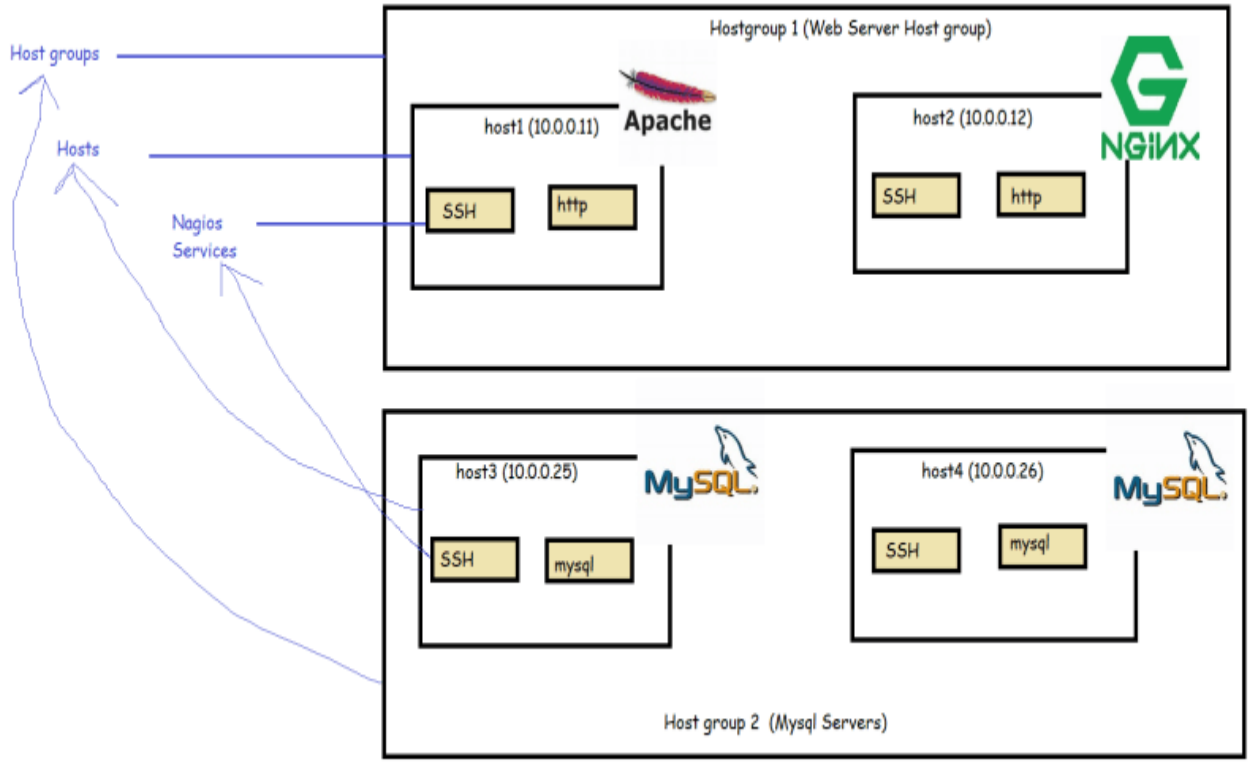
System Monitoring with Nagios

- Nagios is a popular tool for System Monitoring
- System monitoring in Nagios is split into two categories
    - hosts: Represent physical or virtual device (server, router, printer)
    - services: Represents particular functionality of hosts (ssh, http)



- Host groups are logical collection of hosts
- In Nagios when we perform checks it uses four states
    - Ok
    - Warning
    - Critical
    - UnKnown
- To collect the States for the Checks Nagios uses plugins
- Nagios performs all of its checks using plugins. These are external components for which Nagios passes information on what should be checked and what are warning, critical and ok limits are.
- Plugins are responsible for performing the checks and analyzing results. The output from check is status.
- Nagios provides set of standard plugins that allow performance checks for almost all the services. Moreover if you need to perform a specific check, Nagios provides an approach to write your own plugins in any language.

Main features

- Nagios Main strength is flexibility, It has a mechanism to react automatically to problems and a powerful notification system.
- For this flexibility is based on object definition system
- The object definitions are based on few types of objects
    - Commands
    - Time periods
    - Hosts and Host Groups
    - Services
    - Contacts and Contact Groups
    - Notifications

Soft and hard states

- A service is down for a very short time or the test is temporarily failed etc are the normal failures
- When a previous state of check is different from the current one (Critical), Nagios will re test the host or service for a couple of times to make sure change is permanent. Nagios assumes the new result is soft-state, after additional test have verified that the new state is permanent, it is considered to be hard state.

Configuring Nagios

- Nagios stores its configuration in a separate directory. Usually in /etc/nagios or /usr/local/nagios/etc
- The main configuration file is called **nagios.cfg**.
- The syntax in the main nagios configuration file

<parameter>=<value>

- Configuration options: Refer Here for the official docs
- The Nagios option resource_file defines a file to store the user variables. This file can be used to store additional information that can be accessed in all object definitions. These usually contain sensitive data as they can only be used in object definitions

Understanding macro definitions

Macro	Description
HOSTNAME	Short, unique name of the host; maps to host_name directive in the host object
HOSTADDRESS	The IP or hostname of the hosts; maps to address directive in host object
HOSTDISPLAYNAME	Description of host; Maps to the alias directive in host object
HOSTSTATE	The current state of host
HOSTGROUPNAMES	Short names of all host groups a host belongs to (Comma separated)
LASTHOSTCHECK	The date and time of last check of the host (in UNIX timestamp)
LASTHOSTSTATE	The last known state of host
SERVICEDESC	Description of service
SERVICESTATE	The current state of Service
CONTACTNAME	unique name of contact
CONTACTALIAS	Description of Contact
CONTACTEMAIL	The email address of contact
CONTACTGROUPNAME	Short names of all contact groups (comma separated)

Configuring hosts

```
define host {
   host_name       node1
   alias           Node 1 AWS
   address         172.31.29.140
   check_command       check-host-alive
   max_check_attempts    5
   check_interval      5
   retry_interval      1
   check_period        24x7
   notification_period   24x7
   notification_interval  120
   notification_options   d,u,r
   contact_groups      admins  }
```

- Things to know for Nagios configuration
    - Object Definitions
        - Host
        - Host Group
        - Services
        - Commands
        - Contact
        - Templates

Understanding how checks work

- Nagios requires all plugins to follow a specific, easy to follow behaviour
- Nagios relies on exit codes of the Nagios plugins

Exit code	Status	Description
0	OK	Working correctly
1	WARNING	Working but needs attention
2	CRITICAL	Not working or requires attention
3	UNKNOWN	Plugin was unable to determine the status of host or service

- Standard output from command is not parsed by Nagios and is usually formatted in the following way

Configuring Nagios

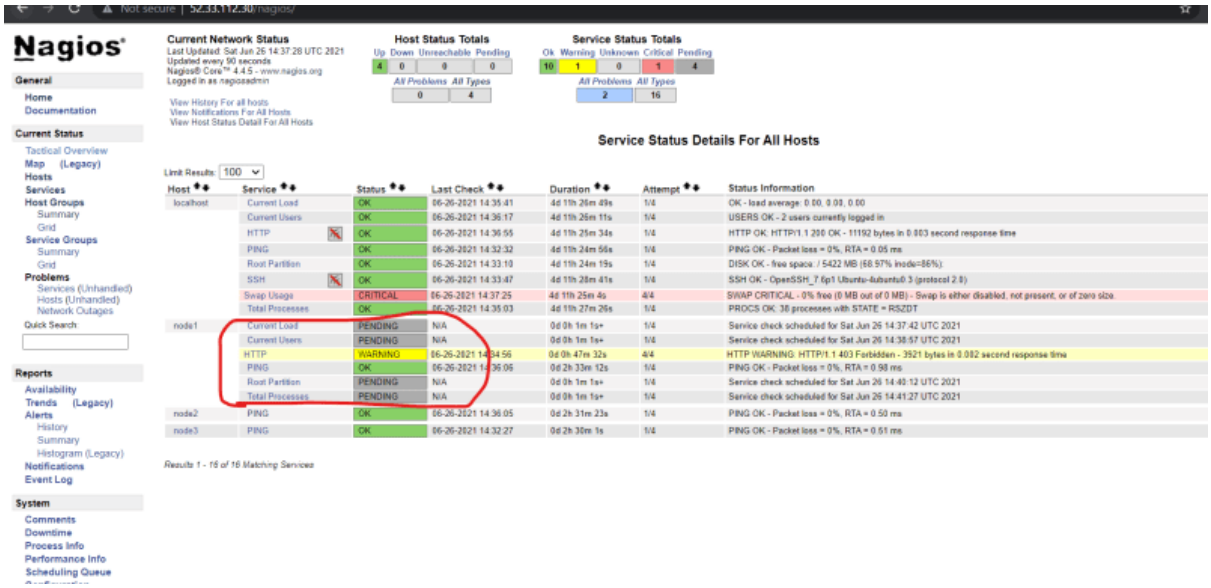
- Create Templates for the below so that we can add all the generic information inside the template
    - host definitions
    - service definitions
- Create Commands and define all the necessary commands for performing checks
- Create hostgroups and add different hosts to host groups (allservers, webservers, dbservers)
- Now create service defintions where we define checks using commands defined at the host group level

Monitoring Remote Hosts

- Remote Checks are usually used in the combination of Nagios plugins package that use either SSH or Nagios Remote Plugin Executor (NRPE)
- Monitoring over SSH
    - Install nagios plugins on the remote servers
    - Nagios offers a check_by_ssh plugin that takes the hostname and actual command to run on the remote server
    - switch to nagios user
    - Configure SSH Connection by using ssh_keys

```
root@ip-172-31-18-72:~# sudo -i
root@ip-172-31-18-72:~# su -s /bin/bash
root@ip-172-31-18-72:~# su -s /bin/bash nagios
nagios@ip-172-31-18-72:/root$ cd ~
nagios@ip-172-31-18-72:~$ pwd
/home/nagios
nagios@ip-172-31-18-72:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nagios/.ssh/id_rsa):
Created directory '/home/nagios/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nagios/.ssh/id_rsa.
Your public key has been saved in /home/nagios/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:jNjy51miSbdyYGItC6s4+Yaz/VeUp842yLhWSK9WokE nagios@ip-172-31-18-72
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|         .       |
|  E .o oo .      |
| . .o+o.So       |
|  o *oB o        |
| o * %o*+ .      |
|*.+ *.=**=       |
|+Bo+ooo++.       |
+----[SHA256]-----+
```

services.cfg - mynagioscfg - Vis... nagios5.md - Classroomnotes - ...



- Monitoring using NRPE:
  - overview