CitiusTech

IT Monitoring with Nagios

This CPD gives an insight on significance of IT Monitoring using Nagios

Author Sagar Shah

Reviewed by Manisha Bafna

Keyword Nagios

Contents

Background

- **Why Monitoring**
  - To anticipate and resolve issues before they're problems
  - To maximize return on network investments for business application delivery
  - To make staff more effective
  - To ensure quality and service levels
- Various tools and products are already available in the Market that can help you monitor entire IT Infrastructure
- Nagios is one of such tools that offers various products in this area

Contents

Nagios Products

- **Nagios XI**
  - Most powerful IT infrastructure monitoring and alerting solution
  - Goes beyond basic IT monitoring capabilities
- **Nagios Fusion**
  - Provides an ability to quickly identify and solve the problems on an infrastructure-wide basis before they affect critical business processes
- **Nagios Incident Manager**
  - An enterprise-class incident management application that allows teams and individuals to track and solve problems faster using a powerful web-based application that offers security, mobility, third-party integration, and tools for collaboration
- **Nagios Network Analyzer**
  - Provides network traffic & bandwidth information for entire IT infrastructure, making it easier to ensure that systems, applications, services, and business processes are functioning properly
- **Nagios Core**
  - The highly awarded, industry standard Open Source core for IT infrastructure monitoring

Contents

About Nagios Core

- An Industry standard, Open Source IT monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes
- Foundation for Commercial products of Nagios like Nagios – XI
- Provides a set of core commands to monitor few of the services
- Extensible architecture facilitating developers to write their own plugins for custom monitoring
- Plugin guidelines have been well defined to ensure that all plugins follow same standards
- Bunch of plugins are already available & published on Nagios

Contents

Nagios Core - Features

- **Comprehensive Monitoring:** Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, system metrics, and network infrastructure
- **Visibility:** Provides central view of your entire IT operations network and business processes
- **Awareness:** Alerts are delivered to IT staff via email and SMS
- **Problem Remediation:** Event handlers allow you to automatically restart failed applications, services, servers, and devices when problems are detected
- **Extendable Architecture:** Provides easy integration with in-house and third-party applications. Hundreds of community-developed addons extend the core functionality
- **Reports:** Ensure SLAs are being met, provides historical records of outages, notifications, and alert response for later analysis

Contents

Existing Plugins

- Bunch of plugins have already been published under various groups to monitor on various protocols, databases, devices, servers, etc.

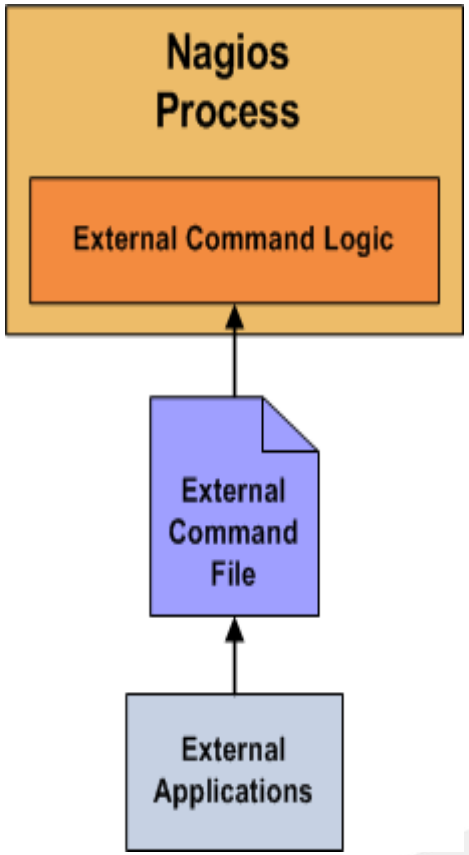
  - **Network Protocols:** DHCP, IMAP & POP3, SMTP, FTP, TCP & UDP, HTTP, etc.
  - **Databases:** MySQL, Postgres, SQLServer, etc.
  - **Java applications & servers:** Apache Tomcat, WebLogic, JBOSS, ActiveMQ, etc.
  - **Hardware:** Printers, UPS, Mobile Devices, Storage Systems, etc.
  - **Operating Systems:** Windows, Mac OS, Linux, Solaris, etc.
  - **Security:** Firewall, VPN, etc.

And many more available at http://exchange.nagios.org/directory/Plugins …

Contents

Nagios Core Configuration (1/2)

- It is deployable on linux system
- It also includes CGI script for accessing application over browser to monitor the statistics and data
- It allows running commands from an external system as well
- It allows easy configuration of services, hosts, printers, switches, routers, etc. for monitoring
- Based on all configuration parameters, it will keep on monitoring specific services on configured hosts and store the results in file system (configurable)
- It supports extensible set of plugins offering good monitoring tools for various devices, services and hosts



Nagios Core Configuration (2/2)

- Listed below are the important configuration files for Nagios core
  - nagios.cfg – This file contains overall configuration for nagios system including log file, other configuration files related to commands, contacts, object cache, etc.
  - objects.cache – Object definitions are cached in this file by default when restarting Nagios server
  - status.dat – This file contains statistics about monitored systems, services and devices. This file contains all information about what is being monitored and results of monitoring of the specific services
  - nagios.cmd – This is the file that Nagios checks for external command requests

Contents

Other Monitoring Tools & Comparison (1/2)

- **Microsoft Network Monitor**
  - Allows you to capture, view and analyze network traffic
- **BandwidthD**
  - Monitors TCP/IP network usage and displays the data it has gathered in the form of graphs and tables over different time periods
- **EasyNetMonitor**
  - Super lightweight tool for monitoring local and remote hosts to determine if they are alive or not.
  - Useful for monitoring critical servers from your desktop, allowing you to get immediate notification
- **Fiddler**
  - Web debugging tool that captures HTTP traffic between chosen computers and the Internet. It allows you to analyze incoming and outgoing data to monitor and modify requests and responses before they hit the browser

Other Monitoring Tools & Comparison (2/2)

Nagios	Other Tools
Generic Solution for almost entire IT monitoring. It helps in monitoring of various applications, services and devices	Specific solution to monitor a specific area of entire IT infrastructure For example, • Microsoft Network Monitor allows to capture, view and analyze network traffic. • Fiddler acts as a good Web debugging tool that captures HTTP traffic
Extensible architecture with the help of plugins that can be developer/customized to monitor services/devices as per IT need	Not extensible or have limited capabilities
Overall a good choice to monitor different applications built using different technologies using standard plugins	Have to use different tools for monitoring different areas of IT infrastructure

Contents

References

http://www.nagios.com/products/nagioscore

http://exchange.nagios.org/directory/Plugins

http://en.wikipedia.org/wiki/Nagios

https://www.nagios-plugins.org/doc/guidelines.html

http://nagios.sourceforge.net/docs/3_0/quickstart-fedora.html

Contents

Configuration Example (1/5)

- **hosts.cfg – Defines all the hosts and host groups**

```
define host {
        host_name               MyLocalHostName
        use                     linux-server
        alias                   LOCAL HOST
        address                 127.0.0.1
}

define hostgroup {
        hostgroup_name          local-host-group
        alias                   Local HOST GROUP
        members                 MyLocalHostName
}
```

- Above example configures just one host 127.0.0.1 and one host group, which includes this single host (127.0.0.1).
- Multiple hosts can be included in single host group by using comma separated list for the members attribute

Configuration Example (2/5)

- **services.cfg – Defines all the services to be monitored on configured host groups**

```
define service {
        name                    disk-service
        use                     local-service
        service_description     checks disk space
        check_command           check_local_disk!250000!250000!/dev
        hostgroup_name          local-host-group
}
```

- Above example defines a service named disk-service that monitors local disk storage space using check_local_disk command on all the hosts that are members of local-host-group host group.

Configuration Example (3/5)

- **Status.dat containing monitoring statistics**

```
servicestatus {
        host_name=MyLocalHostName
        service_description=Checks disk space
        modified_attributes=0
        check_command=check_local_disk!250000!250000!/dev
        check_interval=5.000000
        retry_interval=1.000000
        current_state=2
        current_event_id=4
        current_problem_id=3
        last_time_ok=1379430545
        last_time_warning=0
        last_time_unknown=0
        last_time_critical=1379602950
        plugin_output=DISK CRITICAL-free space:/15897  MB (82% inode=90%):
        last_check=1379602950
        next_check=1379603250
}
```

Snapshot of Monitoring with Nagios XI (4/5)

Monitoring capabilities of Nagios XI (5/5)

Nagios XI - Features

Nagios®

Technical Features

Network Monitoring

- TCP/UDP Port
- SMTP
- POP3
- IMAP
- HTTP(S)
- FTP
- SSH
- DNS
- DHCP
- SNMP
- Bandwidth
- Port State
- and more...

Operating System Monitoring

- Windows
- Linux
- Unix

Hardware Monitoring

- Routers
- Switches
- Firewalls
- Servers
- Workstations
- Printers
- Environmental Devices
- Generic Network Elements

Website Monitoring

- Web Content
- Web Transactions
- FQDNS / IP Match
- SSL Certificates
- HTTP(S)

Reporting

- SLA availability reports
- Alert and notification history
- Trending reports
- Performance graphs

Notifications

- Email
- Mobile text
- Custom script

Extendable

- Hundreds of community-developed addons and scripts extend native capabilities

More

- Multi-tenant/multi-user capabilities
- Notification escalations
- Scheduled downtime
- Acknowledge problems online

System Requirements

Server Operating System

- **Virtual Hosts:**
  - VMware Player, Workstation
  - VMware Server, ESX
  - Microsoft Virtual PC
  - Microsoft Virtual Server
- **Linux:**
  - RHEL 5/6 (32-bit/64-bit)
  - CentOS 5/6 (32-bit/64-bit)

Server Hardware

- 1 GHz CPU, 1024 MB RAM (minimum)
- 2 GHz+ CPU, 2 GB+ RAM (recommended)

Server Storage

- 1 GB free space (minimum)
- 4 GB free space (recommended)

Browsers

- Firefox 4.0+
- Internet Explorer 9+
- Safari 2.0+

Client Operating Systems

- **Windows**: Windows 2000, XP, 2003, Vista, 7
- **Max**: OS/X
- **Linux/Unix**: 2.4+ kernel Linux distributions, Solaris 9+ , FreeBSD 6.4+, AIX 5.2/5.3

Thank You