Network Monitoring, Management and Automation

Nagios

npNOG 5

Dec 8 - 12, 2019



This material is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/)

Introduction

• Possibly the most used open source network monitoring software

Nagios & Core

- Web interface for viewing status, browsing history, scheduling downtime etc
- Sends out alerts via E-mail. Can be configured to use other mechanisms, e.g. SMS
- Nagios actively monitors the *availability* of
 - Hosts (devices)
 - Services

Nagios: Tactical Overview

Nagios	Tactical Monitorin		Monitoring Performance				
lugios	Last Updated: wed Nov Updated every 90 secon Nacios® Core™ 3.5.1 -	nds www.nagios.org		Service Check Execution	me: 0.00 / 10.02 / 2.384 sec		
General	Logged in as nagiosadr	nin		Service Check Latency:	0.01 / 0.19 / 0.088 sec		
Home				Host Check Execution Ti	me: 0.01 / 10.09 / 3.10 / sec		
Documentation				Host Check Latency:	0.0070.2470.080 sec		
Current Status			2	# Passive Host / Service C	Checks: 0/0		
Tactical Overview							
Мар							
Hosts	Network Outages	5		Networ	k Health		
Services	1 Outages			Host H	ealth:		
Host Groups	1 Blocking			10311			
Summary	Outages			Servic	e Health:		
Grid							
Service Groups							
Summary	Hosts						
Grid	4 Damm	Allenseshelt	0.11.	0 Danalin n			
Sonvices (Unbandled)	1 Down	4 Unreachable	2 Up	U Pending			
Hosts (Unbandled)	1 Unhandled	4 Unhandled					
Network Outages	Problems	Problems					
Quick Search							
Quick Search:	Services						
		0.144	0.11.1	0.01			
	10 Critical	0 warning	0 Unknown	<u>6 OK</u>	0 Pending		
Reports	9 on Problem Hosts						
Availability	1 Acknowledge	t					
Trends							
Alerts							
History	Monitoring Featu	res					
Summary	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks		
Notifications	All Services	All Services	All Services	All Service	All Services		
Fvent Log	Enabled	Enabled	Enabled	Enabled	Enabled		
Lvent Log	No Services	All Hosts Enab	All Hosts En	All Hosts E	Enabled All Hosts Enabled		
System	Flapping						
Comments	All Hosts Enab	ed					
Downtime	No Hosts Flapp	bing					
Process Info							
Performance Info							
Scheduling Queue							

npNOG5

Configuration

Nagios: Host Detail View

<u>Nagios</u>

General

Reports

System

Home **Documentation**

Current Status

Tactical Overview Мар Hosts Services Host Grou Summar Grid Service Gr Summar Grid Problems Services Hosts (L Network Quick Search

Current Network Status

Last Updated: Wed Nov 13 17:43:50 +0545 2019 Updated every 90 seconds Nagios® Core[™] 3.5.1 - www.nagios.org Logged in as nagiosadmin

View Service Status Detail For All Host Groups View Status Overview For All Host Groups View Status Summary For All Host Groups View Status Grid For All Host Groups

Host Status Totals								
Up Down Unreachable Pending								
9 1	4 5	0						
All Problems All Types								
	69	78	3					

Service Status Totals Ok Warning Unknown Critical Pending 22 0 0 129 0 All Problems All Types 129 151

?

Host Status Details For All Host Groups

HUSIS	Limit Doculto:	100				
Services			• -	A -	A -	
Host Groups	Host 🏞		Status 🏞	Last Check **	Duration **	Status Information
Summary Grid	gw-rtr	- Ç 🔒	UP	2019-11-13 17:42:26	123d 1h 45m 27s	PING OK - Packet loss = 0%, RTA = 0.12 ms
Service Groups	localhost	- 🗳 💁 -	UP	2019-11-13 17:39:36	124d 23h 8m 36s	PING OK - Packet loss = 0%, RTA = 0.03 ms
Summary Grid	noc	🍳 💁	UP	2019-11-13 17:39:36	124d 6h 8m 36s	PING OK - Packet loss = 0%, RTA = 0.03 ms
Problems	ns1	🛟 💁	UP	2019-11-13 17:39:46	124d 6h 8m 36s	PING OK - Packet loss = 0%, RTA = 0.91 ms
Services (Unhandled) Hosts (Unhandled)	ns2	🔅 🔒	UP	2019-11-13 17:39:46	124d 6h 8m 36s	PING OK - Packet loss = 0%, RTA = 0.06 ms
Network Outages	rtr1-g1	🕴 😫	UP	2019-11-13 17:39:56	20d 4h 11m 4s	PING OK - Packet loss = 0%, RTA = 7.37 ms
Quick Search:	rtr1-g10	3	DOWN	2019-11-13 17:39:56	121d 3h 53m 35s	CRITICAL - Host Unreachable (rtr1-g10.lab.workalaya.net)
	rtr1-g11	🙆 🖺	DOWN	2019-11-13 17:39:56	121d 3h 53m 35s	CRITICAL - Host Unreachable (rtr1-g11.lab.workalaya.net)
	rtr1-g12	送 😫	DOWN	2019-11-13 17:40:06	121d 3h 53m 25s	CRITICAL - Host Unreachable (rtr1-g12.lab.workalaya.net)
eports	rtr1-g2	🕴 🔼	DOWN	2019-11-13 17:39:06	19d 2h 6m 4s	CRITICAL - Host Unreachable (rtr1-g2.lab.workalaya.net)
Availability Trends	rtr1-g3	🛎 통	DOWN	2019-11-13 17:40:16	121d 3h 53m 25s	CRITICAL - Host Unreachable (rtr1-g3.lab.workalaya.net)
Alerts	rtr1-g4	🚨 🖺	DOWN	2019-11-13 17:40:16	121d 3h 53m 5s	CRITICAL - Host Unreachable (rtr1-g4.lab.workalaya.net)
History Summary	rtr1-g5	3	DOWN	2019-11-13 17:40:16	121d 3h 53m 5s	CRITICAL - Host Unreachable (rtr1-g5.lab.workalaya.net)
Histogram	rtr1-g6	🙆 🖺	DOWN	2019-11-13 17:40:26	121d 3h 53m 5s	CRITICAL - Host Unreachable (rtr1-g6.lab.workalaya.net)
Notifications Event Log	rtr1-g7	3	DOWN	2019-11-13 17:40:26	121d 3h 52m 55s	CRITICAL - Host Unreachable (rtr1-g7.lab.workalaya.net)
-	rtr1-g8	🙆 🖺	DOWN	2019-11-13 17:40:36	121d 4h 23m 55s	CRITICAL - Host Unreachable (rtr1-g8.lab.workalaya.net)
ystem	rtr1-g9	🙆 🖺	DOWN	2019-11-13 17:40:36	121d 3h 52m 55s	CRITICAL - Host Unreachable (rtr1-g9.lab.workalaya.net)
Comments Downtime	srv1-g1	08	UP	2019-11-13 17:39:06	19d 1h 45m 24s	PING OK - Packet loss = 0%, RTA = 19.96 ms
Process Info	srv1-g10	- 🗘 🔒	UNREACHABLE	2019-11-13 17:42:36	121d 4h 3m 55s	CRITICAL - Host Unreachable (srv1-g10.lab.workalaya.net)
Scheduling Queue	srv1-g11	🗘 💁	UNREACHABLE	2019-11-13 17:38:36	121d 4h 3m 55s	PING CRITICAL - Packet loss = 100%
Configuration	srv1-g12	🗘 🔒	UNREACHABLE	2019-11-13 17:39:26	121d 4h 3m 45s	PING CRITICAL - Packet loss = 100%

Nagios: Service Detail View

<u>Nagios</u>

General

Home Documentation

Current Status

Tactical Overview Мар

Current Network Status

Last Updated: Wed Nov 13 17:45:11 +0545 2019 Updated every 90 seconds Nagios® Core™ 3.5.1 - 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								
9	14	55		0				
All Problems All Types								
	(69	78	3				

Service Status Totals **Ok Warning Unknown Critical Pending** 0 0 129 0 All Problems All Types 129 151

22

?

Service Status Details For All Hosts

Hosts Services	Limit Results: 100 🗘 🕅 🕄 💭 Results 0 - 100 of 151 Matching Services								
Host Groups	Host * ₹		Service **	Status **	Last Check 🏞	Duration **	Attempt **	Status Information	
Summary Grid Service Groups Summary	gw-rtr	Q	DNS	ок	2019-11-13 17:43:47	0d 0h 11m 24s	1/4	DNS OK: 2.610 seconds response time www.google.com returns 172.217.166.36,2404:6800:4009:80c:::	
Grid			NTP	CRITICAL	2019-11-13 17:42:17	124d 6h 10m 27s	4/4	CRITICAL - Socket timeout after 10 seconds	
Services (Unhandled) Hosts (Unhandled)			SSH	ок	2019-11-13 17:44:48	124d 6h 7m 55s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu- 4ubuntu0.3 (protocol 2.0)	
Network Outages Quick Search:	localhost	Q	Current Load	ОК	2019-11-13 17:42:19	121d 4h 26m 53s	1/4	OK - load average: 0.04, 0.05, 0.07	
			Current Users	ОК	2019-11-13 17:44:50	124d 23h 9m 7s	1/4	USERS OK - 0 users currently logged	
Reports			Disk Space	ОК	2019-11-13 17:42:21	124d 23h 8m 17s	1/4	DISK OK	
Availability			Disk space /	CRITICAL	2019-11-13 17:44:52	123d 21h 24m 35s	4/4	(null)	
Trends Alerts			NAGIOS	ОК	2019-11-13 17:42:23	123d 20h 15m 14s	1/4	HTTP OK: HTTP/1.1 200 OK - 1065 by in 0.002 second response time	
Summary Histogram Notifications			SNMP	ок	2019-11-13 17:44:56	123d 1h 36m 22s	1/4	SNMP OK - Linux noc 4.15.0-58-gener #64-Ubuntu SMP Tue Aug 6 11:12:41 L 2019 x86_64	
Event Log			SSH	ОК	2019-11-13 17:42:25	123d 1h 44m 1s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu- 4ubuntu0.3 (protocol 2.0)	
Comments			Total Processes	ОК	2019-11-13 17:44:56	123d 1h 42m 27s	1/4	PROCS OK: 50 processes	
Downtime Process Info Performance Info	noc	Q	HTTP	ОК	2019-11-13 17:42:27	122d 1h 35m 3s	1/4	HTTP OK: HTTP/1.1 302 Found - 1312 bytes in 0.038 second response time	
Scheduling Queue Configuration			SSH	ок	2019-11-13 17:44:58	122d 1h 33m 1s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu- 4ubuntu0.3 (protocol 2.0)	

Features

- Utilizes topology to determine dependencies.
 - Differentiates between what is *down* vs. what is *unreachable*. Avoids running unnecessary checks and sending redundant alarms
- Allows you to define how to send notifications 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

Plugins

Plugins are used to verify services and devices:

- Nagios architecture is simple enough that writing new plugins is fairly easy in the language of your choice.
- There are many, many plugins available (thousands).
 - o http://exchange.nagios.org/
 - o http://nagiosplugins.org/



Pre-installed Plugins for Ubuntu

/usr/lib/nagios/plugins

check_apt check_breeze check_by_ssh check_clamd check_cluster check_dbi check_dhcp check_dig check_disk check_disk_smb check_dns check_dummy check_file_age check_flexlm check_fping check_ftp check_game check_host check_host check_hpjd check_http check_icmp check_ide_smart check_ifoperstatus check_ifstatus check_imap check_ircd check_jabber check_ldap check_ldaps check_load check_log check_mailq check_mrtg check_mrtg check_mysql check_mysql_query

check_nagios check_nntp check_ntps check_ntp check_ntp_peer check_ntp_time check_nwstat check_oracle check_overcr check_pgsql check_ping check_pop check_procs check_real check_rpc check_rta_multi check_sensors check_simap check_smtp check_snmp check_spop check_ssh check_ssmtp check_swap check_tcp check_upe check_ups check_users check_wave negate urlize utils.pm utils.sh

/usr/lib/nagios/plugins

disk.cfg ftp.cfg ldap.cfg mysql.cfg pgsql.cfg snmp.cfg	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 mailq.cfg mrtg.cfg mysql.cfg	netware.cfg news.cfg nt.cfg ntp.cfg pgsql.cfg	ping.cfg procs.cfg real.cfg rpc-nfs.cfg snmp.cfg	ssh.cfg tcp_udp.cfg telnet.cfg users.cfg
--	---	--	--	--	---	--	---

How Checks Work

- Periodically nagios calls a plugin to test the state of each service. Possible Responses are:
 - **OK**
 - WARNING
 - CRITICAL
 - UNKNOWN
- If a service is not OK it goes into a "soft" error state.
 After a number of retries (default 3) it goes into a "hard" error state. At that point an alert is sent.
- You can also trigger external event handlers based on these state transitions

How Checks Work (Continued)

Parameters

- Normal checking interval
- Retry interval (i.e. when not OK)
- Maximum number of retries
- Time period for performing checks
- Time period for sending notifications

Scheduling

- Nagios spreads its checks throughout the time period to even out the workload
- Web UI shows when next check is scheduled

Hierarchy: The Concept of Parents

Hosts can have parents:

- The parent of a server connected to a switch would be the switch or router.
- Allows us to specify the dependencies between devices.
- Avoids sending alarms when parent does not respond.
- A node can have multiple parents (dual homed).



Network Viewpoint

- Where you locate your Nagios server will determine your point of view of the network
- The Nagios server becomes the "root" of your dependency tree



Demo of Nagios http://noc.lab.workalaya.net/nagios3/

nagioisadmin/<lab_password>

More Features

- Allows you to acknowledge an event
 A user can add comments via the GUI
- You can define maintenance periods
 - By device or a group of devices
- Maintains availability statistics and generates reports
- Can detect flapping and suppress additional notifications
- Allows for multiple notification methods:
 e-mail, pager, SMS, winpopup, audio, etc...
- Allows you to define notification levels for escalation

More info and documentation

- Nagios web site https://www.nagios.org/
- Nagios plugins site https://nagios-plugins.org/
- Nagios Exchange site https://exchange.nagios.org/
- A Debian tutorial on Nagios http://www.debianhelp.co.uk/nagios.htm
- Commercial Nagios support http://www.nagios.com/

