Nagios Monitoring

@CHAITANYA R GAAJULA

Monitoring

- System Monitoring is crucial in an organization's mission critical system
- Monitoring alerts system admins about a problem in the system beforehand
- It enables you to take preventive measures before any issue affects the system
- Monitoring is essential in ensuring System availability
  - Keeping track of the status of a system
  - For Example:- Server Disk Space, file system status, status changes in the services etc

Benefits of Monitoring

- It helps in getting rid of periodic testing
- It detects split-second failures when the wrist strap is still in the “intermittent” stage
- It reduces maintenance cost without sacrificing performance
- It provides timely notification to the management of control and breakdown

Why Use Monitoring Tools

- 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 troubleshoot server performance issues

Nagios

“It is an open source continuous monitoring tool which monitors network, applications and servers.”

- It allows you to detect and repair problems and mitigate future issues before they affect end-users and customers
- It is developed for monitoring servers, applications and networks
- It provides a centralized view of your entire IT infrastructure and detailed up-to-date status information

Features of Nagios

Detailed Monitoring

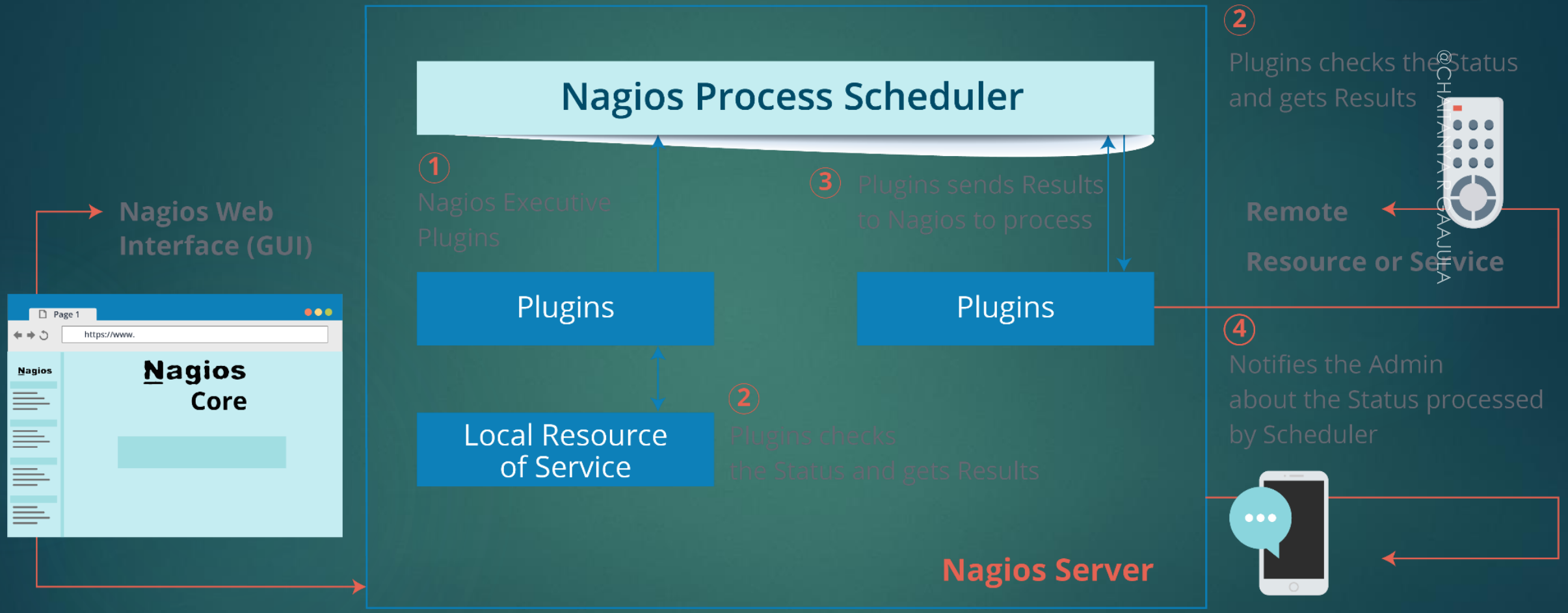
Good Community Support

Fast And Reliable

Extendable Architecture

Extended reporting

Nagios Architecture



Nagios Composition

Plugins

- Standalone extensions for Nagios
- They check a service and return results to the Nagios server

Scheduler

- Server part of Nagios
- Checks Plugins at regular intervals

GUI

- Interface of Nagios

Nagios Plugins

- Plugins are compiled executables or scripts(Perl or non-Perl) that extends Nagios functionality to monitor servers and hosts
- Nagios will execute a Plugin to check the status of a service or host
- Nagios can be compiled with support for an embedded Perl interpreter to execute Perl plugins
- Without it, Nagios executes Perl and non-Perl plugins by forking and executing the plugins as an external command

Types of Nagios Plugins

Official Nagios Plugins

- There are 50 official Nagios Plugins
- Official Nagios plugins are developed and maintained by the official Nagios Plugins Team

Community Plugins

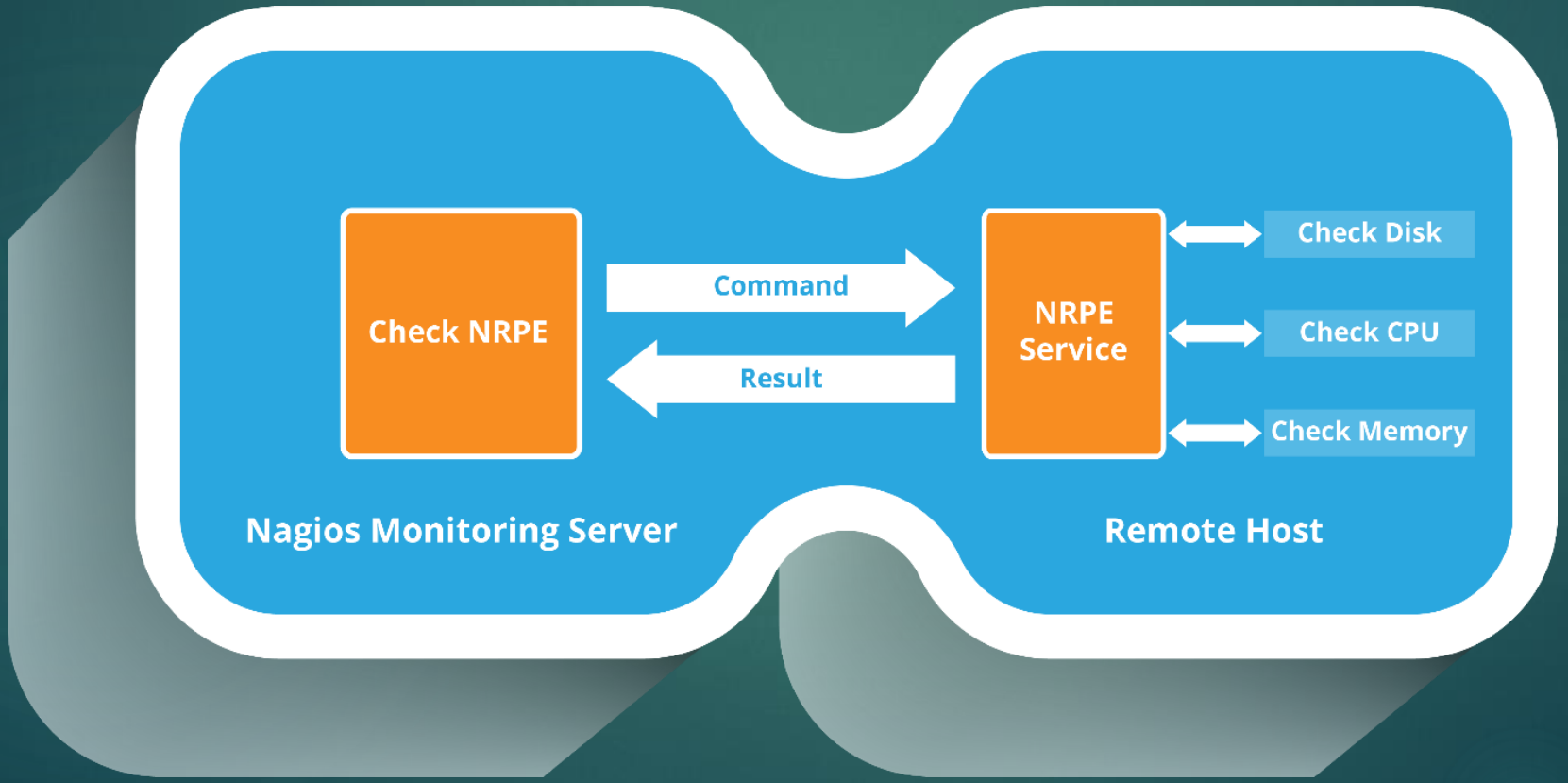
- There are over 3,000 third party Nagios plugins that have been developed by Nagios community members

Custom Plugins

- You can also write your own Custom Plugins
- There are certain guidelines that must be followed to write Custom Plugins.

Nagios Remote Plugin Executor (NRPE)

- NRPE allows you to remotely execute Nagios plugins on other Linux/Unix machines. This allows you to monitor remote machine metrics such as disk usage, CPU load etc
- It can communicate with some of the Windows agent addons, so you can execute scripts and check metrics on remote Windows machines as well



Nagios Remote Data Processor

- Nagios Remote Data Processor (NRDP) is an agent which allows flexible data transport
- It uses standard protocols such as:

NSClient ++ Agent

- NSClient++ is mainly used to monitor Windows machines
- It is used to monitor CPU and disk usage
- Nagios polls the plugin which listens on port 12489

Nagios Objects

Type of Object	Description
Services	Services are associated with attributes(CPU load, disk usage) and services (HTTP, POP3, FTP) provided by hosts
Service Groups	Service Groups are groups of one or more services
Hosts	A Host is a physical server, workstation, device, etc. that resides on your network.
Host Groups	Host Groups are groups of one or more hosts
Contacts	Contacts are people involved in the notification process who receive notifications for hosts and services they are responsible for
Contact Groups	Contact Groups are groups of one or more contacts
Commands	Used to tell Nagios what programs, scripts, etc. it should execute to perform.
Time Periods	A Time Period is a list of times during various days that are considered to be "valid" times for notifications and service checks of hosts and services

Nagios Configuration Files

- Nagios.cfg is the main configuration file.
- Individual object config files can be specified in Nagios.cfg
  - services.cfg
  - hosts.cfg
  - contacts.cfg
  - checkcommands.cfg
  - misccommands.cfg
  - timeperiods.cfg

Nagios Service Checks

- Service states are the mirror of what Nagios observes
- States: OK, WARNING, CRITICAL, UNKNOWN
- Transitions from one state to another one based on results provided by checks
- Critical and warning states are shadowed by related *soft* states
- A service goes first to a *soft* state
- Attempt count mechanism to reach a definitive *hard* state
- User notification can only occur when *hard* states are reached

Nagios State Types: Soft State

- The states type plays an important role in monitor logic, and help to decide event handlers execution when notifications are initially sent out.
- There are two types of states in Nagios:
- Soft State:
- The following things occur when hosts or services experience SOFT state changes:
  - Log of soft state is created
  - To manage soft state, event handlers are executed

Nagios State Types: Hard State

The following things occur when hosts or services experience HARD state changes:

- Log of Hard state is created
- To manage Hard state, event handler are executed
- Host or service problem or recovery is notified to contacts

Nagios Command

- A command definition defines a command
- Commands include service checks, service notifications, service event handlers, host checks, host notifications, and host event handlers
- Format for defining of a Command:

```
define command{
command_name      command_name
command_line      command_line
          }
```

Command name- This directive is used to identify the command. It is referenced in contact, host, and service definitions

Command line- This directive is used to define what is actually executed by Nagios when the command is used for service or host checks, notifications, or event handlers.

- Command definitions for Nagios are defined in commands.cfg file

Nagios Command Example


```
define command{
        command_name    check_ssh

        command_line    /usr/lib/nagios/plugins/check_ssh '$HOSTADDRESS$'
}
```

Name of the command

This command will execute the plugin: /usr/libl/nagios/plugins/check_ssh with 1 parameter : '$HOSTADDRESS$'

```
define command{
        command_name    check_pop

        command_line    /usr/local/nagios/libexec/check_pop '$HOSTADDRESS$'
        }
```

Notifications in Nagios

- The decision to send out notifications is made in the service check and host check logic
- Each host and service definition has a <*contact_groups*> option that specifies what contact groups receive notifications for that particular host or service
- There are several filters that notifications encounters before reaching to the receiver

Prerequisites for delivering notification

- Nagios supports optional detection of hosts and services that are "flapping"
- Flapping occurs when a service or host changes state too frequently, resulting a problem and recovery notifications

Nagios Notification Methods

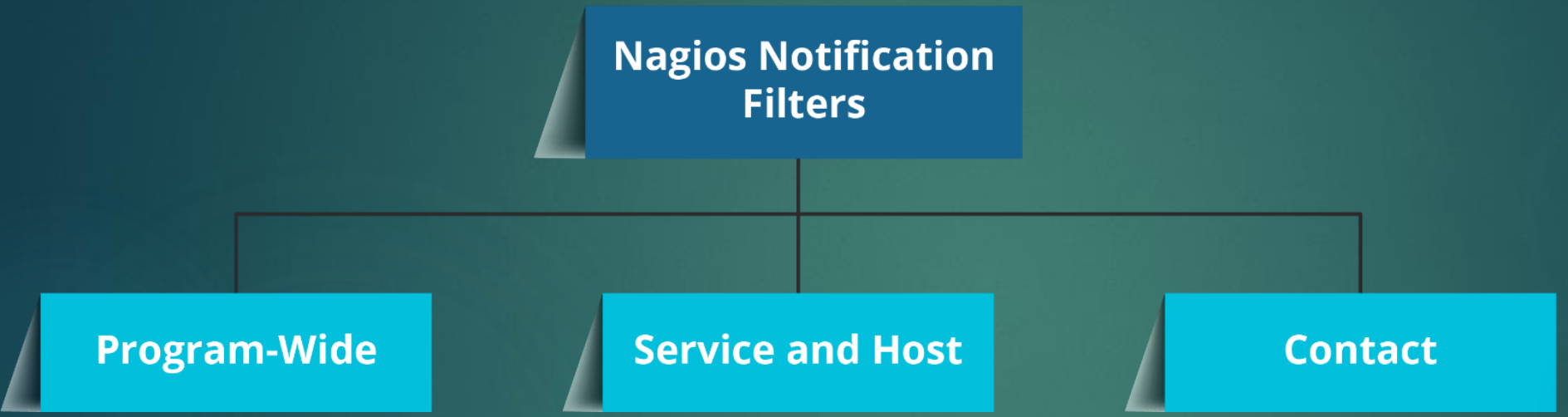
- There are many ways through which Nagios notifies about a problem or recovery

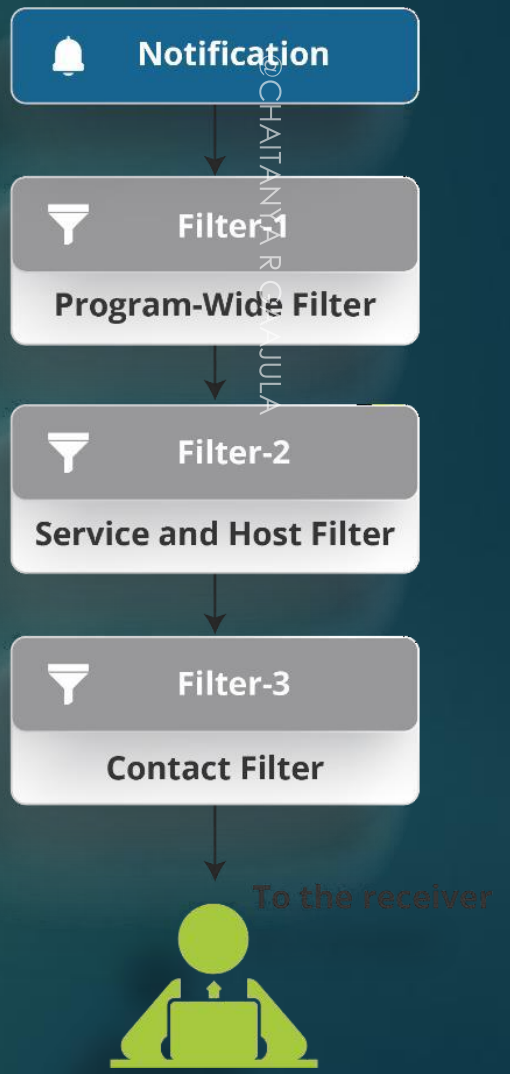
  Example: Mail, Instant message, Audio alert etc.

- How notifications are sent depend on the notification commands that are defined in your object definition files
- While writing your notification commands, you need to take into account what type of notification is occurring
- The $NOTIFICATIONTYPE$ macro (macroinstruction)contains a string that identifies the type of notification occurring

Nagios Notification Filters

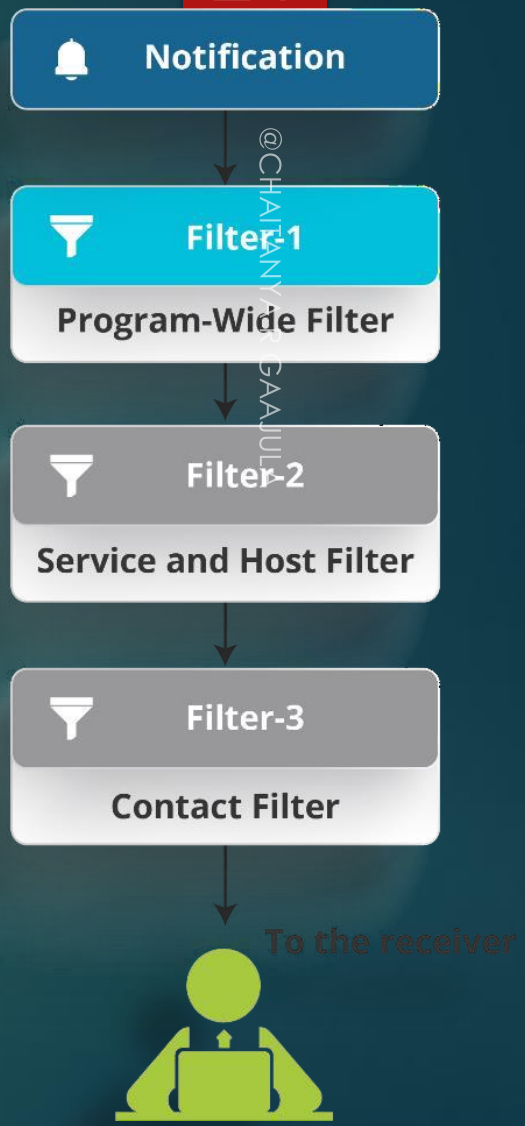
- A notification must pass through these filters before they are eligible enough to be sent out to the receiver





Program Wide Filters

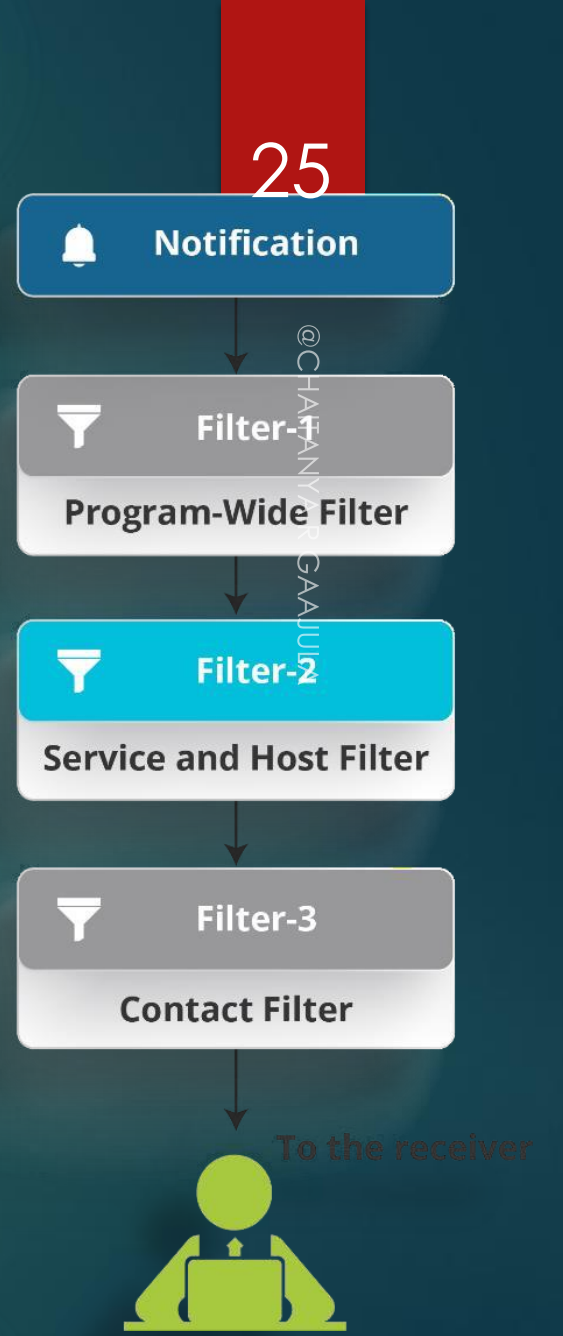
- Filter to test of whether or not notifications are enabled on a program-wide basis
- This is initially determined by the enable_notifications directive in the main config file
- If notifications are disabled on a program-wide basis, no host or service notifications can be sent out or else notifications move to the next filter



Service & Host Filters

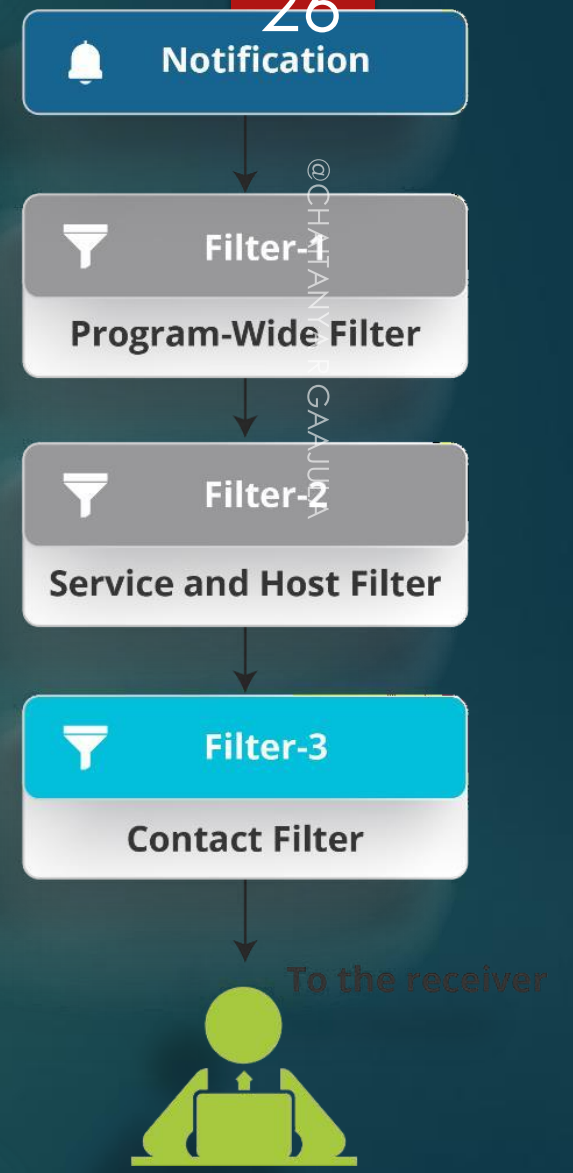
- This filter is a check to see if
  - The host or service is in a period of scheduled downtime
  - The host or service is flapping
  - Notifications can be sent out for warning states, critical states, and recoveries
  - Notifications fall in valid notification time period

- Scheduled downtime- Scheduled periods of planned downtime for hosts and service that you're monitoring.
- This is an event of taking a server down for an upgrade, etc.



Contact Filter

- At this point the notification has passed the program mode filter and all host or service filters and Nagios starts to notify all the people it should
- Contact filters are specific to each contact and do not affect other contacts receive notifications



Macro Values

Value	Description
PROBLEM	A service or host has just entered (or is still in) a problem state. If this is a service notification, it means the service is either in a WARNING, UNKNOWN or CRITICAL state. If this is a host notification, it means the host is in a DOWN or UNREACHABLE state.
RECOVERY	A service or host recovery has occurred
ACKNOWLEDGEMENT	This notification is an acknowledgement notification for a host or service problem.
FLAPPINGSTART	The host or service has just started flapping
FLAPPINGSTOP	The host or service has just stopped flapping.
FLAPPINGDISABLED	The host or service has just stopped flapping because flap detection was disabled..
DOWNTIMESTART	The host or service has just entered a period of scheduled downtime. Future notifications will be suppressed.
DOWNTIMESTOP	The host or service has just exited from a period of scheduled downtime. Notifications about problems can now resume.
DOWNTIMECANCELLED	The period of scheduled downtime for the host or service was just cancelled. Notifications about problems can now resume.

Nagios Host & Host Groups


```
define host{
        use                     windows-server  ; Inherit default values from a template
        host_name               DESKTOP-38ICBQG ; The name we're giving to this host
        alias                   My Windows Server       ; A longer name associated with the host
        address                 192.168.2.69    ; IP address of the host
        }
```

```
define hostgroup{
        hostgroup_name  windows-servers ; The name of the hostgroup
        alias           Windows Servers ; Long name of the group
        }
```

Nagios Service

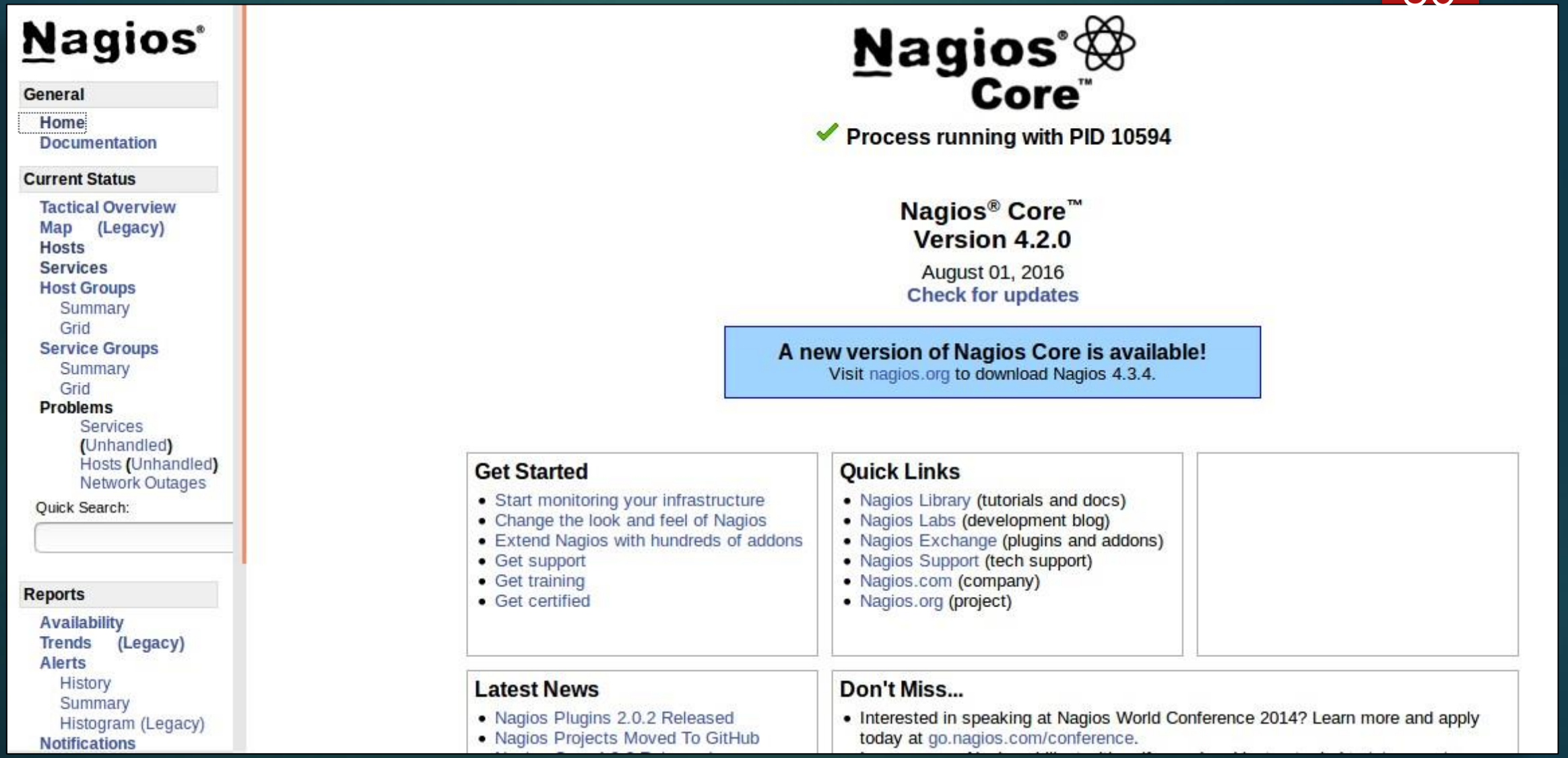

```
define service{
        use                             generic-service
        host_name                       DESKTOP-38ICBQG
        service_description             Uptime
        check_command                   check_nt!UPTIME
        }
```

Types of Nagios services

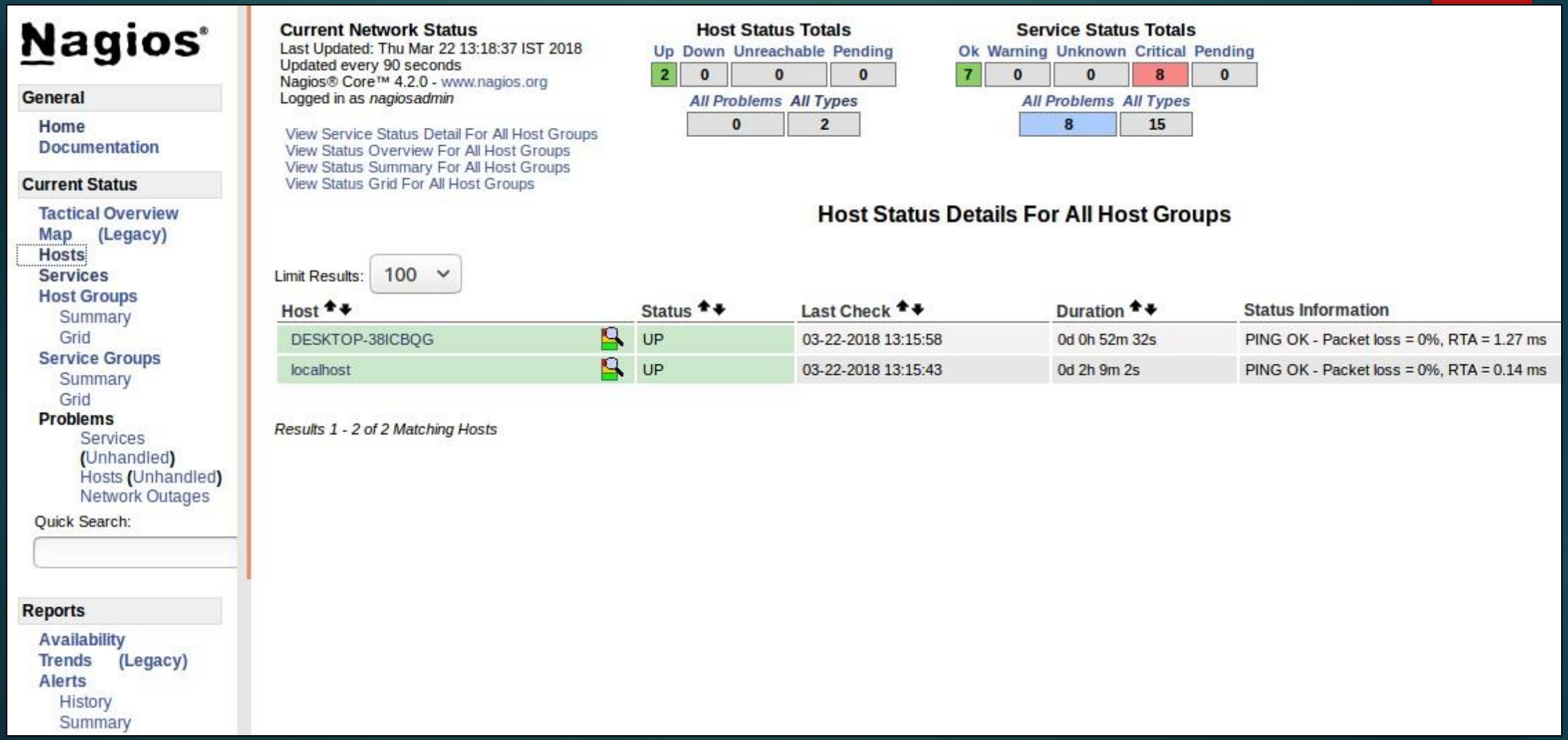
```
define service{
        use                             generic-service
        host_name                       DESKTOP-38ICBQG
        service_description             CPU Load
        check_command                   check_nt!CPULOAD!-l 5,80,90
        }
```

```
define service{
        use                             generic-service
        host_name                       DESKTOP-38ICBQG
        service_description             C:\ Drive Space
        check_command                   check_nt!USEDDISKSPACE!-l c -w 80 -c 90
        }
```

Nagios GUI Web Console



Nagios Server : Hosts



Nagios Server : Services

Nagios®

General
- Home
- Documentation

Current Status
- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

Reports
- Availability
- Trends (Legacy)
- Alerts
  - History
  - Summary

Current Network Status
Last Updated: Thu Mar 22 15:48:36 IST 2018
Updated every 90 seconds
Nagios® Core™ 4.2.0 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	0	8	0

All Problems	All Types
8	15

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
DESKTOP-38ICBQG	C:\ Drive Space	CRITICAL	03-22-2018 15:41:56	0d 2h 10m 39s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	CPU Load	CRITICAL	03-22-2018 15:42:56	0d 2h 9m 40s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Explorer	CRITICAL	03-22-2018 15:43:55	0d 2h 8m 41s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Memory Usage	CRITICAL	03-22-2018 15:44:53	0d 2h 7m 43s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	NSClient++ Version	CRITICAL	03-22-2018 15:45:52	0d 2h 6m 44s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Uptime	CRITICAL	03-22-2018 15:46:51	0d 2h 5m 45s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	W3SVC	CRITICAL	03-22-2018 15:47:49	0d 2h 4m 47s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
localhost	Current Load	OK	03-22-2018 15:46:27	0d 3h 27m 9s	1/4	OK - load average: 0.50, 0.52, 0.50
	Current Users	OK	03-22-2018 15:47:05	0d 3h 26m 31s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	03-22-2018 15:47:42	0d 3h 25m 54s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.003 second response time
	PING	OK	03-22-2018 15:48:20	0d 3h 25m 16s	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	03-22-2018 15:43:57	0d 3h 24m 39s	1/4	DISK OK - free space: / 9557 MB (55% inode=78%):
	SSH	CRITICAL	03-22-2018 15:47:35	0d 3h 24m 1s	4/4	connect to address 127.0.0.1 and port 22: Connection refused
	Swap Usage	OK	03-22-2018 15:45:11	0d 3h 23m 24s	1/4	SWAP OK - 58% free (1180 MB out of 2045 MB)
	Total Processes	OK	03-22-2018 15:45:50	0d 3h 22m 46s	1/4	PROCS OK: 55 processes with STATE = RSZDT

Results 1 - 15 of 15 Matching Services

THANK YOU