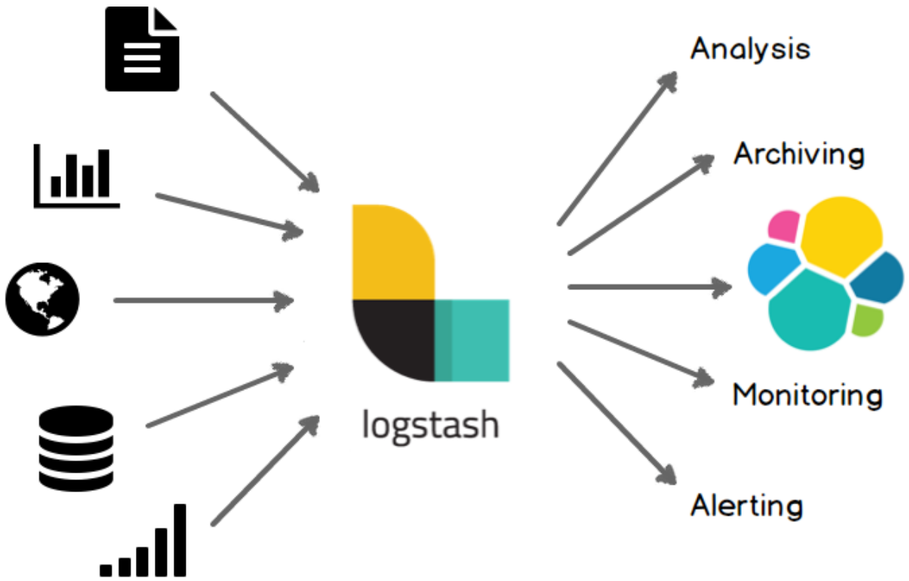
1. **Store**: It stores complex data structures that are serialized as JSON documents

1. **Index**: Documents are indexed almost real-time

1. **Search**: Supports searches through inverted index

1. **Analyze**: Dynamic mapping makes schema-less possible by detecting and adding new fields

Logstash

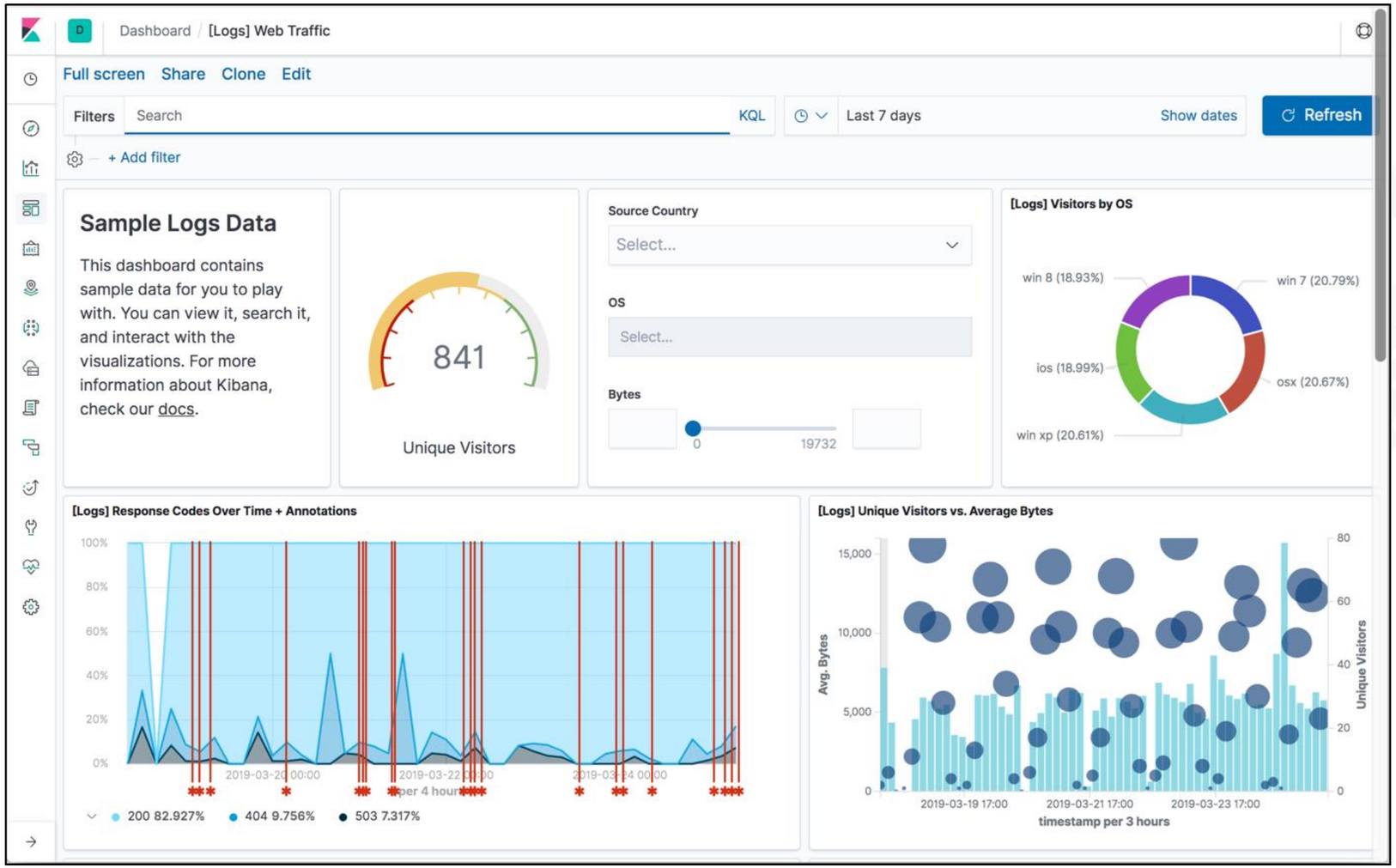


- It is the data processing component of the ELK Stack.
- Collects data from various sources and feeds Elasticsearch or normalizes it to other destinations.

Source: https://elastic-stack.readthedocs.io/en/latest/introduction.html#main-components

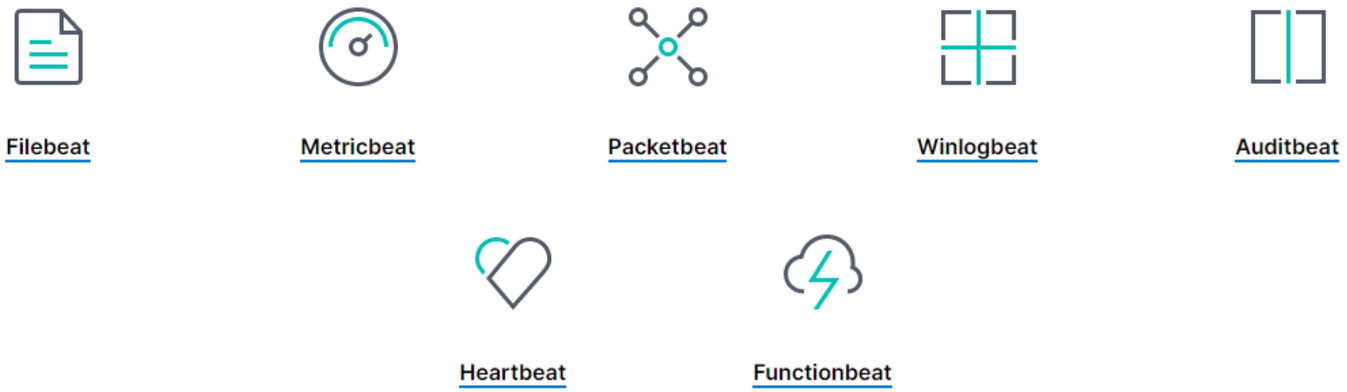
Kibana

Kibana is the data visualization tool that provides the graphical user interface for Elasticsearch.



Beats

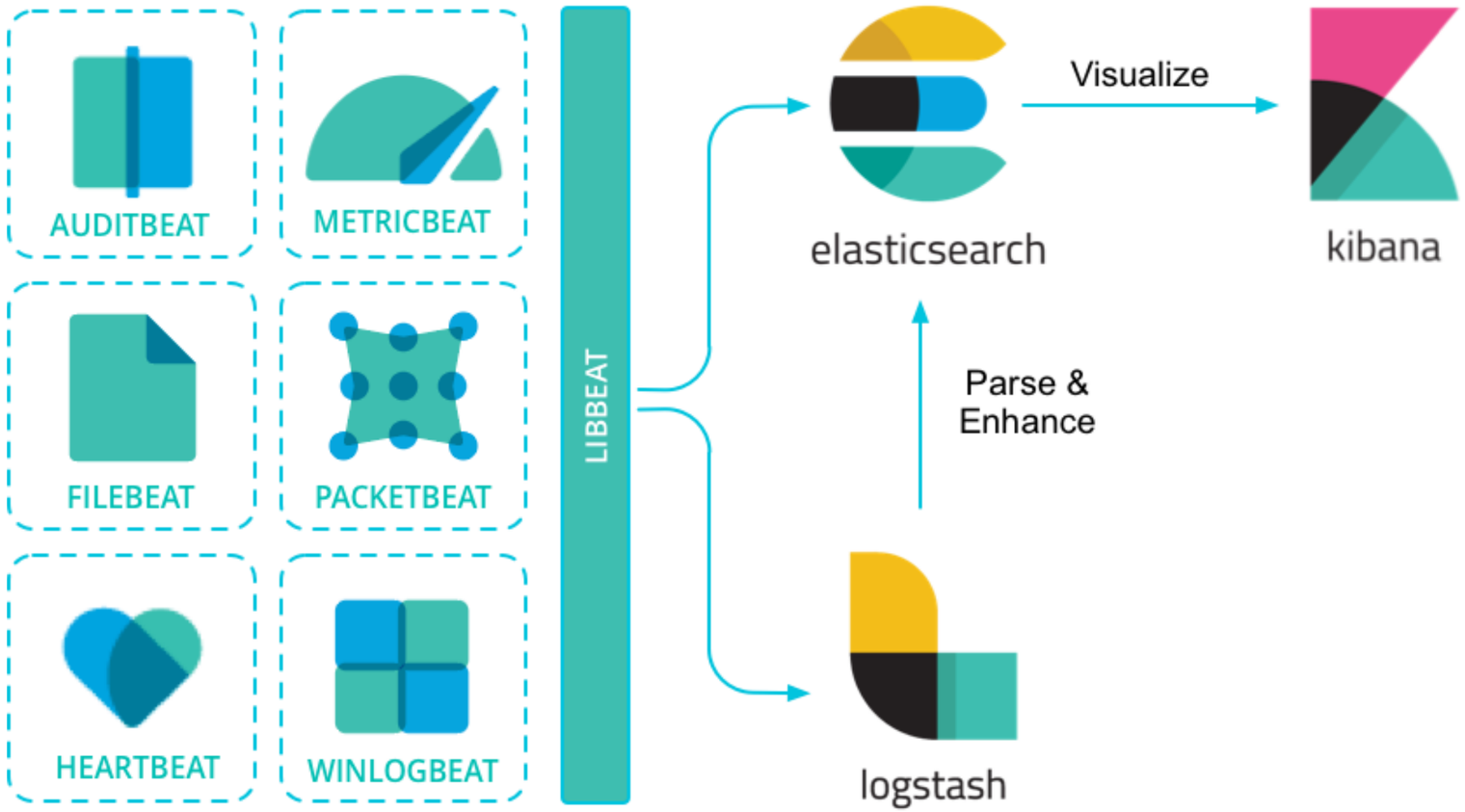
Beats are lightweight data collectors that are installed directly on the data source and collect data for specific purposes, which are then sent to Elasticsearch or Logstash. Most frequently used collectors are:



- *Filebeat*: sends local file records.
- *Winlogbeat*: sends Windows event logs.
- *Metricbeat*: sends system or application performance metrics.

Source: https://elastic-stack.readthedocs.io/en/latest/introduction.html#main-components

ELK Stack Overview



Source: https://elastic-stack.readthedocs.io/en/latest/introduction.html#main-components

ELK Stack Overview

1. A set of utilities provide the most powerful analytics for the business
2. Combination of Elasticsearch for searching data, Logstash to process and store various stats, and Kibana to visualize stats on front-end application
3. Open-source. Collects logs from servers and applications that can be analyzed for improvement
4. Backup of monitoring stats and able to store our monitoring system
5. View stats to detect defects in applications
6. Logstash can be used to gather stats from a variety of data sources and sent to Kibana
7. Install clients to collect data and send it back to the ELK Stack

Setting up Complete ELK Stack for Log Management

Based on the use-case and environment, businesses might need different logging architectures. The classic ELK stack architecture can support small environments as shown below:

Data collection and processing

Data storage and indexing

Data analysis and visualization

Setting up Complete ELK Stack for Log Management

For environments that provides Big Data, some additional components might be required as shown below:

Data collection

Buffering

Accumulation and processing

Storage and indexing

Data analysis and visualization

Implementing Continuous Monitoring on Docker with ELK Stack

Duration: 35 Min.

Problem Statement:

You are given a project to demonstrate continuous monitoring on Docker with ELK Stack.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to setup continuous monitoring on Docker with ELK Stack:

1. Setup ELK Stack on Docker.
2. Configure Jenkins pipeline for Docker build and deployment.
3. Run the Spring Boot application and check the logs in Kibana.

Key Takeaways

- Continuous monitoring involves monitoring and identifying compliance issues, security risks in each phase of the DevOps lifecycle.
- Nagios is an open-source continuous monitoring tool used to monitor the system, network, and IT infrastructure.
- NRPE is a Nagios addon that allows you to run Nagios plugins on remote machines to monitor remote machine metrics.
- ELK Stack is a distributed monitoring solution with centralized logging, metric and application performance monitoring capabilities.
- ELK Stack is a combination of Elasticsearch for searching data, Logstash to process and store various stats, and Kibana to visualize stats on front-end application.