

Effective Monitoring for Demanding Operations Environments

Rodrigue Chakode

Nagios World Conference, Saint-Paul, US
2013-10-01

Agenda

- Introduction, Background
- Challenges for Effective Monitoring
- Move to Business Service Management (BSM)
- RealOpInsight: An Advanced Software for BSM
- Experience Feedback

Rodrigue Chakode



Author & Leader



PhD, R&D HPC/Cloud Software Engineer



Community Manager



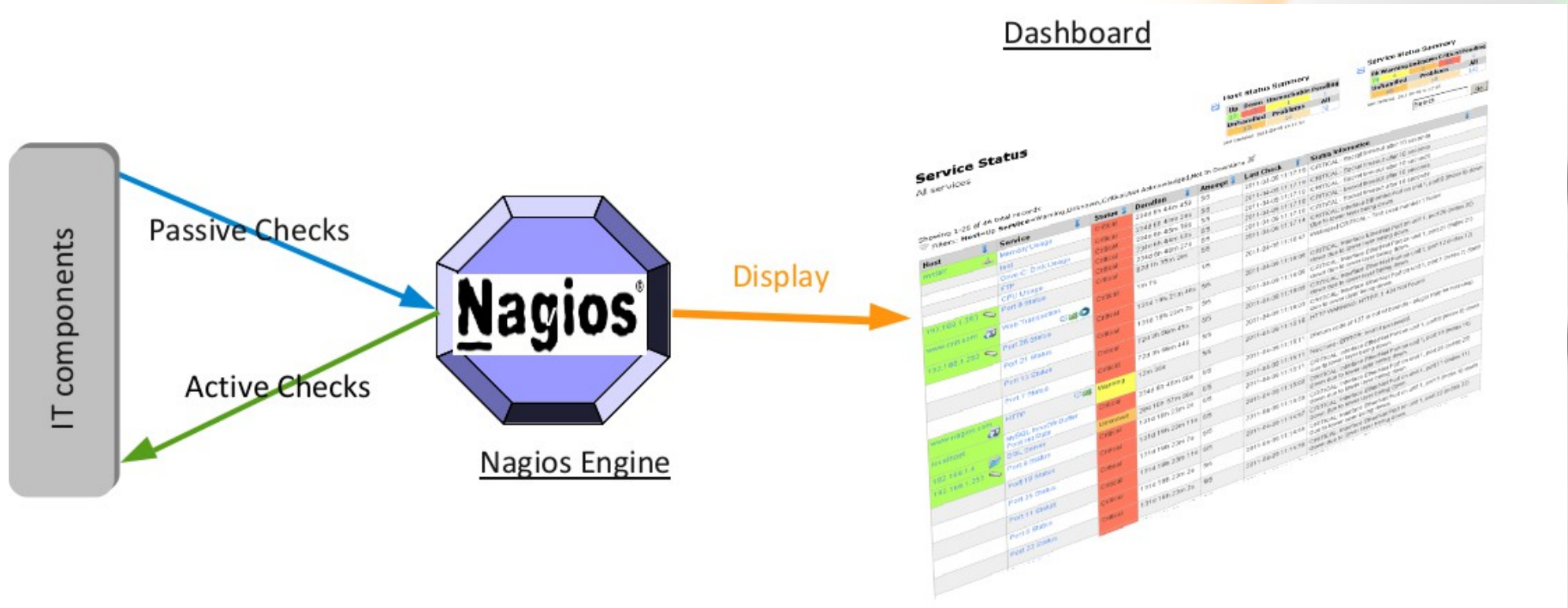
<http://fr.linkedin.com/in/rodriguechakode>

Background

- **Service** : IT functionality (e.g. mysqld service)
- **Business Service** : service providing high-level value-added to applications or to end-users (e.g. hosting service)
 - aka Business Process
- Abbreviations
 - **BS**: Business Service
 - **BSM**: Business Service Monitoring/Management
 - **OSM**: Open Source Monitoring
 - **OSMS** : Open Source Monitoring System/Software

“Too many alarms kill alarm”
S. Bortzmeye

Basic Monitoring Scheme



Flat display, no notion of high level services

Today's IT infrastructures facts

- Huge number of checks to handle
 - E.g. 100 hosts, 8 checks/host => 8,00 checks
- False alerts are the bane of administrators
 - Not a matter of being a lazy admin
- **No way to be effective with flat display !**

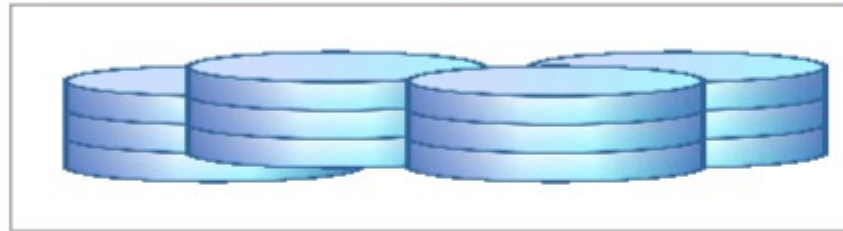
Challenges for effective monitoring

- How a failure actually impacts your business ?

Streaming



Databases

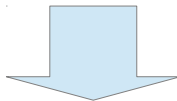
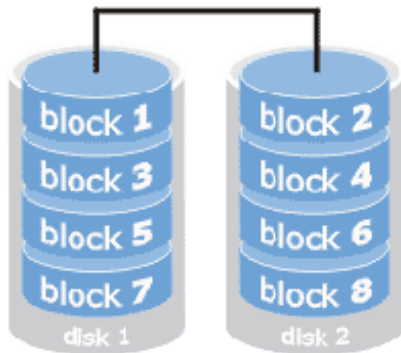


Hard discs



Is there a disruption of services?

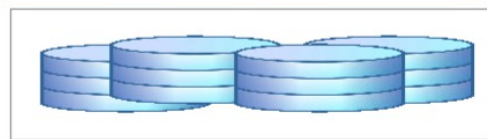
RAID 0
(striping)



Streaming



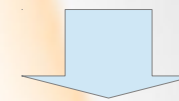
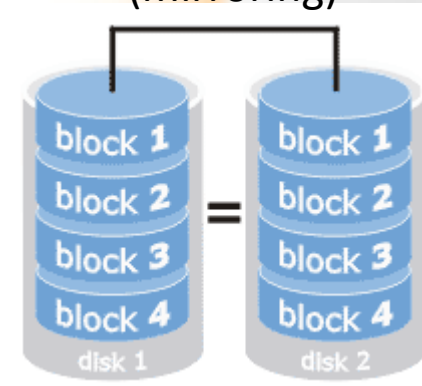
Databases



Hard discs



RAID 1
(mirroring)



Streaming



Databases



Hard discs



“Network tools cannot actually determine what is and is not important. Only the owner of applications can do that”

Anonymous

“prioritize and orchestrate work based on business needs”

<http://www.bmc.com/solutions/bsm/>

Go beyond individual checks

- Think business services
 - A failure don't necessarily mean disruptions on business applications or end-user services
- Benefits
 - Reduce downtime by up to 75%
 - Deliver services up to 30% more efficiently
 - Credit: <http://www.bmc.com/solutions/bsm/>

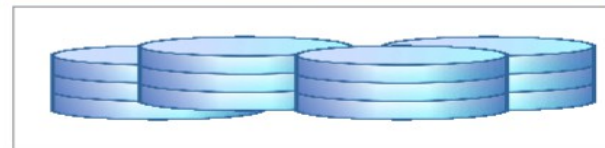
Think relational services

- A business service may depend on :
 - one or many IT services, and/or on
 - other business services
 - E.g. Streaming ← Web Server ← Databases ← Network ← Operating System ← Hardware Devices...

Streaming



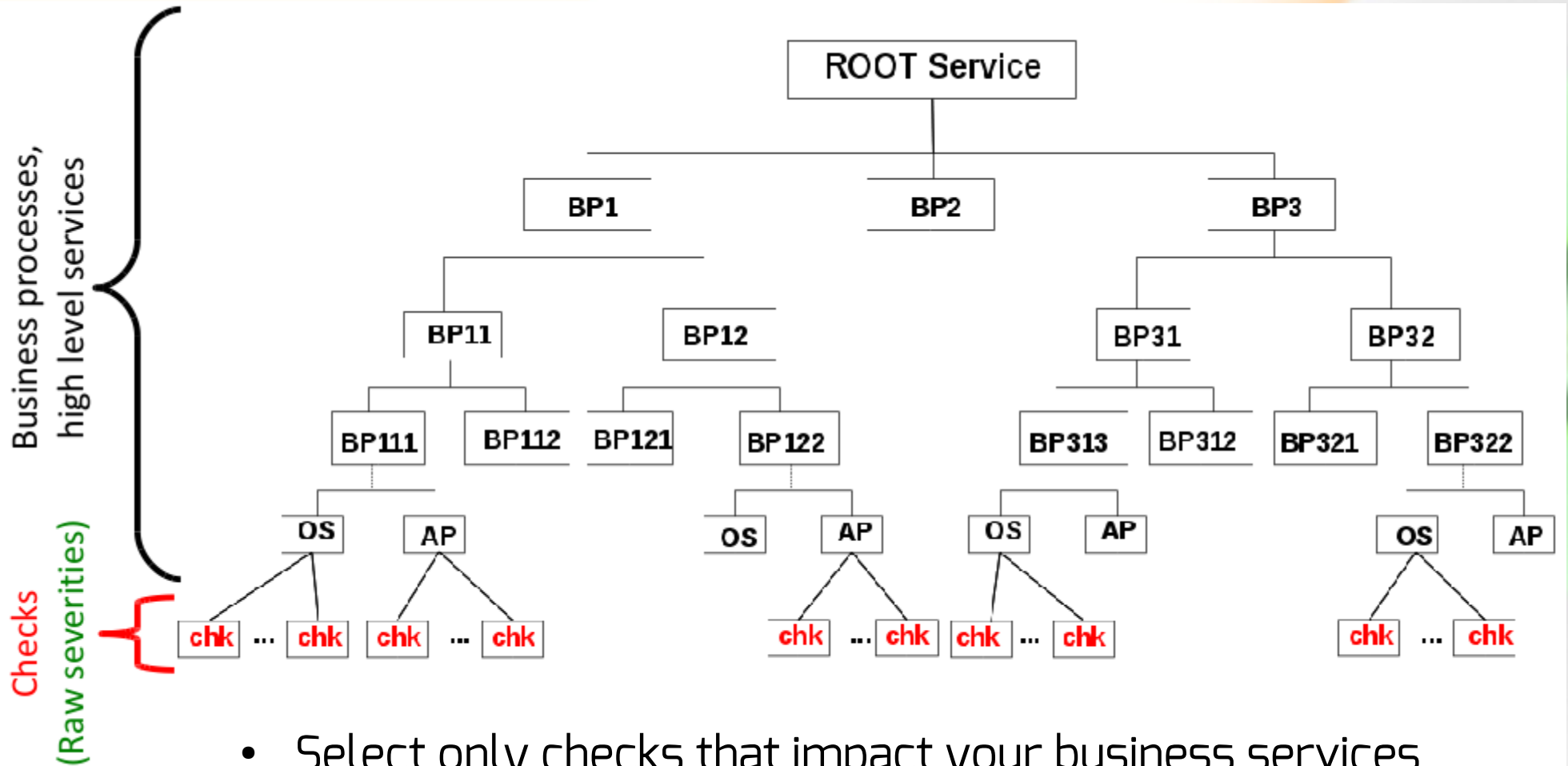
Databases



Hard discs

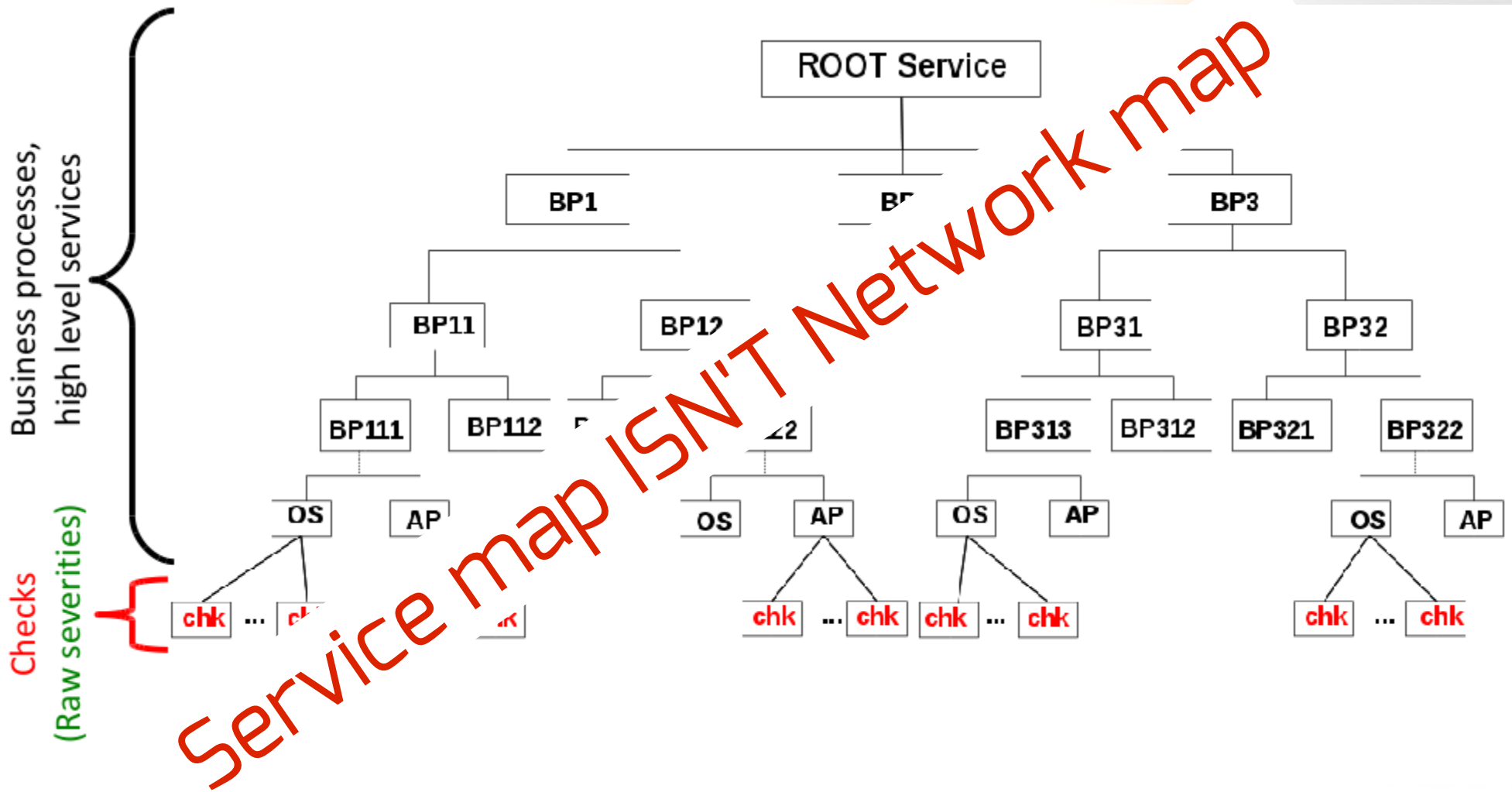


Service hierarchy and mapping



- Select only checks that impact your business services
- Advanced severity calculation and propagation rules
 - Severity aggregation, severity propagation

Service hierarchy and mapping



Use cases

- RAID 0



- RAID 1



- Redundant databases



- Merchant-site



“Takes the IT you already have, and adds to it the visibility and control of a unified platform”

<http://www.bmc.com/>

Nagios BP Add-on

- Good starting point
 - Service tree, aggregation rules, **no propagation rules**
 - **No service map**, not suited for a huge number of services



The screenshot displays the Nagios XI web interface. The top navigation bar includes links for Home, Views, Dashboards, Reports, Configure, Help, and Admin. The user is logged in as 'nagiosadmin'. The main content area shows a service tree for the 'Tutorial' group, which has 4 problem(s). The services listed include:

- 192.168.5.32: Ping (OK - 192.168.5.32: rta 1.034ms, lost 0%)
- 192.168.5.64: _testservice_1 (WARNING: Results are stale.)
- 192.168.5.64: _testservice_2 (WARNING: Results are stale.)
- 192.168.5.1: Default_Gateway (Ping OK - 192.168.5.1: rta 3.088ms, lost 0%)
- 192.168.5.99: Down Host (Ping CRITICAL - 192.168.5.99: Host unreachable @ 192.168.5.59. rta nan, lost 100%)
- 192.168.5.42: LAN Switch-42 (Ping CRITICAL - 192.168.5.42: rta nan, lost 100%)
- localhost: Check Latency (Latency OK: Active Host=0.228ms, Active Service=0.196ms, Passive Host=0.388ms, Passive Service=0ms)
- localhost: Current Load (OK - load average: 0.97, 0.59, 0.40)
- localhost: Current Users (USERS OK - 0 users currently logged in)
- localhost: Execution Time (Execution Time OK: Host=2.98ms, Service=2.416ms)
- localhost: More Local Services (URL 0 problem(s) Demo Group 2 Edit Delete)
- localhost: Rant Paribon (DISK OK - free space: / 4395 MB (63% inode=95%):)
- localhost: SSH (SSH OK - OpenSSH_4.3 (protocol 2.0))
- localhost: Swap Usage (SWAP OK - 100% free (511 MB out of 511 MB))
- localhost: Total Processes (PROCS OK: 65 processes with STATE= R5ZDT)
- localhost: Local Services (1 problem(s) Example BPI Group Edit Delete)
- localhost: Current Load (OK - load average: 0.97, 0.59, 0.40)
- localhost: Current Users (USERS OK - 0 users currently logged in)
- localhost: HTTP (HTTP WARNING: HTTP/1.1 403 Forbidden.)
- localhost: PING (PING OK - Packet loss= 0%, RTA = 0.03 ms)

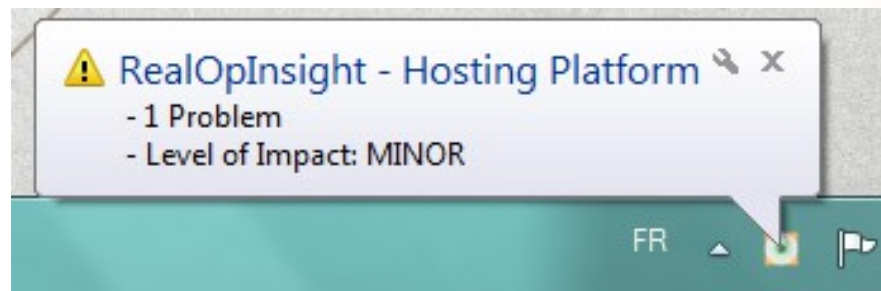
RealOpInsight

- Powerful and easy-to-use BSM dashboard toolkit
 - C++/Qt-based GUI application
 - Cross-platform (Linux, Windows, OS X)
 - Better interactiveness vs Web interfaces
- Generic and scalable Add-on
 - Central dashboard for distributed environments
 - Up to 10 monitoring servers simultaneously
- <http://realopinsight.com>

“small and efficient and gets the job done”
lukaswhite, SourceForger.net

RealOpInsight In a Nutshell

- **Effective operations management**
 - Prioritize incidents based on business impact
 - Specialized dashboards (business service-centric or operator competency-centric)
- **Advanced event processing rules**
 - average, high impact, decrease, increase...
- **Central dashboard for distributed monitoring**
 - Versatile, supports up to 10 monitoring backends simultaneously
- **Free, open source and Cross-platform**
 - Windows, Linux, OS X
- **Comprehensive messages**
 - e.g. “the CPU load on server **<IP/hostname>** is more than **<threshold>** percent
- **System tray notifications**
- **Embedded Browser**



TreeView, Map and Events in One Console

Service Mapping

- Tooltips, Zooming, Dragging and Scrolling, Focus, Service-related message filtering...

Service Tree

- Tooltips
- Focus
- Service-related message filtering...

The screenshot displays the Nagios XI interface. On the left is the 'TV Explorer' (Service Tree) showing a hierarchical view of services across different hosts. The main area shows a 'Service Mapping' map with a tooltip for 'Service: ngrt4n.com' displaying details like 'Severity: Major', 'Calc. Rule: High Severity', and 'Prop. Rule: Decreased'. At the bottom is the 'Message Console' table.

Date & Hour	Severity	Host	Service	Message
Sat Dec 11 09:35:57 2010	Critical	vspher...	Load	CRITICAL - load average: 0.40, 0.39, 0.36
Sat Dec 11 08:59:34 2010	Normal	songish	Disk Space	PING OK - Paquets perdus = 0%, RTA = 0.05 ms
Sat Dec 11 08:59:44 2010	Normal	linksys-srw224p	Firewall	PING OK - Paquets perdus = 0%, RTA = 0.68 ms
Sat Dec 11 09:37:30 2010	Normal	nebula-front	nfsd	The NFS daemon is now up
Sat Dec 11 10:56:05 2010	Normal	kvm02	/srv/cloud	OK: all mounts were found
Sat Dec 11 09:37:24 2010	Normal	nebula-front	NFS Badcalls	NORMAL: There were 0 bad calls since the last nfs-server monitoring
Sat Dec 11 09:33:47 2010	Normal	kvm01	ssh	The ssh server on the host kvm01 is up
Sat Dec 11 09:37:04 2010	Normal	vmm01	ssh	The ssh server on the host vmm01 is up

Message Console

- Trouble view filtering...

Advanced Incident Management

- Severity aggregation
- Severity increasing
- Severity decreasing
- ...

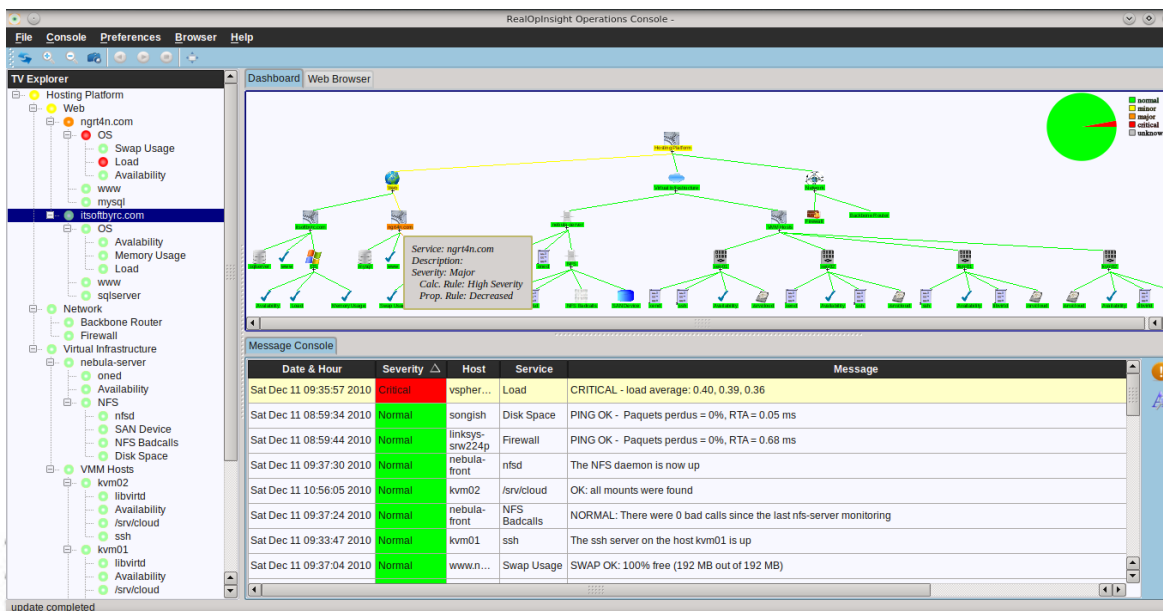
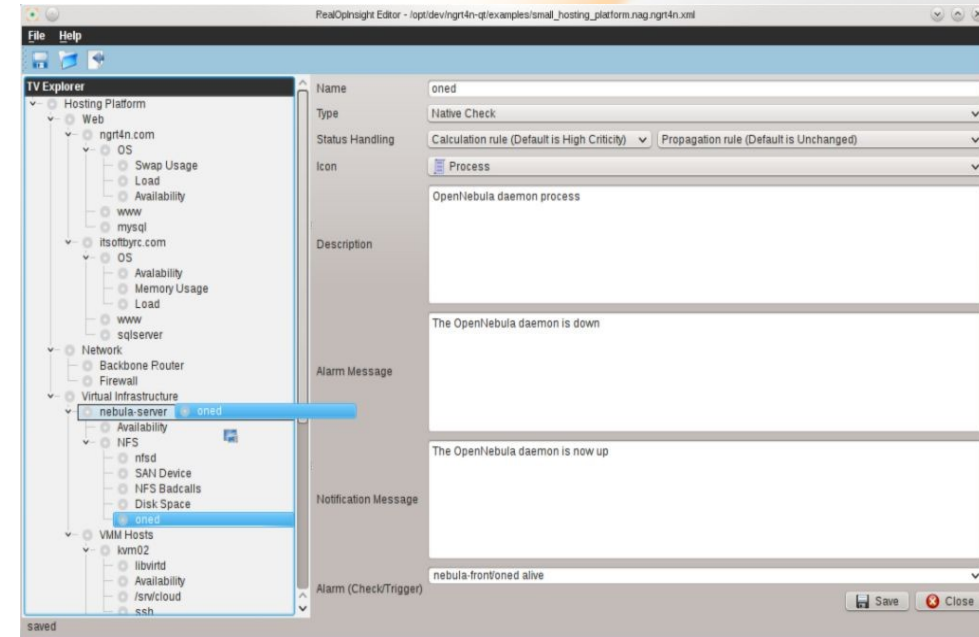
The screenshot displays the Nagios RealOpsInsight Operations Console. The main view is a hierarchical tree of services. The root node is 'nrt4n.com', which branches into 'mysql' and 'www'. The 'www' node further branches into 'Load', 'Memory Usage', 'Swap Usage', 'Load', and 'Availability'. The 'Availability' node branches into 'Disk Space', 'nfsd', 'NFS Badcalls', 'SAN Device', 'kexec', and 'ssh'. The 'nfsd' node branches into 'Availability', 'oned', and 'NFS'. The 'NFS' node branches into 'NFS Badcalls', 'SAN Device', 'kexec', and 'ssh'. A legend in the top right corner indicates severity levels: normal (green), minor (yellow), major (orange), critical (red), and unknow (grey). A circular gauge in the top right corner shows the overall system health, with a red needle pointing towards the critical level.

The Message Console at the bottom displays a list of incidents:

Date & Hour	Severity	Host	Service	Message
Sat Dec 11 09:35:57 2010	Critical	vspher...	Load	CRITICAL - load average: 0.40, 0.39, 0.36
Sat Dec 11 08:59:34 2010	Normal	songish	Disk Space	PING OK - Paquets perdus = 0%, RTA = 0.05 ms
Sat Dec 11 08:59:44 2010	Normal	linksys-srw224p	Firewall	PING OK - Paquets perdus = 0%, RTA = 0.68 ms
Sat Dec 11 09:37:30 2010	Normal	nebula-front	nfsd	The NFS daemon is now up
Sat Dec 11 10:56:05 2010	Normal	kvm02	/srv/cloud	OK: all mounts were found
Sat Dec 11 09:37:24 2010	Normal	nebula-front	NFS Badcalls	NORMAL: There were 0 bad calls since the last nfs-server monitoring
Sat Dec 11 09:33:47 2010	Normal	kvm01	ssh	The ssh server on the host kvm01 is up
Sat Dec 11 09:37:04 2010	Normal	www.n...	Swap Usage	SWAP OK: 100% free (192 MB out of 192 MB)

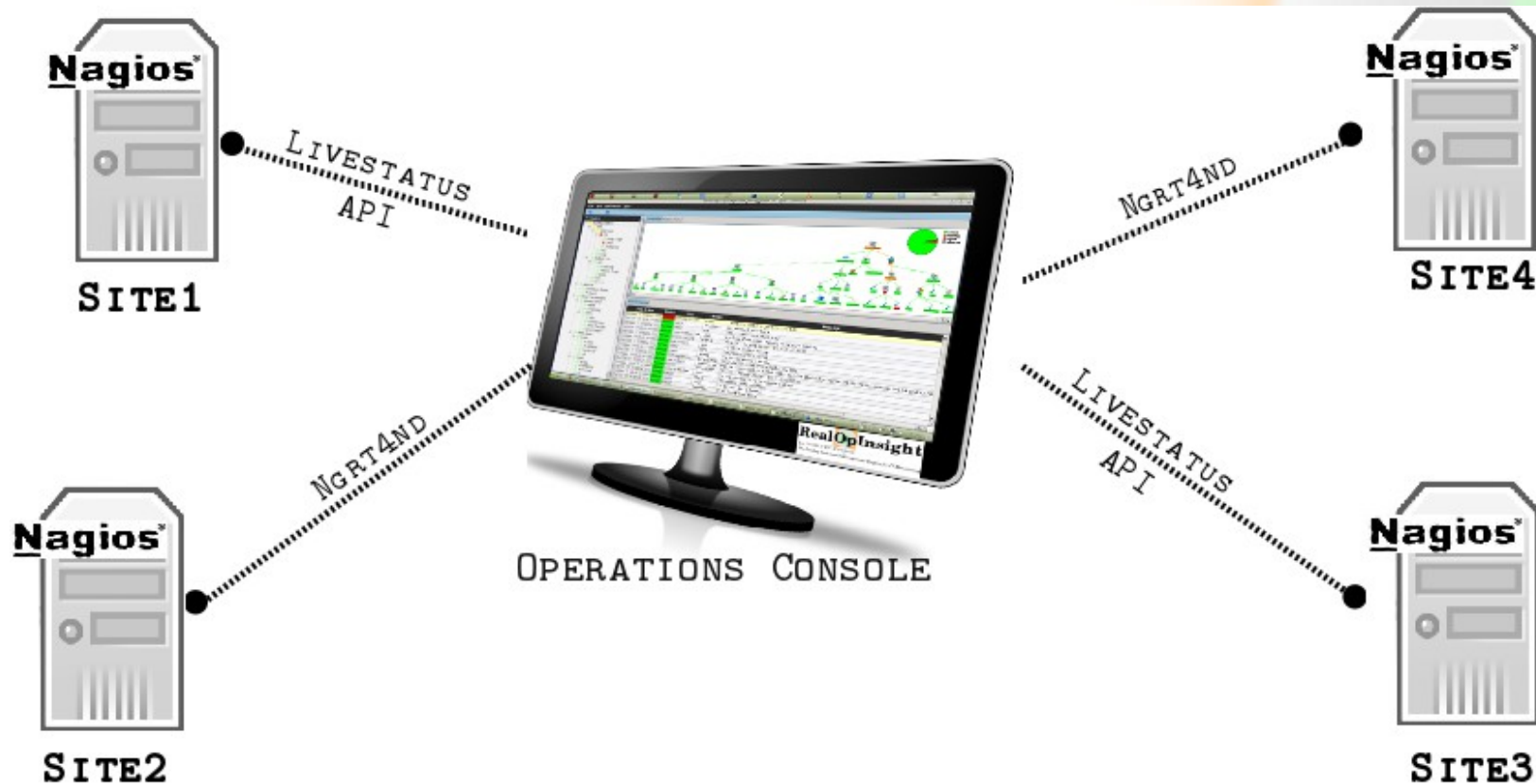
Simple and Efficient Design

- Service Views as XML files
- Native **WYSIWYG** Editor
- Dynamic **Operations Console**
- Simple **Integration**



Distributed Monitoring/Unified Dashboard

- Loosely-coupled and scalable architecture
 - Status data retrieved through RPC APIs



Ngrt4nd Integration - How To (1)

- Specific daemon on Nagios server (ngrt4nd)
 - Relies on status.dat file
 - ZeroMQ-based RPC APIs
- **Non recommended**
 - Non-scalable, delayed status data

Livestatus Integration - How To (2)

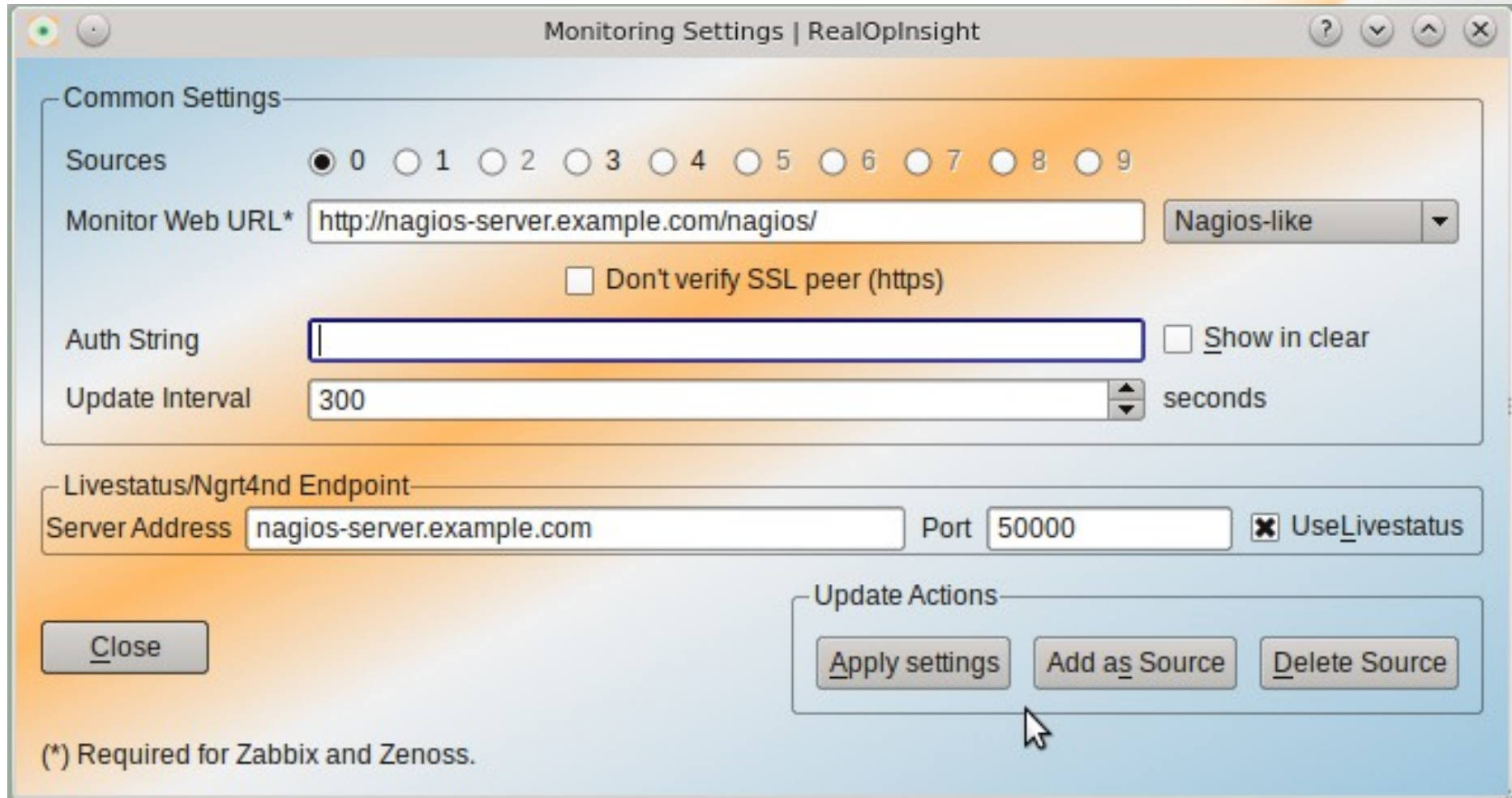
- Xinetd TCP-based data retrieving
 - Xinetd socket over the native LS NEB socket
 - /etc/xinetd.d/livestatus

- **Recommended**

- Scalable, NEB → up-to-date data

```
service livestatus
{
    type            = UNLISTED
    port            = 6557
    socket_type     = stream
    protocol        = tcp
    wait            = no
    cps              = 100 3
    instances       = 500
    per_source      = 250
    flags           = NODELAY
    user            = nagios
    server          = /usr/bin/unixcat
    server_args     = /var/lib/nagios/rw/live
    disable         = no
}
```

Configuration



Monitoring Settings | RealOpInsight

Common Settings

Sources 0 1 2 3 4 5 6 7 8 9

Monitor Web URL* Nagios-like

Don't verify SSL peer (https)

Auth String Show in clear

Update Interval seconds

Livestatus/Ngrt4nd Endpoint

Server Address Port UseLivestatus

Close

Update Actions

(*) Required for Zabbix and Zenoss.

<http://realopinsight.com/en/index.php?page=configuring-realopinsight-operations-console>

Identifying status data

Service in Nagios

```
define service{  
    use          local-service  
    host_name    mysql-server  
    service_description Root Partition  
    check_command check_local_disk!30%!10%!/  
}
```

Selection in RealOpInsight

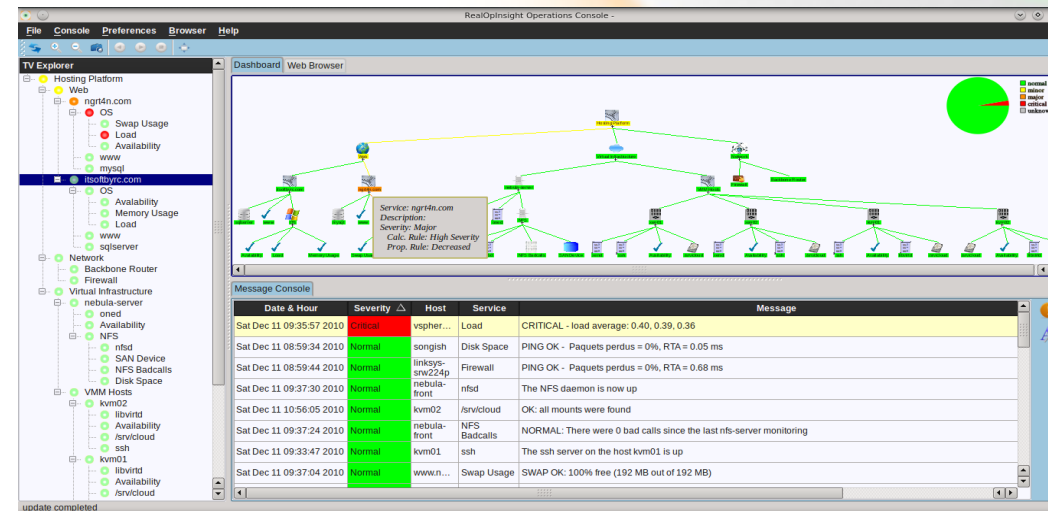
[SourceId:]host_name[/service_description]

Data Point ?

mysql-server/Root Partition

Getting started in 3 steps

- Run the Editor
 - ... and edit your service view configuration
- Run the Configuration Manager
 - ... and set the access to the remote API
- Run the Operations Console
 - ... and load the configuration file
- Then fall in love !



The screenshot displays the RealOpInsight Operations Console. On the left, a 'TV Explorer' pane shows a tree structure of services and hosts, including 'Hosting Platform', 'Web', 'OS', 'Network', and 'Virtual Infrastructure'. The main area shows a dashboard with a network diagram and a 'Message Console' at the bottom. The message console contains the following log entries:

Date & Hour	Severity	Host	Service	Message
Sat Dec 11 09:35:57 2010	Critical	vspher...	Load	CRITICAL - load average: 0.40, 0.39, 0.36
Sat Dec 11 08:59:34 2010	Normal	songish	Disk Space	PING OK - Paquets perdue = 0%, RTA = 0.05 ms
Sat Dec 11 08:59:44 2010	Normal	linksys-srv224p	Firewall	PING OK - Paquets perdue = 0%, RTA = 0.68 ms
Sat Dec 11 09:37:30 2010	Normal	nebula-front	nfsd	The NFS daemon is now up
Sat Dec 11 10:56:05 2010	Normal	kvm02	/srv/cloud	OK: all mounts were found
Sat Dec 11 09:37:24 2010	Normal	nebula-front	NFS Badcalls	NORMAL: There were 0 bad calls since the last nfs-server monitoring
Sat Dec 11 09:33:47 2010	Normal	kvm01	ssh	The ssh server on the host kvm01 is up
Sat Dec 11 09:37:04 2010	Normal	www.n...	Swap Usage	SWAP OK: 100% free (192 MB out of 192 MB)

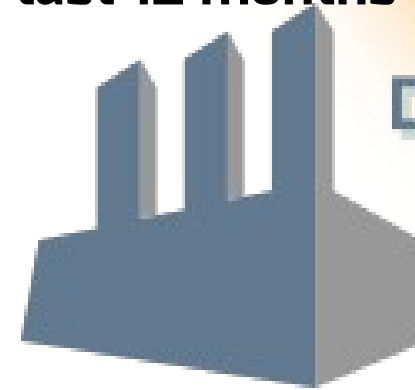
History: The birth

- 2008 : the Idea
- May 2010 : 1st lines of code
- March 2011 (1st release, 1.0)
 - <30 downloads a month
- May - August 2012 (version 2.0)
 - New architecture, GPLv3 License
 - **SourceForge.net, Nagios Exchange**
 - Windows Installer
 - 200 downloads a month



Today: The life cycle

- A major release every 3/4 months
 - V2.1, December 2012
 - V2.2, March 2013
 - V2.3, May 2013 (Support for Livestatus API)
 - V2.4, September 2013 (support for distributed environments)
- Downloads and statistics
 - Source tarballs, Binaries for Windows, Fedora, openSUSE, Debian
 - **~7k+ downloads from 120+ countries, last 12 months**
 - **700+ downloads a month**
 - Nagios Affiliate



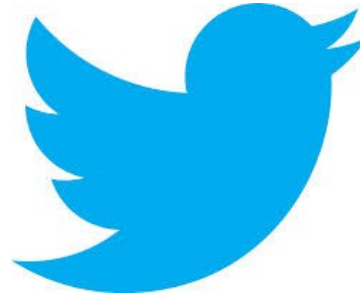
open
build
service

And the story continues..., Thanks

- 2014 : Web Edition

<http://realopinsight.com/index.php?page=contribute>

@ngrt4n



<http://fr.linkedin.com/in/rodriguechakode>