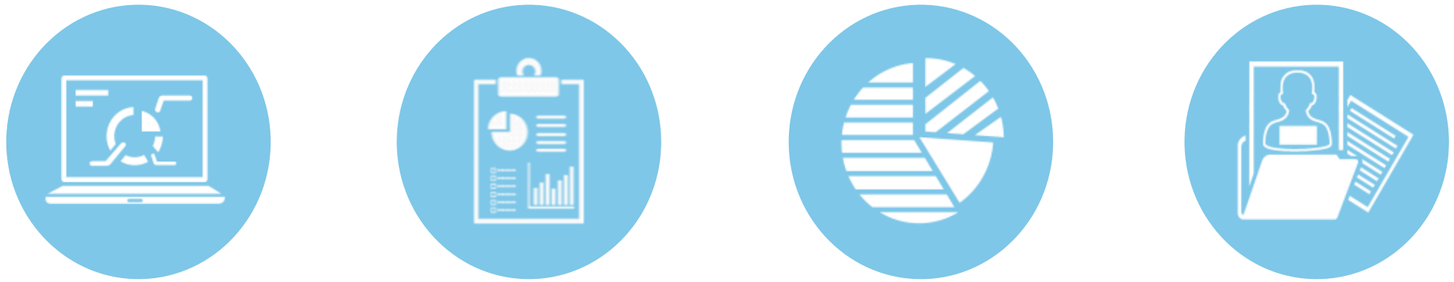
DevOps Certification Training

Lesson 07: Continuous Monitoring



Learning Objectives

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

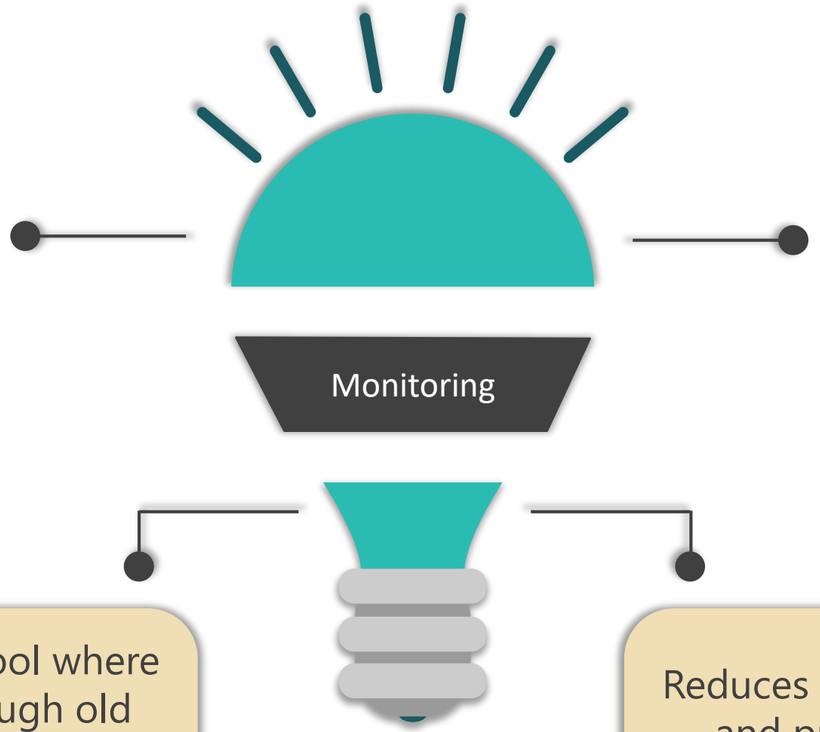
- Explain the role of continuous monitoring tools in DevOps
- Demonstrate Nagios
- Describe Grafana
- Describe ELK Stack
- Identify the suitable continuous monitoring tool for your organization

Continuous Monitoring

Overview of Continuous Monitoring

Continuous Monitoring

Helps detect risk, compliance, and security issues for an operational environment



Helps in continuous monitoring of environment so that adequate precautions are taken

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

Reduces the chances of failure and provides comfort to business in terms of 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

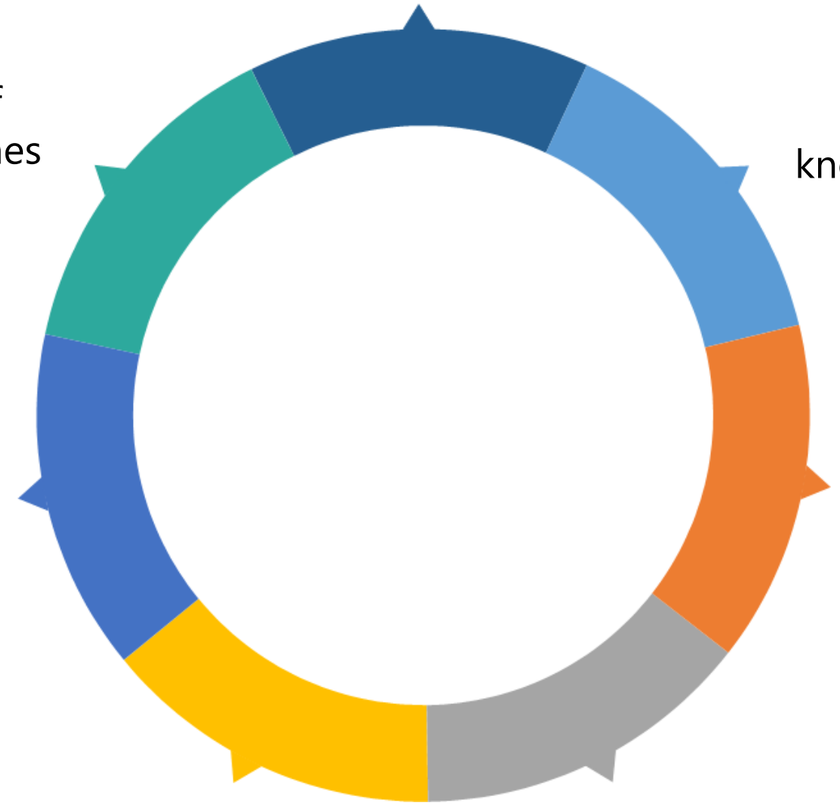
Alerts any issue in infrastructure or application service

Monitors production environment for risks and failures

Fetches old data for analysis

Displays application behavior during peak business hours

Reduces the risk of application downtimes



Continuous Monitoring

Types of Monitoring System

Types of Monitoring

Real-Time Monitoring

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

Infrastructure Monitoring

- CPU and memory
- Network and routers
- App servers, web servers, and DB servers

Application Monitoring

- API success/failures count
- API accessibility
- API HTTP error code

Popular Monitoring Tools

DevOps Monitoring Tools

Nagios Core is a free open-source, application and infrastructure monitoring tool. Nagios was launched in 2002 and it became one of the popular monitoring tools in many organizations. 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. Nagios enterprise version is also available.

ELK is a log monitoring and open-source tool. ELK is a combination of three open-source tools: Elasticsearch, Logstash, and Kibana. Elasticsearch is the heart of the stack since it acts as data engine, stores all applications, server logs, and fetches the data to analyze. 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 fetched from data engine.

DevOps Monitoring Tools (Contd.)

ZABBIX

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

sensu

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

DevOps Monitoring Tools (Contd.)

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.

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.

DevOps Monitoring Tools (Contd.)

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.

DevOps Monitoring Tools (Contd.)

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.

Continuous Monitoring

Demonstrate Nagios

Nagios Installation

```
root@ip-172-31-15-211:~# curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   629  100   629    0     0    436      0  0:00:01  0:00:01 --:--:--   435
/usr/bin/wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.19.4-1ubuntu2.1).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
check if /tmp/nagiosxi exists
Downloading latest Nagios XI release
--2018-11-22 02:41:48--  https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 72.14.181.71, 2600:3c00::f03c:91ff:fedf:b821
Connecting to assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54397198 (52M) [application/x-gzip]
Saving to: â/tmp/xi-latest.tar.gzâ

/tmp/xi-latest.tar.gz                     100%[=============================================================================

2018-11-22 02:42:07 (2.81 MB/s) - â/tmp/xi-latest.tar.gzâ saved [54397198/54397198]

Checking MySQL credentials...
MySQL not yet installed - that's okay.
Running './0-repos'...
Configuring Repos...
Repos configured OK
RESULT=0
Running './1-prereqs'...
Installing prerequisites...
Checking conflicting packages
```

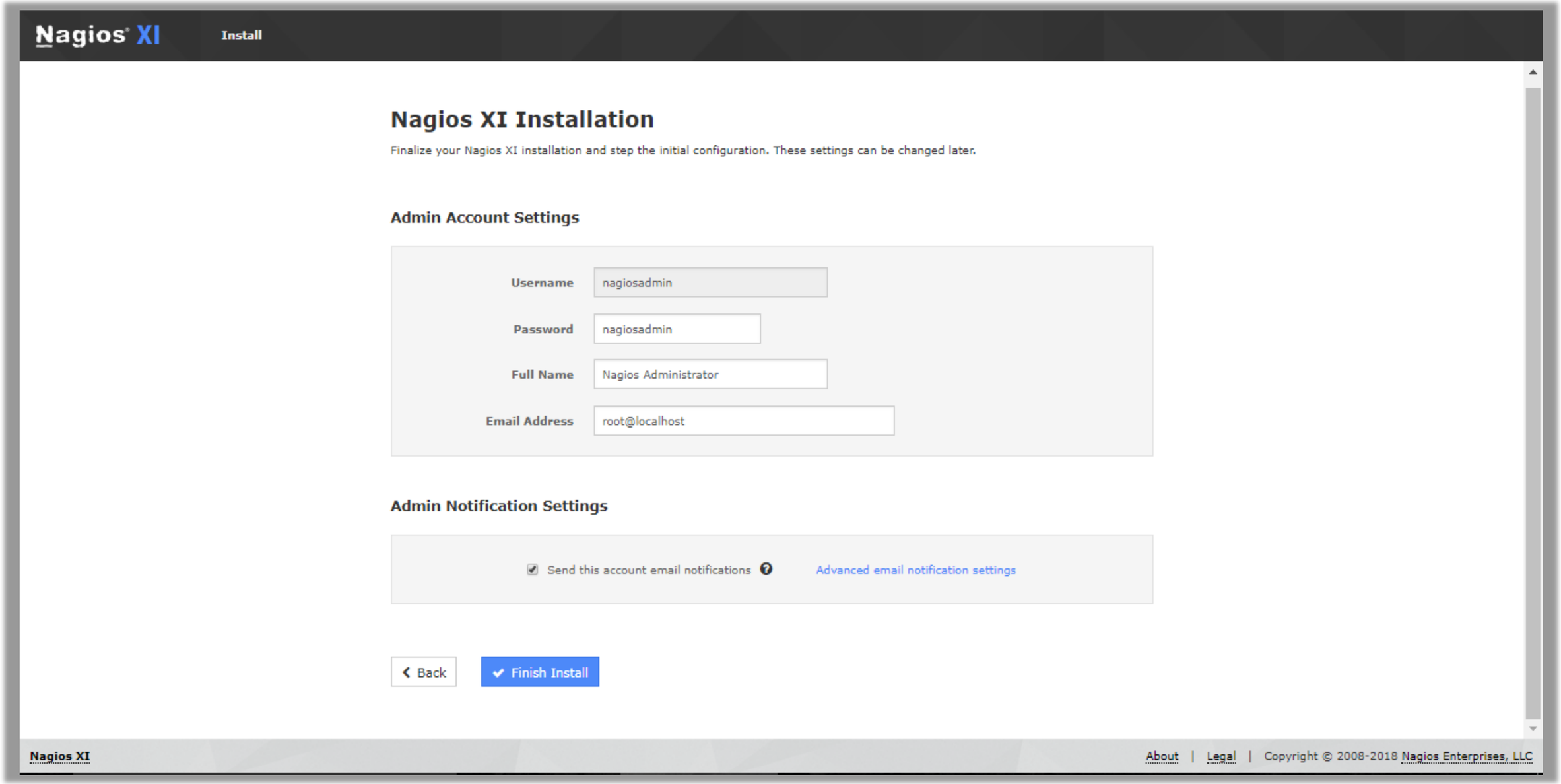
Nagios Installation (Contd.)

```
root@ip-172-31-15-211:~# service postgresql status
â postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: enabled)
   Active: active (exited) since Thu 2018-11-22 02:46:47 UTC; 37min ago
 Main PID: 7625 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 1152)
   CGroup: /system.slice/postgresql.service

Nov 22 02:46:47 ip-172-31-15-211 systemd[1]: Starting PostgreSQL RDBMS...
Nov 22 02:46:47 ip-172-31-15-211 systemd[1]: Started PostgreSQL RDBMS.
root@ip-172-31-15-211:~# service apache2 status
â apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           ââapache2-systemd.conf
   Active: active (running) since Thu 2018-11-22 02:56:48 UTC; 28min ago
  Process: 4267 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 11567 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Process: 4272 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 4287 (apache2)
    Tasks: 6 (limit: 1152)
   CGroup: /system.slice/apache2.service
           ââ 4287 /usr/sbin/apache2 -k start
           ââ11576 /usr/sbin/apache2 -k start
           ââ11577 /usr/sbin/apache2 -k start
           ââ11578 /usr/sbin/apache2 -k start
           ââ11579 /usr/sbin/apache2 -k start
           ââ11580 /usr/sbin/apache2 -k start

Nov 22 02:56:48 ip-172-31-15-211 systemd[1]: Stopped The Apache HTTP Server.
Nov 22 02:56:48 ip-172-31-15-211 systemd[1]: Starting The Apache HTTP Server...
Nov 22 02:56:48 ip-172-31-15-211 systemd[1]: Started The Apache HTTP Server.
Nov 22 03:09:11 ip-172-31-15-211 systemd[1]: Reloading The Apache HTTP Server.
Nov 22 03:09:12 ip-172-31-15-211 systemd[1]: Reloaded The Apache HTTP Server.
root@ip-172-31-15-211:~#
```

Nagios Installation (Contd.)

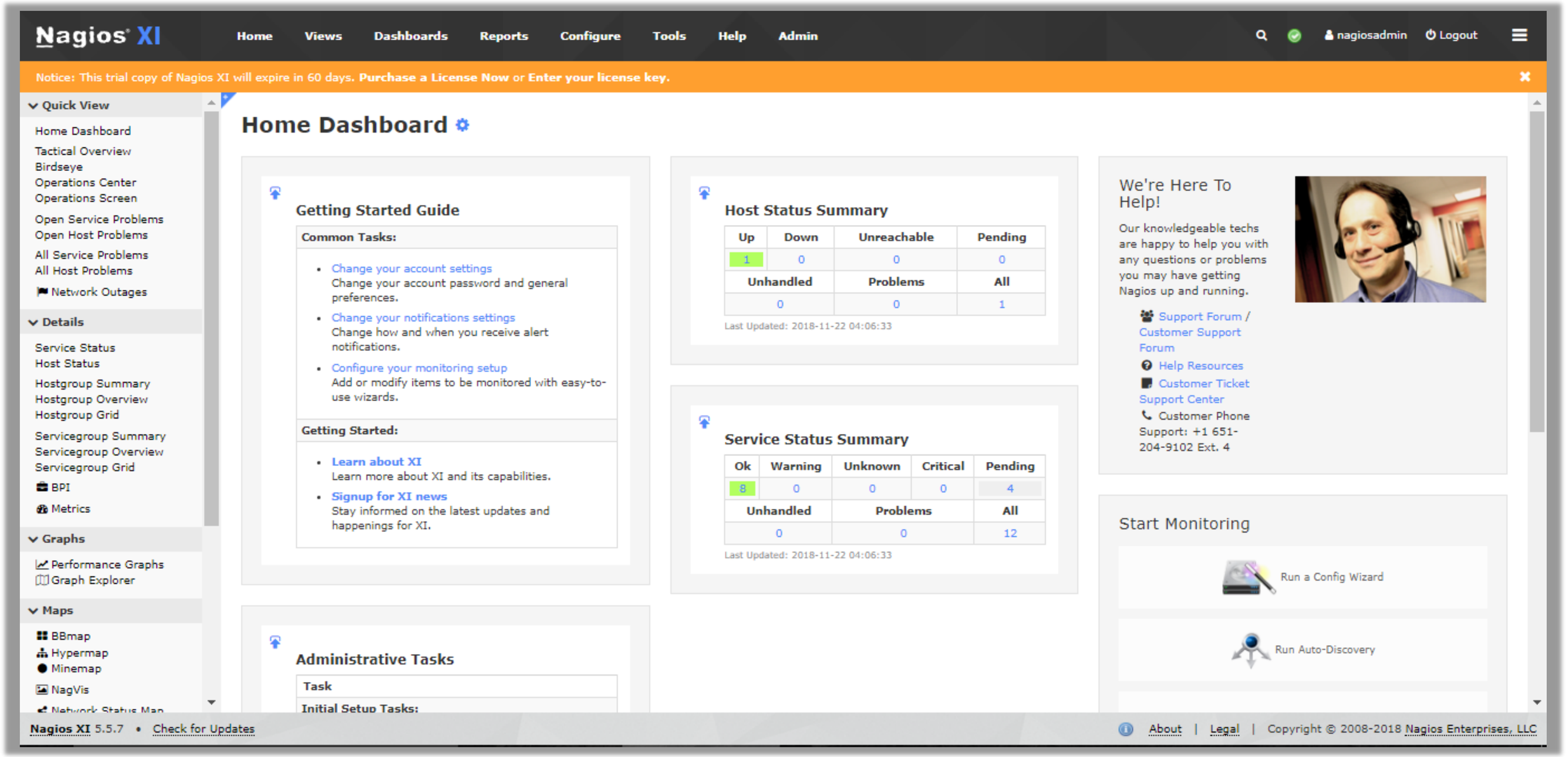
```
root@ip-172-31-15-211:~# service shellinabox status
â shellinabox.service - LSB: Shell In A Box Daemon
   Loaded: loaded (/etc/init.d/shellinabox; generated)
   Active: active (running) since Thu 2018-11-22 02:56:24 UTC; 32min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 2955 ExecStop=/etc/init.d/shellinabox stop (code=exited, status=0/SUCCESS)
  Process: 2962 ExecStart=/etc/init.d/shellinabox start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 1152)
   CGroup: /system.slice/shellinabox.service
           ââ2997 /usr/bin/shellinaboxd -q --background=/var/run/shellinaboxd.pid -c /var/lib/shellinabox -p 7878 -u she
           ââ3003 /usr/bin/shellinaboxd -q --background=/var/run/shellinaboxd.pid -c /var/lib/shellinabox -p 7878 -u she

Nov 22 02:56:24 ip-172-31-15-211 systemd[1]: Stopped LSB: Shell In A Box Daemon.
Nov 22 02:56:24 ip-172-31-15-211 systemd[1]: Starting LSB: Shell In A Box Daemon...
Nov 22 02:56:24 ip-172-31-15-211 systemd[1]: Started LSB: Shell In A Box Daemon.
root@ip-172-31-15-211:~# service mysql status
â mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-11-22 02:52:51 UTC; 35min ago
 Main PID: 32491 (mysqld)
    Tasks: 30 (limit: 1152)
   CGroup: /system.slice/mysql.service
           ââ32491 /usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/mysqld.pid

Nov 22 02:52:51 ip-172-31-15-211 systemd[1]: Stopped MySQL Community Server.
Nov 22 02:52:51 ip-172-31-15-211 systemd[1]: Starting MySQL Community Server...
Nov 22 02:52:51 ip-172-31-15-211 systemd[1]: Started MySQL Community Server.
root@ip-172-31-15-211:~#
```

Nagios: Account Setup



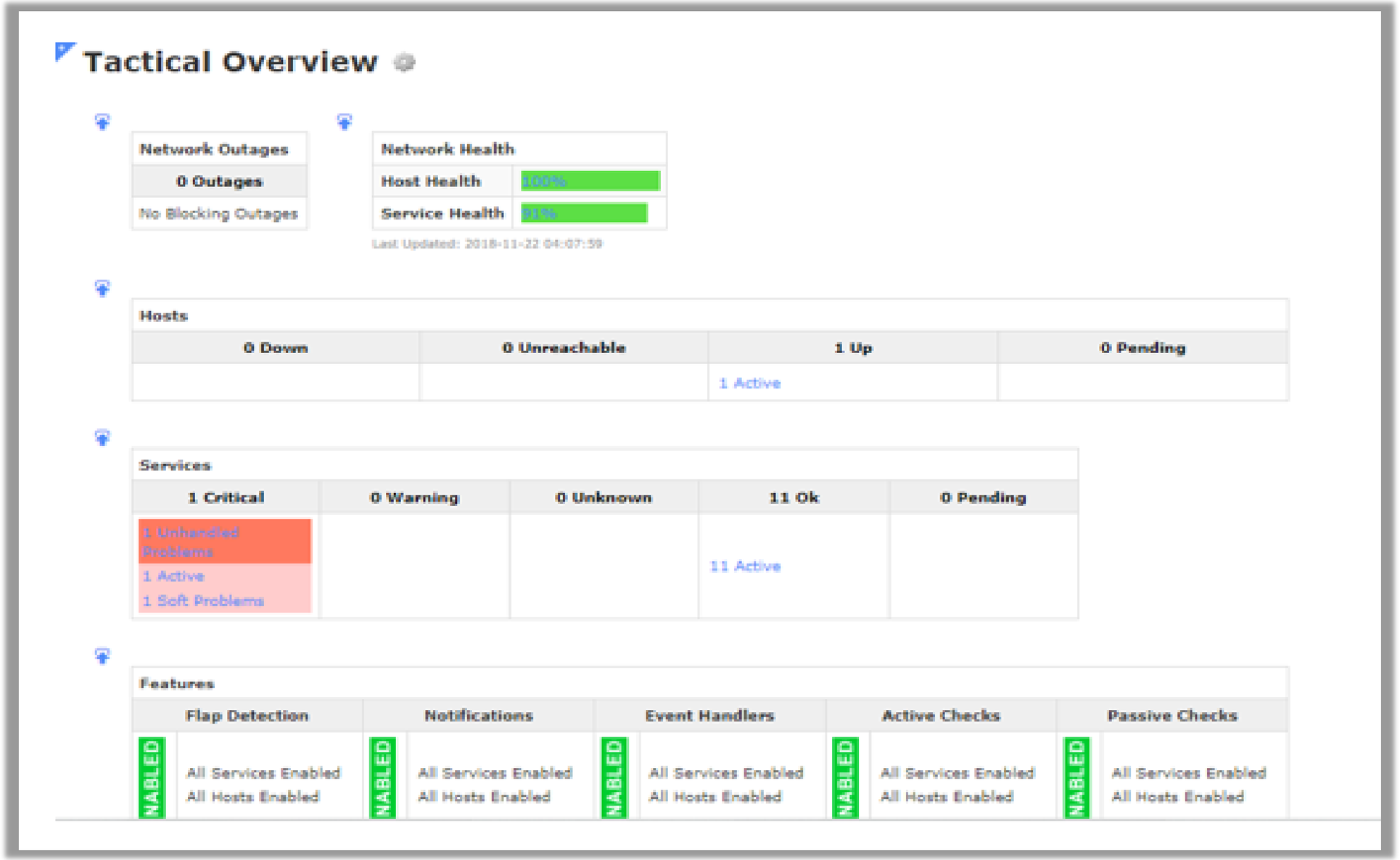
simplilearn

Nagios: Dashboard

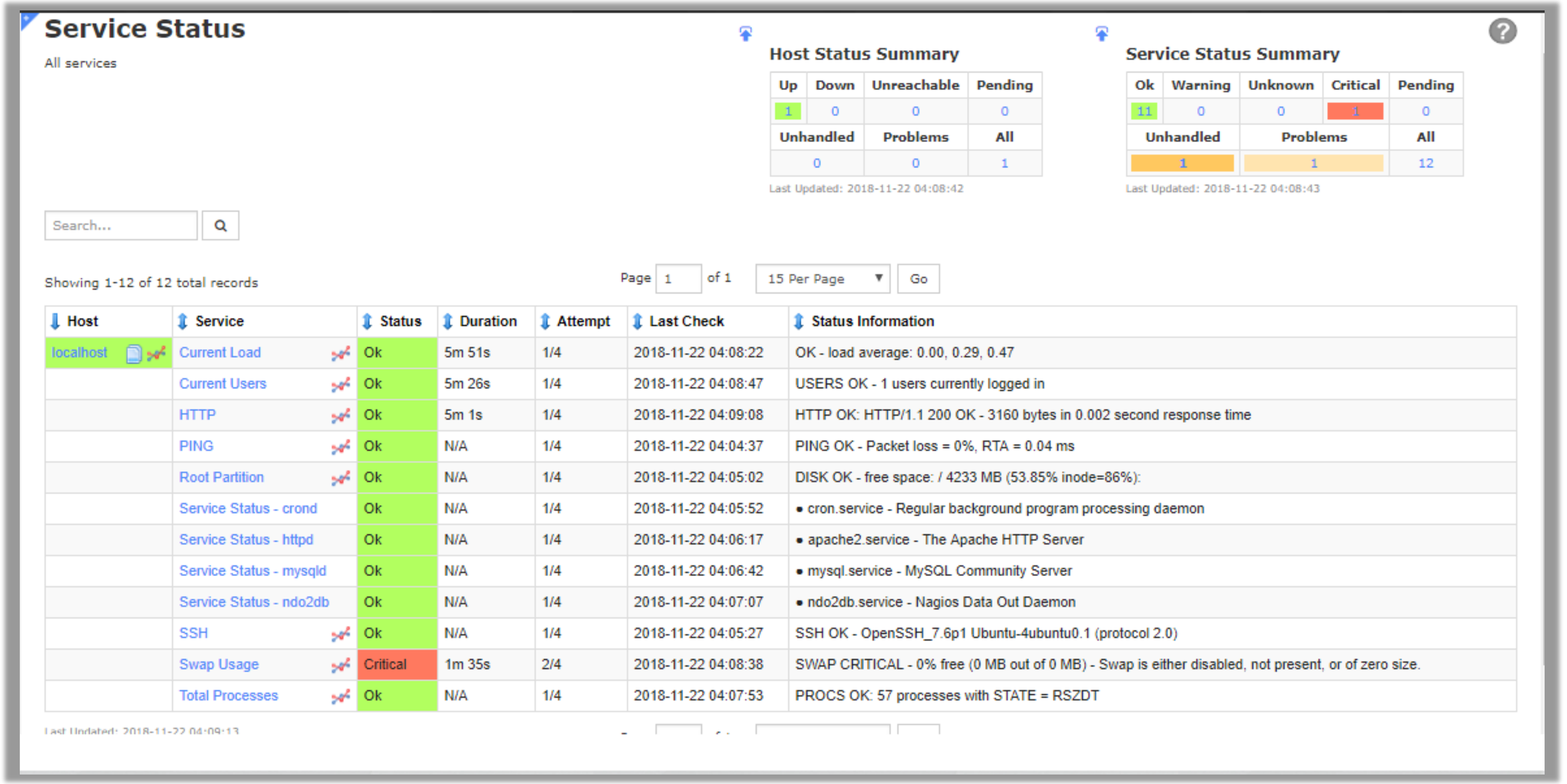


simplilearn

Nagios: Tactical Overview



Nagios: Service Status



Service Status

All services

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0

Unhandled	Problems	All
0	0	1

Last Updated: 2018-11-22 04:08:42

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	0	0	1	0

Unhandled	Problems	All
1	1	12

Last Updated: 2018-11-22 04:08:43

Search...

Showing 1-12 of 12 total records

Page 1 of 1 15 Per Page Go

Host	Service	Status	Duration	Attempt	Last Check	Status Information
localhost	Current Load	Ok	5m 51s	1/4	2018-11-22 04:08:22	OK - load average: 0.00, 0.29, 0.47
	Current Users	Ok	5m 26s	1/4	2018-11-22 04:08:47	USERS OK - 1 users currently logged in
	HTTP	Ok	5m 1s	1/4	2018-11-22 04:09:08	HTTP OK: HTTP/1.1 200 OK - 3160 bytes in 0.002 second response time
	PING	Ok	N/A	1/4	2018-11-22 04:04:37	PING OK - Packet loss = 0%, RTA = 0.04 ms
	Root Partition	Ok	N/A	1/4	2018-11-22 04:05:02	DISK OK - free space: / 4233 MB (53.85% inode=86%):
	Service Status - crond	Ok	N/A	1/4	2018-11-22 04:05:52	• cron.service - Regular background program processing daemon
	Service Status - httpd	Ok	N/A	1/4	2018-11-22 04:06:17	• apache2.service - The Apache HTTP Server
	Service Status - mysqld	Ok	N/A	1/4	2018-11-22 04:06:42	• mysql.service - MySQL Community Server
	Service Status - ndo2db	Ok	N/A	1/4	2018-11-22 04:07:07	• ndo2db.service - Nagios Data Out Daemon
	SSH	Ok	N/A	1/4	2018-11-22 04:05:27	SSH OK - OpenSSH_7.6p1 Ubuntu-4ubuntu0.1 (protocol 2.0)
	Swap Usage	Critical	1m 35s	2/4	2018-11-22 04:08:38	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	Ok	N/A	1/4	2018-11-22 04:07:53	PROCS OK: 57 processes with STATE = RSZDT

Last Updated: 2018-11-22 04:09:13

Nagios: Host Status

Host Status

All hosts

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0
Unhandled		**Problems**	**All**
0		0	1

Last Updated: 2018-11-22 04:11:04

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	0	0	1	0
Unhandled		**Problems**		**All**
1		1		12

Last Updated: 2018-11-22 04:11:04

Search...

Showing 1-1 of 1 total records

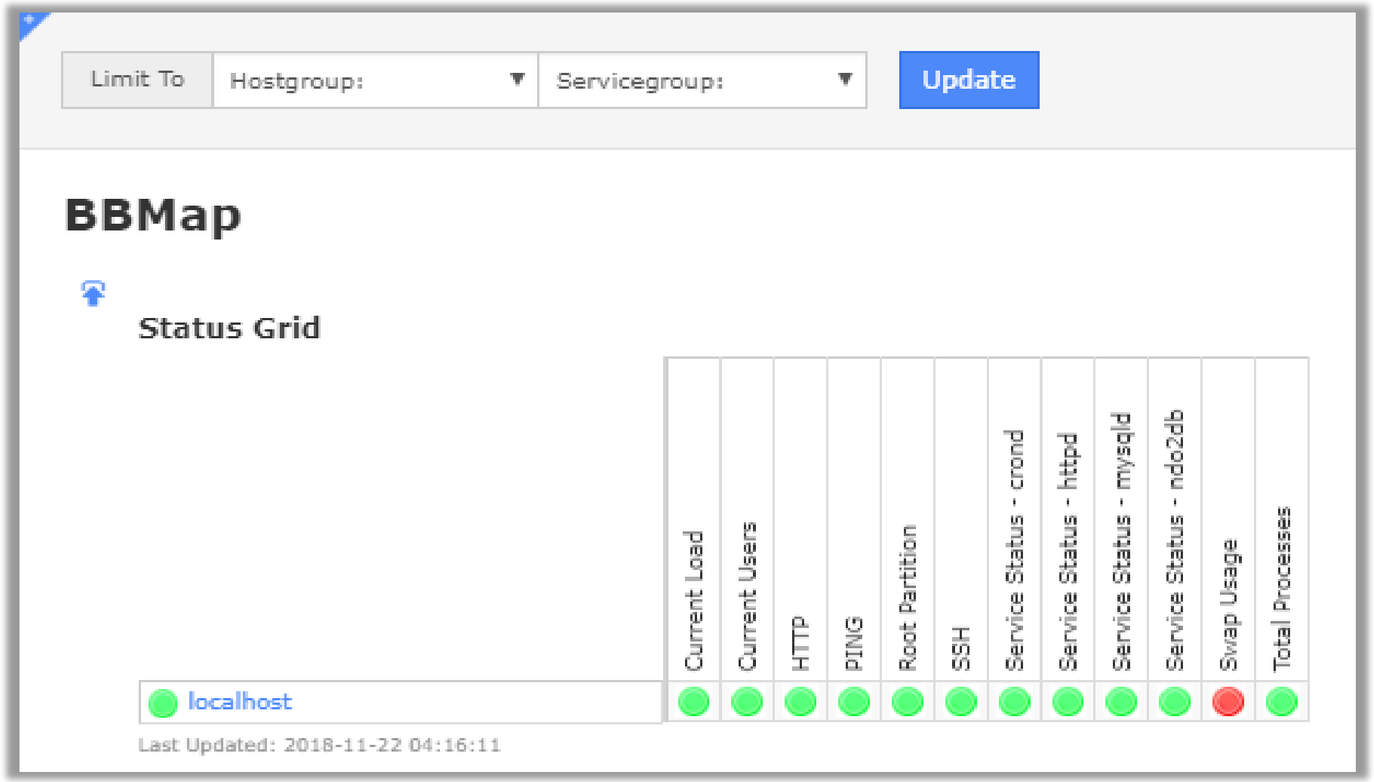
Page 1 of 1 15 Per Page Go

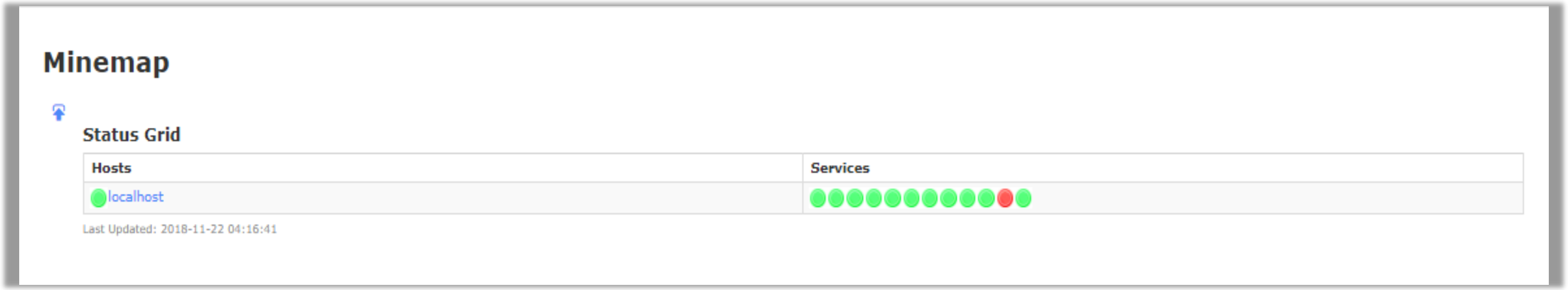
Host	Status	Duration	Attempt	Last Check	Status Information
localhost	Up	8m 6s	1/10	2018-11-22 04:07:38	OK - 127.0.0.1: rta 0.015ms, lost 0%

Last Updated: 2018-11-22 04:11:04

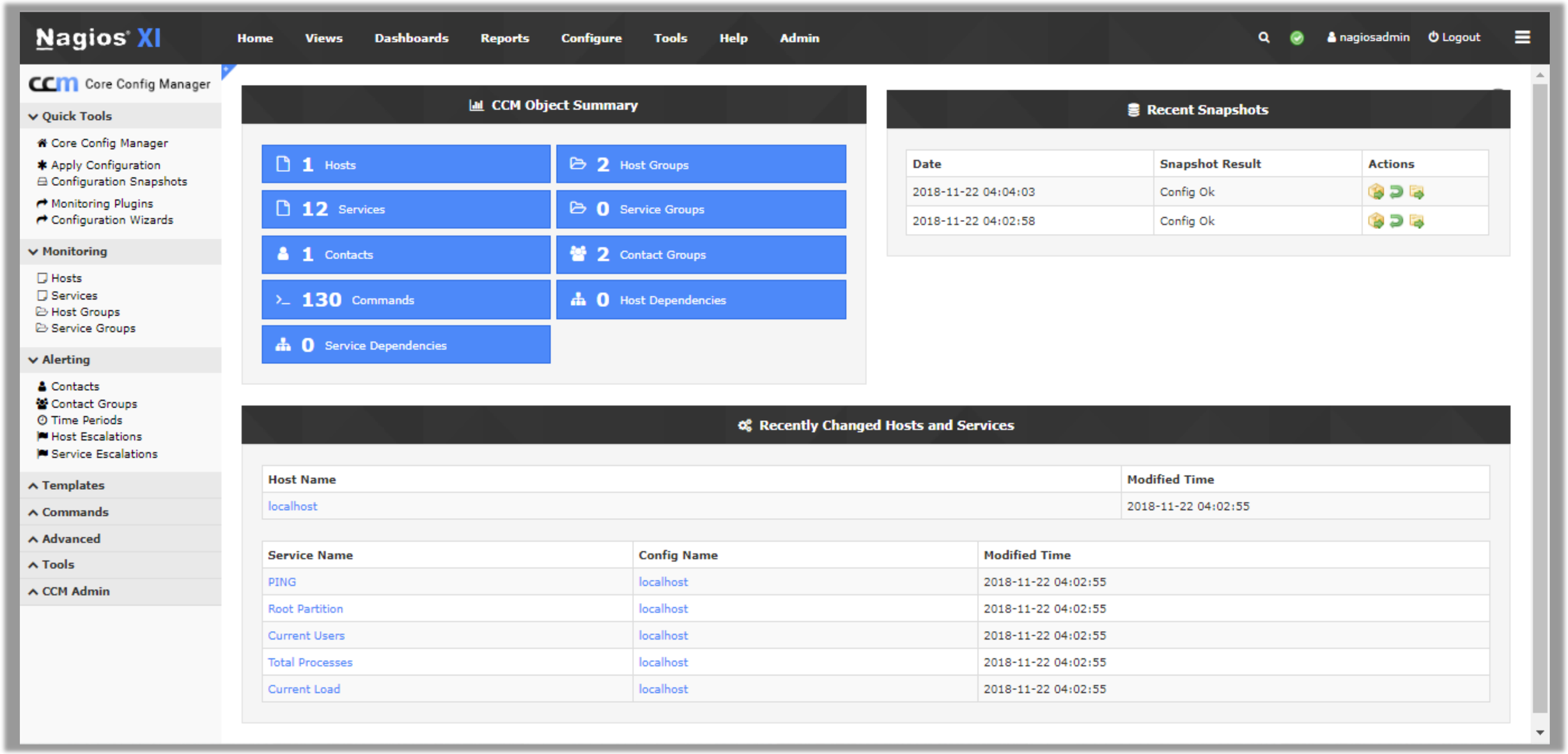
Page 1 of 1 15 Per Page Go

Nagios: Map Diagrams





Nagios: Core Configuration Manager



Assisted Practice

Duration: 90 mins

Working with Nagios Monitoring Tool

Problem Statement: You are given a project to demonstrate Nagios installation, install plugin, validate the installation, add a node, and validate the node details from Nagios dashboard.

Access: Click on the **Labs** tab on the left side panel of the LMS. Copy or note the username and password that is generated. Click on the **Launch Lab** button. On the page that appears, enter the username and password in the respective fields, and click **Login**.

Assisted Practice: Guidelines to Demonstrate Nagios Monitoring

1. Login to your Ubuntu Lab and open the terminal.
2. Download Nagios plugin source code.
3. Open Admin console of Nagios to install plugins.
4. Validate installation of Nagios plugin.
5. Add node details in Nagios portal.
6. Install Nagios agent on node machine.
7. Validate node details from Nagios dashboard.

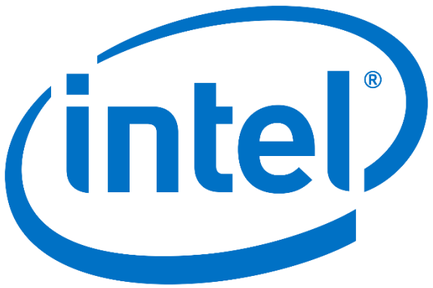
Continuous Monitoring

Describe Grafana

Grafana Monitoring System

Grafana is an open-source monitoring system that supports alerts and graphical representation of monitoring stats from various sources.

Some of the companies using Grafana:



Features of Grafana Monitoring System

Visualize
Able to download Heatmaps, histograms, graphs, and geomaps

Alert
Defines thresholds visually and notifies via PagerDuty and Slack

Unify
Supports multiple databases which can be visualized in the Dashboard

Open-Source
Use Hosted Grafana or easily install on any platform.

Extend
The Official Grafana library has hundreds of dashboards and plugins to choose from

Collaborate
Shares data and dashboards across teams.

Grafana: Dashboard

Continuous Monitoring

Describe ELK Stack

ELK Stack

1. A set of utilities are available which combine together to 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. Browse through the stats to detect defects in application
6. Logstash can be used to gather stats from a variety of data sources and pushed to Kibana
7. Install clients to collect data and post it back to the ELK stack

ELK Stack Installation

```
root@ip-172-31-27-81:~# apt install apt-transport-https software-properties-common wget -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
software-properties-common is already the newest version (0.96.24.32.5).
wget is already the newest version (1.19.4-1ubuntu2.1).
apt-transport-https is already the newest version (1.6.6).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ip-172-31-27-81:~# apt -y install openjdk-8-jdk
Reading package lists... Done
Building dependency tree
Reading state information... Done
openjdk-8-jdk is already the newest version (8u181-b13-1ubuntu0.18.04.1).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ip-172-31-27-81:~# java -version
openjdk version "1.8.0_181"
OpenJDK Runtime Environment (build 1.8.0_181-8u181-b13-1ubuntu0.18.04.1-b13)
OpenJDK 64-Bit Server VM (build 25.181-b13, mixed mode)
root@ip-172-31-27-81:~#
```

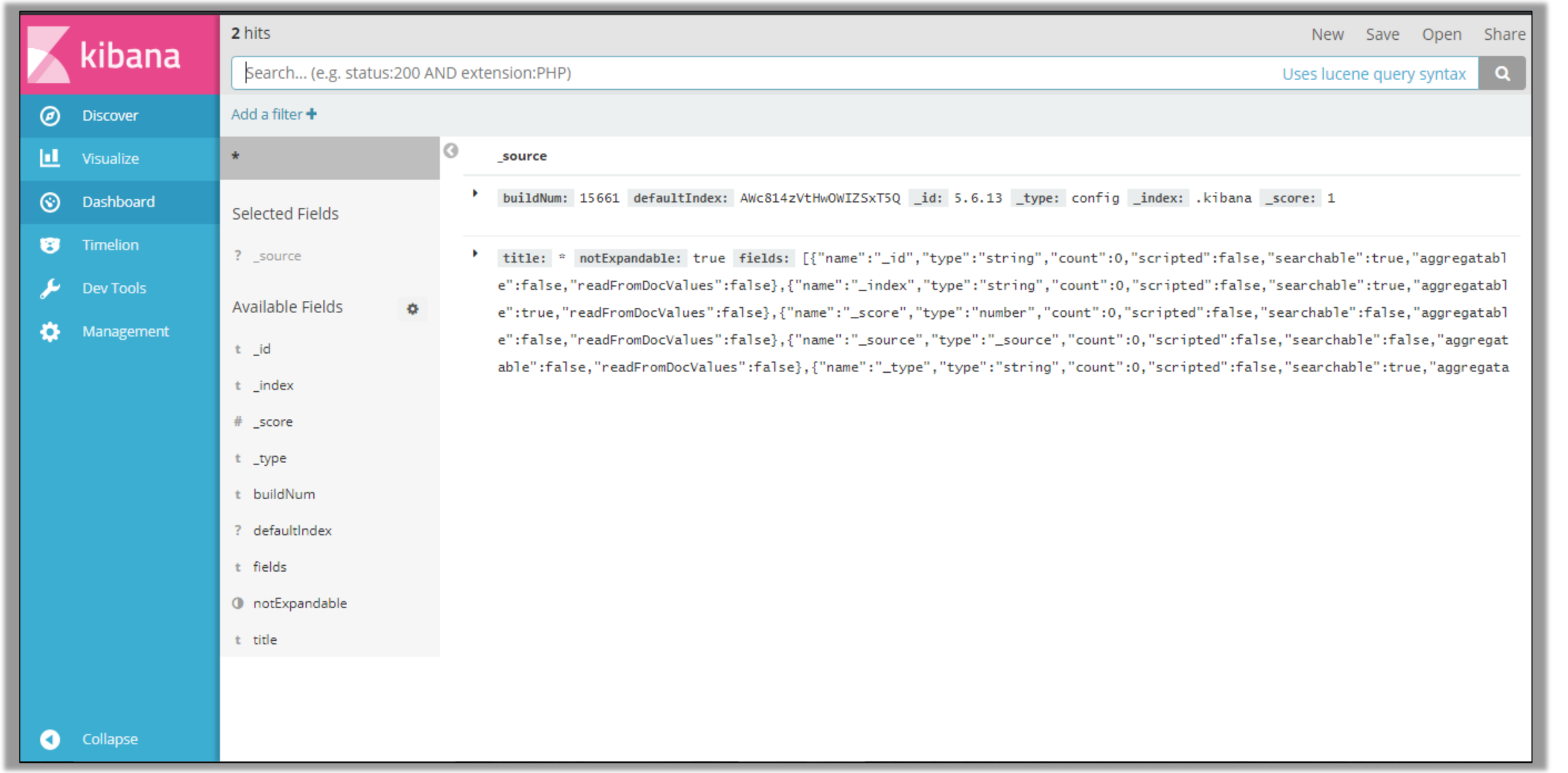
ELK Stack Installation (Contd.)

```
root@ip-172-31-27-81:/etc/elasticsearch# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@ip-172-31-27-81:/etc/elasticsearch# echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a
deb https://artifacts.elastic.co/packages/5.x/apt stable main
root@ip-172-31-27-81:/etc/elasticsearch# vi /etc/apt/sources.list.d/elastic-5.x.list
root@ip-172-31-27-81:/etc/elasticsearch# apt install elasticsearch
Reading package lists... Done
Building dependency tree
Reading state information... Done
elasticsearch is already the newest version (5.6.13).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ip-172-31-27-81:/etc/elasticsearch# service elasticsearch restart
root@ip-172-31-27-81:/etc/elasticsearch# service elasticsearch status
â elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2018-11-22 18:23:57 UTC; 3s ago
     Docs: http://www.elastic.co
  Process: 20146 ExecStartPre=/usr/share/elasticsearch/bin/elasticsearch-systemd-pre-exec (code=exited, status=0/SUCCESS)
 Main PID: 20155 (java)
    Tasks: 14 (limit: 1152)
   CGroup: /system.slice/elasticsearch.service
           ââ20155 /usr/bin/java -Xms300m -Xmx300m -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMS

Nov 22 18:23:57 ip-172-31-27-81 systemd[1]: Starting Elasticsearch...
Nov 22 18:23:57 ip-172-31-27-81 systemd[1]: Started Elasticsearch.
root@ip-172-31-27-81:/etc/elasticsearch#
```

ELK Stack Installation (Contd.)

```
root@ip-172-31-27-81:/etc/elasticsearch# apt install kibana nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
nginx is already the newest version (1.14.0-0ubuntu1.2).
kibana is already the newest version (5.6.13).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ip-172-31-27-81:/etc/elasticsearch# echo "admin:$(openssl passwd -apr1 YourStrongPassword)" | sudo tee -a /etc/nginx/htpasswd.kibana
admin:$apr1$aWn15jgb$w52VfFuc67qTHfTd879gr0
root@ip-172-31-27-81:/etc/elasticsearch# service nginx restart
root@ip-172-31-27-81:/etc/elasticsearch# apt install logstash -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 105 not upgraded.
Need to get 106 MB of archives.
After this operation, 201 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/5.x/apt stable/main amd64 logstash all 1:5.6.13-1 [106 MB]
Fetched 106 MB in 14s (7415 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 112407 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a5.6.13-1_all.deb ...
Unpacking logstash (1:5.6.13-1) ...
Setting up logstash (1:5.6.13-1) ...
Using provided startup.options file: /etc/logstash/startup.options
Successfully created system startup script for Logstash
root@ip-172-31-27-81:/etc/elasticsearch#
```

Kibana Visualizer Application



Key Takeaways

You are now able to:

- Explain the role of continuous monitoring tools in DevOps
- Demonstrate Nagios
- Describe Grafana
- Describe ELK Stack
- Identify the suitable continuous monitoring tool for your organization

Knowledge Check

Knowledge Check

1

Which one of the following is a task of monitoring system?

a. Server Monitoring

b. Application Monitoring

c. Network Monitoring

d. All of the above

Knowledge Check

1

Which one of the following is a task of monitoring system?

a. Server Monitoring

b. Application Monitoring

c. Network Monitoring

d. All of the above

The correct answer is **d. All of the above**

Server monitoring, application monitoring, and networking are used for monitoring stats of various infrastructure components.

Knowledge Check 2	**Which one of the following is the valid monitoring agent for Nagios in Linux environment?**

a. NRPE

b. NSClient ++

c. RDP

d. Agent is not required

Knowledge Check

2

Which one of the following is the valid monitoring agent for Nagios in Linux environment?

a. NRPE

b. NSClient ++

c. RDP

d. Agent is not required

The correct answer is **a. NRPE**

NRPE agent is installed on various Linux servers to gather various monitoring stats from server.

Knowledge Check

3

Which one of the following is the data source in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of above

Knowledge Check

3

Which one of the following is the data source in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of above

The correct answer is **a. Elasticsearch**

Elasticsearch is the data source used to store monitoring stats from various nodes.

Knowledge Check

4

Which one of the following is the data pipeline component in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of the above

Knowledge Check

4

Which one of the following is the data pipeline component in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of the above

The correct answer is **b. Logstash**

Logstash is the data pipeline component which is used to redirect the logs from nodes to datastore.

Knowledge Check

5

Which one of the following is the web component in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of the above

Knowledge Check

5

Which one of the following is the web component in ELK Stack?

a. Elasticsearch

b. Logstash

c. Kibana

d. None of the above

The correct answer is **c. Kibana**

Kibana is the component used to visualize monitoring stats fetched from Elasticsearch.

Lesson-End Project

Add a Node in Nagios Monitoring Tool

Duration: 60 mins

Problem Statement:

Perform the following actions:

- Download Nagios plugin source code.
- Open Admin console of Nagios to install plugin.
- Find the required plugin.
- Install the plugin.
- Validate if it is working.

Access: Click on the **Labs** tab on the left side panel of the LMS. Copy or note the username and password that is generated. Click on the **Launch Lab** button. On the page that appears, enter the username and password in the respective fields, and click **Login**.

Thank You