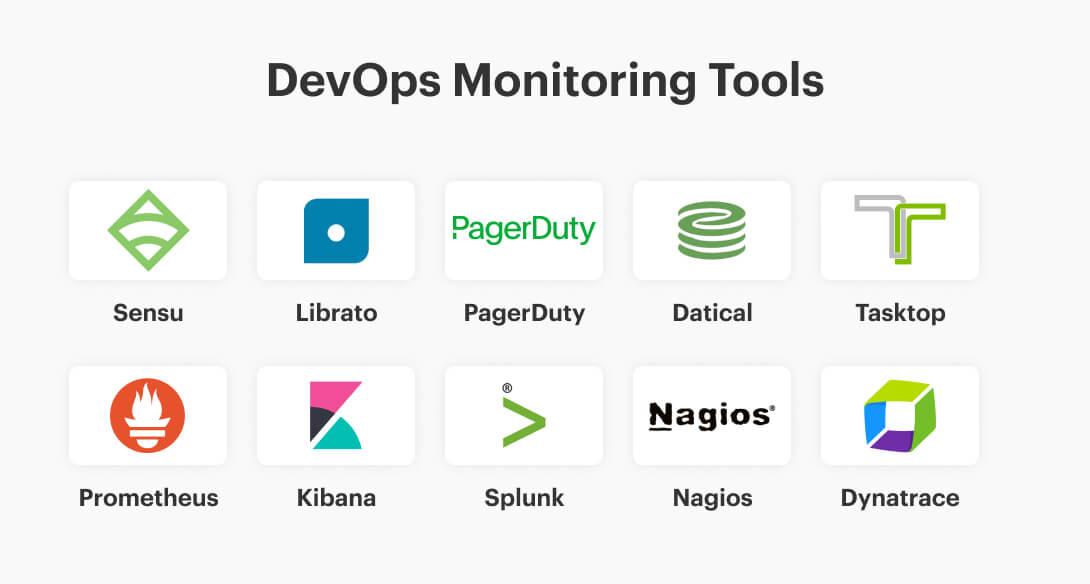
**WHY WE NEED CONTINOUS MONITORING?**

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

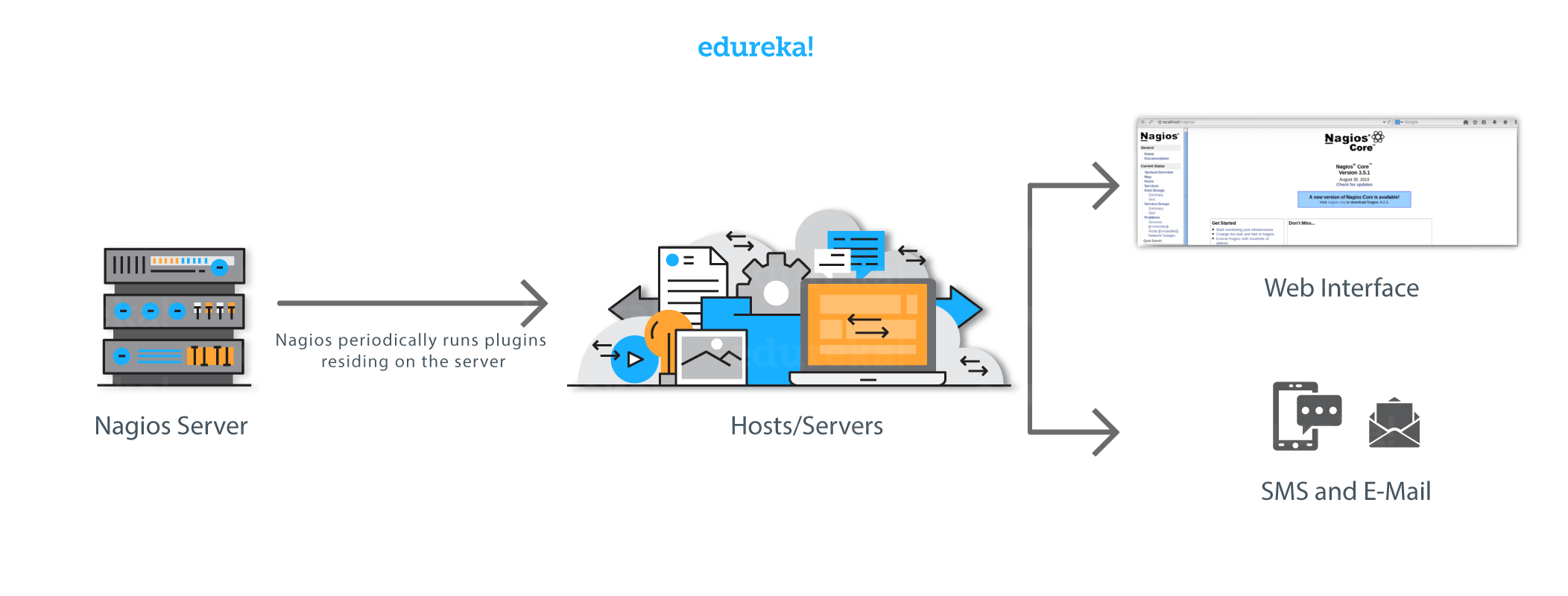
**WHAT IS CONTINOUS MONITORING?**

* Continuous Monitoring is all about the ability of an organization to detect, report, respond, contain and mitigate the attacks that occur, in its infrastructure.
* Security professionals are performing static analysis from – system log, firewall logs, IDS logs, IPS logs etc. But, it did not provide proper analysis and response. Today’s Continuous Monitoring approach gives us the ability to aggregate all of the above events, co-relate them, compare them and then estimate the organization’s risk posture.



WHAT IS NAGIOS?

* 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. With Nagios, you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line.



Get Started with Nagios

---------------------

**Create two AWS instances**.

1st machine name it as -- nagios\_server

2nd machine name it as - server1( remote server which will be monitored. )

**Add security group**

Add 3 rules

-- Custom TCP -- Anywhere

-- HTTP -- Anywhere

-- Custom ICMP V4 -- Anywhere

-------

Installation of nagios

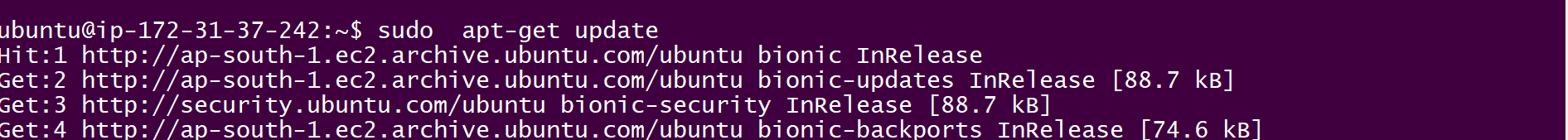
---------------------------

Open gitbash connect to 1st server ( nagios\_server)

Text

Description automatically generated

$ sudo apt-get update



$ sudo apt-get install nagios3

Graphical user interface, text

Description automatically generated

**OK --- OK -- System mail name: ( Just OK )**

**Nagios administration password - archana**

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated

**To check nagios is installed or not?**

**Go to the AWS machine**

**select the public DNS**

**ec2-43-205-99-225.ap-south-1.compute.amazonaws.com/nagios3**

Graphical user interface, text, application

Description automatically generated

Go to newbrowser paste ec2-43-205-99-225.ap-south-1.compute.amazonaws.com/nagios3

Graphical user interface, application

Description automatically generated

**default username - nagiosadmin**

**password – archana**

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated with medium confidence

-----------------------------------

**select services**

**currently , we find only localhost**

-----------------

Graphical user interface, table

Description automatically generated

**To add remote servers to Nagios**

**Go to gitbash**

$ sudo vi /etc/nagios3/nagios.cfg

**check\_external\_command= 1 ( line 145 )**

Text

Description automatically generated

:wq

$ sudo vi /etc/group

**nagios:x:119:www.data ( line 58 )**

Shape, rectangle

Description automatically generated

$ sudo chmod g+w /var/lib/nagios3/rw

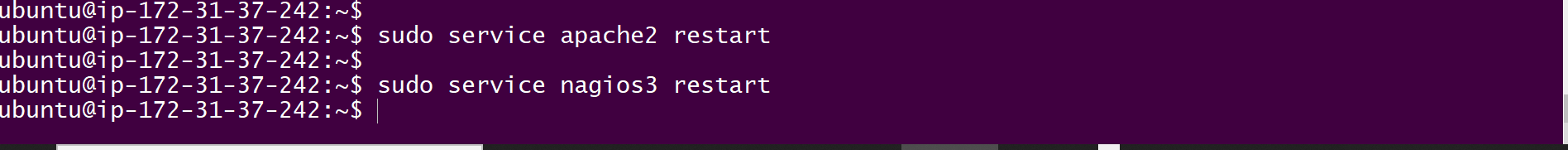
$ sudo chmod g+w /var/lib/nagios3

Text

Description automatically generated

$ sudo service apache2 restart

$ sudo service nagios3 restart

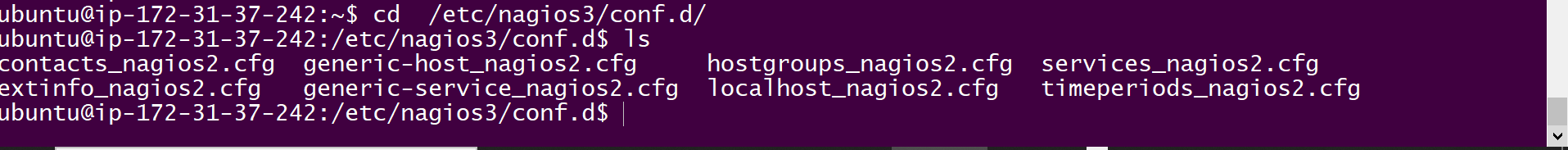


++++++++++++++++++++++++

**Monitor remote serves on nagios**

$ cd /etc/nagios3/conf.d/

$ ls ( we can see the configuration files )



**create a new file**

$ sudo vim server1.cfg

**( In google - adding server to nagios urban penguin)**

**URL -- https://www.theurbanpenguin.com/nagios-defining-a-new-host/**

**change -- host\_name , alias , address ( private\_ip )**

define host {

host\_name ec2-3-110-215-123.ap-south-1.compute.amazonaws.com

alias server1

address 172.31.35.203

max\_check\_attempts 3

check\_period 24x7

check\_command check-host-alive

contacts root

notification\_interval 60

notification\_period 24x7

}

Text

Description automatically generated

**Restart nagios3**

$ sudo /etc/init.d/nagios3 restart

**Go to nagios home page and refresh**

select host groups

We can see the new host.

Graphical user interface, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Application

Description automatically generated with medium confidence

+++++++++++++++++++++