IntelliGrape | TO THE NEW

Nagios®

The Industry Standard In IT Infrastructure Monitoring

Who are using Nagios

Agenda

- What is Nagios
- What can you do with Nagios
- Features
- Basic
  - Architecture
  - Terminology
- Monitoring
- State Types
- Active / Passive Checks
- Reports

What is Nagios Core

Open Source system and network monitoring application

With Nagios you can

- Monitor your entire IT infrastructure
- Spot problems before they occur
- Know immediately when problems arise
- Share availability data with stakeholders
- Detect security breaches
- Plan and budget for IT upgrades
- Reduce downtime and business losses

Features

- Monitoring of network services
  - SMTP
  - POP3
  - HTTP
  - PING and more
- Monitoring of host resources
  - Processor load
  - Disk usage and more
- Simple plugin design that allows users to easily develop their own service checks
- Parallelized service checks

Features

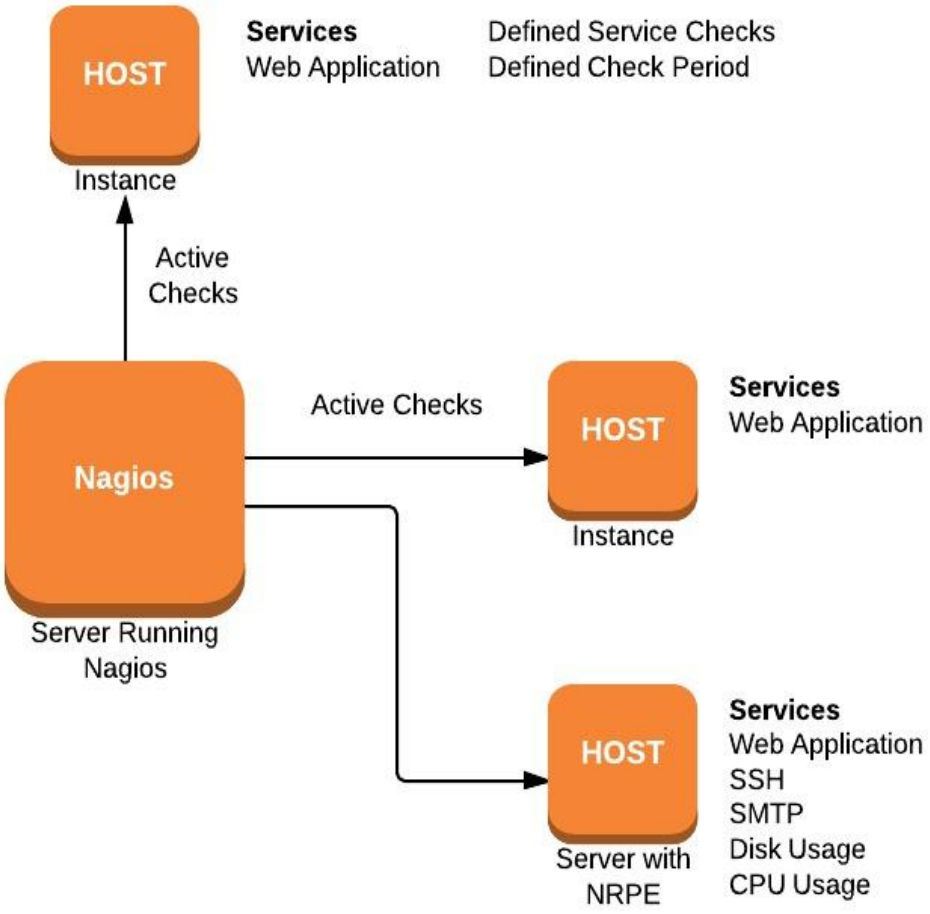
- Ability to define network host hierarchy/groups
- Allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved via
  - Email
  - Pager
  - or user-defined methods
- Ability to define event handlers to be run during service or host events for proactive problem resolution

Features

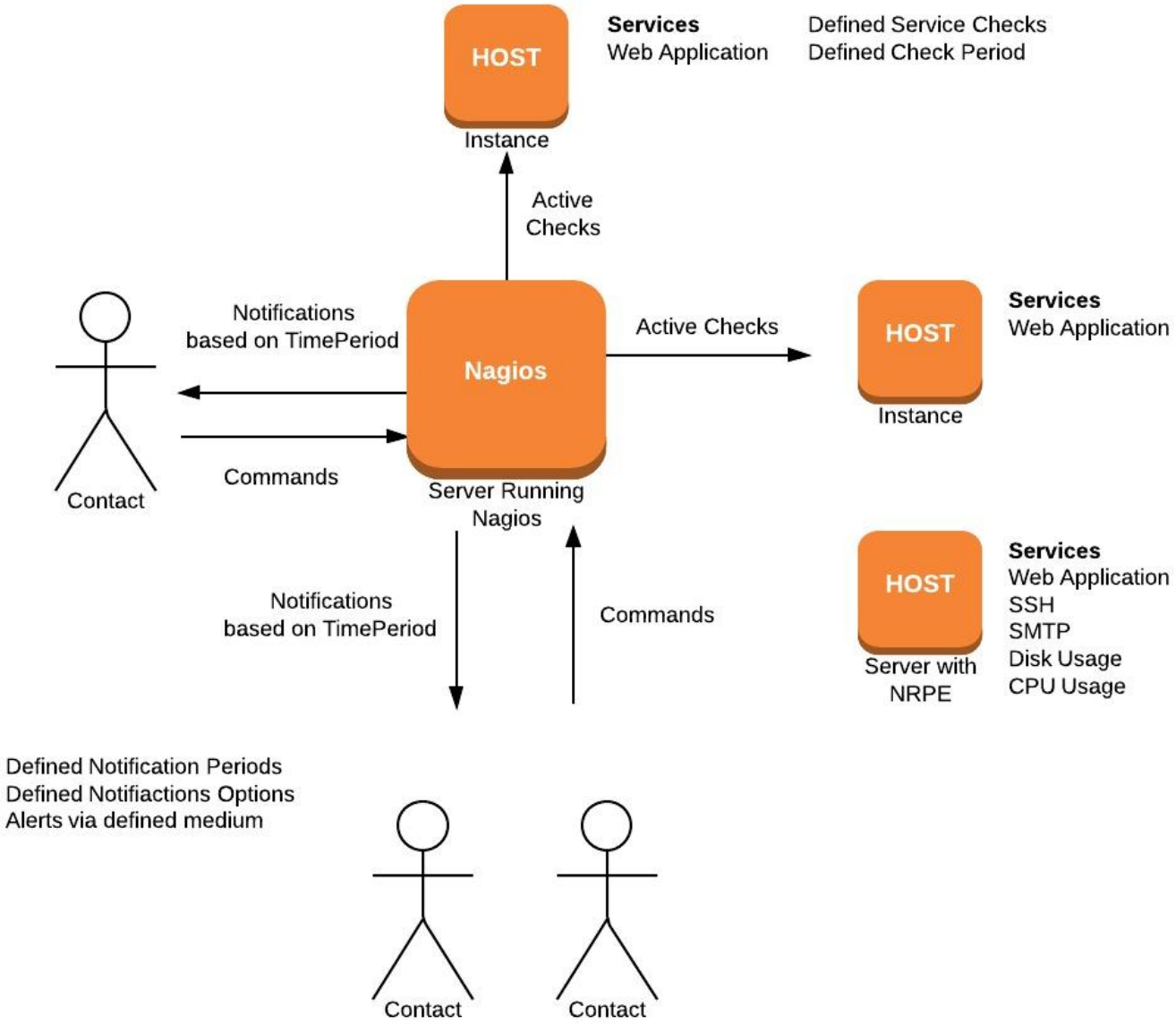
- Automatic log file rotation
- Support for implementing redundant monitoring hosts
- Optional web interface for viewing
  - Current network status
  - Notification
  - Problem history
  - Log file and more

Basics

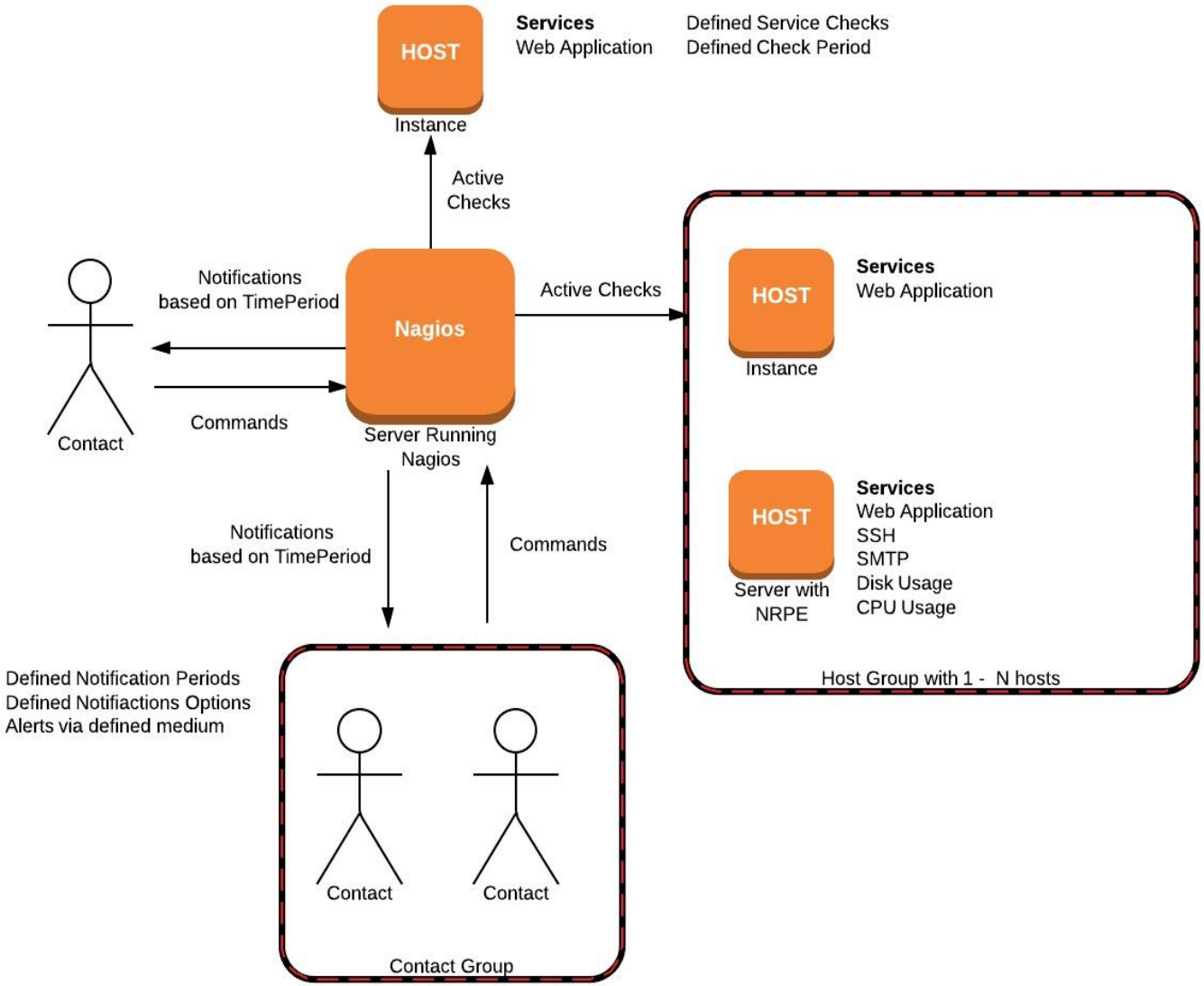
Basics


HOST
Instance
Services
Web Application
Defined Service Checks
Defined Check Period
Active
Checks
Nagios
Server Running
Nagios
Active Checks
HOST
Instance
Services
Web Application
HOST
Server with
NRPE
Services
Web Application
SSH
SMTP
Disk Usage
CPU Usage

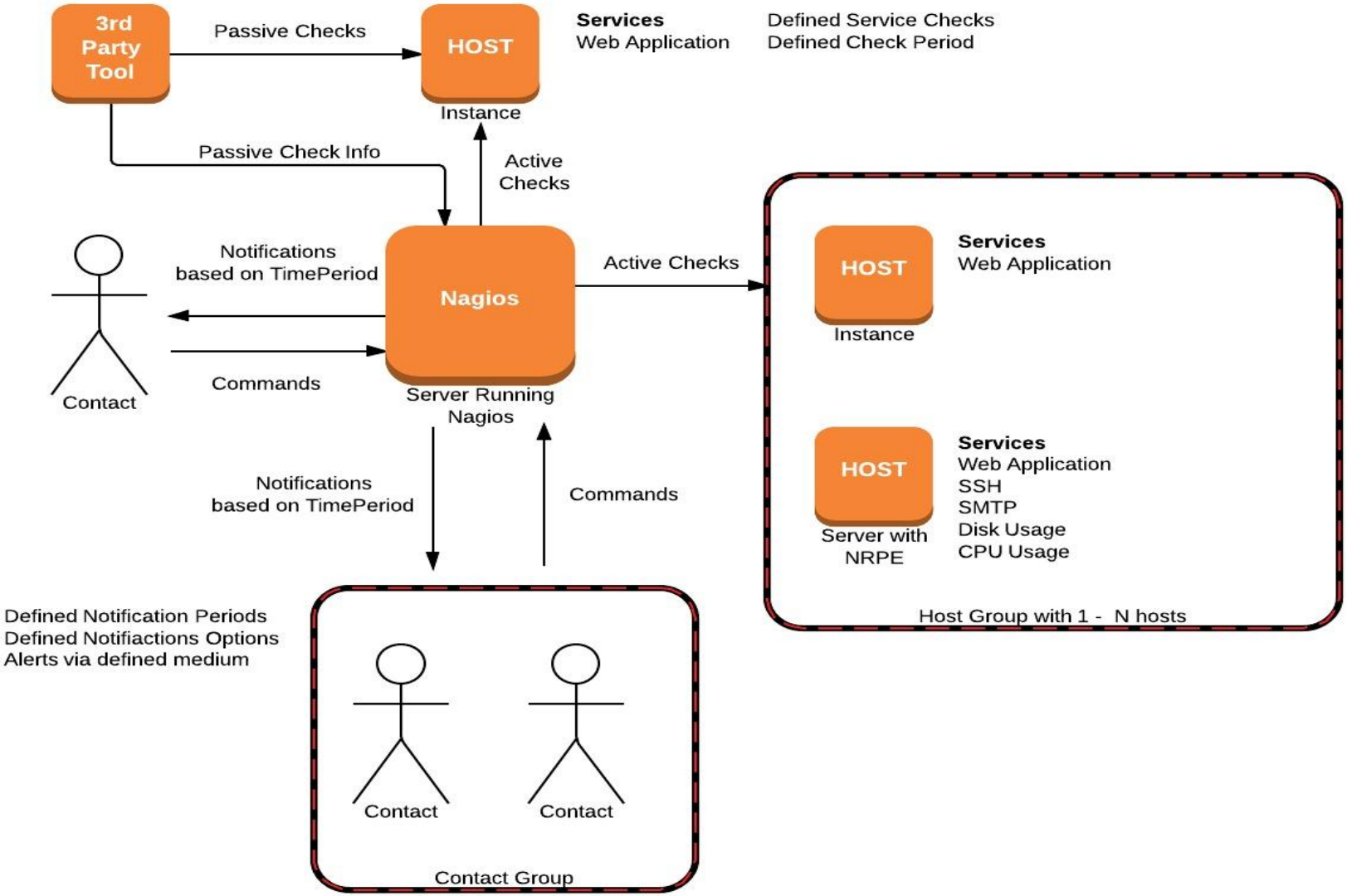
Basics


HOST
Instance
Services
Web Application
Defined Service Checks
Defined Check Period
Active
Checks
Notifications
based on TimePeriod
Nagios
Active Checks
HOST
Instance
Services
Web Application
Contact
Commands
Server Running
Nagios
Notifications
based on TimePeriod
Commands
HOST
Server with
NRPE
Services
Web Application
SSH
SMTP
Disk Usage
CPU Usage
Defined Notification Periods
Defined Notifiactions Options
Alerts via defined medium
Contact
Contact

Basics


HOST
Instance
Services
Web Application
Defined Service Checks
Defined Check Period
Active
Checks
Notifications
based on TimePeriod
Nagios
Server Running
Nagios
Active Checks
Commands
Contact
HOST
Instance
Services
Web Application
HOST
Server with
NRPE
Services
Web Application
SSH
SMTP
Disk Usage
CPU Usage
Host Group with 1 - N hosts
Notifications
based on TimePeriod
Commands
Defined Notification Periods
Defined Notifiactions Options
Alerts via defined medium
Contact
Contact
Contact Group

Basics


3rd Party Tool
Passive Checks
HOST
Instance
Services
Web Application
Defined Service Checks
Defined Check Period
Passive Check Info
Active Checks
Contact
Notifications based on TimePeriod
Commands
Nagios
Server Running Nagios
Active Checks
HOST
Instance
Services
Web Application
HOST
Server with NRPE
Services
Web Application
SSH
SMTP
Disk Usage
CPU Usage
Host Group with 1 - N hosts
Notifications based on TimePeriod
Commands
Defined Notification Periods
Defined Notifiactions Options
Alerts via defined medium
Contact
Contact
Contact Group

Basics

Definitions

- Host
- Service
- Contacts
- Commands
- TimePeriod
- Eventhandlers

Basics

Host

Defines a physical server, workstation, device, etc. that resides on your network.

Host Status Totals

Up	Down	Unreachable	Pending
12	1	0	0

All Problems	All Types
1	13

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
192.168.4.18	DOWN	08-29-2014 09:51:11	0d 0h 37m 42s	CRITICAL - 192.168.4.18: rta nan, lost 100%
Firewall	UP	08-29-2014 09:51:29	0d 0h 40m 27s+	OK - 127.0.0.1: rta 0.039ms, lost 0%
NOAA	UP	01-02-2012 15:44:09	1169d 12h 39m 44s	HTTP OK HTTP/1.1 200 OK - 99753 bytes in 0.478 seconds
Router	UP	08-29-2014 09:46:48	0d 0h 40m 27s+	OK - 127.0.0.1: rta 0.048ms, lost 0%
localhost	UP	08-29-2014 09:47:28	1661d 6h 37m 25s	OK - 127.0.0.1: rta 0.046ms, lost 0%
secure.nagios.com	UP	08-29-2014 09:50:16	1496d 4h 13m 18s	HTTP OK: HTTP/1.1 302 Found - 530 bytes in 0.084 second response time
testbpi	UP	08-29-2014 09:49:58	0d 0h 44m 47s	OK: BPI
vs1.nagios.org	UP	08-29-2014 09:48:09	1517d 22h 22m 28s	OK - vs1.nagios.org: rta 0.332ms, lost 0%
www.acme.com	UP	08-29-2014 09:48:33	1483d 15h 12m 3s	OK - 216.27.178.28: rta 61.483ms, lost 0%
www.chaoticmoon.com	UP	08-29-2014 09:49:15	1484d 2h 49m 21s	HTTP OK: HTTP/1.1 200 OK - 50458 bytes in 0.269 second response time
www.cnn.com	UP	08-29-2014 09:49:33	1523d 14h 21m 28s	HTTP OK: HTTP/1.1 200 OK - 126517 bytes in 0.172 second response time
www.nagios.com	UP	08-29-2014 09:50:28	1494d 6h 57m 38s	HTTP OK: HTTP/1.1 200 OK - 54443 bytes in 0.666 second response time
www.twitter.com	UP	08-29-2014 09:50:59	1483d 15h 11m 17s	HTTP OK: HTTP/1.1 301 Moved Permanently - 270 bytes in 0.104 second response time

Basics

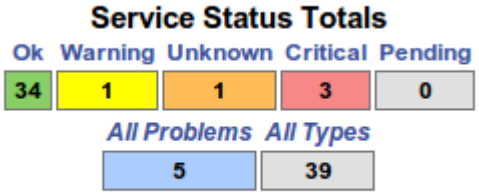
Host

```
define host{
        host_name                       remotehost
        alias                           some Remote Host
        address                         192.168.1.50
        contacts                        admin
        max_check_attempts              3
        check_period                    24x7
        notification_interval           60
        notification_period             24x7
}
```

Basics

Service

- Its a service that runs on the host.
- Actual service on the host like POP, SMTP, HTTP, etc.)
- Metric associated with the host (response to a ping, number of logged in users, free disk space, etc.



Basics

Service

Host	Status	Last Check	Duration	Status Information
Firewall	UP	08-29-2014 11:06:54	0d 0h 6m 4s+	OK - 127.0.0.1: rta 0.045ms, lost 0%
NOAA	UP	01-02-2012 15:44:09	1169d 13h 55m 50s	HTTP OK HTTP/1.1 200 OK - 99753 bytes in 0.478 seconds
Router	UP	08-29-2014 11:07:08	0d 0h 6m 4s+	OK - 127.0.0.1: rta 0.033ms, lost 0%
localhost	UP	08-29-2014 11:07:29	1661d 7h 53m 31s	OK - 127.0.0.1: rta 0.049ms, lost 0%
secure.nagios.com	UP	08-29-2014 11:05:35	1496d 5h 29m 24s	HTTP OK: HTTP/1.1 302 Found - 530 bytes in 0.063 second response time
vs1.nagios.org	UP	08-29-2014 11:03:26	1517d 23h 38m 34s	OK - vs1.nagios.org: rta 0.324ms, lost 0%
www.acme.com	UP	08-29-2014 11:04:08	1483d 16h 28m 9s	OK - 216.27.178.28: rta 53.859ms, lost 0%
www.chaoticmoon.com	UP	08-29-2014 11:04:35	1484d 4h 5m 27s	HTTP OK: HTTP/1.1 200 OK - 50640 bytes in 0.242 second response time

Basics

Service

```
define service {
        host_name                       linux-server
        service_description             check-disk-sda1
        check_command                   check-disk!/dev/sda1
        max_check_attempts              5
        check_interval                  5
        retry_interval                  3
        check_period                    24x7
        notification_interval           30
        notification_period             24x7
        notification_options            w,c,r
        contact_groups                  admins
}
```

Basics

Contacts

Identify someone who should be contacted in the event of a problem.

```
define contact{
        contact_name                    admin
        alias                           admin
        host_notifications_enabled      1
        service_notifications_enabled   1
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,u,r
        service_notification_commands   notify-by-email
        host_notification_commands      host-notify-by-email
        email                           admin@organisation.com
        address1                        abc.def@organisation.com
}
```

Basics

Commands

```
define command{
        name                    check_http
        command_name            check_http
        command_line            $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
}
```

```
define host {
        ..
        address 192.168.1.50
        ..
}
```

```
define service {
  ..
  check_command  check-disk!/dev/sda1
  ..
}
```

Basics

Time Period
Valid times for notifications and service checks.

```
define timeperiod{
        timeperiod_name         nonworkhours
        alias                   Non-Work Hours
        sunday                  00:00-24:00 week
        monday                  00:00-09:00,17:00-24:00
        tuesday                 00:00-09:00,17:00-24:00
        wednesday               00:00-09:00,17:00-24:00
        thursday                00:00-09:00,17:00-24:00
        friday                  00:00-09:00,17:00-24:00
        saturday                00:00-24:00
}
```

Event Handlers

Event handlers are optional system commands (scripts or executables) that are run whenever a host or service state change occurs.

- Restarting a failed service
- Entering a trouble ticket into a helpdesk system
- Logging event information to a database
- Cycling power on a host

Event Handlers

Event handlers are executed when a service or host:

- Is in a SOFT problem state
- Initially goes into a HARD problem state
- Initially recovers from a SOFT or HARD problem state

```
define service {
  ..
     event_handler command_name
     event_handler_enabled [0/1]
  ..
}
```

Basics

Other Blocks

- contactgroup
- servicegroup
- servicedependency
- serviceescalation
- serviceextinfo
- hostdependency
- hostescalation
- hostextinfo

Monitoring Services

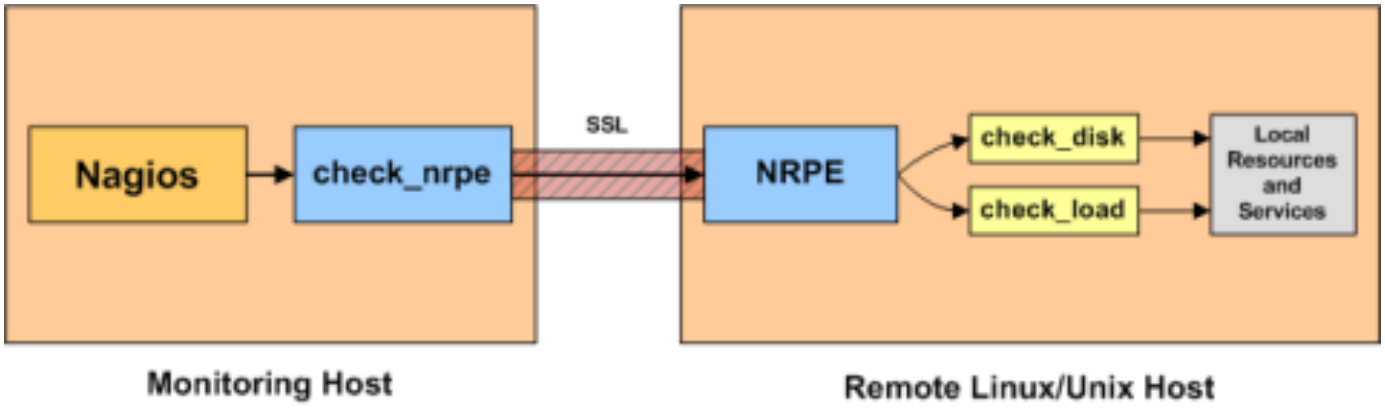
Nagios can be used to monitor Public and Private Services

- Private Services
  - CPU load
  - Memory usage
  - Disk usage
  - Logged in users
  - Running processes

- Publicly available services that are provided by Linux servers
  - HTTP
  - FTP
  - SSH
  - SMTP

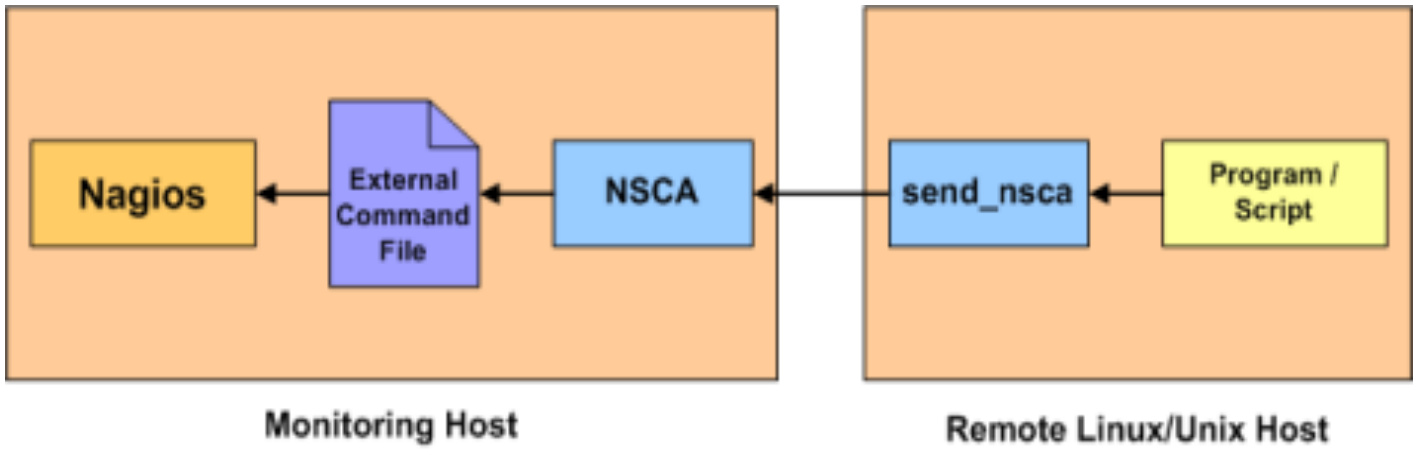
Monitoring Private Services

- Plugins/Addons are mostly used for monitoring private services.
- NRPE addon is installed on the target servers (Nagios Remote Plugin Executor)
- Its is an addon that allows you to execute plugins on remote Linux/Unix hosts



Monitoring Private Services

- NCSA addon (Nagios Service Check Adapter))
- Allows you to send passive check results from remote Linux/Unix to the Nagios daemon running on the monitoring server.
- This is very useful in distributed and redundant/failover monitoring setups.



Monitoring Public Services

- Check plugins first @ Nagios Exchange

- Walk through

  - Create host in file within cfg dir
  - Define Service for each process/service that needs to be monitored.
  - Service uses pre-defined/custom defined commands.
  - Define contacts who would receive notifications and take action.

State Types

- Based on variable *max_check_attempts*
- The SOFT state is logged, when
  - Number of checks haven't completed yet
- When a service or host recovers from a soft error. This is considered a soft recovery.

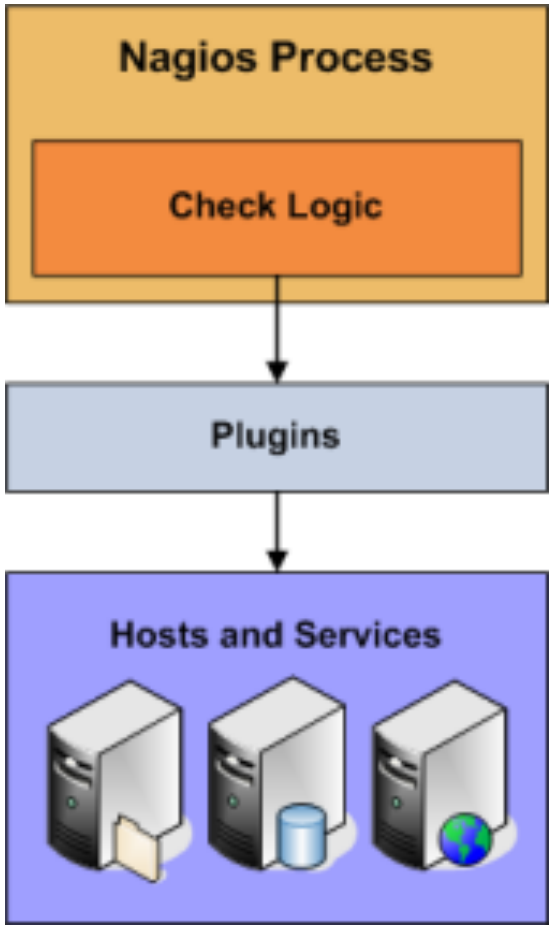
State Types

- HARD state is logged, when
  - Number of checks have completed
- When a host or service transitions from one hard error state to another error state (e.g. WARNING to CRITICAL).
  - ex. Running to Down
- When a service check results in a non-OK state and its corresponding host is either DOWN or UNREACHABLE.
- When a host or service recovers from a hard error state. This is considered to be a hard recovery.
- Contacts are notified of the host or service problem or recovery.

Active / Passive Checks

Active Checks

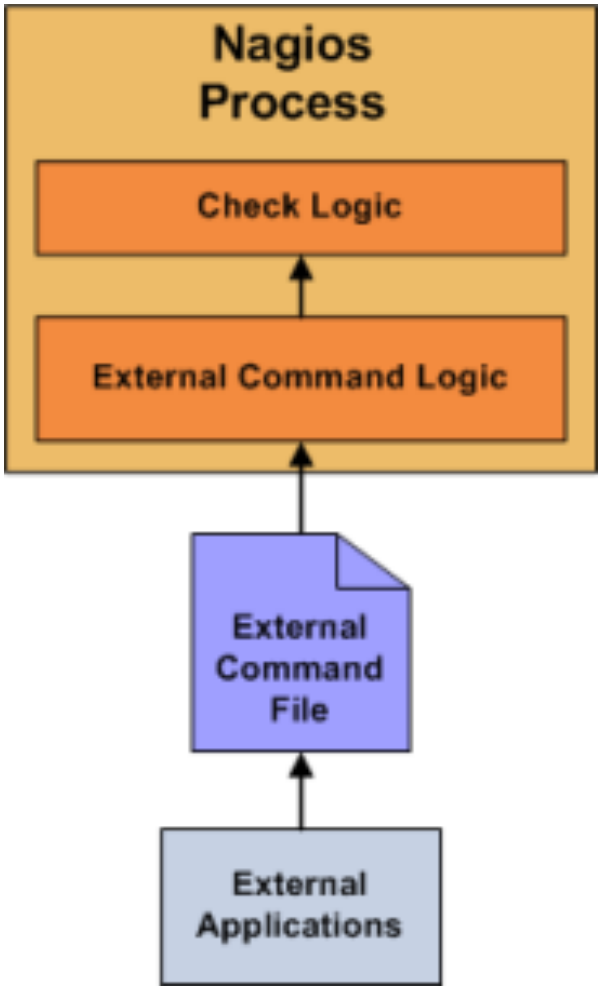
- Initiated by the Nagios process
- Ran on a regularly scheduled basis



Active / Passive Checks

Passive Checks

- Passive checks are initiated and performed by external applications/processes
- Passive check results are submitted to Nagios for processing
- Used for
  - Checks that are asynchronous in nature
  - Located behind a firewall and cannot be checked actively from the monitoring host



Nagios in Action

Demo Time：http://nagioscore.demos.nagios.com/

Reports

- ## Availability Report

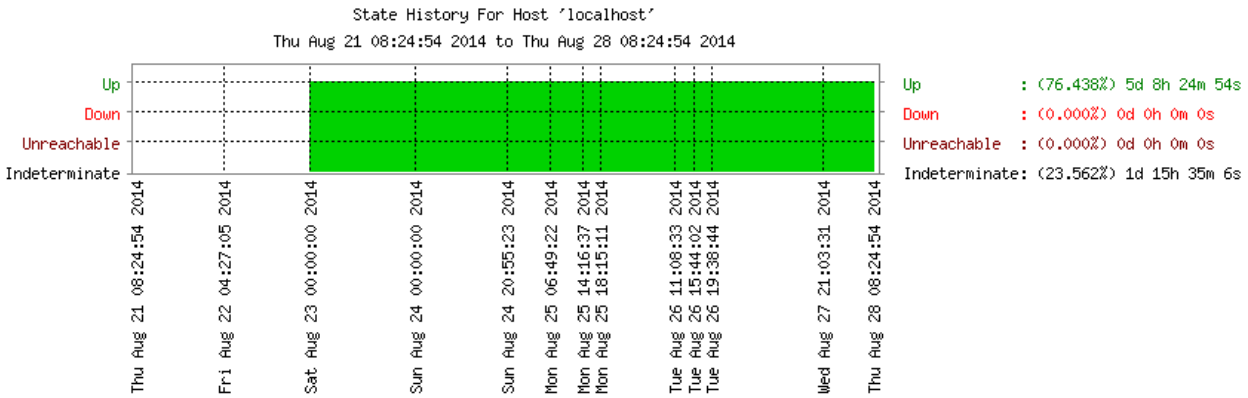
  Report for uptime and services

Hostgroup 'all' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
localhost	76.405% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	23.595%
wordpress-machine	22.756% (99.811%)	0.043% (0.189%)	0.000% (0.000%)	77.201%
wordpress-second	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
Average	33.053% (66.604%)	0.014% (0.063%)	0.000% (0.000%)	66.932%

- ## Trends Report

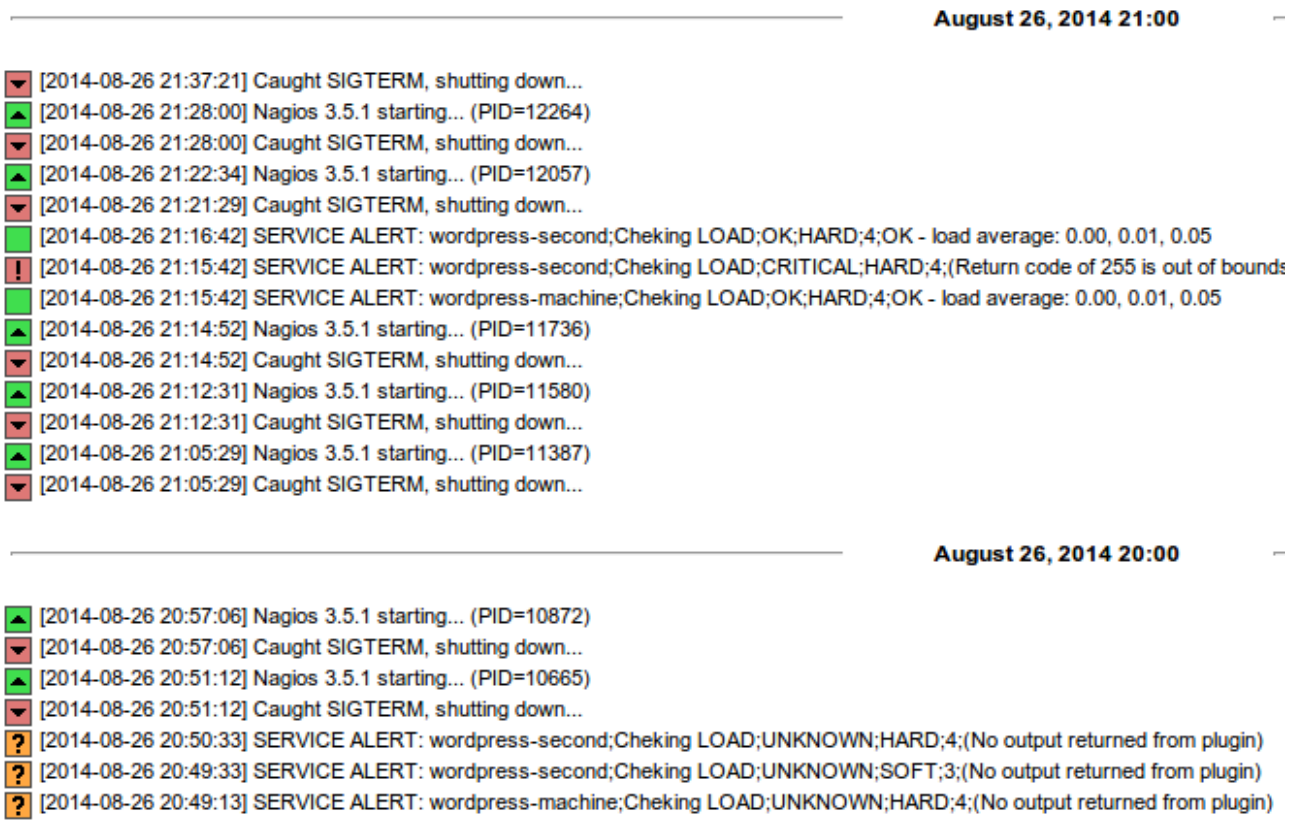
  Graphical breakdown of of state of particular host, service.



Reports

- Alert History Report

  Record of historical alerts



Reports

- Alert Summary Report

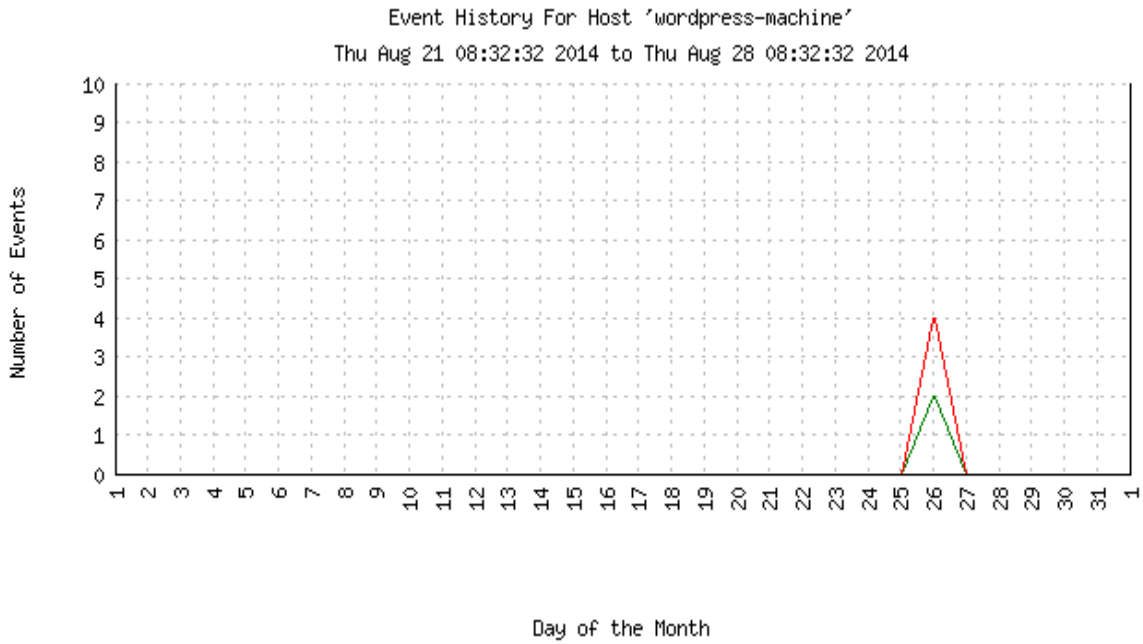
Displaying most recent 25 of 29 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
2014-08-26 21:16:42	Service Alert	wordpress-second	Cheking LOAD	OK	HARD	OK - load average: 0.00, 0.01, 0.05
2014-08-26 21:15:42	Service Alert	wordpress-second	Cheking LOAD	CRITICAL	HARD	(Return code of 255 is out of bounds)
2014-08-26 21:15:42	Service Alert	wordpress-machine	Cheking LOAD	OK	HARD	OK - load average: 0.00, 0.01, 0.05
2014-08-26 20:50:33	Service Alert	wordpress-second	Cheking LOAD	UNKNOWN	HARD	(No output returned from plugin)
2014-08-26 20:49:33	Service Alert	wordpress-second	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 20:49:13	Service Alert	wordpress-machine	Cheking LOAD	UNKNOWN	HARD	(No output returned from plugin)
2014-08-26 20:48:33	Service Alert	wordpress-second	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 20:48:13	Service Alert	wordpress-machine	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 20:47:33	Service Alert	wordpress-second	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 20:47:13	Service Alert	wordpress-machine	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 20:46:13	Service Alert	wordpress-machine	Cheking LOAD	UNKNOWN	SOFT	(No output returned from plugin)
2014-08-26 19:59:54	Service Alert	wordpress-second	Cheking SSH Service	OK	HARD	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
2014-08-26 19:58:24	Service Alert	wordpress-machine	Cheking SSH Service	OK	HARD	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
2014-08-26 19:44:54	Service Alert	wordpress-second	Cheking SSH Service	CRITICAL	HARD	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:43:54	Service Alert	wordpress-second	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:43:24	Service Alert	wordpress-machine	Cheking SSH Service	CRITICAL	HARD	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:42:54	Service Alert	wordpress-second	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:42:24	Service Alert	wordpress-machine	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:41:54	Service Alert	wordpress-second	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:41:24	Service Alert	wordpress-machine	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 19:40:24	Service Alert	wordpress-machine	Cheking SSH Service	CRITICAL	SOFT	CRITICAL - Socket timeout after 10 seconds
2014-08-26 18:07:48	Host Alert	wordpress-machine	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 0.59 ms

Reports

- Alert Histogram Report

  Frequency graph of host and service alerts



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	2	2	0.06
Down:	0	4	4	0.13
Unreachable:	0	0	0	0.00

Reports

- ## Notification Report

  Provides historical record of notifications sent to contacts

File: /var/log/nagios3/nagios.log

Host	Service	Type	Time	Contact	Notification Command	Information
wordpress-second	Cheking LOAD	OK	2014-08-26 21:16:42	hitesh	notify-service-by-email	OK - load average: 0.00, 0.01, 0.05
wordpress-second	Cheking LOAD	OK	2014-08-26 21:16:42	root	notify-service-by-email	OK - load average: 0.00, 0.01, 0.05
wordpress-second	Cheking LOAD	CRITICAL	2014-08-26 21:15:42	hitesh	notify-service-by-email	(Return code of 255 is out of bounds)
wordpress-second	Cheking LOAD	CRITICAL	2014-08-26 21:15:42	root	notify-service-by-email	(Return code of 255 is out of bounds)
wordpress-machine	Cheking LOAD	OK	2014-08-26 21:15:42	hitesh	notify-service-by-email	OK - load average: 0.00, 0.01, 0.05
wordpress-machine	Cheking LOAD	OK	2014-08-26 21:15:42	root	notify-service-by-email	OK - load average: 0.00, 0.01, 0.05
wordpress-second	Cheking LOAD	UNKNOWN	2014-08-26 20:50:33	hitesh	notify-service-by-email	(No output returned from plugin)
wordpress-second	Cheking LOAD	UNKNOWN	2014-08-26 20:50:33	root	notify-service-by-email	(No output returned from plugin)
wordpress-machine	Cheking LOAD	UNKNOWN	2014-08-26 20:49:13	hitesh	notify-service-by-email	(No output returned from plugin)
wordpress-machine	Cheking LOAD	UNKNOWN	2014-08-26 20:49:13	root	notify-service-by-email	(No output returned from plugin)
wordpress-second	Cheking SSH Service	OK	2014-08-26 19:59:54	hitesh	notify-service-by-email	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
wordpress-second	Cheking SSH Service	OK	2014-08-26 19:59:54	root	notify-service-by-email	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
wordpress-machine	Cheking SSH Service	OK	2014-08-26 19:58:24	hitesh	notify-service-by-email	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
wordpress-machine	Cheking SSH Service	OK	2014-08-26 19:58:24	root	notify-service-by-email	SSH OK - OpenSSH_5.9p1 Debian-5ubuntu1.4 (protocol 2.0)
wordpress-second	Cheking SSH Service	CRITICAL	2014-08-26 19:44:54	hitesh	notify-service-by-email	CRITICAL - Socket timeout after 10 seconds
wordpress-second	Cheking SSH Service	CRITICAL	2014-08-26 19:44:54	root	notify-service-by-email	CRITICAL - Socket timeout after 10 seconds
wordpress-machine	Cheking SSH Service	CRITICAL	2014-08-26 19:43:24	hitesh	notify-service-by-email	CRITICAL - Socket timeout after 10 seconds
wordpress-machine	Cheking SSH Service	CRITICAL	2014-08-26 19:43:24	root	notify-service-by-email	CRITICAL - Socket timeout after 10 seconds
wordpress-machine	N/A	HOST UP	2014-08-26 18:07:48	hitesh	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 0.59 ms
wordpress-machine	N/A	HOST UP	2014-08-26 18:07:48	root	notify-host-by-email	PING OK - Packet loss = 0%, RTA = 0.59 ms
wordpress-machine	N/A	HOST DOWN	2014-08-26 18:03:28	hitesh	notify-host-by-email	PING CRITICAL - Packet loss = 100%
wordpress-machine	N/A	HOST DOWN	2014-08-26 18:03:28	root	notify-host-by-email	PING CRITICAL - Packet loss = 100%

Summary

- Infra monitoring
- Anomaly Outage detection
- Automatic Problem remedy
- Schedule Downtime
- Outage Alerts
- Alert Escalations
- Historical Reporting
- Maintenance Planning

Advice for Beginners

- Relax - it's going to take some time.
- Use the quickstart instructions.
- Read the documentation.
- visiting the Nagios Support Forum at http://support.nagios.com/forum/.

Next Steps

- Get your hands dirty
- Get training
  Live / Self paced training
- Get certified
  Nagios Certified Professional
  Nagios Certified Administrator
- Use it to Monitor your infra.

References

- Nagios Documentation
- Nagios Online Demo
- Slideshare
- NRPE Blog

Thank You