

Nagios Essential

By – Rajesh Kumar

Twitter - RajeshKumarIN

Email – DevOps@RajeshKumar.xyz

Outline

- ▶ What is Nagios?
- ▶ Getting Started
 - ▶ Hosts, Commands, Services, Timeperiods and Contacts
 - ▶ Remote Checks with NRPE
 - ▶ Hostgroups and Servicegroups
 - ▶ Templates
 - ▶ Config File(s)
 - ▶ Active v. Passive checks
- ▶ Going Further
 - ▶ Writing you own Checks
 - ▶ NSCA
 - ▶ Service Hierarchies
 - ▶ Eventhandlers
 - ▶ Modifying the Web Pages

What is Nagios

- ▶ “Nagios is an enterprise-class monitoring solutions for hosts, services, and networks released under an Open Source license.”

www.nagios.org

- ▶ “Nagios is a popular [open source computer system](#) and [network monitoring application software](#). It watches [hosts](#) and services that you specify, alerting you when things go bad and again when they get better.”

www.wikipedia.org

What is Nagios?

- ▶ Free network monitoring tool
- ▶ Open source
- ▶ Comes in pieces - use what you need

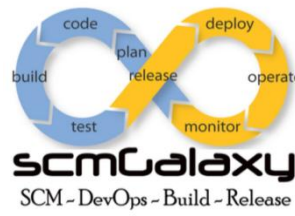
What is Nagios?

- ▶ Nagios watches your computers through user-defined commands
- ▶ It can be set to inform you when a service or host becomes unavailable
- ▶ In fact, it can inform you, the Sysadmin, your best friend, and even run commands to try to bring a system back up

Where is Nagios?

- ▶ Nagios runs on nagman, a dedicated server in ML-29
 - ▶ 1U PC
 - ▶ Debian Linux
- ▶ Backup machine exists
 - ▶ Not configured
 - ▶ Will be installed at Foothills

Who uses Nagios?



- ▶ Anyone with a web browser and a Nagios account
 - ▶ NOC staff

What does Nagios do?

- ▶ Monitors 331 network devices
- ▶ Monitors HMTL on access points
- ▶ Monitors BGP on routers
- ▶ Makes noises in the NOC
- ▶ Links to web pages with instructions

What's good about Nagios?

- ▶ It's conceptually simple
- ▶ It handles the load
- ▶ It has a web interface
- ▶ It's extensible
- ▶ It's not overly noisy

What's bad about Nagios?

- ▶ Lots of configuration
- ▶ No discovery
- ▶ Manual network hierarchy
- ▶ Doesn't understand multihomed devices
- ▶ Limited support for SNMP

Nagios: a measurement tool that actively monitors availability of devices and services:

- **Popular:** One of the most used open source network monitoring software packages.
- **Fast:** Uses CGI functionality written in C for faster response and scalability.
- **Scalable:** Can support up to thousands of devices and services.
- **Modular**
- **Cool-Looking Web Interface[®]**

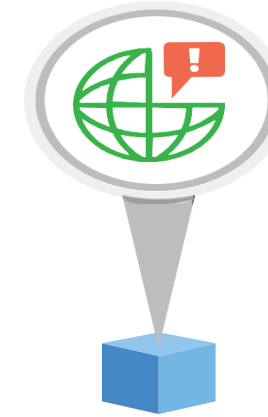
MONITOR YOUR ENTIRE IT INFRASTRUCTURE WITH NAGIOS XI

Nagios® XI™ is the most powerful IT infrastructure monitoring solution on the market. Nagios XI extends on proven, enterprise-class open source components to deliver the best monitoring solution for today's demanding organizational requirements.

Designed for scalability and flexibility, XI is designed to make problematic IT monitoring tasks simple, while retaining the powerful attributes of its enterprise-class foundation blocks.



COMPREHENSIV
E MONITORING



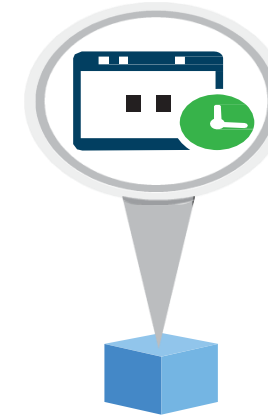
ALERTING VIA
EMAIL & MOBILE



UNPARALLED
PERFORMANCE



INCREASED
VISIBILITY



PROACTIE
PLANNING



MULTI-TENANT
CAPABILITIES

Features 1: Plug-Ins or Modular

The Nagios package in Ubuntu comes with a number of pre-installed plugins:

apt.cfg breeze.cfg dhcp.cfg disk-smb.cfg disk.cfg dns.cfg
dummy.cfg flexlm.cfg fping.cfg ftp.cfg games.cfg hppjd.cfg
http.cfg ifstatus.cfg ldap.cfg load.cfg mail.cfg mrtg.cfg mysql.cfg
netware.cfg news.cfg nt.cfg ntp.cfg pgsqll.cfg ping.cfg
procs.cfg radius.cfg real.cfg rpc-nfs.cfg snmp.cfg ssh.cfg
tcp_udp.cfg telnet.cfg users.cfg vsz.cfg

There are many more available (e.g.)...

<http://sourceforge.net/projects/nagiosplugins>

Features: 2

Fast and Scalable

- Compiled, binary CGIs and common plug-ins for faster performance.
- Parallel checking and forking of checks to support large numbers of devices.
 - This has been considerably improved in version 3 of Nagios.
- Improvement of efficiency is a controversial topic in the Nagios community. There is now a fork, *icinga*, trying to re-write Nagios in a different manner.

Features: 3

- Uses “intelligent” checking capabilities.
 - Attempts to distribute the server load of running Nagios (for larger sites) and the load placed on devices being checked.
- Configuration is done in simple, plain text files, that can contain much detail and are based on templates.
- Nagios reads it's configuration from an entire directory. You decide how to define individual files.

Features: 4

- **Topology Aware:** To determine dependencies.
 - *Differentiates between what is down vs. what is not available. This way it avoids running unnecessary checks. This is done using parent-child relationships between devices.*
- **Notifications:** How they are sent is based on combinations of:
 - *Contacts and lists of contacts.*
 - *Devices and groups of devices*
 - *Services and groups of services*
 - *Defined hours by persons or groups.*
 - *The state of a service.*

Features: 5

Service state:

- When configuring a service you have the following notification options:
 - **d**: DOWN: The service is down (not available)
 - **u**: UNREACHABLE: When the host is not visible
 - **r**: RECOVERY: (OK) Host is coming back up
 - **f**: FLAPPING: When a host first starts or stops or it's state is undetermined.
 - **n**: NONE: Don't send any notifications

Why Nagios

- ▶ Avoidance of “**Too many red flashing lights**”
- ▶ “Just the facts” – only want root cause failures to be reported, not cascade of every downstream failure.
- ▶ also avoids unnecessary checks
- ▶ e.g. HTTP responds, therefore no need to ping
- ▶ e.g. power outage, no ping response, so don't bother trying anything else
- ▶ Services are running fine no need to do check if the host itself is alive

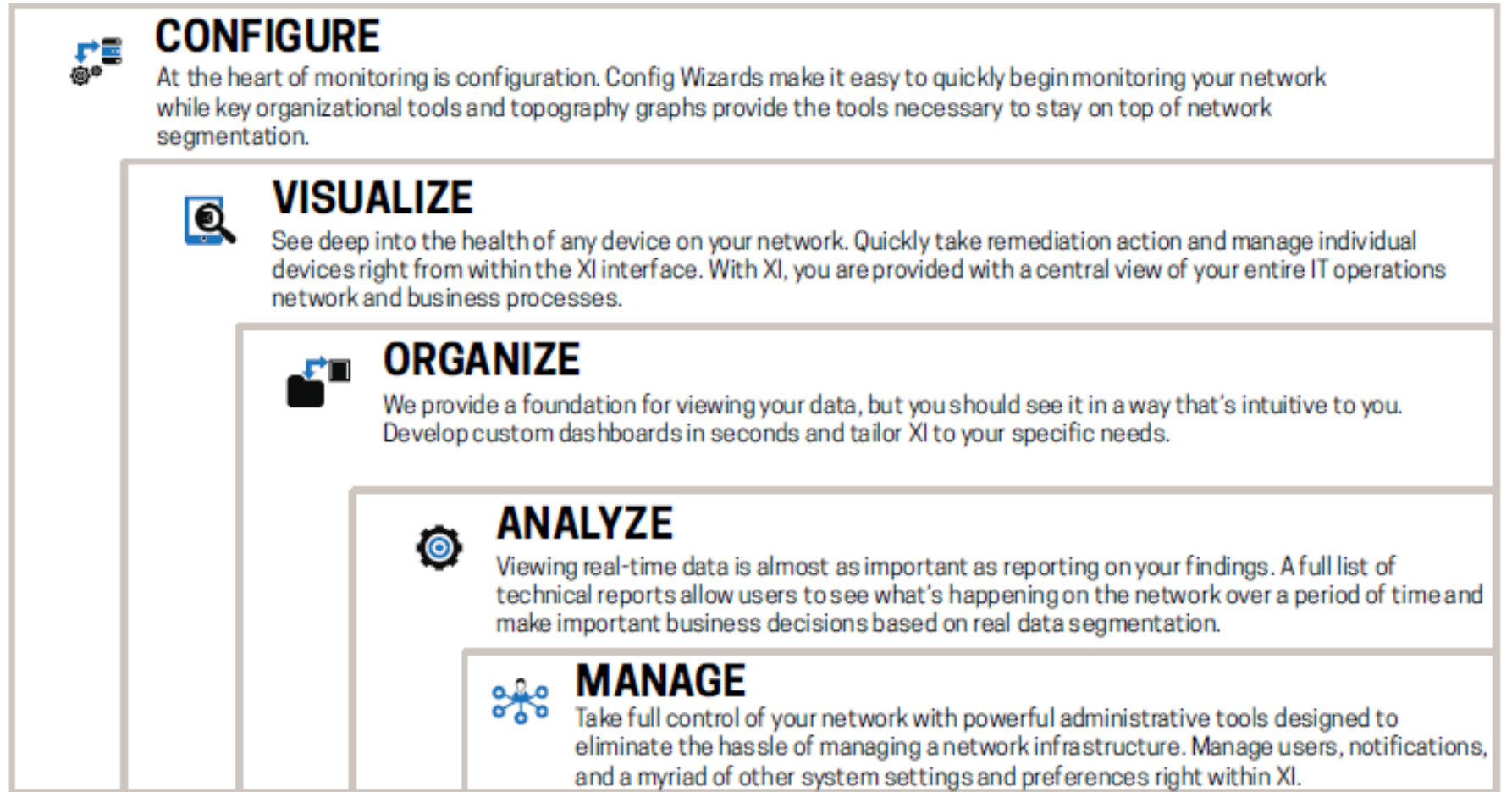
What Can it Do?

A lot, including:

- Service monitoring
- Alerts from SNMP traps
- Monitoring redundancy
- Detection of primary failure to avoid multiple like alerts.
- Notifications via email, pager, etc.
- Notifications to individuals or defined groups
- Log information
- Use databases to store history
- Graph generation from MRTG
- Very extensible via plug-ins, add-ons and local scripts.
- Can scale to large installations
- Allows for redundant monitoring
- Aggregation of like-data across multiple nodes.
- Ability to escalate alerts
- Runs on multiple Unices
- Licensed under GPL v2

Overall

We'll walk you through the basics and best practices of Nagios XI, explain key terms, and get you familiar with monitoring, analysis and management.



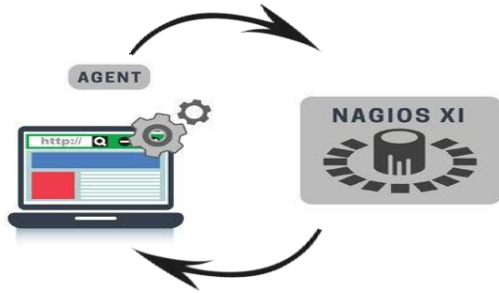
CONFIGURING

Nagios XI is designed to provide the most flexible and powerful configuration foundation in monitoring. If it uses electricity, chances are, XI can monitor it. Easy-to-use Configuration Wizards allow you to enter information in a step-by-step program and instantly monitor your network. Extend beyond out-of-box capabilities with custom plugins and wizards from the Nagios Exchange.





Now is a good time to determine what you want to gain from monitoring your network. It's important to have an idea of how your network is segmented, your organizational strategy, the metrics you **NEED** to monitor, and the metrics you **WANT** to monitor. Another thing to think about is **HOW** you want to monitor. Agent-based, agent-less, SNMP traps, etc.



Agent-based

A small piece of software is installed on the monitored device (called a host) to provide in-depth information about the monitoring metrics (called services) on that host.



Agent-less

Without installing anything on the host, monitor services with XI. For example, using WMI on Windows machines, or SNMP on Linux machines can accomplish an agent-less setup.



Active Monitoring

A type of monitoring strategy where the Nagios XI server reaches out to the host device for information and actively checks to see if anything has changed. Usually aided by an agent, this strategy can get resource intensive in large environments.



Passive Monitoring

A monitoring strategy where XI does not actively reach out to the hosts for information, rather it listens for new information. This strategy can prove very efficient when monitoring large infrastructures by decreasing the load on the Nagios XI server.

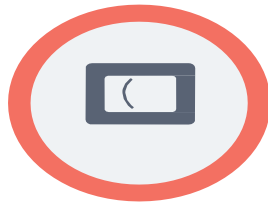
Configuration Wizards

Configuration Wizards are simple step-by-step programs that configure your network devices, servers, databases, etc. for monitoring in Nagios XI. Stay away from the command line and give these wizards a try!



Step One

Find the wizard for you! With over 40+ pre-installed wizards, you can monitor nearly anything your network can throw at XI.



Step Two

Enter the device information and the wizards will do the rest!



Step Three

Determine your desired notification settings and click apply. You are now monitoring.



Top 5 Configuration Wizards

1. Windows Server Wizard
2. Linux Server Wizard
3. Network Switch & Router Wizard
4. Database Wizards – MongoDB, MSSQL, MySQL, Oracle, Postgres
5. Exchange Server Wizard

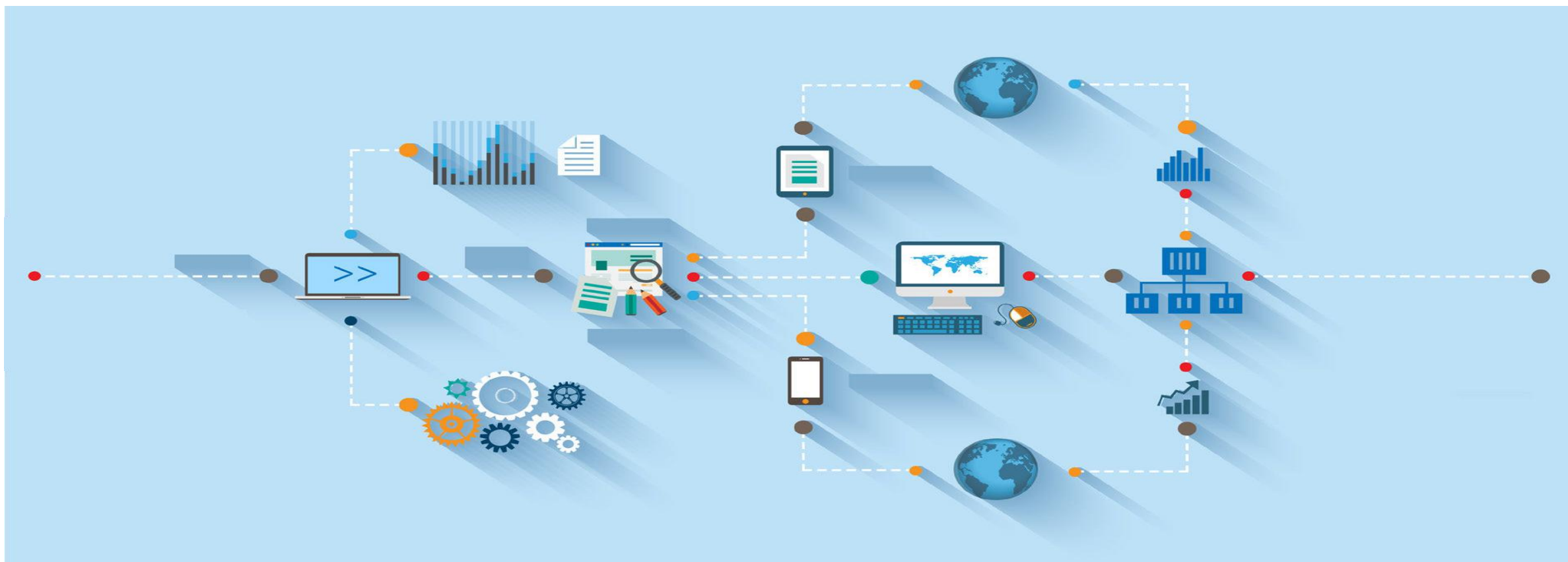
Monitoring Wizard - Step 1

Monitoring wizards guide you through the process of monitoring devices, servers, applications, services, and more. Select the appropriate wizard below to get started. You can find additional configuration wizards for Nagios XI at [Nagios Exchange](#). Need a custom configuration wizard created for your organization? No problem! [Contact us](#) for pricing information.

- AIX**
Monitor an AIX server.
- Auto-Discovery**
Monitor devices and services found by auto-discovery jobs.
- BPI Wizard**
Create service checks for your Nagios BPI groups.
- Bulk Host Cloning and Import**
Clones existing hosts quickly and easily. Supports import from
- Dell OpenManage**
Monitor a Dell® Server using OpenManage.
- DHCP**
Monitor a DHCP server.
- SNMP Walk**
Scan an SNMP-enabled device for elements to monitor.
- Solaris**
Monitor a Solaris server.
- SSH Login**
Monitor the availability and response times of SSH logins.
- SSH Prxy**
Monitor a remote Linux, Unix, or Mac OS/X machine using SSH
- Network Switch / Router**
Monitor a network switch or router.
- TCP/UDP Port**
Monitor common and custom TCP/UDP ports.
- VMware**
Monitor a VMware host or guest VM.
- VMware ESX / vSphere / vCenter**
Monitor a VMware® ESX® 3.x / vSphere® 4.x Host or vCente
- WatchGuard**
Monitor a WatchGuard device.
- Website**
Monitor a website.
- Website Defacement**
Monitor a website for defacement.
- Website URL**
Monitor a specific web URL.
- Web Transaction**
Monitor a synthetic web transaction.
- Windows Desktop**
Monitor a Microsoft® Windows XP, Windows Vista, or Window
- Windows Event Log**
Monitor Windows event logs.
- Windows Server**
Monitor a Microsoft® Windows 2000, 2003, 2008 or 2012 ser
- Windows SNMP**
Monitor a Microsoft® Windows workstation or server using S
- Windows WMI**
Monitor a Microsoft® Windows workstation or server using W
- MongoDB Server**
Monitor a MongoDB Server
- MSSQL Database**
Monitor a MSSQL Database
- MSSQL Query**
Monitor a MSSQL Database Query
- MSSQL Server**
Monitor a MSSQL Server.
- MySQL Query**
Monitor a MySQL database query.
- MySQL Server**
Monitor a MySQL server.
- Nagiosstats Wizard**
Monitor internal performance of your XI server.
- Nagios XI Server**
Monitor a remote Nagios XI server.
- NCPA Agent**
Monitor an NCPA Agent
- Nagios Network Analyzer**
Monitor a source, view, or sourcegroup on a Nagios Network Analyzer server.
- NRPE**
Monitor a remote Linux/Unix server using NRPE.
- Oracle Query**
Monitor a Oracle Query
- Oracle Serverspace**
Monitor an Oracle Server
- Oracle Tablespace**
Monitor an Oracle Tablespace
- Passive Check**
Monitor passive service checks and events such as security alerts.
- Postgres Database**
Monitor a Postgres database.
- Postgres Query**
Monitor a Postgres database query.
- Postgres Server**
Monitor a Postgres server.
- Printer**
Monitor an HP JetDirect® compatible network printer.
- RADIUS Server**
Monitor a RADIUS server.
- Nagios Reflector**
Scan Nagios Reflector for hosts/services to monitor.
- SNMP**
Monitor a device, service, or application using SNMP.
- SNMP Trap**
Monitor SNMP Traps.
- SNMP Walk**
Scan an SNMP-enabled device for elements to monitor.
- Solaris**
Monitor a Solaris server.

VISUALIZE

Viewing your devices and being able to take remediation actions immediately is extremely important in your monitoring solution. The host and service detail pages are great for drilling down into a device to see exactly what's going on and also to take action. Let's take a look!



Quick Actions

Quick Actions are customizable links that can be programmed to take remediation action as well as other administrative tasks. Among the many options, you can schedule a check to make sure your host or service is truly up or down. You can take action on your remote devices right from Nagios XI.

Quick Actions are fully customizable. Add links to repair scripts event handlers or other custom scripts to take remediation action.

Performance Graphs

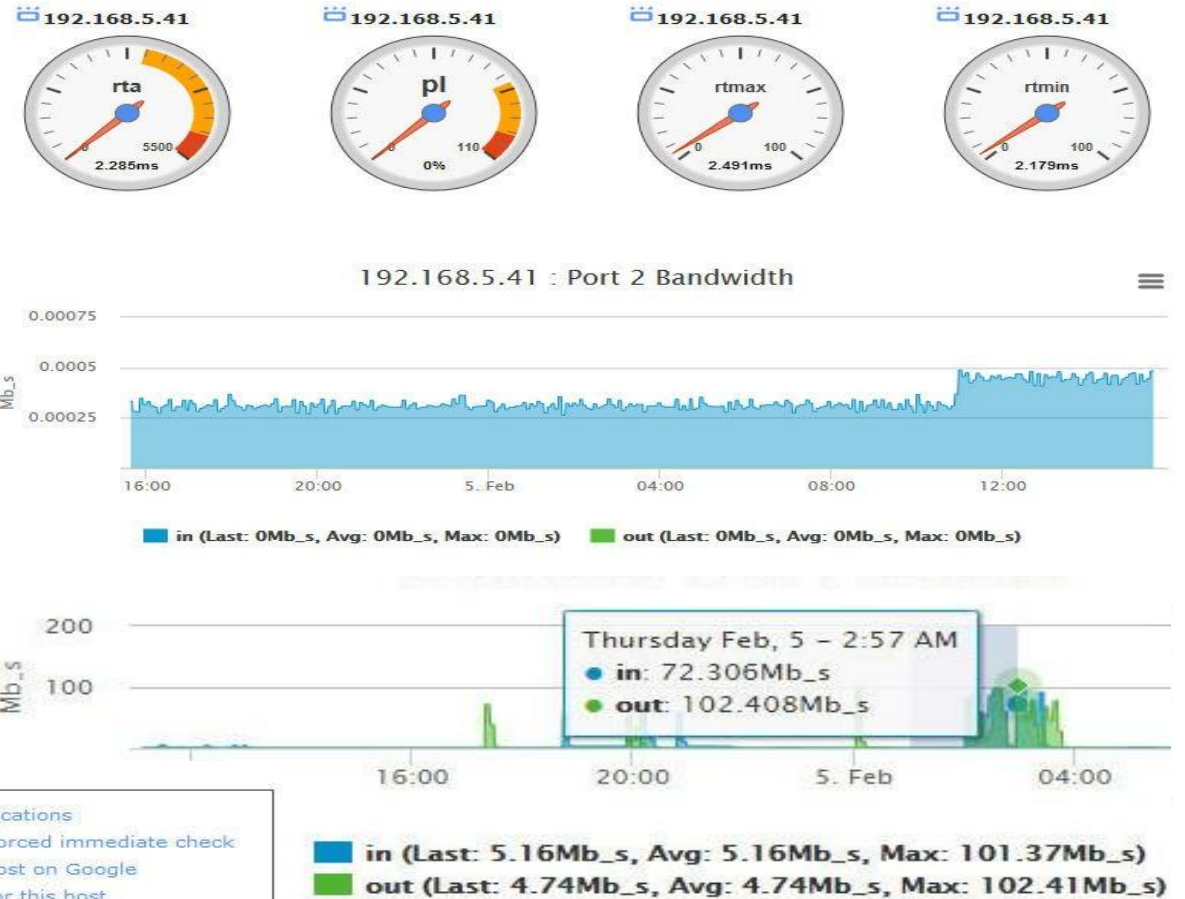
With Performance Graphs, you can see the historical data that Nagios XI has collected. These graphs allow for extensive analysis of monitoring metrics including custom time frames, user menu memory, and direct linking to monitored devices. Within the graph you can:

- 1.Zoom – Drill down to specific events to see what's going on
- 2.Stats – Hover over data points for more detailed information
- 3.Dashify – Add to your dashboards for a customized view.

Quick Actions

- Disable notifications
- Schedule a forced immediate check
- Search for host on Google
- Action URL for this host
- Notes URL for this host
- Ping this host
- Connect to 192.168.5.41
- Traceroute to this host

Performance Graph Examples



Graph Explorer: Drill down to specific Hosts/Services to see what's happening on your network. Get an overview of top alert producers, overall Host/Service health, and Multi-Metric performance graphs.

Top Alerts Last 24hrs

Host Health

Service Health

Scalable Performance Graph

Time Stacked Performance Graph

Multistacked Performance Graph

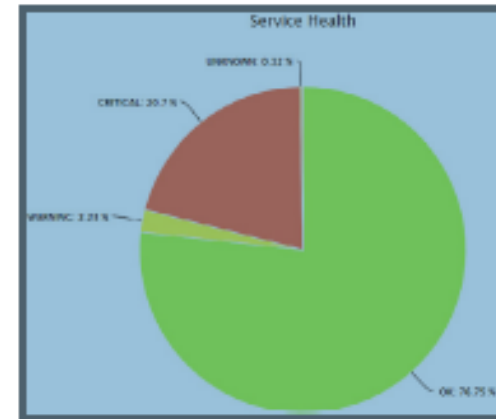
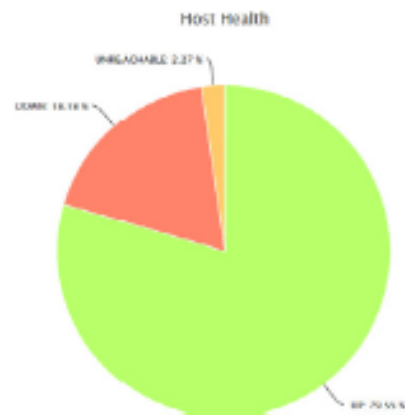
Top Alert Producers

See which devices are causing the most alerts



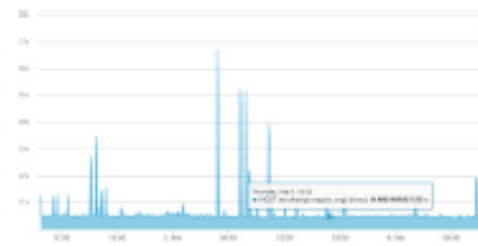
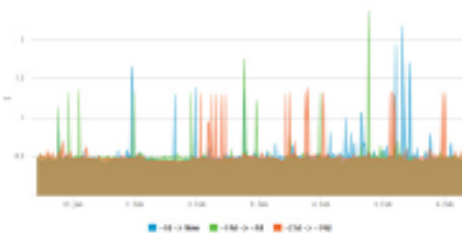
Host Health & Service Health

Quick pie charts showing the overall health of your network.



Time-Stacked & Multi-Stacked Performance Graphs

View service data over time, or compare and contrast multiple hosts and services in one easy to read graph.

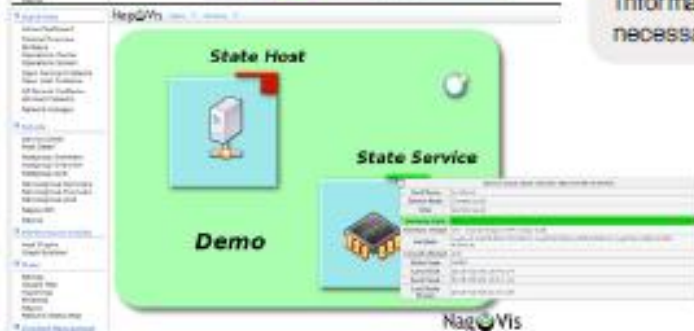


4. Maps: Being able to view your monitoring data & network performance on a map can be extremely beneficial. Saving users time & allowing for at-a-glance network visibility, maps can be customized to users' viewing preferences & give administrators the awareness necessary to maintain their network health.



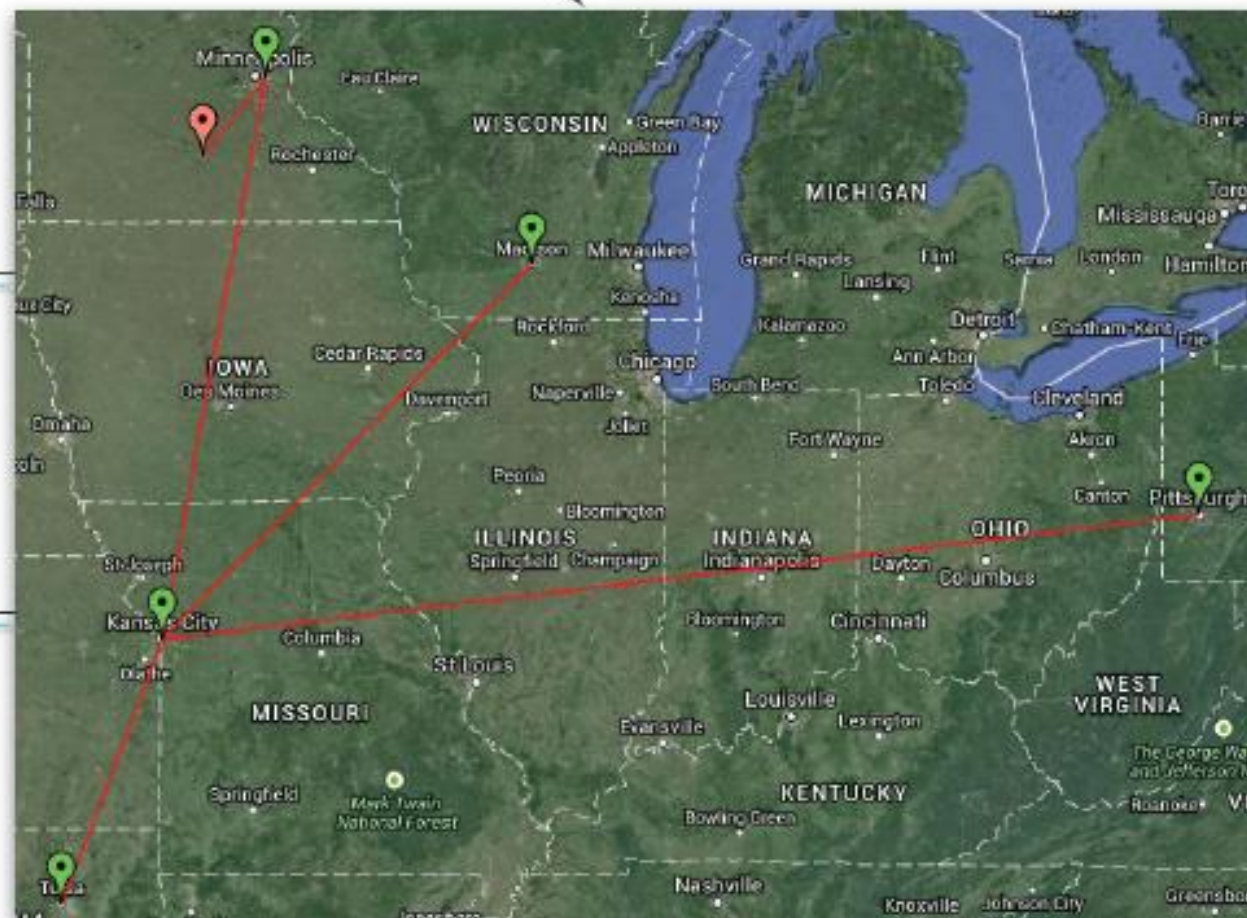
NagVis

Don't limit your creativity! NagVis allows users to create custom maps to represent their network visualization on preferences. The server room visualization shows a real-world image of a server room and plots device information on the exact server blade. View detailed information about the server and take action when necessary.



Google Map

Visualize your network across any geographical region. Perfect for service providers or large organizations, the Google Map feature allows users to quickly spot the problem areas and regions of their network. Segment your network based on office location, datacenter, or client location and plot the geo-coordinates on the map. Drill down to the details of a particular location and quickly react to network incidents.



ORGANIZE

XI provides you with a lot of tools and options for segmenting, viewing, and mapping your network. Your data needs to make sense to you. Use the Hostgroups and Servicegroups as well as Nagios BPI to keep track of device groupings and organize complex business processes. The Hypermap feature auto-generates a network topography map based on your Parent-Child relationships built into your host configurations so you can see a quick overview of your networking environment.





Nagios Business Process Intelligence (BPI)

Nagios Business Process Intelligence is a simple way to monitor the overall health of complex processes in your network.

- Determine essential group members in the process. When an essential member goes down, you'll receive an alert, regardless of the overall health of the process.
- Receive alerts on overall health % thresholds.

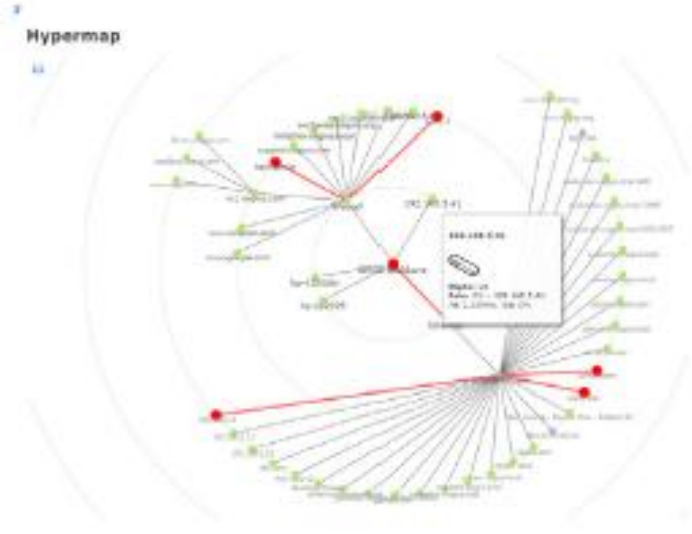
QUICK TIP

To get the most out of XI, and the Hypermap, make sure you define the proper parent-child relationships for each device you're monitoring. This will minimize false positive alerts, and mitigate alert fatigue.



Hostgroups & Servicegroups

Segment your network into logical groupings and easily view breakdowns of host health and service health.

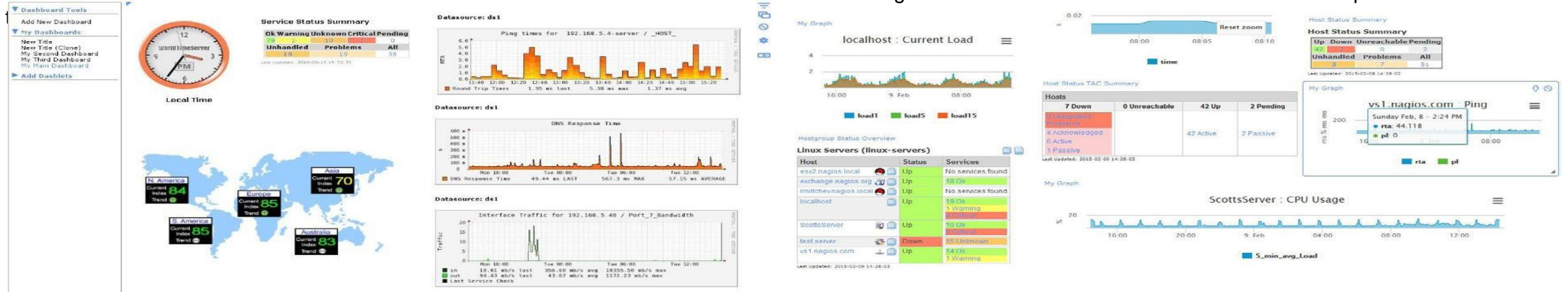


Hypermap

Auto-generated by the parent-child relationships you configure, this network topography visualization lets you see exactly how things are connected in your network infrastructure.

Dashboards

Dashboards are a powerful feature of Nagios XI designed to provide individual users with customized information they find useful. Dashboards are often used to display important, relevant information where it is needed most. Dashboards are specific to individual Nagios XI users. Each user can create their own unique set of dashboards



Adding Dashboards

Nagios XI allows users to create multiple customized dashboards. To add a new dashboard, select the **Add New Dashboard** link under the **Dashboard Tools** Menu. This will open a dialog box where users can enter a title and background color for their new dashboard. Once you have named your dashboard and selected a background color, click **Submit**. This new dashboard can be accessed from the **My Dashboards** menu on the left side of the page.

Adding Dashlets

Select the **Add Dashlets** link on the left side of the page to expand the menu. To add a dashlet, click on the **Add This To A Dashboard** icon located to the left of each of the list items. Nagios XI also allows you to add dashlets to your dashboard from other pages within the site. Any summary, graph, or chart that has the **Add To Dashboard** icon can be added to your custom dashboard.

Manipulating Dashlets

Dashlets can be moved and resized within the dashboard to create a custom layout to fit a user's particular needs. To manipulate a dashlet, move your mouse over it to reveal a blue border and a set of icons.

The **Pin/Float Dashlet** icon controls whether the dashlet is fixed to the page, or if it can be moved.

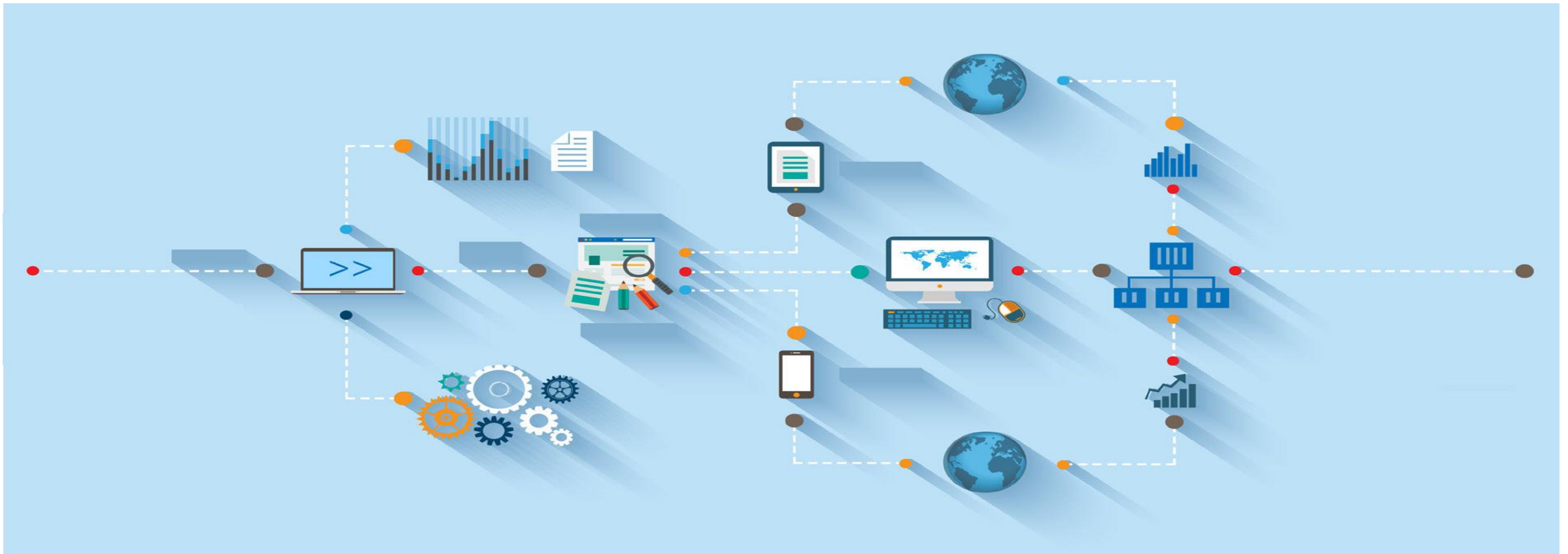
The tab icon located at the bottom right corner of the dashlet controls the size. To re-size your dashlet, click & drag the tab

Home Page Dashboard

Each user has a special home page dashboard that is shown to them when they login. This dashboard can be modified from the dashboards page, and dashlets can be added, manipulated, or removed using the methods described above.

ANALYZE AND MANAGE

XI's powerful reporting features allow you to not only view your data, but make informed business decisions for your organization. Reports are essentially static dashboards that contain summarized monitoring data that can be scheduled, exported, saved, and shared.





Executive Summary

Overview of some of the most useful pieces of information to help you determine the overall state of the network. Availability, Top Alert Producers, Alert Histogram, and Latest Alerts make this report perfect for C-level executives.

SLA Report

Period: Last 24 Hours

Limit To: Host: Hostgroup: Servicegroup:

SLA Target: 95% Hide downtime

[Show Advanced Options](#)

SLA Target: 95.000%

Report Covers From: 2015-02-08 15:52:42 To: 2015-02-09 15:52:42

Host Data

Host	Uptime	SLA Status
All hosts averaged. Show details		
Average	88.100%	FAILED

Service Data

Host	Service	Uptime	SLA Status
All services averaged. Show details			
Average		70.055%	FAILED

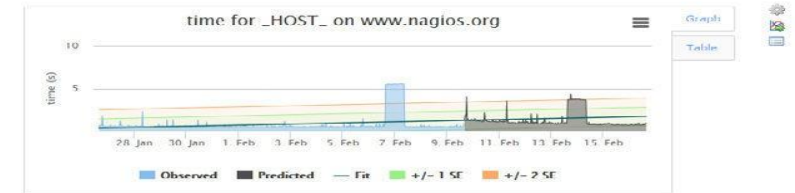
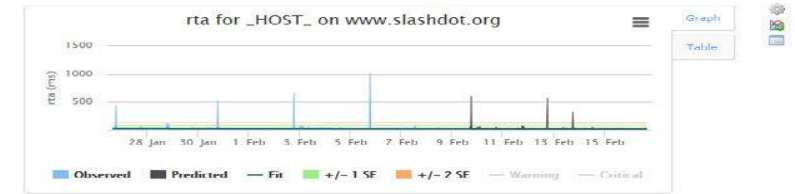
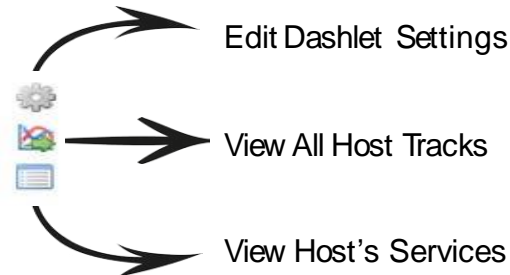
Service Level Agreement (SLA)

Service Level Agreements are important for every organization to maintain. Whether you're a service provider, or you have a strict IT budget, the SLA Report in Nagios XI is perfect for determining if you're meeting your SLA or not. Just select a host, hostgroup, or servicegroup, determine your timeframe, and click "update."



QUICK TIP

Use the buttons in the upper right-hand corner of any report to see what actions you can take on them.



Capacity Planning

Designed to provide you with the ability to predict when network incidents will occur, the capacity planning report allows users to plan for hardware upgrades, future outages, and more. Stay ahead of the curve with four prediction methods. Add the report to a dashboard to keep an eye on a specific host or service.

Add New User

General Settings

Username:

Password:

Repeat Password:

Force Password Change at Next Login:

Email User Account Information:

Name:

Email Address:

Create as Monitoring Contact:

Preferences

Date Format:

Number Format:

Security Settings

Authorization Level:

Can see all hosts and services:

Can (re)configure hosts and services:

Can control all hosts and services:

Can acc/control monitoring engine:

Can access advanced features:

Has read-only access:

2015-03-21 16:52:02	Config Ok	1426974722.tar.gz			
2015-03-20 16:51:02	Config Ok	1426888262.tar.gz			
2015-03-19 16:50:02	Config Ok	1426801802.tar.gz			
2015-03-19 09:55:18	Config Ok	1426776918.tar.gz			
2015-03-18 16:49:02	Config Ok	1426715342.tar.gz			
2015-03-17 17:15:21	Config Ok	1426630521.tar.gz			
2015-03-17 16:48:02	Config Ok	1426628882.tar.gz			
2015-03-17 09:55:22	Config Ok	1426604122.tar.gz			
2015-03-17 05:15:17	Config Ok	1426587317.tar.gz			
2015-01-14 10:20:23	Config Error	1421252423.tar.gz			
2015-01-14 10:15:22	Config Error	1421252122.tar.gz			
2015-01-14 10:14:59	Config Error	1421252099.tar.gz			
2015-01-14 10:12:35	Config Error	1421251955.tar.gz			
2015-01-14 10:11:27	Config Error	1421251887.tar.gz			
2015-01-14 10:09:00	Config Error	1421251740.tar.gz			
2015-01-14 06:15:16	Config Error	1421237716.tar.gz			
2015-01-14 06:10:16	Config Error	1421237416.tar.gz			

Home Directory About

Nagios Exchange

Nagios Exchange is the central place where you'll find all types of Nagios projects: plugins, addons, documentation, extensions, and more. This site is designed for the Nagios Community to share its Nagios creations.

Have a new project for Nagios that you'd like to share? Just create an account and add it to the directory. (Read the FAQ)



Search Exchange

search...

 Advanced Search

Search All Sites

Download Nagios
 NOW AVAILABLE | [DOWNLOAD NOW](#)

Nagios Live Webinars
 Let our experts show you how Nagios can help your organization.

Contact Us
 Phone: 1-888-NAGIOS-1
 Email: sales@nagios.com

Login

Username:

Password:

Remember Me

Featured Project

Check_Interface_NetApp.pl
 /Category: SNMP
 Views: 29092

Project Categories

- Addons (739)
- Certified Compatible (2)
- Comparisons (7)
- Cool Stuff (110)
- Demos (4)
- Distributions (21)
- Documentation (208)
- Graphics and Logos (38)
- Media Coverage (8)
- Multimedia (151)
- Patches (24)
- Plugins (3687)
- Seedcamp (13)
- Translations (12)
- Tutorials (340)
- Utilities (31)

Popular Projects

Jump to the most requested...

Nagios XI Addons:

- Config Wizards
- Components

General Addons:

- Nagios BPI
- Escalation
- nagiosgraph
- Nagios V-Shell
- NRDP
- NSPE
- NSClient++
- Nageventlog

Project Stats

There are **4788** listings in **442** categories on Nagios Exchange!

Newest Nagios Projects

check_backup (for any backup system)

The check_backup plugin is designed to provide a generic way to check the status of backup processes by reading the contents of a file your scripts will leave either locally to the Nagios server, or on a remotely accessible host through ssh. The file it checks is in the format [timestamp] [extcode] on one line, [timestamp] is seconds since the epoch of backup completion, [extcode] is 0 for success. All of this is documented in the

Manage Users &

Notifications

Sending notifications when things go wrong on your network is extremely important. Making sure the person responsible for that device receives a notification is crucial. In the Admin panel, XI allows the management of users, notifications, and preference to ensure the right people are notified with the information necessary to resolve the issue.

Backups & Configuration

Snapshots

XI allows you to send critical monitoring data to an off-loaded data storage device. Schedule your system to run regular backups to ensure your data is never lost, or create local backups to restore from later.

Configuration Snapshots are taken after each 'Apply Configuration', storing the last 10 'good' and last 5 'bad' configuration files allowing users to archive, download, & restore from a previous configuration. The archive feature is perfect for storing milestone upgrades or configuration changes to roll back to if something goes wrong.

Extend Your Monitoring

Capabilities

Feature customization is where Nagios XI truly excels. Manage components, dashlets, Config Wizards, plugins, and MIBs all from the admin panel in XI. Adapt your monitoring solution to meet your exact specifications or upload custom created plugins to monitor your network. Choose from over 3500+ projects on the Nagios Exchange to make your monitoring fit your environment.

How Checks Work

- A node/host/device consists of one or more service checks (PING, HTTP, MYSQL, SSH, etc)
- Periodically Nagios checks each service for each node and determines if state has changed. State changes are:
 - CRITICAL
 - WARNING
 - UNKNOWN
- For each state change you can assign:
 - Notification options (as mentioned before)
 - Event handlers (scripts, actions to take)

How Checks Work

- **Parameters:** Set in `/etc/nagios3/nagios.cfg`:
 - Normal checking interval
 - Re-check interval
 - Maximum number of checks.
 - Period for each check
- Services check(s) only happen when a node responds (ping check or “is alive = yes”):
 - Remember a node can be:
 - DOWN
 - UNREACHABLE

(What's the difference?)

How Checks Work: 2

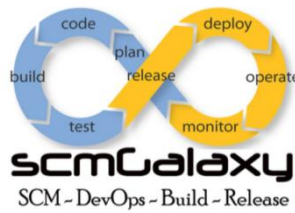
In this manner it can take some time before a host changes its state to “down” as Nagios first does a service check and then a node check.

By default Nagios does a node check 3 times before it will change the nodes state to down.

You can, of course, change all this.

- `/etc/nagios3/nagios.cfg`
- Lots of configuration settings and combinations
- Default settings have been tested for large install

GLOSSARY



Active Check

A check that is initiated and performed by Nagios Core or Nagios XI - usually on a pre-determined schedule. Plugins are used to perform active checks.

Agent

Software that is installed on servers/workstations so they can be monitored. Agents are available for Windows and Linux machines/servers. In contrast, agentless monitoring refers to the ability to monitor a machine without having to install an agent on it - usually using SNMP or WMI.

Alert

A check that is initiated and performed by Nagios Core or Nagios XI - usually on a pre-determined schedule. Plugins are used to perform

Auto-Discovery Wizard

Nagios XI has a builtin Auto-Discovery wizard. When running an Auto-Discovery job the user will enter an network of addresses they would like to scan and a job is created which utilizes fping and nmap to scan the network defined for alive machines and then performs an nmap scan on the host to determine which ports it is listening on. The results of the Auto-Discovery scan additionally report the OS of the machine discovered as well as all of the ports the host is listening on. A user can then optionally pass these results into a wizard that will monitor to make sure all of these ports continue to be responsive.

Config Snapshots

When the configuration is applied in Nagios XI a snapshot is made of the current configuration. These configuration snapshots are stored and used to automatically roll back to the last known good configuration if a configuration cannot be applied. Additionally, the configuration snapshots can be used to store good configurations and allow users to roll back to previously known good configurations.

Config Wizards

Configuration wizards guide users through the process of monitoring new devices, services, and applications – all without having to understand complex monitoring concepts. You can download Config Wizards at the Nagios Exchange.

Dashboard

In Nagios XI: A customizable page on which dashlets can be placed. Nagios XI offers each user the ability to have multiple dashboards for customized views of important data.

Dashlet

A moveable container that can be placed on a dashboard in Nagios XI. Different dashlets provide performance graphs, custom HTML, and other data.

Device

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems.

Host

In Nagios XI, a Host is a device that is monitored. Generally a server, VM, switch/router, or other network device.

Host Group

A host group is a collection of hosts that share access to storage array volumes. Creating host groups lets administrators use the combined processing power of the host group computers to access the volumes.

Nagios Exchange

Nagios Exchange is the central place where you'll find all types of Nagios projects - plugins, addons, documentation, extensions, and more. Nagios Exchange is designed for the Nagios Community to share its Nagios creations. Have a new project for Nagios that you'd like to share? Just create an account and add it to the directory.

Notification

Nagios supports optional escalation of contact notifications for hosts and services. Escalation of host and service notifications is accomplished by defining host escalations and service escalations in your object configuration file(s). Once a notification is escalated, the contact/groups and notification options for the object will be overridden by the escalation's settings.

NRDS

NRDS is a component pre-installed on a Nagios XI server that allows the administrator to create and manage configurations and plugins to be deployed with a passive agent that can be installed on a variety of operating systems including Windows, Linux, AIX & Solaris. The passive agents download the current configuration and the required plugin from the Nagios XI server and run the checks and posting the results to the XI server.

Passive Check

A check that is performed by an external application, operating system, or device and is submitted to Nagios Core or Nagios XI for processing. Some monitoring agents - including NSCA, NCPA, and NRDP can be used to send passive checks to Nagios. An SNMP trap is also considered a passive check.

Plugins

Plugins allow you to monitor anything and everything with Nagios - databases, operating systems, applications, network equipment, protocols and more. Nagios Plugins can be found on the Nagios Exchange.

Report

Nagios XI provides users the ability to measure effectiveness of specific hosts, services, and business processes to determine if service-level agreements are being met. Schedule reports to be sent on a recurring basis for quick and accurate network performance statistics.

Service

A metric on a particular Host that is being monitored. For example, CPU usage, Memory usage, or HDD space. Nagios XI pricing does not count the number of services someone wants to monitor.

Service Group

A service group definition is used to group one or more services together for simplifying configuration with object tricks or display purposes in the CGIs.

SNMP Trap

Simple Network Management Protocol (SNMP) is a protocol-based network management system. SNMP traps are alerts generated by agents on a managed device.

thank
thank
you!