

Nagios Version 3.x Documentation

Copyright © 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Ethan Galstad, Nagios Enterprises

Nagios and the Nagios logo are registered trademarks of Ethan Galstad. All other trademarks, servicemarks, registered trademarks, and registered servicemarks mentioned herein may be the property of their respective owner(s). The information contained herein is provided 'AS IS' with 'NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.'

Nagios is licensed under the terms of the GNU General Public License Version 2 as published by the Free Software Foundation. This gives you legal permission to copy, distribute and/or modify Nagios under certain conditions. Read the 'LICENSE' file in the Nagios distribution or read the online version of the license for more details.

Nagios is provided 'AS IS' with 'NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.'

COLLABORATORS

	<i>TITLE :</i> Nagios Version 3.x Documentation		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY	Ethan Galstad	February 10, 2010	
HTML to Docbook transformation	Sébastien Guilbaud	February 10, 2010	
HTML to Docbook transformation	Olivier Jan	February 10, 2010	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME
2	2008-11-28	First docbook beta release	sg, oj
1	2008-11-13	First Release	eg

Contents

I	About	1
1	About Nagios	2
1.1	What Is This?	2
1.2	System Requirements	2
1.3	Licensing	3
1.4	Acknowledgements	3
1.5	Downloading The Latest Version	3
1.6	Support	3
2	What's New in Nagios 3	4
2.1	Change Log	4
2.2	Changes and New Features	4
2.2.1	Documentation	4
2.2.2	Macros	4
2.2.3	Scheduled Downtime	5
2.2.4	Comments	5
2.2.5	State Retention Data	5
2.2.6	Flap Detection	5
2.2.7	External Commands	6
2.2.8	Status Data	6
2.2.9	Embedded Perl	6
2.2.10	Adaptive Monitoring	6
2.2.11	Notifications	6
2.2.12	Object Definitions	6
2.2.13	Object Inheritance	7
2.2.14	Performance Improvements	7
2.2.15	Plugin Output	8
2.2.16	Service Checks	8
2.2.17	Host Checks	8

2.2.18	Freshness checks	8
2.2.19	IPC	9
2.2.20	Timeperiods	9
2.2.21	Event Broker	9
2.2.22	Web Interface	9
2.2.23	Debugging Info	9
2.2.24	Misc	10

II Getting Started 11

3 Advice for Beginners 12

4 Quickstart Installation Guides 13

4.1	Guides	1
4.2	Post-Installation Modifications	1

5 Fedora Quickstart 2

5.1	What You'll End Up With	1
5.2	Prerequisites	1
5.3	Create Account Information	1
5.4	Download Nagios and the Plugins	2
5.5	Compile and Install Nagios	2
5.6	Customize Configuration	2
5.7	Configure the Web Interface	3
5.8	Compile and Install the Nagios Plugins	3
5.9	Start Nagios	3
5.10	Modify SELinux Settings	3
5.11	Login to the Web Interface	4
5.12	Other Modifications	4
5.13	You're Done	4

6 openSUSE Quickstart 5

6.1	Required Packages	1
6.2	Create Account Information	1
6.3	Download Nagios and the Plugins	1
6.4	Compile and Install Nagios	1
6.5	Customize Configuration	2
6.6	Configure the Web Interface	2
6.7	Compile and Install the Nagios Plugins	2
6.8	Start Nagios	3
6.9	Login to the Web Interface	3
6.10	Other Modifications	3

7	Ubuntu Quickstart	4
7.1	What You'll End Up With	1
7.2	Required Packages	1
7.3	Create Account Information	1
7.4	Download Nagios and the Plugins	2
7.5	Compile and Install Nagios	2
7.6	Customize Configuration	2
7.7	Configure the Web Interface	3
7.8	Compile and Install the Nagios Plugins	3
7.9	Start Nagios	3
7.10	Login to the Web Interface	3
7.11	Other Modifications	4
8	Upgrading Nagios	5
8.1	Upgrading From Previous Nagios 3.x Releases	5
8.2	Upgrading From Nagios 2.x	6
8.3	Upgrading From an RPM Installation	6
9	Monitoring Windows Machines	7
9.1	Introduction	1
9.2	Overview	1
9.3	Steps	1
9.4	What's Already Done For You	2
9.5	Prerequisites	2
9.6	Installing the Windows Agent	2
9.7	Configuring Nagios	3
9.8	Password Protection	5
9.9	Restarting Nagios	5
10	Monitoring Linux/Unix Machines	6
10.1	Introduction	1
10.2	Overview	1
11	Monitoring Network Servers	2
11.1	External Resources	1
12	Monitoring Network Printers	2
12.1	Introduction	1
12.2	Overview	1
12.3	Steps	2
12.4	What's Already Done For You	2
12.5	Prerequisites	2
12.6	Configuring Nagios	2
12.7	Restarting Nagios	3

13 Monitoring Routers and Switches	4
13.1 Introduction	1
13.2 Overview	1
13.3 Steps	2
13.4 What's Already Done For You	2
13.5 Prerequisites	2
13.6 Configuring Nagios	2
13.7 Monitoring Services	3
13.8 Monitoring Packet Loss and RTA	3
13.9 Monitoring SNMP Status Information	4
13.10 Monitoring Bandwidth / Traffic Rate	4
13.11 Restarting Nagios	5
14 Monitoring Publicly Available Services	6
14.1 Introduction	1
14.2 Plugins For Monitoring Services	1
14.3 Creating A Host Definition	1
14.4 Creating Service Definitions	2
14.5 Monitoring HTTP	2
14.6 Monitoring FTP	3
14.7 Monitoring SSH	3
14.8 Monitoring SMTP	4
14.9 Monitoring POP3	4
14.10 Monitoring IMAP	5
14.11 Restarting Nagios	5
III Configuring Nagios	6
15 Configuration Overview	7
15.1 Introduction	7
15.2 Main Configuration File	7
15.3 Resource File(s)	8
15.4 Object Definition Files	8
15.5 CGI Configuration File	8

16 Main Configuration File Options	9
16.1 Sample Configuration File	9
16.2 Config File Location	9
16.3 Configuration File Variables	9
16.3.1 Log File	9
16.3.2 Object Configuration File	10
16.3.3 Object Configuration Directory	10
16.3.4 Object Cache File	10
16.3.5 Precached Object File	11
16.3.6 Resource File	11
16.3.7 Temp File	11
16.3.8 Temp Path	11
16.3.9 Status File	12
16.3.10 Status File Update Interval	12
16.3.11 Nagios User	12
16.3.12 Nagios Group	13
16.3.13 Notifications Option	13
16.3.14 Service Check Execution Option	13
16.3.15 Passive Service Check Acceptance Option	14
16.3.16 Host Check Execution Option	14
16.3.17 Passive Host Check Acceptance Option	15
16.3.18 Event Handler Option	15
16.3.19 Log Rotation Method	16
16.3.20 Log Archive Path	16
16.3.21 External Command Check Option	16
16.3.22 External Command Check Interval	17
16.3.23 External Command File	17
16.3.24 External Command Buffer Slots	17
16.3.25 Lock File	18
16.3.26 State Retention Option	18
16.3.27 State Retention File	19
16.3.28 Automatic State Retention Update Interval	19
16.3.29 Use Retained Program State Option	19
16.3.30 Use Retained Scheduling Info Option	19
16.3.31 Retained Host and Service Attribute Masks	20
16.3.32 Retained Process Attribute Masks	20
16.3.33 Retained Contact Attribute Masks	21
16.3.34 Syslog Logging Option	21
16.3.35 Notification Logging Option	21

16.3.36 Service Check Retry Logging Option	22
16.3.37 Host Check Retry Logging Option	22
16.3.38 Event Handler Logging Option	22
16.3.39 Initial States Logging Option	23
16.3.40 External Command Logging Option	23
16.3.41 Passive Check Logging Option	23
16.3.42 Global Host Event Handler Option	24
16.3.43 Global Service Event Handler Option	24
16.3.44 Inter-Check Sleep Time	24
16.3.45 Service Inter-Check Delay Method	25
16.3.46 Maximum Service Check Spread	25
16.3.47 Service Interleave Factor	26
16.3.48 Maximum Concurrent Service Checks	26
16.3.49 Check Result Reaper Frequency	26
16.3.50 Maximum Check Result Reaper Time	27
16.3.51 Check Result Path	27
16.3.52 Max Check Result File Age	27
16.3.53 Host Inter-Check Delay Method	28
16.3.54 Maximum Host Check Spread	28
16.3.55 Timing Interval Length	28
16.3.56 Auto-Rescheduling Option	29
16.3.57 Auto-Rescheduling Interval	29
16.3.58 Auto-Rescheduling Window	29
16.3.59 Aggressive Host Checking Option	30
16.3.60 Translate Passive Host Checks Option	30
16.3.61 Passive Host Checks Are SOFT Option	31
16.3.62 Predictive Host Dependency Checks Option	31
16.3.63 Predictive Service Dependency Checks Option	31
16.3.64 Cached Host Check Horizon	32
16.3.65 Cached Service Check Horizon	32
16.3.66 Large Installation Tweaks Option	32
16.3.67 Child Process Memory Option	32
16.3.68 Child Processes Fork Twice	33
16.3.69 Environment Macros Option	33
16.3.70 Flap Detection Option	34
16.3.71 Low Service Flap Threshold	34
16.3.72 High Service Flap Threshold	34
16.3.73 Low Host Flap Threshold	35
16.3.74 High Host Flap Threshold	35

16.3.75 Soft State Dependencies Option	35
16.3.76 Service Check Timeout	36
16.3.77 Host Check Timeout	36
16.3.78 Event Handler Timeout	36
16.3.79 Notification Timeout	37
16.3.80 Obsessive Compulsive Service Processor Timeout	37
16.3.81 Obsessive Compulsive Host Processor Timeout	37
16.3.82 Performance Data Processor Command Timeout	37
16.3.83 Obsess Over Services Option	38
16.3.84 Obsessive Compulsive Service Processor Command	38
16.3.85 Obsess Over Hosts Option	38
16.3.86 Obsessive Compulsive Host Processor Command	39
16.3.87 Performance Data Processing Option	39
16.3.88 Host Performance Data Processing Command	39
16.3.89 Service Performance Data Processing Command	40
16.3.90 Host Performance Data File	40
16.3.91 Service Performance Data File	40
16.3.92 Host Performance Data File Template	41
16.3.93 Service Performance Data File Template	41
16.3.94 Host Performance Data File Mode	41
16.3.95 Service Performance Data File Mode	42
16.3.96 Host Performance Data File Processing Interval	42
16.3.97 Service Performance Data File Processing Interval	42
16.3.98 Host Performance Data File Processing Command	42
16.3.99 Service Performance Data File Processing Command	43
16.3.100 Orphaned Service Check Option	43
16.3.101 Orphaned Host Check Option	43
16.3.102 Service Freshness Checking Option	44
16.3.103 Service Freshness Check Interval	44
16.3.104 Host Freshness Checking Option	45
16.3.105 Host Freshness Check Interval	45
16.3.106 Additional Freshness Threshold Latency Option	45
16.3.107 Embedded Perl Interpreter Option	45
16.3.108 Embedded Perl Implicit Use Option	46
16.3.109 Date Format	46
16.3.110 Timezone Option	46
16.3.111 Illegal Object Name Characters	47
16.3.112 Illegal Macro Output Characters	47
16.3.113 Regular Expression Matching Option	48

16.3.114	True Regular Expression Matching Option	48
16.3.115	Administrator Email Address	48
16.3.116	Administrator Pager	49
16.3.117	Event Broker Options	49
16.3.118	Event Broker Modules	49
16.3.119	Debug File	50
16.3.120	Debug Level	50
16.3.121	Debug Verbosity	51
16.3.122	Maximum Debug File Size	51

17 Object Configuration Overview 52

17.1	What Are Objects?	52
17.2	Where Are Objects Defined?	52
17.3	How Are Objects Defined?	53
17.4	Objects Explained	53
17.4.1	Hosts	53
17.4.2	Host Groups	53
17.4.3	Services	53
17.4.4	Service Groups	53
17.4.5	Contacts	53
17.4.6	Contact Groups	54
17.4.7	Timeperiods	54
17.4.8	Commands	54

18 Object Definitions 55

18.1	Introduction	55
18.2	Retention Notes	55
18.3	Sample Configuration Files	55
18.4	Object Types	56
18.4.1	Host Definition	56
18.4.1.1	Description	56
18.4.1.2	Definition Format	56
18.4.1.3	Example Definition	57
18.4.1.4	Directive Descriptions	57
18.4.2	Host Group Definition	61
18.4.2.1	Description	61
18.4.2.2	Definition Format	61
18.4.2.3	Example Definition	61
18.4.2.4	Directive Descriptions	61

18.4.3	Service Definition	62
18.4.3.1	Description	62
18.4.3.2	Definition Format	62
18.4.3.3	Example Definition	63
18.4.3.4	Directive Descriptions:	63
18.4.4	Service Group Definition	67
18.4.4.1	Description	67
18.4.4.2	Definition Format	67
18.4.4.3	Example Definition	67
18.4.4.4	Directive Descriptions:	67
18.4.5	Contact Definition	68
18.4.5.1	Description	68
18.4.5.2	Definition Format	68
18.4.5.3	Example Definition	68
18.4.5.4	Directive Descriptions	69
18.4.6	Contact Group Definition	70
18.4.6.1	Description	70
18.4.6.2	Definition Format:	71
18.4.6.3	Example Definition:	71
18.4.6.4	Directive Descriptions:	71
18.4.7	Time Period Definition	71
18.4.7.1	Description	71
18.4.7.2	Definition Format	71
18.4.7.3	Example Definitions	72
18.4.7.4	Directive Descriptions	73
18.4.8	Command Definition	73
18.4.8.1	Description	73
18.4.8.2	Definition Format	73
18.4.8.3	Example Definition	74
18.4.8.4	Directive Descriptions	74
18.4.9	Service Dependency Definition	74
18.4.9.1	Description	74
18.4.9.2	Definition Format	74
18.4.9.3	Example Definition	75
18.4.9.4	Directive Descriptions	75
18.4.10	Service Escalation Definition	76
18.4.10.1	Description	76
18.4.10.2	Definition Format	76
18.4.10.3	Example Definition	76

18.4.10.4 Directive Descriptions	77
18.4.11 Host Dependency Definition	78
18.4.11.1 Description	78
18.4.11.2 Definition Format	78
18.4.11.3 Example Definition	78
18.4.11.4 Directive Descriptions	78
18.4.12 Host Escalation Definition	79
18.4.12.1 Description	79
18.4.12.2 Definition Format	79
18.4.12.3 Example Definition	80
18.4.12.4 Directive Descriptions	80
18.4.13 Extended Host Information Definition	81
18.4.13.1 Description	81
18.4.13.2 Definition Format	81
18.4.13.3 Example Definition:	81
18.4.13.4 Variable Descriptions	81
18.4.14 Extended Service Information Definition	82
18.4.14.1 Description	82
18.4.14.2 Definition Format	83
18.4.14.3 Example Definition	83
18.4.14.4 Variable Descriptions	83
19 Custom Object Variables	85
19.1 Introduction	85
19.2 Custom Variable Basics	85
19.3 Examples	85
19.4 Custom Variables As Macros	86
19.5 Custom Variables And Inheritance	86
20 CGI Configuration File Options	87
20.1 Sample Configuration	87
20.2 Config File Location	87
20.3 Configuration File Variables	87
20.3.1 Main Configuration File Location	87
20.3.2 Physical HTML Path	88
20.3.3 URL HTML Path	88
20.3.4 Authentication Usage	88
20.3.5 Default User Name	88
20.3.6 System/Process Information Access	89

20.3.7	System/Process Command Access	89
20.3.8	Configuration Information Access	89
20.3.9	Global Host Information Access	89
20.3.10	Global Host Command Access	89
20.3.11	Global Service Information Access	90
20.3.12	Global Service Command Access	90
20.3.13	Lock Author Names	90
20.3.14	Statusmap CGI Background Image	90
20.3.15	Default Statusmap Layout Method	91
20.3.16	Statuswrl CGI Include World	91
20.3.17	Default Statuswrl Layout Method	91
20.3.18	CGI Refresh Rate	92
20.3.19	Audio Alerts	92
20.3.20	Ping Syntax	92
20.3.21	Escape HTML Tags Option	92
20.3.22	Notes URL Target	92
20.3.23	Action URL Target	93
20.3.24	Splunk Integration Option	93
20.3.25	Splunk URL	93

21 Authentication And Authorization In The CGIs **94**

21.1	Introduction	94
21.2	Definitions	94
21.3	Setting Up Authenticated Users	94
21.4	Enabling Authentication/Authorization Functionality In The CGIs	94
21.5	Default Permissions To CGI Information	95
21.6	Granting Additional Permissions To CGI Information	96
21.7	CGI Authorization Requirements	96
21.8	Authentication On Secured Web Servers	96

IV Running Nagios **97**

22 Verifying Your Configuration **98**

22.1	Verifying Your Configuration	98
------	--	----

23 Starting and Stopping Nagios **99**

23.1	Starting Nagios	99
23.2	Restarting Nagios	99
23.3	Stopping Nagios	100

V	The Basics	101
24	Nagios Plugins	102
24.1	Introduction	102
24.2	What Are Plugins?	102
24.3	Plugins As An Abstraction Layer	103
24.4	What Plugins Are Available?	103
24.5	Obtaining Plugins	104
24.6	How Do I Use Plugin X?	104
24.7	Plugin API	104
25	Understanding Macros and How They Work	105
25.1	Macros	105
25.2	Macro Substitution - How Macros Work	105
25.3	Example 1: Host Address Macro	105
25.4	Example 2: Command Argument Macros	106
25.5	On-Demand Macros	106
25.6	On-Demand Group Macros	107
25.7	Custom Variable Macros	107
25.8	Macro Cleansing	108
25.9	Macros as Environment Variables	108
25.10	Available Macros	108
26	Standard Macros in Nagios	109
26.1	Macro Validity	109
26.2	Macro Availability Chart	109
26.3	Macro Descriptions	115
26.4	Notes	126
27	Host Checks	127
27.1	Introduction	127
27.2	When Are Host Checks Performed?	127
27.3	Cached Host Checks	127
27.4	Dependencies and Checks	128
27.5	Parallelization of Host Checks	128
27.6	Host States	128
27.7	Host State Determination	128
27.8	Host State Changes	129

28 Service Checks	130
28.1 Introduction	130
28.2 When Are Service Checks Performed?	130
28.3 Cached Service Checks	130
28.4 Dependencies and Checks	130
28.5 Parallelization of Service Checks	130
28.6 Service States	131
28.7 Service State Determination	131
28.8 Services State Changes	131
29 Active Checks	132
29.1 Introduction	132
29.2 How Are Active Checks Performed?	132
29.3 When Are Active Checks Executed?	133
30 Passive Checks	134
30.1 Introduction	134
30.2 Uses For Passive Checks	134
30.3 How Passive Checks Work	135
30.4 Enabling Passive Checks	135
30.5 Submitting Passive Service Check Results	136
30.6 Submitting Passive Host Check Results	136
30.7 Passive Checks and Host States	137
30.8 Submitting Passive Check Results From Remote Hosts	137
31 State Types	138
31.1 Introduction	138
31.2 Service and Host Check Retries	138
31.3 Soft States	138
31.4 Hard States	139
31.5 Example	139
32 Time Periods	141
32.1 Introduction	1
32.2 Precedence in Time Periods	1
32.3 How Time Periods Work With Host and Service Checks	1
32.4 How Time Periods Work With Contact Notifications	2
32.5 How Time Periods Work With Notification Escalations	2
32.6 How Time Periods Work With Dependencies	2

33	Determining Status and Reachability of Network Hosts	3
33.1	Introduction	3
33.2	Example Network	3
33.3	Defining Parent/Child Relationships	4
33.4	Reachability Logic in Action	6
33.5	UNREACHABLE States and Notifications	8
34	Notifications	9
34.1	Introduction	9
34.2	When Do Notifications Occur?	9
34.3	Who Gets Notified?	9
34.4	What Filters Must Be Passed In Order For Notifications To Be Sent?	10
34.5	Program-Wide Filter:	10
34.6	Service and Host Filters:	10
34.7	Contact Filters:	11
34.8	Notification Methods	11
34.9	Notification Type Macro	11
34.10	Helpful Resources	12
35	Information On The CGIs	14
35.1	Introduction	14
35.2	Status CGI	14
35.3	Status Map CGI	14
35.4	WAP Interface CGI	15
35.5	Status World CGI (VRML)	16
35.6	Tactical Overview CGI	16
35.7	Network Outages CGI	17
35.8	Configuration CGI	18
35.9	Command CGI	18
35.10	Extended Information CGI	19
35.11	Event Log CGI	19
35.12	Alert History CGI	20
35.13	Notifications CGI	21
35.14	Trends CGI	21
35.15	Availability Reporting CGI	22
35.16	Alert Histogram CGI	22
35.17	Alert Summary CGI	23

VI	Advanced Topics	24
36	External Commands	25
36.1	Introduction	25
36.2	Enabling External Commands	25
36.3	When Does Nagios Check For External Commands?	26
36.4	Using External Commands	26
36.5	Command Format	26
37	Event Handlers	27
37.1	Introduction	27
37.2	When Are Event Handlers Executed?	27
37.3	Event Handler Types	28
37.4	Enabling Event Handlers	28
37.5	Event Handler Execution Order	28
37.6	Writing Event Handler Commands	28
37.7	Permissions For Event Handler Commands	29
37.8	Service Event Handler Example	29
38	Volatile Services	32
38.1	Introduction	32
38.2	What Are They Useful For?	32
38.3	What's So Special About Volatile Services?	32
38.4	The Power Of Two	33
38.4.1	Nagios Configuration	33
38.4.2	PortSentry Configuration	33
38.4.3	Port Scan Script	33
39	Service and Host Freshness Checks	35
39.1	Introduction	35
39.2	How Does Freshness Checking Work?	35
39.3	Enabling Freshness Checking	36
39.4	Example	36
40	Distributed Monitoring	38
40.1	Introduction	38
40.2	Goals	38
40.3	Reference Diagram	38
40.4	Central Server vs. Distributed Servers	40
40.5	Obtaining Service Check Information From Distributed Monitors	40
40.6	Distributed Server Configuration	40

40.7	Central Server Configuration	42
40.8	Problems With Passive Checks	42
40.9	Freshness Checking	43
40.10	Performing Host Checks	43
41	Redundant and Failover Network Monitoring	45
41.1	Introduction	45
41.2	Prerequisites	45
41.3	Sample Scripts	45
41.4	Scenario 1 - Redundant Monitoring	45
41.4.1	Introduction	45
41.4.2	Goals	46
41.4.3	Network Layout Diagram	46
41.4.4	Initial Program Settings	46
41.4.5	Initial Configuration	46
41.4.6	Event Handler Command Definitions	47
41.4.7	Event Handler Scripts	47
41.4.8	What This Does For Us	48
41.4.9	Time Lags	48
41.4.10	Special Cases	49
41.5	Scenario 2 - Failover Monitoring	49
41.5.1	Introduction	49
41.5.2	Goals	49
41.5.3	Initial Program Settings	50
41.5.4	Master Process Check	50
41.5.5	Additional Issues	50
42	Detection and Handling of State Flapping	51
42.1	Introduction	51
42.2	How Flap Detection Works	51
42.3	Example	51
42.4	Flap Detection for Services	53
42.5	Flap Detection for Hosts	53
42.6	Flap Detection Thresholds	53
42.7	States Used For Flap Detection	53
42.8	Flap Handling	54
42.9	Enabling Flap Detection	54

43 Notification Escalations	55
43.1 Introduction	55
43.2 When Are Notifications Escalated?	55
43.3 Contact Groups	56
43.4 Overlapping Escalation Ranges	56
43.5 Recovery Notifications	57
43.6 Notification Intervals	57
43.7 Time Period Restrictions	59
43.8 State Restrictions	59
44 On-Call Rotations	60
44.1 Introduction	60
44.2 Scenario 1: Holidays and Weekends	60
44.3 Scenario 2: Alternating Days	61
44.4 Scenario 3: Alternating Weeks	62
44.5 Scenario 4: Vacation Days	63
44.6 Other Scenarios	64
45 Monitoring Service and Host Clusters	65
45.1 Introduction	65
45.2 Plan of Attack	65
45.3 Using the check_cluster Plugin	66
45.4 Monitoring Service Clusters	66
45.5 Monitoring Host Clusters	66
46 Host and Service Dependencies	68
46.1 Introduction	68
46.2 Service Dependencies Overview	68
46.3 Defining Service Dependencies	68
46.4 Example Service Dependencies	68
46.5 How Service Dependencies Are Tested	70
46.6 Execution Dependencies	71
46.7 Notification Dependencies	71
46.8 Dependency Inheritance	71
46.9 Host Dependencies	72
46.10Example Host Dependencies	72
47 State Stalking	74
47.1 Introduction	74
47.2 How Does It Work?	74
47.3 Should I Enable Stalking?	75
47.4 How Do I Enable Stalking?	75
47.5 How Does Stalking Differ From Volatile Services?	75
47.6 Caveats	75

48 Performance Data	76
48.1 Introduction	76
48.2 Types of Performance Data	76
48.3 Plugin Performance Data	76
48.4 Processing Performance Data	77
48.5 Processing Performance Data Using Commands	77
48.6 Writing Performance Data To Files	78
49 Scheduled Downtime	79
49.1 Introduction	79
49.2 Scheduling Downtime	79
49.3 Fixed vs. Flexible Downtime	79
49.4 Triggered Downtime	80
49.5 How Scheduled Downtime Affects Notifications	80
49.6 Overlapping Scheduled Downtime	80
50 Using The Embedded Perl Interpreter	81
50.1 Introduction	81
50.2 Advantages	82
50.3 Disadvantages	82
50.4 Using The Embedded Perl Interpreter	83
50.5 Compiling Nagios With Embedded Perl	83
50.6 Plugin-Specific Use of the Perl Interpreter	83
50.7 Developing Plugins For Use With Embedded Perl	83
51 Adaptive Monitoring	84
51.1 Introduction	84
51.2 What Can Be Changed?	84
51.3 External Commands For Adaptive Monitoring	85
52 Predictive Dependency Checks	86
52.1 Introduction	86
52.2 How Do Predictive Checks Work?	86
52.3 Enabling Predictive Checks	87
52.4 Cached Checks	87
53 Cached Checks	88
53.1 Introduction	88
53.2 For On-Demand Checks Only	88
53.3 How Caching Works	89
53.4 What This Really Means	89
53.5 Configuration Variables	90
53.6 Optimizing Cache Effectiveness	90

54	Passive Host State Translation	93
54.1	Introduction	93
54.2	Different World Views	93
54.3	Enabling State Translation	94
55	Service and Host Check Scheduling	95
55.1	TODO	95
56	Custom CGI Headers and Footers	96
56.1	Introduction	96
56.2	How Does It Work?	96
57	Object Inheritance	97
57.1	Introduction	97
57.2	Basics	97
57.3	Local Variables vs. Inherited Variables	97
57.4	Inheritance Chaining	98
57.5	Using Incomplete Object Definitions as Templates	99
57.6	Custom Object Variables	100
57.7	Cancelling Inheritance of String Values	100
57.8	Additive Inheritance of String Values	101
57.9	Implied Inheritance	101
57.10	Implied/Additive Inheritance in Escalations	102
57.11	Multiple Inheritance Sources	103
57.12	Precedence With Multiple Inheritance Sources	103
58	Time-Saving Tricks For Object Definitions	105
58.1	Introduction	1
58.2	Regular Expression Matching	1
58.3	Service Definitions	1
58.3.1	Multiple Hosts:	1
58.3.2	All Hosts In Multiple Hostgroups:	2
58.3.3	All Hosts:	2
58.3.4	Excluding Hosts:	2
58.4	Service Escalation Definitions	2
58.4.1	Multiple Hosts:	2
58.4.2	All Hosts In Multiple Hostgroups:	3
58.4.3	All Hosts:	3
58.4.4	Excluding Hosts:	3
58.4.5	All Services On Same Host:	3

58.4.6	Multiple Services On Same Host:	4
58.4.7	All Services In Multiple Servicegroups:	4
58.5	Service Dependency Definitions	4
58.5.1	Multiple Hosts:	4
58.5.2	All Hosts In Multiple Hostgroups:	4
58.5.3	All Services On A Host:	5
58.5.4	Multiple Services On A Host:	5
58.5.5	All Services In Multiple Servicegroups:	5
58.5.6	Same Host Dependencies:	5
58.6	Host Escalation Definitions	6
58.6.1	Multiple Hosts:	6
58.6.2	All Hosts In Multiple Hostgroups:	6
58.6.3	All Hosts:	6
58.6.4	Excluding Hosts:	6
58.7	Host Dependency Definitions	7
58.7.1	Multiple Hosts:	7
58.7.2	All Hosts In Multiple Hostgroups:	7
58.8	Hostgroups	7
58.8.1	All Hosts:	7

VII Security and Performance Tuning **8**

59 Security Considerations **9**

59.1	Introduction	9
59.2	Best Practices	9

60 Enhanced CGI Security and Authentication **13**

60.1	Introduction	13
60.2	Additional Techniques	13
60.2.1	Implementing Digest Authentication	13
60.2.2	Implementing Forced TLS/SSL	14
60.2.3	Implementing IP subnet lockdown	15
60.3	Important Notes	15

61 Tuning Nagios For Maximum Performance **16**

61.1	Introduction	16
61.2	Optimization Tips:	16

62 Fast Startup Options	19
62.1 Introduction	19
62.2 Background	19
62.3 Evaluating Startup Times	20
62.4 Pre-Caching Object Configuration	21
62.5 Skipping Circular Path Tests	21
62.6 Putting It All Together	22
63 Large Installation Tweaks	23
63.1 Introduction	23
63.2 Effects	23
64 Using The Nagiosstats Utility	24
64.1 Introduction	24
64.2 Usage Information	24
64.3 Human-Readable Output	24
64.4 MRTG Integration	25
65 Graphing Performance Info With MRTG	26
65.1 Introduction	26
65.2 Sample MRTG Configuration	26
65.3 Example Graphs	26
VIII Integration With Other Software	31
66 Integration Overview	32
66.1 Introduction	32
66.2 Integration Points	32
66.3 Integration Examples	33
67 SNMP Trap Integration	34
67.1 Introduction	34
68 TCP Wrappers Integration	35
68.1 Introduction	35
68.2 Defining A Service	35
68.3 Configuring TCP Wrappers	36
68.4 Writing The Script	36
68.5 Finishing Up	37

IX Nagios Addons **38**

69 Nagios Addons **39**

69.1 Introduction	39
69.2 NRPE	39
69.3 NSCA	40
69.4 NDOUtils	40

X Development **41**

70 Nagios Plugin API **42**

70.1 Other Resources	42
70.2 Plugin Overview	42
70.3 Return Code	42
70.4 Plugin Output Spec	43
70.5 Plugin Output Examples	43
70.6 Plugin Output Length Restrictions	44
70.7 Examples	44
70.8 Perl Plugins	44

71 Developing Plugins For Use With Embedded Perl **45**

71.1 Introduction	45
71.2 Target Audience	45
71.3 Things you should do when developing a Perl Plugin (ePN or not)	45
71.4 Things you must do to develop a Perl plugin for ePN	46

Part I

About

Chapter 1

About Nagios

1.1 What Is This?

Nagios is a system and network monitoring application. It watches hosts and services that you specify, alerting you when things go bad and when they get better.

Nagios was originally designed to run under **Linux**, although it should work under most other unices as well.

Some of the many features of Nagios include:

- Monitoring of network services (SMTP, POP3, HTTP, NTP, PING, etc.)
- Monitoring of host resources (processor load, disk usage, etc.)
- Simple plugin design that allows users to easily develop their own service checks
- Parallelized service checks
- Ability to define network host hierarchy using "parent" hosts, 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 method)
- Ability to define event handlers to be run during service or host events for proactive problem resolution
- Automatic log file rotation
- Support for implementing redundant monitoring hosts
- Optional web interface for viewing current network status, notification and problem history, log file, etc.

1.2 System Requirements

The only requirement of running Nagios is a machine running Linux (or UNIX variant) and a C compiler. You will probably also want to have TCP/IP configured, as most service checks will be performed over the network.

You are not required to use the CGIs included with Nagios. However, if you do decide to use them, you will need to have the following software installed...

1. A web server (preferably **Apache**)
 2. Thomas Boutell's **gd library** version 1.6.3 or higher (required by the **statusmap** and **trends** CGIs)
-

1.3 Licensing

Nagios is licensed under the terms of the [GNU General Public License](#) Version 2 as published by the [Free Software Foundation](#). This gives you legal permission to copy, distribute and/or modify Nagios under certain conditions. Read the 'LICENSE' file in the Nagios distribution or read the [online version of the license](#) for more details.

Nagios is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

1.4 Acknowledgements

Several people have contributed to Nagios by either reporting bugs, suggesting improvements, writing plugins, etc. A list of some of the many contributors to the development of Nagios can be found at <http://www.nagios.org/>.

1.5 Downloading The Latest Version

You can check for new versions of Nagios at <http://www.nagios.org/>.

1.6 Support

[Support options](#)

Chapter 2

What's New in Nagios 3



Important

Make sure you read through the documentation and the FAQs at nagios.org before sending a question to the mailing lists.

2.1 Change Log

The change log for Nagios can be found online at <http://www.nagios.org/development/changelog.php> or in the **Changelog** file in the root directory of the source code distribution.

2.2 Changes and New Features

2.2.1 Documentation

- **Doc updates** - I'm slowly making my way through rewriting most all portions of the documentation. This is going to take a while, as (1) there's a lot of documentation and (2) writing documentation is not my favorite thing in the world. Expect some portions of the docs to be different than others for a while. I hope the changes I'm making will make things clearer/easier for new and seasoned Nagios users alike.

2.2.2 Macros

- **New macros** - New macros have been added, including: `$TEMPPATH$`, `$LONGHOSTOUTPUT$`, `$LONGSERVICEOUTPUT$`, `$HOSTNOTIFICATIONID$`, `$SERVICENOTIFICATIONID$`, `$HOSTEVENTID$`, `$SERVICEEVENTID$`, `$SERVICEISVOLATILE$`, `$LASTHOSTEVENTID$`, `$LASTSERVICEEVENTID$`, `$HOSTDISPLAYNAME$`, `$SERVICEDISPLAYNAME$`, `$MAXHOSTATTEMPTS$`, `$MAXSERVICEATTEMPTS$`, `$TOTALHOSTSERVICES$`, `$TOTALHOSTSERVICESOK$`, `$TOTALHOSTSERVICESWARNING$`, `$TOTALHOSTSERVICESUNKNOWN$`, `$TOTALHOSTSERVICESCRITICAL$`, `$CONTACTGROUPNAME$`, `$CONTACTGROUPNAMES$`, `$CONTACTGROUPALIAS$`, `$CONTACTGROUPMEMBERS$`, `$NOTIFICATIONRECIPIENTS$`, `$NOTIFICATIONISESCALATED$`, `$NOTIFICATIONAUTHOR$`, `$NOTIFICATIONAUTHORNAME$`, `$NOTIFICATIONAUTHORALIAS$`, `$NOTIFICATIONCOMMENT$`, `$EVENTSTARTTIME$`, `$HOSTPROBLEMID$`, `$LASTHOSTPROBLEMID$`, `$SERVICEPROBLEMID$`, `$LASTSERVICEPROBLEMID$`, `$LASTHOSTSTATE$`, `$LASTHOSTSTATEID$`, `$LASTSERVICESTATE$`, `$LASTSERVICESTATEID$`. Two special on-demand time macros have also been added: `$ISVALIDTIME:$` and `$NEXTVALIDTIME:$`.
- **Removed macros** - The old `$NOTIFICATIONNUMBER$` macro has been deprecated in favor of new `$HOSTNOTIFICATIONNUMBER$` and `$SERVICENOTIFICATIONNUMBER$` macros.

- **Changes** - The `$HOSTNOTES$` and `$SERVICENOTES$` macros may now contain macros themselves, just like the `$HOSTNOTESURL$`, `$HOSTACTIONURL$`, `$SERVICENOTESURL$` and `$SERVICEACTIONURL$` macros.
- Macros are normally available as environment variables when check, event handler, notification, and other commands are run. This can be rather CPU intensive in large Nagios installations, so you can disable this behavior with the `enable_environment_macros` option.
- Macro information can be found [here](#).

2.2.3 Scheduled Downtime

- **Scheduled downtime** entries are no longer stored in their own file (previously specified with a `downtime_file` directive in the main configuration file). Current and retained scheduled downtime entries are now stored in the **status file** and **retention file**, respectively.

2.2.4 Comments

- Host and service comments are no longer stored in their own file (previously specified with a `comment_file` directive in the main configuration file). Current and retained comments are now stored in the **status file** and **retention file**, respectively.
- Acknowledgement comments that are marked as non-persistent are now only deleted when the acknowledgement is removed. They were previously automatically deleted when Nagios restarted, which was not ideal.

2.2.5 State Retention Data

- Status information for individual contacts is now retained across program restarts.
- Comment and downtime IDs are now retained across program restarts and should be unique unless the retention data is deleted or ignored.
- Added `retained_host_attribute_mask` and `retained_service_attribute_mask` variables to control what host/service attributes are retained globally across program restarts.
- Added `retained_process_host_attribute_mask` and `retained_process_service_attribute_mask` variables to control what process attributes are retained across program restarts.
- Added `retained_contact_host_attribute_mask` and `retained_contact_service_attribute_mask` variables to control what contact attributes are retained globally across program restarts.

2.2.6 Flap Detection

- Added `flap_detection_options` directive to host and service definitions to allow you to specify what host/service states should be used by the flap detection logic (by default all states are used).
 - Percent state change and state history are now retained and recorded even when flap detection is disabled.
 - Hosts and services are immediately checked for flapping when flap detection is enabled program-wide.
 - Hosts and services that are flapping when flap detection is disabled program-wide are now logged.
 - More information on flap detection can be found [here](#).
-

2.2.7 External Commands

- Added a new **PROCESS_FILE** external command to allow processing of external commands found in an external (regular) file. Useful for processing large amounts of passive checks with long output, or for scripting regular commands. More information can be found [here](#).
- Custom commands may now be submitted to Nagios. Custom command names are prefixed with an underscore and are not processed internally by the Nagios daemon. They may, however, be processed by a loaded NEB module.
- The **check_external_commands** option is now enabled by default, which means Nagios is configured to check for external commands "out of the box". All 2.x and earlier versions of Nagios had this option disabled by default.

2.2.8 Status Data

- Contact status information (last notification times, notifications enabled/disabled, etc.) is now saved in the **status** and **retention** files, although it is not processed by the CGIs.

2.2.9 Embedded Perl

- Added new **enable_embedded_perl** and **use_embedded_perl_implicitly** variables to control use of the embedded Perl interpreter.
- Perl scripts/plugins can now explicitly tell Nagios whether or not they should be run under the embedded Perl interpreter. This is useful if you have troublesome scripts that don't function well under the ePN.
- More information about these new options can be found [here](#).

2.2.10 Adaptive Monitoring

- The check timeperiod for hosts and services can now be modified on-the-fly with the appropriate external command (**CHANGE_HOST** or **CHANGE_SVC_CHECK_TIMEPERIOD**). Look [here](#) for available adaptive monitoring commands.

2.2.11 Notifications

- A **first_notification_delay** option has been added to host and service definitions to (what else) introduce a delay between when a host/service problem first occurs and when the first problem notification goes out. In previous versions you had to use some mighty config-fu with escalations to accomplish this. Now this feature is available to normal mortals.
- Notifications are now sent out for hosts/services that are flapping when flap detection is disabled on a host- or service-specific basis or on a program-wide basis. The **\$NOTIFICATIONTYPE\$** macro will be set to 'FLAPPINGDISABLED' in this situation.
- Notifications can now be sent out when scheduled downtime start, ends, and is cancelled for hosts and services. The **\$NOTIFICATIONTYPE\$** macro will be set to 'DOWNTIMESTART', 'DOWNTIMEEND', or 'DOWNTIMECANCELLED', respectively. In order to receive notifications on scheduled downtime events, specify 's' or 'downtime' in your contact, host, and/or service notification options.
- More information on notifications can be found [here](#).

2.2.12 Object Definitions

- Service dependencies can now be created to easily define "same host" dependencies for different services on one or more hosts. ([Read more](#))
-

- Extended host and service definitions (`hostextinfo` and `serviceextinfo`, respectively) have been deprecated. All values that from extended definitions have been merged with host or service definitions, as appropriate. Nagios 3 will continue to read and process older extended information definitions, but will log a warning. Future versions of Nagios (4.x and later) will not support separate extended info definitions.
- New `hostgroup_members`, `servicegroup_members`, and `contactgroup_members` directives have been added to `hostgroup`, `servicegroup`, and `contactgroups` definitions, respectively. This allows you to include hosts, services, or contacts from sub-groups in your group definitions.
- New `notes`, `notes_url`, and `action_url` have been added to `hostgroup` and `servicegroup` definition.
- Contact definitions have the new `host_notifications_enabled`, `service_notifications_enabled`, and `c-an_submit_commands` directives to better control notifications and determine whether or not they can submit commands through the web interface.
- Host and service dependencies now support an optional `dependency_period` directive. This allows you to limit the times during which dependencies are valid.
- The `parallelize` directive in service definitions is now deprecated and no longer used. All service checks are run in parallel in Nagios 3.
- There are no longer any inherent limitations on the length of host names or service descriptions.
- Extended regular expressions are now used if you enable the `use_regexp_matching` config option. Regular expression matching is only used in certain object definition directives that contain `*`, `?`, `+`, or `\.`
- A new `initial_state` directive has been added to host and service definitions, so you can tell Nagios that a host/service should default to a specific state when Nagios starts, rather than UP or OK (which is still the default).

2.2.13 Object Inheritance

- You can now inherit object variables/values from multiple templates by specifying more than one template name in the `use` directive of object definitions. This can allow for some very powerful (and complex) inheritance setups. ([Read more](#))
- Services now inherit contact groups, notification interval, and notification period from their associated host if not otherwise specified. ([Read more](#))
- Host and service escalations now inherit contact groups, notification interval, and escalation timeperiod from their associated host or service if not otherwise specified. ([Read more](#))
- String variables in host, service, and contact definitions can now be prevented from being inherited by specifying a value of 'null' (without quotes) for the value of the variable. ([Read more](#))
- Most string variables in local object definitions can now be appended to the string values that are inherited. This is quite handy in large configurations. ([Read more](#))

2.2.14 Performance Improvements

- Add ability to precache object config files and exclude circular path detection checks from verification process. This can speed up Nagios start time immensely in large environments! Read more [here](#).
 - A new `use_large_installation_tweaks` option has been added that should improve performance in large Nagios installations. Read more about this [here](#).
 - A number of internal improvements have been made with regards to how Nagios deals with internal data structures and object (e.g. host and service) relationships. These improvements should result in a speedup for larger installations.
 - New `external_command_buffer_slots` option has been added to allow you to more easily scale Nagios in large environments. For best results you should consider using [MRTG to graph](#) Nagios' usage of buffer slots over time.
-

2.2.15 Plugin Output

- Multiline plugin output is now supported for host and service checks. Hooray! The plugin API has been updated to support multiple lines of output in a manner that retains backward compatability with older plugins. Additional lines of output (aside from the first line) are now stored in new `$LONGHOSTOUTPUT$` and `$LONGSERVICEOUTPUT$` macros.
- The maximum length of plugin output has been increased to 4K (from around 350 bytes in previous versions). This 4K limit has been arbitrarily chosen to protect again runaway plugins that dump back too much data to Nagios.
- More information on the plugins, multiline output, and max plugin output length can be found [here](#).

2.2.16 Service Checks

- Nagios now checks for orphaned service checks by default.
- Added a new `enable_predictive_service_dependency_checks` option to control whether or not Nagios will initiate predictive check of service that are being depended upon (in dependency definitions). Predictive checks help ensure that the dependency logic is as accurate as possible. ([Read more](#))
- A new cached service check feature has been implemented that can significantly improve performance for many people Instead of executing a plugin to check the status of a service, Nagios can often use a cached service check result instead. More information on this can be found [here](#).

2.2.17 Host Checks

- Host checks are now run in parallel! Host checks used to be run in a serial fashion, which meant they were a major holdup in terms of performance. No longer! ([Read more](#))
- Host check retries are now performed like service check retries. That is to say, host definitions now have a new `retry_interval` that specifies how much time to wait before trying the host check again. :-)
- Regularly scheduled host checks now longer hinder performance. In fact, they can help to increase performance with the new cached check logic (see below).
- Added a new `check_for_orphaned_hosts` option to enable checks of orphaned host checks. This is need now that host checks are run in parallel.
- Added a new `enable_predictive_host_dependency_checks` option to control whether or not Nagios will initiate predictive check of hosts that are being depended upon (in dependency definitions). Predictive checks help ensure that the dependency logic is as accurate as possible. ([Read more](#))
- A new cached host check feature has been implemented that can significantly improve performance for many people Instead of executing a plugin to check the status of a host, Nagios can often use a cached host check result instead. More information on this can be found [here](#).
- Passive host checks that have a DOWN or UNREACHABLE result can now be automatically translated to their proper state from the point of view of the Nagios instance that receives them. This is very useful in failover and distributed monitoring setups. More information on passive host check state translation can be found [here](#).
- Passive host checks normally put a host into a HARD state. This can now be changed by enabling the `passive_host_checks_are_soft` option.

2.2.18 Freshness checks

- A new `additional_freshness_latency` option has been added to allow to you specify the number of seconds that should be added to any host or service freshness threshold that is automatically calculated by Nagios.
-

2.2.19 IPC

- The IPC mechanism that is used to transfer host/service check results back to the Nagios daemon from (grand)child processes has changed! This should help to reduce load/latency issues related to processing large numbers of passive checks in distributed monitoring environments.
- Check results are now transferred by writing check results to files in directory specified by the `check_result_path` option. Files that are older than the `max_check_result_file_age` option will be mercilessly deleted without further processing.

2.2.20 Timeperiods

- Timeperiods were overdue for a major overhaul and have finally been extended to allow for date exceptions, skip dates (every 3 days), etc! This should help you out when defining notification timeperiods for pager rotations.
- More information on the new timeperiod directives can be found [here](#) and [here](#).

2.2.21 Event Broker

- Updated NEB API version
- Modified callback for adaptive program status data
- Added callback for adaptive contact status data
- Added precheck callbacks for hosts and services to allow modules to cancel/override internal host/service checks.

2.2.22 Web Interface

- Hostgroup and servicegroup summaries now show important/unimportant problem breakdowns like the TAC CGI.
- Minor layout changes to host and service detail views in extinfo CGI.
- New check statistics and have been added to the 'Performance Info' screen.
- Added **Splunk** integration options to various CGIs. Integration is controlled by the `enable_splunk_integration` and `splunk_url` options in the CGI config file.
- Added new `notes_url_target` and `action_url_target` options to control what frame notes and action URLs are opened in.
- Added new `lock_author_names` option to prevent alteration of author names when users submit comments, acknowledgements, and scheduled downtime.

2.2.23 Debugging Info

- The `DEBUGx` compile options available in the configure script have been removed.
 - Debugging information can now be written to a separate debug file, which is automatically rotated when it reaches a user-defined size. This should make debugging problems much easier, as you don't need to recompile Nagios. Full support for writing debugging information to file is being added during the alpha development phase, so it may not be complete when you try it.
 - Variables that affect the debug log in `debug_file`, `debug_level`, `debug_verbosity`, and `max_debug_file_size`.
-

2.2.24 Misc

- **Temp path variable** - A new `temp_path` variable has been added to specify a scratch directory that Nagios can use for temporary scratch space.
- **Unique notification and event ID numbers** - A unique ID number is now assigned to each host and service notification. Another unique ID is now assigned to all host and service state changes as well. The unique IDs can be accessed using the following respective macros: `$HOSTNOTIFICATIONID$`, `$SERVICENOTIFICATIONID$`, `$HOSTEVENTID$`, `$SERVICEEVENTID$`, `$LASTHOSTEVENTID$`, `$LASTSERVICEEVENTID$`.
- **New macros** - A few new macros (other than those already mentioned elsewhere above) have been added. They include `$HOSTGROUPNAMES$`, `$SERVICEGROUPNAMES$`, `$HOSTACKAUTHORNAME$`, `$HOSTACKAUTHORALIAS$`, `$SERVICEACKAUTHORNAME$`, and `$SERVICEACKAUTHORALIAS$`.
- **Reaper frequency** - The old `service_reaper_frequency` variable has been renamed to `check_result_reaper_frequency`, as it is now also used to process host check results.
- **Max reaper time** - A new `max_check_result_reaper_time` variable has been added to limit the amount of time a single reaper event is allowed to run.
- **Fractional intervals** - Fractional notification and check intervals (e.g. '3.5' minutes) are now supported in host, service, host escalation, and service escalation definitions.
- **Escaped command arguments** - You can now pass bang (!) characters in your command arguments by escaping them with a backslash (\). If you need to include backslashes in your command arguments, they should also be escaped with a backslash.
- **Multiline system command output** - Nagios will now read multiple lines out output from system commands it runs (notification scripts, etc.), up to 4K. This matches the limits on plugin output mentioned earlier. Output from system commands is not directly processed by Nagios, but support for it is there nonetheless.
- **Better scheduling information** - More detailed information is given when Nagios is executed with the `-s` command line option. This information can be used to help **reduce** the time it takes to start/restart Nagios.
- **Aggregated status file updates** - The old `aggregate_status_updates` option has been removed. All status file updates are now aggregated at a minimum interval of 1 second.
- **New performance data file mode** - A new 'p' option has been added to the `host_perfdata_file_mode` and `service_perfdata_file_mode` options. This new mode will open the file in non-blocking read/write mode, which is useful for pipes.
- **Timezone offset** - A new `use_timezone` option has been added to allow you to run different instances of Nagios in timezones different from the local zone.

Part II

Getting Started

Chapter 3

Advice for Beginners



Congratulations on choosing Nagios! Nagios is quite powerful and flexible, but it can take a lot of work to get it configured just the way you'd like. Once you become familiar with how it works and what it can do for you, you'll never want to be without it :-). Here are some important things to keep in mind for first-time Nagios users:

1. **Relax - it's going to take some time.** Don't expect to be able to get things working exactly the way you want them right off the bat. It's not that easy. Setting up Nagios can involve a bit of work - partly because of the options that Nagios offers, partly because you need to know what to monitor on your network (and how best to do it).
2. **Use the quickstart instructions.** The [Quickstart installation guide](#) is designed to get most new users up and running with a basic Nagios setup fairly quickly. Within 20 minutes you can have Nagios installed and monitoring your local system. Once that's complete, you can move on to learning how to configure Nagios to do more.
3. **Read the documentation.** Nagios can be tricky to configure when you've got a good grasp of what's going on, and nearly impossible if you don't. Make sure you read the documentation (particularly the sections on 'Configuring Nagios' and 'The Basics'). Save the advanced topics for when you've got a good understanding of the basics.
4. **Seek the help of others.** If you've read the documentation, reviewed the sample config files, and are still having problems, send an email message describing your problems to the [nagios-users](#) mailing list. Due to the amount of work that I have to do for this project, I am unable to answer most of the questions that get sent directly to me, so your best source of help is going to be the mailing list. If you've done some background reading and you provide a good problem description, odds are that someone will give you some pointers on getting things working properly. More information on subscribing to the mailing lists or searching the list archives can be found at <http://www.nagios.org/support/>.

Chapter 4

Quickstart Installation Guides



Abstract

These quickstart guides are intended to provide you with simple instructions on how to install Nagios from source (code) and have it monitoring your local machine inside of 20 minutes. No advanced installation options are discussed here - just the basics that will work for 95% of users who want to get started.

4.1 Guides

Quickstart installation guides are currently available for the following Linux distributions:

- [Fedora Quickstart](#)
- [openSUSE Quickstart](#)
- [Ubuntu Quickstart](#)

You can also find additional quickstart guides on the [NagiosCommunity.org wiki](#). Can't find a quickstart for your particular OS ? Write one and post it to the wiki for others!

If you are installing Nagios on an operating system or Linux distribution that isn't listed above, read the [Fedora Quickstart](#) for an overview of what you'll need to do. Command names, paths, etc. vary widely across different OSes/distributions, so you'll likely need to tweak the installation docs a bit to work for your particular case.

4.2 Post-Installation Modifications

Once you get Nagios installed and running properly, you'll no doubt want to start monitoring more than just your local machine. Check out the following docs for how to go about monitoring other things...

- [Monitoring Windows machines](#)
 - [Monitoring Linux/Unix machines](#)
 - [Monitoring Netware servers](#)
 - [Monitoring routers/switches](#)
 - [Monitoring network printers](#)
 - [Monitoring publicly available services \(HTTP, FTP, SSH, etc.\)](#)
-

Chapter 5

Fedora Quickstart

Abstract

This guide is intended to provide you with simple instructions on how to install Nagios from source (code) on Fedora and have it monitoring your local machine inside of 20 minutes. No advanced installation options are discussed here - just the basics that will work for 95% of users who want to get started.

These instructions were written based on a standard Fedora Core 6 Linux distribution.

5.1 What You'll End Up With

If you follow these instructions, here's what you'll end up with:

- Nagios and the plugins will be installed underneath `/usr/local/nagios`
- Nagios will be configured to monitor a few aspects of your local system (CPU load, disk usage, etc.)
- The Nagios web interface will be accessible at `http://localhost/nagios/`

5.2 Prerequisites

During portions of the installation you'll need to have root access to your machine.

Make sure you've installed the following packages on your Fedora installation before continuing.

- Apache
- GCC compiler
- **GD** development libraries

You can use **yum** to install these packages by running the following commands (as root):

```
linux:~ # yum install httpd
linux:~ # yum install gcc
linux:~ # yum install glibc glibc-common
linux:~ # yum install gd gd-devel
```

5.3 Create Account Information

Become the root user.

```
linux:~ $ su -l
```

Create a new nagios user account and give it a password.

```
linux:~ # /usr/sbin/useradd -m nagios
linux:~ # passwd nagios
```

Create a new nagcmd group for allowing external commands to be submitted through the web interface. Add both the nagios user and the apache user to the group.

```
linux:~ # /usr/sbin/groupadd nagcmd
linux:~ # /usr/sbin/usermod -G nagcmd nagios
linux:~ # /usr/sbin/usermod -G nagcmd apache
```

5.4 Download Nagios and the Plugins

Create a directory for storing the downloads.

```
linux:~ # mkdir ~/downloads
linux:~ # cd ~/downloads
```

Download the source code tarballs of both Nagios and the Nagios plugins (visit <http://www.nagios.org/download/> for links to the latest versions). At the time of writing, the latest versions of Nagios and the Nagios plugins were 3.0.3 and 1.4.11, respectively.

```
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0.2.tar.gz
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11. ↵
tar.gz
```

5.5 Compile and Install Nagios

Extract the Nagios source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-3.0.2.tar.gz
linux:~ # cd nagios-3.0.2
```

Run the Nagios configure script, passing the name of the group you created earlier like so:

```
linux:~ # ./configure --with-command-group=nagcmd
```

Compile the Nagios source code.

```
linux:~ # make all
```

Install binaries, init script, sample config files and set permissions on the external command directory.

```
linux:~ # make install
linux:~ # make install-init
linux:~ # make install-config
linux:~ # make install-commandmode
```

Don't start Nagios yet - there's still more that needs to be done...

5.6 Customize Configuration

Sample **configuration files** have now been installed in the `/usr/local/nagios/etc` directory. These sample files should work fine for getting started with Nagios. You'll need to make just one change before you proceed...

Edit the `/usr/local/nagios/etc/objects/contacts.cfg` config file with your favorite editor and change the email address associated with the nagiosadmin contact definition to the address you'd like to use for receiving alerts.

```
linux:~ # vi /usr/local/nagios/etc/objects/contacts.cfg
```

5.7 Configure the Web Interface

Install the Nagios web config file in the Apache `conf.d` directory.

```
linux:~ # make install-webconf
```

Create a `nagiosadmin` account for logging into the Nagios web interface. Remember the password you assign to this account - you'll need it later.

```
linux:~ # htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Restart Apache to make the new settings take effect.

```
linux:~ # service httpd restart
```

5.8 Compile and Install the Nagios Plugins

Extract the Nagios plugins source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-plugins-1.4.11.tar.gz
linux:~ # cd nagios-plugins-1.4.11
```

Compile and install the plugins.

```
linux:~ # ./configure --with-nagios-user=nagios --with-nagios-group=nagios
linux:~ # make
linux:~ # make install
```

5.9 Start Nagios

Add Nagios to the list of system services and have it automatically start when the system boots.

```
linux:~ # chkconfig --add nagios
linux:~ # chkconfig nagios on
```

Verify the sample Nagios configuration files.

```
linux:~ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

If there are no errors, start Nagios.

```
linux:~ # service nagios start
```

5.10 Modify SELinux Settings

Fedora ships with SELinux (Security Enhanced Linux) installed and in Enforcing mode by default. This can result in Internal Server Error messages when you attempt to access the Nagios CGIs.

See if SELinux is in Enforcing mode.

```
linux:~ # getenforce
```

Put SELinux into Permissive mode.

```
linux:~ # setenforce 0
```

To make this change permanent, you'll have to modify the settings in `/etc/selinux/config` and reboot.

Instead of disabling SELinux or setting it to permissive mode, you can use the following command to run the CGIs under SELinux enforcing/targeted mode:

```
linux:~ # chcon -R -t httpd_sys_content_t /usr/local/nagios/sbin/  
linux:~ # chcon -R -t httpd_sys_content_t /usr/local/nagios/share/
```

For information on running the Nagios CGIs under Enforcing mode with a targeted policy, visit the NagiosCommunity.org wiki at <http://www.nagioscommunity.org/wiki>.

5.11 Login to the Web Interface

You should now be able to access the Nagios web interface at the URL below. You'll be prompted for the username (nagiosadmin) and password you specified earlier.

<http://localhost/nagios/>

Click on the Service Detail navbar link to see details of what's being monitored on your local machine. It will take a few minutes for Nagios to check all the services associated with your machine, as the checks are spread out over time.

5.12 Other Modifications

Make sure your machine's firewall rules are configured to allow access to the web server if you want to access the Nagios interface remotely.

Configuring email notifications is out of the scope of this documentation. While Nagios is currently configured to send you email notifications, your system may not yet have a mail program properly installed or configured. Refer to your system documentation, search the web, or look to the [NagiosCommunity.org wiki](http://www.nagioscommunity.org/wiki) for specific instructions on configuring your system to send email messages to external addresses. More information on notifications can be found [here](#).

5.13 You're Done

Congratulations! You successfully installed Nagios. Your journey into monitoring is just beginning. You'll no doubt want to monitor more than just your local machine, so check out the following docs...

- [Monitoring Windows machines](#)
- [Monitoring Linux/Unix machines](#)
- [Monitoring Network servers](#)
- [Monitoring routers/switches](#)
- [Monitoring publicly available services \(HTTP, FTP, SSH, etc.\)](#)

Chapter 6

openSUSE Quickstart

Abstract

This guide is intended to provide you with simple instructions on how to install Nagios from source (code) on openSUSE and have it monitoring your local machine inside of 20 minutes. No advanced installation options are discussed here - just the basics that will work for 95% of users who want to get started.

These instructions were written based on an openSUSE 10.2 installation.

6.1 Required Packages

Make sure you've installed the following packages on your openSUSE installation before continuing. You can use **yast** to install packages under openSUSE.

1. apache2
2. C/C++ development libraries

6.2 Create Account Information

Become the root user.

```
linux:~ $ su -l
```

Create a new nagios user account and give it a password.

```
linux:~ # /usr/sbin/useradd -m nagios
linux:~ # passwd nagios
```

Create a new nagios group. Add the nagios user to the group.

```
linux:~ # /usr/sbin/groupadd nagios
linux:~ # /usr/sbin/usermod -G nagios nagios
```

Create a new nagcmd group for allowing external commands to be submitted through the web interface. Add both the nagios user and the apache user to the group.

```
linux:~ # /usr/sbin/groupadd nagcmd
linux:~ # /usr/sbin/usermod -G nagcmd nagios
linux:~ # /usr/sbin/usermod -G nagcmd wwwrun
```

6.3 Download Nagios and the Plugins

Create a directory for storing the downloads.

```
linux:~ # mkdir ~/downloads
linux:~ # cd ~/downloads
```

Download the source code tarballs of both Nagios and the Nagios plugins (visit <http://www.nagios.org/download/> for links to the latest versions). At the time of writing, the latest versions of Nagios and the Nagios plugins were 3.0.3 and 1.4.11, respectively.

```
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0.2.tar.gz
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11. ←
tar.gz
```

6.4 Compile and Install Nagios

Extract the Nagios source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-3.0.2.tar.gz
linux:~ # cd nagios-3.0.2
```

Run the Nagios configure script, passing the name of the group you created earlier like so:

```
linux:~ # ./configure --with-command-group=nagcmd
```

Compile the Nagios source code.

```
linux:~ # make all
```

Install binaries, init script, sample config files and set permissions on the external command directory.

```
linux:~ # make install
linux:~ # make install-init
linux:~ # make install-config
linux:~ # make install-commandmode
```

Don't start Nagios yet - there's still more that needs to be done...

6.5 Customize Configuration

Sample **configuration files** have now been installed in the `/usr/local/nagios/etc` directory. These sample files should work fine for getting started with Nagios. You'll need to make just one change before you proceed...

Edit the `/usr/local/nagios/etc/objects/contacts.cfg` config file with your favorite editor and change the email address associated with the nagiosadmin contact definition to the address you'd like to use for receiving alerts.

```
linux:~ # vi /usr/local/nagios/etc/objects/contacts.cfg
```

6.6 Configure the Web Interface

Install the Nagios web config file in the Apache conf.d directory.

```
linux:~ # make install-webconf
```

Create a nagiosadmin account for logging into the Nagios web interface. Remember the password you assign to this account - you'll need it later.

```
linux:~ # htpasswd2 -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Restart Apache to make the new settings take effect.

```
linux:~ # service apache2 restart
```

6.7 Compile and Install the Nagios Plugins

Extract the Nagios plugins source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-plugins-1.4.11.tar.gz
linux:~ # cd nagios-plugins-1.4.11
```

Compile and install the plugins.

```
linux:~ # ./configure --with-nagios-user=nagios --with-nagios-group=nagios
linux:~ # make
linux:~ # make install
```

6.8 Start Nagios

Add Nagios to the list of system services and have it automatically start when the system boots.

```
linux:~ # chkconfig --add nagios  
linux:~ # chkconfig nagios on
```

Verify the sample Nagios configuration files.

```
linux:~ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

If there are no errors, start Nagios.

```
linux:~ # service nagios start
```

6.9 Login to the Web Interface

You should now be able to access the Nagios web interface at the URL below. You'll be prompted for the username (nagiosadmin) and password you specified earlier.

<http://localhost/nagios/>

Click on the Service Detail navbar link to see details of what's being monitored on your local machine. It will take a few minutes for Nagios to check all the services associated with your machine, as the checks are spread out over time.

6.10 Other Modifications

Make sure your machine's firewall rules are configured to allow access to the web server if you want to access the Nagios interface remotely.

You can do this by:

1. Opening the control center
2. Select Open Administrator Settings to open the YaST administrator control center
3. Select Firewall from the Security and Users category
4. Click the Allowed Services option in the Firewall Configuration window
5. Add HTTP Server to the allowed services list for the External Zone
6. Click Next and Accept to activate the new firewall settings

Configuring email notifications is outside the scope of this documentation. Refer to your system documentation, search the web, or look to the [NagiosCommunity.org wiki](http://NagiosCommunity.org/wiki) for specific instructions on configuring your openSUSE system to send email messages to external addresses.

Chapter 7

Ubuntu Quickstart

Abstract

This guide is intended to provide you with simple instructions on how to install Nagios from source (code) on Ubuntu and have it monitoring your local machine inside of 20 minutes. No advanced installation options are discussed here - just the basics that will work for 95% of users who want to get started.

These instructions were written based on an Ubuntu 6.10 (desktop) installation. They should work for an Ubuntu 7.10 install as well.

7.1 What You'll End Up With

If you follow these instructions, here's what you'll end up with:

1. Nagios and the plugins will be installed underneath `/usr/local/nagios`
2. Nagios will be configured to monitor a few aspects of your local system (CPU load, disk usage, etc.)
3. The Nagios web interface will be accessible at `http://localhost/nagios/`

7.2 Required Packages

Make sure you've installed the following packages on your Ubuntu installation before continuing.

1. Apache 2
2. GCC compiler and development libraries
3. GD development libraries

You can use **apt-get** to install these packages by running the following commands:

```
linux:~ $ sudo apt-get install apache2
linux:~ $ sudo apt-get install build-essential
```

With Ubuntu 6.10, install the gd2 library with this command:

```
linux:~ $ sudo apt-get install libgd2-dev
```

With Ubuntu 7.10, the gd2 library name has changed, so you'll need to use the following:

```
linux:~ $ sudo apt-get install libgd2-xpm-dev
```

7.3 Create Account Information

Become the root user.

```
linux:~ $ sudo -s
```

Create a new nagios user account and give it a password.

```
linux:~ # /usr/sbin/useradd -m nagios
linux:~ # passwd nagios
```

On Ubuntu server edition (6.01 and possible newer versions), you will need to also add a nagios group (it's not created by default). You should be able to skip this step on desktop editions of Ubuntu.

```
linux:~ # /usr/sbin/groupadd nagios
linux:~ # /usr/sbin/usermod -G nagios nagios
```

Create a new nagcmd group for allowing external commands to be submitted through the web interface. Add both the nagios user and the apache user to the group.

```
linux:~ # /usr/sbin/groupadd nagcmd
linux:~ # /usr/sbin/usermod -G nagcmd nagios
linux:~ # /usr/sbin/usermod -G nagcmd www-data
```

7.4 Download Nagios and the Plugins

Create a directory for storing the downloads.

```
linux:~ # mkdir ~/downloads
linux:~ # cd ~/downloads
```

Download the source code tarballs of both Nagios and the Nagios plugins (visit <http://www.nagios.org/download/> for links to the latest versions). At the time of writing, the latest versions of Nagios and the Nagios plugins were 3.0.3 and 1.4.11, respectively.

```
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0.2.tar.gz
linux:~ # wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.11. ↵
tar.gz
```

7.5 Compile and Install Nagios

Extract the Nagios source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-3.0.2.tar.gz
linux:~ # cd nagios-3.0.2
```

Run the Nagios configure script, passing the name of the group you created earlier like so:

```
linux:~ # ./configure --with-command-group=nagcmd
```

Compile the Nagios source code.

```
linux:~ # make all
```

Install binaries, init script, sample config files and set permissions on the external command directory.

```
linux:~ # make install
linux:~ # make install-init
linux:~ # make install-config
linux:~ # make install-commandmode
```

Don't start Nagios yet - there's still more that needs to be done...

7.6 Customize Configuration

Sample **configuration files** have now been installed in the `/usr/local/nagios/etc` directory. These sample files should work fine for getting started with Nagios. You'll need to make just one change before you proceed...

Edit the `/usr/local/nagios/etc/objects/contacts.cfg` config file with your favorite editor and change the email address associated with the nagiosadmin contact definition to the address you'd like to use for receiving alerts.

```
linux:~ # vi /usr/local/nagios/etc/objects/contacts.cfg
```

7.7 Configure the Web Interface

Install the Nagios web config file in the Apache `conf.d` directory.

```
linux:~ # make install-webconf
```

Create a nagiosadmin account for logging into the Nagios web interface. Remember the password you assign to this account - you'll need it later.

```
linux:~ # htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Restart Apache to make the new settings take effect.

```
linux:~ # /etc/init.d/apache2 reload
```

7.8 Compile and Install the Nagios Plugins

Extract the Nagios plugins source code tarball.

```
linux:~ # cd ~/downloads
linux:~ # tar xzf nagios-plugins-1.4.11.tar.gz
linux:~ # cd nagios-plugins-1.4.11
```

Compile and install the plugins.

```
linux:~ # ./configure --with-nagios-user=nagios --with-nagios-group=nagios
linux:~ # make
linux:~ # make install
```

7.9 Start Nagios

Configure Nagios to automatically start when the system boots.

```
linux:~ # ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Verify the sample Nagios configuration files.

```
linux:~ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

If there are no errors, start Nagios.

```
linux:~ # /etc/init.d/nagios start
```

7.10 Login to the Web Interface

You should now be able to access the Nagios web interface at the URL below. You'll be prompted for the username (nagiosadmin) and password you specified earlier.

<http://localhost/nagios/>

Click on the Service Detail navbar link to see details of what's being monitored on your local machine. It will take a few minutes for Nagios to check all the services associated with your machine, as the checks are spread out over time.

7.11 Other Modifications

If you want to receive email notifications for Nagios alerts, you need to install the mailx (Postfix) package.

```
linux:~ $ sudo apt-get install mailx
```

You'll have to edit the Nagios email notification commands found in `/usr/local/nagios/etc/objects/commands.cfg` and change any `/bin/mail` references to `/usr/bin/mail`. Once you do that you'll need to restart Nagios to make the configuration changes live.

```
linux:~ $ sudo /etc/init.d/nagios restart
```

Configuring email notifications is outside the scope of this documentation. Refer to your system documentation, search the web, or look to the NagiosCommunity.org wiki for specific instructions on configuring your Ubuntu system to send email messages to external addresses.

Chapter 8

Upgrading Nagios

8.1 Upgrading From Previous Nagios 3.x Releases

As newer alpha, beta, and stable releases of Nagios 3.x are released, you should strongly consider upgrading as soon as possible. Newer releases usually contain critical bug fixes, so its important to stay up to date. Assuming you've already installed Nagios from source code as described in the [quickstart guide](#), you can install newer versions of Nagios 3.x easily. You don't even need root access to do it, as everything that needed to be done as root was done during the initial install. Here's the upgrade process...

Make sure you have a good backup of your existing Nagios installation and configuration files. If anything goes wrong or doesn't work, this will allow you to rollback to your old version.

Become the nagios user. Debian/Ubuntu users should use **sudo -s nagios**.

```
linux:~ $ su -l nagios
```

Download the source code tarball of the latest version of Nagios (visit <http://www.nagios.org/download/> for the link to the latest version).

```
linux:~ $ wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.x.tar.gz
```

Extract the Nagios source code tarball.

```
linux:~ $ tar xzf nagios-3.x.tar.gz
linux:~ $ cd nagios-3.x
```

Run the Nagios configure script, passing the name of the group used to control external command file permissions like so:

```
linux:~ $ ./configure --with-command-group=nagcmd
```

Compile the Nagios source code.

```
linux:~ $ make all
```

Install updated binaries, documentation, and web web interface. Your existing configuration files will not be overwritten by this step.

```
linux:~ $ make install
```

Verify your configuration files and restart Nagios.

```
linux:~ $ /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
linux:~ $ /sbin/service nagios restart
```

That's it - you're done!

8.2 Upgrading From Nagios 2.x

It shouldn't be too difficult to upgrade from Nagios 2.x to Nagios 3. The upgrade is essentially the same as what is described above for upgrading to newer 3.x releases. You will, however, have to change your configuration files a bit so they work with Nagios 3:

- The old `service_reaper_frequency` variable in the main config file has been renamed to `check_result_reaper_frequency`.
- The old `$NOTIFICATIONNUMBER$` macro has been deprecated in favor of new `$HOSTNOTIFICATIONNUMBER$` and `$SERVICENOTIFICATIONNUMBER$` macros.
- The old `parallelize` directive in service definitions is now deprecated and no longer used, as all service checks are run in parallel.
- The old `aggregate_status_updates` option has been removed. All status file updates are now aggregated at a minimum interval of 1 second.
- Extended host and extended service definitions have been deprecated. They are still read and processed by Nagios, but it is recommended that you move the directives found in these definitions to your host and service definitions, respectively.
- The old `downtime_file` file variable in the main config file is no longer supported, as scheduled downtime entries are now saved in the **retention file**. To preserve existing downtime entries, stop Nagios 2.x and append the contents of your old downtime file to the retention file.
- The old `comment_file` file variable in the main config file is no longer supported, as comments are now saved in the **retention file**. To preserve existing comments, stop Nagios 2.x and append the contents of your old comment file to the retention file.

Also make sure to read the 'What's New' section of the documentation. It describes all the changes that were made to the Nagios 3 code since the latest stable release of Nagios 2.x. Quite a bit has changed, so make sure you read it over.

8.3 Upgrading From an RPM Installation

If you currently have an RPM- or Debian/Ubuntu APT package-based installation of Nagios and you would like to transition to installing Nagios from the official source code distribution, here's the basic process you should follow:

1. Backup your existing Nagios installation
 - Configuration files
 - Main config file (usually `nagios.cfg`)
 - Resource config file (usually `resource.cfg`)
 - CGI config file (usually `cgi.cfg`)
 - All your object definition files
 - Retention file (usually `retention.dat`)
 - Current Nagios log file (usually `nagios.log`)
 - Archived Nagios log files
2. Uninstall the original RPM or APT package
3. Install Nagios from source by following the **quickstart guide**
4. Restore your original Nagios configuration files, retention file, and log files
5. **Verify** your configuration and **start** Nagios

Note

Different RPMs or APT packages may install Nagios in different ways and in different locations. Make sure you've backed up all your critical Nagios files before removing the original RPM or APT package, so you can revert back if you encounter problems.

Chapter 9

Monitoring Windows Machines

Abstract

This document describes how you can monitor "private" services and attributes of Windows machines, such as:

- Memory usage
- CPU load
- Disk usage
- Service states
- Running processes
- etc.

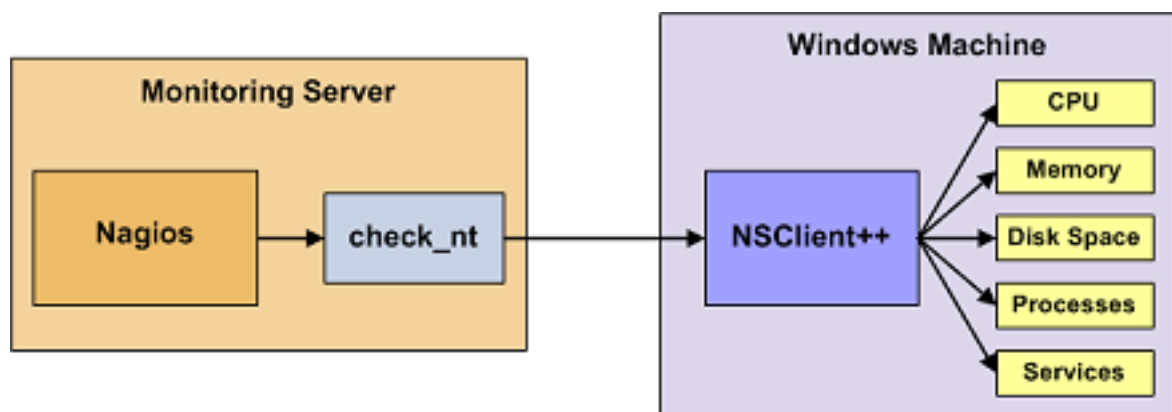
9.1 Introduction

Publicly available services that are provided by Windows machines (HTTP, FTP, POP3, etc.) can be monitored easily by following the documentation on [Monitoring publicly available services \(HTTP, FTP, SSH, etc.\)](#).

Note

These instructions assume that you've installed Nagios according to the [quickstart guide](#). The sample configuration entries below reference objects that are defined in the sample config files (`commands.cfg`, `templates.cfg`, etc.) that are installed if you follow the quickstart.

9.2 Overview



Monitoring private services or attributes of a Windows machine requires that you install an agent on it. This agent acts as a proxy between the Nagios plugin that does the monitoring and the actual service or attribute of the Windows machine. Without installing an agent on the Windows box, Nagios would be unable to monitor private services or attributes of the Windows box.

For this example, we will be installing the **NSClient++** addon on the Windows machine and using the **check_nt** plugin to communicate with the NSClient++ addon. The **check_nt** plugin should already be installed on the Nagios server if you followed the quickstart guide.

Other Windows agents (like **NC_Net**) could be used instead of NSClient++ if you wish - provided you change command and service definitions, etc. a bit. For the sake of simplicity I will only cover using the NSClient++ addon in these instructions.

9.3 Steps

There are several steps you'll need to follow in order to monitor a new Windows machine. They are:

1. Perform first-time prerequisites
2. Install a monitoring agent on the Windows machine
3. Create new host and service definitions for monitoring the Windows machine
4. Restart the Nagios daemon

9.4 What's Already Done For You

To make your life a bit easier, a few configuration tasks have already been done for you:

- A **check_nt** command definition has been added to the `commands.cfg` file. This allows you to use the **check_nt** plugin to monitor Windows services.
- A Windows server host template (called `windows-server`) has already been created in the `templates.cfg` file. This allows you to add new Windows host definitions in a simple manner.

The above-mentioned config files can be found in the `/usr/local/nagios/etc/objects/` directory. You can modify the definitions in these and other definitions to suit your needs better if you'd like. However, I'd recommend waiting until you're more familiar with configuring Nagios before doing so. For the time being, just follow the directions outlined below and you'll be monitoring your Windows boxes in no time.

9.5 Prerequisites

The first time you configure Nagios to monitor a Windows machine, you'll need to do a bit of extra work. Remember, you only need to do this for the **first** Windows machine you monitor.

Edit the main Nagios config file.

```
linux:~ # vi /usr/local/nagios/etc/nagios.cfg
```

Remove the leading pound (#) sign from the following line in the main configuration file:

```
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Save the file and exit.

What did you just do? You told Nagios to look to the `/usr/local/nagios/etc/objects/windows.cfg` to find additional object definitions. That's where you'll be adding Windows host and service definitions. That configuration file already contains some sample host, hostgroup, and service definitions. For the **first** Windows machine you monitor, you can simply modify the sample host and service definitions in that file, rather than creating new ones.

9.6 Installing the Windows Agent

Before you can begin monitoring private services and attributes of Windows machines, you'll need to install an agent on those machines. I recommend using the NSClient++ addon, which can be found at <http://sourceforge.net/projects/nsclient>. These instructions will take you through a basic installation of the NSClient++ addon, as well as the configuration of Nagios for monitoring the Windows machine.

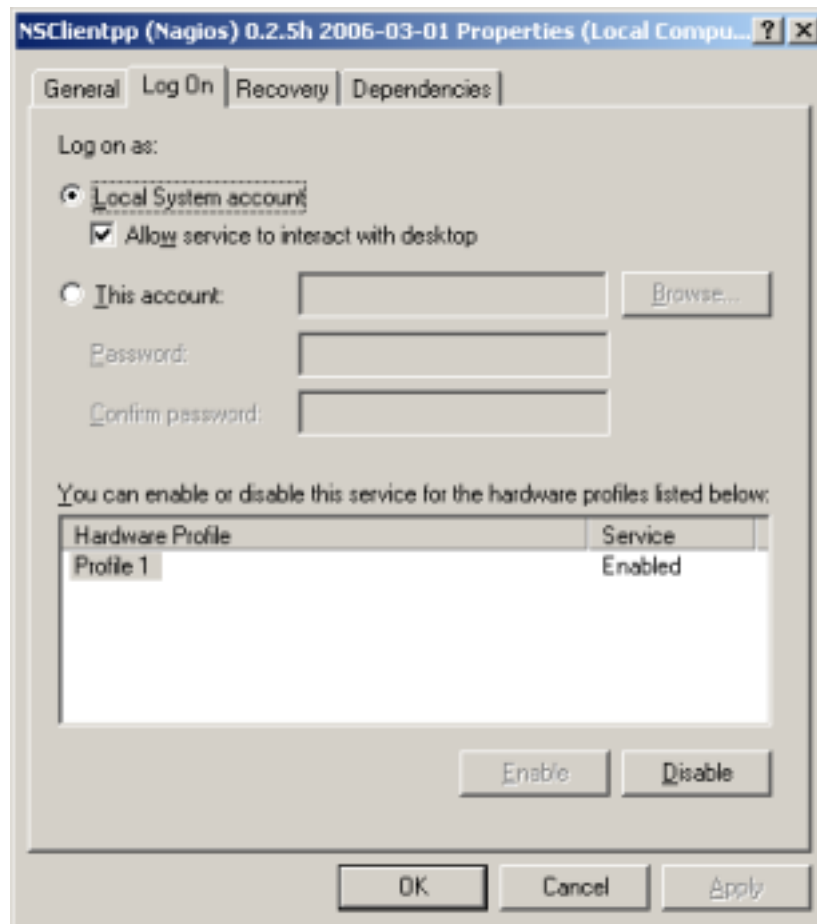
1. Download the latest stable version of the NSClient++ addon from <http://sourceforge.net/projects/nsclient>
2. Unzip the NSClient++ files into a new `C:\NSClient++` directory
3. Open a command prompt and change to the `C:\NSClient++` directory
4. Register the NSClient++ system service with the following command:

```
C:\> nsclient++ /install
```

5. Install the NSClient++ systray with the following command ('SysTray' is case-sensitive):

```
C:\> nsclient++ SysTray
```

6. Open the services manager and make sure the NSClientpp service is allowed to interact with the desktop (see the 'Log On' tab of the services manager). If it isn't already allowed to interact with the desktop, check the box to allow it to.



7. Edit the `NSC.INI` file (located in the `C:\NSClient++` directory) and make the following changes:
- Uncomment all the modules listed in the `[modules]` section, except for `CheckWMI.dll` and `RemoteConfiguration.dll`
 - Optionally require a password for clients by changing the `password` option in the `[Settings]` section.
 - Uncomment the `allowed_hosts` option in the `[Settings]` section. Add the IP address of the Nagios server to this line, or leave it blank to allow all hosts to connect.
 - Make sure the `port` option in the `[NSClient]` section is uncommented and set to '12489' (the default port).
8. Start the NSClient++ service with the following command:
- ```
C:\> nsclient++ /start
```
9. If installed properly, a new icon should appear in your system tray. It will be a yellow circle with a black 'M' inside.
10. Success! The Windows server can now be added to the Nagios monitoring configuration...

## 9.7 Configuring Nagios

Now it's time to define some **object definitions** in your Nagios configuration files in order to monitor the new Windows machine. Open the `windows.cfg` file for editing.

```
linux:~ # vi /usr/local/nagios/etc/objects/windows.cfg
```



Add a new **host** definition for the Windows machine that you're going to monitor. If this is the *\*first\** Windows machine you're monitoring, you can simply modify the sample host definition in `windows.cfg`. Change the `host_name`, `alias`, and `address` fields to appropriate values for the Windows box.

```
define host{
 use windows-server ; Inherit default values from a Windows server template (make ←
 sure you keep this line!)
 host_name winserver
 alias My Windows Server
 address 192.168.1.2
}
```

Good. Now you can add some service definitions (to the same configuration file) in order to tell Nagios to monitor different aspects of the Windows machine. If this is the *\*first\** Windows machine you're monitoring, you can simply modify the sample service definitions in `windows.cfg`.

---

**Note**

Replace `'winserver'` in the example definitions below with the name you specified in the `host_name` directive of the host definition you just added.

---

Add the following service definition to monitor the version of the NSClient++ addon that is running on the Windows server. This is useful when it comes time to upgrade your Windows servers to a newer version of the addon, as you'll be able to tell which Windows machines still need to be upgraded to the latest version of NSClient++.

```
define service{
 use generic-service
 host_name winserver
 service_description NSClient++ Version
 check_command check_nt!CLIENTVERSION
}
```

Add the following service definition to monitor the uptime of the Windows server.

```
define service{
 use generic-service
 host_name winserver
 service_description Uptime
 check_command check_nt!UPTIME
}
```

Add the following service definition to monitor the CPU utilization on the Windows server and generate a **CRITICAL** alert if the 5-minute CPU load is 90% or more or a **WARNING** alert if the 5-minute load is 80% or greater.

```
define service{
 use generic-service
 host_name winserver
 service_description CPU Load
 check_command check_nt!CPULOAD!-l 5,80,90
}
```

Add the following service definition to monitor memory usage on the Windows server and generate a **CRITICAL** alert if memory usage is 90% or more or a **WARNING** alert if memory usage is 80% or greater.

```
define service{
 use generic-service
 host_name winserver
 service_description Memory Usage
 check_command check_nt!MEMUSE!-w 80 -c 90
}
```

---

Add the following service definition to monitor usage of the C:\ drive on the Windows server and generate a **CRITICAL** alert if disk usage is 90% or more or a **WARNING** alert if disk usage is 80% or greater.

```
define service{
 use generic-service
 host_name winserver
 service_description C:\ Drive Space
 check_command check_nt!USEDISKSPACE!-l c -w 80 -c 90
}
```

Add the following service definition to monitor the W3SVC service state on the Windows machine and generate a **CRITICAL** alert if the service is stopped.

```
define service{
 use generic-service
 host_name winserver
 service_description W3SVC
 check_command check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
}
```

Add the following service definition to monitor the Explorer.exe process on the Windows machine and generate a **CRITICAL** alert if the process is not running.

```
define service{
 use generic-service
 host_name winserver
 service_description Explorer
 check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

That's it for now. You've added some basic services that should be monitored on the Windows box. Save the configuration file.

## 9.8 Password Protection

If you specified a password in the NSClient++ configuration file on the Windows machine, you'll need to modify the **check\_nt** command definition to include the password. Open the `commands.cfg` file for editing.

```
linux:~ # vi /usr/local/nagios/etc/commands.cfg
```

Change the definition of the **check\_nt** command to include the `"-s <PASSWORD>"` argument (where `PASSWORD` is the password you specified on the Windows machine) like this:

```
define command{
 command_name check_nt
 command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s PASSWORD -v $ARG1$ $ARG2$
}
```

Save the file.

## 9.9 Restarting Nagios

You're done with modifying the Nagios configuration, so you'll need to **verify your configuration files** and **restart Nagios**.

If the verification process produces any errors messages, fix your configuration file before continuing. Make sure that you don't (re)start Nagios until the verification process completes without any errors!

## Chapter 10

# Monitoring Linux/Unix Machines

## **Abstract**

This document describes how you can monitor "private" services and attributes of Linux/UNIX servers, such as:

- CPU load
- Memory usage
- Disk usage
- Logged in users
- Running processes
- etc.

## 10.1 Introduction

Publicly available services that are provided by Linux servers (HTTP, FTP, SSH, SMTP, etc.) can be monitored easily by following the documentation on [Monitoring publicly available services](#).

---

### Note

These instructions assume that you've installed Nagios according to the [quickstart guide](#). The sample configuration entries below reference objects that are defined in the sample config files (`commands.cfg`, `templates.cfg`, etc.) that are installed if you follow the quickstart.

---

## 10.2 Overview

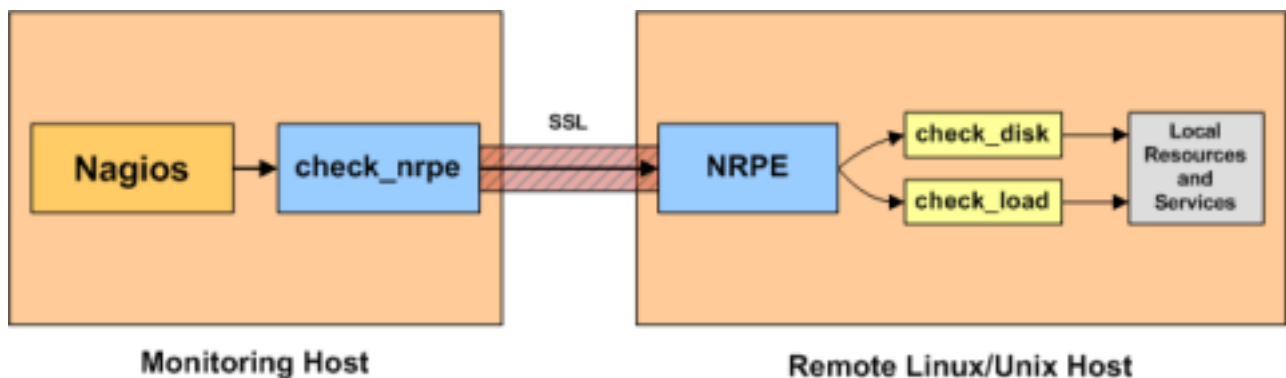
---

### Note

[This document has not been completed. I would recommend you read the documentation on the [NRPE addon](#) for instructions on how to monitor a remote Linux/Unix server.]

---

There are several different ways to monitor attributes or remote Linux/Unix servers. One is by using shared SSH keys and the `check_by_ssh` plugin to execute plugins on remote servers. This method will not be covered here, but can result in high load on your monitoring server if you are monitoring hundreds or thousands of services. The overhead of setting up/destroying SSH connections is the cause of this.



Another common method of monitoring remote Linux/Unix hosts is to use the [NRPE addon](#). NRPE allows you to execute plugins on remote Linux/Unix hosts. This is useful if you need to monitor local resources/attributes like disk usage, CPU load, memory usage, etc. on a remote host.

## **Chapter 11**

# **Monitoring Netware Servers**

## **Introduction**

This document provides information on how you can monitor Novell Netware servers.

## 11.1 External Resources

You can find documentation on monitoring Netware servers with Nagios at Novell's [Cool Solutions](#) site, including:

- [MRTGEXT: NLM module for MRTG and Nagios](#)
- [Nagios: Host and Service Monitoring Tool](#)
- [Nagios and NetWare: SNMP-based Monitoring](#)
- [Monitor DirXML/IDM Driver States with Nagios](#)
- [Check NDS Login ability with Nagios](#)
- [NDPS/iPrint Print Queue Monitoring by Nagios](#)
- [check\\_gwiaRL Plugin for Nagios 2.0](#)

---

### Tip

When you visit Novell's [Cool Solutions](#) site, search for "Nagios" to find more articles and software components related to monitoring.

---

Thanks to [Christian Mies](#), [Rainer Brunold](#), and others for contributing Nagios and Netware documentation, addons, etc. on the Novell site!

---



## **Chapter 12**

# **Monitoring Network Printers**

## **Abstract**

This document describes how you can monitor the status of networked printers. Specifically, HP printers that have internal/external JetDirect cards/devices, or other print servers (like the Troy PocketPro 100S or the Netgear PS101) that support the JetDirect protocol.

## 12.1 Introduction



The **check\_hpjd** plugin (which is part of the standard Nagios plugins distribution) allows you to monitor the status of JetDirect-capable printers which have *SNMP* enabled. The plugin is capable of detecting the following printer states:

- Paper Jam
- Out of Paper
- Printer Offline
- Intervention Required
- Toner Low
- Insufficient Memory
- Open Door
- Output Tray is Full
- and more...

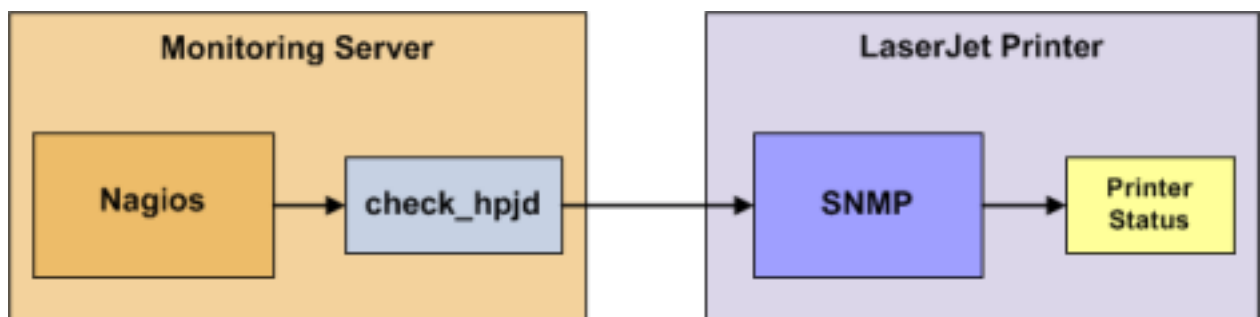
---

### Note

These instructions assume that you've installed Nagios according to the [quickstart guide](#). The sample configuration entries below reference objects that are defined in the sample config files (*commands.cfg*, *templates.cfg*, etc.) that are installed if you follow the quickstart.

---

## 12.2 Overview



Monitoring the status of a networked printer is pretty simple. JetDirect-enabled printers usually have *SNMP* enabled, which allows Nagios to monitor their status using the **check\_hpjd** plugin.

The **check\_hpjd** plugin will only get compiled and installed if you have the *net-snmp* and *net-snmp-utils* packages installed on your system. Make sure the plugin exists in `/usr/local/nagios/libexec` before you continue. If it doesn't, install *net-snmp* and *net-snmp-utils* and recompile/reinstall the Nagios plugins.

---

## 12.3 Steps

There are several steps you'll need to follow in order to monitor a new network printer. They are:

1. Perform first-time prerequisites
2. Create new host and service definitions for monitoring the printer
3. Restart the Nagios daemon

## 12.4 What's Already Done For You

To make your life a bit easier, a few configuration tasks have already been done for you:

- A *check\_hpjd* command definition has been added to the `commands.cfg` file. This allows you to use the **check\_hpjd** plugin to monitor network printers.
- A printer host template (called *generic-printer*) has already been created in the `templates.cfg` file. This allows you to add new printer host definitions in a simple manner.

The above-mentioned config files can be found in the `/usr/local/nagios/etc/objects/` directory. You can modify the definitions in these and other definitions to suit your needs better if you'd like. However, I'd recommend waiting until you're more familiar with configuring Nagios before doing so. For the time being, just follow the directions outlined below and you'll be monitoring your network printers in no time.

## 12.5 Prerequisites

The first time you configure Nagios to monitor a network printer, you'll need to do a bit of extra work. Remember, you only need to do this for the *\*first\** printer you monitor.

Edit the main Nagios config file.

```
linux:~ # vi /usr/local/nagios/etc/nagios.cfg
```

Remove the leading pound (#) sign from the following line in the main configuration file:

```
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg
```

Save the file and exit.

What did you just do? You told Nagios to look to the `/usr/local/nagios/etc/objects/printer.cfg` to find additional object definitions. That's where you'll be adding host and service definitions for the printer. That configuration file already contains some sample host, hostgroup, and service definitions. For the *\*first\** printer you monitor, you can simply modify the sample host and service definitions in that file, rather than creating new ones.

## 12.6 Configuring Nagios

You'll need to create some **object definitions** in order to monitor a new printer.

Open the `printer.cfg` file for editing.

```
linux:~ # vi /usr/local/nagios/etc/objects/printer.cfg
```

Add a new **host** definition for the networked printer that you're going to monitor. If this is the *\*first\** printer you're monitoring, you can simply modify the sample host definition in `printer.cfg`. Change the `host_name`, `alias`, and `address` fields to appropriate values for the printer.

```
define host{
 use generic-printer ; Inherit default values from a template
 host_name hplj2605dn ; The name we're giving to this printer
 alias HP LaserJet 2605dn ; A longer name associated with the printer
 address 192.168.1.30 ; IP address of the printer
 hostgroups allhosts ; Host groups this printer is associated with
}
```

Now you can add some service definitions (to the same configuration file) to monitor different aspects of the printer. If this is the *\*first\** printer you're monitoring, you can simply modify the sample service definition in `printer.cfg`.

---

**Note**

Replace "hplj2605dn" in the example definitions below with the name you specified in the `host_name` directive of the host definition you just added.

---

Add the following service definition to check the status of the printer. The service uses the **check\_hpjd** plugin to check the status of the printer every 10 minutes by default. The SNMP community string used to query the printer is "public" in this example.

```
define service{
 use generic-service ; Inherit values from a template
 host_name hplj2605dn ; The name of the host the service is ↵
 associated with
 service_description Printer Status ; The service description
 check_command check_hpjd!-C public ; The command used to monitor the service
 normal_check_interval 10 ; Check the service every 10 minutes under normal conditions
 retry_check_interval 1 ; Re-check the service every minute until its final/hard ↵
 state is determined
}
```

Add the following service definition to ping the printer every 10 minutes by default. This is useful for monitoring RTA, packet loss, and general network connectivity.

```
define service{
 use generic-service
 host_name hplj2605dn
 service_description PING
 check_command check_ping!3000.0,80%!5000.0,100%
 normal_check_interval 10
 retry_check_interval 1
}
```

Save the file.

## 12.7 Restarting Nagios

Once you've added the new host and service definitions to the `printer.cfg` file, you're ready to start monitoring the printer. To do this, you'll need to **verify your configuration** and **restart Nagios**.

If the verification process produces any errors messages, fix your configuration file before continuing. Make sure that you don't (re)start Nagios until the verification process completes without any errors!

---

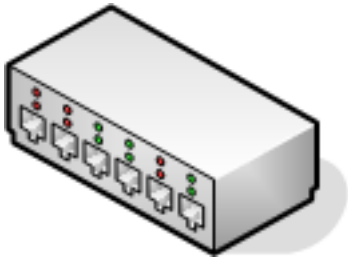
## **Chapter 13**

# **Monitoring Routers and Switches**

## **Abstract**

This document describes how you can monitor the status of network switches and routers. Some cheaper "unmanaged" switches and hubs don't have IP addresses and are essentially invisible on your network, so there's not any way to monitor them. More expensive switches and routers have addresses assigned to them and can be monitored by pinging them or using *SNMP* to query status information.

## 13.1 Introduction



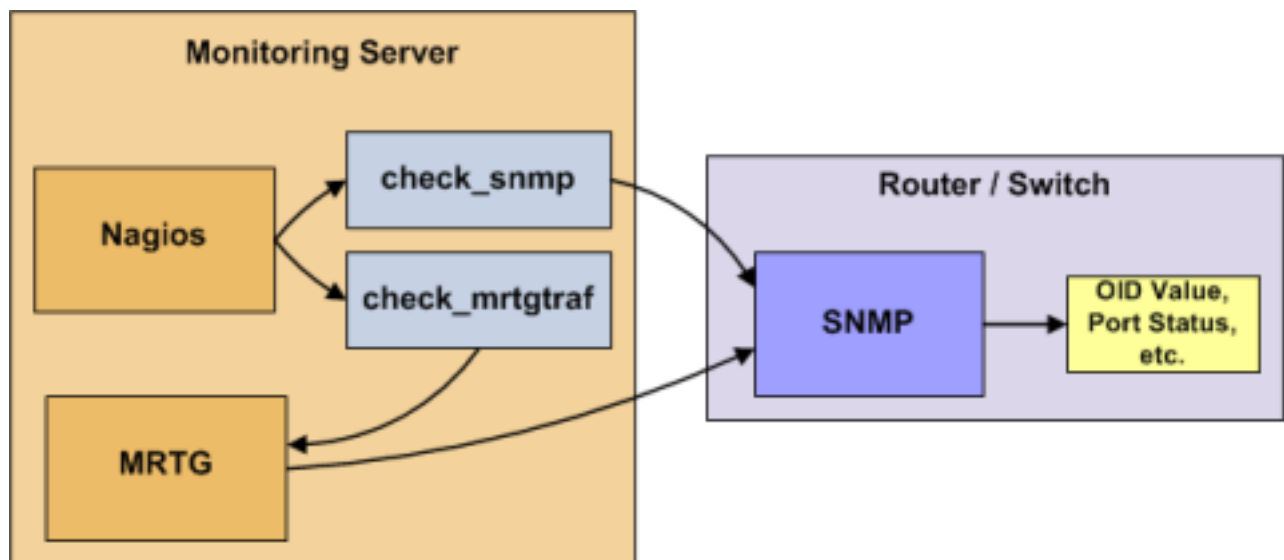
I'll describe how you can monitor the following things on managed switches, hubs, and routers:

- Packet loss, round trip average
- SNMP status information
- Bandwidth / traffic rate

### Note

These instructions assume that you've installed Nagios according to the [quickstart guide](#). The sample configuration entries below reference objects that are defined in the sample config files (`commands.cfg`, `templates.cfg`, etc.) that are installed when you follow the quickstart.

## 13.2 Overview



Monitoring switches and routers can either be easy or more involved - depending on what equipment you have and what you want to monitor. As they are critical infrastructure components, you'll no doubt want to monitor them in at least some basic manner.

Switches and routers can be monitored easily by "pinging" them to determine packet loss, RTA, etc. If your switch supports SNMP, you can monitor port status, etc. with the **check\_snmp** plugin and bandwidth (if you're using MRTG) with the **check\_mrtgtraf** plugin.

The **check\_snmp** plugin will only get compiled and installed if you have the `net-snmp` and `net-snmp-utils` packages installed on your system. Make sure the plugin exists in `/usr/local/nagios/libexec` before you continue. If it doesn't, install `net-snmp` and `net-snmp-utils` and recompile/reinstall the Nagios plugins.



## 13.3 Steps

There are several steps you'll need to follow in order to monitor a new router or switch. They are:

1. Perform first-time prerequisites
2. Create new host and service definitions for monitoring the device
3. Restart the Nagios daemon

## 13.4 What's Already Done For You

To make your life a bit easier, a few configuration tasks have already been done for you:

- Two command definitions (*check\_snmp* and *check\_local\_mrtgtraf*) have been added to the `commands.cfg` file. These allows you to use the **check\_snmp** and **check\_mrtgtraf** plugins to monitor network routers.
- A switch host template (called *generic-switch*) has already been created in the `templates.cfg` file. This allows you to add new router/switch host definitions in a simple manner.

The above-mentioned config files can be found in the `/usr/local/nagios/etc/objects/` directory. You can modify the definitions in these and other definitions to suit your needs better if you'd like. However, I'd recommend waiting until you're more familiar with configuring Nagios before doing so. For the time being, just follow the directions outlined below and you'll be monitoring your network routers/switches in no time.

## 13.5 Prerequisites

The first time you configure Nagios to monitor a network switch, you'll need to do a bit of extra work. Remember, you only need to do this for the *\*first\** switch you monitor.

Edit the main Nagios config file.

```
linux:~ # vi /usr/local/nagios/etc/nagios.cfg
```

Remove the leading pound (#) sign from the following line in the main configuration file:

```
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

Save the file and exit.

What did you just do? You told Nagios to look to the `/usr/local/nagios/etc/objects/switch.cfg` to find additional object definitions. That's where you'll be adding host and service definitions for routers and switches. That configuration file already contains some sample host, hostgroup, and service definitions. For the *\*first\** router/switch you monitor, you can simply modify the sample host and service definitions in that file, rather than creating new ones.

## 13.6 Configuring Nagios

You'll need to create some **object definitions** in order to monitor a new router/switch.

Open the `switch.cfg` file for editing.

```
linux:~ # vi /usr/local/nagios/etc/objects/switch.cfg
```

Add a new **host** definition for the switch that you're going to monitor. If this is the *\*first\** switch you're monitoring, you can simply modify the sample host definition in `switch.cfg`. Change the `host_name`, `alias`, and `address` fields to appropriate values for the switch.

```
define host{
 use generic-switch ; Inherit default values from a template
 host_name linksys-srw224p ; The name we're giving to this switch
 alias Linksys SRW224P Switch ; A longer name associated with the switch
 address 192.168.1.253 ; IP address of the switch
 hostgroups allhosts,switches ; Host groups this switch is associated with
}
```

## 13.7 Monitoring Services

Now you can add some service definitions (to the same configuration file) to monitor different aspects of the switch. If this is the *\*first\** switch you're monitoring, you can simply modify the sample service definition in `switch.cfg`.

### Note

Replace '*linksys-srw224p*' in the example definitions below with the name you specified in the `host_name` directive of the host definition you just added.

## 13.8 Monitoring Packet Loss and RTA

Add the following service definition in order to monitor packet loss and round trip average between the Nagios host and the switch every 5 minutes under normal conditions.

```
define service{
 use generic-service ❶
 host_name linksys-srw224p ❷
 service_description PING ❸
 check_command check_ping!200.0,20%!600.0,60% ❹
 normal_check_interval 5 ❺
 retry_check_interval 1 ❻
}
```

- ❶ Inherit values from a template
- ❷ The name of the host the service is associated with
- ❸ The service description
- ❹ The command used to monitor the service
- ❺ Check the service every 5 minutes under normal conditions
- ❻ Re-check the service every minute until its final/hard state is determined

This service will be:

- CRITICAL if the round trip average (RTA) is greater than 600 milliseconds or the packet loss is 60% or more
- WARNING if the RTA is greater than 200 ms or the packet loss is 20% or more
- OK if the RTA is less than 200 ms and the packet loss is less than 20%



In the example above, the `/var/lib/mrtg/192.168.1.253_1.log` option that gets passed to the `check_local_mrtgtraf` command tells the plugin which MRTG log file to read from.

The `AVG` option tells it that it should use average bandwidth statistics. The `1000000,2000000` options are the warning thresholds (in bytes) for incoming traffic rates.

The `5000000,5000000` are critical thresholds (in bytes) for outgoing traffic rates. The `10` option causes the plugin to return a **CRITICAL** state if the MRTG log file is older than 10 minutes (it should be updated every 5 minutes).

Save the file.

## 13.11 Restarting Nagios

Once you've added the new host and service definitions to the `switch.cfg` file, you're ready to start monitoring the router/switch. To do this, you'll need to **verify your configuration** and **restart Nagios**.

If the verification process produces any errors messages, fix your configuration file before continuing. Make sure that you don't (re)start Nagios until the verification process completes without any errors!

---

## **Chapter 14**

# **Monitoring Publicly Available Services**

## **Abstract**

This document describes how you can monitor publicly available services, applications and protocols. By 'public' I mean services that are accessible across the network - either the local network or the greater Internet. Examples of public services include HTTP, POP3, IMAP, FTP, and SSH. There are many more public services that you probably use on a daily basis. These services and applications, as well as their underlying protocols, can usually be monitored by Nagios without any special access requirements.

## 14.1 Introduction

Private services, in contrast, cannot be monitored with Nagios without an intermediary agent of some kind. Examples of private services associated with hosts are things like CPU load, memory usage, disk usage, current user count, process information, etc. These private services or attributes of hosts are not usually exposed to external clients. This situation requires that an intermediary monitoring agent be installed on any host that you need to monitor such information on. More information on monitoring private services on different types of hosts can be found in the documentation on:

- [Monitoring Windows machines](#)
- [Monitoring Netware servers](#)
- [Monitoring Linux/Unix machines](#)

---

### Tip

Occasionally you will find that information on private services and applications can be monitored with `SNMP`. The `SNMP` agent allows you to remotely monitor otherwise private (and inaccessible) information about the host. For more information about monitoring services using `SNMP`, check out the documentation on [Monitoring routers/switches](#).

---

### Note

These instructions assume that you've installed Nagios according to the [quickstart guide](#). The sample configuration entries below reference objects that are defined in the sample `commands.cfg` and `localhost.cfg` config files.

---

## 14.2 Plugins For Monitoring Services

When you find yourself needing to monitor a particular application, service, or protocol, chances are good that a [plugin](#) exists to monitor it. The official Nagios plugins distribution comes with plugins that can be used to monitor a variety of services and protocols. There are also a large number of contributed plugins that can be found in the `contrib/` subdirectory of the plugin distribution. The [NagiosExchange.org](#) website hosts a number of additional plugins that have been written by users, so check it out when you have a chance.

If you don't happen to find an appropriate plugin for monitoring what you need, you can always write your own. Plugins are easy to write, so don't let this thought scare you off. Read the documentation on [developing plugins](#) for more information.

I'll walk you through monitoring some basic services that you'll probably use sooner or later. Each of these services can be monitored using one of the plugins that gets installed as part of the Nagios plugins distribution. Let's get started...

## 14.3 Creating A Host Definition

Before you can monitor a service, you first need to define a [host](#) that is associated with the service. You can place host definitions in any object configuration file specified by a `cfile` directive or placed in a directory specified by a `cdir` directive. If you have already created a host definition, you can skip this step.

For this example, let's say you want to monitor a variety of services on a remote host. Let's call that host *remotehost*. The host definition can be placed in its own file or added to an already existing object configuration file. Here's what the host definition for *remotehost* might look like:

```
define host{
 use generic-host ; Inherit default values from a template
 host_name remotehost ; The name we're giving to this host
 alias Some Remote Host ; A longer name associated with the host
 address 192.168.1.50 ; IP address of the host
 hostgroups allhosts ; Host groups this host is associated with
}
```

---

Now that a definition has been added for the host that will be monitored, we can start defining services that should be monitored. As with host definitions, service definitions can be placed in any object configuration file.

## 14.4 Creating Service Definitions

For each service you want to monitor, you need to define a **service** in Nagios that is associated with the host definition you just created. You can place service definitions in any object configuration file specified by a **cfg\_file** directive or placed in a directory specified by a **cfg\_dir** directive.

Some example service definitions for monitoring common public service (HTTP, FTP, etc) are given below.

## 14.5 Monitoring HTTP

Chances are you're going to want to monitor web servers at some point - either yours or someone else's. The **check\_http** plugin is designed to do just that. It understands the HTTP protocol and can monitor response time, error codes, strings in the returned HTML, server certificates, and much more.

The `commands.cfg` file contains a command definition for using the **check\_http** plugin. It looks like this:

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

A simple service definition for monitoring the HTTP service on the *remotehost* machine might look like this:

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description HTTP
 check_command check_http
}
```

This simple service definition will monitor the HTTP service running on *remotehost*. It will produce alerts if the web server doesn't respond within 10 seconds or if it returns HTTP errors codes (403, 404, etc.). That's all you need for basic monitoring. Pretty simple, huh?

---

### Tip

For more advanced monitoring, run the **check\_http** plugin manually with `--help` as a command-line argument to see all the options you can give the plugin. This `--help` syntax works with all of the plugins I'll cover in this document.

---

A more advanced definition for monitoring the HTTP service is shown below. This service definition will check to see if the `/download/index.php` URI contains the string "latest-version.tar.gz". It will produce an error if the string isn't found, the URI isn't valid, or the web server takes longer than 5 seconds to respond.

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description Product Download Link
 check_command check_http!-u /download/index.php -t 5 -s "latest-version.tar.gz"
}
```

---



## 14.6 Monitoring FTP

When you need to monitor FTP servers, you can use the **check\_ftp** plugin. The `commands.cfg` file contains a command definition for using the **check\_ftp** plugin, which looks like this:

```
define command{
 command_name check_ftp
 command_line $USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
}
```

A simple service definition for monitoring the FTP server on *remotehost* would look like this:

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description FTP
 check_command check_ftp
}
```

This service definition will monitor the FTP service and generate alerts if the FTP server doesn't respond within 10 seconds.

A more advanced service definition is shown below. This service will check the FTP server running on port 1023 on *remotehost*. It will generate an alert if the server doesn't respond within 5 seconds or if the server response doesn't contain the string 'Pure-FTPd [TLS]'.

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description Special FTP
 check_command check_ftp!-p 1023 -t 5 -e "Pure-FTPd [TLS]"
}
```

## 14.7 Monitoring SSH

When you need to monitor SSH servers, you can use the **check\_ssh** plugin. The `commands.cfg` file contains a command definition for using the **check\_ssh** plugin, which looks like this:

```
define command{
 command_name check_ssh
 command_line $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
}
```

A simple service definition for monitoring the SSH server on *remotehost* would look like this:

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description SSH
 check_command check_ssh
}
```

This service definition will monitor the SSH service and generate alerts if the SSH server doesn't respond within 10 seconds.

A more advanced service definition is shown below. This service will check the SSH server and generate an alert if the server doesn't respond within 5 seconds or if the server version string doesn't match 'OpenSSH\_4.2'.

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
```

```

service_description SSH Version Check
check_command check_ssh!-t 5 -r "OpenSSH_4.2"
}

```

## 14.8 Monitoring SMTP

The **check\_smtp** plugin can be using for monitoring your email servers. The `commands.cfg` file contains a command definition for using the **check\_smtp** plugin, which looks like this:

```

define command{
 command_name check_smtp
 command_line $USER1$/check_smtp -H $HOSTADDRESS$ $ARG1$
}

```

A simple service definition for monitoring the SMTP server on *remotehost* would look like this:

```

define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description SMTP
 check_command check_smtp
}

```

This service definition will monitor the SMTP service and generate alerts if the SMTP server doesn't respond within 10 seconds.

A more advanced service definition is shown below. This service will check the SMTP server and generate an alert if the server doesn't respond within 5 seconds or if the response from the server doesn't contain "mygreatmailserver.com".

```

define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description SMTP Response Check
 check_command check_smtp!-t 5 -e "mygreatmailserver.com"
}

```

## 14.9 Monitoring POP3

The **check\_pop** plugin can be using for monitoring the POP3 service on your email servers. The `commands.cfg` file contains a command definition for using the **check\_pop** plugin, which looks like this:

```

define command{
 command_name check_pop
 command_line $USER1$/check_pop -H $HOSTADDRESS$ $ARG1$
}

```

A simple service definition for monitoring the POP3 service on *remotehost* would look like this:

```

define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description POP3
 check_command check_pop
}

```

This service definition will monitor the POP3 service and generate alerts if the POP3 server doesn't respond within 10 seconds.

A more advanced service definition is shown below. This service will check the POP3 service and generate an alert if the server doesn't respond within 5 seconds or if the response from the server doesn't contain "mygreatmailserver.com".

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description POP3 Response Check
 check_command check_pop!-t 5 -e "mygreatmailserver.com"
}
```

## 14.10 Monitoring IMAP

The **check\_imap** plugin can be using for monitoring IMAP4 service on your email servers. The `commands.cfg` file contains a command definition for using the **check\_imap** plugin, which looks like this:

```
define command{
 command_name check_imap
 command_line $USER1$/check_imap -H $HOSTADDRESS$ $ARG1$
}
```

A simple service definition for monitoring the IMAP4 service on *remotehost* would look like this:

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description IMAP
 check_command check_imap
}
```

This service definition will monitor the IMAP4 service and generate alerts if the IMAP server doesn't respond within 10 seconds.

A more advanced service definition is shown below. This service will check the IAMP4 service and generate an alert if the server doesn't respond within 5 seconds or if the response from the server doesn't contain 'mygreatmailserver.com'.

```
define service{
 use generic-service ; Inherit default values from a template
 host_name remotehost
 service_description IMAP4 Response Check
 check_command check_imap!-t 5 -e "mygreatmailserver.com"
}
```

## 14.11 Restarting Nagios

Once you've added the new host and service definitions to your object configuration file(s), you're ready to start monitoring them. To do this, you'll need to **verify your configuration** and **restart Nagios**.

If the verification process produces any errors messages, fix your configuration file before continuing. Make sure that you don't (re)start Nagios until the verification process completes without any errors!

## **Part III**

# **Configuring Nagios**

## Chapter 15

# Configuration Overview

### 15.1 Introduction

There are several different configuration files that you're going to need to create or edit before you start monitoring anything. Be patient! Configuring Nagios can take quite a while, especially if you're first-time user. Once you figure out how things work, it'll all be well worth your time. :-)

---

**Note**

Sample configuration files are installed in the `/usr/local/nagios/etc/` directory when you follow the [Quickstart installation guide](#).

---

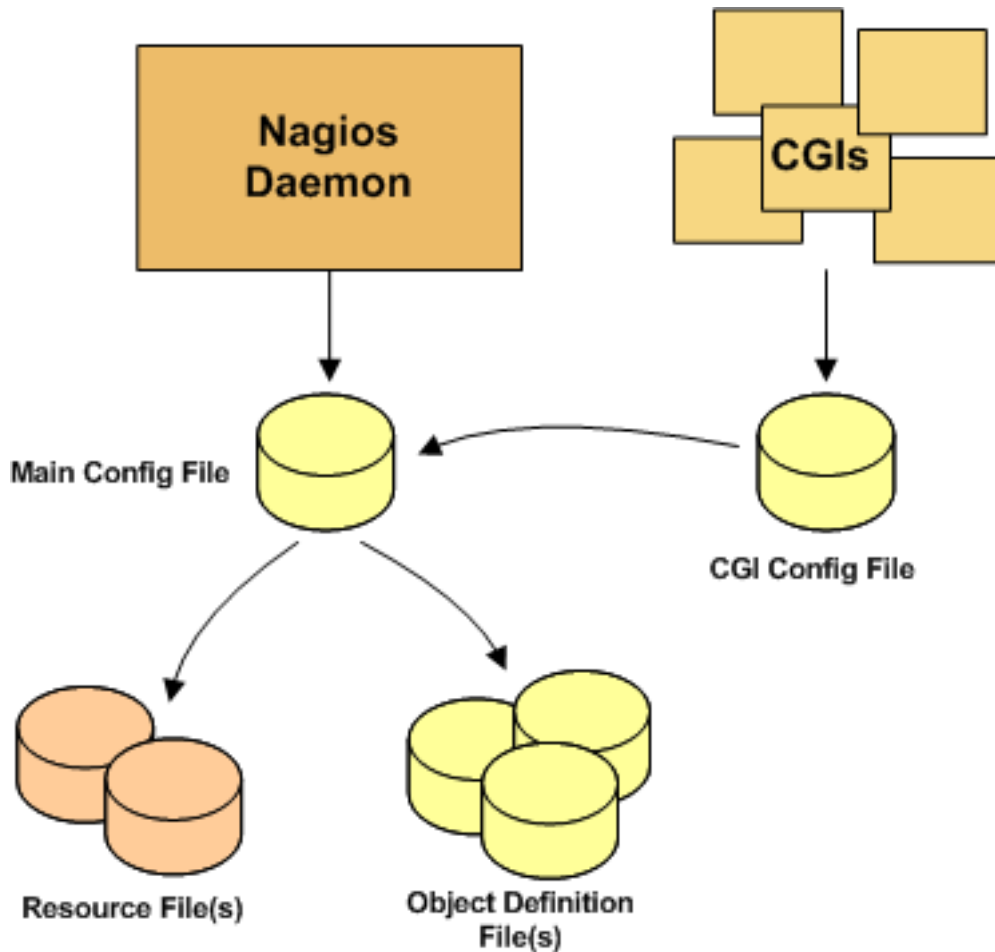
### 15.2 Main Configuration File

The main configuration file contains a number of directives that affect how the Nagios daemon operates. This config file is read by both the Nagios daemon and the CGIs. This is where you're going to want to get started in your configuration adventures.

Documentation for the main configuration file can be found [Main Configuration File Options](#).

---

## 15.3 Resource File(s)



Resource files can be used to store user-defined macros. The main point of having resource files is to use them to store sensitive configuration information (like passwords), without making them available to the CGIs.

You can specify one or more optional resource files by using the `resource_file` directive in your main configuration file.

## 15.4 Object Definition Files

Object definition files are used to define hosts, services, hostgroups, contacts, contactgroups, commands, etc. This is where you define all the things you want monitor and how you want to monitor them.

You can specify one or more object definition files by using the `cfg_file` and/or `cfg_dir` directives in your main configuration file.

An introduction to object definitions, and how they relate to each other, can be found [here](#).

## 15.5 CGI Configuration File

The CGI configuration file contains a number of directives that affect the operation of the `CGIs`. It also contains a reference the main configuration file, so the CGIs know how you've configured Nagios and where your object definitions are stored.

Documentation for the CGI configuration file can be found in the [CGI Configuration File Options](#).

## Chapter 16

# Main Configuration File Options

---

### Note

When creating and/or editing configuration files, keep the following in mind:

- Lines that start with a '#' character are taken to be comments and are not processed
  - Variables names must begin at the start of the line - no white space is allowed before the name
  - Variable names are case-sensitive
- 

## 16.1 Sample Configuration File

---

### Tip

A sample main configuration file (`/usr/local/nagios/etc/nagios.cfg`) is installed for you when you follow the [Quickstart installation guide](#).

---

## 16.2 Config File Location

The main configuration file is usually named `nagios.cfg` and located in the `/usr/local/nagios/etc/` directory.

## 16.3 Configuration File Variables

Below you will find descriptions of each main Nagios configuration file option...

### 16.3.1 Log File

**Format** `log_file=<file_name>`

**Example** `log_file=/usr/local/nagios/var/nagios.log`

This variable specifies where Nagios should create its main log file. This should be the first variable that you define in your configuration file, as Nagios will try to write errors that it finds in the rest of your configuration data to this file. If you have [Log Rotation Method](#) enabled, this file will automatically be rotated every hour, day, week, or month.

---

### 16.3.2 Object Configuration File

Format :

```
cfg_file=<file_name>
```

```
cfg_file=/usr/local/nagios/etc/hosts.cfg
cfg_file=/usr/local/nagios/etc/services.cfg
cfg_file=/usr/local/nagios/etc/commands.cfg
```

#### Format

```
cfg_file=<file_name>
```

**Example** `cfg_file=/usr/local/nagios/etc/hosts.cfg`  
`cfg_file=/usr/local/nagios/etc/services.cfg`  
`cfg_file=/usr/local/nagios/etc/commands.cfg`

This directive is used to specify an **Object Configuration Overview** containing object definitions that Nagios should use for monitoring. Object configuration files contain definitions for hosts, host groups, contacts, contact groups, services, commands, etc. You can separate your configuration information into several files and specify multiple `cfg_file=` statements to have each of them processed.

### 16.3.3 Object Configuration Directory

Format: `cfg_dir=<directory_name>`

Example: `cfg_dir=/usr/local/nagios/etc/commands`  
`cfg_dir=/usr/local/nagios/etc/services`  
`cfg_dir=/usr/local/nagios/etc/hosts`

This directive is used to specify a directory which contains **Object Configuration Overview** that Nagios should use for monitoring. All files in the directory with a `.cfg` extension are processed as object config files. Additionally, Nagios will recursively process all config files in subdirectories of the directory you specify here. You can separate your configuration files into different directories and specify multiple

```
cfg_dir=
```

statements to have all config files in each directory processed.

### 16.3.4 Object Cache File

Format: `object_cache_file=<file_name>`

Example: `object_cache_file=/usr/local/nagios/var/objects.cache`



This directive is used to specify a file in which a cached copy of [Object Configuration Overview](#) should be stored. The cache file is (re)created every time Nagios is (re)started and is used by the CGIs. It is intended to speed up config file caching in the CGIs and allow you to edit the source while Nagios is running without affecting the output displayed in the CGIs.

### 16.3.5 Precached Object File

Format: `precached_object_file=<file_name>`

Example: `precached_object_file=/usr/local/nagios/var/objects.precache`

This directive is used to specify a file in which a pre-processed, pre-cached copy of [Object Configuration Overview](#) should be stored. This file can be used to drastically improve startup times in large/complex Nagios installations. Read more information on how to speed up start times [Fast Startup Options](#).

### 16.3.6 Resource File

Format: `resource_file=<file_name>`

Example: `resource_file=/usr/local/nagios/etc/resource.cfg`

This is used to specify an optional resource file that can contain `$USERn$` [Understanding Macros and How They Work](#) definitions. `$USERn$` macros are useful for storing usernames, passwords, and items commonly used in command definitions (like directory paths). The CGIs will *not* attempt to read resource files, so you can set restrictive permissions (600 or 660) on them to protect sensitive information. You can include multiple resource files by adding multiple `resource_file` statements to the main config file - Nagios will process them all. See the sample `resource.cfg` file in the `sample-config/` subdirectory of the Nagios distribution for an example of how to define `$USERn$` macros.

### 16.3.7 Temp File

Format: `temp_file=<file_name>`

Example: `temp_file=/usr/local/nagios/var/nagios.tmp`

This is a temporary file that Nagios periodically creates to use when updating comment data, status data, etc. The file is deleted when it is no longer needed.

### 16.3.8 Temp Path

---

Format:                `temp_path=<dir_name>`

Example:              `temp_path=/tmp`

This is a directory that Nagios can use as scratch space for creating temporary files used during the monitoring process. You should run **tmpwatch**, or a similiar utility, on this directory occassionally to delete files older than 24 hours.

### 16.3.9 Status File

Format:                `status_file=<file_name>`

Example:              `status_file=/usr/local/nagios/var/status.dat`

This is the file that Nagios uses to store the current status, comment, and downtime information. This file is used by the CGIs so that current monitoring status can be reported via a web interface. The CGIs must have read access to this file in order to function properly. This file is deleted every time Nagios stops and recreated when it starts.

### 16.3.10 Status File Update Interval

Format:                `status_update_interval=<seconds>`

Example:              `status_update_interval=15`

This setting determines how often (in seconds) that Nagios will update status data in the **Status File**. The minimum update interval is 1 second.

### 16.3.11 Nagios User

Format:                `nagios_user=<username/UID>`

Example:              `nagios_user=nagios`

This is used to set the effective user that the Nagios process should run as. After initial program startup and before starting to monitor anything, Nagios will drop its effective privileges and run as this user. You may specify either a username or a UID.

---

### 16.3.12 Nagios Group

Format: `nagios_group=<groupname/GID>`

Example: `nagios_group=nagios`

This is used to set the effective group that the Nagios process should run as. After initial program startup and before starting to monitor anything, Nagios will drop its effective privileges and run as this group. You may specify either a groupname or a GID.

### 16.3.13 Notifications Option

Format: `enable_notifications=<0/1>`

Example: `enable_notifications=1`

This option determines whether or not Nagios will send out **notifications** when it initially (re)starts. If this option is disabled, Nagios will not send out notifications for any host or service.

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Disable notifications
- 1 = Enable notifications (default)

### 16.3.14 Service Check Execution Option

Format: `execute_service_checks=<0/1>`

Example: `execute_service_checks=1`

This option determines whether or not Nagios will execute service checks when it initially (re)starts. If this option is disabled, Nagios will not actively execute any service checks and will remain in a sort of 'sleep' mode (it can still accept **passive checks** unless you've **Passive Service Check Acceptance Option**). This option is most often used when configuring backup monitoring servers, as described in the documentation on **redundancy**, or when setting up a **distributed** monitoring environment.

---

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Don't execute service checks
- 1 = Execute service checks (default)

### 16.3.15 Passive Service Check Acceptance Option

Format: `accept_passive_service_checks=<0/1>`

Example: `accept_passive_service_checks=1`

This option determines whether or not Nagios will accept **passive service checks** when it initially (re)starts. If this option is disabled, Nagios will not accept any passive service checks.

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Don't accept passive service checks
- 1 = Accept passive service checks (default)

### 16.3.16 Host Check Execution Option

Format: `execute_host_checks=<0/1>`

Example: `execute_host_checks=1`

This option determines whether or not Nagios will execute on-demand and regularly scheduled host checks when it initially (re)starts. If this option is disabled, Nagios will not actively execute any host checks, although it can still accept **passive host checks** unless you've **Passive Service Check Acceptance Option**). This option is most often used when configuring backup monitoring servers, as described in the documentation on **redundancy**, or when setting up a **distributed** monitoring environment.

---

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Don't execute host checks
- 1 = Execute host checks (default)

### 16.3.17 Passive Host Check Acceptance Option

Format: `accept_passive_host_checks=<0/1>`

Example: `accept_passive_host_checks=1`

This option determines whether or not Nagios will accept **passive host checks** when it initially (re)starts. If this option is disabled, Nagios will not accept any passive host checks.

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Don't accept passive host checks
- 1 = Accept passive host checks (default)

### 16.3.18 Event Handler Option

Format: `enable_event_handlers=<0/1>`

Example: `enable_event_handlers=1`

This option determines whether or not Nagios will run **event handlers** when it initially (re)starts. If this option is disabled, Nagios will not run any host or service event handlers.

---

---

**Note**

If you have **State Retention Option** enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the **State Retention File**), unless you disable the **Use Retained Program State Option** option. If you want to change this option when state retention is active (and the **Use Retained Program State Option** is enabled), you'll have to use the appropriate **external command** or change it via the web interface. Values are as follows:

---

- 0 = Disable event handlers
- 1 = Enable event handlers (default)

### 16.3.19 Log Rotation Method

Format: `log_rotation_method=<n/h/d/w/m>`

Example: `log_rotation_method=d`

This is the rotation method that you would like Nagios to use for your log file. Values are as follows:

- n = None (don't rotate the log - this is the default)
- h = Hourly (rotate the log at the top of each hour)
- d = Daily (rotate the log at midnight each day)
- w = Weekly (rotate the log at midnight on Saturday)
- m = Monthly (rotate the log at midnight on the last day of the month)

### 16.3.20 Log Archive Path

Format: `log_archive_path=<path>`

Example: `log_archive_path=/usr/local/nagios/var/archives/`

This is the directory where Nagios should place log files that have been rotated. This option is ignored if you choose to not use the **Log Rotation Method** functionality.

### 16.3.21 External Command Check Option

Format: `check_external_commands=<0/1>`

---

Example: `check_external_commands=1`

This option determines whether or not Nagios will check the **External Command File** for commands that should be executed. This option must be enabled if you plan on using the **command CGI** to issue commands via the web interface. More information on external commands can be found [here](#).

- 0 = Don't check external commands
- 1 = Check external commands (default)

### 16.3.22 External Command Check Interval

Format: `command_check_interval=<xxx>[s]`

Example: `command_check_interval=1`

If you specify a number with an "s" appended to it (i.e. 30s), this is the number of seconds to wait between external command checks. If you leave off the "s", this is the number of 'time units' to wait between external command checks. Unless you've changed the **Timing Interval Length** value (as defined below) from the default value of 60, this number will mean minutes.

---

**Note**

By setting this value to **-1**, Nagios will check for external commands as often as possible. Each time Nagios checks for external commands it will read and process all commands present in the **External Command File** before continuing on with its other duties. More information on external commands can be found [here](#).

---

### 16.3.23 External Command File

Format: `command_file=<file_name>`

Example: `command_file=/usr/local/nagios/var/rw/nagios.cmd`

This is the file that Nagios will check for external commands to process. The **command CGI** writes commands to this file. The external command file is implemented as a named pipe (FIFO), which is created when Nagios starts and removed when it shuts down. If the file exists when Nagios starts, the Nagios process will terminate with an error message. More information on external commands can be found [here](#).

### 16.3.24 External Command Buffer Slots

---

Format: `external_command_buffer_slots=<#>`

Example: `external_command_buffer_slots=512`

---

**Note**

This is an advanced feature.

---

This option determines how many buffer slots Nagios will reserve for caching external commands that have been read from the external command file by a worker thread, but have not yet been processed by the main thread of the Nagios daemon. Each slot can hold one external command, so this option essentially determines how many commands can be buffered. For installations where you process a large number of passive checks (e.g. [distributed setups](#)), you may need to increase this number. You should consider using MRTG to graph Nagios' usage of external command buffers. You can read more on how to configure graphing [here](#).

### 16.3.25 Lock File

Format: `lock_file=<file_name>`

Example: `lock_file=/tmp/nagios.lock`

This option specifies the location of the lock file that Nagios should create when it runs as a daemon (when started with the `-d` command line argument). This file contains the process id (PID) number of the running Nagios process.

### 16.3.26 State Retention Option

Format: `retain_state_information=<0/1>`

Example: `retain_state_information=1`

This option determines whether or not Nagios will retain state information for hosts and services between program restarts. If you enable this option, you should supply a value for the [State Retention File](#) variable. When enabled, Nagios will save all state information for hosts and service before it shuts down (or restarts) and will read in previously saved state information when it starts up again.

- 0 = Don't retain state information
  - 1 = Retain state information (default)
-



### 16.3.27 State Retention File

Format: `state_retention_file=<file_name>`

Example: `state_retention_file=/usr/local/nagios/var/retention.dat`

This is the file that Nagios will use for storing status, downtime, and comment information before it shuts down. When Nagios is restarted it will use the information stored in this file for setting the initial states of services and hosts before it starts monitoring anything. In order to make Nagios retain state information between program restarts, you must enable the **State Retention Option** option.

### 16.3.28 Automatic State Retention Update Interval

Format: `retention_update_interval=<minutes>`

Example: `retention_update_interval=60`

This setting determines how often (in minutes) that Nagios will automatically save retention data during normal operation. If you set this value to 0, Nagios will not save retention data at regular intervals, but it will still save retention data before shutting down or restarting. If you have disabled state retention (with the **State Retention Option** option), this option has no effect.

### 16.3.29 Use Retained Program State Option

Format: `use_retained_program_state=<0/1>`

Example: `use_retained_program_state=1`

This setting determines whether or not Nagios will set various program-wide state variables based on the values saved in the retention file. Some of these program-wide state variables that are normally saved across program restarts if state retention is enabled include the **Notifications Option**, **Flap Detection Option**, **Event Handler Option**, **Service Check Execution Option**, and **Passive Service Check Acceptance Option** !!!!!!!! options. If you do not have **State Retention Option** enabled, this option has no effect.

- 0 = Don't use retained program state
- 1 = Use retained program state (default)

### 16.3.30 Use Retained Scheduling Info Option

---

Format: `use_retained_scheduling_info=<0/1>`

Example: `use_retained_scheduling_info=1`

This setting determines whether or not Nagios will retain scheduling info (next check times) for hosts and services when it restarts. If you are adding a large number (or percentage) of hosts and services, I would recommend disabling this option when you first restart Nagios, as it can adversely skew the spread of initial checks. Otherwise you will probably want to leave it enabled.

- 0 = Don't use retained scheduling info
- 1 = Use retained scheduling info (default)

### 16.3.31 Retained Host and Service Attribute Masks

Format: `retained_host_attribute_mask=<number>retained_service_attribute_mask=<↵  
number>`

Example: `retained_host_attribute_mask=0retained_service_attribute_mask=0`



#### Warning

This is an advanced feature. You'll need to read the Nagios source code to use this option effectively.

---

These options determine which host or service attributes are NOT retained across program restarts. The values for these options are a bitwise AND of values specified by the 'MODATTR\_' definitions in the `include/common.h` source code file. By default, all host and service attributes are retained.

### 16.3.32 Retained Process Attribute Masks

Format: `retained_process_host_attribute_mask=<number> ↵  
retained_process_service_attribute_mask=<number>`

Example: `retained_process_host_attribute_mask=0 ↵  
retained_process_service_attribute_mask=0`



#### Warning

This is an advanced feature. You'll need to read the Nagios source code to use this option effectively.

---

These options determine which process attributes are NOT retained across program restarts. There are two masks because there are often separate host and service process attributes that can be changed. For example, host checks can be disabled at the program level, while service checks are still enabled. The values for these options are a bitwise AND of values specified by the 'MODATTR\_' definitions in the `include/common.h` source code file. By default, all process attributes are retained.

### 16.3.33 Retained Contact Attribute Masks

Format: `retained_contact_host_attribute_mask=<number> ↔  
retained_contact_service_attribute_mask=<number>`

Example: `retained_contact_host_attribute_mask=0 ↔  
retained_contact_service_attribute_mask=0`



#### Warning

This is an advanced feature. You'll need to read the Nagios source code to use this option effectively.

These options determine which contact attributes are NOT retained across program restarts. There are two masks because there are often separate host and service contact attributes that can be changed. The values for these options are a bitwise AND of values specified by the 'MODATTR\_' definitions in the `include/common.h` source code file. By default, all process attributes are retained.

### 16.3.34 Syslog Logging Option

Format: `use_syslog=<0/1>`

Example: `use_syslog=1`

This variable determines whether messages are logged to the syslog facility on your local host. Values are as follows:

- 0 = Don't use syslog facility
- 1 = Use syslog facility

### 16.3.35 Notification Logging Option

Format: `log_notifications=<0/1>`

Example: `log_notifications=1`

This variable determines whether or not notification messages are logged. If you have a lot of contacts or regular service failures your log file will grow relatively quickly. Use this option to keep contact notifications from being logged.

- 0 = Don't log notifications
- 1 = Log notifications

### 16.3.36 Service Check Retry Logging Option

Format: `log_service_retries=<0/1>`

Example: `log_service_retries=1`

This variable determines whether or not service check retries are logged. Service check retries occur when a service check results in a non-OK state, but you have configured Nagios to retry the service more than once before responding to the error. Services in this situation are considered to be in "soft" states. Logging service check retries is mostly useful when attempting to debug Nagios or test out service **event handlers**.

- 0 = Don't log service check retries
- 1 = Log service check retries

### 16.3.37 Host Check Retry Logging Option

Format: `log_host_retries=<0/1>`

Example: `log_host_retries=1`

This variable determines whether or not host check retries are logged. Logging host check retries is mostly useful when attempting to debug Nagios or test out host **event handlers**.

- 0 = Don't log host check retries
- 1 = Log host check retries

### 16.3.38 Event Handler Logging Option

Format: `log_event_handlers=<0/1>`

Example: `log_event_handlers=1`

---

This variable determines whether or not service and host **event handlers** are logged. Event handlers are optional commands that can be run whenever a service or hosts changes state. Logging event handlers is most useful when debugging Nagios or first trying out your event handler scripts.

- 0 = Don't log event handlers
- 1 = Log event handlers

### 16.3.39 Initial States Logging Option

Format: `log_initial_states=<0/1>`

Example: `log_initial_states=1`

This variable determines whether or not Nagios will force all initial host and service states to be logged, even if they result in an OK state. Initial service and host states are normally only logged when there is a problem on the first check. Enabling this option is useful if you are using an application that scans the log file to determine long-term state statistics for services and hosts.

- 0 = Don't log initial states (default)
- 1 = Log initial states

### 16.3.40 External Command Logging Option

Format: `log_external_commands=<0/1>`

Example: `log_external_commands=1`

This variable determines whether or not Nagios will log **external commands** that it receives from the **External Command File**.

---

**Note**

This option does not control whether or not **passive service checks** (which are a type of external command) get logged. To enable or disable logging of passive checks, use the **Passive Check Logging Option** option.

---

- 0 = Don't log external commands
- 1 = Log external commands (default)

### 16.3.41 Passive Check Logging Option

---

Format: `log_passive_checks=<0/1>`

Example: `log_passive_checks=1`

This variable determines whether or not Nagios will log **passive host and service checks** that it receives from the **external command file**. If you are setting up a **distributed monitoring environment** or plan on handling a large number of passive checks on a regular basis, you may wish to disable this option so your log file doesn't get too large.

- 0 = Don't log passive checks
- 1 = Log passive checks (default)

### 16.3.42 Global Host Event Handler Option

Format: `global_host_event_handler=<command>`

Example: `global_host_event_handler=log-host-event-to-db`

This option allows you to specify a host event handler command that is to be run for every host state change. The global event handler is executed immediately prior to the event handler that you have optionally specified in each host definition. The command argument is the short name of a command that you define in your **Object Configuration Overview**. The maximum amount of time that this command can run is controlled by the **Event Handler Timeout** option. More information on event handlers can be found [here](#).

### 16.3.43 Global Service Event Handler Option

Format: `global_service_event_handler=<command>`

Example: `global_service_event_handler=log-service-event-to-db`

This option allows you to specify a service event handler command that is to be run for every service state change. The global event handler is executed immediately prior to the event handler that you have optionally specified in each service definition. The command argument is the short name of a command that you define in your **Object Configuration Overview**. The maximum amount of time that this command can run is controlled by the **Event Handler Timeout** option. More information on event handlers can be found [here](#).

### 16.3.44 Inter-Check Sleep Time

---

Format: `sleep_time=<seconds>`

Example: `sleep_time=1`

This is the number of seconds that Nagios will sleep before checking to see if the next service or host check in the scheduling queue should be executed. Note that Nagios will only sleep after it "catches up" with queued service checks that have fallen behind.

### 16.3.45 Service Inter-Check Delay Method

Format: `service_inter_check_delay_method=<n/d/s/x.xx>`

Example: `service_inter_check_delay_method=s`

This option allows you to control how service checks are initially 'spread out' in the event queue. Using a 'smart' delay calculation (the default) will cause Nagios to calculate an average check interval and spread initial checks of all services out over that interval, thereby helping to eliminate CPU load spikes. Using no delay is generally not recommended, as it will cause all service checks to be scheduled for execution at the same time. This means that you will generally have large CPU spikes when the services are all executed in parallel. More information on how to estimate how the inter-check delay affects service check scheduling can be found [here](#). Values are as follows:

- n = Don't use any delay - schedule all service checks to run immediately (i.e. at the same time!)
- d = Use a "dumb" delay of 1 second between service checks
- s = Use a 'smart' delay calculation to spread service checks out evenly (default)
- x.xx = Use a user-supplied inter-check delay of x.xx seconds

### 16.3.46 Maximum Service Check Spread

Format: `max_service_check_spread=<minutes>`

Example: `max_service_check_spread=30`

This option determines the maximum number of minutes from when Nagios starts that all services (that are scheduled to be regularly checked) are checked. This option will automatically adjust the [service inter-check delay method](#) (if necessary) to ensure that the initial checks of all services occur within the timeframe you specify. In general, this option will not have an affect on service check scheduling if scheduling information is being retained using the [Use Retained Scheduling Info Option](#). Default value is 30 (minutes).

---

### 16.3.47 Service Interleave Factor

Format: `service_interleave_factor=<s|x>`

Example: `service_interleave_factor=s`

This variable determines how service checks are interleaved. Interleaving allows for a more even distribution of service checks, reduced load on remote hosts, and faster overall detection of host problems. Setting this value to 1 is equivalent to not interleaving the service checks (this is how versions of Nagios previous to 0.0.5 worked). Set this value to s (smart) for automatic calculation of the interleave factor unless you have a specific reason to change it. The best way to understand how interleaving works is to watch the [status CGI](#) (detailed view) when Nagios is just starting. You should see that the service check results are spread out as they begin to appear. More information on how interleaving works can be found [here](#).

- x = A number greater than or equal to 1 that specifies the interleave factor to use. An interleave factor of 1 is equivalent to not interleaving the service checks.
- s = Use a 'smart' interleave factor calculation (default)

### 16.3.48 Maximum Concurrent Service Checks

Format: `max_concurrent_checks=<max_checks>`

Example: `max_concurrent_checks=20`

This option allows you to specify the maximum number of service checks that can be run in parallel at any given time. Specifying a value of 1 for this variable essentially prevents any service checks from being run in parallel. Specifying a value of 0 (the default) does not place any restrictions on the number of concurrent checks. You'll have to modify this value based on the system resources you have available on the machine that runs Nagios, as it directly affects the maximum load that will be imposed on the system (processor utilization, memory, etc.). More information on how to estimate how many concurrent checks you should allow can be found [here](#).

### 16.3.49 Check Result Reaper Frequency

Format: `check_result_reaper_frequency=<frequency_in_seconds>`

Example: `check_result_reaper_frequency=5`

This option allows you to control the frequency in seconds of check result "reaper" events. "Reaper" events process the results from host and service checks that have finished executing. These events constitute the core of the monitoring logic in Nagios.

---



### 16.3.50 Maximum Check Result Reaper Time

Format: `max_check_result_reaper_time=<seconds>`

Example: `max_check_result_reaper_time=30`

This option allows you to control the maximum amount of time in seconds that host and service check result "reaper" events are allowed to run. "Reaper" events process the results from host and service checks that have finished executing. If there are a lot of results to process, reaper events may take a long time to finish, which might delay timely execution of new host and service checks. This variable allows you to limit the amount of time that an individual reaper event will run before it hands control back over to Nagios for other portions of the monitoring logic.

### 16.3.51 Check Result Path

Format: `check_result_path=<path>`

Example: `check_result_path=/var/spool/nagios/checkresults`

This option determines which directory Nagios will use to temporarily store host and service check results before they are processed. This directory should not be used to store any other files, as Nagios will periodically clean this directory of old files (see the [Max Check Result File Age](#) option for more information).

---

**Note**

Make sure that only a single instance of Nagios has access to the check result path. If multiple instances of Nagios have their check result path set to the same directory, you will run into problems with check results being processed (incorrectly) by the wrong instance of Nagios!

---

### 16.3.52 Max Check Result File Age

Format: `max_check_result_file_age=<seconds>`

Example: `max_check_result_file_age=3600`

This option determines the maximum age in seconds that Nagios will consider check result files found in the [check\\_result\\_path](#) directory to be valid. Check result files that are older than this threshold will be deleted by Nagios and the check results they contain will not be processed. By using a value of zero (0) with this option, Nagios will process all check result files - even if they're older than your hardware :-).

---

### 16.3.53 Host Inter-Check Delay Method

Format: `host_inter_check_delay_method=<n/d/s/x.xx>`

Example: `host_inter_check_delay_method=s`

This option allows you to control how host checks that are scheduled to be checked on a regular basis are initially ‘spread out’ in the event queue. Using a ‘smart’ delay calculation (the default) will cause Nagios to calculate an average check interval and spread initial checks of all hosts out over that interval, thereby helping to eliminate CPU load spikes. Using no delay is generally not recommended. Using no delay will cause all host checks to be scheduled for execution at the same time. More information on how to estimate how the inter-check delay affects host check scheduling can be found [here](#). Values are as follows:

- n = Don’t use any delay - schedule all host checks to run immediately (i.e. at the same time!)
- d = Use a "dumb" delay of 1 second between host checks
- s = Use a ‘smart’ delay calculation to spread host checks out evenly (default)
- x.xx = Use a user-supplied inter-check delay of x.xx seconds

### 16.3.54 Maximum Host Check Spread

Format: `max_host_check_spread=<minutes>`

Example: `max_host_check_spread=30`

This option determines the maximum number of minutes from when Nagios starts that all hosts (that are scheduled to be regularly checked) are checked. This option will automatically adjust the [host inter-check delay method](#) (if necessary) to ensure that the initial checks of all hosts occur within the timeframe you specify. In general, this option will not have an affect on host check scheduling if scheduling information is being retained using the [use\\_retained\\_scheduling\\_info](#) option. Default value is 30 (minutes).

### 16.3.55 Timing Interval Length

Format: `interval_length=<seconds>`

Example: `interval_length=60`

This is the number of seconds per ‘unit interval’ used for timing in the scheduling queue, re-notifications, etc. "Units intervals" are used in the object configuration file to determine how often to run a service check, how often to re-notify a contact, etc.

---

**Important**

The default value for this is set to 60, which means that a "unit value" of 1 in the object configuration file will mean 60 seconds (1 minute). I have not really tested other values for this variable, so proceed at your own risk if you decide to do so!

---

### 16.3.56 Auto-Rescheduling Option

Format: `auto_reschedule_checks=<0/1>`

Example: `auto_reschedule_checks=1`

This option determines whether or not Nagios will attempt to automatically reschedule active host and service checks to 'smooth' them out over time. This can help to balance the load on the monitoring server, as it will attempt to keep the time between consecutive checks consistent, at the expense of executing checks on a more rigid schedule.

**Warning**

THIS IS AN EXPERIMENTAL FEATURE AND MAY BE REMOVED IN FUTURE VERSIONS. ENABLING THIS OPTION CAN DEGRADE PERFORMANCE - RATHER THAN INCREASE IT - IF USED IMPROPERLY!

---

### 16.3.57 Auto-Rescheduling Interval

Format: `auto_rescheduling_interval=<seconds>`

Example: `auto_rescheduling_interval=30`

This option determines how often (in seconds) Nagios will attempt to automatically reschedule checks. This option only has an effect if the **Auto-Rescheduling Option** option is enabled. Default is 30 seconds.

**Warning**

THIS IS AN EXPERIMENTAL FEATURE AND MAY BE REMOVED IN FUTURE VERSIONS. ENABLING THE AUTO-RESCHEDULING OPTION CAN DEGRADE PERFORMANCE - RATHER THAN INCREASE IT - IF USED IMPROPERLY!

---

### 16.3.58 Auto-Rescheduling Window

Format: `auto_rescheduling_window=<seconds>`

---

Example: `auto_rescheduling_window=180`

This option determines the ‘window’ of time (in seconds) that Nagios will look at when automatically rescheduling checks. Only host and service checks that occur in the next X seconds (determined by this variable) will be rescheduled. This option only has an effect if the **Auto-Rescheduling Option** is enabled. Default is 180 seconds (3 minutes).

**Warning**

THIS IS AN EXPERIMENTAL FEATURE AND MAY BE REMOVED IN FUTURE VERSIONS. ENABLING THE AUTO-RESCHEDULING OPTION CAN DEGRADE PERFORMANCE - RATHER THAN INCREASE IT - IF USED IMPROPERLY!

---

### 16.3.59 Aggressive Host Checking Option

Format: `use_aggressive_host_checking=<0/1>`

Example: `use_aggressive_host_checking=0`

Nagios tries to be smart about how and when it checks the status of hosts. In general, disabling this option will allow Nagios to make some smarter decisions and check hosts a bit faster. Enabling this option will increase the amount of time required to check hosts, but may improve reliability a bit. Unless you have problems with Nagios not recognizing that a host recovered, I would suggest not enabling this option.

- 0 = Don't use aggressive host checking (default)
- 1 = Use aggressive host checking

### 16.3.60 Translate Passive Host Checks Option

Format: `translate_passive_host_checks=<0/1>`

Example: `translate_passive_host_checks=1`

This option determines whether or not Nagios will translate DOWN/UNREACHABLE passive host check results to their ‘correct’ state from the viewpoint of the local Nagios instance. This can be very useful in distributed and failover monitoring installations. More information on passive check state translation can be found [here](#).

- 0 = Disable check translation (default)
  - 1 = Enable check translation
-

### 16.3.61 Passive Host Checks Are SOFT Option

Format: `passive_host_checks_are_soft=<0/1>`

Example: `passive_host_checks_are_soft=1`

This option determines whether or not Nagios will treat **passive host checks** as HARD states or SOFT states. By default, a passive host check result will put a host into a **HARD state type**. You can change this behavior by enabling this option.

- 0 = Passive host checks are HARD (default)
- 1 = Passive host checks are SOFT

### 16.3.62 Predictive Host Dependency Checks Option

Format: `enable_predictive_host_dependency_checks=<0/1>`

Example: `enable_predictive_host_dependency_checks=1`

This option determines whether or not Nagios will execute predictive checks of hosts that are being depended upon (as defined in **host dependencies**) for a particular host when it changes state. Predictive checks help ensure that the dependency logic is as accurate as possible. More information on how predictive checks work can be found [here](#).

- 0 = Disable predictive checks
- 1 = Enable predictive checks (default)

### 16.3.63 Predictive Service Dependency Checks Option

Format: `enable_predictive_service_dependency_checks=<0/1>`

Example: `enable_predictive_service_dependency_checks=1`

This option determines whether or not Nagios will execute predictive checks of services that are being depended upon (as defined in **service dependencies**) for a particular service when it changes state. Predictive checks help ensure that the dependency logic is as accurate as possible. More information on how predictive checks work can be found [here](#).

- 0 = Disable predictive checks
  - 1 = Enable predictive checks (default)
-

### 16.3.64 Cached Host Check Horizon

Format: `cached_host_check_horizon=<seconds>`

Example: `cached_host_check_horizon=15`

This option determines the maximum amount of time (in seconds) that the state of a previous host check is considered current. Cached host states (from host checks that were performed more recently than the time specified by this value) can improve host check performance immensely. Too high of a value for this option may result in (temporarily) inaccurate host states, while a low value may result in a performance hit for host checks. Use a value of 0 if you want to disable host check caching. More information on cached checks can be found [here](#).

### 16.3.65 Cached Service Check Horizon

Format: `cached_service_check_horizon=<seconds>`

Example: `cached_service_check_horizon=15`

This option determines the maximum amount of time (in seconds) that the state of a previous service check is considered current. Cached service states (from service checks that were performed more recently than the time specified by this value) can improve service check performance when a lot of [service dependencies](#) are used. Too high of a value for this option may result in inaccuracies in the service dependency logic. Use a value of 0 if you want to disable service check caching. More information on cached checks can be found [here](#).

### 16.3.66 Large Installation Tweaks Option

Format: `use_large_installation_tweaks=<0/1>`

Example: `use_large_installation_tweaks=0`

This option determines whether or not the Nagios daemon will take several shortcuts to improve performance. These shortcuts result in the loss of a few features, but larger installations will likely see a lot of benefit from doing so. More information on what optimizations are taken when you enable this option can be found [here](#).

- 0 = Don't use tweaks (default)
- 1 = Use tweaks

### 16.3.67 Child Process Memory Option

---

Format: `free_child_process_memory=<0/1>`

Example: `free_child_process_memory=0`

This option determines whether or not Nagios will free memory in child processes when they are fork()ed off from the main process. By default, Nagios frees memory. However, if the `use_large_installation_tweaks` option is enabled, it will not. By defining this option in your configuration file, you are able to override things to get the behavior you want.

- 0 = Don't free memory
- 1 = Free memory

### 16.3.68 Child Processes Fork Twice

Format: `child_processes_fork_twice=<0/1>`

Example: `child_processes_fork_twice=0`

This option determines whether or not Nagios will fork() child processes twice when it executes host and service checks. By default, Nagios fork()s twice. However, if the `use_large_installation_tweaks` option is enabled, it will only fork() once. By defining this option in your configuration file, you are able to override things to get the behavior you want.

- 0 = Fork() just once
- 1 = Fork() twice

### 16.3.69 Environment Macros Option

Format: `enable_environment_macros=<0/1>`

Example: `enable_environment_macros=0`

This option determines whether or not the Nagios daemon will make all standard `macros` available as environment variables to your check, notification, event handler, etc. commands. In large Nagios installations this can be problematic because it takes additional memory and (more importantly) CPU to compute the values of all macros and make them available to the environment.

- 0 = Don't make macros available as environment variables
  - 1 = Make macros available as environment variables (default)
-

### 16.3.70 Flap Detection Option

Format: `enable_flap_detection=<0/1>`

Example: `enable_flap_detection=0`

This option determines whether or not Nagios will try and detect hosts and services that are ‘flapping’. Flapping occurs when a host or service changes between states too frequently, resulting in a barrage of notifications being sent out. When Nagios detects that a host or service is flapping, it will temporarily suppress notifications for that host/service until it stops flapping.



#### Caution

Flap detection is very experimental at this point, so use this feature with caution! More information on how flap detection and handling works can be found [here](#).

---

#### Note

If you have [state retention](#) enabled, Nagios will ignore this setting when it (re)starts and use the last known setting for this option (as stored in the [state retention file](#)), unless you disable the [use\\_retained\\_program\\_state](#) option. If you want to change this option when state retention is active (and the [use\\_retained\\_program\\_state](#) is enabled), you'll have to use the appropriate [external command](#) or change it via the web interface.

---

- 0 = Don't enable flap detection (default)
- 1 = Enable flap detection

### 16.3.71 Low Service Flap Threshold

Format: `low_service_flap_threshold=<percent>`

Example: `low_service_flap_threshold=25.0`

This option is used to set the low threshold for detection of service flapping. For more information on how flap detection and handling works (and how this option affects things) read [this](#).

### 16.3.72 High Service Flap Threshold

Format: `high_service_flap_threshold=<percent>`

---



Example: `high_service_flap_threshold=50.0`

This option is used to set the high threshold for detection of service flapping. For more information on how flap detection and handling works (and how this option affects things) read [this](#).

### 16.3.73 Low Host Flap Threshold

Format: `low_host_flap_threshold=<percent>`

Example: `low_host_flap_threshold=25.0`

This option is used to set the low threshold for detection of host flapping. For more information on how flap detection and handling works (and how this option affects things) read [this](#).

### 16.3.74 High Host Flap Threshold

Format: `high_host_flap_threshold=<percent>`

Example: `high_host_flap_threshold=50.0`

This option is used to set the high threshold for detection of host flapping. For more information on how flap detection and handling works (and how this option affects things) read [this](#).

### 16.3.75 Soft State Dependencies Option

Format: `soft_state_dependencies=<0/1>`

Example: `soft_state_dependencies=0`

This option determines whether or not Nagios will use soft state information when checking [host and service dependencies](#). Normally Nagios will only use the latest hard host or service state when checking dependencies. If you want it to use the latest state (regardless of whether its a soft or hard [state type](#)), enable this option.

- 0 = Don't use soft state dependencies (default)
  - 1 = Use soft state dependencies
-

### 16.3.76 Service Check Timeout

Format: `service_check_timeout=<seconds>`

Example: `service_check_timeout=60`

This is the maximum number of seconds that Nagios will allow service checks to run. If checks exceed this limit, they are killed and a CRITICAL state is returned. A timeout error will also be logged.

There is often widespread confusion as to what this option really does. It is meant to be used as a last ditch mechanism to kill off plugins which are misbehaving and not exiting in a timely manner. It should be set to something high (like 60 seconds or more), so that each service check normally finishes executing within this time limit. If a service check runs longer than this limit, Nagios will kill it off thinking it is a runaway processes.

### 16.3.77 Host Check Timeout

Format: `host_check_timeout=<seconds>`

Example: `host_check_timeout=60`

This is the maximum number of seconds that Nagios will allow host checks to run. If checks exceed this limit, they are killed and a CRITICAL state is returned and the host will be assumed to be DOWN. A timeout error will also be logged.

There is often widespread confusion as to what this option really does. It is meant to be used as a last ditch mechanism to kill off plugins which are misbehaving and not exiting in a timely manner. It should be set to something high (like 60 seconds or more), so that each host check normally finishes executing within this time limit. If a host check runs longer than this limit, Nagios will kill it off thinking it is a runaway processes.

### 16.3.78 Event Handler Timeout

Format: `event_handler_timeout=<seconds>`

Example: `event_handler_timeout=60`

This is the maximum number of seconds that Nagios will allow **event handlers** to be run. If an event handler exceeds this time limit it will be killed and a warning will be logged.

There is often widespread confusion as to what this option really does. It is meant to be used as a last ditch mechanism to kill off commands which are misbehaving and not exiting in a timely manner. It should be set to something high (like 60 seconds or more), so that each event handler command normally finishes executing within this time limit. If an event handler runs longer than this limit, Nagios will kill it off thinking it is a runaway processes.

---

### 16.3.79 Notification Timeout

Format: `notification_timeout=<seconds>`

Example: `notification_timeout=60`

This is the maximum number of seconds that Nagios will allow notification commands to be run. If a notification command exceeds this time limit it will be killed and a warning will be logged.

There is often widespread confusion as to what this option really does. It is meant to be used as a last ditch mechanism to kill off commands which are misbehaving and not exiting in a timely manner. It should be set to something high (like 60 seconds or more), so that each notification command finishes executing within this time limit. If a notification command runs longer than this limit, Nagios will kill it off thinking it is a runaway processes.

### 16.3.80 Obsessive Compulsive Service Processor Timeout

Format: `ocsp_timeout=<seconds>`

Example: `ocsp_timeout=5`

This is the maximum number of seconds that Nagios will allow an **obsessive compulsive service processor command** to be run. If a command exceeds this time limit it will be killed and a warning will be logged.

### 16.3.81 Obsessive Compulsive Host Processor Timeout

Format: `ochp_timeout=<seconds>`

Example: `ochp_timeout=5`

This is the maximum number of seconds that Nagios will allow an **Obsessive Compulsive Host Processor Command** to be run. If a command exceeds this time limit it will be killed and a warning will be logged.

### 16.3.82 Performance Data Processor Command Timeout

Format: `perfdata_timeout=<seconds>`

---

Example:            `perfdata_timeout=5`

This is the maximum number of seconds that Nagios will allow a [host performance data processor command](#) or [service performance data processor command](#) to be run. If a command exceeds this time limit it will be killed and a warning will be logged.

### 16.3.83 Obsess Over Services Option

Format:            `obsess_over_services=<0/1>`

Example:            `obsess_over_services=1`

This value determines whether or not Nagios will ‘obsess’ over service checks results and run the [obsessive compulsive service processor command](#) you define. I know - funny name, but it was all I could think of. This option is useful for performing [distributed monitoring](#). If you’re not doing distributed monitoring, don’t enable this option.

- 0 = Don’t obsess over services (default)
- 1 = Obsess over services

### 16.3.84 Obsessive Compulsive Service Processor Command

Format:            `ocsp_command=<command>`

Example:            `ocsp_command=obsessive_service_handler`

This option allows you to specify a command to be run after every service check, which can be useful in [distributed monitoring](#). This command is executed after any [event handler](#) or [notification](#) commands. The command argument is the short name of a [command definition](#) that you define in your object configuration file. The maximum amount of time that this command can run is controlled by the [Obsessive Compulsive Service Processor Timeout](#) option. More information on distributed monitoring can be found [here](#). This command is only executed if the [Obsess Over Services Option](#) option is enabled globally and if the `obsess_over_service` directive in the [service definition](#) is enabled.

### 16.3.85 Obsess Over Hosts Option

Format:            `obsess_over_hosts=<0/1>`

---

Example: `obsess_over_hosts=1`

This value determines whether or not Nagios will ‘obsess’ over host checks results and run the **obsessive compulsive host processor command** you define. I know - funny name, but it was all I could think of. This option is useful for performing **distributed monitoring**. If you’re not doing distributed monitoring, don’t enable this option.

- 0 = Don’t obsess over hosts (default)
- 1 = Obsess over hosts

### 16.3.86 Obsessive Compulsive Host Processor Command

Format: `ochp_command=<command>`

Example: `ochp_command=obsessive_host_handler`

This option allows you to specify a command to be run after every host check, which can be useful in **distributed monitoring**. This command is executed after any **event handler** or **notification** commands. The command argument is the short name of a **command definition** that you define in your object configuration file. The maximum amount of time that this command can run is controlled by the **Obsessive Compulsive Host Processor Timeout** option. More information on distributed monitoring can be found [here](#). This command is only executed if the **Obsess Over Hosts Option** option is enabled globally and if the `obsess_over_host` directive in the **host definition** is enabled.

### 16.3.87 Performance Data Processing Option

Format: `process_performance_data=<0/1>`

Example: `process_performance_data=1`

This value determines whether or not Nagios will process host and service check **performance data**.

- 0 = Don’t process performance data (default)
- 1 = Process performance data

### 16.3.88 Host Performance Data Processing Command

Format: `host_perfdata_command=<command>`

---

Example: `host_perfdata_command=process-host-perfdata`

This option allows you to specify a command to be run after every host check to process host **performance data** that may be returned from the check. The command argument is the short name of a **command definition** that you define in your object configuration file. This command is only executed if the **Performance Data Processing Option** option is enabled globally and if the `process_perf_data` directive in the **host definition** is enabled.

### 16.3.89 Service Performance Data Processing Command

Format: `service_perfdata_command=<command>`

Example: `service_perfdata_command=process-service-perfdata`

This option allows you to specify a command to be run after every service check to process service **performance data** that may be returned from the check. The command argument is the short name of a **command definition** that you define in your object configuration file. This command is only executed if the **process\_performance\_data** option is enabled globally and if the `process_perf_data` directive in the **service definition** is enabled.

### 16.3.90 Host Performance Data File

Format: `host_perfdata_file=<file_name>`

Example: `host_perfdata_file=/usr/local/nagios/var/host-perfdata.dat`

This option allows you to specify a file to which host **performance data** will be written after every host check. Data will be written to the performance file as specified by the **Host Performance Data File Template** option. Performance data is only written to this file if the **Performance Data Processing Option** option is enabled globally and if the `process_perf_data` directive in the **host definition** is enabled.

### 16.3.91 Service Performance Data File

Format: `service_perfdata_file=<file_name>`

Example: `service_perfdata_file=/usr/local/nagios/var/service-perfdata.dat`

This option allows you to specify a file to which service **performance data** will be written after every service check. Data will

---

be written to the performance file as specified by the **Service Performance Data File Template** option. Performance data is only written to this file if the **Performance Data Processing Option** option is enabled globally and if the `process_perf_data` directive in the **service definition** is enabled.

### 16.3.92 Host Performance Data File Template

Format: `host_perfdata_file_template=<template>`

Example: `host_perfdata_file_template=[HOSTPERFDATA]\t$TIMET$\t$HOSTNAME$\t$HOSTEXECUTIONTIME$\t$HOSTOUTPUT$\t$HOSTPERFDATA$`

This option determines what (and how) data is written to the **host performance data file**. The template may contain **macros**, special characters (`\t` for tab, `\r` for carriage return, `\n` for newline) and plain text. A newline is automatically added after each write to the performance data file.

### 16.3.93 Service Performance Data File Template

Format: `service_perfdata_file_template=<template>`

Example: `service_perfdata_file_template=[SERVICEPERFDATA]\t$TIMET$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICEEXECUTIONTIME$\t$SERVICELATENCY$\t$SERVICEOUTPUT$\t$SERVICEPERFDATA$`

This option determines what (and how) data is written to the **service performance data file**. The template may contain **macros**, special characters (`\t` for tab, `\r` for carriage return, `\n` for newline) and plain text. A newline is automatically added after each write to the performance data file.

### 16.3.94 Host Performance Data File Mode

Format: `host_perfdata_file_mode=<mode>`

Example: `host_perfdata_file_mode=a`

This option determines how the **host performance data file** is opened. Unless the file is a named pipe you'll probably want to use the default mode of append.

- a = Open file in append mode (default)
- w = Open file in write mode
- p = Open in non-blocking read/write mode (useful when writing to pipes)

### 16.3.95 Service Performance Data File Mode

Format: `service_perfdata_file_mode=<mode>`

Example: `service_perfdata_file_mode=a`

This option determines how the **service performance data file** is opened. Unless the file is a named pipe you'll probably want to use the default mode of append.

- a = Open file in append mode (default)
- w = Open file in write mode
- p = Open in non-blocking read/write mode (useful when writing to pipes)

### 16.3.96 Host Performance Data File Processing Interval

Format: `host_perfdata_file_processing_interval=<seconds>`

Example: `host_perfdata_file_processing_interval=0`

This option allows you to specify the interval (in seconds) at which the **host performance data file** is processed using the **host performance data file processing command**. A value of 0 indicates that the performance data file should not be processed at regular intervals.

### 16.3.97 Service Performance Data File Processing Interval

Format: `service_perfdata_file_processing_interval=<seconds>`

Example: `service_perfdata_file_processing_interval=0`

This option allows you to specify the interval (in seconds) at which the **service performance data file** is processed using the **service performance data file processing command**. A value of 0 indicates that the performance data file should not be processed at regular intervals.

### 16.3.98 Host Performance Data File Processing Command

---



Format: `host_perfdata_file_processing_command=<command>`

Example: `host_perfdata_file_processing_command=process-host-perfdata-file`

This option allows you to specify the command that should be executed to process the **host performance data file**. The command argument is the short name of a **command definition** that you define in your object configuration file. The interval at which this command is executed is determined by the **host\_perfdata\_file\_processing\_interval** directive.

### 16.3.99 Service Performance Data File Processing Command

Format: `service_perfdata_file_processing_command=<command>`

Example: `service_perfdata_file_processing_command=process-service-perfdata-file`

This option allows you to specify the command that should be executed to process the **service performance data file**. The command argument is the short name of a **command definition** that you define in your object configuration file. The interval at which this command is executed is determined by the **Service Performance Data File Processing Interval** directive.

### 16.3.100 Orphaned Service Check Option

Format: `check_for_orphaned_services=<0/1>`

Example: `check_for_orphaned_services=1`

This option allows you to enable or disable checks for orphaned service checks. Orphaned service checks are checks which have been executed and have been removed from the event queue, but have not had any results reported in a long time.

Since no results have come back in for the service, it is not rescheduled in the event queue. This can cause service checks to stop being executed. Normally it is very rare for this to happen - it might happen if an external user or process killed off the process that was being used to execute a service check.

If this option is enabled and Nagios finds that results for a particular service check have not come back, it will log an error message and reschedule the service check. If you start seeing service checks that never seem to get rescheduled, enable this option and see if you notice any log messages about orphaned services.

- 0 = Don't check for orphaned service checks
- 1 = Check for orphaned service checks (default)

### 16.3.101 Orphaned Host Check Option

---

Format: `check_for_orphaned_hosts=<0/1>`

Example: `check_for_orphaned_hosts=1`

This option allows you to enable or disable checks for orphaned host checks. Orphaned host checks are checks which have been executed and have been removed from the event queue, but have not had any results reported in a long time.

Since no results have come back in for the host, it is not rescheduled in the event queue. This can cause host checks to stop being executed. Normally it is very rare for this to happen - it might happen if an external user or process killed off the process that was being used to execute a host check.

If this option is enabled and Nagios finds that results for a particular host check have not come back, it will log an error message and reschedule the host check. If you start seeing host checks that never seem to get rescheduled, enable this option and see if you notice any log messages about orphaned hosts.

- 0 = Don't check for orphaned host checks
- 1 = Check for orphaned host checks (default)

### 16.3.102 Service Freshness Checking Option

Format: `check_service_freshness=<0/1>`

Example: `check_service_freshness=0`

This option determines whether or not Nagios will periodically check the 'freshness' of service checks. Enabling this option is useful for helping to ensure that **passive service checks** are received in a timely manner. More information on freshness checking can be found [here](#).

- 0 = Don't check service freshness
- 1 = Check service freshness (default)

### 16.3.103 Service Freshness Check Interval

Format: `service_freshness_check_interval=<seconds>`

Example: `service_freshness_check_interval=60`

This setting determines how often (in seconds) Nagios will periodically check the 'freshness' of service check results. If you have disabled service freshness checking (with the **check\_service\_freshness** option), this option has no effect. More information on freshness checking can be found [here](#).

---

### 16.3.104 Host Freshness Checking Option

Format: `check_host_freshness=<0/1>`

Example: `check_host_freshness=0`

This option determines whether or not Nagios will periodically check the ‘freshness’ of host checks. Enabling this option is useful for helping to ensure that **passive host checks** are received in a timely manner. More information on freshness checking can be found [here](#).

- 0 = Don’t check host freshness
- 1 = Check host freshness (default)

### 16.3.105 Host Freshness Check Interval

Format: `host_freshness_check_interval=<seconds>`

Example: `host_freshness_check_interval=60`

This setting determines how often (in seconds) Nagios will periodically check the ‘freshness’ of host check results. If you have disabled host freshness checking (with the **check\_host\_freshness** option), this option has no effect. More information on freshness checking can be found [here](#).

### 16.3.106 Additional Freshness Threshold Latency Option

Format: `additional_freshness_latency=<#>`

Example: `additional_freshness_latency=15`

This option determines the number of seconds Nagios will add to any host or services freshness threshold it automatically calculates (e.g. those not specified explicitly by the user). More information on freshness checking can be found [here](#).

### 16.3.107 Embedded Perl Interpreter Option

Format: `enable_embedded_perl=<0/1>`

---

Example: `enable_embedded_perl=1`

This setting determines whether or not the embedded Perl interpreter is enabled on a program-wide basis. Nagios must be compiled with support for embedded Perl for this option to have an effect. More information on the embedded Perl interpreter can be found [here](#).

### 16.3.108 Embedded Perl Implicit Use Option

Format: `use_embedded_perl_implicitly=<0/1>`

Example: `use_embedded_perl_implicitly=1`

This setting determines whether or not the embedded Perl interpreter should be used for Perl plugins/scripts that do not explicitly enable/disable it. Nagios must be compiled with support for embedded Perl for this option to have an effect. More information on the embedded Perl interpreter and the effect of this setting can be found [here](#).

### 16.3.109 Date Format

Format: `date_format=<option>`

Example: `date_format=us`

This option allows you to specify what kind of date/time format Nagios should use in the web interface and date/time [macros](#). Possible options (along with example output) include:

| Option         | Output Format       | Sample Output       |
|----------------|---------------------|---------------------|
| us             | MM/DD/YYYY HH:MM:SS | 06/30/2002 03:15:00 |
| euro           | DD/MM/YYYY HH:MM:SS | 30/06/2002 03:15:00 |
| iso8601        | YYYY-MM-DD HH:MM:SS | 2002-06-30 03:15:00 |
| strict-iso8601 | YYYY-MM-DDTHH:MM:SS | 2002-06-30T03:15:00 |

### 16.3.110 Timezone Option

Format: `use_timezone=<tz>`

Example: `use_timezone=US/Mountain`

This option allows you to override the default timezone that this instance of Nagios runs in. Useful if you have multiple instances of Nagios that need to run from the same server, but have different local times associated with them. If not specified, Nagios will use the system configured timezone.

---

**Note**

If you use this option to specify a custom timezone, you will also need to alter the Apache configuration directives for the CGIs to specify the timezone you want. Example:

---

```
<Directory "/usr/local/nagios/sbin/">
 SetEnv TZ "US/Mountain"
 ...
</Directory>
```

### 16.3.111 Illegal Object Name Characters

Format: `illegal_object_name_chars=<chars...>`

Example: `illegal_object_name_chars='~!$%^&*"'<>?,()=`

This option allows you to specify illegal characters that cannot be used in host names, service descriptions, or names of other object types. Nagios will allow you to use most characters in object definitions, but I recommend not using the characters shown in the example above. Doing may give you problems in the web interface, notification commands, etc.

### 16.3.112 Illegal Macro Output Characters

Format: `illegal_macro_output_chars=<chars...>`

Example: `illegal_macro_output_chars='~$^&"'<>`

This option allows you to specify illegal characters that should be stripped from **macros** before being used in notifications, event handlers, and other commands. This DOES NOT affect macros used in service or host check commands. You can choose to not strip out the characters shown in the example above, but I recommend you do not do this. Some of these characters are interpreted by the shell (i.e. the backtick) and can lead to security problems. The following macros are stripped of the characters you specify:

- \$HOSTOUTPUT\$
  - \$HOSTPERFDATA\$
  - \$HOSTACKAUTHOR\$
  - \$HOSTACKCOMMENT\$
  - \$SERVICEOUTPUT\$
  - \$SERVICEPERFDATA\$
-

- \$SERVICEACKAUTHOR\$
- \$SERVICEACKCOMMENT\$

### 16.3.113 Regular Expression Matching Option

Format: `use_regexp_matching=<0/1>`

Example: `use_regexp_matching=0`

This option determines whether or not various directives in your [Object Configuration Overview](#) will be processed as regular expressions. More information on how this works can be found [here](#).

- 0 = Don't use regular expression matching (default)
- 1 = Use regular expression matching

### 16.3.114 True Regular Expression Matching Option

Format: `use_true_regexp_matching=<0/1>`

Example: `use_true_regexp_matching=0`

If you've enabled regular expression matching of various object directives using the [Regular Expression Matching Option](#) option, this option will determine when object directives are treated as regular expressions. If this option is disabled (the default), directives will only be treated as regular expressions if they contain \*, ?, +, or \.. If this option is enabled, all appropriate directives will be treated as regular expression - be careful when enabling this! More information on how this works can be found [here](#).

- 0 = Don't use true regular expression matching (default)
- 1 = Use true regular expression matching

### 16.3.115 Administrator Email Address

Format: `admin_email=<email_address>`

Example: `admin_email=root@localhost.localdomain`

This is the email address for the administrator of the local machine (i.e. the one that Nagios is running on). This value can be

used in notification commands by using the `$ADMINEMAIL$` [macro](#).

### 16.3.116 Administrator Pager

Format: `admin_pager=<pager_number_or_pager_email_gateway>`

Example: `admin_pager=pageroot@localhost.localdomain`

This is the pager number (or pager email gateway) for the administrator of the local machine (i.e. the one that Nagios is running on). The pager number/address can be used in notification commands by using the `$ADMINPAGER$` [macro](#).

### 16.3.117 Event Broker Options

Format: `event_broker_options=<#>`

Example: `event_broker_options=-1`

This option controls what (if any) data gets sent to the event broker and, in turn, to any loaded event broker modules. This is an advanced option. When in doubt, either broker nothing (if not using event broker modules) or broker everything (if using event broker modules). Possible values are shown below.

- 0 = Broker nothing
- -1 = Broker everything
- # = See `BROKER_*` definitions in source code (`include/broker.h`) for other values that can be OR'ed together

### 16.3.118 Event Broker Modules

Format: `broker_module=<modulepath> [moduleargs]`

Example: `broker_module=/usr/local/nagios/bin/ndomod.o  
cfg_file=/usr/local/nagios/etc/ndomod.cfg`

This directive is used to specify an event broker module that should be loaded by Nagios at startup. Use multiple directives if you want to load more than one module. Arguments that should be passed to the module at startup are separated from the module path by a space.

---

**Warning**

Do NOT overwrite modules while they are being used by Nagios or Nagios will crash in a fiery display of SEGFAULT glory. This is a bug/limitation either in `dlopen()`, the kernel, and/or the filesystem. And maybe Nagios...

---

The correct/safe way of updating a module is by using one of these methods:

- Shutdown Nagios, replace the module file, restart Nagios
- While Nagios is running... delete the original module file, move the new module file into place, restart Nagios

### 16.3.119 Debug File

Format: `debug_file=<file_name>`

Example: `debug_file=/usr/local/nagios/var/nagios.debug`

This option determines where Nagios should write debugging information. What (if any) information is written is determined by the **Debug Level** and **Debug Verbosity** options. You can have Nagios automatically rotate the debug file when it reaches a certain size by using the **Maximum Debug File Size** option.

### 16.3.120 Debug Level

Format: `debug_level=<#>`

Example: `debug_level=24`

This option determines what type of information Nagios should write to the **Debug File**. This value is a logical OR of the values below.

- -1 = Log everything
  - 0 = Log nothing (default)
  - 1 = Function enter/exit information
  - 2 = Config information
  - 4 = Process information
  - 8 = Scheduled event information
  - 16 = Host/service check information
  - 32 = Notification information
  - 64 = Event broker information
-



### 16.3.121 Debug Verbosity

Format: `debug_verbosity=<#>`

Example: `debug_verbosity=1`

This option determines how much debugging information Nagios should write to the **Debug File**.

- 0 = Basic information
- 1 = More detailed information (default)
- 2 = Highly detailed information

### 16.3.122 Maximum Debug File Size

Format: `max_debug_file_size=<#>`

Example: `max_debug_file_size=1000000`

This option determines the maximum size (in bytes) of the **debug file**. If the file grows larger than this size, it will be renamed with a .old extension. If a file already exists with a .old extension it will automatically be deleted. This helps ensure your disk space usage doesn't get out of control when debugging Nagios.

---

## Chapter 17

# Object Configuration Overview

### 17.1 What Are Objects?

Objects are all the elements that are involved in the monitoring and notification logic. Types of objects include:

- Services
- Service Groups
- Hosts
- Host Groups
- Contacts
- Contact Groups
- Commands
- Time Periods
- Notification Escalations
- Notification and Execution Dependencies

More information on what objects are and how they relate to each other can be found below.

### 17.2 Where Are Objects Defined?

Objects can be defined in one or more configuration files and/or directories that you specify using the `cfg_file` and/or `cfg_dir` directives in the main configuration file.

---

**Tip**

When you follow the [Quickstart installation guide](#), several sample object configuration files are placed in `/usr/local/nagios/etc/objects/`. You can use these sample files to see how object inheritance works and learn how to define your own object definitions.

---

## 17.3 How Are Objects Defined?

Objects are defined in a flexible template format, which can make it much easier to manage your Nagios configuration in the long term. Basic information on how to define objects in your configuration files can be found [here](#).

Once you get familiar with the basics of how to define objects, you should read up on [object inheritance](#), as it will make your configuration more robust for the future. Seasoned users can exploit some advanced features of object definitions as described in the documentation on [object tricks](#).

## 17.4 Objects Explained

Some of the main object types are explained in greater detail below...

### 17.4.1 Hosts

**Hosts** are one of the central objects in the monitoring logic. Important attributes of hosts are as follows:

- Hosts are usually physical devices on your network (servers, workstations, routers, switches, printers, etc).
- Hosts have an address of some kind (e.g. an IP or MAC address).
- Hosts have one or more services associated with them.
- Hosts can have parent/child relationships with other hosts, often representing real-world network connections, which is used in the [network reachability](#) logic.

### 17.4.2 Host Groups

**Host Groups** are groups of one or more hosts. Host groups can make it easier to (1) view the status of related hosts in the Nagios web interface and (2) simplify your configuration through the use of [object tricks](#).

### 17.4.3 Services

**Services** are one of the central objects in the monitoring logic. Services are associated with hosts and can be:

- Attributes of a host (CPU load, disk usage, uptime, etc.)
- Services provided by the host (HTTP, POP3, FTP, SSH, etc.)
- Other things associated with the host (DNS records, etc.)

### 17.4.4 Service Groups

**Service Groups** are groups of one or more services. Service groups can make it easier to (1) view the status of related services in the Nagios web interface and (2) simplify your configuration through the use of [object tricks](#).

### 17.4.5 Contacts

**Contacts** are people involved in the notification process:

- Contacts have one or more notification methods (cellphone, pager, email, instant messaging, etc.)
  - Contacts receive notifications for hosts and service they are responsible for
-

### 17.4.6 Contact Groups

**Contact Groups** are groups of one or more contacts. Contact groups can make it easier to define all the people who get notified when certain host or service problems occur.

### 17.4.7 Timeperiods

**Timeperiods** are used to control:

- When hosts and services can be monitored
- When contacts can receive notifications

Information on how timeperiods work can be found [here](#).

### 17.4.8 Commands

**Commands** are used to tell Nagios what programs, scripts, etc. it should execute to perform:

- Host and service checks
  - Notifications
  - Event handlers
  - and more...
-

## Chapter 18

# Object Definitions

### 18.1 Introduction

One of the features of Nagios' object configuration format is that you can create object definitions that inherit properties from other object definitions. An explanation of how object inheritance works can be found [here](#). I strongly suggest that you familiarize yourself with object inheritance once you read over the documentation presented below, as it will make the job of creating and maintaining object definitions much easier than it otherwise would be. Also, read up on the [object tricks](#) that offer shortcuts for otherwise tedious configuration tasks.

---

**Note**

When creating and/or editing configuration files, keep the following in mind:

1. Lines that start with a '#' character are taken to be comments and are not processed
  2. Directive names are case-sensitive
- 

### 18.2 Retention Notes

It is important to point out that several directives in host, service, and contact definitions may not be picked up by Nagios when you change them in your configuration files. Object directives that can exhibit this behavior are marked with an asterisk (\*). The reason for this behavior is due to the fact that Nagios chooses to honor values stored in the [state retention file](#) over values found in the config files, assuming you have [state retention](#) enabled on a program-wide basis and the value of the directive is changed during runtime with an [external command](#).

One way to get around this problem is to disable the retention of non-status information using the `retain_nonstatus_information` directive in the host, service, and contact definitions. Disabling this directive will cause Nagios to take the initial values for these directives from your config files, rather than from the state retention file when it (re)starts.

### 18.3 Sample Configuration Files

---

**Note**

Sample object configuration files are installed in the `/usr/local/nagios/etc/` directory when you follow the [quickstart installation guide](#).

---

## 18.4 Object Types

[Host definitions](#)
[Host group definitions](#)
[Service definitions](#)
[Service group definitions](#)
[Contact definitions](#)
[Contact group definitions](#)
[Time period definitions](#)
[Command definitions](#)
[Service dependency definitions](#)
[Service escalation definitions](#)
[Host dependency definitions](#)
[Host escalation definitions](#)
[Extended host information definitions](#)
[Extended service information definitions](#)

### 18.4.1 Host Definition

#### 18.4.1.1 Description

A host definition is used to define a physical server, workstation, device, etc. that resides on your network.

#### 18.4.1.2 Definition Format

##### Note

Directives in red are required, while those in black are optional.

|                              |                        |
|------------------------------|------------------------|
| define host{                 |                        |
| host_name                    | <i>host_name</i>       |
| alias                        | <i>alias</i>           |
| display_name                 | <i>display_name</i>    |
| address                      | <i>address</i>         |
| parents                      | <i>host_names</i>      |
| hostgroups                   | <i>hostgroup_names</i> |
| check_command                | <i>command_name</i>    |
| initial_state                | [o,d,u]                |
| max_check_attempts           | #                      |
| check_interval               | #                      |
| retry_interval               | #                      |
| active_checks_enabled        | [0/1]                  |
| passive_checks_enabled       | [0/1]                  |
| check_period                 | <i>timeperiod_name</i> |
| obsess_over_host             | [0/1]                  |
| check_freshness              | [0/1]                  |
| freshness_threshold          | #                      |
| event_handler                | <i>command_name</i>    |
| event_handler_enabled        | [0/1]                  |
| low_flap_threshold           | #                      |
| high_flap_threshold          | #                      |
| flap_detection_enabled       | [0/1]                  |
| flap_detection_options       | [o,d,u]                |
| process_perf_data            | [0/1]                  |
| retain_status_information    | [0/1]                  |
| retain_nonstatus_information | [0/1]                  |
| contacts                     | <i>contacts</i>        |
| contact_groups               | <i>contact_groups</i>  |
| notification_interval        | #                      |
| first_notification_delay     | #                      |
| notification_period          | <i>timeperiod_name</i> |
| notification_options         | [d,u,r,f,s]            |
| notifications_enabled        | [0/1]                  |
| stalking_options             | [o,d,u]                |

|                 |                                |
|-----------------|--------------------------------|
| notes           | <i>note_string</i>             |
| notes_url       | <i>url</i>                     |
| action_url      | <i>url</i>                     |
| icon_image      | <i>image_file</i>              |
| icon_image_alt  | <i>alt_string</i>              |
| vrml_image      | <i>image_file</i>              |
| statusmap_image | <i>image_file</i>              |
| 2d_coords       | <i>x_coord,y_coord</i>         |
| 3d_coords       | <i>x_coord,y_coord,z_coord</i> |
| }               |                                |

#### 18.4.1.3 Example Definition

```
define host{
 host_name bogus-router
 alias Bogus Router #1
 address 192.168.1.254
 parents server-backbone
 check_command check-host-alive
 check_interval 5
 retry_interval 1
 max_check_attempts 5
 check_period 24x7
 process_perf_data 0
 retain_nonstatus_information 0
 contact_groups router-admins
 notification_interval 30
 notification_period 24x7
 notification_options d,u,r
}
```

#### 18.4.1.4 Directive Descriptions

**host\_name** This directive is used to define a short name used to identify the host. It is used in host group and service definitions to reference this particular host. Hosts can have multiple services (which are monitored) associated with them. When used properly, the \$HOSTNAME\$ **macro** will contain this short name.

**alias** This directive is used to define a longer name or description used to identify the host. It is provided in order to allow you to more easily identify a particular host. When used properly, the \$HOSTALIAS\$ **macro** will contain this alias/description.

**address** This directive is used to define the address of the host. Normally, this is an IP address, although it could really be anything you want (so long as it can be used to check the status of the host). You can use a FQDN to identify the host instead of an IP address, but if DNS services are not available this could cause problems. When used properly, the \$HOSTADDRESS\$ **macro** will contain this address.

##### Note

If you do not specify an address directive in a host definition, the name of the host will be used as its address.



##### Caution

A word of caution about doing this, however - if DNS fails, most of your service checks will fail because the plugins will be unable to resolve the host name.

**display\_name** This directive is used to define an alternate name that should be displayed in the web interface for this host. If not specified, this defaults to the value you specify for the *host\_name* directive.

---

**Note**

The current CGIs do not use this option, although future versions of the web interface will.

---

**parents** This directive is used to define a comma-delimited list of short names of the "parent" hosts for this particular host. Parent hosts are typically routers, switches, firewalls, etc. that lie between the monitoring host and a remote hosts. A router, switch, etc. which is closest to the remote host is considered to be that host's "parent". Read the "Determining Status and Reachability of Network Hosts" document located [here](#) for more information. If this host is on the same network segment as the host doing the monitoring (without any intermediate routers, etc.) the host is considered to be on the local network and will not have a parent host. Leave this value blank if the host does not have a parent host (i.e. it is on the same segment as the Nagios host). The order in which you specify parent hosts has no effect on how things are monitored.

**hostgroups** This directive is used to identify the *short name(s)* of the [hostgroup\(s\)](#) that the host belongs to. Multiple hostgroups should be separated by commas. This directive may be used as an alternative to (or in addition to) using the *members* directive in [hostgroup](#) definitions.

**check\_command** This directive is used to specify the *short name* of the [command](#) that should be used to check if the host is up or down. Typically, this command would try and ping the host to see if it is "alive". The command must return a status of OK (0) or Nagios will assume the host is down. If you leave this argument blank, the host will *not* be actively checked. Thus, Nagios will likely always assume the host is up (it may show up as being in a "PENDING" state in the web interface). This is useful if you are monitoring printers or other devices that are frequently turned off. The maximum amount of time that the notification command can run is controlled by the [host\\_check\\_timeout](#) option.

**initial\_state** By default Nagios will assume that all hosts are in UP states when in starts. You can override the initial state for a host by using this directive. Valid options are: **o** = UP, **d** = DOWN, and **u** = UNREACHABLE.

**max\_check\_attempts** This directive is used to define the number of times that Nagios will retry the host check command if it returns any state other than an OK state. Setting this value to 1 will cause Nagios to generate an alert without retrying the host check again.

---

**Note**

If you do not want to check the status of the host, you must still set this to a minimum value of 1. To bypass the host check, just leave the `check_command` option blank.

---

**check\_interval** This directive is used to define the number of 'time units' between regularly scheduled checks of the host. Unless you've changed the [interval\\_length](#) directive from the default value of 60, this number will mean minutes. More information on this value can be found in the [check scheduling](#) documentation.

**retry\_interval** This directive is used to define the number of 'time units' to wait before scheduling a re-check of the hosts. Hosts are rescheduled at the retry interval when they have changed to a non-UP state. Once the host has been retried **max\_check\_attempts** times without a change in its status, it will revert to being scheduled at its 'normal' rate as defined by the **check\_interval** value. Unless you've changed the [interval\\_length](#) directive from the default value of 60, this number will mean minutes. More information on this value can be found in the [check scheduling](#) documentation.

**active\_checks\_enabled\*** This directive is used to determine whether or not active checks (either regularly scheduled or on-demand) of this host are enabled. Values: 0 = disable active host checks, 1 = enable active host checks.

**passive\_checks\_enabled \*** This directive is used to determine whether or not passive checks are enabled for this host. Values: 0 = disable passive host checks, 1 = enable passive host checks.

**check\_period** This directive is used to specify the short name of the [time period](#) during which active checks of this host can be made.

**obsess\_over\_host \*** This directive determines whether or not checks for the host will be 'obsessed' over using the [ochp\\_command](#).

**check\_freshness \*** This directive is used to determine whether or not [freshness checks](#) are enabled for this host. Values: 0 = disable freshness checks, 1 = enable freshness checks.

---



**freshness\_threshold** This directive is used to specify the freshness threshold (in seconds) for this host. If you set this directive to a value of 0, Nagios will determine a freshness threshold to use automatically.

**event\_handler** This directive is used to specify the *short name* of the **command** that should be run whenever a change in the state of the host is detected (i.e. whenever it goes down or recovers). Read the documentation on **event handlers** for a more detailed explanation of how to write scripts for handling events. The maximum amount of time that the event handler command can run is controlled by the **event\_handler\_timeout** option.

**event\_handler\_enabled** \* This directive is used to determine whether or not the event handler for this host is enabled. Values: 0 = disable host event handler, 1 = enable host event handler.

**low\_flap\_threshold** This directive is used to specify the low state change threshold used in flap detection for this host. More information on flap detection can be found [here](#). If you set this directive to a value of 0, the program-wide value specified by the **low\_host\_flap\_threshold** directive will be used.

**high\_flap\_threshold** This directive is used to specify the high state change threshold used in flap detection for this host. More information on flap detection can be found [here](#). If you set this directive to a value of 0, the program-wide value specified by the **high\_host\_flap\_threshold** directive will be used.

**flap\_detection\_enabled** \* This directive is used to determine whether or not flap detection is enabled for this host. More information on flap detection can be found [here](#). Values: 0 = disable host flap detection, 1 = enable host flap detection.

**flap\_detection\_options** This directive is used to determine what host states the **flap detection logic** will use for this host. Valid options are a combination of one or more of the following: **o** = UP states, **d** = DOWN states, **u** = UNREACHABLE states.

**process\_perf\_data** \* This directive is used to determine whether or not the processing of performance data is enabled for this host. Values: 0 = disable performance data processing, 1 = enable performance data processing.

**retain\_status\_information** This directive is used to determine whether or not status-related information about the host is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value: 0 = disable status information retention, 1 = enable status information retention.

**retain\_nonstatus\_information** This directive is used to determine whether or not non-status information about the host is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value: 0 = disable non-status information retention, 1 = enable non-status information retention.

**contacts** This is a list of the *short names* of the **contacts** that should be notified whenever there are problems (or recoveries) with this host. Multiple contacts should be separated by commas. Useful if you want notifications to go to just a few people and don't want to configure **contact groups**. You must specify at least one contact or contact group in each host definition.

**contact\_groups** This is a list of the *short names* of the **contact groups** that should be notified whenever there are problems (or recoveries) with this host. Multiple contact groups should be separated by commas. You must specify at least one contact or contact group in each host definition.

**notification\_interval** This directive is used to define the number of 'time units' to wait before re-notifying a contact that this service is *still* down or unreachable. Unless you've changed the **interval\_length** directive from the default value of 60, this number will mean minutes. If you set this value to 0, Nagios will *not* re-notify contacts about problems for this host - only one problem notification will be sent out.

**first\_notification\_delay** This directive is used to define the number of 'time units' to wait before sending out the first problem notification when this host enters a non-UP state. Unless you've changed the **interval\_length** directive from the default value of 60, this number will mean minutes. If you set this value to 0, Nagios will start sending out notifications immediately.

**notification\_period** This directive is used to specify the short name of the **time period** during which notifications of events for this host can be sent out to contacts. If a host goes down, becomes unreachable, or recovers during a time which is not covered by the time period, no notifications will be sent out.

**notification\_options** This directive is used to determine when notifications for the host should be sent out. Valid options are a combination of one or more of the following: **d** = send notifications on a DOWN state, **u** = send notifications on an UNREACHABLE state, **r** = send notifications on recoveries (OK state), **f** = send notifications when the host starts and stops **flapping**, and **s** = send notifications when **scheduled downtime** starts and ends. If you specify **n** (none) as an option,

no host notifications will be sent out. If you do not specify any notification options, Nagios will assume that you want notifications to be sent out for all possible states.

If you specify **d,r** in this field, notifications will only be sent out when the host goes DOWN and when it recovers from a DOWN state.

**notifications\_enabled** \* This directive is used to determine whether or not notifications for this host are enabled. Values: 0 = disable host notifications, 1 = enable host notifications.

**talking\_options** This directive determines which host states "stalking" is enabled for. Valid options are a combination of one or more of the following: **o** = stalk on UP states, **d** = stalk on DOWN states, and **u** = stalk on UNREACHABLE states. More information on state stalking can be found [here](#).

**notes** This directive is used to define an optional string of notes pertaining to the host. If you specify a note here, you will see the it in the [extended information](#) CGI (when you are viewing information about the specified host).

**notes\_url** This variable is used to define an optional URL that can be used to provide more information about the host. If you specify an URL, you will see a red folder icon in the CGIs (when you are viewing host information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*). This can be very useful if you want to make detailed information on the host, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the host. If you specify an URL, you will see a red 'splat' icon in the CGIs (when you are viewing host information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*).

**icon\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this host. This image will be displayed in the various places in the CGIs. The image will look best if it is 40x40 pixels in size. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. */usr/local/nagios/share/images/logos/*).

**icon\_image\_alt** This variable is used to define an optional string that is used in the ALT tag of the image specified by the *<icon\_image>* argument.

**vrml\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this host. This image will be used as the texture map for the specified host in the [statuswrl](#) CGI. Unlike the image you use for the *<icon\_image>* variable, this one should probably *not* have any transparency. If it does, the host object will look a bit wierd. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. */usr/local/nagios/share/images/logos/*).

**statusmap\_image** This variable is used to define the name of an image that should be associated with this host in the [statusmap](#) CGI. You can specify a JPEG, PNG, and GIF image if you want, although I would strongly suggest using a GD2 format image, as other image formats will result in a lot of wasted CPU time when the statusmap image is generated. GD2 images can be created from PNG images by using the **pngtogd2** utility supplied with Thomas Boutell's [gd library](#). The GD2 images should be created in *uncompressed* format in order to minimize CPU load when the statusmap CGI is generating the network map image. The image will look best if it is 40x40 pixels in size. You can leave these option blank if you are not using the statusmap CGI. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. */usr/local/nagios/share/images/logos/*).

**2d\_coords** This variable is used to define coordinates to use when drawing the host in the [statusmap](#) CGI. Coordinates should be given in positive integers, as they correspond to physical pixels in the generated image. The origin for drawing (0,0) is in the upper left hand corner of the image and extends in the positive x direction (to the right) along the top of the image and in the positive y direction (down) along the left hand side of the image. For reference, the size of the icons drawn is usually about 40x40 pixels (text takes a little extra space). The coordinates you specify here are for the upper left hand corner of the host icon that is drawn.

---

#### Note

Don't worry about what the maximum x and y coordinates that you can use are. The CGI will automatically calculate the maximum dimensions of the image it creates based on the largest x and y coordinates you specify.

---

**3d\_coords** This variable is used to define coordinates to use when drawing the host in the [statuswrl](#) CGI. Coordinates can be positive or negative real numbers. The origin for drawing is (0.0,0.0,0.0). For reference, the size of the host cubes drawn is 0.5 units on each side (text takes a little more space). The coordinates you specify here are used as the center of the host cube.

## 18.4.2 Host Group Definition

### 18.4.2.1 Description

A host group definition is used to group one or more hosts together for simplifying configuration with [object tricks](#) or display purposes in the [CGIs](#).

### 18.4.2.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                   |                       |
|-------------------|-----------------------|
| define hostgroup{ |                       |
| hostgroup_name    | <i>hostgroup_name</i> |
| alias             | <i>alias</i>          |
| members           | <i>hosts</i>          |
| hostgroup_members | <i>hostgroups</i>     |
| notes             | <i>note_string</i>    |
| notes_url         | <i>url</i>            |
| action_url        | <i>url</i>            |
| }                 |                       |

### 18.4.2.3 Example Definition

```
define hostgroup{
 hostgroup_name novell-servers
 alias Novell Servers
 members netware1,netware2,netware3,netware4
}
```

### 18.4.2.4 Directive Descriptions

**hostgroup\_name** This directive is used to define a short name used to identify the host group.

**alias** This directive is used to define a longer name or description used to identify the host group. It is provided in order to allow you to more easily identify a particular host group.

**members** This is a list of the *short names* of [hosts](#) that should be included in this group. Multiple host names should be separated by commas. This directive may be used as an alternative to (or in addition to) the *hostgroups* directive in [host definitions](#).

**hostgroup\_members** This optional directive can be used to include hosts from other ‘sub’ host groups in this host group. Specify a comma-delimited list of short names of other host groups whose members should be included in this group.

**notes** This directive is used to define an optional string of notes pertaining to the host. If you specify a note here, you will see the it in the [extended information](#) CGI (when you are viewing information about the specified host).

**notes\_url** This variable is used to define an optional URL that can be used to provide more information about the host group. If you specify an URL, you will see a red folder icon in the CGIs (when you are viewing hostgroup information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*). This can be very useful if you want to make detailed information on the host group, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the host group. If you specify an URL, you will see a red 'splat' icon in the CGIs (when you are viewing hostgroup information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*).

## 18.4.3 Service Definition

### 18.4.3.1 Description

A service definition is used to identify a 'service' that runs on a host. The term 'service' is used very loosely. It can mean an actual service that runs on the host (POP, SMTP, HTTP, etc.) or some other type of metric associated with the host (response to a ping, number of logged in users, free disk space, etc.). The different arguments to a service definition are outlined below.

### 18.4.3.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                              |                            |
|------------------------------|----------------------------|
| define service{              |                            |
| host_name                    | <i>host_name</i>           |
| hostgroup_name               | <i>hostgroup_name</i>      |
| service_description          | <i>service_description</i> |
| display_name                 | <i>display_name</i>        |
| servicegroups                | servicegroup_names         |
| is_volatile                  | [0/1]                      |
| check_command                | <i>command_name</i>        |
| initial_state                | [o,w,u,c]                  |
| max_check_attempts           | #                          |
| check_interval               | #                          |
| retry_interval               | #                          |
| active_checks_enabled        | [0/1]                      |
| passive_checks_enabled       | [0/1]                      |
| check_period                 | <i>timeperiod_name</i>     |
| obsess_over_service          | [0/1]                      |
| check_freshness              | [0/1]                      |
| freshness_threshold          | #                          |
| event_handler                | <i>command_name</i>        |
| event_handler_enabled        | [0/1]                      |
| low_flap_threshold           | #                          |
| high_flap_threshold          | #                          |
| flap_detection_enabled       | [0/1]                      |
| flap_detection_options       | [o,w,c,u]                  |
| process_perf_data            | [0/1]                      |
| retain_status_information    | [0/1]                      |
| retain_nonstatus_information | [0/1]                      |
| notification_interval        | #                          |
| first_notification_delay     | #                          |

|                                    |                        |
|------------------------------------|------------------------|
| <code>notification_period</code>   | <i>timeperiod_name</i> |
| <code>notification_options</code>  | [w,u,c,r,f,s]          |
| <code>notifications_enabled</code> | [0/1]                  |
| <code>contacts</code>              | <i>contacts</i>        |
| <code>contact_groups</code>        | <i>contact_groups</i>  |
| <code>stalking_options</code>      | [o,w,u,c]              |
| <code>notes</code>                 | <i>note_string</i>     |
| <code>notes_url</code>             | <i>url</i>             |
| <code>action_url</code>            | <i>url</i>             |
| <code>icon_image</code>            | <i>image_file</i>      |
| <code>icon_image_alt</code>        | <i>alt_string</i>      |
| }                                  |                        |

### 18.4.3.3 Example Definition

```
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 linux-admins
}
```

### 18.4.3.4 Directive Descriptions:

**host\_name** This directive is used to specify the *short name(s)* of the **host(s)** that the service "runs" on or is associated with. Multiple hosts should be separated by commas.

**hostgroup\_name** This directive is used to specify the *short name(s)* of the **hostgroup(s)** that the service "runs" on or is associated with. Multiple hostgroups should be separated by commas. The `hostgroup_name` may be used instead of, or in addition to, the `host_name` directive.

**service\_description** This directive is used to define the description of the service, which may contain spaces, dashes, and colons (semicolons, apostrophes, and quotation marks should be avoided). No two services associated with the same host can have the same description. Services are uniquely identified with their *host\_name* and *service\_description* directives.

**display\_name** This directive is used to define an alternate name that should be displayed in the web interface for this service. If not specified, this defaults to the value you specify for the *service\_description* directive.

---

#### Note

The current CGIs do not use this option, although future versions of the web interface will.

---

**servicegroups** This directive is used to identify the *short name(s)* of the **servicegroup(s)** that the service belongs to. Multiple servicegroups should be separated by commas. This directive may be used as an alternative to using the *members* directive in **servicegroup** definitions.

**is\_volatile** This directive is used to denote whether the service is "volatile". Services are normally *not* volatile. More information on volatile service and how they differ from normal services can be found [here](#). Value: 0 = service is not volatile, 1 = service is volatile.

---

**check\_command** This directive is used to specify the *short name* of the **command** that Nagios will run in order to check the status of the service. The maximum amount of time that the service check command can run is controlled by the **service\_check\_timeout** option.

**initial\_state** By default Nagios will assume that all services are in OK states when in starts. You can override the initial state for a service by using this directive. Valid options are:

- **o** = OK
- **w** = WARNING
- **u** = UNKNOWN
- **c** = CRITICAL.

**max\_check\_attempts** This directive is used to define the number of times that Nagios will retry the service check command if it returns any state other than an OK state. Setting this value to 1 will cause Nagios to generate an alert without retrying the service check again.

**check\_interval** This directive is used to define the number of ‘time units’ to wait before scheduling the next ‘regular’ check of the service. ‘Regular’ checks are those that occur when the service is in an OK state or when the service is in a non-OK state, but has already been rechecked **max\_check\_attempts** number of times. Unless you’ve changed the **interval\_length** directive from the default value of 60, this number will mean minutes. More information on this value can be found in the **check scheduling** documentation.

**retry\_interval** This directive is used to define the number of ‘time units’ to wait before scheduling a re-check of the service. Services are rescheduled at the retry interval when they have changed to a non-OK state. Once the service has been retried **max\_check\_attempts** times without a change in its status, it will revert to being scheduled at its ‘normal’ rate as defined by the **check\_interval** value. Unless you’ve changed the **interval\_length** directive from the default value of 60, this number will mean minutes. More information on this value can be found in the **check scheduling** documentation.

**active\_checks\_enabled\*** This directive is used to determine whether or not active checks of this service are enabled. Values:

- 0 = disable active service checks
- 1 = enable active service checks.

**passive\_checks\_enabled \*** This directive is used to determine whether or not passive checks of this service are enabled. Values:

- 0 = disable passive service checks
- 1 = enable passive service checks.

**check\_period** This directive is used to specify the short name of the **time period** during which active checks of this service can be made.

**obsess\_over\_service \*** This directive determines whether or not checks for the service will be ‘obsessed’ over using the **ocsp\_command**.

**check\_freshness \*** This directive is used to determine whether or not **freshness checks** are enabled for this service. Values:

- 0 = disable freshness checks
- 1 = enable freshness checks

**freshness\_threshold** This directive is used to specify the freshness threshold (in seconds) for this service. If you set this directive to a value of 0, Nagios will determine a freshness threshold to use automatically.

**event\_handler** This directive is used to specify the *short name* of the **command** that should be run whenever a change in the state of the service is detected (i.e. whenever it goes down or recovers). Read the documentation on **event handlers** for a more detailed explanation of how to write scripts for handling events. The maximum amount of time that the event handler command can run is controlled by the **event\_handler\_timeout** option.

**event\_handler\_enabled \*** This directive is used to determine whether or not the event handler for this service is enabled. Values:

- 0 = disable service event handler

- 1 = enable service event handler.

**low\_flap\_threshold** This directive is used to specify the low state change threshold used in flap detection for this service. More information on flap detection can be found [here](#). If you set this directive to a value of 0, the program-wide value specified by the **low\_service\_flap\_threshold** directive will be used.

**high\_flap\_threshold** This directive is used to specify the high state change threshold used in flap detection for this service. More information on flap detection can be found [here](#). If you set this directive to a value of 0, the program-wide value specified by the **high\_service\_flap\_threshold** directive will be used.

**flap\_detection\_enabled** \* This directive is used to determine whether or not flap detection is enabled for this service. More information on flap detection can be found [here](#). Values:

- 0 = disable service flap detection
- 1 = enable service flap detection.

**flap\_detection\_options** This directive is used to determine what service states the **flap detection logic** will use for this service. Valid options are a combination of one or more of the following :

- **o** = OK states
- **w** = WARNING states
- **c** = CRITICAL states
- **u** = UNKNOWN states.

**process\_perf\_data** \* This directive is used to determine whether or not the processing of performance data is enabled for this service. Values:

- 0 = disable performance data processing
- 1 = enable performance data processing

**retain\_status\_information** This directive is used to determine whether or not status-related information about the service is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value:

- 0 = disable status information retention
- 1 = enable status information retention.

**retain\_nonstatus\_information** This directive is used to determine whether or not non-status information about the service is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value:

- 0 = disable non-status information retention
- 1 = enable non-status information retention

**notification\_interval** This directive is used to define the number of ‘time units’ to wait before re-notifying a contact that this service is *still* in a non-OK state. Unless you’ve changed the **interval\_length** directive from the default value of 60, this number will mean minutes. If you set this value to 0, Nagios will *not* re-notify contacts about problems for this service - only one problem notification will be sent out.

**first\_notification\_delay** This directive is used to define the number of ‘time units’ to wait before sending out the first problem notification when this service enters a non-OK state. Unless you’ve changed the **interval\_length** directive from the default value of 60, this number will mean minutes. If you set this value to 0, Nagios will start sending out notifications immediately.

**notification\_period** This directive is used to specify the short name of the **time period** during which notifications of events for this service can be sent out to contacts. No service notifications will be sent out during times which is not covered by the time period.

**notification\_options** This directive is used to determine when notifications for the service should be sent out. Valid options are a combination of one or more of the following:



- **w** = send notifications on a WARNING state
- **u** = send notifications on an UNKNOWN state
- **c** = send notifications on a CRITICAL state
- **r** = send notifications on recoveries (OK state)
- **f** = send notifications when the service starts and stops **flapping**
- **s** = send notifications when **scheduled downtime** starts and ends
- **n** (none) as an option, no service notifications will be sent out. If you do not specify any notification options, Nagios will assume that you want notifications to be sent out for all possible states

If you specify **w,r** in this field, notifications will only be sent out when the service goes into a WARNING state and when it recovers from a WARNING state.

**notifications\_enabled** \* This directive is used to determine whether or not notifications for this service are enabled. Values:

- **0** = disable service notifications
- **1** = enable service notifications.

**contacts** This is a list of the *short names* of the **contacts** that should be notified whenever there are problems (or recoveries) with this service. Multiple contacts should be separated by commas. Useful if you want notifications to go to just a few people and don't want to configure **contact groups**. You must specify at least one contact or contact group in each service definition.

**contact\_groups** This is a list of the *short names* of the **contact groups** that should be notified whenever there are problems (or recoveries) with this service. Multiple contact groups should be separated by commas. You must specify at least one contact or contact group in each service definition.

**stalking\_options** This directive determines which service states "stalking" is enabled for. Valid options are a combination of one or more of the following :

- **o** = stalk on OK states
- **w** = stalk on WARNING states
- **u** = stalk on UNKNOWN states
- **c** = stalk on CRITICAL states

More information on state stalking can be found [here](#).

**notes** This directive is used to define an optional string of notes pertaining to the service. If you specify a note here, you will see the it in the **extended information** CGI (when you are viewing information about the specified service).

**notes\_url** This directive is used to define an optional URL that can be used to provide more information about the service. If you specify an URL, you will see a red folder icon in the CGIs (when you are viewing service information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*). This can be very useful if you want to make detailed information on the service, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the service. If you specify an URL, you will see a red 'splat' icon in the CGIs (when you are viewing service information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*).

**icon\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this service. This image will be displayed in the **status** and **extended information** CGIs. The image will look best if it is 40x40 pixels in size. Images for services are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. */usr/local/nagios/share/images/logos/*).

**icon\_image\_alt** This variable is used to define an optional string that is used in the ALT tag of the image specified by the *<icon\_image>* argument. The ALT tag is used in the **status**, **extended information** and **statusmap** CGIs.



## 18.4.4 Service Group Definition

### 18.4.4.1 Description

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**.

### 18.4.4.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                      |                          |
|----------------------|--------------------------|
| define servicegroup{ |                          |
| servicegroup_name    | <i>servicegroup_name</i> |
| alias                | <i>alias</i>             |
| members              | <i>services</i>          |
| servicegroup_members | <i>servicegroups</i>     |
| notes                | <i>note_string</i>       |
| notes_url            | <i>url</i>               |
| action_url           | <i>url</i>               |
| }                    |                          |

### 18.4.4.3 Example Definition

```
define servicegroup{
 servicegroup_name dbservices
 alias Database Services
 members ms1,SQL Server,ms1,SQL Serverc Agent,ms1,SQL DTC
}
```

### 18.4.4.4 Directive Descriptions:

**servicegroup\_name** This directive is used to define a short name used to identify the service group.

**alias** This directive is used to define is a longer name or description used to identify the service group. It is provided in order to allow you to more easily identify a particular service group.

**members** This is a list of the *descriptions* of **services** (and the names of their corresponding hosts) that should be included in this group. Host and service names should be separated by commas. This directive may be used as an alternative to the *servicegroups* directive in **service definitions**. The format of the member directive is as follows (note that a host name must precede a service name/description):

```
members=<host1>,<service1>,<host2>,<service2>,...,<hostn>,<servicen>
```

**servicegroup\_members** This optional directive can be used to include services from other 'sub' service groups in this service group. Specify a comma-delimited list of short names of other service groups whose members should be included in this group.

**notes** This directive is used to define an optional string of notes pertaining to the service group. If you specify a note here, you will see the it in the **extended information** CGI (when you are viewing information about the specified service group).

**notes\_url** This directive is used to define an optional URL that can be used to provide more information about the service group. If you specify an URL, you will see a red folder icon in the CGIs (when you are viewing service group information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*). This can be very useful if you want to make detailed information on the service group, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the service group. If you specify an URL, you will see a red 'splat' icon in the CGIs (when you are viewing service group information) that links to the URL you specify here. Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*).

## 18.4.5 Contact Definition

### 18.4.5.1 Description

A contact definition is used to identify someone who should be contacted in the event of a problem on your network. The different arguments to a contact definition are described below.

### 18.4.5.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                               |                                            |
|-------------------------------|--------------------------------------------|
| define contact{               |                                            |
| contact_name                  | <i>contact_name</i>                        |
| alias                         | <i>alias</i>                               |
| contactgroups                 | <i>contactgroup_names</i>                  |
| host_notifications_enabled    | [0/1]                                      |
| service_notifications_enabled | [0/1]                                      |
| host_notification_period      | <i>timeperiod_name</i>                     |
| service_notification_period   | <i>timeperiod_name</i>                     |
| host_notification_options     | [d,u,r,f,s,n]                              |
| service_notification_options  | [w,u,c,r,f,s,n]                            |
| host_notification_commands    | <i>command_name</i>                        |
| service_notification_commands | <i>command_name</i>                        |
| email                         | <i>email_address</i>                       |
| pager                         | <i>pager_number or pager_email_gateway</i> |
| addressx                      | <i>additional_contact_address</i>          |
| can_submit_commands           | [0/1]                                      |
| retain_status_information     | [0/1]                                      |
| retain_nonstatus_information  | [0/1]                                      |
| }                             |                                            |

### 18.4.5.3 Example Definition

```
define contact{
 contact_name jdoe
 alias John Doe
 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 jdoe@localhost.localdomain
 pager 555-5555@pagergateway.localhost.localdomain
 address1 xxxxx.xyyy@icq.com
 address2 555-555-5555
 can_submit_commands 1
}

```

#### 18.4.5.4 Directive Descriptions

**contact\_name** This directive is used to define a short name used to identify the contact. It is referenced in **contact group** definitions. Under the right circumstances, the `$CONTACTNAME$` **macro** will contain this value.

**alias** This directive is used to define a longer name or description for the contact. Under the right circumstances, the `$CONTACTALIAS$` **macro** will contain this value. If not specified, the *contact\_name* will be used as the alias.

**contactgroups** This directive is used to identify the *short name(s)* of the **contactgroup(s)** that the contact belongs to. Multiple contactgroups should be separated by commas. This directive may be used as an alternative to (or in addition to) using the *members* directive in **contactgroup** definitions.

**host\_notifications\_enabled** This directive is used to determine whether or not the contact will receive notifications about host problems and recoveries. Values :

- 0 = don't send notifications
- 1 = send notifications

**service\_notifications\_enabled** This directive is used to determine whether or not the contact will receive notifications about service problems and recoveries. Values:

- 0 = don't send notifications
- 1 = send notifications

**host\_notification\_period** This directive is used to specify the short name of the **time period** during which the contact can be notified about host problems or recoveries. You can think of this as an 'on call' time for host notifications for the contact. Read the documentation on **time periods** for more information on how this works and potential problems that may result from improper use.

**service\_notification\_period** This directive is used to specify the short name of the **time period** during which the contact can be notified about service problems or recoveries. You can think of this as an 'on call' time for service notifications for the contact. Read the documentation on **time periods** for more information on how this works and potential problems that may result from improper use.

**host\_notification\_commands** This directive is used to define a list of the *short names* of the **commands** used to notify the contact of a *host* problem or recovery. Multiple notification commands should be separated by commas. All notification commands are executed when the contact needs to be notified. The maximum amount of time that a notification command can run is controlled by the **notification\_timeout** option.

**host\_notification\_options** This directive is used to define the host states for which notifications can be sent out to this contact. Valid options are a combination of one or more of the following:

- d = notify on DOWN host states
- u = notify on UNREACHABLE host states
- r = notify on host recoveries (UP states)
- f = notify when the host starts and stops **flapping**.
- s = send notifications when host or service **scheduled downtime** starts and ends. If you specify **n** (none) as an option, the contact will not receive any type of host notifications.

**service\_notification\_options** This directive is used to define the service states for which notifications can be sent out to this contact. Valid options are a combination of one or more of the following:

- w = notify on WARNING service states
- u = notify on UNKNOWN service states
- c = notify on CRITICAL service states
- r = notify on service recoveries (OK states)
- f = notify when the service starts and stops **flapping**.
- n = (none) : the contact will not receive any type of service notifications.

**service\_notification\_commands** This directive is used to define a list of the *short names* of the **commands** used to notify the contact of a *service* problem or recovery. Multiple notification commands should be separated by commas. All notification commands are executed when the contact needs to be notified. The maximum amount of time that a notification command can run is controlled by the **notification\_timeout** option.

**email** This directive is used to define an email address for the contact. Depending on how you configure your notification commands, it can be used to send out an alert email to the contact. Under the right circumstances, the \$CONTACTEMAIL\$ **macro** will contain this value.

**pager** This directive is used to define a pager number for the contact. It can also be an email address to a pager gateway (i.e. **pagejoe@pagenet.com**). Depending on how you configure your notification commands, it can be used to send out an alert page to the contact. Under the right circumstances, the \$CONTACTPAGER\$ **macro** will contain this value.

**addressx** Address directives are used to define additional ‘addresses’ for the contact. These addresses can be anything - cell phone numbers, instant messaging addresses, etc. Depending on how you configure your notification commands, they can be used to send out an alert to the contact. Up to six addresses can be defined using these directives (*address1* through *address6*). The \$CONTACTADDRESSx\$ **macro** will contain this value.

**can\_submit\_commands** This directive is used to determine whether or not the contact can submit **external commands** to Nagios from the CGIs. Values:

- 0 = don’t allow contact to submit commands
- 1 = allow contact to submit commands.

**retain\_status\_information** This directive is used to determine whether or not status-related information about the contact is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value :

- 0 = disable status information retention
- 1 = enable status information retention.

**retain\_nonstatus\_information** This directive is used to determine whether or not non-status information about the contact is retained across program restarts. This is only useful if you have enabled state retention using the **retain\_state\_information** directive. Value :

- 0 = disable non-status information retention
- 1 = enable non-status information retention

## 18.4.6 Contact Group Definition

### 18.4.6.1 Description

A contact group definition is used to group one or more **contacts** together for the purpose of sending out alert/recovery **notifications**.

#### 18.4.6.2 Definition Format:

---

##### Note

Directives in red are required, while those in black are optional.

---

|                      |                          |
|----------------------|--------------------------|
| define contactgroup{ |                          |
| contactgroup_name    | <i>contactgroup_name</i> |
| alias                | <i>alias</i>             |
| members              | <i>contacts</i>          |
| contactgroup_members | <i>contactgroups</i>     |
| }                    |                          |

#### 18.4.6.3 Example Definition:

```
define contactgroup{
 contactgroup_name novell-admins
 alias Novell Administrators
 members jdoe,rtobert,tzach
}
```

#### 18.4.6.4 Directive Descriptions:

**contactgroup\_name** This directive is a short name used to identify the contact group.

**alias** This directive is used to define a longer name or description used to identify the contact group.

**members** This directive is used to define a list of the *short names* of **contacts** that should be included in this group. Multiple contact names should be separated by commas. This directive may be used as an alternative to (or in addition to) using the *contactgroups* directive in **contact** definitions.

**contactgroup\_members** This optional directive can be used to include contacts from other 'sub' contact groups in this contact group. Specify a comma-delimited list of short names of other contact groups whose members should be included in this group.

### 18.4.7 Time Period Definition

#### 18.4.7.1 Description

A time period is a list of times during various days that are considered to be 'valid' times for notifications and service checks. It consists of time ranges for each day of the week that 'rotate' once the week has come to an end. Different types of exceptions to the normal weekly time are supported, including: specific weekdays, days of generic months, days of specific months, and calendar dates.

#### 18.4.7.2 Definition Format

---

##### Note

Directives in red are required, while those in black are optional.

---

|                    |                                                  |
|--------------------|--------------------------------------------------|
| define timeperiod{ |                                                  |
| timeperiod_name    | <i>timeperiod_name</i>                           |
| alias              | <i>alias</i>                                     |
| [weekday]          | <i>timeranges</i>                                |
| [exception]        | <i>timeranges</i>                                |
| exclude            | <i>[timeperiod1,timeperiod2,...,timeperiodn]</i> |
| }                  |                                                  |

### 18.4.7.3 Example Definitions

```

define timeperiod{
 timeperiod_name nonworkhours
 alias Non-Work Hours
 sunday 00:00-24:00 ; Every Sunday of every week
 monday 00:00-09:00,17:00-24:00 ; Every Monday of every week
 tuesday 00:00-09:00,17:00-24:00 ; Every Tuesday of every week
 wednesday 00:00-09:00,17:00-24:00 ; Every Wednesday of every week
 thursday 00:00-09:00,17:00-24:00 ; Every Thursday of every week
 friday 00:00-09:00,17:00-24:00 ; Every Friday of every week
 saturday 00:00-24:00 ; Every Saturday of every week
}

define timeperiod{
 timeperiod_name misc-single-days
 alias Misc Single Days
 1999-01-28 00:00-24:00 ; January 28th, 1999
 monday 3 00:00-24:00 ; 3rd Monday of every month
 day 2 00:00-24:00 ; 2nd day of every month
 february 10 00:00-24:00 ; February 10th of every year
 february -1 00:00-24:00 ; Last day in February of every year
 friday -2 00:00-24:00 ; 2nd to last Friday of every month
 thursday -1 november 00:00-24:00 ; Last Thursday in November of every ←
 year
}

define timeperiod{
 timeperiod_name misc-date-ranges
 alias Misc Date Ranges
 2007-01-01 - 2008-02-01 00:00-24:00 ; January 1st, 2007 to February 1st, ←
 2008
 monday 3 - thursday 4 00:00-24:00 ; 3rd Monday to 4th Thursday of ←
 every month
 day 1 - 15 00:00-24:00 ; 1st to 15th day of every month
 day 20 - -1 00:00-24:00 ; 20th to the last day of every ←
 month
 july 10 - 15 00:00-24:00 ; July 10th to July 15th of every ←
 year
 april 10 - may 15 00:00-24:00 ; April 10th to May 15th of every ←
 year
 tuesday 1 april - friday 2 may 00:00-24:00 ; 1st Tuesday in April to 2nd Friday ←
 in May of every year
}

define timeperiod{
 timeperiod_name misc-skip-ranges
 alias Misc Skip Ranges
 2007-01-01 - 2008-02-01 / 3 00:00-24:00 ; Every 3 days from January 1st, ←
 2007 to February 1st, 2008
 2008-04-01 / 7 00:00-24:00 ; Every 7 days from April 1st, ←
 2008 (continuing forever)
}

```

```

monday 3 - thursday 4 / 2 00:00-24:00 ; Every other day from 3rd Monday ↵
 to 4th Thursday of every month
day 1 - 15 / 5 00:00-24:00 ; Every 5 days from the 1st to ↵
 the 15th day of every month
july 10 - 15 / 2 00:00-24:00 ; Every other day from July 10th ↵
 to July 15th of every year
tuesday 1 april - friday 2 may / 6 00:00-24:00 ; Every 6 days from the 1st ↵
 Tuesday in April to the 2nd Friday in May of every year
}

```

#### 18.4.7.4 Directive Descriptions

**timeperiod\_name** This directive is the short name used to identify the time period.

**alias** This directive is a longer name or description used to identify the time period.

**[weekday]** The weekday directives ('*sunday*' through '*saturday*') are comma-delimited lists of time ranges that are 'valid' times for a particular day of the week. Notice that there are seven different days for which you can define time ranges (Sunday through Saturday). Each time range is in the form of **HH:MM-HH:MM**, where hours are Specified on a 24 hour clock. For example, **00:15-24:00** means 12:15am in the morning for this day until 12:00am midnight (a 23 hour, 45 minute total time range). If you wish to exclude an entire day from the timeperiod, simply do not include it in the timeperiod definition.

**[exception]** You can specify several different types of exceptions to the standard rotating weekday schedule. Exceptions can take a number of different forms including single days of a specific or generic month, single weekdays in a month, or single calendar dates. You can also specify a range of days/dates and even specify skip intervals to obtain functionality described by 'every 3 days between these dates'. Rather than list all the possible formats for exception strings, I'll let you look at the example timeperiod definitions above to see what's possible. :-) Weekdays and different types of exceptions all have different levels of precedence, so it's important to understand how they can affect each other. More information on this can be found in the documentation on [timeperiods](#).

**exclude** This directive is used to specify the short names of other timeperiod definitions whose time ranges should be excluded from this timeperiod. Multiple timeperiod names should be separated with a comma.

### 18.4.8 Command Definition

#### 18.4.8.1 Description

A command definition is just that. It defines a command. Commands that can be defined include service checks, service notifications, service event handlers, host checks, host notifications, and host event handlers. Command definitions can contain [macros](#), but you must make sure that you include only those macros that are 'valid' for the circumstances when the command will be used. More information on what macros are available and when they are 'valid' can be found [here](#). The different arguments to a command definition are outlined below.

#### 18.4.8.2 Definition Format

---

##### Note

Directives in red are required, while those in black are optional.

---

|                 |                     |
|-----------------|---------------------|
| define command{ |                     |
| command_name    | <i>command_name</i> |
| command_line    | <i>command_line</i> |
| }               |                     |

---

### 18.4.8.3 Example Definition

```
define command{
 command_name check_pop
 command_line /usr/local/nagios/libexec/check_pop -H $HOSTADDRESS$ ~ ~
}
```

### 18.4.8.4 Directive Descriptions

**command\_name** This directive is the short name used to identify the command. It is referenced in **contact**, **host**, and **service** definitions (in notification, check, and event handler directives), among other places.

**command\_line** This directive is used to define what is actually executed by Nagios when the command is used for service or host checks, notifications, or **event handlers**. Before the command line is executed, all valid **macros** are replaced with their respective values. See the documentation on macros for determining when you can use different macros. Note that the command line is *not* surrounded in quotes. Also, if you want to pass a dollar sign (\$) on the command line, you have to escape it with another dollar sign.

#### Note

You may not include a **semicolon** (;) in the *command\_line* directive, because everything after it will be ignored as a config file comment. You can work around this limitation by setting one of the **\$USER\$** macros in your **resource file** to a semicolon and then referencing the appropriate **\$USER\$** macro in the *command\_line* directive in place of the semicolon.

If you want to pass arguments to commands during runtime, you can use **\$ARGn\$ macros** in the *command\_line* directive of the command definition and then separate individual arguments from the command name (and from each other) using bang (!) characters in the object definition directive (host check command, service event handler command, etc.) that references the command. More information on how arguments in command definitions are processed during runtime can be found in the documentation on **macros**.

## 18.4.9 Service Dependency Definition

### 18.4.9.1 Description

Service dependencies are an advanced feature of Nagios that allow you to suppress notifications and active checks of services based on the status of one or more other services. Service dependencies are optional and are mainly targeted at advanced users who have complicated monitoring setups. More information on how service dependencies work (read this!) can be found [here](#).

### 18.4.9.2 Definition Format

#### Note

Directives in red are required, while those in black are optional. However, you must supply at least one type of criteria for the definition to be of much use.

|                               |                            |
|-------------------------------|----------------------------|
| define servicedependency{     |                            |
| dependent_host_name           | <i>host_name</i>           |
| dependent_hostgroup_name      | <i>hostgroup_name</i>      |
| dependent_service_description | <i>service_description</i> |
| host_name                     | <i>host_name</i>           |
| hostgroup_name                | <i>hostgroup_name</i>      |
| service_description           | <i>service_description</i> |



|                                            |                              |
|--------------------------------------------|------------------------------|
| <code>inherits_parent</code>               | <code>[0/1]</code>           |
| <code>execution_failure_criteria</code>    | <code>[o,w,u,c,p,n]</code>   |
| <code>notification_failure_criteria</code> | <code>[o,w,u,c,p,n]</code>   |
| <code>dependency_period</code>             | <code>timeperiod_name</code> |
| <code>}</code>                             |                              |

### 18.4.9.3 Example Definition

```
define servicedependency{
 host_name WWW1
 service_description Apache Web Server
 dependent_host_name WWW1
 dependent_service_description Main Web Site
 execution_failure_criteria n
 notification_failure_criteria w,u,c
}
```

### 18.4.9.4 Directive Descriptions

**dependent\_host** This directive is used to identify the *short name(s)* of the **host(s)** that the *dependent* service ‘runs’ on or is associated with. Multiple hosts should be separated by commas. Leaving this directive blank can be used to create **same host dependencies**.

**dependent\_hostgroup** This directive is used to specify the *short name(s)* of the **hostgroup(s)** that the *dependent* service "runs" on or is associated with. Multiple hostgroups should be separated by commas. The `dependent_hostgroup` may be used instead of, or in addition to, the `dependent_host` directive.

**dependent\_service\_description** This directive is used to identify the *description* of the *dependent service*.

**host\_name** This directive is used to identify the *short name(s)* of the **host(s)** that the service *that is being depended upon* (also referred to as the master service) "runs" on or is associated with. Multiple hosts should be separated by commas.

**hostgroup\_name** This directive is used to identify the *short name(s)* of the **hostgroup(s)** that the service *that is being depended upon* (also referred to as the master service) "runs" on or is associated with. Multiple hostgroups should be separated by commas. The `hostgroup_name` may be used instead of, or in addition to, the `host_name` directive.

**service\_description** This directive is used to identify the *description* of the **service that is being depended upon** (also referred to as the master service).

**inherits\_parent** This directive indicates whether or not the dependency inherits dependencies of the service *that is being depended upon* (also referred to as the master service). In other words, if the master service is dependent upon other services and any one of those dependencies fail, this dependency will also fail.

**execution\_failure\_criteria** This directive is used to specify the criteria that determine when the dependent service should *not* be actively checked. If the *master* service is in one of the failure states we specify, the *dependent* service will not be actively checked. Valid options are a combination of one or more of the following (multiple options are separated with commas):

- **o** = fail on an OK state
- **w** = fail on a WARNING state
- **u** = fail on an UNKNOWN state
- **c** = fail on a CRITICAL state
- **p** = fail on a pending state (e.g. the service has not yet been checked).
- **n** (none) : the execution dependency will never fail and checks of the dependent service will always be actively checked (if other conditions allow for it to be).

If you specify **o,c,u** in this field, the *dependent* service will not be actively checked if the *master* service is in either an OK, a CRITICAL, or an UNKNOWN state.

**notification\_failure\_criteria** This directive is used to define the criteria that determine when notifications for the dependent service should *not* be sent out. If the *master* service is in one of the failure states we specify, notifications for the *dependent* service will not be sent to contacts. Valid options are a combination of one or more of the following:

- **o** = fail on an OK state
- **w** = fail on a WARNING state
- **u** = fail on an UNKNOWN state
- **c** = fail on a CRITICAL state
- **p** = fail on a pending state (e.g. the service has not yet been checked).
- **n** = (none) : the notification dependency will never fail and notifications for the dependent service will always be sent out.

If you specify **w** in this field, the notifications for the *dependent* service will not be sent out if the *master* service is in a WARNING state.

**dependency\_period** This directive is used to specify the short name of the **time period** during which this dependency is valid. If this directive is not specified, the dependency is considered to be valid during all times.

## 18.4.10 Service Escalation Definition

### 18.4.10.1 Description

Service escalations are completely optional and are used to escalate notifications for a particular service. More information on how notification escalations work can be found [here](#).

### 18.4.10.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                           |                            |
|---------------------------|----------------------------|
| define serviceescalation{ |                            |
| host_name                 | <i>host_name</i>           |
| hostgroup_name            | <i>hostgroup_name</i>      |
| service_description       | <i>service_description</i> |
| contacts                  | <i>contacts</i>            |
| contact_groups            | <i>contactgroup_name</i>   |
| first_notification        | #                          |
| last_notification         | #                          |
| notification_interval     | #                          |
| escalation_period         | timeperiod_name            |
| escalation_options        | [w,u,c,r]                  |
| }                         |                            |

### 18.4.10.3 Example Definition

```
define serviceescalation{
 host_name nt-3
 service_description Processor Load
 first_notification 4
}
```

```

 last_notification 0
 notification_interval 30
 contact_groups all-nt-admins,themanagers
}

```

#### 18.4.10.4 Directive Descriptions

**host\_name** This directive is used to identify the *short name(s)* of the **host(s)** that the **service** escalation should apply to or is associated with.

**hostgroup\_name** This directive is used to specify the *short name(s)* of the **hostgroup(s)** that the service escalation should apply to or is associated with. Multiple hostgroups should be separated by commas. The `hostgroup_name` may be used instead of, or in addition to, the `host_name` directive.

**service\_description** This directive is used to identify the *description* of the **service** the escalation should apply to.

**first\_notification** This directive is a number that identifies the *first* notification for which this escalation is effective. For instance, if you set this value to 3, this escalation will only be used if the service is in a non-OK state long enough for a third notification to go out.

**last\_notification** This directive is a number that identifies the *last* notification for which this escalation is effective. For instance, if you set this value to 5, this escalation will not be used if more than five notifications are sent out for the service. Setting this value to 0 means to keep using this escalation entry forever (no matter how many notifications go out).

**contacts** This is a list of the *short names* of the **contacts** that should be notified whenever there are problems (or recoveries) with this service. Multiple contacts should be separated by commas. Useful if you want notifications to go to just a few people and don't want to configure **contact groups**. You must specify at least one contact or contact group in each service escalation definition.

**contact\_groups** This directive is used to identify the *short name* of the **contact group** that should be notified when the service notification is escalated. Multiple contact groups should be separated by commas. You must specify at least one contact or contact group in each service escalation definition.

**notification\_interval** This directive is used to determine the interval at which notifications should be made while this escalation is valid. If you specify a value of 0 for the interval, Nagios will send the first notification when this escalation definition is valid, but will then prevent any more problem notifications from being sent out for the host. Notifications are sent out again until the host recovers. This is useful if you want to stop having notifications sent out after a certain amount of time.

---

##### Note

If multiple escalation entries for a host overlap for one or more notification ranges, the smallest notification interval from all escalation entries is used.

---

**escalation\_period** This directive is used to specify the short name of the **time period** during which this escalation is valid. If this directive is not specified, the escalation is considered to be valid during all times.

**escalation\_options** This directive is used to define the criteria that determine when this service escalation is used. The escalation is used only if the service is in one of the states specified in this directive. If this directive is not specified in a service escalation, the escalation is considered to be valid during all service states. Valid options are a combination of one or more of the following:

- **r** = escalate on an OK (recovery) state
- **w** = escalate on a WARNING state
- **u** = escalate on an UNKNOWN state
- **c** = escalate on a CRITICAL state

If you specify **w** in this field, the escalation will only be used if the service is in a WARNING state.

---

## 18.4.11 Host Dependency Definition

### 18.4.11.1 Description

Host dependencies are an advanced feature of Nagios that allow you to suppress notifications for hosts based on the status of one or more other hosts. Host dependencies are optional and are mainly targeted at advanced users who have complicated monitoring setups. More information on how host dependencies work (read this!) can be found [here](#).

### 18.4.11.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                               |                       |
|-------------------------------|-----------------------|
| define hostdependency{        |                       |
| dependent_host_name           | <i>host_name</i>      |
| dependent_hostgroup_name      | <i>hostgroup_name</i> |
| host_name                     | <i>host_name</i>      |
| hostgroup_name                | <i>hostgroup_name</i> |
| inherits_parent               | [0/1]                 |
| execution_failure_criteria    | [o,d,u,p,n]           |
| notification_failure_criteria | [o,d,u,p,n]           |
| dependency_period             | timeperiod_name       |
| }                             |                       |

### 18.4.11.3 Example Definition

```
define hostdependency{
 host_name WWW1
 dependent_host_name DBASE1
 notification_failure_criteria d,u
}
```

### 18.4.11.4 Directive Descriptions

**dependent\_host\_name** This directive is used to identify the *short name(s)* of the *dependent* **host(s)**. Multiple hosts should be separated by commas.

**dependent\_hostgroup\_name** This directive is used to identify the *short name(s)* of the *dependent* **hostgroup(s)**. Multiple hostgroups should be separated by commas. The `dependent_hostgroup_name` may be used instead of, or in addition to, the `dependent_host_name` directive.

**host\_name** This directive is used to identify the *short name(s)* of the **host(s)** *that is being depended upon* (also referred to as the master host). Multiple hosts should be separated by commas.

**hostgroup\_name** This directive is used to identify the *short name(s)* of the **hostgroup(s)** *that is being depended upon* (also referred to as the master host). Multiple hostgroups should be separated by commas. The `hostgroup_name` may be used instead of, or in addition to, the `host_name` directive.

**inherits\_parent** This directive indicates whether or not the dependency inherits dependencies of the host *that is being depended upon* (also referred to as the master host). In other words, if the master host is dependent upon other hosts and any one of those dependencies fail, this dependency will also fail.

**execution\_failure\_criteria** This directive is used to specify the criteria that determine when the dependent host should *not* be actively checked. If the *master* host is in one of the failure states we specify, the *dependent* host will not be actively checked. Valid options are a combination of one or more of the following (multiple options are separated with commas):

- **o** = fail on an UP state
- **d** = fail on a DOWN state
- **u** = fail on an UNREACHABLE state
- **p** = fail on a pending state (e.g. the host has not yet been checked)
- **n** (none) : the execution dependency will never fail and the dependent host will always be actively checked (if other conditions allow for it to be).

If you specify **u,d** in this field, the *dependent* host will not be actively checked if the *master* host is in either an UNREACHABLE or DOWN state.

**notification\_failure\_criteria** This directive is used to define the criteria that determine when notifications for the dependent host should *not* be sent out. If the *master* host is in one of the failure states we specify, notifications for the *dependent* host will not be sent to contacts. Valid options are a combination of one or more of the following:

- **o** = fail on an UP state
- **d** = fail on a DOWN state
- **u** = fail on an UNREACHABLE state
- **p** = fail on a pending state (e.g. the host has not yet been checked)
- **n** = (none) : the notification dependency will never fail and notifications for the dependent host will always be sent out.

If you specify **d** in this field, the notifications for the *dependent* host will not be sent out if the *master* host is in a DOWN state.

**notification\_failure\_criteria** This directive is used to specify the short name of the **time period** during which this dependency is valid. If this directive is not specified, the dependency is considered to be valid during all times.

## 18.4.12 Host Escalation Definition

### 18.4.12.1 Description

Host escalations are completely optional and are used to escalate notifications for a particular host. More information on how notification escalations work can be found [here](#).

### 18.4.12.2 Definition Format

#### Note

Directives in red are required, while those in black are optional.

|                        |                          |
|------------------------|--------------------------|
| define hostescalation{ |                          |
| host_name              | <i>host_name</i>         |
| hostgroup_name         | <i>hostgroup_name</i>    |
| contacts               | <i>contacts</i>          |
| contact_groups         | <i>contactgroup_name</i> |
| first_notification     | #                        |
| last_notification      | #                        |
| notification_interval  | #                        |
| escalation_period      | timeperiod_name          |
| escalation_options     | [d,u,r]                  |
| }                      |                          |

### 18.4.12.3 Example Definition

```
define hostescalation{
 host_name router-34
 first_notification 5
 last_notification 8
 notification_interval 60
 contact_groups all-router-admins
}
```

### 18.4.12.4 Directive Descriptions

**host\_name** This directive is used to identify the *short name* of the **host** that the escalation should apply to.

**hostgroup\_name** This directive is used to identify the *short name(s)* of the **hostgroup(s)** that the escalation should apply to. Multiple hostgroups should be separated by commas. If this is used, the escalation will apply to all hosts that are members of the specified hostgroup(s).

**first\_notification** This directive is a number that identifies the *first* notification for which this escalation is effective. For instance, if you set this value to 3, this escalation will only be used if the host is down or unreachable long enough for a third notification to go out.

**last\_notification** This directive is a number that identifies the *last* notification for which this escalation is effective. For instance, if you set this value to 5, this escalation will not be used if more than five notifications are sent out for the host. Setting this value to 0 means to keep using this escalation entry forever (no matter how many notifications go out).

**contacts** This is a list of the *short names* of the **contacts** that should be notified whenever there are problems (or recoveries) with this host. Multiple contacts should be separated by commas. Useful if you want notifications to go to just a few people and don't want to configure **contact groups**. You must specify at least one contact or contact group in each host escalation definition.

**contact\_groups** This directive is used to identify the *short name* of the **contact group** that should be notified when the host notification is escalated. Multiple contact groups should be separated by commas. You must specify at least one contact or contact group in each host escalation definition.

**notification\_interval** This directive is used to determine the interval at which notifications should be made while this escalation is valid. If you specify a value of 0 for the interval, Nagios will send the first notification when this escalation definition is valid, but will then prevent any more problem notifications from being sent out for the host. Notifications are sent out again until the host recovers. This is useful if you want to stop having notifications sent out after a certain amount of time.

---

#### Note

If multiple escalation entries for a host overlap for one or more notification ranges, the smallest notification interval from all escalation entries is used.

---

**escalation\_period** This directive is used to specify the short name of the **time period** during which this escalation is valid. If this directive is not specified, the escalation is considered to be valid during all times.

**escalation\_options** This directive is used to define the criteria that determine when this host escalation is used. The escalation is used only if the host is in one of the states specified in this directive. If this directive is not specified in a host escalation, the escalation is considered to be valid during all host states. Valid options are a combination of one or more of the following :

- **r** = escalate on an UP (recovery) state
- **d** = escalate on a DOWN state
- **u** = escalate on an UNREACHABLE state

If you specify **d** in this field, the escalation will only be used if the host is in a DOWN state.

---

## 18.4.13 Extended Host Information Definition

### 18.4.13.1 Description

Extended host information entries are basically used to make the output from the [status](#), [statusmap](#), [statuswrl](#), and [extinfo](#) CGIs look pretty. They have no effect on monitoring and are completely optional.

#### Tip

As of Nagios 3.x, all directives contained in extended host information definitions are also available in [host definitions](#). Thus, you can choose to define the directives below in your host definitions if it makes your configuration simpler. Separate extended host information definitions will continue to be supported for backward compatability.

### 18.4.13.2 Definition Format

#### Note

Variables in red are required, while those in black are optional. However, you need to supply at least one optional variable in each definition for it to be of much use.

|                     |                                |
|---------------------|--------------------------------|
| define hostextinfo{ |                                |
| host_name           | <i>host_name</i>               |
| notes               | <i>note_string</i>             |
| notes_url           | <i>url</i>                     |
| action_url          | <i>url</i>                     |
| icon_image          | <i>image_file</i>              |
| icon_image_alt      | <i>alt_string</i>              |
| vrml_image          | <i>image_file</i>              |
| statusmap_image     | <i>image_file</i>              |
| 2d_coords           | <i>x_coord,y_coord</i>         |
| 3d_coords           | <i>x_coord,y_coord,z_coord</i> |
| }                   |                                |

### 18.4.13.3 Example Definition:

```
define hostextinfo{
 host_name netware1
 notes This is the primary Netware file server
 notes_url http://webserver.localhost.localdomain/hostinfo.pl?host=netware1
 icon_image novell40.png
 icon_image_alt IntranetWare 4.11
 vrml_image novell40.png
 statusmap_image novell40.gd2
 2d_coords 100,250
 3d_coords 100.0,50.0,75.0
}
```

### 18.4.13.4 Variable Descriptions

**host\_name** This variable is used to identify the *short name* of the [host](#) which the data is associated with.

**notes** This directive is used to define an optional string of notes pertaining to the host. If you specify a note here, you will see the it in the [extended information](#) CGI (when you are viewing information about the specified host).

**notes\_url** This variable is used to define an optional URL that can be used to provide more information about the host. If you specify an URL, you will see a link that says ‘Extra Host Notes’ in the **extended information** CGI (when you are viewing information about the specified host). Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. `/cgi-bin/nagios/`). This can be very useful if you want to make detailed information on the host, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the host. If you specify an URL, you will see a link that says ‘Extra Host Actions’ in the **extended information** CGI (when you are viewing information about the specified host). Any valid URL can be used. If you plan on using relative paths, the base path will be the same as what is used to access the CGIs (i.e. `/cgi-bin/nagios/`).

**icon\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this host. This image will be displayed in the **status** and **extended information** CGIs. The image will look best if it is 40x40 pixels in size. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. `/usr/local/nagios/share/images/logos/`).

**icon\_image\_alt** This variable is used to define an optional string that is used in the ALT tag of the image specified by the `<icon_image>` argument. The ALT tag is used in the **status**, **extended information** and **statusmap** CGIs.

**vrml\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this host. This image will be used as the texture map for the specified host in the **statuswrl** CGI. Unlike the image you use for the `<icon_image>` variable, this one should probably *not* have any transparency. If it does, the host object will look a bit weird. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. `/usr/local/nagios/share/images/logos/`).

**statusmap\_image** This variable is used to define the name of an image that should be associated with this host in the **statusmap** CGI. You can specify a JPEG, PNG, and GIF image if you want, although I would strongly suggest using a GD2 format image, as other image formats will result in a lot of wasted CPU time when the statusmap image is generated. GD2 images can be created from PNG images by using the **pngtogd2** utility supplied with Thomas Boutell’s **gd library**. The GD2 images should be created in *uncompressed* format in order to minimize CPU load when the statusmap CGI is generating the network map image. The image will look best if it is 40x40 pixels in size. You can leave these option blank if you are not using the statusmap CGI. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. `/usr/local/nagios/share/images/logos/`).

**2d\_coords** This variable is used to define coordinates to use when drawing the host in the **statusmap** CGI. Coordinates should be given in positive integers, as they correspond to physical pixels in the generated image. The origin for drawing (0,0) is in the upper left hand corner of the image and extends in the positive x direction (to the right) along the top of the image and in the positive y direction (down) along the left hand side of the image. For reference, the size of the icons drawn is usually about 40x40 pixels (text takes a little extra space). The coordinates you specify here are for the upper left hand corner of the host icon that is drawn.

---

**Note**

Don’t worry about what the maximum x and y coordinates that you can use are. The CGI will automatically calculate the maximum dimensions of the image it creates based on the largest x and y coordinates you specify.

---

**3d\_coords** This variable is used to define coordinates to use when drawing the host in the **statuswrl** CGI. Coordinates can be positive or negative real numbers. The origin for drawing is (0.0,0.0,0.0). For reference, the size of the host cubes drawn is 0.5 units on each side (text takes a little more space). The coordinates you specify here are used as the center of the host cube.

## 18.4.14 Extended Service Information Definition

### 18.4.14.1 Description

Extended service information entries are basically used to make the output from the **status** and **extinfo** CGIs look pretty. They have no effect on monitoring and are completely optional.

---



**Tip**

As of Nagios 3.x, all directives contained in extended service information definitions are also available in **service definitions**. Thus, you can choose to define the directives below in your service definitions if it makes your configuration simpler. Separate extended service information definitions will continue to be supported for backward compatability.

**18.4.14.2 Definition Format****Note**

Variables in red are required, while those in black are optional. However, you need to supply at least one optional variable in each definition for it to be of much use.

|                        |                            |
|------------------------|----------------------------|
| define serviceextinfo{ |                            |
| host_name              | <i>host_name</i>           |
| service_description    | <i>service_description</i> |
| notes                  | <i>note_string</i>         |
| notes_url              | <i>url</i>                 |
| action_url             | <i>url</i>                 |
| icon_image             | <i>image_file</i>          |
| icon_image_alt         | <i>alt_string</i>          |
| }                      |                            |

**18.4.14.3 Example Definition**

```
define serviceextinfo{
 host_name linux2
 service_description Log Anomalies
 notes Security-related log anomalies on secondary Linux server
 notes_url http://webserver.localhost.localdomain/serviceinfo.pl?host= ↵
 linux2&service=Log+Anomalies
 icon_image security.png
 icon_image_alt Security-Related Alerts
}
```

**18.4.14.4 Variable Descriptions**

**host\_name** This directive is used to identify the *short name* of the host that the **service** is associated with.

**service\_description** This directive is description of the **service** which the data is associated with.

**notes** This directive is used to define an optional string of notes pertaining to the service. If you specify a note here, you will see the it in the **extended information** CGI (when you are viewing information about the specified service).

**notes\_url** This directive is used to define an optional URL that can be used to provide more information about the service. If you specify an URL, you will see a link that says 'Extra Service Notes' in the **extended information** CGI (when you are viewing information about the specified service). Any valid URL can be used. If you plan on using relative paths, the base path will the the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*). This can be very useful if you want to make detailed information on the service, emergency contact methods, etc. available to other support staff.

**action\_url** This directive is used to define an optional URL that can be used to provide more actions to be performed on the service. If you specify an URL, you will see a link that says 'Extra Service Actions' in the **extended information** CGI (when you are viewing information about the specified service). Any valid URL can be used. If you plan on using relative paths, the base path will the the same as what is used to access the CGIs (i.e. */cgi-bin/nagios/*).

**icon\_image** This variable is used to define the name of a GIF, PNG, or JPG image that should be associated with this host. This image will be displayed in the **status** and **extended information** CGIs. The image will look best if it is 40x40 pixels in size. Images for hosts are assumed to be in the **logos/** subdirectory in your HTML images directory (i.e. `/usr/local/nagios/share/images/logos`).

**icon\_image\_alt** This variable is used to define an optional string that is used in the ALT tag of the image specified by the `<icon_image>` argument. The ALT tag is used in the **status**, **extended information** and **statusmap** CGIs.

---

## Chapter 19

# Custom Object Variables

### 19.1 Introduction

Users often request that new variables be added to host, service, and contact definitions. These include variables for `SNMP` community, MAC address, AIM username, Skype number, and street address. The list is endless. The problem that I see with doing this is that it makes Nagios less generic and more infrastructure-specific. Nagios was intended to be flexible, which meant things needed to be designed in a generic manner. Host definitions in Nagios, for example, have a generic "address" variable that can contain anything from an IP address to human-readable driving directions - whatever is appropriate for the user's setup.

Still, there needs to be a method for admins to store information about their infrastructure components in their Nagios configuration without imposing a set of specific variables on others. Nagios attempts to solve this problem by allowing users to define custom variables in their object definitions. Custom variables allow users to define additional properties in their host, service, and contact definitions, and use their values in notifications, event handlers, and host and service checks.

### 19.2 Custom Variable Basics

There are a few important things that you should note about custom variables:

- Custom variable names must begin with an underscore (`_`) to prevent name collision with standard variables
- Custom variable names are case-insensitive
- Custom variables are **inherited** from object templates like normal variables
- Scripts can reference custom variable values with **macros and environment variables**

### 19.3 Examples

Here's an example of how custom variables can be defined in different types of object definitions:

```
define host{
 host_name linuxserver
 _mac_address 00:06:5B:A6:AD:AA ; <-- Custom MAC_ADDRESS variable
 _rack_number R32 ; <-- Custom RACK_NUMBER variable
 ...
}
```

```

define service{
 host_name linuxserver
 description Memory Usage
 _SNMP_community public ; <-- Custom SNMP_COMMUNITY variable
 _TechContact Jane Doe ; <-- Custom TECHCONTACT variable

}

define contact{
 contact_name john
 _AIM_username john16 ; <-- Custom AIM_USERNAME variable
 _YahooID john32 ; <-- Custom YAHOOID variable
 ...
}

```

## 19.4 Custom Variables As Macros

Custom variable values can be referenced in scripts and executables that Nagios runs for checks, notifications, etc. by using **macros** or environment variables.

In order to prevent name collision among custom variables from different object types, Nagios prepends ‘\_HOST’, ‘\_SERVICE’, or ‘\_CONTACT’ to the beginning of custom host, service, or contact variables, respectively, in macro and environment variable names. The table below shows the corresponding macro and environment variable names for the custom variables that were defined in the example above.

| Object Type | Variable Name  | Macro Name                 | Environment Variable          |
|-------------|----------------|----------------------------|-------------------------------|
| Host        | MAC_ADDRESS    | \$_HOSTMAC_ADDRESS\$       | NAGIOS__HOSTMAC_ADDRESS       |
| Host        | RACK_NUMBER    | \$_HOSTRACK_NUMBER\$       | NAGIOS__HOSTRACK_NUMBER       |
| Service     | SNMP_COMMUNITY | \$_SERVICESNMP_COMMUNITY\$ | NAGIOS__SERVICESNMP_COMMUNITY |
| Service     | TECHCONTACT    | \$_SERVICETECHCONTACT\$    | NAGIOS__SERVICETECHCONTACT    |
| Contact     | AIM_USERNAME   | \$_CONTACTAIM_USERNAME\$   | NAGIOS__CONTACTAIM_USERNAME   |
| Contact     | YAHOOID        | \$_CONTACTYAHOOID\$        | NAGIOS__CONTACTYAHOOID        |

## 19.5 Custom Variables And Inheritance

Custom object variables are **inherited** just like standard host, service, or contact variables.

## Chapter 20

# CGI Configuration File Options

---

### Note

When creating and/or editing configuration files, keep the following in mind:

- Lines that start with a '#' character are taken to be comments and are not processed
  - Variables names must begin at the start of the line - no white space is allowed before the name
  - Variable names are case-sensitive
- 

## 20.1 Sample Configuration

---

### Tip

A sample CGI configuration file (`/usr/local/nagios/etc/cgi.cfg`) is installed for you when you follow the [quickstart installation guide](#).

---

## 20.2 Config File Location

By default, Nagios expects the CGI configuration file to be named `cgi.cfg` and located in the config file directory along with the [main config file](#). If you need to change the name of the file or its location, you can configure Apache to pass an environment variable named `NAGIOS_CGI_CONFIG` (which points to the correct location) to the CGIs. See the Apache documentation for information on how to do this.

## 20.3 Configuration File Variables

Below you will find descriptions of each main Nagios configuration file option...

### 20.3.1 Main Configuration File Location

|          |                                                                |
|----------|----------------------------------------------------------------|
| Format:  | <code>main_config_file=&lt;file_name&gt;</code>                |
| Example: | <code>main_config_file=/usr/local/nagios/etc/nagios.cfg</code> |

---

This specifies the location of your **main configuration file**. The CGIs need to know where to find this file in order to get information about configuration information, current host and service status, etc.

### 20.3.2 Physical HTML Path

|          |                                                         |
|----------|---------------------------------------------------------|
| Format:  | <code>physical_html_path=&lt;path&gt;</code>            |
| Example: | <code>physical_html_path=/usr/local/nagios/share</code> |

This is the physical path where the HTML files for Nagios are kept on your workstation or server. Nagios assumes that the documentation and images files (used by the CGIs) are stored in subdirectories called `docs/` and `images/`, respectively.

### 20.3.3 URL HTML Path

|          |                                         |
|----------|-----------------------------------------|
| Format:  | <code>url_html_path=&lt;path&gt;</code> |
| Example: | <code>url_html_path=/nagios</code>      |

If, when accessing Nagios via a web browser, you point to an URL like `http://www.myhost.com/nagios`, this value should be `/nagios`. Basically, its the path portion of the URL that is used to access the Nagios HTML pages.

### 20.3.4 Authentication Usage

|          |                                             |
|----------|---------------------------------------------|
| Format:  | <code>use_authentication=&lt;0/1&gt;</code> |
| Example: | <code>use_authentication=1</code>           |

This option controls whether or not the CGIs will use the authentication and authorization functionality when determining what information and commands users have access to. I would strongly suggest that you use the authentication functionality for the CGIs. If you decide not to use authentication, make sure to remove the **command CGI** to prevent unauthorized users from issuing commands to Nagios. The CGI will not issue commands to Nagios if authentication is disabled, but I would suggest removing it altogether just to be on the safe side. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

- 0 = Don't use authentication functionality
- 1 = Use authentication and authorization functionality (default)

### 20.3.5 Default User Name

|          |                                                 |
|----------|-------------------------------------------------|
| Format:  | <code>default_user_name=&lt;username&gt;</code> |
| Example: | <code>default_user_name=guest</code>            |

Setting this variable will define a default username that can access the CGIs. This allows people within a secure domain (i.e., behind a firewall) to access the CGIs without necessarily having to authenticate to the web server. You may want to use this to avoid having to use basic authentication if you are not using a secure server, as basic authentication transmits passwords in clear text over the Internet.



#### Important

Do not define a default username unless you are running a secure web server and are sure that everyone who has access to the CGIs has been authenticated in some manner! If you define this variable, anyone who has not authenticated to the web server will inherit all rights you assign to this user!

### 20.3.6 System/Process Information Access

|          |                                                                                             |
|----------|---------------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_system_information=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_system_information=nagiosadmin,theboss</code>                          |

This is a comma-delimited list of names of authenticated users who can view system/process information in the **extended information CGI**. Users in this list are not automatically authorized to issue system/process commands. If you want users to be able to issue system/process commands as well, you must add them to the **authorized\_for\_system\_commands** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.7 System/Process Command Access

|          |                                                                                          |
|----------|------------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_system_commands=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_system_commands=nagiosadmin</code>                                  |

This is a comma-delimited list of names of authenticated users who can issue system/process commands via the **command CGI**. Users in this list are not automatically authorized to view system/process information. If you want users to be able to view system/process information as well, you must add them to the **authorized\_for\_system\_information** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.8 Configuration Information Access

|          |                                                                                                    |
|----------|----------------------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_configuration_information=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_configuration_information=nagiosadmin</code>                                  |

This is a comma-delimited list of names of authenticated users who can view configuration information in the **configuration CGI**. Users in this list can view information on all configured hosts, host groups, services, contacts, contact groups, time periods, and commands. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.9 Global Host Information Access

|          |                                                                                    |
|----------|------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_all_hosts=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_all_hosts=nagiosadmin,theboss</code>                          |

This is a comma-delimited list of names of authenticated users who can view status and configuration information for all hosts. Users in this list are also automatically authorized to view information for all services. Users in this list are not automatically authorized to issue commands for all hosts or services. If you want users able to issue commands for all hosts and services as well, you must add them to the **authorized\_for\_all\_host\_commands** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.10 Global Host Command Access

|          |                                                                                            |
|----------|--------------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_all_host_commands=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_all_host_commands=nagiosadmin</code>                                  |

This is a comma-delimited list of names of authenticated users who can issue commands for all hosts via the **command CGI**. Users in this list are also automatically authorized to issue commands for all services. Users in this list are not automatically authorized to view status or configuration information for all hosts or services. If you want users able to view status and configuration information for all hosts and services as well, you must add them to the **authorized\_for\_all\_hosts** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.11 Global Service Information Access

|          |                                                                                       |
|----------|---------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_all_services=&lt;user1&gt;,&lt;user2&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_all_services=nagiosadmin,theboss</code>                          |

This is a comma-delimited list of names of authenticated users who can view status and configuration information for all services. Users in this list are not automatically authorized to view information for all hosts. Users in this list are not automatically authorized to issue commands for all services. If you want users able to issue commands for all services as well, you must add them to the **authorized\_for\_all\_service\_commands** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.12 Global Service Command Access

|          |                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------|
| Format:  | <code>authorized_for_all_service_commands=&lt;user1&gt;,&lt;user2&gt;,&lt;user3&gt;,...&lt;usern&gt;</code> |
| Example: | <code>authorized_for_all_service_commands=nagiosadmin</code>                                                |

This is a comma-delimited list of names of authenticated users who can issue commands for all services via the **command CGI**. Users in this list are not automatically authorized to issue commands for all hosts. Users in this list are not automatically authorized to view status or configuration information for all hosts. If you want users able to view status and configuration information for all services as well, you must add them to the **authorized\_for\_all\_services** variable. More information on how to setup authentication and configure authorization for the CGIs can be found [here](#).

### 20.3.13 Lock Author Names

|          |                                      |
|----------|--------------------------------------|
| Format:  | <code>lock_author_names=[0/1]</code> |
| Example: | <code>lock_author_names=1</code>     |

This option allows you to restrict users from changing the author name when submitting comments, acknowledgements, and scheduled downtime from the web interface. If this option is enabled, users will be unable to change the author name associated with the command request.

- 0 = Allow users to change author names when submitting commands
- 1 = Prevent users from changing author names (default)

### 20.3.14 Statusmap CGI Background Image

|          |                                                            |
|----------|------------------------------------------------------------|
| Format:  | <code>statusmap_background_image=&lt;image_file&gt;</code> |
| Example: | <code>statusmap_background_image=smbbackground.gd2</code>  |

This option allows you to specify an image to be used as a background in the **statusmap CGI** if you use the user-supplied coordinates layout method. The background image is not be available in any other layout methods. It is assumed that the image resides in the HTML images path (i.e. `/usr/local/nagios/share/images`). This path is automatically determined by



appending '/images' to the path specified by the `physical_html_path` directive.

---

**Note**

The image file can be in GIF, JPEG, PNG, or GD2 format. However, GD2 format (preferably in uncompressed format) is recommended, as it will reduce the CPU load when the CGI generates the map image.

---

### 20.3.15 Default Statusmap Layout Method

|          |                                                             |
|----------|-------------------------------------------------------------|
| Format:  | <code>default_statusmap_layout=&lt;layout_number&gt;</code> |
| Example: | <code>default_statusmap_layout=4</code>                     |

This option allows you to specify the default layout method used by the `statusmap CGI`. Valid options are:

| <layout_number> Value | Layout Method            |
|-----------------------|--------------------------|
| 0                     | User-defined coordinates |
| 1                     | Depth layers             |
| 2                     | Collapsed tree           |
| 3                     | Balanced tree            |
| 4                     | Circular                 |
| 5                     | Circular (Marked Up)     |
| 6                     | Circular (Balloon)       |

### 20.3.16 Statuswrl CGI Include World

|          |                                                  |
|----------|--------------------------------------------------|
| Format:  | <code>statuswrl_include=&lt;vrml_file&gt;</code> |
| Example: | <code>statuswrl_include=myworld.wrl</code>       |

This option allows you to include your own objects in the generated VRML world. It is assumed that the file resides in the path specified by the `physical_html_path` directive.

---

**Note**

This file must be a fully qualified VRML world (i.e. you can view it by itself in a VRML browser).

---

### 20.3.17 Default Statuswrl Layout Method

|          |                                                             |
|----------|-------------------------------------------------------------|
| Format:  | <code>default_statuswrl_layout=&lt;layout_number&gt;</code> |
| Example: | <code>default_statuswrl_layout=4</code>                     |

This option allows you to specify the default layout method used by the `statuswrl CGI`. Valid options are:

| <layout_number> Value | Layout Method                   |
|-----------------------|---------------------------------|
| <b>0</b>              | <b>User-defined coordinates</b> |
| 2                     | Collapsed tree                  |
| 3                     | Balanced tree                   |
| 4                     | Circular                        |

---

### 20.3.18 CGI Refresh Rate

|          |                                |
|----------|--------------------------------|
| Format:  | refresh_rate=<rate_in_seconds> |
| Example: | refresh_rate=90                |

This option allows you to specify the number of seconds between page refreshes for the **status**, **statusmap**, and **extinfo** CGIs.

### 20.3.19 Audio Alerts

|           |                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Formats:  | host_unreachable_sound=<sound_file> host_down_sound=<sound_file><br>service_critical_sound=<sound_file> service_warning_sound=<sound_file><br>service_unknown_sound=<sound_file> |
| Examples: | host_unreachable_sound=hostu.wav host_down_sound=hostd.wav<br>service_critical_sound=critical.wav service_warning_sound=warning.wav<br>service_unknown_sound=unknown.wav         |

These options allow you to specify an audio file that should be played in your browser if there are problems when you are viewing the **status CGI**. If there are problems, the audio file for the most critical type of problem will be played. The most critical type of problem is on or more unreachable hosts, while the least critical is one or more services in an unknown state (see the order in the example above). Audio files are assumed to be in the `media/` subdirectory in your HTML directory (i.e. `/usr/local/nagios/share/media`).

### 20.3.20 Ping Syntax

|          |                                                  |
|----------|--------------------------------------------------|
| Format:  | ping_syntax=<command>                            |
| Example: | ping_syntax=/bin/ping -n -U -c 5 \$HOSTADDRESS\$ |

This option determines what syntax should be used when attempting to ping a host from the WAP interface (using the **statuswml CGI**). You must include the full path to the ping binary, along with all required options. The `$HOSTADDRESS$` macro is substituted with the address of the host before the command is executed.

### 20.3.21 Escape HTML Tags Option

|          |                        |
|----------|------------------------|
| Format:  | escape_html_tags=[0/1] |
| Example: | escape_html_tags=1     |

This option determines whether or not HTML tags in host and service (plugin) output is escaped in the CGIs. If you enable this option, your plugin output will not be able to contain clickable hyperlinks.

### 20.3.22 Notes URL Target

|          |                           |
|----------|---------------------------|
| Format:  | notes_url_target=[target] |
| Example: | notes_url_target=_blank   |

This option determines the name of the frame target that notes URLs should be displayed in. Valid options include `_blank`, `_self`, `_top`, `_parent`, or any other valid target name.

### 20.3.23 Action URL Target

|          |                                         |
|----------|-----------------------------------------|
| Format:  | <code>action_url_target=[target]</code> |
| Example: | <code>action_url_target=_blank</code>   |

This option determines the name of the frame target that action URLs should be displayed in. Valid options include `_blank`, `_self`, `_top`, `_parent`, or any other valid target name.

### 20.3.24 Splunk Integration Option

|          |                                              |
|----------|----------------------------------------------|
| Format:  | <code>enable_splunk_integration=[0/1]</code> |
| Example: | <code>enable_splunk_integration=1</code>     |

This option determines whether integration functionality with Splunk is enabled in the web interface. If enabled, you'll be presented with 'Splunk It' links in various places in the CGIs (log file, alert history, host/service detail, etc). Useful if you're trying to research why a particular problem occurred. For more information on Splunk, visit <http://www.splunk.com/>.

### 20.3.25 Splunk URL

|          |                                                |
|----------|------------------------------------------------|
| Format:  | <code>splunk_url=&lt;path&gt;</code>           |
| Example: | <code>splunk_url=http://127.0.0.1:8000/</code> |

This option is used to define the base URL to your Splunk interface. This URL is used by the CGIs when creating links if the `enable_splunk_integration` option is enabled.

## Chapter 21

# Authentication And Authorization In The CGIs

### 21.1 Introduction

This documentation describes how the Nagios CGIs decide who has access to view monitoring and configuration information, and who can submit commands to the Nagios daemon through the web interface.

### 21.2 Definitions

Before continuing, it is important that you understand the meaning of and difference between authenticated users and authenticated contacts:

- An authenticated user is an someone who has authenticated to the web server with a username and password and has been granted access to the Nagios web interface.
- An authenticated contact is an authenticated user whose username matches the short name of a **contact definition**.

### 21.3 Setting Up Authenticated Users

Assuming you configured your web server as described in the **Quickstart installation guide**quickstart guide, it should require that you authenticate before accessing the Nagios CGIs. You should also have one user account (nagiosadmin) that can access the CGIs.

As you define more **contacts** for receiving host and service notifications, you'll most likely want to let them access the Nagios web interface. You can use the following command to add additional users who can authenticate to the CGIs. Replace <username> with the actual username you want to add. In most cases, the username should match the short name of a **contact** that has been defined.

```
linux:~ # htpasswd /usr/local/nagios/etc/htpasswd.users <username>
```

### 21.4 Enabling Authentication/Authorization Functionality In The CGIs

The next thing you need to do is make sure that the CGIs are configured to use the authentication and authorization functionality in determining what information and/or commands users have access to. This is done by setting the **use\_authentication** variable in the **CGI Configuration File Options**CGI configuration file to a non-zero value. Example:

```
use_authentication=1
```

Okay, you're now done with setting up basic authentication/authorization functionality in the CGIs.

## 21.5 Default Permissions To CGI Information

So what default permissions do users have in the CGIs by default when the authentication/authorization functionality is enabled?

| CGI Data                          | Authenticated Contacts* | Other Authenticated Users* |
|-----------------------------------|-------------------------|----------------------------|
| Host Status Information           | Yes                     | No                         |
| Host Configuration Information    | Yes                     | No                         |
| Host History                      | Yes                     | No                         |
| Host Notifications                | Yes                     | No                         |
| Host Commands                     | Yes                     | No                         |
| Service Status Information        | Yes                     | No                         |
| Service Configuration Information | Yes                     | No                         |
| Service History                   | Yes                     | No                         |
| Service Notifications             | Yes                     | No                         |
| Service Commands                  | Yes                     | No                         |
| All Configuration Information     | No                      | No                         |
| System/Process Information        | No                      | No                         |
| System/Process Commands           | No                      | No                         |

Authenticated contacts\* are granted the following permissions for each service for which they are contacts (but not for services for which they are not contacts)...

- Authorization to view service status information
- Authorization to view service configuration information
- Authorization to view history and notifications for the service
- Authorization to issue service commands

Authenticated contacts\* are granted the following permissions for each host for which they are contacts (but not for hosts for which they are not contacts)...

- Authorization to view host status information
- Authorization to view host configuration information
- Authorization to view history and notifications for the host
- Authorization to issue host commands
- Authorization to view status information for all services on the host
- Authorization to view configuration information for all services on the host
- Authorization to view history and notification information for all services on the host
- Authorization to issue commands for all services on the host

It is important to note that by default no one is authorized for the following...

- Viewing the raw log file via the [showlog CGI](#)
- Viewing Nagios process information via the [extended information CGI](#)
- Issuing Nagios process commands via the [command CGI](#)
- Viewing host group, contact, contact group, time period, and command definitions via the [configuration CGI](#)

You will undoubtedly want to access this information, so you'll have to assign additional rights for yourself (and possibly other users) as described below...

## 21.6 Granting Additional Permissions To CGI Information

You can grant authenticated contacts or other authenticated users permission to additional information in the CGIs by adding them to various authorization variables in the [CGI configuration file](#). I realize that the available options don't allow for getting really specific about particular permissions, but its better than nothing..

Additional authorization can be given to users by adding them to the following variables in the CGI configuration file...

- [authorized\\_for\\_system\\_information](#)
- [authorized\\_for\\_system\\_commands](#)
- [authorized\\_for\\_configuration\\_information](#)
- [authorized\\_for\\_all\\_hosts](#)
- [authorized\\_for\\_all\\_host\\_commands](#)
- [authorized\\_for\\_all\\_services](#)
- [authorized\\_for\\_all\\_service\\_commands](#)

## 21.7 CGI Authorization Requirements

If you are confused about the authorization needed to access various information in the CGIs, read the Authorization Requirements section for each CGI as described [here](#).

## 21.8 Authentication On Secured Web Servers

If your web server is located in a secure domain (i.e., behind a firewall) or if you are using SSL, you can define a default username that can be used to access the CGIs. This is done by defining the [default\\_user\\_name](#) option in the [CGI configuration file](#). By defining a default username that can access the CGIs, you can allow users to access the CGIs without necessarily having to authenticate to the web server. You may want to use this to avoid having to use basic web authentication, as basic authentication transmits passwords in clear text over the Internet.



### Important

Do not define a default username unless you are running a secure web server and are sure that everyone who has access to the CGIs has been authenticated in some manner. If you define this variable, anyone who has not authenticated to the web server will inherit all rights you assign to this user!

---

## **Part IV**

# **Running Nagios**

---

## Chapter 22

# Verifying Your Configuration

### 22.1 Verifying Your Configuration

Every time you modify your [Configuration Overview](#), you should run a sanity check on them. It is important to do this before you (re)start Nagios, as Nagios will shut down if your configuration contains errors.

In order to verify your configuration, run Nagios with the `-v` command line option like so:

```
linux:~ # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

If you've forgotten to enter some critical data or misconfigured things, Nagios will spit out a warning or error message that should point you to the location of the problem. Error messages generally print out the line in the configuration file that seems to be the source of the problem. On errors, Nagios will often exit the pre-flight check and return to the command prompt after printing only the first error that it has encountered. This is done so that one error does not cascade into multiple errors as the remainder of the configuration data is verified. If you get any error messages you'll need to go and edit your configuration files to remedy the problem. Warning messages can generally be safely ignored, since they are only recommendations and not requirements.

Once you've verified your configuration files and fixed any errors you can go ahead and [\(re\)start Nagios](#).

---



## Chapter 23

# Starting and Stopping Nagios

There's more than one way to start, stop, and restart Nagios. Here are some of the more common ones...

---

**Tip**

Always make sure you [Verifying Your Configuration](#) before you (re)start Nagios.

---

### 23.1 Starting Nagios

1. Init Script: The easiest way to start the Nagios daemon is by using the init script like so:

```
linux:~ # /etc/rc.d/init.d/nagios start
```

2. Manually: You can start the Nagios daemon manually with the `-d` command line option like so:

```
linux:~ # /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

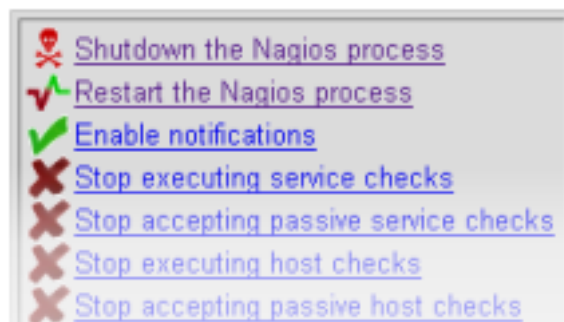
### 23.2 Restarting Nagios

Restarting/reloading is necessary when you modify your configuration files and want those changes to take effect.

1. Init Script: The easiest way to restart the Nagios daemon is by using the init script like so:

```
linux:~ # /etc/rc.d/init.d/nagios reload
```

2. Web Interface: You can restart the Nagios through the web interface by clicking the Process Info navigation link and selecting Restart the Nagios process:



3. Manually: You can restart the Nagios process by sending it a SIGHUP signal like so:

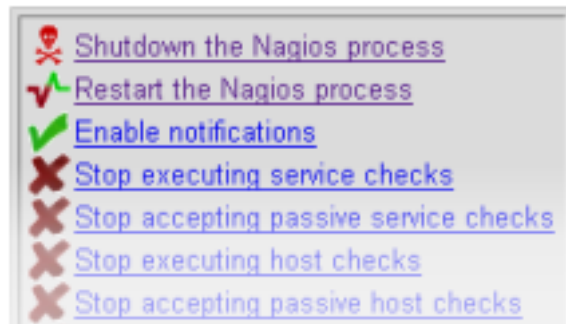
```
linux:~ # kill -HUP <nagios_pid>
```

## 23.3 Stopping Nagios

1. Init Script: The easiest way to stop the Nagios daemon is by using the init script like so:

```
linux:~ # /etc/rc.d/init.d/nagios stop
```

2. Web Interface: You can stop the Nagios through the web interface by clicking the Process Info navigation link and selecting Shutdown the Nagios process:



3. Manually: You can stop the Nagios process by sending it a SIGTERM signal like so:

```
linux:~ # kill <nagios_pid>
```

## **Part V**

# **The Basics**

---

## Chapter 24

# Nagios Plugins

### 24.1 Introduction

Unlike many other monitoring tools, Nagios does not include any internal mechanisms for checking the status of hosts and services on your network. Instead, Nagios relies on external programs (called plugins) to do all the dirty work.

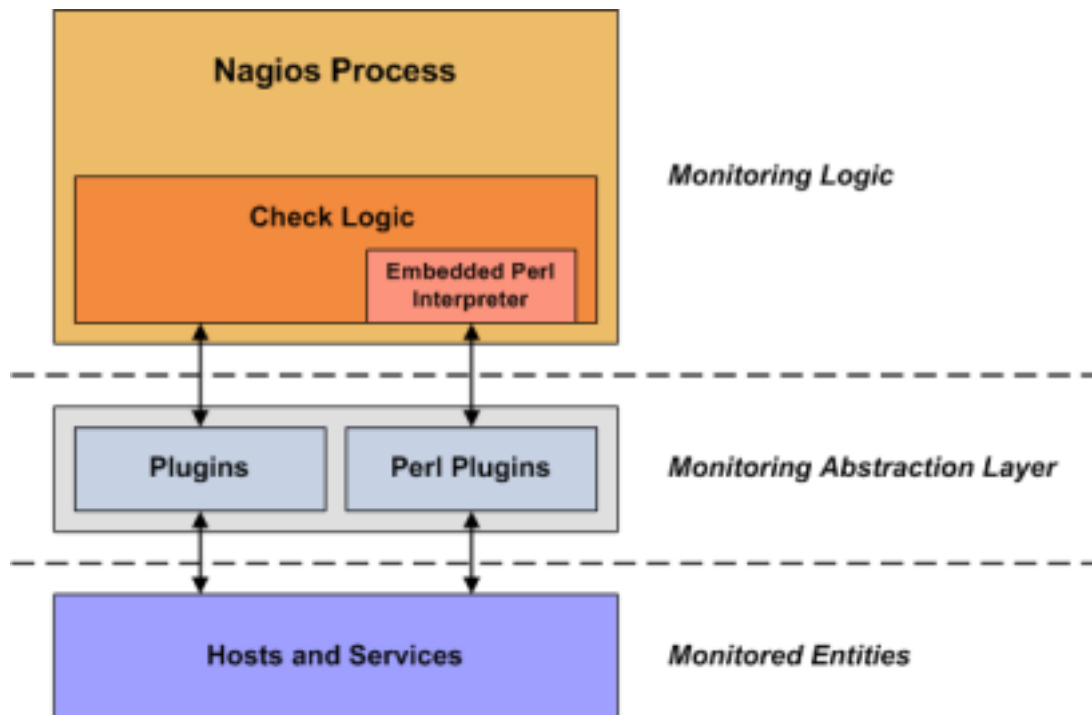
### 24.2 What Are Plugins?

Plugins are compiled executables or scripts (Perl scripts, shell scripts, etc.) that can be run from a command line to check the status of a host or service. Nagios uses the results from plugins to determine the current status of hosts and services on your network.

Nagios will execute a plugin whenever there is a need to check the status of a service or host. The plugin does something (notice the very general term) to perform the check and then simply returns the results to Nagios. Nagios will process the results that it receives from the plugin and take any necessary actions (running **event handlers**, sending out **notifications**, etc).

---

## 24.3 Plugins As An Abstraction Layer



Plugins act as an abstraction layer between the monitoring logic present in the Nagios daemon and the actual services and hosts that are being monitored.

The upside of this type of plugin architecture is that you can monitor just about anything you can think of. If you can automate the process of checking something, you can monitor it with Nagios. There are already a lot of plugins that have been created in order to monitor basic resources such as processor load, disk usage, ping rates, etc. If you want to monitor something else, take a look at the documentation on [writing plugins](#) and roll your own. Its simple!

The downside to this type of plugin architecture is the fact that Nagios has absolutely no idea what it is that you're monitoring. You could be monitoring network traffic statistics, data error rates, room temperate, CPU voltage, fan speed, processor load, disk space, or the ability of your super-fantastic toaster to properly brown your bread in the morning... Nagios doesn't understand the specifics of what's being monitored - it just tracks changes in the state of those resources. Only the plugins themselves know exactly what they're monitoring and how to perform the actual checks.

## 24.4 What Plugins Are Available?

There are plugins currently available to monitor many different kinds of devices and services, including:

- HTTP, POP3, IMAP, FTP, SSH, DHCP
- CPU Load, Disk Usage, Memory Usage, Current Users
- Unix/Linux, Windows, and Netware Servers
- Routers and Switches
- etc.

## 24.5 Obtaining Plugins

Plugins are not distributed with Nagios, but you can download the official Nagios plugins and many additional plugins created and maintained by Nagios users from the following locations:

- Nagios Plugins Project: <http://nagiosplug.sourceforge.net/>
- Nagios Downloads Page: <http://www.nagios.org/download/>
- NagiosExchange.org: <http://www.nagiosexchange.org/>

## 24.6 How Do I Use Plugin X?

Most all plugins will display basic usage information when you execute them using `-h` or `--help` on the command line. For example, if you want to know how the **check\_http** plugin works or what options it accepts, you should try executing the following command: `./check_http --help`

## 24.7 Plugin API

You can find information on the technical aspects of plugins, as well as how to go about creating your own custom plugins [here](#).

---

## Chapter 25

# Understanding Macros and How They Work

### 25.1 Macros

One of the main features that make Nagios so flexible is the ability to use macros in command definitions. Macros allow you to reference information from hosts, services, and other sources in your commands.

### 25.2 Macro Substitution - How Macros Work

Before Nagios executes a command, it will replace any macros it finds in the command definition with their corresponding values. This macro substitution occurs for all types of commands that Nagios executes - host and service checks, notifications, event handlers, etc.

Certain macros may themselves contain other macros. These include the `$HOSTNOTES$`, `$HOSTNOTESURL$`, `$HOSTACTIONURL$`, `$SERVICENOTES$`, `$SERVICENOTESURL$`, and `$SERVICEACTIONURL$` macros.

### 25.3 Example 1: Host Address Macro

When you use host and service macros in command definitions, they refer to values for the host or service for which the command is being run. Let's try an example. Assuming we are using a host definition and a `check_ping` command defined like this:

```
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ linuxbox
~ ~ ~ ~ address ~ ~ ~ ~ 192.168.1.2
~ ~ ~ ~ check_command ~ check_ping
~ ~ ~ ~ ...
~ ~ ~ ~ }
~ ~ ~ ~
define command{
~ ~ ~ ~ command_name ~ ~check_ping
~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/check_ping -H $HOSTADDRESS$ -w ↔
100.0,90% -c 200.0,60%
~ ~ ~ ~ }
```

the expanded/final command line to be executed for the host's check command would look like this:

```
/usr/local/nagios/libexec/check_ping -H 192.168.1.2 -w 100.0,90% -c 200.0,60%
```

Pretty simple, right? The beauty in this is that you can use a single command definition to check an unlimited number of hosts. Each host can be checked with the same command definition because each host's address is automatically substituted in the command line before execution.

## 25.4 Example 2: Command Argument Macros

You can pass arguments to commands as well, which is quite handy if you'd like to keep your command definitions rather generic. Arguments are specified in the object (i.e. host or service) definition, by separating them from the command name with exclamation points (!) like so:

```
define service{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ linuxbox
 ~ ~ ~ ~ service_description ~ ~ PING
 ~ ~ ~ ~ check_command ~ check_ping!200.0,80%!400.0,40%
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```

In the example above, the service check command has two arguments (which can be referenced with **\$ARGn\$** macros). The **\$ARG1\$** macro will be "200.0,80%" and **\$ARG2\$** will be "400.0,40%" (both without quotes). Assuming we are using the host definition given earlier and a **check\_ping** command defined like this:

```
define command{
 ~ ~ ~ ~ command_name ~ ~check_ping
 ~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/check_ping -H $HOSTADDRESS$ -w $ARG1$ ←
 -c $ARG2$
 ~ ~ ~ ~ }
```

the expanded/final command line to be executed for the service's check command would look like this:

```
/usr/local/nagios/libexec/check_ping -H 192.168.1.2 -w 200.0,80% -c 400.0,40%
```

### Tip

If you need to pass bang (!) characters in your command arguments, you can do so by escaping them with a backslash (\). If you need to include backslashes in your command arguments, they should also be escaped with a backslash.

## 25.5 On-Demand Macros

Normally when you use host and service macros in command definitions, they refer to values for the host or service for which the command is being run. For instance, if a host check command is being executed for a host named "linuxbox", all the **standard host macros** will refer to values for that host ("linuxbox").

If you would like to reference values for another host or service in a command (for which the command is not being run), you can use what are called "on-demand" macros. On-demand macros look like normal macros, except for the fact that they contain an identifier for the host or service from which they should get their value. Here's the basic format for on-demand macros:

- **\$HOSTMACRONAME:host\_name\$**
- **\$SERVICEMACRONAME:host\_name:service\_description\$**

Replace **HOSTMACRONAME** and **SERVICEMACRONAME** with the name of one of the standard host or service macros found [here](#).

Note that the macro name is separated from the host or service identifier by a colon (:). For on-demand service macros, the service identifier consists of both a host name and a service description - these are separated by a colon (:) as well.

### Tip

On-demand service macros can contain an empty host name field. In this case the name of the host associated with the service will automatically be used.



Examples of on-demand host and service macros follow:

```
$HOSTDOWNTIME:myhost$ <--- On-demand host macro
$SERVICESTATEID:novellserver:DS Database$ <--- On-demand service macro
$SERVICESTATEID::CPU Load$ <--- On-demand service macro with blank host name field
```

On-demand macros are also available for hostgroup, servicegroup, contact, and contactgroup macros. For example:

```
$CONTACTEMAIL:john$ <--- On-demand contact macro
$CONTACTGROUPMEMBERS:linux-admins$ <--- On-demand contactgroup macro
$HOSTGROUPALIAS:linux-servers$ <--- On-demand hostgroup macro
$SERVICEGROUPALIAS:DNS-Cluster$ <--- On-demand servicegroup macro
```

## 25.6 On-Demand Group Macros

You can obtain the values of a macro across all contacts, hosts, or services in a specific group by using a special format for your on-demand macro declaration. You do this by referencing a specific host group, service group, or contact group name in an on-demand macro, like so:

- `$HOSTMACRONAME:hostgroup_name:delimiter$`
- `$SERVICEMACRONAME:servicegroup_name:delimiter$`
- `$CONTACTMACRONAME:contactgroup_name:delimiter$`

Replace `HOSTMACRONAME`, `SERVICEMACRONAME`, and `CONTACTMACRONAME` with the name of one of the standard host, service, or contact macros found [here](#). The delimiter you specify is used to separate macro values for each group member.

For example, the following macro will return a comma-separated list of host state ids for hosts that are members of the `hg1` hostgroup:

```
$HOSTSTATEID:hg1:,$
```

This macro definition will return something that looks like this:

```
0, 2, 1, 1, 0, 0, 2
```

## 25.7 Custom Variable Macros

Any [custom object variables](#) that you define in host, service, or contact definitions are also available as macros. Custom variable macros are named as follows:

- `$_HOSTvarname$`
- `$_SERVICEvarname$`
- `$_CONTACTvarname$`

Take the following host definition with a custom variable called `"_MACADDRESS"`...

```
define host{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ linuxbox
 ~ ~ ~ ~ address ~ ~ ~ ~ 192.168.1.1
 ~ ~ ~ ~ _MACADDRESS ~ ~ 00:01:02:03:04:05
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```

The `_MACADDRESS` custom variable would be available in a macro called `$_HOSTMACADDRESS$`. More information on custom object variables and how they can be used in macros can be found [here](#).

## 25.8 Macro Cleansing

Some macros are stripped of potentially dangerous shell metacharacters before being substituted into commands to be executed. Which characters are stripped from the macros depends on the setting of the `illegal_macro_output_chars` directive. The following macros are stripped of potentially dangerous characters:

1. `$HOSTOUTPUT$`
2. `$LONGHOSTOUTPUT$`
3. `$HOSTPERFDATA$`
4. `$HOSTACKAUTHOR$`
5. `$HOSTACKCOMMENT$`
6. `$SERVICEOUTPUT$`
7. `$LONGSERVICEOUTPUT$`
8. `$SERVICEPERFDATA$`
9. `$SERVICEACKAUTHOR$`
10. `$SERVICEACKCOMMENT$`

## 25.9 Macros as Environment Variables

Most macros are made available as environment variables for easy reference by scripts or commands that are executed by Nagios. For purposes of security and sanity, `$USERn$` and "on-demand" host and service macros are not made available as environment variables.

Environment variables that contain standard macros are named the same as their corresponding macro names (listed [here](#)), with "NAGIOS\_" prepended to their names. For example, the `$HOSTNAME$` macro would be available as an environment variable named "NAGIOS\_HOSTNAME".

### 25.10 Available Macros

A list of all the macros that are available in Nagios, as well as a chart of when they can be used, can be found [here](#).

---

## Chapter 26

# Standard Macros in Nagios

Standard macros that are available in Nagios are listed here. On-demand macros and macros for custom variables are described [here](#).

### 26.1 Macro Validity

Although macros can be used in all commands you define, not all macros may be ‘valid’ in a particular type of command. For example, some macros may only be valid during service notification commands, whereas other may only be valid during host check commands. There are ten types of commands that Nagios recognizes and treats differently. They are as follows:

1. Service checks
2. Service notifications
3. Host checks
4. Host notifications
5. Service **event handlers** and/or a global service event handler
6. Host **event handlers** and/or a global host event handler
7. **OCSP** command
8. **OCHP** command
9. Service **performance data** commands
10. Host **performance data** commands

The tables below list all macros currently available in Nagios, along with a brief description of each and the types of commands in which they are valid. If a macro is used in a command in which it is invalid, it is replaced with an empty string. It should be noted that macros consist of all uppercase characters and are enclosed in \$ characters.

### 26.2 Macro Availability Chart

Legend:

|     |                            |
|-----|----------------------------|
| No  | The macro is not available |
| Yes | The macro is available     |

| Macro Name                    | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
|-------------------------------|----------------|-----------------------|-------------|--------------------|---------------------------------|------------------------------|-------------------|----------------|
| Host Macros: 3                |                |                       |             |                    |                                 |                              |                   |                |
| \$HOSTNAME\$                  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTDISPLAYNAME\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTALIAS\$                 | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTADDRESS\$               | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTSTATUS\$                | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTSTATE\$                 | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTSTATE\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTSTATEID\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTSTATETYPES\$            | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTATTENTION\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$MAXHOSTATTEMPTS\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTEVENTID\$               | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTEVENTID\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTPROBLEMID\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTPROBLEMID\$         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTLATECY\$                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTEXECUTIONTIME\$         | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTDURATION\$              | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTDURATIONSEC\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTDOWNTIME\$              | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTPERCENTCHANGE\$         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPNAME\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPNAME\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTCHECK\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTSTATECHANGE\$       | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOST\$                  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTDOWN\$              | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LASTHOSTREACHABLE\$         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTOUTPUT\$                | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LONGHOSTOUTPUT\$            | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTPERFDATA\$              | Yes            | Yes                   | Yes 1       | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTCHECKCOMMAND\$          | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTACKAUTHOR\$<br>8        | No             | No                    | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTACKAUTHORNAME\$<br>8    | No             | No                    | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTACKAUTHORALIAS\$<br>8   | No             | No                    | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTACKCOMMENTS\$<br>8      | No             | No                    | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTACTIONURL\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTNOTEURL\$               | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTNOTE\$                  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSERVICES\$         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSERVICESOK\$       | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSERVICESWARNINGS\$ | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSERVICESUNKNOWN\$  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSERVICESCRITICAL\$ | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |

| Macro Name                  | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
|-----------------------------|----------------|-----------------------|-------------|--------------------|---------------------------------|------------------------------|-------------------|----------------|
| Macro Name                  | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Host Group Macros:          |                |                       |             |                    |                                 |                              |                   |                |
| \$HOSTGROUPALIAS\$<br>5     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPMEMBERS\$<br>5   | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPNOTES\$<br>5     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPNOTESURL\$<br>5  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTGROUPACTIONURL\$<br>5 | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
|                             |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                  | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Service Macros:             |                |                       |             |                    |                                 |                              |                   |                |
| \$SERVICEDESC\$             | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEDISPLAYNAME\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICESTATES\$           | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICESTATEID\$          | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICESTATES\$       | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICESTATEID\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICESTATESTYPES\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEATTEMPT\$          | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$MAXSERVICEATTEMPTS\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEISVOLATILE\$       | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEEVENTID\$          | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICEEVENTID\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEPROBLEMID\$        | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICEPROBLEMID\$    | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEAGENCY\$           | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEEXECUTIONTIME\$    | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEDURATION\$         | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEDURATIONSEC\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEDOWNTIME\$         | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEPERCENTCHANGES\$   | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEGROUPNAME\$        | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEGROUPNAMESY\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICECHECK\$        | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICESTATECHANGES\$ | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICEOK\$           | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICEWARNING\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICEUNKNOWN\$      | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$LASTSERVICECRITICAL\$     | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEOUTPUT\$           | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |

| Macro Name                 | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
|----------------------------|----------------|-----------------------|-------------|--------------------|---------------------------------|------------------------------|-------------------|----------------|
| \$LONGSERVICEOUTPUT\$      |                |                       |             |                    |                                 |                              |                   |                |
| \$SERVICEPERFDATA\$        | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICECHECKCOMMANDS\$   | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICEACKAUTHORS\$8     | No             | Yes                   | No          | No                 | No                              | No                           | No                | No             |
| \$SERVICEACKAUTHORNAME\$8  | No             | Yes                   | No          | No                 | No                              | No                           | No                | No             |
| \$SERVICEACKAUTHORALIAS\$8 | No             | Yes                   | No          | No                 | No                              | No                           | No                | No             |
| \$SERVICEACKCOMMENTS\$8    | No             | Yes                   | No          | No                 | No                              | No                           | No                | No             |
| \$SERVICEACTIONURL\$       | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICENOTESURL\$        | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
| \$SERVICENOTES\$           | Yes            | Yes                   | No          | No                 | Yes                             | No                           | Yes               | No             |
|                            |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                 | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Service Group Macros:      |                |                       |             |                    |                                 |                              |                   |                |
| \$SERVICEGROUPALIAS\$6     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SERVICEGROUPMEMBERS\$6   | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SERVICEGROUPNOTES\$6     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SERVICEGROUPNOTESURL\$6  | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SERVICEGROUPACTIONURL\$6 | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
|                            |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                 | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Contact Macros:            |                |                       |             |                    |                                 |                              |                   |                |
| \$CONTACTNAME\$            | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$CONTACTALIAS\$           | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$CONTACTEMAIL\$           | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$CONTACTPAGER\$           | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$CONTACTADDRESSn\$        | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
|                            |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                 | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Contact Group Macros:      |                |                       |             |                    |                                 |                              |                   |                |
| \$CONTACTGROUPALIAS\$7     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |

| Macro Name                               | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
|------------------------------------------|----------------|-----------------------|-------------|--------------------|---------------------------------|------------------------------|-------------------|----------------|
| \$CONTACTGROUPMEMBERS\$<br>7             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
|                                          |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                               | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Summary Macros:                          |                |                       |             |                    |                                 |                              |                   |                |
| \$TOTALHOSTSUP\$<br>10                   | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSDOWNS\$<br>10                | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSUNREACHABLE\$<br>10          | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSDOWNUNHANDLED\$<br>10        | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTSUNREACHABLEUNHANDLED\$<br>10 | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTPROBLEMS\$<br>10              | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALHOSTPROBLEMSUNHANDLED\$<br>10     | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESOK\$<br>10                | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESWARNINGS\$<br>10          | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESCRITICAL\$<br>10          | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESUNKNOWN\$<br>10           | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESWARNINGUNHANDLED\$<br>10  | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESCRITICALUNHANDLED\$<br>10 | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICESUNKNOWNUNHANDLED\$<br>10  | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICEPROBLEMS\$<br>10           | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
| \$TOTALSERVICEPROBLEMSUNHANDLED\$<br>10  | Yes            | Yes 4                 | Yes         | Yes 4              | Yes                             | Yes                          | Yes               | Yes            |
|                                          |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                               | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Notification Macros:                     |                |                       |             |                    |                                 |                              |                   |                |
| \$NOTIFICATIONTYPES\$                    | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$NOTIFICATIONRECIPIENTS\$               | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$NOTIFICATIONISESCALATED\$              | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$NOTIFICATIONAUTHORITY\$                | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |

| Macro Name                       | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
|----------------------------------|----------------|-----------------------|-------------|--------------------|---------------------------------|------------------------------|-------------------|----------------|
| \$NOTIFICATIONAUTHORITYNAME\$    | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$NOTIFICATIONAUTHORITYCLASS\$   | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$NOTIFICATIONCOMMENT\$          | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTNOTIFICATIONNUMBER\$       | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$HOSTNOTIFICATIONID\$           | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$SERVICE_NOTIFICATION_NUMBERS\$ | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
| \$SERVICE_NOTIFICATION\$         | No             | Yes                   | No          | Yes                | No                              | No                           | No                | No             |
|                                  |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                       | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Date/Time Macros:                |                |                       |             |                    |                                 |                              |                   |                |
| \$LONGDATETIME\$                 | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SHORTDATETIME\$                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$DATE\$                         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TIME\$                         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TIMET\$                        | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$ISVALIDTIME:\$9                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$NEXTVALIDTIME:\$9              | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
|                                  |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                       | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| File Macros:                     |                |                       |             |                    |                                 |                              |                   |                |
| \$MAINCONFFILES\$                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$STATUSDATAFILES\$              | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$COMMENTDATAFILES\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes<5/td>      |
| \$DOWNTIMEFILES\$                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$RETENTIONDATAFILES\$           | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$OBJECTCACHEFILES\$             | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TEMPFILES\$                    | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$TEMPPATHS\$                    | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$LOGFILES\$                     | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$RESOURCEFILES\$                | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$COMMANDFILES\$                 | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$HOSTPERFDATAFILES\$            | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
| \$SERVICEPERFDATAFILES\$         | Yes            | Yes                   | Yes         | Yes                | Yes                             | Yes                          | Yes               | Yes            |
|                                  |                |                       |             |                    |                                 |                              |                   |                |
| Macro Name                       | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OSCP | Host Event Handlers and OCHP | Service Perf Data | Host Perf Data |
| Misc Macros:                     |                |                       |             |                    |                                 |                              |                   |                |



| Macro Name  | Service Checks | Service Notifications | Host Checks | Host Notifications | Service Event Handlers and OCS | Host Event Handlers and OCH | Service Perf Data | Host Perf Data |
|-------------|----------------|-----------------------|-------------|--------------------|--------------------------------|-----------------------------|-------------------|----------------|
| \$PROCESSOR | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |
| \$EVENTS    | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |
| \$ADMINMAIL | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |
| \$ADMINPAGE | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |
| \$ARGn      | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |
| \$USERn     | Yes            | Yes                   | Yes         | Yes                | Yes                            | Yes                         | Yes               | Yes            |

## 26.3 Macro Descriptions

|                     |                                                                                                                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Macros: 3      |                                                                                                                                                                                                                                                                                                                 |
| \$HOSTNAME\$        | Short name for the host (i.e. "biglinuxbox"). This value is taken from the host_name directive in the <b>host definition</b> .                                                                                                                                                                                  |
| \$HOSTDISPLAYNAME\$ | An alternate display name for the host. This value is taken from the display_name directive in the <b>host definition</b> .                                                                                                                                                                                     |
| \$HOSTALIAS\$       | Long name/description for the host. This value is taken from the alias directive in the <b>host definition</b> .                                                                                                                                                                                                |
| \$HOSTADDRESS\$     | Address of the host. This value is taken from the address directive in the <b>host definition</b> .                                                                                                                                                                                                             |
| \$HOSTSTATE\$       | A string indicating the current state of the host ("UP", "DOWN", or "UNREACHABLE").                                                                                                                                                                                                                             |
| \$HOSTSTATEID\$     | A number that corresponds to the current state of the host: 0=UP, 1=DOWN, 2=UNREACHABLE.                                                                                                                                                                                                                        |
| \$LASTHOSTSTATE\$   | A string indicating the last state of the host ("UP", "DOWN", or "UNREACHABLE").                                                                                                                                                                                                                                |
| \$LASTHOSTSTATEID\$ | A number that corresponds to the last state of the host: 0=UP, 1=DOWN, 2=UNREACHABLE.                                                                                                                                                                                                                           |
| \$HOSTSTATETYPE\$   | A string indicating the <b>state type</b> for the current host check ("HARD" or "SOFT"). Soft states occur when host checks return a non-OK (non-UP) state and are in the process of being retried. Hard states result when host checks have been checked a specified maximum number of times.                  |
| \$HOSTATTEMPT\$     | The number of the current host check retry. For instance, if this is the second time that the host is being rechecked, this will be the number two. Current attempt number is really only useful when writing host event handlers for "soft" states that take a specific action based on the host retry number. |
| \$MAXHOSTATTEMPTS\$ | The max check attempts as defined for the current host. Useful when writing host event handlers for "soft" states that take a specific action based on the host retry number.                                                                                                                                   |
| \$HOSTEVENTID\$     | A globally unique number associated with the host's current state. Every time a host (or service) experiences a state change, a global event ID number is incremented by one (1). If a host has experienced no state changes, this macro will be set to zero (0).                                               |
| \$LASTHOSTEVENTID\$ | The previous (globally unique) event number that was given to the host.                                                                                                                                                                                                                                         |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$HOSTPROBLEMID\$       | A globally unique number associated with the host's current problem state. Every time a host (or service) transitions from an UP or OK state to a problem state, a global problem ID number is incremented by one (1). This macro will be non-zero if the host is currently a non-UP state. State transitions between non-UP states (e.g. DOWN to UNREACHABLE) do not cause this problem id to increase. If the host is currently in an UP state, this macro will be set to zero (0). Combined with event handlers, this macro could be used to automatically open trouble tickets when hosts first enter a problem state. |
| \$LASTHOSTPROBLEMID\$   | The previous (globally unique) problem number that was given to the host. Combined with event handlers, this macro could be used for automatically closing trouble tickets, etc. when a host recovers to an UP state.                                                                                                                                                                                                                                                                                                                                                                                                      |
| \$HOSTLATENCY\$         | A (floating point) number indicating the number of seconds that a scheduled host check lagged behind its scheduled check time. For instance, if a check was scheduled for 03:14:15 and it didn't get executed until 03:14:17, there would be a check latency of 2.0 seconds. On-demand host checks have a latency of zero seconds.                                                                                                                                                                                                                                                                                         |
| \$HOSTEXECUTIONTIME\$   | A (floating point) number indicating the number of seconds that the host check took to execute (i.e. the amount of time the check was executing).                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| \$HOSTDURATION\$        | A string indicating the amount of time that the host has spent in its current state. Format is "XXh YYm ZZs", indicating hours, minutes and seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| \$HOSTDURATIONSEC\$     | A number indicating the number of seconds that the host has spent in its current state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| \$HOSTDOWNTIME\$        | A number indicating the current "downtime depth" for the host. If this host is currently in a period of <b>scheduled downtime</b> , the value will be greater than zero. If the host is not currently in a period of downtime, this value will be zero.                                                                                                                                                                                                                                                                                                                                                                    |
| \$HOSTPERCENTCHANGE\$   | A (floating point) number indicating the percent state change the host has undergone. Percent state change is used by the <b>flap detection</b> algorithm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| \$HOSTGROUPNAME\$       | The short name of the hostgroup that this host belongs to. This value is taken from the hostgroup_name directive in the <b>hostgroup definition</b> . If the host belongs to more than one hostgroup this macro will contain the name of just one of them.                                                                                                                                                                                                                                                                                                                                                                 |
| \$HOSTGROUPNAMES\$      | A comma separated list of the short names of all the hostgroups that this host belongs to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| \$LASTHOSTCHECK\$       | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which a check of the host was last performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| \$LASTHOSTSTATECHANGE\$ | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time the host last changed state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| \$LASTHOSTUP\$          | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the host was last detected as being in an UP state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| \$LASTHOSTDOWN\$        | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the host was last detected as being in a DOWN state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                               |                                                                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$LASTHOSTUNREACHABLE\$       | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the host was last detected as being in an UNREACHABLE state.                                                                                                                                  |
| \$HOSTOUTPUT\$                | The first line of text output from the last host check (i.e. "Ping OK").                                                                                                                                                                                                                       |
| \$LONGHOSTOUTPUT\$            | The full text output (aside from the first line) from the last host check.                                                                                                                                                                                                                     |
| \$HOSTPERFDATA\$              | This macro contains any <b>performance data</b> that may have been returned by the last host check.                                                                                                                                                                                            |
| \$HOSTCHECKCOMMAND\$          | This macro contains the name of the command (along with any arguments passed to it) used to perform the host check.                                                                                                                                                                            |
| \$HOSTACKAUTHOR\$ 8           | A string containing the name of the user who acknowledged the host problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                                                                                                        |
| \$HOSTACKAUTHORNAME\$ 8       | A string containing the short name of the contact (if applicable) who acknowledged the host problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                                                                               |
| \$HOSTACKAUTHORALIAS\$ 8      | A string containing the alias of the contact (if applicable) who acknowledged the host problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                                                                                    |
| \$HOSTACKCOMMENT\$ 8          | A string containing the acknowledgement comment that was entered by the user who acknowledged the host problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                                                                    |
| \$HOSTACTIONURL\$             | Action URL for the host. This macro may contain other macros (e.g. \$HOSTNAME\$), which can be useful when you want to pass the host name to a web page.                                                                                                                                       |
| \$HOSTNOTESURL\$              | Notes URL for the host. This macro may contain other macros (e.g. \$HOSTNAME\$), which can be useful when you want to pass the host name to a web page.                                                                                                                                        |
| \$HOSTNOTES\$                 | Notes for the host. This macro may contain other macros (e.g. \$HOSTNAME\$), which can be useful when you want to host-specific status information, etc. in the description.                                                                                                                   |
| \$TOTALHOSTSERVICES\$         | The total number of services associated with the host.                                                                                                                                                                                                                                         |
| \$TOTALHOSTSERVICESOK\$       | The total number of services associated with the host that are in an OK state.                                                                                                                                                                                                                 |
| \$TOTALHOSTSERVICESWARNING\$  | The total number of services associated with the host that are in a WARNING state.                                                                                                                                                                                                             |
| \$TOTALHOSTSERVICESUNKNOWN\$  | The total number of services associated with the host that are in an UNKNOWN state.                                                                                                                                                                                                            |
| \$TOTALHOSTSERVICESCRITICAL\$ | The total number of services associated with the host that are in a CRITICAL state.                                                                                                                                                                                                            |
| Host Group Macros: 5          |                                                                                                                                                                                                                                                                                                |
| \$HOSTGROUPALIAS\$ 5          | The long name / alias of either 1) the hostgroup name passed as an on-demand macro argument or 2) the primary hostgroup associated with the current host (if not used in the context of an on-demand macro). This value is taken from the alias directive in the <b>hostgroup definition</b> . |

|                          |                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$HOSTGROUPMEMBERS\$ 5   | A comma-separated list of all hosts that belong to either 1) the hostgroup name passed as an on-demand macro argument or 2) the primary hostgroup associated with the current host (if not used in the context of an on-demand macro).                                                                                      |
| \$HOSTGROUPNOTES\$ 5     | The notes associated with either 1) the hostgroup name passed as an on-demand macro argument or 2) the primary hostgroup associated with the current host (if not used in the context of an on-demand macro). This value is taken from the notes directive in the <b>hostgroup definition</b> .                             |
| \$HOSTGROUPNOTESURL\$ 5  | The notes URL associated with either 1) the hostgroup name passed as an on-demand macro argument or 2) the primary hostgroup associated with the current host (if not used in the context of an on-demand macro). This value is taken from the notes_url directive in the <b>hostgroup definition</b> .                     |
| \$HOSTGROUPACTIONURL\$ 5 | The action URL associated with either 1) the hostgroup name passed as an on-demand macro argument or 2) the primary hostgroup associated with the current host (if not used in the context of an on-demand macro). This value is taken from the action_url directive in the <b>hostgroup definition</b> .                   |
| Service Macros:          |                                                                                                                                                                                                                                                                                                                             |
| \$SERVICEDESC\$          | The long name/description of the service (i.e. "Main Website"). This value is taken from the description directive of the <b>service definition</b> .                                                                                                                                                                       |
| \$SERVICEDISPLAYNAME\$   | An alternate display name for the service. This value is taken from the display_name directive in the <b>service definition</b> .                                                                                                                                                                                           |
| \$SERVICESTATE\$         | A string indicating the current state of the service ("OK", "WARNING", "UNKNOWN", or "CRITICAL").                                                                                                                                                                                                                           |
| \$SERVICESTATEID\$       | A number that corresponds to the current state of the service: 0=OK, 1=WARNING, 2=CRITICAL, 3=UNKNOWN.                                                                                                                                                                                                                      |
| \$LASTSERVICESTATE\$     | A string indicating the last state of the service ("OK", "WARNING", "UNKNOWN", or "CRITICAL").                                                                                                                                                                                                                              |
| \$LASTSERVICESTATEID\$   | A number that corresponds to the last state of the service: 0=OK, 1=WARNING, 2=CRITICAL, 3=UNKNOWN.                                                                                                                                                                                                                         |
| \$SERVICESTATETYPE\$     | A string indicating the <b>state type</b> for the current service check ("HARD" or "SOFT"). Soft states occur when service checks return a non-OK state and are in the process of being retried. Hard states result when service checks have been checked a specified maximum number of times.                              |
| \$SERVICEATTEMPT\$       | The number of the current service check retry. For instance, if this is the second time that the service is being rechecked, this will be the number two. Current attempt number is really only useful when writing service event handlers for "soft" states that take a specific action based on the service retry number. |
| \$MAXSERVICEATTEMPT\$    | The max check attempts as defined for the current service. Useful when writing host event handlers for "soft" states that take a specific action based on the service retry number.                                                                                                                                         |
| \$SERVICEISVOLATILE\$    | Indicates whether the service is marked as being volatile or not: 0 = not volatile, 1 = volatile.                                                                                                                                                                                                                           |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>\$\$SERVICEEVENTID\$</code>        | A globally unique number associated with the service's current state. Every time a service (or host) experiences a state change, a global event ID number is incremented by one (1). If a service has experienced no state changes, this macro will be set to zero (0).                                                                                                                                                                                                                                                                                                                                                                |
| <code>\$LASTSERVICEEVENTID\$</code>      | The previous (globally unique) event number that given to the service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>\$\$SERVICEPROBLEMID\$</code>      | A globally unique number associated with the service's current problem state. Every time a service (or host) transitions from an OK or UP state to a problem state, a global problem ID number is incremented by one (1). This macro will be non-zero if the service is currently a non-OK state. State transitions between non-OK states (e.g. WARNING to CRITICAL) do not cause this problem id to increase. If the service is currently in an OK state, this macro will be set to zero (0). Combined with event handlers, this macro could be used to automatically open trouble tickets when services first enter a problem state. |
| <code>\$LASTSERVICEPROBLEMID\$</code>    | The previous (globally unique) problem number that was given to the service. Combined with event handlers, this macro could be used for automatically closing trouble tickets, etc. when a service recovers to an OK state.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>\$\$SERVICELATENCY\$</code>        | A (floating point) number indicating the number of seconds that a scheduled service check lagged behind its scheduled check time. For instance, if a check was scheduled for 03:14:15 and it didn't get executed until 03:14:17, there would be a check latency of 2.0 seconds.                                                                                                                                                                                                                                                                                                                                                        |
| <code>\$\$SERVICEEXECUTIONTIMES\$</code> | A (floating point) number indicating the number of seconds that the service check took to execute (i.e. the amount of time the check was executing).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>\$\$SERVICEDURATION\$</code>       | A string indicating the amount of time that the service has spent in its current state. Format is "XXh YYm ZZs", indicating hours, minutes and seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>\$\$SERVICEDURATIONSEC\$</code>    | A number indicating the number of seconds that the service has spent in its current state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>\$\$SERVICEDOWNTIMES\$</code>      | A number indicating the current "downtime depth" for the service. If this service is currently in a period of <b>scheduled downtime</b> , the value will be greater than zero. If the service is not currently in a period of downtime, this value will be zero.                                                                                                                                                                                                                                                                                                                                                                       |
| <code>\$\$SERVICEPERCENTCHANGES\$</code> | A (floating point) number indicating the percent state change the service has undergone. Percent state change is used by the <b>flap detection</b> algorithm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>\$\$SERVICEGROUPNAMES\$</code>     | The short name of the servicegroup that this service belongs to. This value is taken from the <code>servicegroup_name</code> directive in the <b>servicegroup</b> definition. If the service belongs to more than one servicegroup this macro will contain the name of just one of them.                                                                                                                                                                                                                                                                                                                                               |
| <code>\$\$SERVICEGROUPNAMES\$</code>     | A comma separated list of the short names of all the servicegroups that this service belongs to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>\$LASTSERVICECHECK\$</code>        | This is a timestamp in <code>time_t</code> format (seconds since the UNIX epoch) indicating the time at which a check of the service was last performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>\$LASTSERVICESTATECHANGE\$</code>  | This is a timestamp in <code>time_t</code> format (seconds since the UNIX epoch) indicating the time the service last changed state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                    |                                                                                                                                                                                                                                |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$LASTSERVICEOK\$                  | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the service was last detected as being in an OK state.                                                                        |
| \$LASTSERVICEWARNING\$             | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the service was last detected as being in a WARNING state.                                                                    |
| \$LASTSERVICEUNKNOWN\$             | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the service was last detected as being in an UNKNOWN state.                                                                   |
| \$LASTSERVICECRITICAL\$            | This is a timestamp in time_t format (seconds since the UNIX epoch) indicating the time at which the service was last detected as being in a CRITICAL state.                                                                   |
| \$SERVICEOUTPUT\$                  | The first line of text output from the last service check (i.e. "Ping OK").                                                                                                                                                    |
| \$LONGSERVICEOUTPUT\$              | The full text output (aside from the first line) from the last service check.                                                                                                                                                  |
| \$SERVICEPERFDATA\$                | This macro contains any <b>performance data</b> that may have been returned by the last service check.                                                                                                                         |
| \$SERVICECHECKCOMMAND\$            | This macro contains the name of the command (along with any arguments passed to it) used to perform the service check.                                                                                                         |
| \$SERVICEACKAUTHOR\$ <b>8</b>      | A string containing the name of the user who acknowledged the service problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                                     |
| \$SERVICEACKAUTHORNAME\$ <b>8</b>  | A string containing the short name of the contact (if applicable) who acknowledged the service problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".            |
| \$SERVICEACKAUTHORALIAS\$ <b>8</b> | A string containing the alias of the contact (if applicable) who acknowledged the service problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT".                 |
| \$SERVICEACKCOMMENT\$ <b>8</b>     | A string containing the acknowledgement comment that was entered by the user who acknowledged the service problem. This macro is only valid in notifications where the \$NOTIFICATIONTYPE\$ macro is set to "ACKNOWLEDGEMENT". |
| \$SERVICEACTIONURL\$               | Action URL for the service. This macro may contain other macros (e.g. \$HOSTNAME\$ or \$SERVICEDESC\$), which can be useful when you want to pass the service name to a web page.                                              |
| \$SERVICENOTESURL\$                | Notes URL for the service. This macro may contain other macros (e.g. \$HOSTNAME\$ or \$SERVICEDESC\$), which can be useful when you want to pass the service name to a web page.                                               |
| \$SERVICENOTES\$                   | Notes for the service. This macro may contain other macros (e.g. \$HOSTNAME\$ or \$SERVICESTATE\$), which can be useful when you want to service-specific status information, etc. in the description                          |
| Service Group Macros: <b>6</b>     |                                                                                                                                                                                                                                |



|                                                         |                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>\$SERVICEGROUPALIAS\$</code> <a href="#">6</a>    | The long name / alias of either 1) the servicegroup name passed as an on-demand macro argument or 2) the primary servicegroup associated with the current service (if not used in the context of an on-demand macro). This value is taken from the alias directive in the <a href="#">servicegroup definition</a> .                        |
| <code>\$SERVICEGROUPMEMBERS\$</code> <a href="#">6</a>  | A comma-separated list of all services that belong to either 1) the servicegroup name passed as an on-demand macro argument or 2) the primary servicegroup associated with the current service (if not used in the context of an on-demand macro).                                                                                         |
| <code>\$SERVICEGROUPNOTES\$</code> <a href="#">6</a>    | The notes associated with either 1) the servicegroup name passed as an on-demand macro argument or 2) the primary servicegroup associated with the current service (if not used in the context of an on-demand macro). This value is taken from the notes directive in the <a href="#">servicegroup definition</a> .                       |
| <code>\$SERVICEGROUPNOTESURL\$</code> <a href="#">6</a> | The notes URL associated with either 1) the servicegroup name passed as an on-demand macro argument or 2) the primary servicegroup associated with the current service (if not used in the context of an on-demand macro). This value is taken from the notes_url directive in the <a href="#">servicegroup definition</a> .               |
| <code>\$SERVICEGROUPNOTES\$</code> <a href="#">6</a>    | The action URL associated with either 1) the servicegroup name passed as an on-demand macro argument or 2) the primary servicegroup associated with the current service (if not used in the context of an on-demand macro). This value is taken from the action_url directive in the <a href="#">servicegroup definition</a> .             |
| Contact Macros:                                         |                                                                                                                                                                                                                                                                                                                                            |
| <code>\$CONTACTNAME\$</code>                            | Short name for the contact (i.e. "jdoe") that is being notified of a host or service problem. This value is taken from the contact_name directive in the <a href="#">contact definition</a> .                                                                                                                                              |
| <code>\$CONTACTALIAS\$</code>                           | Long name/description for the contact (i.e. "John Doe") being notified. This value is taken from the alias directive in the <a href="#">contact definition</a> .                                                                                                                                                                           |
| <code>\$CONTACTEMAIL\$</code>                           | Email address of the contact being notified. This value is taken from the email directive in the <a href="#">contact definition</a> .                                                                                                                                                                                                      |
| <code>\$CONTACTPAGER\$</code>                           | Pager number/address of the contact being notified. This value is taken from the pager directive in the <a href="#">contact definition</a> .                                                                                                                                                                                               |
| <code>\$CONTACTADDRESSn\$</code>                        | Address of the contact being notified. Each contact can have six different addresses (in addition to email address and pager number). The macros for these addresses are <code>\$CONTACTADDRESS1\$</code> - <code>\$CONTACTADDRESS6\$</code> . This value is taken from the addressx directive in the <a href="#">contact definition</a> . |
| <code>\$CONTACTGROUPNAME\$</code>                       | The short name of the contactgroup that this contact is a member of. This value is taken from the contactgroup_name directive in the <a href="#">contactgroup definition</a> . If the contact belongs to more than one contactgroup this macro will contain the name of just one of them.                                                  |
| <code>\$CONTACTGROUPNAME\$</code>                       | A comma separated list of the short names of all the contactgroups that this contact is a member of.                                                                                                                                                                                                                                       |
| Contact Group Macros: <a href="#">5</a>                 |                                                                                                                                                                                                                                                                                                                                            |

|                                    |                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$CONTACTGROUPALIAS\$ 7            | The long name / alias of either 1) the contactgroup name passed as an on-demand macro argument or 2) the primary contactgroup associated with the current contact (if not used in the context of an on-demand macro). This value is taken from the alias directive in the <a href="#">contactgroup definition</a> . |
| \$CONTACTGROUPMEMBERS\$ 7          | A comma-separated list of all contacts that belong to either 1) the contactgroup name passed as an on-demand macro argument or 2) the primary contactgroup associated with the current contact (if not used in the context of an on-demand macro).                                                                  |
| SUMMARY Macros:                    |                                                                                                                                                                                                                                                                                                                     |
| \$TOTALHOSTSUP\$                   | This macro reflects the total number of hosts that are currently in an UP state.                                                                                                                                                                                                                                    |
| \$TOTALHOSTSDOWN\$                 | This macro reflects the total number of hosts that are currently in a DOWN state.                                                                                                                                                                                                                                   |
| \$TOTALHOSTSUNREACHABLE\$          | This macro reflects the total number of hosts that are currently in an UNREACHABLE state.                                                                                                                                                                                                                           |
| \$TOTALHOSTSDOWNUNHANDLED\$        | This macro reflects the total number of hosts that are currently in a DOWN state that are not currently being "handled". Unhandled host problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                                          |
| \$TOTALHOSTSUNREACHABLEUNHANDLED\$ | This macro reflects the total number of hosts that are currently in an UNREACHABLE state that are not currently being "handled". Unhandled host problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                                  |
| \$TOTALHOSTPROBLEMS\$              | This macro reflects the total number of hosts that are currently either in a DOWN or an UNREACHABLE state.                                                                                                                                                                                                          |
| \$TOTALHOSTPROBLEMSUNHANDLED\$     | This macro reflects the total number of hosts that are currently either in a DOWN or an UNREACHABLE state that are not currently being "handled". Unhandled host problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                 |
| \$TOTALSERVICESOK\$                | This macro reflects the total number of services that are currently in an OK state.                                                                                                                                                                                                                                 |
| \$TOTALSERVICESWARNING\$           | This macro reflects the total number of services that are currently in a WARNING state.                                                                                                                                                                                                                             |
| \$TOTALSERVICESCRITICAL\$          | This macro reflects the total number of services that are currently in a CRITICAL state.                                                                                                                                                                                                                            |
| \$TOTALSERVICESUNKNOWN\$           | This macro reflects the total number of services that are currently in an UNKNOWN state.                                                                                                                                                                                                                            |
| \$TOTALSERVICESWARNINGUNHANDLED\$  | This macro reflects the total number of services that are currently in a WARNING state that are not currently being "handled". Unhandled services problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                                |
| \$TOTALSERVICESCRITICALUNHANDLED\$ | This macro reflects the total number of services that are currently in a CRITICAL state that are not currently being "handled". Unhandled services problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                               |



|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$TOTALSERVICESUNKNOWNUNHANDLED\$ | This macro reflects the total number of services that are currently in an UNKNOWN state that are not currently being "handled". Unhandled services problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                                                                                                                                                                                                                                                                     |
| \$TOTALSERVICEPROBLEMS\$          | This macro reflects the total number of services that are currently either in a WARNING, CRITICAL, or UNKNOWN state.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| \$TOTALSERVICEPROBLEMSUNHANDLED\$ | This macro reflects the total number of services that are currently either in a WARNING, CRITICAL, or UNKNOWN state that are not currently being "handled". Unhandled services problems are those that are not acknowledged, are not currently in scheduled downtime, and for which checks are currently enabled.                                                                                                                                                                                                                                         |
| Notification Macros:              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| \$NOTIFICATIONTYPE\$              | A string identifying the type of notification that is being sent ("PROBLEM", "RECOVERY", "ACKNOWLEDGEMENT", "FLAPPINGSTART", "FLAPPINGSTOP", "FLAPPINGDISABLED", "DOWNTIMESTART", "DOWNTIMEEND", or "DOWNTIMECANCELLED").                                                                                                                                                                                                                                                                                                                                 |
| \$NOTIFICATIONRECIPIENTS\$        | A comma-separated list of the short names of all contacts that are being notified about the host or service.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| \$NOTIFICATIONISESCALATED\$       | An integer indicating whether this was sent to normal contacts for the host or service or if it was escalated. 0 = Normal (non-escalated) notification , 1 = Escalated notification.                                                                                                                                                                                                                                                                                                                                                                      |
| \$NOTIFICATIONAUTHOR\$            | A string containing the name of the user who authored the notification. If the \$NOTIFICATIONTYPE\$ macro is set to "DOWNTIMESTART" or "DOWNTIMEEND", this will be the name of the user who scheduled downtime for the host or service. If the \$NOTIFICATIONTYPE\$ macro is "ACKNOWLEDGEMENT", this will be the name of the user who acknowledged the host or service problem. If the \$NOTIFICATIONTYPE\$ macro is "CUSTOM", this will be name of the user who initiated the custom host or service notification.                                       |
| \$NOTIFICATIONAUTHORNAME\$        | A string containing the short name of the contact (if applicable) specified in the \$NOTIFICATIONAUTHOR\$ macro.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| \$NOTIFICATIONAUTHORALIAS\$       | A string containing the alias of the contact (if applicable) specified in the \$NOTIFICATIONAUTHOR\$ macro.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| \$NOTIFICATIONCOMMENT\$           | A string containing the comment that was entered by the notification author. If the \$NOTIFICATIONTYPE\$ macro is set to "DOWNTIMESTART" or "DOWNTIMEEND", this will be the comment entered by the user who scheduled downtime for the host or service. If the \$NOTIFICATIONTYPE\$ macro is "ACKNOWLEDGEMENT", this will be the comment entered by the user who acknowledged the host or service problem. If the \$NOTIFICATIONTYPE\$ macro is "CUSTOM", this will be comment entered by the user who initiated the custom host or service notification. |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$HOSTNOTIFICATIONNUMBER\$    | The current notification number for the host. The notification number increases by one (1) each time a new notification is sent out for the host (except for acknowledgements). The notification number is reset to 0 when the host recovers (after the recovery notification has gone out). Acknowledgements do not cause the notification number to increase, nor do notifications dealing with flap detection or scheduled downtime.                                                                                    |
| \$HOSTNOTIFICATIONID\$        | A unique number identifying a host notification. Notification ID numbers are unique across both hosts and service notifications, so you could potentially use this unique number as a primary key in a notification database. Notification ID numbers should remain unique across restarts of the Nagios process, so long as you have state retention enabled. The notification ID number is incremented by one (1) each time a new host notification is sent out, and regardless of how many contacts are notified.       |
| \$SERVICENOTIFICATIONNUMBER\$ | The current notification number for the service. The notification number increases by one (1) each time a new notification is sent out for the service (except for acknowledgements). The notification number is reset to 0 when the service recovers (after the recovery notification has gone out). Acknowledgements do not cause the notification number to increase, nor do notifications dealing with flap detection or scheduled downtime.                                                                           |
| \$SERVICENOTIFICATIONID\$     | A unique number identifying a service notification. Notification ID numbers are unique across both hosts and service notifications, so you could potentially use this unique number as a primary key in a notification database. Notification ID numbers should remain unique across restarts of the Nagios process, so long as you have state retention enabled. The notification ID number is incremented by one (1) each time a new service notification is sent out, and regardless of how many contacts are notified. |
| Date/Time Macros:             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| \$LONGDATETIME\$              | Current date/time stamp (i.e. Fri Oct 13 00:30:28 CDT 2000). Format of date is determined by <b>date_format</b> directive.                                                                                                                                                                                                                                                                                                                                                                                                 |
| \$SHORTDATETIME\$             | Current date/time stamp (i.e. 10-13-2000 00:30:28). Format of date is determined by <b>date_format</b> directive.                                                                                                                                                                                                                                                                                                                                                                                                          |
| \$DATE\$                      | Date stamp (i.e. 10-13-2000). Format of date is determined by <b>date_format</b> directive.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| \$TIME\$                      | Current time stamp (i.e. 00:30:28).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| \$TIMET\$                     | Current time stamp in time_t format (seconds since the UNIX epoch).                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$ISVALIDTIME:\$ 9      | <p>This is a special on-demand macro that returns a 1 or 0 depending on whether or not a particular time is valid within a specified timeperiod. There are two ways of using this macro:</p> <ul style="list-style-type: none"> <li>0. \$ISVALIDTIME:24x7\$ will be set to "1" if the current time is valid within the "24x7" timeperiod. If not, it will be set to "0".</li> <li>0. \$ISVALIDTIME:24x7:timestamp\$ will be set to "1" if the time specified by the "timestamp" argument (which must be in time_t format) is valid within the "24x7" timeperiod. If not, it will be set to "0".</li> </ul>                                                                    |
| \$NEXTVALIDTIME:\$ 9    | <p>This is a special on-demand macro that returns the next valid time (in time_t format) for a specified timeperiod. There are two ways of using this macro:</p> <ul style="list-style-type: none"> <li>0. \$NEXTVALIDTIME:24x7\$ will return the next valid time - from and including the current time - in the "24x7" timeperiod.</li> <li>0. \$NEXTVALIDTIME:24x7:timestamp\$ will return the next valid time - from and including the time specified by the "timestamp" argument (which must be specified in time_t format) - in the "24x7" timeperiod.</li> </ul> <p>If a next valid time cannot be found in the specified timeperiod, the macro will be set to "0".</p> |
|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Macros:            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| \$MAINCONFIGFILES       | The location of the <b>main config file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| \$STATUSDATAFILE\$      | The location of the <b>status data file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| \$COMMENTDATAFILE\$     | The location of the comment data file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| \$DOWNTIMEDATAFILE\$    | The location of the downtime data file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| \$RETENTIONDATAFILE\$   | The location of the <b>retention data file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| \$OBJECTCACHEFILES      | The location of the <b>object cache file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| \$TEMPFILES             | The location of the <b>temp file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| \$TEMPPATH\$            | The directory specified by the <b>temp path</b> variable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| \$LOGFILES              | The location of the <b>log file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| \$RESOURCEFILES         | The location of the <b>resource file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| \$COMMANDFILE\$         | The location of the <b>command file</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| \$HOSTPERFDATAFILE\$    | The location of the host performance data file (if defined).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| \$SERVICEPERFDATAFILE\$ | The location of the service performance data file (if defined).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Misc Macros:            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| \$PROCESSSTARTTIME\$    | Time stamp in time_t format (seconds since the UNIX epoch) indicating when the Nagios process was last (re)started. You can determine the number of seconds that Nagios has been running (since it was last restarted) by subtracting \$PROCESSSTARTTIME\$ from <b>\$TIMET\$</b> .                                                                                                                                                                                                                                                                                                                                                                                            |

|                    |                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$EVENTSTARTTIME\$ | Time stamp in time_t format (seconds since the UNIX epoch) indicating when the Nagios process starting process events (checks, etc.). You can determine the number of seconds that it took for Nagios to startup by subtracting \$PROCESSSTARTTIME\$ from \$EVENTSTARTTIME\$. |
| \$ADMINEMAIL\$     | Global administrative email address. This value is taken from the <a href="#">admin_email</a> directive.                                                                                                                                                                      |
| \$ADMINPAGER\$     | Global administrative pager number/address. This value is taken from the <a href="#">admin_pager</a> directive.                                                                                                                                                               |
| \$ARGn\$           | The nth argument passed to the command (notification, event handler, service check, etc.). Nagios supports up to 32 argument macros (\$ARG1\$ through \$ARG32\$).                                                                                                             |
| \$USERn\$          | The nth user-definable macro. User macros can be defined in one or more <a href="#">resource files</a> . Nagios supports up to 32 user macros (\$USER1\$ through \$USER32\$).                                                                                                 |

## 26.4 Notes

- 1 These macros are not valid for the host they are associated with when that host is being checked (i.e. they make no sense, as they haven't been determined yet).
- 2 These macros are not valid for the service they are associated with when that service is being checked (i.e. they make no sense, as they haven't been determined yet).
- 3 When host macros are used in service-related commands (i.e. service notifications, event handlers, etc) they refer to the host that the service is associated with.
- 4 When host and service summary macros are used in notification commands, the totals are filtered to reflect only those hosts and services for which the contact is authorized (i.e. hosts and services they are configured to receive notifications for).
- 5 These macros are normally associated with the first/primary hostgroup associated with the current host. They could therefore be considered host macros in many cases. However, these macros are not available as on-demand host macros. Instead, they can be used as on-demand hostgroup macros when you pass the name of a hostgroup to the macro. For example: \$HOSTGROUPMEMBERS:hg1\$ would return a comma-delimited list of all (host) members of the hostgroup hg1.
- 6 These macros are normally associated with the first/primary servicegroup associated with the current service. They could therefore be considered service macros in many cases. However, these macros are not available as on-demand service macros. Instead, they can be used as on-demand servicegroup macros when you pass the name of a servicegroup to the macro. For example: \$SERVICEGROUPMEMBERS:sg1\$ would return a comma-delimited list of all (service) members of the servicegroup sg1.
- 7 These macros are normally associated with the first/primary contactgroup associated with the current contact. They could therefore be considered contact macros in many cases. However, these macros are not available as on-demand contact macros. Instead, they can be used as on-demand contactgroup macros when you pass the name of a contactgroup to the macro. For example: \$CONTACTGROUPMEMBERS:cg1\$ would return a comma-delimited list of all (contact) members of the contactgroup cg1.
- 8 These acknowledgement macros are deprecated. Use the more generic \$NOTIFICATIONAUTHOR\$, \$NOTIFICATIONAUTHORNAME\$, \$NOTIFICATIONAUTHORALIAS\$ or \$NOTIFICATIONAUTHORCOMMENT\$ macros instead.
- 9 These macros are only available as on-demand macros - e.g. you must supply an additional argument with them in order to use them. These macros are not available as environment variables.
- 10 Summary macros are not available as environment variables if the [use\\_large\\_installation\\_tweaks](#) option is enabled, as they are quite CPU-intensive to calculate.

## Chapter 27

# Host Checks

### 27.1 Introduction

The basic workings of host checks are described here...

### 27.2 When Are Host Checks Performed?

Hosts are checked by the Nagios daemon:

- At regular intervals, as defined by the `check_interval` and `retry_interval` options in your [host definitions](#).
- On-demand when a service associated with the host changes state.
- On-demand as needed as part of the [host reachability](#) logic.
- On-demand as needed for [predictive host dependency checks](#).

Regularly scheduled host checks are optional. If you set the `check_interval` option in your host definition to zero (0), Nagios will not perform checks of the hosts on a regular basis. It will, however, still perform on-demand checks of the host as needed for other parts of the monitoring logic.

On-demand checks are made when a service associated with the host changes state because Nagios needs to know whether the host has also changed state. Services that change state are often an indicator that the host may have also changed state. For example, if Nagios detects that the HTTP service associated with a host just changed from a CRITICAL to an OK state, it may indicate that the host just recovered from a reboot and is now back up and running.

On-demand checks of hosts are also made as part of the [host reachability](#) logic. Nagios is designed to detect network outages as quickly as possible, and distinguish between DOWN and UNREACHABLE host states. These are very different states and can help an admin quickly locate the cause of a network outage.

On-demand checks are also performed as part of the [predictive host dependency check](#) logic. These checks help ensure that the dependency logic is as accurate as possible.

### 27.3 Cached Host Checks

The performance of on-demand host checks can be significantly improved by implementing the use of cached checks, which allow Nagios to forgo executing a host check if it determines a relatively recent check result will do instead. More information on cached checks can be found [here](#).

---

## 27.4 Dependencies and Checks

You can define **host execution dependencies** that prevent Nagios from checking the status of a host depending on the state of one or more other hosts. More information on dependencies can be found [here](#).

## 27.5 Parallelization of Host Checks

Scheduled host checks are run in parallel. When Nagios needs to run a scheduled host check, it will initiate the host check and then return to doing other work (running service checks, etc). The host check runs in a child process that was fork()ed from the main Nagios daemon. When the host check has completed, the child process will inform the main Nagios process (its parent) of the check results. The main Nagios process then handles the check results and takes appropriate action (running event handlers, sending notifications, etc.).

On-demand host checks are also run in parallel if needed. As mentioned earlier, Nagios can forgo the actual execution of an on-demand host check if it can use the cached results from a relatively recent host check.

When Nagios processes the results of scheduled and on-demand host checks, it may initiate (secondary) checks of other hosts. These checks can be initiated for two reasons: **predictive dependency checks** and to determining the status of the host using the **network reachability** logic. The secondary checks that are initiated are usually run in parallel. However, there is one big exception that you should be aware of, as it can have negative effect on performance...

---

### Note

Hosts which have their `max_check_attempts` value set to 1 can cause serious performance problems. The reason? If Nagios needs to determine their true state using the **network reachability** logic (to see if they're DOWN or UNREACHABLE), it will have to launch serial checks of all of the host's immediate parents. Just to reiterate, those checks are run serially, rather than in parallel, so it can cause a big performance hit. For this reason, I would recommend that you always use a value greater than 1 for the `max_check_attempts` directives in your host definitions.

---

## 27.6 Host States

Hosts that are checked can be in one of three different states:

- UP
- DOWN
- UNREACHABLE

## 27.7 Host State Determination

Host checks are performed by **plugins**, which can return a state of OK, WARNING, UNKNOWN, or CRITICAL. How does Nagios translate these plugin return codes into host states of UP, DOWN, or UNREACHABLE? Lets see...

The table below shows how plugin return codes correspond with preliminary host states. Some post-processing (which is described later) is done which may then alter the final host state.

| Plugin Result | Preliminary Host State |
|---------------|------------------------|
| OK            | UP                     |
| WARNING       | UP or DOWN*            |
| UNKNOWN       | DOWN                   |
| CRITICAL      | DOWN                   |

---

**Note**

WARNING results usually means the host is UP. However, WARNING results are interpreted to mean the host is DOWN if the [use\\_aggressive\\_host\\_checking](#) option is enabled.

If the preliminary host state is DOWN, Nagios will attempt to see if the host is really DOWN or if it is UNREACHABLE. The distinction between DOWN and UNREACHABLE host states is important, as it allows admins to determine root cause of network outages faster. The following table shows how Nagios makes a final state determination based on the state of the hosts parent(s). A host's parents are defined in the parents directive in host definition.

---

| Preliminary Host State | Parent Host State                          | Final Host State |
|------------------------|--------------------------------------------|------------------|
| DOWN                   | At least one parent is UP                  | DOWN             |
| DOWN                   | All parents are either DOWN or UNREACHABLE | UNREACHABLE      |

More information on how Nagios distinguishes between DOWN and UNREACHABLE states can be found [here](#).

## 27.8 Host State Changes

As you are probably well aware, hosts don't always stay in one state. Things break, patches get applied, and servers need to be rebooted. When Nagios checks the status of hosts, it will be able to detect when a host changes between UP, DOWN, and UNREACHABLE states and take appropriate action. These state changes result in different [state types](#) (HARD or SOFT), which can trigger [event handlers](#) to be run and [notifications](#) to be sent out. Detecting and dealing with state changes is what Nagios is all about.

When hosts change state too frequently they are considered to be 'flapping'. A good example of a flapping host would be server that keeps spontaneously rebooting as soon as the operating system loads. That's always a fun scenario to have to deal with. Nagios can detect when hosts start flapping, and can suppress notifications until flapping stops and the host's state stabilizes. More information on the flap detection logic can be found [here](#).

## Chapter 28

# Service Checks

### 28.1 Introduction

The basic workings of service checks are described here...

### 28.2 When Are Service Checks Performed?

Services are checked by the Nagios daemon:

- At regular intervals, as defined by the `check_interval` and `retry_interval` options in your [service definitions](#).
- On-demand as needed for [predictive service dependency checks](#).

On-demand checks are performed as part of the [predictive service dependency check](#) logic. These checks help ensure that the dependency logic is as accurate as possible. If you don't make use of [service dependencies](#), Nagios won't perform any on-demand service checks.

### 28.3 Cached Service Checks

The performance of on-demand service checks can be significantly improved by implementing the use of cached checks, which allow Nagios to forgo executing a service check if it determines a relatively recent check result will do instead. Cached checks will only provide a performance increase if you are making use of [service dependencies](#). More information on cached checks can be found [here](#).

### 28.4 Dependencies and Checks

You can define [service execution dependencies](#) that prevent Nagios from checking the status of a service depending on the state of one or more other services. More information on dependencies can be found [here](#).

### 28.5 Parallelization of Service Checks

Scheduled service checks are run in parallel. When Nagios needs to run a scheduled service check, it will initiate the service check and then return to doing other work (running host checks, etc). The service check runs in a child process that was fork()ed from the main Nagios daemon. When the service check has completed, the child process will inform the main Nagios process

---



(its parent) of the check results. The main Nagios process then handles the check results and takes appropriate action (running event handlers, sending notifications, etc.).

On-demand service checks are also run in parallel if needed. As mentioned earlier, Nagios can forgo the actual execution of an on-demand service check if it can use the cached results from a relatively recent service check.

## 28.6 Service States

Services that are checked can be in one of four different states:

- OK
- WARNING
- UNKNOWN
- CRITICAL

## 28.7 Service State Determination

Service checks are performed by [plugins](#), which can return a state of OK, WARNING, UNKNOWN, or CRITICAL. These plugin states directly translate to service states. For example, a plugin which returns a WARNING state will cause a service to have a WARNING state.

## 28.8 Services State Changes

When Nagios checks the status of services, it will be able to detect when a service changes between OK, WARNING, UNKNOWN, and CRITICAL states and take appropriate action. These state changes result in different [state types](#) (HARD or SOFT), which can trigger [event handlers](#) to be run and [notifications](#) to be sent out. Service state changes can also trigger on-demand [host checks](#). Detecting and dealing with state changes is what Nagios is all about.

When services change state too frequently they are considered to be ‘flapping’. Nagios can detect when services start flapping, and can suppress notifications until flapping stops and the service’s state stabilizes. More information on the flap detection logic can be found [here](#).

---

## Chapter 29

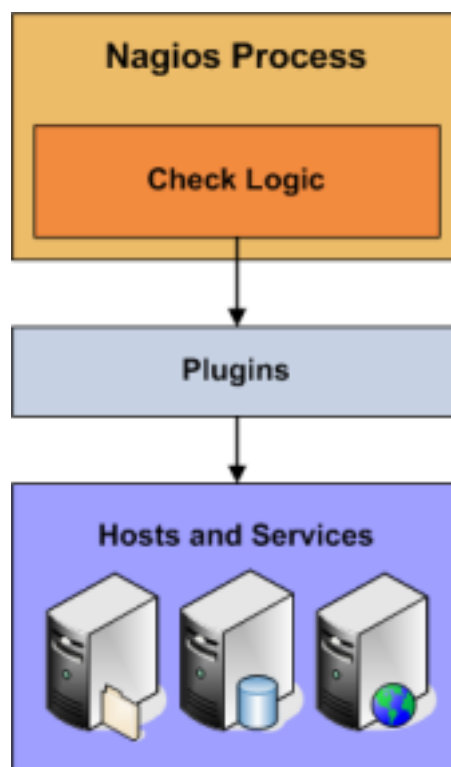
# Active Checks

### 29.1 Introduction

Nagios is capable of monitoring hosts and services in two ways: actively and passively. Passive checks are described [elsewhere](#), so we'll focus on active checks here. Active checks are the most common method for monitoring hosts and services. The main features of active checks are as follows:

- Active checks are initiated by the Nagios process
- Active checks are run on a regularly scheduled basis

### 29.2 How Are Active Checks Performed?



Active checks are initiated by the check logic in the Nagios daemon. When Nagios needs to check the status of a host or service it will execute a plugin and pass it information about what needs to be checked. The plugin will then check the operational state

of the host or service and report the results back to the Nagios daemon. Nagios will process the results of the host or service check and take appropriate action as necessary (e.g. send notifications, run event handlers, etc).

More information on how plugins work can be found [here](#).

## 29.3 When Are Active Checks Executed?

Active check are executed:

- At regular intervals, as defined by the `check_interval` and `retry_interval` options in your host and service definitions
- On-demand as needed

Regularly scheduled checks occur at intervals equaling either the `check_interval` or the `retry_interval` in your host or service definitions, depending on what **type of state** the host or service is in. If a host or service is in a **HARD** state, it will be actively checked at intervals equal to the `check_interval` option. If it is in a **SOFT** state, it will be checked at intervals equal to the `retry_interval` option.

On-demand checks are performed whenever Nagios sees a need to obtain the latest status information about a particular host or service. For example, when Nagios is determining the **reachability** of a host, it will often perform on-demand checks of parent and child hosts to accurately determine the status of a particular network segment. On-demand checks also occur in the **predictive dependency check** logic in order to ensure Nagios has the most accurate status information.

---

## Chapter 30

# Passive Checks

### 30.1 Introduction

In most cases you'll use Nagios to monitor your hosts and services using regularly scheduled **active checks**. Active checks can be used to "poll" a device or service for status information every so often. Nagios also supports a way to monitor hosts and services passively instead of actively. The key features of passive checks are as follows:

- Passive checks are initiated and performed external applications/processes
- Passive check results are submitted to Nagios for processing

The major difference between active and passive checks is that active checks are initiated and performed by Nagios, while passive checks are performed by external applications.

### 30.2 Uses For Passive Checks

Passive checks are useful for monitoring services that are:

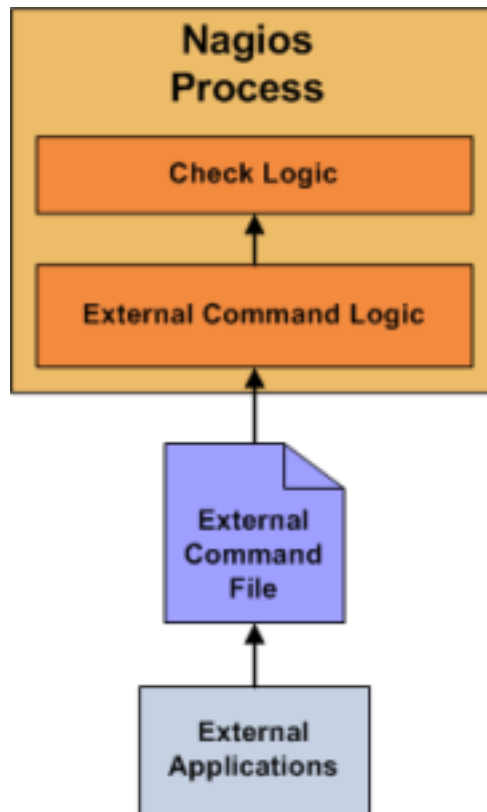
- Asynchronous in nature and cannot be monitored effectively by polling their status on a regularly scheduled basis
- Located behind a firewall and cannot be checked actively from the monitoring host

Examples of asynchronous services that lend themselves to being monitored passively include **SNMP** traps and security alerts. You never know how many (if any) traps or alerts you'll receive in a given time frame, so it's not feasible to just monitor their status every few minutes.

Passive checks are also used when configuring **distributed** or **redundant** monitoring installations.

---

### 30.3 How Passive Checks Work



Here's how passive checks work in more detail...

1. An external application checks the status of a host or service.
2. The external application writes the results of the check to the **external command file**.
3. The next time Nagios reads the external command file it will place the results of all passive checks into a queue for later processing. The same queue that is used for storing results from active checks is also used to store the results from passive checks.
4. Nagios will periodically execute a **check result reaper event** and scan the check result queue. Each service check result that is found in the queue is processed in the same manner - regardless of whether the check was active or passive. Nagios may send out notifications, log alerts, etc. depending on the check result information.

The processing of active and passive check results is essentially identical. This allows for seamless integration of status information from external applications with Nagios.

### 30.4 Enabling Passive Checks

In order to enable passive checks in Nagios, you'll need to do the following:

- Set **accept\_passive\_service\_checks** directive is set to 1.
- Set the **passive\_checks\_enabled** directive in your host and service definitions is set to 1.

If you want to disable processing of passive checks on a global basis, set the **accept\_passive\_service\_checks** directive to 0.

If you would like to disable passive checks for just a few hosts or services, use the **passive\_checks\_enabled** directive in the host and/or service definitions to do so.

## 30.5 Submitting Passive Service Check Results

External applications can submit passive service check results to Nagios by writing a `PROCESS_SERVICE_CHECK_RESULT` external command to the external command file.

The format of the command is as follows: `[<timestamp>] PROCESS_SERVICE_CHECK_RESULT;<host_name>;<-svc_description>;<return_code>;<plugin_output> where...`

- `timestamp` is the time in `time_t` format (seconds since the UNIX epoch) that the service check was performed (or submitted). Please note the single space after the right bracket.
- `host_name` is the short name of the host associated with the service in the service definition
- `svc_description` is the description of the service as specified in the service definition
- `return_code` is the return code of the check (0=OK, 1=WARNING, 2=CRITICAL, 3=UNKNOWN)
- `plugin_output` is the text output of the service check (i.e. the plugin output)

---

### Note

A service must be defined in Nagios before you can submit passive check results for it! Nagios will ignore all check results for services that had not been configured before it was last (re)started.

---

---

### Tip

An example shell script of how to submit passive service check results to Nagios can be found in the documentation on [volatile services](#).

---

## 30.6 Submitting Passive Host Check Results

External applications can submit passive host check results to Nagios by writing a `PROCESS_HOST_CHECK_RESULT` external command to the external command file.

The format of the command is as follows: `[<timestamp>] PROCESS_HOST_CHECK_RESULT;<host_name>;<host-_status>;<plugin_output> where...`

- `timestamp` is the time in `time_t` format (seconds since the UNIX epoch) that the host check was performed (or submitted). Please note the single space after the right bracket.
- `host_name` is the short name of the host (as defined in the host definition)
- `host_status` is the status of the host (0=UP, 1=DOWN, 2=UNREACHABLE)
- `plugin_output` is the text output of the host check

---

### Note

A host must be defined in Nagios before you can submit passive check results for it! Nagios will ignore all check results for hosts that had not been configured before it was last (re)started.

---

## 30.7 Passive Checks and Host States

Unlike with active host checks, Nagios does not (by default) attempt to determine whether or host is DOWN or UNREACHABLE with passive checks. Rather, Nagios takes the passive check result to be the actual state the host is in and doesn't try to determine the host's actual state using the [reachability logic](#). This can cause problems if you are submitting passive checks from a remote host or you have a [distributed monitoring setup](#) where the parent/child host relationships are different.

You can tell Nagios to translate DOWN/UNREACHABLE passive check result states to their "proper" state by using the [translate\\_passive\\_host\\_checks](#) variable. More information on how this works can be found [here](#).

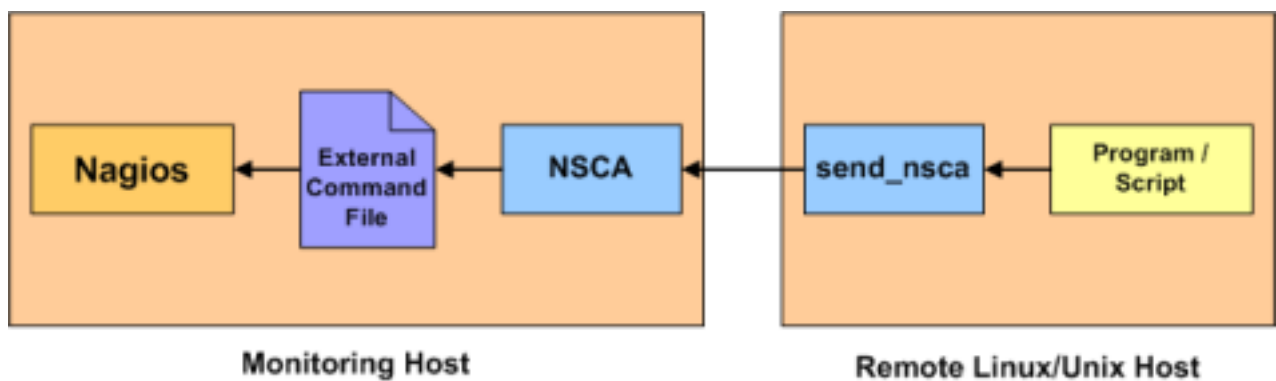
---

**Note**

Passive host checks are normally treated as **HARD states**, unless the [passive\\_host\\_checks\\_are\\_soft](#) option is enabled.

---

## 30.8 Submitting Passive Check Results From Remote Hosts



If an application that resides on the same host as Nagios is sending passive host or service check results, it can simply write the results directly to the external command file as outlined above. However, applications on remote hosts can't do this so easily.

In order to allow remote hosts to send passive check results to the monitoring host, I've developed the **NSCA** addon. The NSCA addon consists of a daemon that runs on the Nagios hosts and a client that is executed from remote hosts. The daemon will listen for connections from remote clients, perform some basic validation on the results being submitted, and then write the check results directly into the external command file (as described above). More information on the NSCA addon can be found [here](#).

## Chapter 31

# State Types

### 31.1 Introduction

The current state of monitored services and hosts is determined by two components:

- The status of the service or host (i.e. OK, WARNING, UP, DOWN, etc.)
- The type of state the service or host is in

There are two state types in Nagios - SOFT states and HARD states. These state types are a crucial part of the monitoring logic, as they are used to determine when **event handlers** are executed and when **notifications** are initially sent out.

This document describes the difference between SOFT and HARD states, how they occur, and what happens when they occur.

### 31.2 Service and Host Check Retries

In order to prevent false alarms from transient problems, Nagios allows you to define how many times a service or host should be (re)checked before it is considered to have a "real" problem. This is controlled by the `max_check_attempts` option in the host and service definitions. Understanding how hosts and services are (re)checked in order to determine if a real problem exists is important in understanding how state types work.

### 31.3 Soft States

Soft states occur in the following situations...

- When a service or host check results in a non-OK or non-UP state and the service check has not yet been (re)checked the number of times specified by the `max_check_attempts` directive in the service or host definition. This is called a soft error.
- When a service or host recovers from a soft error. This is considered a soft recovery.

The following things occur when hosts or services experience SOFT state changes:

- The SOFT state is logged.
- Event handlers are executed to handle the SOFT state.

SOFT states are only logged if you enabled the `log_service_retries` or `log_host_retries` options in your main configuration file.

The only important thing that really happens during a soft state is the execution of event handlers. Using event handlers can be particularly useful if you want to try and proactively fix a problem before it turns into a HARD state. The `$HOSTSTATETYPE$` or `$SERVICESTATETYPE$` macros will have a value of "SOFT" when event handlers are executed, which allows your event handler scripts to know when they should take corrective action. More information on event handlers can be found [here](#).

---



## 31.4 Hard States

Hard states occur for hosts and services in the following situations:

- When a host or service check results in a non-UP or non-OK state and it has been (re)checked the number of times specified by the `max_check_attempts` option in the host or service definition. This is a hard error state.
- When a host or service transitions from one hard error state to another error state (e.g. WARNING to CRITICAL).
- 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.
- When a **passive host check** is received. Passive host checks are treated as HARD unless the `passive_host_checks_are_soft` option is enabled.

The following things occur when hosts or services experience HARD state changes:

- The HARD state is logged.
- Event handlers are executed to handle the HARD state.
- Contacts are notified of the host or service problem or recovery.

The `$HOSTSTATETYPES` or `$SERVICESTATETYPES` macros will have a value of "HARD" when event handlers are executed, which allows your event handler scripts to know when they should take corrective action. More information on event handlers can be found [here](#).

## 31.5 Example

Here's an example of how state types are determined, when state changes occur, and when event handlers and notifications are sent out. The table below shows consecutive checks of a service over time. The service has a `max_check_attempts` value of 3.

| Time | Check # | State    | State Type | State Change | Notes                                                                                                                                                                                        |
|------|---------|----------|------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | 1       | OK       | HARD       | No           | Initial state of the service                                                                                                                                                                 |
| 1    | 1       | CRITICAL | SOFT       | Yes          | First detection of a non-OK state. Event handlers execute.                                                                                                                                   |
| 2    | 2       | WARNING  | SOFT       | Yes          | Service continues to be in a non-OK state. Event handlers execute.                                                                                                                           |
| 3    | 3       | CRITICAL | HARD       | Yes          | Max check attempts has been reached, so service goes into a HARD state. Event handlers execute and a problem notification is sent out. Check # is reset to 1 immediately after this happens. |

| Time | Check # | State   | State Type | State Change | Notes                                                                                                                                                                                                         |
|------|---------|---------|------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4    | 1       | WARNING | HARD       | Yes          | Service changes to a HARD WARNING state. Event handlers execute and a problem notification is sent out.                                                                                                       |
| 5    | 1       | WARNING | HARD       | No           | Service stabilizes in a HARD problem state. Depending on what the notification interval for the service is, another notification might be sent out.                                                           |
| 6    | 1       | OK      | HARD       | Yes          | Service experiences a HARD recovery. Event handlers execute and a recovery notification is sent out.                                                                                                          |
| 7    | 1       | OK      | HARD       | No           | Service is still OK.                                                                                                                                                                                          |
| 8    | 1       | UNKNOWN | SOFT       | Yes          | Service is detected as changing to a SOFT non-OK state. Event handlers execute.                                                                                                                               |
| 9    | 2       | OK      | SOFT       | Yes          | Service experiences a SOFT recovery. Event handlers execute, but notification are not sent, as this wasn't a "real" problem. State type is set HARD and check # is reset to 1 immediately after this happens. |
| 10   | 1       | OK      | HARD       | No           | Service stabilizes in an OK state.                                                                                                                                                                            |

## Chapter 32

# Time Periods

---

## **Abstract**

or...‘Is This a Good Time?’

## 32.1 Introduction



**Timeperiod** definitions allow you to control when various aspects of the monitoring and alerting logic can operate. For instance, you can restrict:

- When regularly scheduled host and service checks can be performed
- When notifications can be sent out
- When notification escalations can be used
- When dependencies are valid

## 32.2 Precedence in Time Periods

Timeperiod **definitions** may contain multiple types of directives, including weekdays, days of the month, and calendar dates. Different types of directives have different precedence levels and may override other directives in your timeperiod definitions. The order of precedence for different types of directives (in descending order) is as follows:

- Calendar date (2008-01-01)
- Specific month date (January 1st)
- Generic month date (Day 15)
- Offset weekday of specific month (2nd Tuesday in December)
- Offset weekday (3rd Monday)
- Normal weekday (Tuesday)

Examples of different timeperiod directives can be found [here](#).

## 32.3 How Time Periods Work With Host and Service Checks

Host and service definitions have an optional `check_period` directive that allows you to specify a timeperiod that should be used to restrict when regularly scheduled, active checks of the host or service can be made.

If you do not use the `check_period` directive to specify a timeperiod, Nagios will be able to schedule active checks of the host or service anytime it needs to. This is essentially a 24x7 monitoring scenario.

Specifying a timeperiod in the `check_period` directive allows you to restrict the time that Nagios perform regularly scheduled, active checks of the host or service. When Nagios attempts to reschedule a host or service check, it will make sure that the next check falls within a valid time range within the defined timeperiod. If it doesn't, Nagios will adjust the next check time to coincide with the next 'valid' time in the specified timeperiod. This means that the host or service may not get checked again for another hour, day, or week, etc.

---

### Note

On-demand checks and passive checks are not restricted by the timeperiod you specify in the `check_period` directive. Only regularly scheduled active checks are restricted.

---

Unless you have a good reason not to do so, I would recommend that you monitor all your hosts and services using timeperiods that cover a 24x7 time range. If you don't do this, you can run into some problems during "blackout" times (times that are not valid in the timeperiod definition):

1. The status of the host or service will appear unchanged during the blackout time.
2. Contacts will mostly likely not get re-notified of problems with a host or service during blackout times.
3. If a host or service recovers during a blackout time, contacts will not be immediately notified of the recovery.

## 32.4 How Time Periods Work With Contact Notifications

By specifying a timeperiod in the `notification_period` directive of a host or service definition, you can control when Nagios is allowed to send notifications out regarding problems or recoveries for that host or service. When a host notification is about to get sent out, Nagios will make sure that the current time is within a valid range in the `notification_period` timeperiod. If it is a valid time, then Nagios will attempt to notify each contact of the problem or recovery.

You can also use timeperiods to control when notifications can be sent out to individual contacts. By using the `service_notification_period` and `host_notification_period` directives in [contact definitions](#), you're able to essentially define an 'on call' period for each contact. Contacts will only receive host and service notifications during the times you specify in the notification period directives.

Examples of how to create timeperiod definitions for use for on-call rotations can be found [On-Call Rotations](#)here.

## 32.5 How Time Periods Work With Notification Escalations

Service and host [Notification Escalations](#) notification escalations have an optional `escalation_period` directive that allows you to specify a timeperiod when the escalation is valid and can be used. If you do not use the `escalation_period` directive in an escalation definition, the escalation is considered valid at all times. If you specify a timeperiod in the `escalation_period` directive, Nagios will only use the escalation definition during times that are valid in the timeperiod definition.

## 32.6 How Time Periods Work With Dependencies

Service and host [Host and Service Dependencies](#)dependencies have an optional `dependency_period` directive that allows you to specify a timeperiod when the dependencies are valid and can be used. If you do not use the `dependency_period` directive in a dependency definition, the dependency can be used at any time. If you specify a timeperiod in the `dependency_period` directive, Nagios will only use the dependency definition during times that are valid in the timeperiod definition.

---

## Chapter 33

# Determining Status and Reachability of Network Hosts

### 33.1 Introduction

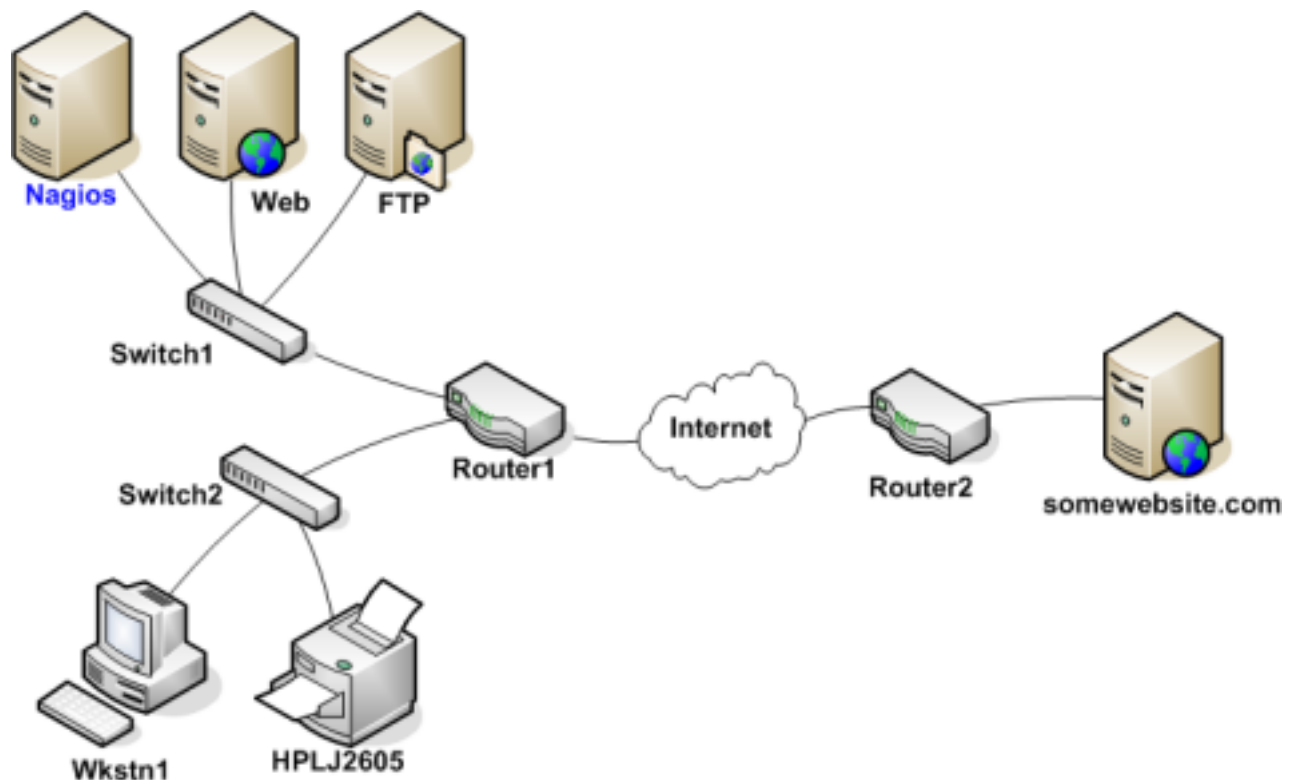
If you've ever work in tech support, you've undoubtedly had users tell you "the Internet is down". As a techie, you're pretty sure that no one pulled the power cord from the Internet. Something must be going wrong somewhere between the user's chair and the Internet.

Assuming its a technical problem, you begin to search for the problem. Perhaps the user's computer is turned off, maybe their network cable is unplugged, or perhaps your organization's core router just took a dive. Whatever the problem might be, one thing is most certain - the Internet isn't down. It just happens to be unreachable for that user.

Nagios is able to determine whether the hosts you're monitoring are in a `DOWN` or `UNREACHABLE` state. These are very different (although related) states and can help you quickly determine the root cause of network problems. Here's how the reachability logic works to distinguish between these two states...

### 33.2 Example Network

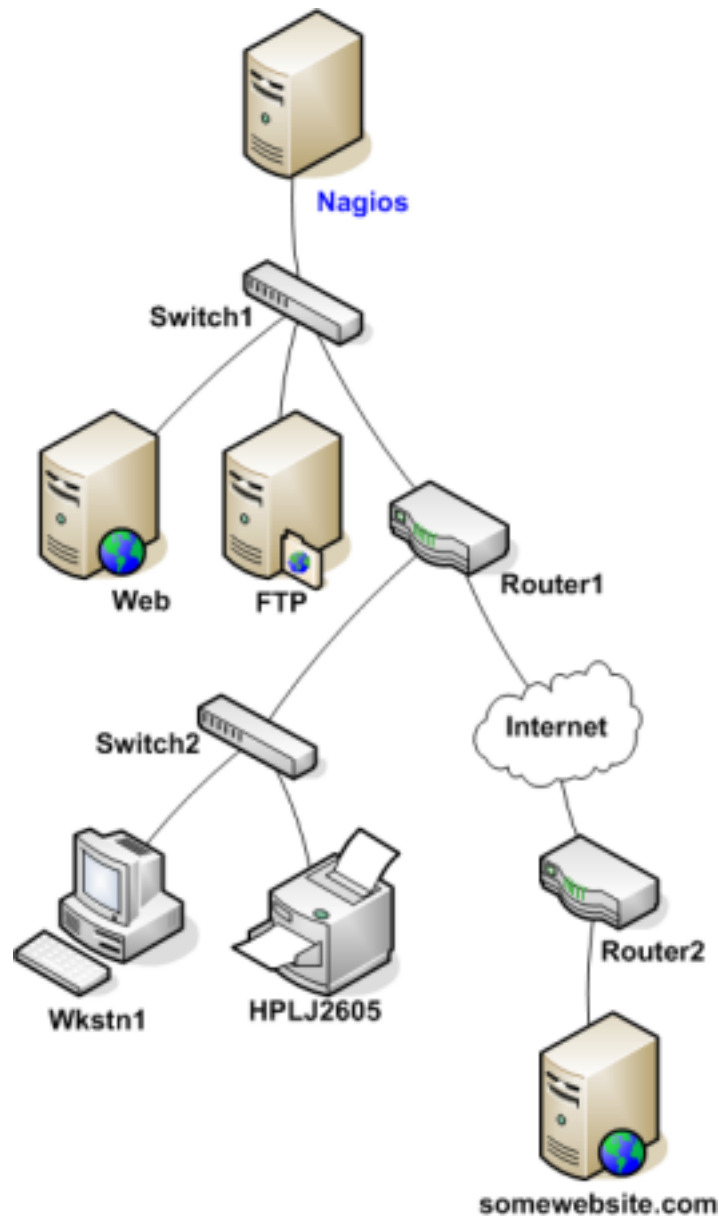
Take a look at the simple network diagram below. For this example, lets assume you're monitoring all the hosts (server, routers, switches, etc) that are pictured. Nagios is installed and running on the Nagios host.



### 33.3 Defining Parent/Child Relationships

In order for Nagios to be able to distinguish between DOWN and UNREACHABLE states for the hosts that are being monitored, you'll need to tell Nagios how those hosts are connected to each other - from the standpoint of the Nagios daemon. To do this, trace the path that a data packet would take from the Nagios daemon to each individual host. Each switch, router, and server the packet encounters or passes through is considered a "hop" and will require that you define a parent/child host relationship in Nagios. Here's what the host parent/child relationships look like from the viewpoint of Nagios:





Now that you know what the parent/child relationships look like for hosts that are being monitored, how do you configure Nagios to reflect them? The `parents` directive in your **host definitions** allows you to do this. Here's what the (abbreviated) host definitions with parent/child relationships would look like for this example:

```

define host{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Nagios ~ ; <-- The local host has no parent - it is the ←
 topmost host
 ~ ~ ~ ~ }

define host{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Switch1
 ~ ~ ~ ~ parents ~ ~ ~ ~ Nagios
 ~ ~ ~ ~ }
 ~ ~ ~ ~

define host{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Web
 ~ ~ ~ ~ parents ~ ~ ~ ~ Switch1
 ~ ~ ~ ~ }
 ~ ~ ~ ~

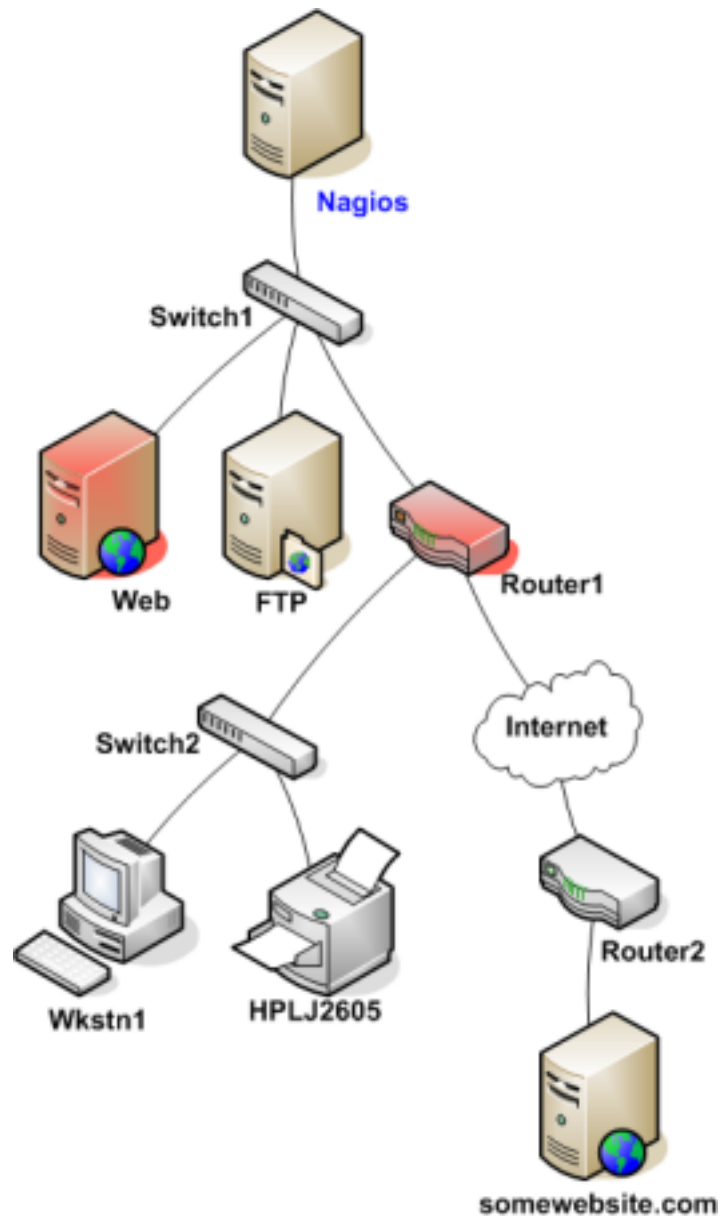
define host{

```

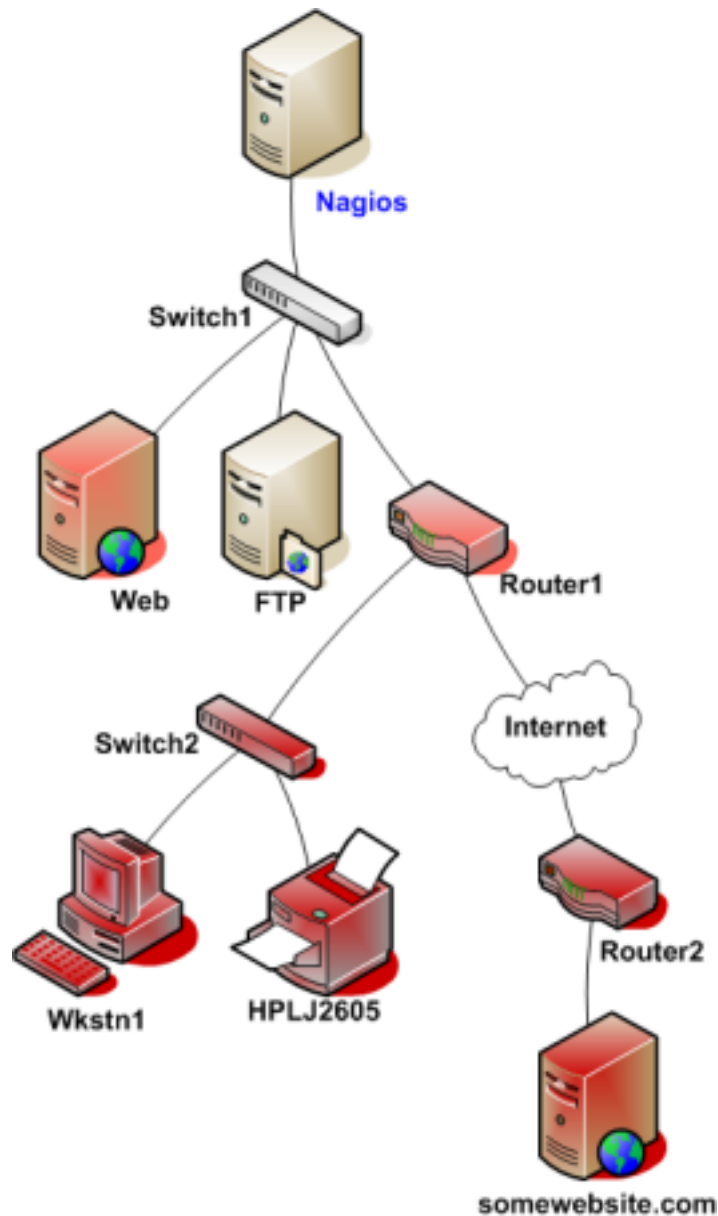
```
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ FTP
~ ~ ~ ~ parents ~ ~ ~ ~ Switch1
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Router1
~ ~ ~ ~ parents ~ ~ ~ ~ Switch1
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Switch2
~ ~ ~ ~ parents ~ ~ ~ ~ Router1
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Wkstn1
~ ~ ~ ~ parents ~ ~ ~ ~ Switch2
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ HPLJ2605
~ ~ ~ ~ parents ~ ~ ~ ~ Switch2
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ Router2
~ ~ ~ ~ parents ~ ~ ~ ~ Router1
~ ~ ~ ~ }
~ ~ ~ ~
define host{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ somewebsite.com
~ ~ ~ ~ parents ~ ~ ~ ~ Router2
~ ~ ~ ~ }
```

## 33.4 Reachability Logic in Action

Now that you're configured Nagios with the proper parent/child relationships for your hosts, let's see what happens when problems arise. Assume that two hosts - Web and Router1 - go offline...



When hosts change state (i.e. from UP to DOWN), the host reachability logic in Nagios kicks in. The reachability logic will initiate parallel checks of the parents and children of whatever hosts change state. This allows Nagios to quickly determine the current status of your network infrastructure when changes occur.



In this example, Nagios will determine that Web and Router1 are both in DOWN states because the "path" to those hosts is not being blocked.

Nagios will determine that all the hosts "beneath" Router1 are all in an UNREACHABLE state because Nagios can't reach them. Router1 is DOWN and is blocking the path to those other hosts. Those hosts might be running fine, or they might be offline - Nagios doesn't know because it can't reach them. Hence Nagios considers them to be UNREACHABLE instead of DOWN.

### 33.5 UNREACHABLE States and Notifications

By default, Nagios will notify contacts about both DOWN and UNREACHABLE host states. As an admin/tech, you might not want to get notifications about hosts that are UNREACHABLE. You know your network structure, and if Nagios notifies you that your router/firewall is down, you know that everything behind it is unreachable.

If you want to spare yourself from a flood of UNREACHABLE notifications during network outages, you can exclude the unreachable (u) option from the notification\_options directive in your **host** definitions and/or the host\_notification\_options directive in your **contact** definitions.

## Chapter 34

# Notifications

### 34.1 Introduction



I've had a lot of questions as to exactly how notifications work. This will attempt to explain exactly when and how host and service notifications are sent out, as well as who receives them.

Notification escalations are explained [here](#).

### 34.2 When Do Notifications Occur?

The decision to send out notifications is made in the service check and host check logic. Host and service notifications occur in the following instances...

- When a hard state change occurs. More information on state types and hard state changes can be found [here](#).
- When a host or service remains in a hard non-OK state and the time specified by the `<notification_interval>` option in the host or service definition has passed since the last notification was sent out (for that specified host or service).

### 34.3 Who Gets Notified?

Each host and service definition has a `<contact_groups>` option that specifies what contact groups receive notifications for that particular host or service. Contact groups can contain one or more individual contacts.

When Nagios sends out a host or service notification, it will notify each contact that is a member of any contact groups specified in the `<contactgroups>` option of the service definition. Nagios realizes that a contact may be a member of more than one contact group, so it removes duplicate contact notifications before it does anything.

---

## 34.4 What Filters Must Be Passed In Order For Notifications To Be Sent?

Just because there is a need to send out a host or service notification doesn't mean that any contacts are going to get notified. There are several filters that potential notifications must pass before they are deemed worthy enough to be sent out. Even then, specific contacts may not be notified if their notification filters do not allow for the notification to be sent to them. Let's go into the filters that have to be passed in more detail...

### 34.5 Program-Wide Filter:

The first filter that notifications must pass is a test of whether or not notifications are enabled on a program-wide basis. This is initially determined by the `enable_notifications` directive in the main config file, but may be changed during runtime from the web interface. If notifications are disabled on a program-wide basis, no host or service notifications can be sent out - period. If they are enabled on a program-wide basis, there are still other tests that must be passed...

### 34.6 Service and Host Filters:

The first filter for host or service notifications is a check to see if the host or service is in a period of `scheduled downtime`. If it is in a scheduled downtime, no one gets notified. If it isn't in a period of downtime, it gets passed on to the next filter. As a side note, notifications for services are suppressed if the host they're associated with is in a period of scheduled downtime.

The second filter for host or service notification is a check to see if the host or service is `flapping` (if you enabled flap detection). If the service or host is currently flapping, no one gets notified. Otherwise it gets passed to the next filter.

The third host or service filter that must be passed is the host- or service-specific notification options. Each service definition contains options that determine whether or not notifications can be sent out for warning states, critical states, and recoveries. Similarly, each host definition contains options that determine whether or not notifications can be sent out when the host goes down, becomes unreachable, or recovers. If the host or service notification does not pass these options, no one gets notified. If it does pass these options, the notification gets passed to the next filter...

---

#### Note

Notifications about host or service recoveries are only sent out if a notification was sent out for the original problem. It doesn't make sense to get a recovery notification for something you never knew was a problem.

---

The fourth host or service filter that must be passed is the time period test. Each host and service definition has a `<notification_period>` option that specifies which time period contains valid notification times for the host or service. If the time that the notification is being made does not fall within a valid time range in the specified time period, no one gets contacted. If it falls within a valid time range, the notification gets passed to the next filter...

---

#### Note

If the time period filter is not passed, Nagios will reschedule the next notification for the host or service (if its in a non-OK state) for the next valid time present in the time period. This helps ensure that contacts are notified of problems as soon as possible when the next valid time in time period arrives.

---

The last set of host or service filters is conditional upon two things: (1) a notification was already sent out about a problem with the host or service at some point in the past and (2) the host or service has remained in the same non-OK state that it was when the last notification went out. If these two criteria are met, then Nagios will check and make sure the time that has passed since the last notification went out either meets or exceeds the value specified by the `<notification_interval>` option in the host or service definition. If not enough time has passed since the last notification, no one gets contacted. If either enough time has passed since the last notification or the two criteria for this filter were not met, the notification will be sent out! Whether or not it actually is sent to individual contacts is up to another set of filters...

---

## 34.7 Contact Filters:

At this point the notification has passed the program mode filter and all host or service filters and Nagios starts to notify **all the people it should**. Does this mean that each contact is going to receive the notification? No! Each contact has their own set of filters that the notification must pass before they receive it.

---

**Note**

Contact filters are specific to each contact and do not affect whether or not other contacts receive notifications.

---

The first filter that must be passed for each contact are the notification options. Each contact definition contains options that determine whether or not service notifications can be sent out for warning states, critical states, and recoveries. Each contact definition also contains options that determine whether or not host notifications can be sent out when the host goes down, becomes unreachable, or recovers. If the host or service notification does not pass these options, the contact will not be notified. If it does pass these options, the notification gets passed to the next filter...

---

**Note**

Notifications about host or service recoveries are only sent out if a notification was sent out for the original problem. It doesn't make sense to get a recovery notification for something you never knew was a problem...

---

The last filter that must be passed for each contact is the time period test. Each contact definition has a `<notification_period>` option that specifies which time period contains valid notification times for the contact. If the time that the notification is being made does not fall within a valid time range in the specified time period, the contact will not be notified. If it falls within a valid time range, the contact gets notified!

## 34.8 Notification Methods

You can have Nagios notify you of problems and recoveries pretty much anyway you want: pager, cellphone, email, instant message, audio alert, electric shocker, etc. How notifications are sent depend on the **notification commands** that are defined in your **object definition files**.

---

**Note**

If you install Nagios according to the **quickstart guide**, it should be configured to send email notifications. You can see the email notification commands that are used by viewing the contents of the following file: `/usr/local/nagios/etc/objects/commands.cfg`.

---

Specific notification methods (paging, etc.) are not directly incorporated into the Nagios code as it just doesn't make much sense. The "core" of Nagios is not designed to be an all-in-one application. If service checks were embedded in Nagios' core it would be very difficult for users to add new check methods, modify existing checks, etc. Notifications work in a similar manner. There are a thousand different ways to do notifications and there are already a lot of packages out there that handle the dirty work, so why re-invent the wheel and limit yourself to a bike tire? It's much easier to let an external entity (i.e. a simple script or a full-blown messaging system) do the messy stuff. Some messaging packages that can handle notifications for pagers and cellphones are listed below in the resource section.

## 34.9 Notification Type Macro

When crafting your notification commands, you need to take into account what type of notification is occurring. The **\$NOTIFICATIONTYPE\$** macro contains a string that identifies exactly that. The table below lists the possible values for the macro and their respective descriptions:

---

| Value             | Description                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PROBLEM           | A service or host has just entered (or is still in) a problem state. If this is a service notification, it means the service is either in a WARNING, UNKNOWN or CRITICAL state. If this is a host notification, it means the host is in a DOWN or UNREACHABLE state. |
| RECOVERY          | A service or host recovery has occurred. If this is a service notification, it means the service has just returned to an OK state. If it is a host notification, it means the host has just returned to an UP state.                                                 |
| ACKNOWLEDGEMENT   | This notification is an acknowledgement notification for a host or service problem. Acknowledgement notifications are initiated via the web interface by contacts for the particular host or service.                                                                |
| FLAPPINGSTART     | The host or service has just started <b>flapping</b> .                                                                                                                                                                                                               |
| FLAPPINGSTOP      | The host or service has just stopped <b>flapping</b> .                                                                                                                                                                                                               |
| FLAPPINGDISABLED  | The host or service has just stopped <b>flapping</b> because flap detection was disabled..                                                                                                                                                                           |
| DOWNTIMESTART     | The host or service has just entered a period of <b>scheduled downtime</b> . Future notifications will be suppressed.                                                                                                                                                |
| DOWNTIMESTOP      | The host or service has just exited from a period of <b>scheduled downtime</b> . Notifications about problems can now resume.                                                                                                                                        |
| DOWNTIMECANCELLED | The period of <b>scheduled downtime</b> for the host or service was just cancelled. Notifications about problems can now resume.                                                                                                                                     |

## 34.10 Helpful Resources

There are many ways you could configure Nagios to send notifications out. Its up to you to decide which method(s) you want to use. Once you do that you'll have to install any necessary software and configure notification commands in your config files before you can use them. Here are just a few possible notification methods:

- Email
- Pager
- Phone (SMS)
- WinPopup message
- Yahoo, ICQ, or MSN instant message
- Audio alerts
- etc...

Basically anything you can do from a command line can be tailored for use as a notification command.

If you're looking for an alternative to using email for sending messages to your pager or cellphone, check out these packages. They could be used in conjunction with Nagios to send out a notification via a modem when a problem arises. That way you don't have to rely on email to send notifications out (remember, email may *\*not\** work if there are network problems). I haven't actually tried these packages myself, but others have reported success using them...

- **Gnokii** (SMS software for contacting Nokia phones via GSM network)
- **QuickPage** (alphanumeric pager software)



- [Sendpage](#) (paging software)
- [SMS Client](#) (command line utility for sending messages to pagers and mobile phones)

If you want to try out a non-traditional method of notification, you might want to mess around with audio alerts. If you want to have audio alerts played on the monitoring server (with synthesized speech), check out [Festival](#). If you'd rather leave the monitoring box alone and have audio alerts played on another box, check out the [Network Audio System \(NAS\)](#) and [rplay](#) projects.

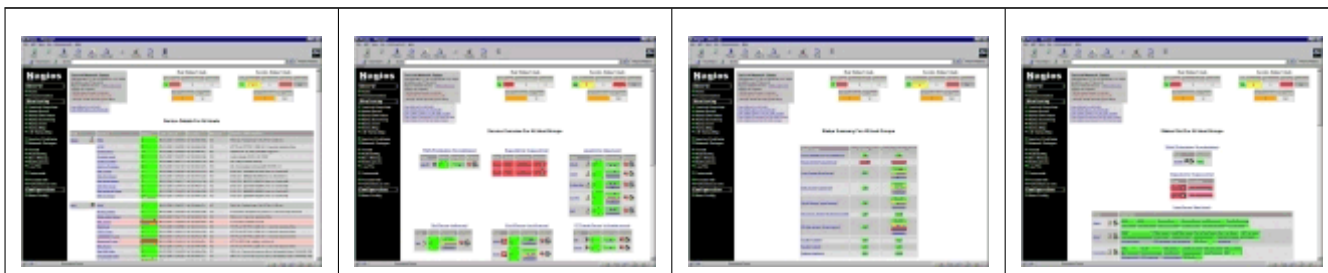
## Chapter 35

# Information On The CGIs

### 35.1 Introduction

The various CGIs distributed with Nagios are described here, along with the authorization requirements for accessing and using each CGI. By default the CGIs require that you have authenticated to the web server and are authorized to view any information you are requesting. More information on configuring authorization can be found [here](#).

### 35.2 Status CGI



File Name:

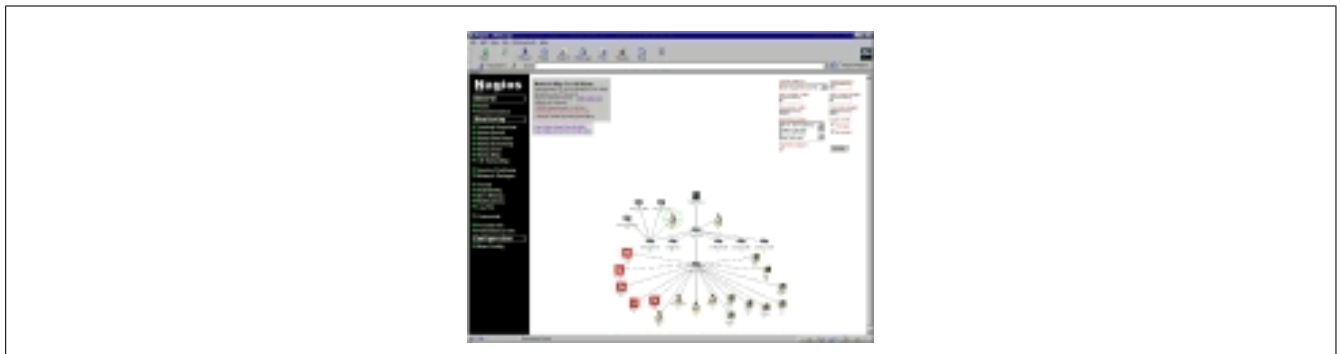
status.cgi

Description: This is the most important CGI included with Nagios. It allows you to view the current status of all hosts and services that are being monitored. The status CGI can produce two main types of output - a status overview of all host groups (or a particular host group) and a detailed view of all services (or those associated with a particular host).

Authorization Requirements:

- If you are **authorized for all hosts** you can view all hosts and all services.
- If you are **authorized for all services** you can view all services.
- If you are an authenticated contact you can view all hosts and services for which you are a contact.

### 35.3 Status Map CGI



|            |               |
|------------|---------------|
| File Name: | statusmap.cgi |
|------------|---------------|

Description: This CGI creates a map of all hosts that you have defined on your network. The CGI uses Thomas Boutell's [gd](#) library (version 1.6.3 or higher) to create a PNG image of your network layout. The coordinates used when drawing each host (along with the optional pretty icons) are taken from [host](#) definitions. If you'd prefer to let the CGI automatically generate drawing coordinates for you, use the [default\\_statusmap\\_layout](#) directive to specify a layout algorithm that should be used.

Authorization Requirements:

- If you are [authorized for all hosts](#) you can view all hosts.
- If you are an authenticated contact you can view hosts for which you are a contact.

---

**Note**

Users who are not authorized to view specific hosts will see unknown nodes in those positions. I realize that they really shouldn't see anything there, but it doesn't make sense to even generate the map if you can't see all the host dependencies...

---

## 35.4 WAP Interface CGI



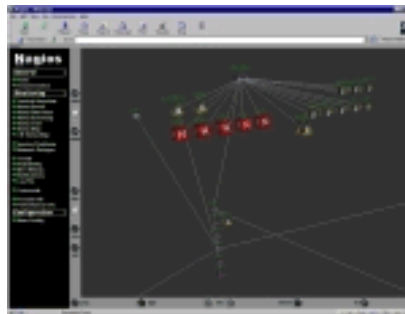
|            |               |
|------------|---------------|
| File Name: | statuswml.cgi |
|------------|---------------|

Description: This CGI serves as a WAP interface to network status information. If you have a WAP-enabled device (i.e. an Internet-ready cellphone), you can view status information while you're on the go. Different status views include hostgroup summary, hostgroup overview, host detail, service detail, all problems, and unhandled problems. In addition to viewing status information, you can also disable notifications and checks and acknowledge problems from your cellphone. Pretty cool, huh?

Authorization Requirements:

- If you are **authorized for system information** you can view Nagios process information.
- If you are **authorized for all hosts** you can view status data for all hosts and services.
- If you are **authorized for all services** you can view status data for all services.
- If you are an authenticated contact you can view status data for all hosts and services for which you are a contact.

## 35.5 Status World CGI (VRML)



File Name:

statuswrl.cgi

Description: This CGI creates a 3-D VRML model of all hosts that you have defined on your network. Coordinates used when drawing the hosts (as well as pretty texture maps) are taken from **host** definitions. If you'd prefer to let the CGI automatically generate drawing coordinates for you, use the **default\_statuswrl\_layout** directive to specify a layout algorithm that should be used. You'll need a VRML browser (like **Cortona**, **Cosmo Player** or **WorldView**) installed on your system before you can actually view the generated model.

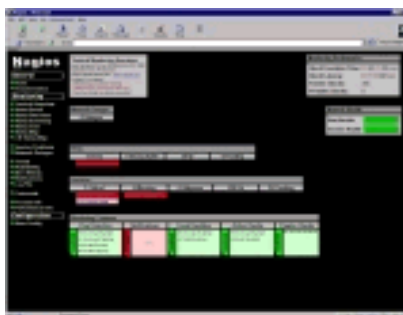
Authorization Requirements:

- If you are **authorized for all hosts** you can view all hosts.
- If you are an authenticated contact you can view hosts for which you are a contact.

### Note

Users who are not authorized to view specific hosts will see unknown nodes in those positions. I realize that they really shouldn't see anything there, but it doesn't make sense to even generate the map if you can't see all the host dependencies...

## 35.6 Tactical Overview CGI



|            |         |
|------------|---------|
| File Name: | tac.cgi |
|------------|---------|

Description: This CGI is designed to server as a "birds-eye view" of all network monitoring activity. It allows you to quickly see network outages, host status, and service status. It distinguishes between problems that have been "handled" in some way (i.e. been acknowledged, had notifications disabled, etc.) and those which have not been handled, and thus need attention. Very useful if you've got a lot of hosts/services you're monitoring and you need to keep a single screen up to alert you of problems.

Authorization Requirements:

- If you are **authorized for all hosts** you can view all hosts and all services.
- If you are **authorized for all services** you can view all services.
- If you are an authenticated contact you can view all hosts and services for which you are a contact.

## 35.7 Network Outages CGI



|            |             |
|------------|-------------|
| File Name: | outages.cgi |
|------------|-------------|

Description: This CGI will produce a listing of "problem" hosts on your network that are causing network outages. This can be particularly useful if you have a large network and want to quickly identify the source of the problem. Hosts are sorted based on the severity of the outage they are causing.

Authorization Requirements:

- If you are **authorized for all hosts** you can view all hosts.
- If you are an authenticated contact you can view hosts for which you are a contact.

## 35.8 Configuration CGI



File Name:

config.cgi

Description: This CGI allows you to view objects (i.e. hosts, host groups, contacts, contact groups, time periods, services, etc.) that you have defined in your **object configuration file(s)**.

Authorization Requirements:

- You must be **authorized for configuration information** in order to any kind of configuration information.

## 35.9 Command CGI



File Name:

cmd.cgi

Description: This CGI allows you to send commands to the Nagios process. Although this CGI has several arguments, you would be better to leave them alone. Most will change between different revisions of Nagios. Use the **extended information CGI** as a starting point for issuing commands.

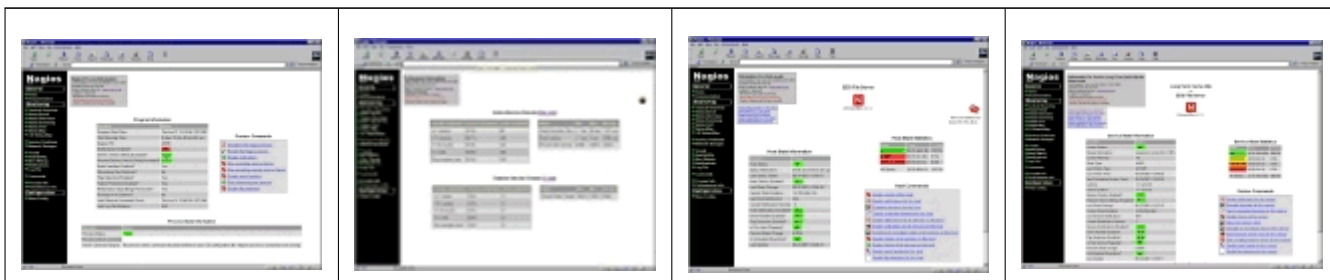
Authorization Requirements:

- You must be **authorized for system commands** in order to issue commands that affect the Nagios process (restarts, shutdowns, mode changes, etc.).
- If you are **authorized for all host commands** you can issue commands for all hosts and services.
- If you are **authorized for all service commands** you can issue commands for all services.
- If you are an authenticated contact you can issue commands for all hosts and services for which you are a contact.

Notes:

- If you have chosen not to **use authentication** with the CGIs, this CGI will not allow anyone to issue commands to Nagios. This is done for your own protection. I would suggest removing this CGI altogether if you decide not to use authentication with the CGIs.

## 35.10 Extended Information CGI



File Name:

extinfo.cgi

Description: This CGI allows you to view Nagios process information, host and service state statistics, host and service comments, and more. It also serves as a launching point for sending commands to Nagios via the **command CGI**. Although this CGI has several arguments, you would be better to leave them alone - they are likely to change between different releases of Nagios. You can access this CGI by clicking on the 'Network Health' and 'Process Information' links on the side navigation bar, or by clicking on a host or service link in the output of the **status CGI**.

Authorization Requirements:

- You must be **authorized for system information** in order to view Nagios process information.
- If you are **authorized for all hosts** you can view extended information for all hosts and services.
- If you are **authorized for all services** you can view extended information for all services.
- If you are an authenticated contact you can view extended information for all hosts and services for which you are a contact.

## 35.11 Event Log CGI



|            |             |
|------------|-------------|
| File Name: | showlog.cgi |
|------------|-------------|

Description: This CGI will display the **log file**. If you have **log rotation** enabled, you can browse notifications present in archived log files by using the navigational links near the top of the page.

Authorization Requirements:

- You must be **authorized for system information** in order to view the log file.

## 35.12 Alert History CGI



|            |             |
|------------|-------------|
| File Name: | history.cgi |
|------------|-------------|

Description: This CGI is used to display the history of problems with either a particular host or all hosts. The output is basically a subset of the information that is displayed by the **log file CGI**. You have the ability to filter the output to display only the specific types of problems you wish to see (i.e. hard and/or soft alerts, various types of service and host alerts, all types of alerts, etc.). If you have **log rotation** enabled, you can browse history information present in archived log files by using the navigational links near the top of the page.

Authorization Requirements:

- If you are **authorized for all hosts** you can view history information for all hosts and all services.
- If you are **authorized for all services** you can view history information for all services.
- If you are an authenticated contact you can view history information for all services and hosts for which you are a contact.



## 35.13 Notifications CGI



|            |                   |
|------------|-------------------|
| File Name: | notifications.cgi |
|------------|-------------------|

Description: This CGI is used to display host and service notifications that have been sent to various contacts. The output is basically a subset of the information that is displayed by the [log file CGI](#). You have the ability to filter the output to display only the specific types of notifications you wish to see (i.e. service notifications, host notifications, notifications sent to specific contacts, etc). If you have [log rotation](#) enabled, you can browse notifications present in archived log files by using the navigational links near the top of the page.

Authorization Requirements:

- If you are [authorized for all hosts](#) you can view notifications for all hosts and all services.
- If you are [authorized for all services](#) you can view notifications for all services.
- If you are an authenticated contact you can view notifications for all services and hosts for which you are a contact.

## 35.14 Trends CGI



|            |            |
|------------|------------|
| File Name: | trends.cgi |
|------------|------------|

Description: This CGI is used to create a graph of host or service states over an arbitrary period of time. In order for this CGI to be of much use, you should enable **log rotation** and keep archived logs in the path specified by the **log\_archive\_path** directive. The CGI uses Thomas Boutell's **gd** library (version 1.6.3 or higher) to create the trends image. Authorization Requirements:

- If you are **authorized for all hosts** you can view trends for all hosts and all services.
- If you are **authorized for all services** you can view trends for all services.
- If you are an authenticated contact you can view trends for all services and hosts for which you are a contact.

## 35.15 Availability Reporting CGI



File Name:

avail.cgi

Description: This CGI is used to report on the availability of hosts and services over a user-specified period of time. In order for this CGI to be of much use, you should enable **log rotation** and keep archived logs in the path specified by the **log\_archive\_path** directive.

Authorization Requirements:

- If you are **authorized for all hosts** you can view availability data for all hosts and all services.
- If you are **authorized for all services** you can view availability data for all services.
- If you are an authenticated contact you can view availability data for all services and hosts for which you are a contact.

## 35.16 Alert Histogram CGI



|            |               |
|------------|---------------|
| File Name: | histogram.cgi |
|------------|---------------|

Description: This CGI is used to report on the availability of hosts and services over a user-specified period of time. In order for this CGI to be of much use, you should enable **log rotation** and keep archived logs in the path specified by the **log\_archive\_path** directive. The CGI uses Thomas Boutell's **gd** library (version 1.6.3 or higher) to create the histogram image.

Authorization Requirements:

- If you are **authorized for all hosts** you can view histograms for all hosts and all services.
- If you are **authorized for all services** you can view histograms for all services.
- If you are an authenticated contact you can view histograms for all services and hosts for which you are a contact.

## 35.17 Alert Summary CGI



|            |             |
|------------|-------------|
| File Name: | summary.cgi |
|------------|-------------|

Description: This CGI provides some generic reports about host and service alert data, including alert totals, top alert producers, etc.

Authorization Requirements:

- If you are **authorized for all hosts** you can view summary information for all hosts and all services.
- If you are **authorized for all services** you can view summary information for all services.
- If you are an authenticated contact you can view summary information for all services and hosts for which you are a contact.

# **Part VI**

## **Advanced Topics**

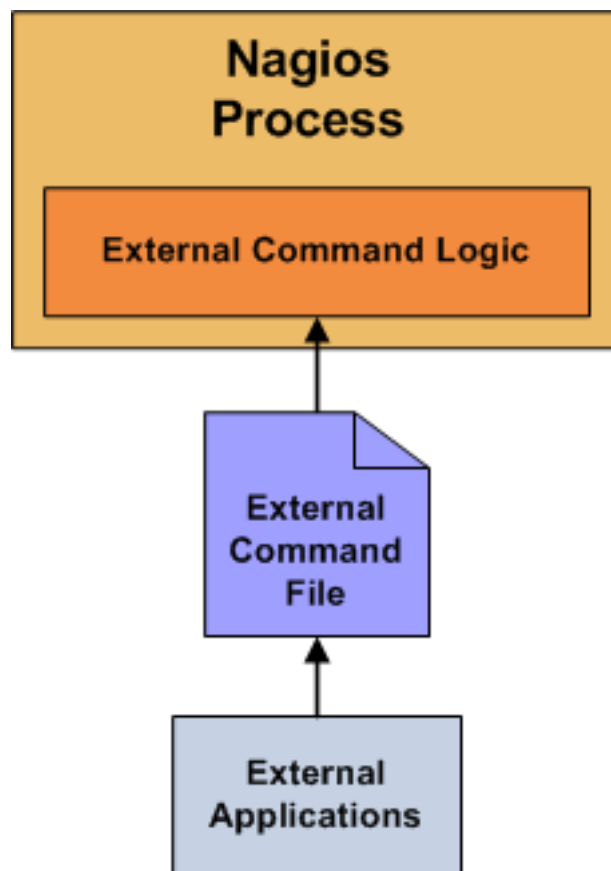
## Chapter 36

# External Commands

### 36.1 Introduction

Nagios can process commands from external applications (including the CGIs) and alter various aspects of its monitoring functions based on the commands it receives. External applications can submit commands by writing to the **command file**, which is periodically processed by the Nagios daemon.

### 36.2 Enabling External Commands



In order to have Nagios process external commands, make sure you do the following:

- Enable external command checking with the `check_external_commands` option.
- Set the frequency of command checks with the `command_check_interval` option.
- Specify the location of the command file with the `command_file` option.
- Setup proper permissions on the directory containing the external command file, as described in the [quickstart guide](#).

### 36.3 When Does Nagios Check For External Commands?

- At regular intervals specified by the `command_check_interval` option in the main configuration file
- Immediately after `event handlers` are executed. This is in addition to the regular cycle of external command checks and is done to provide immediate action if an event handler submits commands to Nagios.

### 36.4 Using External Commands

External commands can be used to accomplish a variety of things while Nagios is running. Example of what can be done include temporarily disabling notifications for services and hosts, temporarily disabling service checks, forcing immediate service checks, adding comments to hosts and services, etc.

### 36.5 Command Format

External commands that are written to the `command file` have the following format...

```
[time] command_id;command_arguments
```

...where time is the time (in `time_t` format) that the external application submitted the external command to the command file. The values for the `command_id` and `command_arguments` arguments will depend on what command is being submitted to Nagios.

A full listing of external commands that can be used (along with examples of how to use them) can be found online at the following URL:

<http://www.nagios.org/developerinfo/externalcommands/>

---

## Chapter 37

# Event Handlers

### 37.1 Introduction



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

An obvious use for event handlers is the ability for Nagios to proactively fix problems before anyone is notified. Some other uses for event handlers include:

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



#### **Important**

Cycling power on a host that is experiencing problems with an automated script should not be implemented lightly. Consider the consequences of this carefully before implementing automatic reboots. :-)

---

### 37.2 When Are Event Handlers Executed?

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

SOFT and HARD states are described in detail [here](#) .

### 37.3 Event Handler Types

There are different types of optional event handlers that you can define to handle host and state changes:

- Global host event handler
- Global service event handler
- Host-specific event handlers
- Service-specific event handlers

Global host and service event handlers are run for every host or service state change that occurs, immediately prior to any host- or service-specific event handler that may be run. You can specify global event handler commands by using the `global_host_event_handler` and `global_service_event_handler` options in your main configuration file.

Individual hosts and services can have their own event handler command that should be run to handle state changes. You can specify an event handler that should be run by using the `event_handler` directive in your `host` and `service` definitions. These host- and service-specific event handlers are executed immediately after the (optional) global host or service event handler is executed.

### 37.4 Enabling Event Handlers

Event handlers can be enabled or disabled on a program-wide basis by using the `enable_event_handlers` in your main configuration file.

Host- and service-specific event handlers can be enabled or disabled by using the `event_handler_enabled` directive in your `host` and `service` definitions. Host- and service-specific event handlers will not be executed if the global `enable_event_handlers` option is disabled.

### 37.5 Event Handler Execution Order

As already mentioned, global host and service event handlers are executed immediately before host- or service-specific event handlers.

Event handlers are executed for HARD problem and recovery states immediately after notifications are sent out.

### 37.6 Writing Event Handler Commands

Event handler commands will likely be shell or perl scripts, but they can be any type of executable that can run from a command prompt. At a minimum, the scripts should take the following `macros` as arguments:

For Services: `$SERVICESTATE$`, `$SERVICESTATETYPE$`, `$SERVICEATTEMPT$` For Hosts: `$HOSTSTATE$`, `$HOSTSTATETYPE$`, `$HOSTATTEMPT$`

The scripts should examine the values of the arguments passed to it and take any necessary action based upon those values. The best way to understand how event handlers work is to see an example. Lucky for you, one is provided [below](#).



**Tip**

Additional sample event handler scripts can be found in the `contrib/eventhandlers/` subdirectory of the Nagios distribution. Some of these sample scripts demonstrate the use of **external commands** to implement a **redundant** and **distributed** monitoring environments.

## 37.7 Permissions For Event Handler Commands

Event handler commands will normally execute with the same permissions as the user under which Nagios is running on your machine. This can present a problem if you want to write an event handler that restarts system services, as root privileges are generally required to do these sorts of tasks.

Ideally you should evaluate the types of event handlers you will be implementing and grant just enough permissions to the Nagios user for executing the necessary system commands. You might want to try using **sudo** to accomplish this.

## 37.8 Service Event Handler Example

The example below assumes that you are monitoring the HTTP server on the local machine and have specified `restart-httpd` as the event handler command for the HTTP service definition. Also, I will be assuming that you have set the `max_check_attempts` option for the service to be a value of 4 or greater (i.e. the service is checked 4 times before it is considered to have a real problem). An abbreviated example service definition might look like this...

```
define service{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ somehost
 ~ ~ ~ ~ service_description ~ ~ HTTP
 ~ ~ ~ ~ max_check_attempts ~ ~ ~4
 ~ ~ ~ ~ event_handler ~ ~ ~ ~ restart-httpd
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```

Once the service has been defined with an event handler, we must define that event handler as a command. An example command definition for `restart-httpd` is shown below. Notice the macros in the command line that I am passing to the event handler script - these are important!

```
define command{
 ~ ~ ~ ~ command_name ~ ~restart-httpd
 ~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/eventhandlers/restart-httpd ~ ↔
 ~ ~ ~ ~ $SERVICESTATE$ $SERVICESTATETYPE$ $SERVICEATTEMPTS$
 ~ ~ ~ ~ }
```

Now, let's actually write the event handler script (this is the `/usr/local/nagios/libexec/eventhandlers/restart-httpd` script).

```
#!/bin/sh
#
Event handler script for restarting the web server on the local machine
#
Note: This script will only restart the web server if the service is
~ ~ ~ retried 3 times (in a "soft" state) or if the web service somehow
~ ~ ~ manages to fall into a "hard" error state.
#
What state is the HTTP service in?
case "$1" in
 OK)
 ~ ~ ~ ~ # The service just came back up, so don't do anything...
 ~ ~ ~ ~ ;;
 WARNING)
```

```

~ ~ ~ ~ # We don't really care about warning states, since the service is probably ↵
still running...
~ ~ ~ ~ ;;
UNKNOWN)
~ ~ ~ ~ # We don't know what might be causing an unknown error, so don't do anything ↵
...
~ ~ ~ ~ ;;
CRITICAL)
~ ~ ~ ~ # Aha! ~The HTTP service appears to have a problem - perhaps we should ↵
restart the server...
~ ~ ~ ~ # Is this a "soft" or a "hard" state?
~ ~ ~ ~ case "$2" in

~ ~ ~ ~ # We're in a "soft" state, meaning that Nagios is in the middle of retrying ↵
the
~ ~ ~ ~ # check before it turns into a "hard" state and contacts get notified...
~ ~ ~ ~ SOFT)

~ ~ ~ ~ ~ ~ ~ ~ # What check attempt are we on? ~We don't want to restart the web ↵
server on the first
~ ~ ~ ~ ~ ~ ~ ~ # check, because it may just be a fluke!
~ ~ ~ ~ ~ ~ ~ ~ case "$3" in

~ ~ ~ ~ ~ ~ ~ ~ # Wait until the check has been tried 3 times before restarting the ↵
web server.
~ ~ ~ ~ ~ ~ ~ ~ # If the check fails on the 4th time (after we restart the web server ↵
), the state
~ ~ ~ ~ ~ ~ ~ ~ # type will turn to "hard" and contacts will be notified of the ↵
problem.
~ ~ ~ ~ ~ ~ ~ ~ # Hopefully this will restart the web server successfully, so the 4th ↵
check will
~ ~ ~ ~ ~ ~ ~ ~ # result in a "soft" recovery. ~If that happens no one gets notified ↵
because we
~ ~ ~ ~ ~ ~ ~ ~ # fixed the problem!
~ ~ ~ ~ ~ ~ ~ ~ 3)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ echo -n "Restarting HTTP service (3rd soft critical state) ↵
..."
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ # Call the init script to restart the HTTPD server
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ /etc/rc.d/init.d/httpd restart
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ esac
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;

~ ~ ~ ~ # The HTTP service somehow managed to turn into a hard error without getting ↵
fixed.
~ ~ ~ ~ # It should have been restarted by the code above, but for some reason it ↵
didn't.
~ ~ ~ ~ # Let's give it one last try, shall we? ~
~ ~ ~ ~ # Note: Contacts have already been notified of a problem with the service at ↵
this
~ ~ ~ ~ # point (unless you disabled notifications for this service)
~ ~ ~ ~ HARD)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ echo -n "Restarting HTTP service..."
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ # Call the init script to restart the HTTPD server
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ /etc/rc.d/init.d/httpd restart
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ esac
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
esac
exit 0

```

The sample script provided above will attempt to restart the web server on the local machine in two different instances:

- After the service has been rechecked for the 3rd time and is in a **SOFT CRITICAL** state
- After the service first goes into a **HARD CRITICAL** state

The script should theoretically restart and web server and fix the problem before the service goes into a **HARD** problem state, but we include a fallback case in the event it doesn't work the first time. It should be noted that the event handler will only be executed the first time that the service falls into a **HARD** problem state. This prevents Nagios from continuously executing the script to restart the web server if the service remains in a **HARD** problem state. You don't want that. :-)

That's all there is to it! Event handlers are pretty simple to write and implement, so give it a try and see what you can do.

---

## Chapter 38

# Volatile Services

### 38.1 Introduction

Nagios has the ability to distinguish between ‘normal’ services and "volatile" services. The `is_volatile` option in each service definition allows you to specify whether a specific service is volatile or not. For most people, the majority of all monitored services will be non-volatile (i.e. ‘normal’). However, volatile services can be very useful when used properly...

### 38.2 What Are They Useful For?

Volatile services are useful for monitoring...

- Things that automatically reset themselves to an "OK" state each time they are checked
- Events such as security alerts which require attention every time there is a problem (and not just the first time)

### 38.3 What's So Special About Volatile Services?

Volatile services differ from ‘normal’ services in three important ways. Each time they are checked when they are in a **hard** non-OK state, and the check returns a non-OK state (i.e. no state change has occurred)...

- The non-OK service state is logged
- Contacts are notified about the problem (if that's **what should be done**).

---

**Note**

Notification intervals are ignored for volatile services.

---

- The **event handler** for the service is run (if one has been defined)

These events normally only occur for services when they are in a non-OK state and a hard state change has just occurred. In other words, they only happen the first time that a service goes into a non-OK state. If future checks of the service result in the same non-OK state, no hard state change occurs and none of the events mentioned take place again.

---

**Tip**

If you are only interested in logging, consider using **stalking** options instead.

---

## 38.4 The Power Of Two

If you combine the features of volatile services and **passive service checks**, you can do some very useful things. Examples of this include handling SNMP traps, security alerts, etc.

How about an example... Let's say you're running **PortSentry** to detect port scans on your machine and automatically firewall potential intruders. If you want to let Nagios know about port scans, you could do the following...

### 38.4.1 Nagios Configuration

- Create a service definition called Port Scans and associate it with the host that PortSentry is running on.
- Set the `max_check_attempts` directive in the service definition to 1. This will tell Nagios to immediately force the service into a **hard state** when a non-OK state is reported.
- Set the `active_checks_enabled` directive in the service definition to 0. This prevents Nagios from actively checking the service.
- Set the `passive_checks_enabled` directive in the service definition to 1. This enables passive checks for the service.
- Set this `is_volatile` directive in the service definition to 1.

### 38.4.2 PortSentry Configuration

Edit your PortSentry configuration file (`portsentry.conf`) and define a command for the `KILL_RUN_CMD` directive as follows:

```
KILL_RUN_CMD="/usr/local/Nagios/libexec/eventhandlers/submit_check_result host_name 'Port ↵
Scans' 2 'Port scan from host $TARGET$ on port $PORT$. ~Host has been firewalled.'"
```

Make sure to replace `host_name` with the short name of the host that the service is associated with.

### 38.4.3 Port Scan Script

Create a shell script in the `/usr/local/nagios/libexec/eventhandlers` directory named **submit\_check\_result**. The contents of the shell script should be something similar to the following...

```
#!/bin/sh

Write a command to the Nagios command file to cause
it to process a service check result

echocmd="/bin/echo"

CommandFile="/usr/local/nagios/var/rw/nagios.cmd"

get the current date/time in seconds since UNIX epoch
datetime='date +%s'

create the command line to add to the command file
cmdline="[$datetime] PROCESS_SERVICE_CHECK_RESULT;$1;$2;$3;$4"

append the command to the end of the command file
'$echocmd $cmdline >> $CommandFile'
```

What will happen when PortSentry detects a port scan on the machine in the future?

- PortSentry will firewall the host (this is a function of the PortSentry software)

- PortSentry will execute the **submit\_check\_result** shell script and send a passive check result to Nagios
- Nagios will read the external command file and see the passive service check submitted by PortSentry
- Nagios will put the Port Scans service in a hard CRITICAL state and send notifications to contacts

Pretty neat, huh?

---

## Chapter 39

# Service and Host Freshness Checks

### 39.1 Introduction

Nagios supports a feature that does ‘freshness’ checking on the results of host and service checks. The purpose of freshness checking is to ensure that host and service checks are being provided passively by external applications on a regular basis.

Freshness checking is useful when you want to ensure that **passive checks** are being received as frequently as you want. This can be very useful in **distributed** and **failover** monitoring environments.

### 39.2 How Does Freshness Checking Work?



Nagios periodically checks the freshness of the results for all hosts services that have freshness checking enabled.

- A freshness threshold is calculated for each host or service.
- For each host/service, the age of its last check result is compared with the freshness threshold.
- If the age of the last check result is greater than the freshness threshold, the check result is considered ‘stale’.
- If the check results is found to be stale, Nagios will force an **active check** of the host or service by executing the command specified by in the host or service definition.

---

**Tip**

An active check is executed even if active checks are disabled on a program-wide or host- or service-specific basis.

---

For example, if you have a freshness threshold of 60 for one of your services, Nagios will consider that service to be stale if its last check result is older than 60 seconds.

---

## 39.3 Enabling Freshness Checking

Here's what you need to do to enable freshness checking...

- Enable freshness checking on a program-wide basis with the `check_service_freshness` and `check_host_freshness` directives.
- Use `service_freshness_check_interval` and `host_freshness_check_interval` options to tell Nagios how often it should check the freshness of service and host results.
- Enable freshness checking on a host- and service-specific basis by setting the `check_freshness` option in your host and service definitions to a value of 1.
- Configure freshness thresholds by setting the `freshness_threshold` option in your host and service definitions.
- Configure the `check_command` option in your host or service definitions to reflect a valid command that should be used to actively check the host or service when it is detected as stale.
- The `check_period` option in your host and service definitions is used when Nagios determines when a host or service can be checked for freshness, so make sure it is set to a valid timeperiod.

### Tip

If you do not specify a host- or service-specific `freshness_threshold` value (or you set it to zero), Nagios will automatically calculate a threshold automatically, based on how often you monitor that particular host or service. I would recommend that you explicitly specify a freshness threshold, rather than let Nagios pick one for you.

## 39.4 Example

An example of a service that might require freshness checking might be one that reports the status of your nightly backup jobs. Perhaps you have an external script that submit the results of the backup job to Nagios once the backup is completed. In this case, all of the checks/results for the service are provided by an external application using passive checks. In order to ensure that the status of the backup job gets reported every day, you may want to enable freshness checking for the service. If the external script doesn't submit the results of the backup job, you can have Nagios fake a critical result by doing something like this...

Here's what the definition for the service might look like (some required options are omitted)...

```
define service{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ backup-server
 ~ ~ ~ ~ service_description ~ ~ ArcServe Backup Job
 ~ ~ ~ ~ active_checks_enabled ~ 0 ~ ~ ~ ~ ~ ~ ~ ; active checks are NOT enabled
 ~ ~ ~ ~ passive_checks_enabled ~1 ~ ~ ~ ~ ~ ~ ~ ; passive checks are enabled (this is ←
 how results are reported)
 ~ ~ ~ ~ check_freshness ~ ~ ~ ~ 1
 ~ ~ ~ ~ freshness_threshold ~ ~ 93600 ~ ~ ~ ~ ~ ~ ~ ; 26 hour threshold, since backups may ←
 not always finish at the same time
 ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ no-backup-report ~ ~ ~ ~ ; this command is run only if ←
 the service results are stale
 ~ ~ ~ ~ ...other options...
 ~ ~ ~ ~ }
```

Notice that active checks are disabled for the service. This is because the results for the service are only made by an external application using passive checks. Freshness checking is enabled and the freshness threshold has been set to 26 hours. This is a bit longer than 24 hours because backup jobs sometimes run late from day to day (depending on how much data there is to backup, how much network traffic is present, etc.). The `no-backup-report` command is executed only if the results of the service are determined to be stale. The definition of the `no-backup-report` command might look like this...



```
define command{
 ~ ~ ~ ~ command_name ~ ~no-backup-report
 ~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/check_dummy 2 "CRITICAL: Results of ↵
 backup job were not reported!"
 ~ ~ ~ ~ }
```

If Nagios detects that the service results are stale, it will run the `no-backup-report` command as an active service check. This causes the **check\_dummy** plugin to be executed, which returns a critical state to Nagios. The service will then go into to a critical state (if it isn't already there) and someone will probably get notified of the problem.

## Chapter 40

# Distributed Monitoring

### 40.1 Introduction

Nagios can be configured to support distributed monitoring of network services and resources. I'll try to briefly explain how this can be accomplished...

### 40.2 Goals

The goal in the distributed monitoring environment that I will describe is to offload the overhead (CPU usage, etc.) of performing service checks from a "central" server onto one or more "distributed" servers. Most small to medium sized shops will not have a real need for setting up such an environment. However, when you want to start monitoring hundreds or even thousands of hosts (and several times that many services) using Nagios, this becomes quite important.

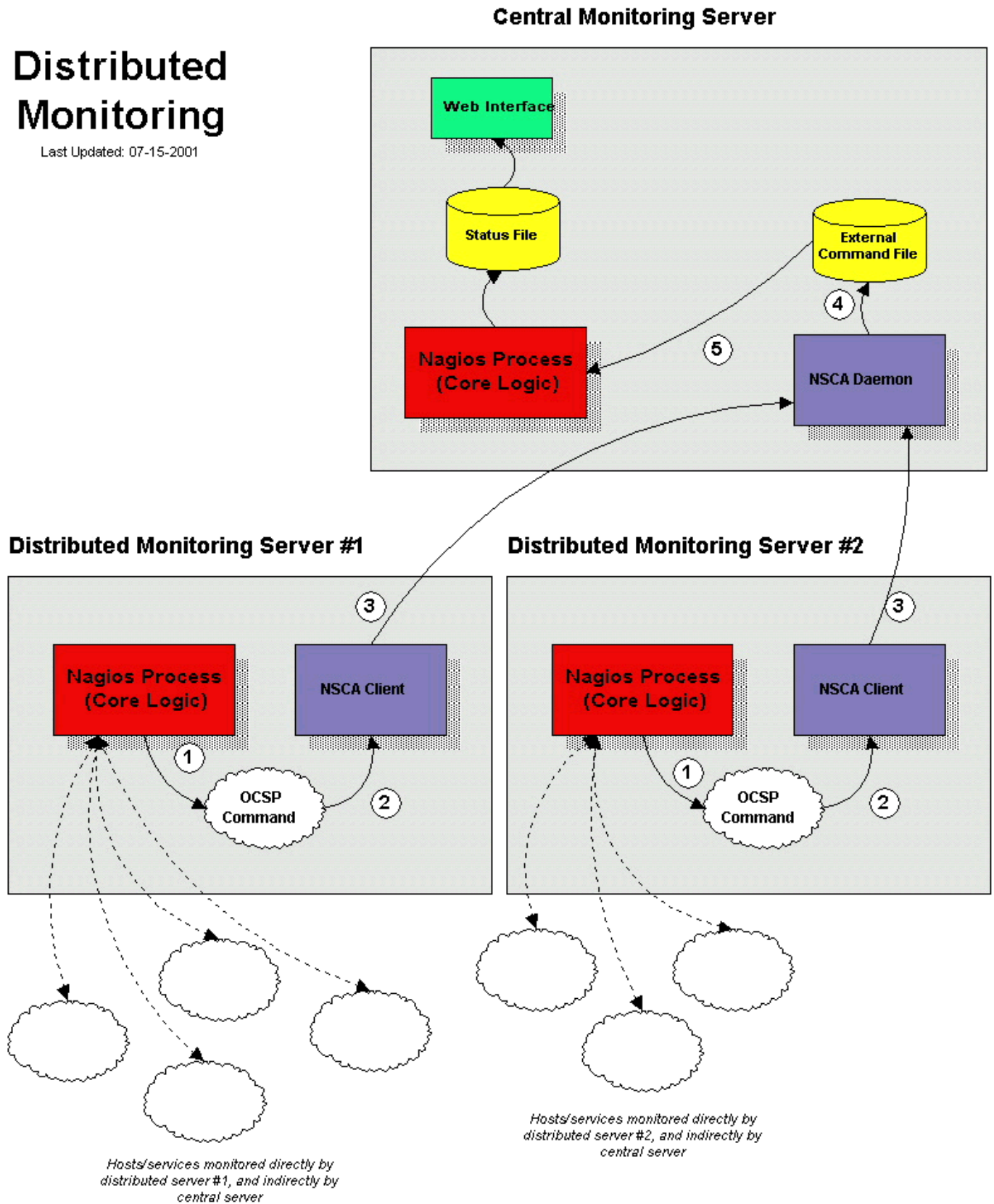
### 40.3 Reference Diagram

The diagram below should help give you a general idea of how distributed monitoring works with Nagios. I'll be referring to the items shown in the diagram as I explain things...

---

# Distributed Monitoring

Last Updated: 07-15-2001



## 40.4 Central Server vs. Distributed Servers

When setting up a distributed monitoring environment with Nagios, there are differences in the way the central and distributed servers are configured. I'll show you how to configure both types of servers and explain what effects the changes being made have on the overall monitoring. For starters, let's describe the purpose of the different types of servers...

The function of a distributed server is to actively perform checks all the services you define for a "cluster" of hosts. I use the term "cluster" loosely - it basically just means an arbitrary group of hosts on your network. Depending on your network layout, you may have several clusters at one physical location, or each cluster may be separated by a WAN, its own firewall, etc. The important thing to remember is that for each cluster of hosts (however you define that), there is one distributed server that runs Nagios and monitors the services on the hosts in the cluster. A distributed server is usually a bare-bones installation of Nagios. It doesn't have to have the web interface installed, send out notifications, run event handler scripts, or do anything other than execute service checks if you don't want it to. More detailed information on configuring a distributed server comes later...

The purpose of the central server is to simply listen for service check results from one or more distributed servers. Even though services are occasionally actively checked from the central server, the active checks are only performed in dire circumstances, so let's just say that the central server only accepts passive check for now. Since the central server is obtaining **passive service check** results from one or more distributed servers, it serves as the focal point for all monitoring logic (i.e. it sends out notifications, runs event handler scripts, determines host states, has the web interface installed, etc).

## 40.5 Obtaining Service Check Information From Distributed Monitors

Okay, before we go jumping into configuration detail we need to know how to send the service check results from the distributed servers to the central server. I've already discussed how to submit passive check results to Nagios from same host that Nagios is running on (as described in the documentation on **passive checks**), but I haven't given any info on how to submit passive check results from other hosts.

In order to facilitate the submission of passive check results to a remote host, I've written the **nsca addon**. The addon consists of two pieces. The first is a client program (`send_nsca`) which is run from a remote host and is used to send the service check results to another server. The second piece is the `nsca` daemon (`nsca`) which either runs as a standalone daemon or under `inetd` and listens for connections from client programs. Upon receiving service check information from a client, the daemon will submit the check information to Nagios (on the central server) by inserting a `PROCESS_SVC_CHECK_RESULT` command into the **external command file**, along with the check results. The next time Nagios checks for **external commands**, it will find the passive service check information that was sent from the distributed server and process it. Easy, huh?

## 40.6 Distributed Server Configuration

So how exactly is Nagios configured on a distributed server? Basically, it's just a bare-bones installation. You don't need to install the web interface or have notifications sent out from the server, as this will all be handled by the central server.

Key configuration changes:

- Only those services and hosts which are being monitored directly by the distributed server are defined in the **object configuration file**.
- The distributed server has its **enable\_notifications** directive set to 0. This will prevent any notifications from being sent out by the server.
- The distributed server is configured to **obsess over services**.
- The distributed server has an **ocsp\_command** defined (as described below).

In order to make everything come together and work properly, we want the distributed server to report the results of all service checks to Nagios. We could use **event handlers** to report changes in the state of a service, but that just doesn't cut it. In order to force the distributed server to report all service check results, you must enable the **obsess\_over\_services** option in the main configuration file and provide a **ocsp\_command** to be run after every service check. We will use the `ocsp` command to send the

In order to accomplish this, you'll need to define an `ocsp` command like this:

```
ocsp_command=submit_check_result
```

```
define command{
~ ~ ~ ~ command_name ~ ~submit_check_result
~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/eventhandlers/submit_check_result ↔
~ ~ ~ ~ ~ $HOSTNAME$ '$SERVICEDESC$' $SERVICESTATE$ '$SERVICEOUTPUT$'
~ ~ ~ ~ ~ }
}
```

```
~ ~ ~ ~ #!/bin/sh

~ ~ ~ ~ # Arguments:
~ ~ ~ ~ # ~$1 = host_name (Short name of host that the service is
~ ~ ~ ~ # ~ ~ ~ associated with)
~ ~ ~ ~ # ~$2 = svc_description (Description of the service)
~ ~ ~ ~ # ~$3 = state_string (A string representing the status of
~ ~ ~ ~ # ~ ~ ~ the given service - "OK", "WARNING", "CRITICAL"
~ ~ ~ ~ # ~ ~ ~ or "UNKNOWN")
~ ~ ~ ~ # ~$4 = plugin_output (A text string that should be used
~ ~ ~ ~ # ~ ~ ~ as the plugin output for the service checks)
~ ~ ~ ~ #

~ ~ ~ ~ # Convert the state string to the corresponding return code
~ ~ ~ ~ return_code=-1

~ ~ ~ ~ case "$3" in
~ ~ ~ ~ ~ OK)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ return_code=0
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ ~ WARNING)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ return_code=1
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ ~ CRITICAL)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ return_code=2
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ ~ UNKNOWN)
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ return_code=-1
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ esac

~ ~ ~ ~ # pipe the service check info into the send_nscd program, which
~ ~ ~ ~ # in turn transmits the data to the nsca daemon on the central
~ ~ ~ ~ # monitoring server

~ ~ ~ ~ /bin/printf "%s\t%s\t%s\t%s\n" "$1" "$2" "$return_code" "$4" | /usr/local/ ↵
nagios/bin/send_nscd -H central_server -c /usr/local/nagios/etc/send_nscd.cfg
```

That's it! We've successfully configured a remote host running Nagios to act as a distributed monitoring server. Let's go over exactly what happens with the distributed server and how it sends service check results to Nagios (the steps outlined below correspond to the numbers in the reference diagram above):

1. After the distributed server finishes executing a service check, it executes the command you defined by the `ocsp_command` variable. In our example, this is the `/usr/local/nagios/libexec/eventhandlers/submit_check_result` script. Note that the definition for the `submit_check_result` command passed four pieces of information to the script: the name of the host the service is associated with, the service description, the return code from the service check, and the plugin output from the service check.
2. The `submit_check_result` script pipes the service check information (host name, description, return code, and output) to the `send_nsca` program.
3. The `send_nsca` program transmits the service check information to the `nsca` daemon on the central monitoring server.
4. The `nsca` daemon on the central server takes the service check information and writes it to the external command file for later pickup by Nagios.
5. The Nagios process on the central server reads the external command file and processes the passive service check information that originated from the distributed monitoring server.

## 40.7 Central Server Configuration

We've looked at how distributed monitoring servers should be configured, so let's turn to the central server. For all intensive purposes, the central is configured as you would normally configure a standalone server. It is setup as follows:

- The central server has the web interface installed (optional, but recommended)
- The central server has its `enable_notifications` directive set to 1. This will enable notifications. (optional, but recommended)
- The central server has `active service checks` disabled (optional, but recommended - see notes below)
- The central server has `external command checks` enabled (required)
- The central server has `passive service checks` enabled (required)

There are three other very important things that you need to keep in mind when configuring the central server:

- The central server must have service definitions for all services that are being monitored by all the distributed servers. Nagios will ignore passive check results if they do not correspond to a service that has been defined.
- If you're only using the central server to process services whose results are going to be provided by distributed hosts, you can simply disable all active service checks on a program-wide basis by setting the `execute_service_checks` directive to 0. If you're using the central server to actively monitor a few services on its own (without the aid of distributed servers), the `enable_active_checks` option of the definitions for service being monitored by distributed servers should be set to 0. This will prevent Nagios from actively checking those services.

It is important that you either disable all service checks on a program-wide basis or disable the `enable_active_checks` option in the definitions for each service that is monitored by a distributed server. This will ensure that active service checks are never executed under normal circumstances. The services will keep getting rescheduled at their normal check intervals (3 minutes, 5 minutes, etc...), but they won't actually be executed. This rescheduling loop will just continue all the while Nagios is running. I'll explain why this is done in a bit...

That's it! Easy, huh?

## 40.8 Problems With Passive Checks

For all intensive purposes we can say that the central server is relying solely on passive checks for monitoring. The main problem with relying completely on passive checks for monitoring is the fact that Nagios must rely on something else to provide the monitoring data. What if the remote host that is sending in passive check results goes down or becomes unreachable? If Nagios isn't actively checking the services on the host, how will it know that there is a problem?

Fortunately, there is a way we can handle these types of problems...

## 40.9 Freshness Checking

Nagios supports a feature that does ‘freshness’ checking on the results of service checks. More information freshness checking can be found [here](#). This feature gives some protection against situations where remote hosts may stop sending passive service checks into the central monitoring server. The purpose of ‘freshness’ checking is to ensure that service checks are either being provided passively by distributed servers on a regular basis or performed actively by the central server if the need arises. If the service check results provided by the distributed servers get ‘stale’, Nagios can be configured to force active checks of the service from the central monitoring host.

So how do you do this? On the central monitoring server you need to configure services that are being monitored by distributed servers as follows...

- The `check_freshness` option in the service definitions should be set to 1. This enables ‘freshness’ checking for the services.
- The `freshness_threshold` option in the service definitions should be set to a value (in seconds) which reflects how “fresh” the results for the services (provided by the distributed servers) should be.
- The `check_command` option in the service definitions should reflect valid commands that can be used to actively check the service from the central monitoring server.

Nagios periodically checks the ‘freshness’ of the results for all services that have freshness checking enabled. The `freshness_threshold` option in each service definition is used to determine how “fresh” the results for each service should be. For example, if you set this value to 300 for one of your services, Nagios will consider the service results to be ‘stale’ if they’re older than 5 minutes (300 seconds). If you do not specify a value for the `freshness_threshold` option, Nagios will automatically calculate a ‘freshness’ threshold by looking at either the `normal_check_interval` or `retry_check_interval` options (depending on what **type of state** the service is in). If the service results are found to be ‘stale’, Nagios will run the service check command specified by the `check_command` option in the service definition, thereby actively checking the service.

Remember that you have to specify a `check_command` option in the service definitions that can be used to actively check the status of the service from the central monitoring server. Under normal circumstances, this check command is never executed (because active checks were disabled on a program-wide basis or for the specific services). When freshness checking is enabled, Nagios will run this command to actively check the status of the service even if active checks are disabled on a program-wide or service-specific basis.

If you are unable to define commands to actively check a service from the central monitoring host (or if it turns out to be a major pain), you could simply define all your services with the `check_command` option set to run a dummy script that returns a critical status. Here’s an example... Let’s assume you define a command called `service-is-stale` and use that command name in the `check_command` option of your services. Here’s what the definition would look like...

```
define command{
 command_name ~ ~service-is-stale
 command_line ~ ~/usr/local/nagios/libexec/check_dummy 2 "CRITICAL: Service results
 are stale"
}
```

When Nagios detects that the service results are stale and runs the **service-is-stale** command, the **check\_dummy** plugin is executed and the service will go into a critical state. This would likely cause notifications to be sent out, so you’ll know that there’s a problem.

## 40.10 Performing Host Checks

At this point you know how to obtain service check results passively from distributed servers. This means that the central server is not actively checking services on its own. But what about host checks? You still need to do them, so how?

Since host checks usually comprise a small part of monitoring activity (they aren’t done unless absolutely necessary), I’d recommend that you perform host checks actively from the central server. That means that you define host checks on the central server the same way that you do on the distributed servers (and the same way you would in a normal, non-distributed setup).

Passive host checks are available (read [here](#)), so you could use them in your distributed monitoring setup, but they suffer from a few problems. The biggest problem is that Nagios does not translate passive host check problem states (DOWN and UNREACHABLE) when they are processed. This means that if your monitoring servers have a different parent/child host structure (and they will, if you monitoring servers are in different locations), the central monitoring server will have an inaccurate view of host states.

If you do want to send passive host checks to a central server in your distributed monitoring setup, make sure:

- The central server has **passive host checks** enabled (required)
- The distributed server is configured to **obsess over hosts**.
- The distributed server has an **ochp command** defined.

The ochp command, which is used for processing host check results, works in a similar manner to the ocsp command, which is used for processing service check results (see documentation above). In order to make sure passive host check results are up to date, you'll want to enable **freshness checking** for hosts (similar to what is described above for services).

---



## Chapter 41

# Redundant and Failover Network Monitoring

### 41.1 Introduction

This section describes a few scenarios for implementing redundant monitoring hosts on various types of network layouts. With redundant hosts, you can maintain the ability to monitor your network when the primary host that runs Nagios fails or when portions of your network become unreachable.

---

**Note**

If you are just learning how to use Nagios, I would suggest not trying to implement redundancy until you have becoming familiar with the [prerequisites](#) I've laid out. Redundancy is a relatively complicated issue to understand, and even more difficult to implement properly.

---

### 41.2 Prerequisites

Before you can even think about implementing redundancy with Nagios, you need to be familiar with the following...

- Implementing [event handlers](#) for hosts and services
- Issuing [external commands](#) to Nagios via shell scripts
- Executing plugins on remote hosts using either the [NRPE addon](#) or some other method
- Checking the status of the Nagios process with the [check\\_nagios](#) plugin

### 41.3 Sample Scripts

All of the sample scripts that I use in this documentation can be found in the `eventhandlers/` subdirectory of the Nagios distribution. You'll probably need to modify them to work on your system...

### 41.4 Scenario 1 - Redundant Monitoring

#### 41.4.1 Introduction

This is an easy (and naive) method of implementing redundant monitoring hosts on your network and it will only protect against a limited number of failures. More complex setups are necessary in order to provide smarter redundancy, better redundancy across different network segments, etc.

---

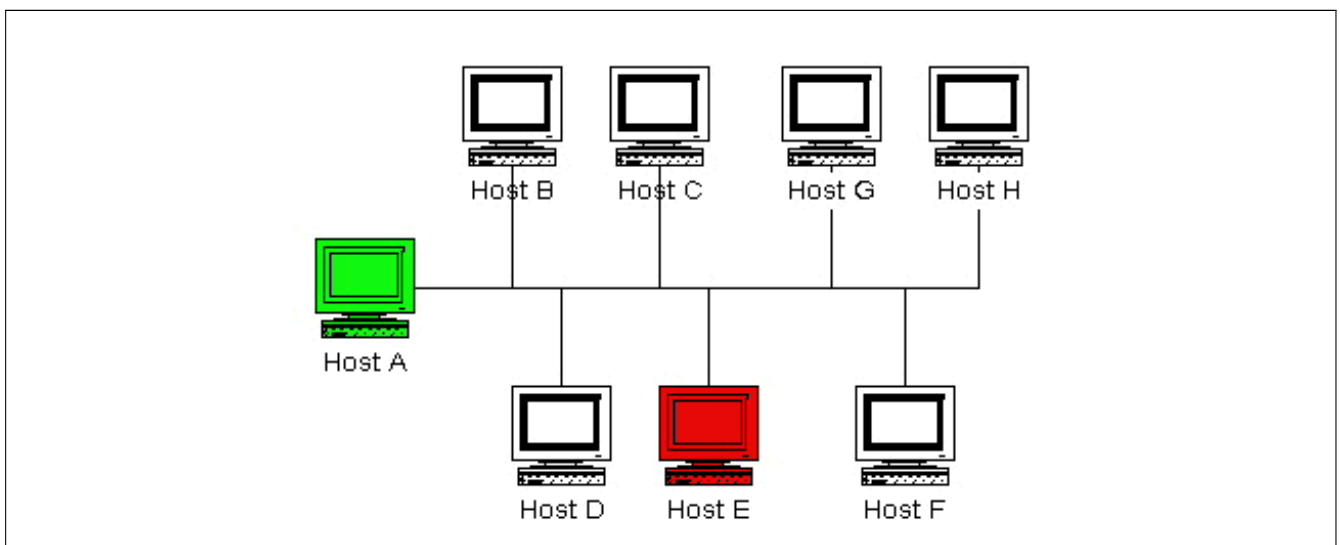
### 41.4.2 Goals

The goal of this type of redundancy implementation is simple. Both the "master" and "slave" hosts monitor the same hosts and service on the network. Under normal circumstances only the "master" host will be sending out notifications to contacts about problems. We want the "slave" host running Nagios to take over the job of notifying contacts about problems if:

1. The "master" host that runs Nagios is down or.
2. The Nagios process on the "master" host stops running for some reason

### 41.4.3 Network Layout Diagram

The diagram below shows a very simple network setup. For this scenario I will be assuming that hosts A and E are both running Nagios and are monitoring all the hosts shown. Host A will be considered the "master" host and host E will be considered the "slave" host.



### 41.4.4 Initial Program Settings

The slave host (host E) has its initial `enable_notifications` directive disabled, thereby preventing it from sending out any host or service notifications. You also want to make sure that the slave host has its `check_external_commands` directive enabled. That was easy enough...

### 41.4.5 Initial Configuration

Next we need to consider the differences between the `object configuration file(s)` on the master and slave hosts...

I will assume that you have the master host (host A) setup to monitor services on all hosts shown in the diagram above. The slave host (host E) should be setup to monitor the same services and hosts, with the following additions in the configuration file...

- The host definition for host A (in the host E configuration file) should have a host `event handler` defined. Lets say the name of the host event handler is `handle-master-host-event`.
- The configuration file on host E should have a service defined to check the status of the Nagios process on host A. Lets assume that you define this service check to run the `check_nagios` plugin on host A. This can be done by using one of the methods described in [this FAQ](#) (update this!).
- The service definition for the Nagios process check on host A should have an `event handler` defined. Lets say the name of the service event handler is `handle-master-proc-event`.

It is important to note that host A (the master host) has no knowledge of host E (the slave host). In this scenario it simply doesn't need to. Of course you may be monitoring services on host E from host A, but that has nothing to do with the implementation of redundancy...

#### 41.4.6 Event Handler Command Definitions

We need to stop for a minute and describe what the command definitions for the event handlers on the slave host look like. Here is an example...

```
define command{
 command_name handle-master-host-event
 command_line /usr/local/nagios/libexec/eventhandlers/handle-master-host-event
 $HOSTSTATE$ $HOSTSTATETYPE$
}
```

```
define command{
 command_name handle-master-proc-event
 command_line /usr/local/nagios/libexec/eventhandlers/handle-master-proc-event
 $SERVICESTATE$ $SERVICESTATETYPE$
}
```

This assumes that you have placed the event handler scripts in the `/usr/local/nagios/libexec/eventhandlers` directory. You may place them anywhere you wish, but you'll need to modify the examples I've given here.

#### 41.4.7 Event Handler Scripts

Okay, now lets take a look at what the event handler scripts look like...

Host Event Handler (handle-master-host-event):

```
#!/bin/sh
Only take action on hard host states...
case "$2" in
 HARD)
 ~ ~ ~ ~ case "$1" in
 ~ ~ ~ ~ DOWN)
 ~ ~ ~ ~ ~ ~ ~ ~ # The master host has gone down!
 ~ ~ ~ ~ ~ ~ ~ ~ # We should now become the master host and take
 ~ ~ ~ ~ ~ ~ ~ ~ # over the responsibilities of monitoring the
 ~ ~ ~ ~ ~ ~ ~ ~ # network, so enable notifications...
 /usr/local/nagios/libexec/eventhandlers/enable_notifications
 ~ ~ ~ ~ ~ ~ ~ ~ ;;
 ~ ~ ~ ~ UP)
 ~ ~ ~ ~ ~ ~ ~ ~ # The master host has recovered!
 ~ ~ ~ ~ ~ ~ ~ ~ # We should go back to being the slave host and
 ~ ~ ~ ~ ~ ~ ~ ~ # let the master host do the monitoring, so
 ~ ~ ~ ~ ~ ~ ~ ~ # disable notifications...
 /usr/local/nagios/libexec/eventhandlers/disable_notifications
 ~ ~ ~ ~ ~ ~ ~ ~ ;;
 ~ ~ ~ ~ esac
 ~ ~ ~ ~ ;;
 esac
exit 0
```

Service Event Handler (handle-master-proc-event):

```
#!/bin/sh
Only take action on hard service states...
case "$2" in
```

```

HARD)
~ ~ ~ ~ case "$1" in
~ ~ ~ ~ CRITICAL)
~ ~ ~ ~ ~ ~ ~ ~ # The master Nagios process is not running!
~ ~ ~ ~ ~ ~ ~ ~ # We should now become the master host and
~ ~ ~ ~ ~ ~ ~ ~ # take over the responsibility of monitoring
~ ~ ~ ~ ~ ~ ~ ~ # the network, so enable notifications...
/usr/local/nagios/libexec/eventhandlers/enable_notifications
~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ WARNING)
~ ~ ~ ~ UNKNOWN)
~ ~ ~ ~ ~ ~ ~ ~ # The master Nagios process may or may not
~ ~ ~ ~ ~ ~ ~ ~ # be running.. We won't do anything here, but
~ ~ ~ ~ ~ ~ ~ ~ # to be on the safe side you may decide you
~ ~ ~ ~ ~ ~ ~ ~ # want the slave host to become the master in
~ ~ ~ ~ ~ ~ ~ ~ # these situations...
~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ OK)
~ ~ ~ ~ ~ ~ ~ ~ # The master Nagios process running again!
~ ~ ~ ~ ~ ~ ~ ~ # We should go back to being the slave host,
~ ~ ~ ~ ~ ~ ~ ~ # so disable notifications...
/usr/local/nagios/libexec/eventhandlers/disable_notifications
~ ~ ~ ~ ~ ~ ~ ~ ;;
~ ~ ~ ~ esac
~ ~ ~ ~ ;;
esac
exit 0

```

#### 41.4.8 What This Does For Us

The slave host (host E) initially has notifications disabled, so it won't send out any host or service notifications while the Nagios process on the master host (host A) is still running.

The Nagios process on the slave host (host E) becomes the master host when...

- The master host (host A) goes down and the handle-master-host-event host event handler is executed.
- The Nagios process on the master host (host A) stops running and the handle-master-proc-event service event handler is executed.

When the Nagios process on the slave host (host E) has notifications enabled, it will be able to send out notifications about any service or host problems or recoveries. At this point host E has effectively taken over the responsibility of notifying contacts of host and service problems!

The Nagios process on host E returns to being the slave host when...

- Host A recovers and the handle-master-host-event host event handler is executed.
- The Nagios process on host A recovers and the handle-master-proc-event service event handler is executed.

When the Nagios process on host E has notifications disabled, it will not send out notifications about any service or host problems or recoveries. At this point host E has handed over the responsibilities of notifying contacts of problems to the Nagios process on host A. Everything is now as it was when we first started!

#### 41.4.9 Time Lags

Redundancy in Nagios is by no means perfect. One of the more obvious problems is the lag time between the master host failing and the slave host taking over. This is affected by the following...

- The time between a failure of the master host and the first time the slave host detects a problem
- The time needed to verify that the master host really does have a problem (using service or host check retries on the slave host)
- The time between the execution of the event handler and the next time that Nagios checks for external commands

You can minimize this lag by...

- Ensuring that the Nagios process on host E (re)checks one or more services at a high frequency. This is done by using the `check_interval` and `retry_interval` arguments in each service definition.
- Ensuring that the number of host rechecks for host A (on host E) allow for fast detection of host problems. This is done by using the `max_check_attempts` argument in the host definition.
- Increase the frequency of **external command** checks on host E. This is done by modifying the `command_check_interval` option in the main configuration file.

When Nagios recovers on the host A, there is also some lag time before host E returns to being a slave host. This is affected by the following...

- The time between a recovery of host A and the time the Nagios process on host E detects the recovery
- The time between the execution of the event handler on host B and the next time the Nagios process on host E checks for external commands

The exact lag times between the transfer of monitoring responsibilities will vary depending on how many services you have defined, the interval at which services are checked, and a lot of pure chance. At any rate, its definitely better than nothing.

#### 41.4.10 Special Cases

Here is one thing you should be aware of... If host A goes down, host E will have notifications enabled and take over the responsibilities of notifying contacts of problems. When host A recovers, host E will have notifications disabled. If - when host A recovers - the Nagios process on host A does not start up properly, there will be a period of time when neither host is notifying contacts of problems! Fortunately, the service check logic in Nagios accounts for this. The next time the Nagios process on host E checks the status of the Nagios process on host A, it will find that it is not running. Host E will then have notifications enabled again and take over all responsibilities of notifying contacts of problems.

The exact amount of time that neither host is monitoring the network is hard to determine. Obviously, this period can be minimized by increasing the frequency of service checks (on host E) of the Nagios process on host A. The rest is up to pure chance, but the total "blackout" time shouldn't be too bad.

### 41.5 Scenario 2 - Failover Monitoring

#### 41.5.1 Introduction

Failover monitoring is similiar to, but slightly different than redundant monitoring (as discussed above in **scenario 1**).

#### 41.5.2 Goals

The basic goal of failover monitoring is to have the Nagios process on the slave host sit idle while the Nagios process on the master host is running. If the process on the master host stops running (or if the host goes down), the Nagios process on the slave host starts monitoring everything.

While the method described in **scenario 1** will allow you to continue receive notifications if the master monitoring hosts goes down, it does have some pitfalls. The biggest problem is that the slave host is monitoring the same hosts and servers as the master at the same time as the master! This can cause problems with excessive traffic and load on the machines being monitored if you have a lot of services defined. Here's how you can get around that problem...

---

### 41.5.3 Initial Program Settings

Disable active service checks and notifications on the slave host using the `execute_service_checks` and `enable_notifications` directives. This will prevent the slave host from monitoring hosts and services and sending out notifications while the Nagios process on the master host is still up and running. Make sure you also have the `check_external_commands` directive enabled on the slave host.

### 41.5.4 Master Process Check

Set up a cron job on the slave host that periodically (say every minute) runs a script that checks the status of the Nagios process on the master host (using the `check_nrpe` plugin on the slave host and the `nrpe daemon` and `check_nagios` plugin on the master host). The script should check the return code of the `check_nrpe` plugin. If it returns a non-OK state, the script should send the appropriate commands to the `external command file` to enable both notifications and active service checks. If the plugin returns an OK state, the script should send commands to the external command file to disable both notifications and active checks.

By doing this you end up with only one process monitoring hosts and services at a time, which is much more efficient than monitoring everything twice.

Also of note, you don't need to define host and service handlers as mentioned in [scenario 1](#) because things are handled differently.

### 41.5.5 Additional Issues

At this point, you have implemented a very basic failover monitoring setup. However, there is one more thing you should consider doing to make things work smoother.

The big problem with the way things have been setup thus far is the fact that the slave host doesn't have the current status of any services or hosts at the time it takes over the job of monitoring. One way to solve this problem is to enable the `ocsp command` on the master host and have it send all service check results to the slave host using the `nsca addon`. The slave host will then have up-to-date status information for all services at the time it takes over the job of monitoring things. Since active service checks are not enabled on the slave host, it will not actively run any service checks. However, it will execute host checks if necessary. This means that both the master and slave hosts will be executing host checks as needed, which is not really a big deal since the majority of monitoring deals with service checks.

That's pretty much it as far as setup goes.

---

## Chapter 42

# Detection and Handling of State Flapping

### 42.1 Introduction

Nagios supports optional detection of hosts and services that are ‘flapping’. Flapping occurs when a service or host changes state too frequently, resulting in a storm of problem and recovery notifications. Flapping can be indicative of configuration problems (i.e. thresholds set too low), troublesome services, or real network problems.

### 42.2 How Flap Detection Works

Before I get into this, let me say that flapping detection has been a little difficult to implement. How exactly does one determine what "too frequently" means in regards to state changes for a particular host or service? When I first started thinking about implementing flap detection I tried to find some information on how flapping could/should be detected. I couldn't find any information about what others were using (where they using any?), so I decided to settle with what seemed to me to be a reasonable solution...

Whenever Nagios checks the status of a host or service, it will check to see if it has started or stopped flapping. It does this by.

- Storing the results of the last 21 checks of the host or service
- Analyzing the historical check results and determine where state changes/transitions occur
- Using the state transitions to determine a percent state change value (a measure of change) for the host or service
- Comparing the percent state change value against low and high flapping thresholds

A host or service is determined to have started flapping when its percent state change first exceeds a high flapping threshold.

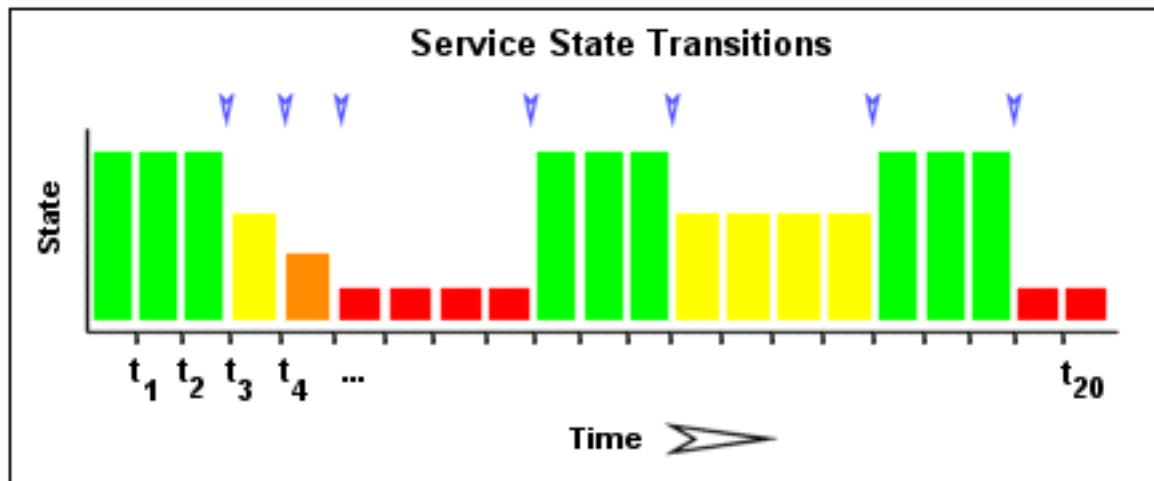
A host or service is determined to have stopped flapping when its percent state goes below a low flapping threshold (assuming that it was previously flapping).

### 42.3 Example

Let's describe in more detail how flap detection works with services...

The image below shows a chronological history of service states from the most recent 21 service checks. OK states are shown in green, WARNING states in yellow, CRITICAL states in red, and UNKNOWN states in orange.

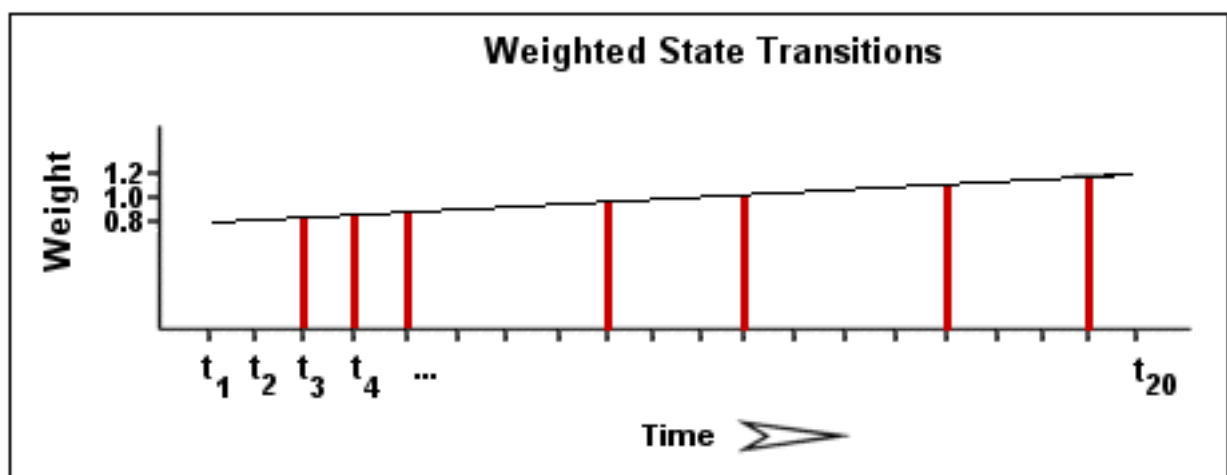
---



The historical service check results are examined to determine where state changes/transitions occur. State changes occur when an archived state is different from the archived state that immediately precedes it chronologically. Since we keep the results of the last 21 service checks in the array, there is a possibility of having at most 20 state changes. In this example there are 7 state changes, indicated by blue arrows in the image above.

The flap detection logic uses the state changes to determine an overall percent state change for the service. This is a measure of volatility/change for the service. Services that never change state will have a 0% state change value, while services that change state each time they're checked will have 100% state change. Most services will have a percent state change somewhere in between.

When calculating the percent state change for the service, the flap detection algorithm will give more weight to new state changes compare to older ones. Specifically, the flap detection routines are currently designed to make the newest possible state change carry 50% more weight than the oldest possible state change. The image below shows how recent state changes are given more weight than older state changes when calculating the overall or total percent state change for a particular service.



Using the images above, let's do a calculation of percent state change for the service. You will notice that there are a total of 7 state changes (at  $t_3, t_4, t_5, t_9, t_{12}, t_{16}$ , and  $t_{19}$ ). Without any weighting of the state changes over time, this would give us a total state change of 35%:

$$(7 \text{ observed state changes} / \text{possible } 20 \text{ state changes}) * 100 = 35 \%$$

Since the flap detection logic will give newer state changes a higher rate than older state changes, the actual calculated percent state change will be slightly less than 35% in this example. Let's say that the weighted percent of state change turned out to be 31%...

The calculated percent state change for the service (31%) will then be compared against flapping thresholds to see what should happen:



- If the service was not previously flapping and 31% is equal to or greater than the high flap threshold, Nagios considers the service to have just started flapping.
- If the service was previously flapping and 31% is less than the low flap threshold, Nagios considers the service to have just stopped flapping.

If neither of those two conditions are met, the flap detection logic won't do anything else with the service, since it is either not currently flapping or it is still flapping.

## 42.4 Flap Detection for Services

Nagios checks to see if a service is flapping whenever the service is checked (either actively or passively).

The flap detection logic for services works as described in the example above.

## 42.5 Flap Detection for Hosts

Host flap detection works in a similar manner to service flap detection, with one important difference: Nagios will attempt to check to see if a host is flapping whenever:

- The host is checked (actively or passively)
- Sometimes when a service associated with that host is checked. More specifically, when at least x amount of time has passed since the flap detection was last performed, where x is equal to the average check interval of all services associated with the host.

Why is this done? With services we know that the minimum amount of time between consecutive flap detection routines is going to be equal to the service check interval. However, you might not be monitoring hosts on a regular basis, so there might not be a host check interval that can be used in the flap detection logic. Also, it makes sense that checking a service should count towards the detection of host flapping. Services are attributes of or things associated with host after all... At any rate, that's the best method I could come up with for determining how often flap detection could be performed on a host, so there you have it.

## 42.6 Flap Detection Thresholds

Nagios uses several variables to determine the percent state change thresholds it uses for flap detection. For both hosts and services, there are global high and low thresholds and host- or service-specific thresholds that you can configure. Nagios will use the global thresholds for flap detection if you do not specify host- or service- specific thresholds.

The table below shows the global and host- or service-specific variables that control the various thresholds used in flap detection.

| Object Type | Global Variables                                                                    | Object-Specific Variables                                           |
|-------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Host        | <code>low_host_flap_threshold</code><br><code>high_host_flap_threshold</code>       | <code>low_flap_threshold</code><br><code>high_flap_threshold</code> |
| Service     | <code>low_service_flap_threshold</code><br><code>high_service_flap_threshold</code> | <code>low_flap_threshold</code><br><code>high_flap_threshold</code> |

## 42.7 States Used For Flap Detection

Normally Nagios will track the results of the last 21 checks of a host or service, regardless of the check result (host/service state), for use in the flap detection logic.

**Tip**

You can exclude certain host or service states from use in flap detection logic by using the `flap_detection_options` directive in your host or service definitions. This directive allows you to specify what host or service states (i.e. "UP", "DOWN", "OK", "CRITICAL") you want to use for flap detection. If you don't use this directive, all host or service states are used in flap detection.

---

## 42.8 Flap Handling

When a service or host is first detected as flapping, Nagios will:

1. Log a message indicating that the service or host is flapping.
2. Add a non-persistent comment to the host or service indicating that it is flapping.
3. Send a "flapping start" notification for the host or service to appropriate contacts.
4. Suppress other notifications for the service or host (this is one of the filters in the **notification logic**).

When a service or host stops flapping, Nagios will:

1. Log a message indicating that the service or host has stopped flapping.
2. Delete the comment that was originally added to the service or host when it started flapping.
3. Send a "flapping stop" notification for the host or service to appropriate contacts.
4. Remove the block on notifications for the service or host (notifications will still be bound to the normal **notification logic**).

## 42.9 Enabling Flap Detection

In order to enable the flap detection features in Nagios, you'll need to:

- Set **enable\_flap\_detection** directive is set to 1.
- Set the `flap_detection_enabled` directive in your host and service definitions is set to 1.

If you want to disable flap detection on a global basis, set the **enable\_flap\_detection** directive to 0.

If you would like to disable flap detection for just a few hosts or services, use the `flap_detection_enabled` directive in the host and/or service definitions to do so.

---

## Chapter 43

# Notification Escalations

### 43.1 Introduction



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 Overview**.

---

#### Note

The examples I provide below all make use of service escalation definitions, but host escalations work the same way. Except, of course, that they're for hosts instead of services. :-)

---

### 43.2 When Are Notifications Escalated?

Notifications are escalated if and only if one or more escalation definitions matches the current notification that is being sent out. If a host or service notification does not have any valid escalation definitions that applies to it, the contact group(s) specified in either the host group or service definition will be used for the notification. Look at the example below:

```
define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 90
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }
```

```
define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~6
```

```

~ ~ ~ ~ last_notification ~ ~ ~ 10
~ ~ ~ ~ notification_interval ~ 60
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers,everyone
~ ~ ~ ~ }

```

Notice that there are "holes" in the notification escalation definitions. In particular, notifications 1 and 2 are not handled by the escalations, nor are any notifications beyond 10. For the first and second notification, as well as all notifications beyond the tenth one, the default contact groups specified in the service definition are used. For all the examples I'll be using, I'll be assuming that the default contact groups for the service definition is called nt-admins.

### 43.3 Contact Groups

When defining notification escalations, it is important to keep in mind that any contact groups that were members of "lower" escalations (i.e. those with lower notification number ranges) should also be included in "higher" escalation definitions. This should be done to ensure that anyone who gets notified of a problem continues to get notified as the problem is escalated. Example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 90
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~6
~ ~ ~ ~ last_notification ~ ~ ~ 0
~ ~ ~ ~ notification_interval ~ 60
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers,everyone
~ ~ ~ ~ }

```

The first (or "lowest") escalation level includes both the nt-admins and managers contact groups. The last (or "highest") escalation level includes the nt-admins, managers, and everyone contact groups. Notice that the nt-admins contact group is included in both escalation definitions. This is done so that they continue to get paged if there are still problems after the first two service notifications are sent out. The managers contact group first appears in the "lower" escalation definition - they are first notified when the third problem notification gets sent out. We want the managers group to continue to be notified if the problem continues past five notifications, so they are also included in the "higher" escalation definition.

### 43.4 Overlapping Escalation Ranges

Notification escalation definitions can have notification ranges that overlap. Take the following example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 20
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~4
~ ~ ~ ~ last_notification ~ ~ ~ 0
~ ~ ~ ~ notification_interval ~ 30
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~on-call-support
~ ~ ~ ~ }

```

In the example above:

- The nt-admins and managers contact groups get notified on the third notification
- All three contact groups get notified on the fourth and fifth notifications
- Only the on-call-support contact group gets notified on the sixth (or higher) notification

## 43.5 Recovery Notifications

Recovery notifications are slightly different than problem notifications when it comes to escalations. Take the following example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 20
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~4
~ ~ ~ ~ last_notification ~ ~ ~ 0
~ ~ ~ ~ notification_interval ~ 30
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~on-call-support
~ ~ ~ ~ }

```

If, after three problem notifications, a recovery notification is sent out for the service, who gets notified? The recovery is actually the fourth notification that gets sent out. However, the escalation code is smart enough to realize that only those people who were notified about the problem on the third notification should be notified about the recovery. In this case, the nt-admins and managers contact groups would be notified of the recovery.

## 43.6 Notification Intervals

You can change the frequency at which escalated notifications are sent out for a particular host or service by using the `notification_interval` option of the hostgroup or service escalation definition. Example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 45
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~6
~ ~ ~ ~ last_notification ~ ~ ~ 0
~ ~ ~ ~ notification_interval ~ 60
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers,everyone
~ ~ ~ ~ }

```

In this example we see that the default notification interval for the services is 240 minutes (this is the value in the service definition). When the service notification is escalated on the 3rd, 4th, and 5th notifications, an interval of 45 minutes will be used between notifications. On the 6th and subsequent notifications, the notification interval will be 60 minutes, as specified in the second escalation definition.

Since it is possible to have overlapping escalation definitions for a particular hostgroup or service, and the fact that a host can be a member of multiple hostgroups, Nagios has to make a decision on what to do as far as the notification interval is concerned when escalation definitions overlap. In any case where there are multiple valid escalation definitions for a particular notification, Nagios will choose the smallest notification interval. Take the following example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 45
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~4
~ ~ ~ ~ last_notification ~ ~ ~ 0
~ ~ ~ ~ notification_interval ~ 60
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers,everyone
~ ~ ~ ~ }

```

We see that the two escalation definitions overlap on the 4th and 5th notifications. For these notifications, Nagios will use a notification interval of 45 minutes, since it is the smallest interval present in any valid escalation definitions for those notifications.

One last note about notification intervals deals with intervals of 0. An interval of 0 means that Nagios should only send a notification out for the first valid notification during that escalation definition. All subsequent notifications for the hostgroup or service will be suppressed. Take this example:

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 45
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```

define serviceescalation{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ webserver
~ ~ ~ ~ service_description ~ ~ HTTP
~ ~ ~ ~ first_notification ~ ~ ~3
~ ~ ~ ~ last_notification ~ ~ ~ 5
~ ~ ~ ~ notification_interval ~ 45
~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
~ ~ ~ ~ }

```

```
define serviceescalation{
 host_name ~ ~ ~ ~ ~ ~ ~ webserver
 ~ ~ ~ ~ service_description ~ ~ HTTP
 ~ ~ ~ ~ first_notification ~ ~ ~7
 ~ ~ ~ ~ last_notification ~ ~ ~ 0
 ~ ~ ~ ~ notification_interval ~ 30
 ~ ~ ~ ~ contact_groups ~ ~ ~ ~ ~nt-admins,managers
 ~ ~ ~ ~ }
```

In the example above, the maximum number of problem notifications that could be sent out about the service would be four. This is because the notification interval of 0 in the second escalation definition indicates that only one notification should be sent out (starting with and including the 4th notification) and all subsequent notifications should be repressed. Because of this, the third service escalation definition has no effect whatsoever, as there will never be more than four notifications.

## 43.7 Time Period Restrictions

Under normal circumstances, escalations can be used at any time that a notification could normally be sent out for the host or service. This "notification time window" is determined by the `notification_period` directive in the **host** or **service** definition.

You can optionally restrict escalations so that they are only used during specific time periods by using the `escalation_period` directive in the host or service escalation definition. If you use the `escalation_period` directive to specify a **Time Period Definition** during which the escalation can be used, the escalation will only be used during that time. If you do not specify any `escalation_period` directive, the escalation can be used at any time within the "notification time window" for the host or service.

---

### Note

Escalated notifications are still subject to the normal time restrictions imposed by the `notification_period` directive in a host or service definition, so the timeperiod you specify in an escalation definition should be a subset of that larger "notification time window".

---

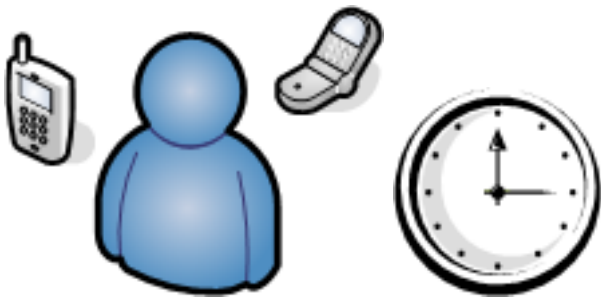
## 43.8 State Restrictions

If you would like to restrict the escalation definition so that it is only used when the host or service is in a particular state, you can use the `escalation_options` directive in the host or service escalation definition. If you do not use the `escalation_options` directive, the escalation can be used when the host or service is in any state.

## Chapter 44

# On-Call Rotations

### 44.1 Introduction



Admins often have to shoulder the burden of answering pagers, cell phone calls, etc. when they least desire them. No one likes to be woken up at 4 am to fix a problem. But its often better to fix the problem in the middle of the night, rather than face the wrath of an unhappy boss when you stroll in at 9 am the next morning.

For those lucky admins who have a team of gurus who can help share the responsibility of answering alerts, on-call rotations are often setup. Multiple admins will often alternate taking notifications on weekends, weeknights, holidays, etc.

I'll show you how you can create **timeperiod** definitions in a way that can facilitate most on-call notification rotations. These definitions won't handle human issues that will inevitably crop up (admins calling in sick, swapping shifts, or throwing their pagers into the river), but they will allow you to setup a basic structure that should work the majority of the time.

### 44.2 Scenario 1: Holidays and Weekends

Two admins - John and Bob - are responsible for responding to Nagios alerts. John receives all notifications for weekdays (and weeknights) - except for holidays - and Bob gets handles notifications during the weekends and holidays. Lucky Bob. Here's how you can define this type of rotation using timeperiods...

First, define a timeperiod that contains time ranges for holidays:

```
define timeperiod{
 ~ ~ ~ name ~ ~holidays
 ~ ~ ~ ~ timeperiod_name holidays
 ~ ~ ~ ~ january 1 ~ ~ ~ ~ ~ ~ 00:00-24:00 ~ ~ ; New Year's Day
 ~ ~ ~ ~ 2008-03-23 ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ; Easter (2008)
 ~ ~ ~ ~ 2009-04-12 ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ; Easter (2009)
 ~ ~ ~ ~ monday -1 may ~ ~ ~ ~ ~ 00:00-24:00 ~ ~ ; Memorial Day (Last Monday in May)
 ~ ~ ~ ~ july 4 ~ ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ; Independence Day
 ~ ~ ~ ~ monday 1 september ~ ~ ~00:00-24:00 ~ ~ ; Labor Day (1st Monday in September)
 ~ ~ ~ ~ thursday 4 november ~ ~ 00:00-24:00 ~ ~ ; Thanksgiving (4th Thursday in
 November)
```



```

~ ~ ~ ~ december 25 ~ ~ ~ ~ ~ 00:00-24:00 ~ ~ ; Christmas
~ ~ ~ ~ december 31 ~ ~ ~ ~ ~ 17:00-24:00 ~ ~ ; New Year's Eve (5pm onwards)
~ ~ ~ ~ }

```

Next, define a timeperiod for John's on-call times that include weekdays and weeknights, but excludes the dates/times defined in the holidays timeperiod above:

```

define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ john-oncall
 ~ ~ ~ ~ monday ~ ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ tuesday ~ ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ wednesday ~ ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ thursday ~ ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ friday ~ ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ exclude ~ ~ ~ ~ ~ holidays ~ ~ ~ ; Exclude holiday dates/times defined elsewhere
 ~ ~ ~ ~ }

```

You can now reference this timeperiod in John's contact definition:

```

define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~ john
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ }

```

Define a new timeperiod for Bob's on-call times that include weekends and the dates/times defined in the holidays timeperiod above:

```

define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ friday ~ ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ saturday ~ ~ ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ use ~ ~ ~ ~ ~ holidays ~ ~ ~ ~ ; Also include holiday date/times defined elsewhere
 ~ ~ ~ ~ }

```

You can now reference this timeperiod in Bob's contact definition:

```

define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~ bob
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ }

```

## 44.3 Scenario 2: Alternating Days

In this scenario John and Bob alternate handling alerts every other day - regardless of whether its a weekend, weekday, or holiday.

Define a timeperiod for when John should receive notifications. Assuming today's date is August 1st, 2007 and John is handling notifications starting today, the definition would look like this:

```

define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ 2007-08-01 / 2 ~00:00-24:00 ~ ~ ; Every two days, starting August 1st, 2007
 ~ ~ ~ ~ }

```

Now define a timeperiod for when Bob should receive notifications. Bob gets notifications on the days that John doesn't, so his first on-call day starts tomorrow (August 2nd, 2007).

```
define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ 2007-08-02 / 2 ~00:00-24:00 ~ ~ ; Every two days, starting August 2nd, 2007
 ~ ~ ~ ~ }
```

Now you need to reference these timeperiod definitions in the contact definitions for John and Bob:

```
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~john
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ ~ ~john-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ }
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~bob
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ ~ ~bob-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ }
```

## 44.4 Scenario 3: Alternating Weeks

In this scenario John and Bob alternate handling alerts every other week. John handles alerts Sunday through Saturday one week, and Bob handles alerts for the following seven days. This continues in perpetuity.

Define a timeperiod for when John should receive notifications. Assuming today's date is Sunday, July 29th, 2007 and John is handling notifications this week (starting today), the definition would look like this:

```
define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ 2007-07-29 / 14 00:00-24:00 ~ ~ ; Every 14 days (two weeks), starting Sunday, ←
 ~ ~ ~ ~ July 29th, 2007
 ~ ~ ~ ~ 2007-07-30 / 14 00:00-24:00 ~ ~ ; Every other Monday starting July 30th, 2007
 ~ ~ ~ ~ 2007-07-31 / 14 00:00-24:00 ~ ~ ; Every other Tuesday starting July 31st, 2007
 ~ ~ ~ ~ 2007-08-01 / 14 00:00-24:00 ~ ~ ; Every other Wednesday starting August 1st, ←
 ~ ~ ~ ~ 2007
 ~ ~ ~ ~ 2007-08-02 / 14 00:00-24:00 ~ ~ ; Every other Thursday starting August 2nd, ←
 ~ ~ ~ ~ 2007
 ~ ~ ~ ~ 2007-08-03 / 14 00:00-24:00 ~ ~ ; Every other Friday starting August 3rd, 2007
 ~ ~ ~ ~ 2007-08-04 / 14 00:00-24:00 ~ ~ ; Every other Saturday starting August 4th, ←
 ~ ~ ~ ~ 2007
 ~ ~ ~ ~ }
```

Now define a timeperiod for when Bob should receive notifications. Bob gets notifications on the weeks that John doesn't, so his first on-call day starts next Sunday (August 5th, 2007).

```
define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ 2007-08-05 / 14 00:00-24:00 ~ ~ ; Every 14 days (two weeks), starting Sunday, ←
 ~ ~ ~ ~ August 5th, 2007
 ~ ~ ~ ~ 2007-08-06 / 14 00:00-24:00 ~ ~ ; Every other Monday starting August 6th, 2007
 ~ ~ ~ ~ 2007-08-07 / 14 00:00-24:00 ~ ~ ; Every other Tuesday starting August 7th, 2007
 ~ ~ ~ ~ 2007-08-08 / 14 00:00-24:00 ~ ~ ; Every other Wednesday starting August 8th, ←
 ~ ~ ~ ~ 2007
 ~ ~ ~ ~ 2007-08-09 / 14 00:00-24:00 ~ ~ ; Every other Thursday starting August 9th, ←
 ~ ~ ~ ~ 2007
 ~ ~ ~ ~ 2007-08-10 / 14 00:00-24:00 ~ ~ ; Every other Friday starting August 10th, 2007
```

```
~ ~ ~ 2007-08-11 / 14 00:00-24:00 ~ ~ ; Every other Saturday starting August 11th, ↵
 2007
~ ~ ~ ~ }
```

Now you need to reference these timeperiod definitions in the contact definitions for John and Bob:

```
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~john
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ ~john-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ }
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~bob
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ ~bob-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ }
```

## 44.5 Scenario 4: Vacation Days

In this scenarios, John handles notifications for all days except those he has off. He has several standing days off each month, as well as some planned vacations. Bob handles notifications when John is on vacation or out of the office.

First, define a timeperiod that contains time ranges for John's vacation days and days off:

```
define timeperiod{
 ~ ~ ~ ~ name ~ ~john-out-of-office
 ~ ~ ~ ~ timeperiod_name john-out-of-office
 ~ ~ ~ ~ day 15 ~ ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ~ ~ ~ ~ ; 15th day of each month
 ~ ~ ~ ~ day -1 ~ ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ~ ~ ~ ~ ; Last day of each month (28 ←
 th, 29th, 30th, or 31st)
 ~ ~ ~ ~ day -2 ~ ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ~ ~ ~ ~ ; 2nd to last day of each ←
 month (27th, 28th, 29th, or 30th)
 ~ ~ ~ ~ january 2 ~ ~ ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ~ ~ ~ ~ ; January 2nd each year
 ~ ~ ~ ~ june 1 - july 5 ~ ~ ~ ~ ~ ~00:00-24:00 ~ ~ ~ ~ ~ ~ ; Yearly camping trip (June 1 ←
 st - July 5th)
 ~ ~ ~ ~ 2007-11-01 - 2007-11-10 00:00-24:00 ~ ~ ~ ~ ~ ~ ; Vacation to the US Virgin ←
 Islands (November 1st-10th, 2007)
 ~ ~ ~ ~ }
```

Next, define a timeperiod for John's on-call times that excludes the dates/times defined in the timeperiod above:

```
define timeperiod{
 ~ ~ ~ ~ timeperiod_name ~ ~ ~ ~ john-oncall
 ~ ~ ~ ~ monday ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ tuesday ~ ~ ~ ~ 00:00-24:00
 ~ ~ ~ ~ wednesday ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ thursday ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ friday ~ ~ ~ ~ ~00:00-24:00
 ~ ~ ~ ~ exclude ~ ~ ~ ~ john-out-of-office ~ ~ ~; Exclude dates/times John is out
 ~ ~ ~ ~ }
}
```

You can now reference this timeperiod in John's contact definition:

```
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~ ~ john
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ ~ john-oncall
}
```

```
~ ~ ~ ~ service_notification_period ~ ~ ~ john-oncall
~ ~ ~ ~ }
```

Define a new timeperiod for Bob's on-call times that include the dates/times that John is out of the office:

```
define timeperiod{
 ~ ~ ~ ~ timeperod_name ~ ~ ~bob-oncall
 ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ john-out-of-office ~ ~ ~; Include holiday date/times that ←
 John is out
 ~ ~ ~ ~ }
}
```

You can now reference this timeperiod in Bob's contact definition:

```
define contact{
 ~ ~ ~ ~ contact_name ~ ~ ~ ~ ~ ~bob
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ host_notification_period ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ service_notification_period ~ ~ ~ ~ bob-oncall
 ~ ~ ~ ~ }
```

## 44.6 Other Scenarios

There are a lot of other on-call notification rotation scenarios that you might have. The date exception directive in [timeperiod definitions](#) is capable of handling most dates and date ranges that you might need to use, so check out the different formats that you can use. If you make a mistake when creating timeperiod definitions, always err on the side of giving someone else more on-call duty time. :-)

## Chapter 45

# Monitoring Service and Host Clusters

### 45.1 Introduction

Several people have asked how to go about monitoring clusters of hosts or services, so I decided to write up a little documentation on how to do this. Its fairly straightforward, so hopefully you find things easy to understand...

First off, we need to define what we mean by a "cluster". The simplest way to understand this is with an example. Let's say that your organization has five hosts which provide redundant DNS services to your organization. If one of them fails, its not a major catastrophe because the remaining servers will continue to provide name resolution services. If you're concerned with monitoring the availability of DNS service to your organization, you will want to monitor five DNS servers. This is what I consider to be a service cluster. The service cluster consists of five separate DNS services that you are monitoring. Although you do want to monitor each individual service, your main concern is with the overall status of the DNS service cluster, rather than the availability of any one particular service.

If your organization has a group of hosts that provide a high-availability (clustering) solution, I would consider those to be a host cluster. If one particular host fails, another will step in to take over all the duties of the failed server. As a side note, check out the [High-Availability Linux Project](#) for information on providing host and service redundancy with Linux.

### 45.2 Plan of Attack

There are several ways you could potentially monitor service or host clusters. I'll describe the method that I believe to be the easiest. Monitoring service or host clusters involves two things:

- Monitoring individual cluster elements
- Monitoring the cluster as a collective entity

Monitoring individual host or service cluster elements is easier than you think. In fact, you're probably already doing it. For service clusters, just make sure that you are monitoring each service element of the cluster. If you've got a cluster of five DNS servers, make sure you have five separate service definitions (probably using the **check\_dns** plugin). For host clusters, make sure you have configured appropriate host definitions for each member of the cluster (you'll also have to define at least one service to be monitored for each of the hosts).



#### Important

You're going to want to disable notifications for the individual cluster elements (host or service definitions). Even though no notifications will be sent about the individual elements, you'll still get a visual display of the individual host or service status in the **status CGI**. This will be useful for pinpointing the source of problems within the cluster in the future.

Monitoring the overall cluster can be done by using the previously cached results of cluster elements. Although you could re-check all elements of the cluster to determine the cluster's status, why waste bandwidth and resources when you already have the results cached? Where are the results cached? Cached results for cluster elements can be found in the **status file** (assuming you are monitoring each element). The **check\_cluster** plugin is designed specifically for checking cached host and service states in the status file.



#### Important

Although you didn't enable notifications for individual elements of the cluster, you will want them enabled for the overall cluster status check.

## 45.3 Using the check\_cluster Plugin

The **check\_cluster** plugin is designed to report the overall status of a host or service cluster by checking the status information of each individual host or service cluster elements.

More to come... The **check\_cluster** plugin can be found in the `contrib` directory of the Nagios Plugins release at <http://sourceforge.net/projects/nagiosplug/>.

## 45.4 Monitoring Service Clusters

Let's say you have three DNS servers that provide redundant services on your network. First off, you need to be monitoring each of these DNS servers separately before you can monitor them as a cluster. I'll assume that you already have three separate services (all called "DNS Service") associated with your DNS hosts (called "host1", "host2" and "host3").

In order to monitor the services as a cluster, you'll need to create a new "cluster" service. However, before you do that, make sure you have a service cluster check command configured. Let's assume that you have a command called `check_service_cluster` defined as follows:

```
define command{
~ ~ ~ ~ command_name ~ ~check_service_cluster
~ ~ ~ ~ command_line ~ ~/usr/local/nagios/libexec/check_cluster --service -l $ARG1$ -w ↔
~ ~ ~ ~ $ARG2$ -c $ARG3$ -d $ARG4$
~ ~ ~ ~ }
```

Now you'll need to create the "cluster" service and use the `check_service_cluster` command you just created as the cluster's check command. The example below gives an example of how to do this. The example below will generate a **CRITICAL** alert if 2 or more services in the cluster are in a non-OK state, and a **WARNING** alert if only 1 of the services is in a non-OK state. If all the individual service members of the cluster are OK, the cluster check will return an OK state as well.

```
define service{
...
check_command ~ check_service_cluster!"DNS Cluster"!1!2!$SERVICESTATEID:host1:DNS ↔
Service$, $SERVICESTATEID:host2:DNS Service$, $SERVICESTATEID:host3:DNS Service$
...
}
```

It is important to notice that we are passing a comma-delimited list of on-demand service state **macros** to the `$ARG4$` macro in the cluster check command. That's important! Nagios will fill those on-demand macros in with the current service state IDs (numerical values, rather than text strings) of the individual members of the cluster.

## 45.5 Monitoring Host Clusters

Monitoring host clusters is very similar to monitoring service clusters. Obviously, the main difference is that the cluster members are hosts and not services. In order to monitor the status of a host cluster, you must define a service that uses the **check\_cluster**

plugin. The service should not be associated with any of the hosts in the cluster, as this will cause problems with notifications for the cluster if that host goes down. A good idea might be to associate the service with the host that Nagios is running on. After all, if the host that Nagios is running on goes down, then Nagios isn't running anymore, so there isn't anything you can do as far as monitoring (unless you've setup **redundant monitoring hosts**)...

Anyway, let's assume that you have a `check_host_cluster` command defined as follows:

```
define command{
 command_name ~ ~check_host_cluster
 command_line ~ ~/usr/local/nagios/libexec/check_cluster --host -l $ARG1$ -w $ARG2$ -c ↵
 $ARG3$ -d $ARG4$
}
```

Let's say you have three hosts (named "host1", "host2" and "host3") in the host cluster. If you want Nagios to generate a warning alert if one host in the cluster is not UP or a critical alert if two or more hosts are not UP, the the service you define to monitor the host cluster might look something like this:

```
define service{
 ~ ~ ~ ...
 ~ ~ ~ check_command ~ check_host_cluster!"Super Host Cluster"!1!2!$HOSTSTATEID:host1$, ↵
 $HOSTSTATEID:host2$, $HOSTSTATEID:host3$
 ~ ~ ~ ...
 ~ ~ ~ ~ }
```

It is important to notice that we are passing a comma-delimited list of on-demand host state **macros** to the `$ARG4$` macro in the cluster check command. That's important! Nagios will fill those on-demand macros in with the current host state IDs (numerical values, rather than text strings) of the individual members of the cluster.

That's it! Nagios will periodically check the status of the host cluster and send notifications to you when its status is degraded (assuming you've enabled notification for the service). Note that for the host definitions of each cluster member, you will most likely want to disable notifications when the host goes down . Remember that you don't care as much about the status of any individual host as you do the overall status of the cluster. Depending on your network layout and what you're trying to accomplish, you may wish to leave notifications for unreachable states enabled for the host definitions.

## Chapter 46

# Host and Service Dependencies

### 46.1 Introduction

Service and host dependencies are an advanced feature of Nagios that allow you to control the behavior of hosts and services based on the status of one or more other hosts or services. I'll explain how dependencies work, along with the differences between host and service dependencies.

### 46.2 Service Dependencies Overview

There are a few things you should know about service dependencies:

1. A service can be dependent on one or more other services
2. A service can be dependent on services which are not associated with the same host
3. Service dependencies are not inherited (unless specifically configured to)
4. Service dependencies can be used to cause service check execution and service notifications to be suppressed under different circumstances (OK, WARNING, UNKNOWN, and/or CRITICAL states)
5. Service dependencies might only be valid during specific **timeperiods**

### 46.3 Defining Service Dependencies

First, the basics. You create service dependencies by adding **service dependency definitions** in your **object config file(s)**. In each definition you specify the *dependent* service, the service you are *depending on*, and the criteria (if any) that cause the execution and notification dependencies to fail (these are described later).

You can create several dependencies for a given service, but you must add a separate service dependency definition for each dependency you create.

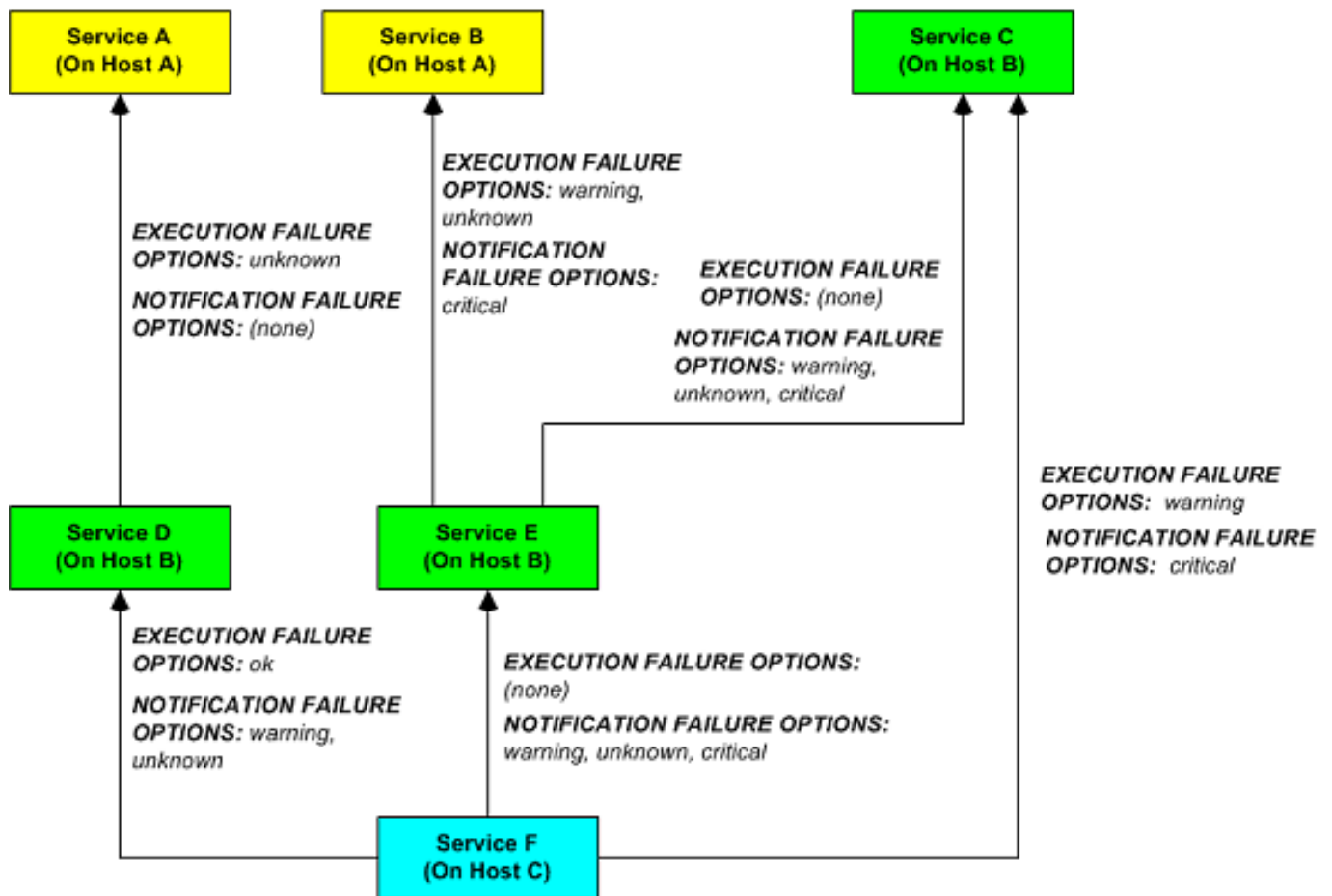
### 46.4 Example Service Dependencies

The image below shows an example logical layout of service notification and execution dependencies. Different services are dependent on other services for notifications and check execution.

---



## Service Dependencies



In this example, the dependency definitions for *Service F* on *Host C* would be defined as follows:

```
define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ ~ ~ Service D
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ dependent_service_description ~ ~ ~ ~ ~ ~ ~ ~ Service F
~ ~ ~ ~ execution_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ o
~ ~ ~ ~ notification_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ w,u
~ ~ ~ ~ }

define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ ~ ~ Service E
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ dependent_service_description ~ ~ ~ ~ ~ ~ ~ ~ Service F
~ ~ ~ ~ execution_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ n
~ ~ ~ ~ notification_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ w,u,c
~ ~ ~ ~ }

define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ ~ ~ Service C
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ dependent_service_description ~ ~ ~ ~ ~ ~ ~ ~ Service F
```

```

~ ~ ~ ~ execution_failure_criteria ~ ~ ~w
~ ~ ~ ~ notification_failure_criteria ~ c
~ ~ ~ ~ }

```

The other dependency definitions shown in the image above would be defined as follows:

```

define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host A
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ Service A
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ dependent_service_description ~ Service D
~ ~ ~ ~ execution_failure_criteria ~ ~ ~u
~ ~ ~ ~ notification_failure_criteria ~ n
~ ~ ~ ~ }

define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host A
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ Service B
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ dependent_service_description ~ Service E
~ ~ ~ ~ execution_failure_criteria ~ ~ ~w,u
~ ~ ~ ~ notification_failure_criteria ~ c
~ ~ ~ ~ }

define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ Service C
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ dependent_service_description ~ Service E
~ ~ ~ ~ execution_failure_criteria ~ ~ ~n
~ ~ ~ ~ notification_failure_criteria ~ w,u,c
~ ~ ~ ~ }

```

## 46.5 How Service Dependencies Are Tested

Before Nagios executes a service check or sends notifications out for a service, it will check to see if the service has any dependencies. If it doesn't have any dependencies, the check is executed or the notification is sent out as it normally would be. If the service *does* have one or more dependencies, Nagios will check each dependency entry as follows:

1. Nagios gets the current status\* of the service that is being *depended upon*.
2. Nagios compares the current status of the service that is being *depended upon* against either the execution or notification failure options in the dependency definition (whichever one is relevant at the time).
3. If the current status of the service that is being *depended upon* matches one of the failure options, the dependency is said to have failed and Nagios will break out of the dependency check loop.
4. If the current state of the service that is being *depended upon* does not match any of the failure options for the dependency entry, the dependency is said to have passed and Nagios will go on and check the next dependency entry.

This cycle continues until either all dependencies for the service have been checked or until one dependency check fails.

### Note

\* One important thing to note is that by default, Nagios will use the most current **hard state** of the service(s) that is/are being depended upon when it does the dependency checks. If you want Nagios to use the most current state of the services (regardless of whether its a soft or hard state), enable the **soft\_state\_dependencies** option.

## 46.6 Execution Dependencies

Execution dependencies are used to restrict when **active checks** of a service can be performed. **Passive checks** are not restricted by execution dependencies.

If all of the execution dependency tests for the service passed, Nagios will execute the check of the service as it normally would. If even just one of the execution dependencies for a service fails, Nagios will temporarily prevent the execution of checks for that (dependent) service. At some point in the future the execution dependency tests for the service may all pass. If this happens, Nagios will start checking the service again as it normally would. More information on the check scheduling logic can be found [here](#).

In the example above, **Service E** would have failed execution dependencies if **Service B** is in a WARNING or UNKNOWN state. If this was the case, the service check would not be performed and the check would be scheduled for (potential) execution at a later time.

## 46.7 Notification Dependencies

If all of the notification dependency tests for the service *passed*, Nagios will send notifications out for the service as it normally would. If even just one of the notification dependencies for a service fails, Nagios will temporarily repress notifications for that (dependent) service. At some point in the future the notification dependency tests for the service may all pass. If this happens, Nagios will start sending out notifications again as it normally would for the service. More information on the notification logic can be found [here](#).

In the example above, **Service F** would have failed notification dependencies if **Service C** is in a CRITICAL state, *and/or* **Service D** is in a WARNING or UNKNOWN state, *and/or* if **Service E** is in a WARNING, UNKNOWN, or CRITICAL state. If this were the case, notifications for the service would not be sent out.

## 46.8 Dependency Inheritance

As mentioned before, service dependencies are not inherited by default. In the example above you can see that Service F is dependent on Service E. However, it does not automatically inherit Service E's dependencies on Service B and Service C. In order to make Service F dependent on Service C we had to add another service dependency definition. There is no dependency definition for Service B, so Service F is not dependent on Service B.

If you do wish to make service dependencies inheritable, you must use the `inherits_parent` directive in the **service dependency** definition. When this directive is enabled, it indicates that the dependency inherits dependencies of the service that is being depended upon (also referred to as the master service). In other words, if the master service is dependent upon other services and any one of those dependencies fail, this dependency will also fail.

In the example above, imagine that you want to add a new dependency for service F to make it dependent on service A. You could create a new dependency definition that specified service F as the dependent service and service A as being the master service (i.e. the service that is being dependend on). You could alternatively modify the dependency definition for services D and F to look like this:

```
define servicedependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ service_description ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Service D
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ dependent_service_description ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Service F
~ ~ ~ ~ execution_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ o
~ ~ ~ ~ notification_failure_criteria ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ n
~ ~ ~ ~ inherits_parent ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 1
~ ~ ~ ~ }
```

Since the `inherits_parent` directive is enabled, the dependency between services A and D will be tested when the dependency between services F and D are being tested.

Dependencies can have multiple levels of inheritance. If the dependency definition between A and D had its `inherits_parent` directive enable and service A was dependent on some other service (let's call it service G), the service F would be dependent on services D, A, and G (each with potentially different criteria).

## 46.9 Host Dependencies

As you'd probably expect, host dependencies work in a similar fashion to service dependencies. The difference is that they're for hosts, not services.

---

### Tip

Do not confuse host dependencies with parent/child host relationships. You should be using parent/child host relationships (defined with the `parents` directive in [host](#) definitions) for most cases, rather than host dependencies. A description of how parent/child host relationships work can be found in the documentation on [network reachability](#).

---

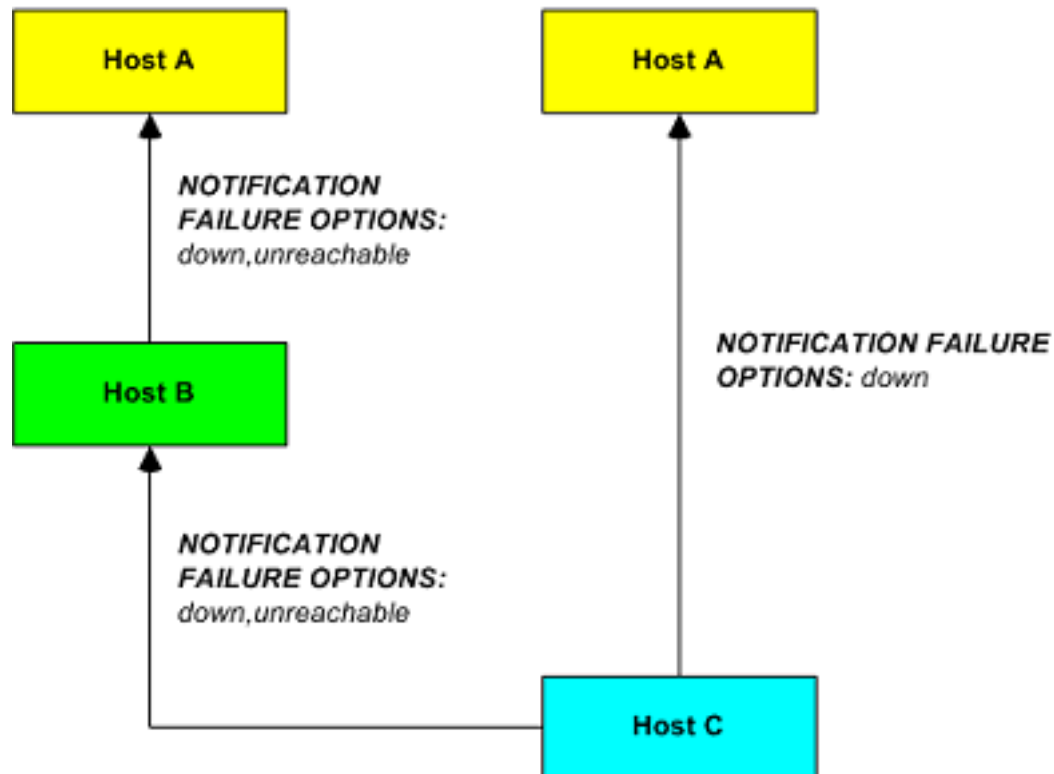
Here are the basics about host dependencies:

1. A host can be dependent on one or more other host
2. Host dependencies are not inherited (unless specifically configured to)
3. Host dependencies can be used to cause host check execution and host notifications to be suppressed under different circumstances (UP, DOWN, and/or UNREACHABLE states)
4. Host dependencies might only be valid during specific [timeperiods](#)

## 46.10 Example Host Dependencies

The image below shows an example of the logical layout of host notification dependencies. Different hosts are dependent on other hosts for notifications.

# Host Dependencies



In the example above, the dependency definitions for Host C would be defined as follows:

```

define hostdependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host A
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ notification_failure_criteria ~ d
~ ~ ~ ~ }

define hostdependency{
~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ Host B
~ ~ ~ ~ dependent_host_name ~ ~ ~ ~ ~ Host C
~ ~ ~ ~ notification_failure_criteria ~ d,u
~ ~ ~ ~ }

```

As with service dependencies, host dependencies are not inherited. In the example image you can see that Host C does not inherit the host dependencies of Host B. In order for Host C to be dependent on Host A, a new host dependency definition must be defined.

Host notification dependencies work in a similar manner to service notification dependencies. If *all* of the notification dependency tests for the host *pass*, Nagios will send notifications out for the host as it normally would. If even just one of the notification dependencies for a host fails, Nagios will temporarily repress notifications for that (dependent) host. At some point in the future the notification dependency tests for the host may all pass. If this happens, Nagios will start sending out notifications again as it normally would for the host. More information on the notification logic can be found [here](#).

## Chapter 47

# State Stalking

### 47.1 Introduction

State "stalking" is a feature which is probably not going to be used by most users. When enabled, it allows you to log changes in the output service and host checks even if the state of the host or service does not change. When stalking is enabled for a particular host or service, Nagios will watch that host or service very carefully and log any changes it sees in the output of check results. As you'll see, it can be very helpful to you in later analysis of the log files.

### 47.2 How Does It Work?

Under normal circumstances, the result of a host or service check is only logged if the host or service has changed state since it was last checked. There are a few exceptions to this, but for the most part, that's the rule.

If you enable stalking for one or more states of a particular host or service, Nagios will log the results of the host or service check if the output from the check differs from the output from the previous check. Take the following example of eight consecutive checks of a service:

| Service Check #: | Service State: | Service Check Output:                                                          | Logged Normally | Logged With Stalking |
|------------------|----------------|--------------------------------------------------------------------------------|-----------------|----------------------|
| x                | OK             | RAID array optimal                                                             | -               | -                    |
| x+1              | OK             | RAID array optimal                                                             | -               | -                    |
| x+2              | WARNING        | RAID array degraded (1 drive bad, 1 hot spare rebuilding)                      | ✓               | ✓                    |
| x+3              | CRITICAL       | RAID array degraded (2 drives bad, 1 hot spare online, 1 hot spare rebuilding) | ✓               | ✓                    |
| x+4              | CRITICAL       | RAID array degraded (3 drives bad, 2 hot spares online)                        | -               | ✓                    |
| x+5              | CRITICAL       | RAID array failed                                                              | -               | ✓                    |
| x+6              | CRITICAL       | RAID array failed                                                              | -               | -                    |
| x+7              | CRITICAL       | RAID array failed                                                              | -               | -                    |

Given this sequence of checks, you would normally only see two log entries for this catastrophe. The first one would occur at service check x+2 when the service changed from an OK state to a WARNING state. The second log entry would occur at service check x+3 when the service changed from a WARNING state to a CRITICAL state.

For whatever reason, you may like to have the complete history of this catastrophe in your log files. Perhaps to help explain to your manager how quickly the situation got out of control, perhaps just to laugh at it over a couple of drinks at the local pub...

Well, if you had enabled stalking of this service for CRITICAL states, you would have events at x+4 and x+5 logged in addition to the events at x+2 and x+3. Why is this? With state stalking enabled, Nagios would have examined the output from each service check to see if it differed from the output of the previous check. If the output differed and the state of the service didn't change between the two checks, the result of the newer service check would get logged.

A similar example of stalking might be on a service that checks your web server. If the **check\_http** plugin first returns a WARNING state because of a 404 error and on subsequent checks returns a WARNING state because of a particular pattern not being found, you might want to know that. If you didn't enable state stalking for WARNING states of the service, only the first WARNING state event (the 404 error) would be logged and you wouldn't have any idea (looking back in the archived logs) that future WARNING states were not due to a 404, but rather some text pattern that could not be found in the returned web page.

## 47.3 Should I Enable Stalking?

First, you must decide if you have a real need to analyze archived log data to find the exact cause of a problem. You may decide you need this feature for some hosts or services, but not for all. You may also find that you only have a need to enable stalking for some host or service states, rather than all of them. For example, you may decide to enable stalking for WARNING and CRITICAL states of a service, but not for OK and UNKNOWN states.

The decision to enable state stalking for a particular host or service will also depend on the plugin that you use to check that host or service. If the plugin always returns the same text output for a particular state, there is no reason to enable stalking for that state.

## 47.4 How Do I Enable Stalking?

You can enable state stalking for hosts and services by using the `stalking_options` directive in [host and service definitions](#).

## 47.5 How Does Stalking Differ From Volatile Services?

**Volatile services** are similar, but will cause notifications and event handlers to run. Stalking is purely for logging purposes.

## 47.6 Caveats

You should be aware that there are some potential pitfalls with enabling stalking. These all relate to the reporting functions found in various **CGIs** (histogram, alert summary, etc.). Because state stalking will cause additional alert entries to be logged, the data produced by the reports will show evidence of inflated numbers of alerts.

As a general rule, I would suggest that you *not* enable stalking for hosts and services without thinking things through. Still, it's there if you need and want it.

---

## Chapter 48

# Performance Data

### 48.1 Introduction

Nagios is designed to allow **plugins** to return optional performance data in addition to normal status data, as well as allow you to pass that performance data to external applications for processing. A description of the different types of performance data, as well as information on how to go about processing that data is described below...

### 48.2 Types of Performance Data

There are two basic categories of performance data that can be obtained from Nagios:

1. Check performance data
2. Plugin performance data

Check performance data is internal data that relates to the actual execution of a host or service check. This might include things like service check latency (i.e. how "late" was the service check from its scheduled execution time) and the number of seconds a host or service check took to execute. This type of performance data is available for all checks that are performed. The **\$HOSTEXECUTIONTIME\$** and **\$SERVICEEXECUTIONTIME\$** macros can be used to determine the number of seconds a host or service check was running and the **\$HOSTLATENCY\$** and **\$SERVICELATENCY\$** macros can be used to determine how "late" a regularly-scheduled host or service check was.

Plugin performance data is external data specific to the plugin used to perform the host or service check. Plugin-specific data can include things like percent packet loss, free disk space, processor load, number of current users, etc. - basically any type of metric that the plugin is measuring when it executes. Plugin-specific performance data is optional and may not be supported by all plugins. Plugin-specific performance data (if available) can be obtained by using the **\$HOSTPERFDATA\$** and **\$SERVICEPERFDATA\$** macros. Read on for more information on how plugins can return performance data to Nagios for inclusion in the **\$HOSTPERFDATA\$** and **\$SERVICEPERFDATA\$** macros.

### 48.3 Plugin Performance Data

At a minimum, Nagios plugins must return a single line of human-readable text that indicates the status of some type of measurable data. For example, the **check\_ping** plugin might return a line of text like the following:

```
PING ok - Packet loss = 0%, RTA = 0.80 ms
```

With this simple type of output, the entire line of text is available in the **\$HOSTOUTPUT\$** or **\$SERVICEOUTPUT\$** macros (depending on whether this plugin was used as a host check or service check).



Plugins can return optional performance data in their output by sending the normal, human-readable text string that they usually would, followed by a pipe character (`|`), and then a string containing one or more performance data metrics. Let's take the **check\_ping** plugin as an example and assume that it has been enhanced to return percent packet loss and average round trip time as performance data metrics. Sample output from the plugin might look like this:

```
PING ok - Packet loss = 0%, RTA = 0.80 ms | percent_packet_loss=0, rta=0.80
```

When Nagios sees this plugin output format it will split the output into two parts:

1. Everything before the pipe character is considered to be the 'normal' plugin output and will be stored in either the `$HOSTOUTPUT$` or `$SERVICEOUTPUT$` macro
2. Everything after the pipe character is considered to be the plugin-specific performance data and will be stored in the `$HOSTPERFDATA$` or `$SERVICEPERFDATA$` macro

In the example above, the `$HOSTOUTPUT$` or `$SERVICEOUTPUT$` macro would contain *"PING ok - Packet loss = 0%, RTA = 0.80 ms"* (without quotes) and the `$HOSTPERFDATA$` or `$SERVICEPERFDATA$` macro would contain *"percent\_packet\_loss=0, rta=0.80"* (without quotes).

Multiple lines of performance data (as well as normal text output) can be obtained from plugins, as described in the [plugin API documentation](#).

#### Note

The Nagios daemon doesn't directly process plugin performance data, so it doesn't really care what the performance data looks like. There aren't really any inherent limitations on the format or content of the performance data. However, if you are using an external addon to process the performance data (i.e. PerfParse), the addon may be expecting that the plugin returns performance data in a specific format. Check the documentation that comes with the addon for more information.

## 48.4 Processing Performance Data

If you want to process the performance data that is available from Nagios and the plugins, you'll need to do the following:

1. Enable the [process\\_performance\\_data](#) option.
2. Configure Nagios so that performance data is either written to files and/or processed by executing commands.

Read on for information on how to process performance data by writing to files or executing commands.

## 48.5 Processing Performance Data Using Commands

The most flexible way to process performance data is by having Nagios execute commands (that you specify) to process or redirect the data for later processing by external applications. The commands that Nagios executes to process host and service performance data are determined by the [host\\_perfdata\\_command](#) and [service\\_perfdata\\_command](#) options, respectively.

An example command definition that redirects service check performance data to a text file for later processing by another application is shown below:

```
define command{
 ~ ~ ~ ~ command_name ~ ~store-service-perfdata
 ~ ~ ~ ~ command_line ~ ~/bin/echo -e "$LASTSERVICECHECK$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICESTATE$\t$SERVICEATTEMPT$\t$SERVICESTATETYPE$\t$SERVICEEXECUTIONTIME$\t$SERVICELATENCY$\t$SERVICEOUTPUT$\t$SERVICEPERFDATA$" >> /usr/local/nagios/var/service-perfdata.dat
 ~ ~ ~ ~ }
```

---

**Tip**

This method, while flexible, comes with a relatively high CPU overhead. If you're processing performance data for a large number of hosts and services, you'll probably want Nagios to write performance data to files instead. This method is described in the next section.

---

## 48.6 Writing Performance Data To Files

You can have Nagios write all host and service performance data directly to text files using the `host_perfdata_file` and `service_perfdata_file` options. The format in which host and service performance data is written to those files is determined by the `host_perfdata_file_template` and `service_perfdata_file_template` options.

An example file format template for service performance data might look like this:

```
service_perfdata_file_template=[SERVICEPERFDATA] \t$TIMET$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICEEXECUTIONTIME$\t$SERVICELATENCY$\t$SERVICEOUTPUT$\t$SERVICEPERFDATA$ ↵
```

By default, the text files will be opened in "append" mode. If you need to change the modes to "write" or "non-blocking read/write" (useful when writing to pipes), you can use the `host_perfdata_file_mode` and `service_perfdata_file_mode` options.

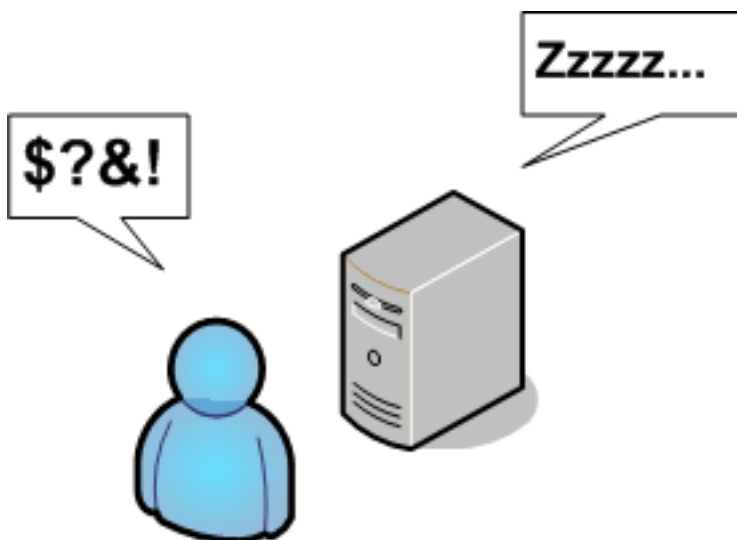
Additionally, you can have Nagios periodically execute commands to periodically process the performance data files (e.g. rotate them) using the `host_perfdata_file_processing_command` and `service_perfdata_file_processing_command` options. The interval at which these commands are executed are governed by the `host_perfdata_file_processing_interval` and `service_perfdata_file_processing_interval` options, respectively.

---

## Chapter 49

# Scheduled Downtime

### 49.1 Introduction



Nagios allows you to schedule periods of planned downtime for hosts and service that you're monitoring. This is useful in the event that you actually know you're going to be taking a server down for an upgrade, etc.

### 49.2 Scheduling Downtime

You can schedule downtime for hosts and service through the [extinfo CGI](#) (either when viewing host or service information). Click in the Schedule downtime for this host/service link to actually schedule the downtime.

Once you schedule downtime for a host or service, Nagios will add a comment to that host/service indicating that it is scheduled for downtime during the period of time you indicated. When that period of downtime passes, Nagios will automatically delete the comment that it added. Nice, huh?

### 49.3 Fixed vs. Flexible Downtime

When you schedule downtime for a host or service through the web interface you'll be asked if the downtime is fixed or flexible. Here's an explanation of how "fixed" and "flexible" downtime differs:

"Fixed" downtime starts and stops at the exact start and end times that you specify when you schedule it. Okay, that was easy enough...

"Flexible" downtime is intended for times when you know that a host or service is going to be down for X minutes (or hours), but you don't know exactly when that'll start. When you schedule flexible downtime, Nagios will start the scheduled downtime sometime between the start and end times you specified. The downtime will last for as long as the duration you specified when you scheduled the downtime. This assumes that the host or service for which you scheduled flexible downtime either goes down (or becomes unreachable) or goes into a non-OK state sometime between the start and end times you specified. The time at which a host or service transitions to a problem state determines the time at which Nagios actually starts the downtime. The downtime will then last for the duration you specified, even if the host or service recovers before the downtime expires. This is done for a very good reason. As we all know, you might think you've got a problem fixed, but then have to restart a server ten times before it actually works right. Smart, eh?

## 49.4 Triggered Downtime

When scheduling host or service downtime you have the option of making it "triggered" downtime. What is triggered downtime, you ask? With triggered downtime the start of the downtime is triggered by the start of some other scheduled host or service downtime. This is extremely useful if you're scheduling downtime for a large number of hosts or services and the start time of the downtime period depends on the start time of another downtime entry. For instance, if you schedule flexible downtime for a particular host (because its going down for maintenance), you might want to schedule triggered downtime for all of that host's "children".

## 49.5 How Scheduled Downtime Affects Notifications

When a host or service is in a period of scheduled downtime, Nagios will not allow normal notifications to be sent out for the host or service. However, a "DOWNTIMESTART" notification will get sent out for the host or service, which will serve to put any admins on notice that they won't receive upcoming problem alerts.

When the scheduled downtime is over, Nagios will allow normal notifications to be sent out for the host or service again. A "DOWNTIMEEND" notification will get sent out notifying admins that the scheduled downtime is over, and they will start receiving normal alerts again.

If the scheduled downtime is cancelled prematurely (before it expires), a "DOWNTIMECANCELLED" notification will get sent out to the appropriate admins.

## 49.6 Overlapping Scheduled Downtime

I like to refer to this as the "Oh crap, its not working" syndrome. You know what I'm talking about. You take a server down to perform a "routine" hardware upgrade, only to later realize that the OS drivers aren't working, the RAID array blew up, or the drive imaging failed and left your original disks useless to the world. Moral of the story is that any routine work on a server is quite likely to take three or four times as long as you had originally planned...

Let's take the following scenario:

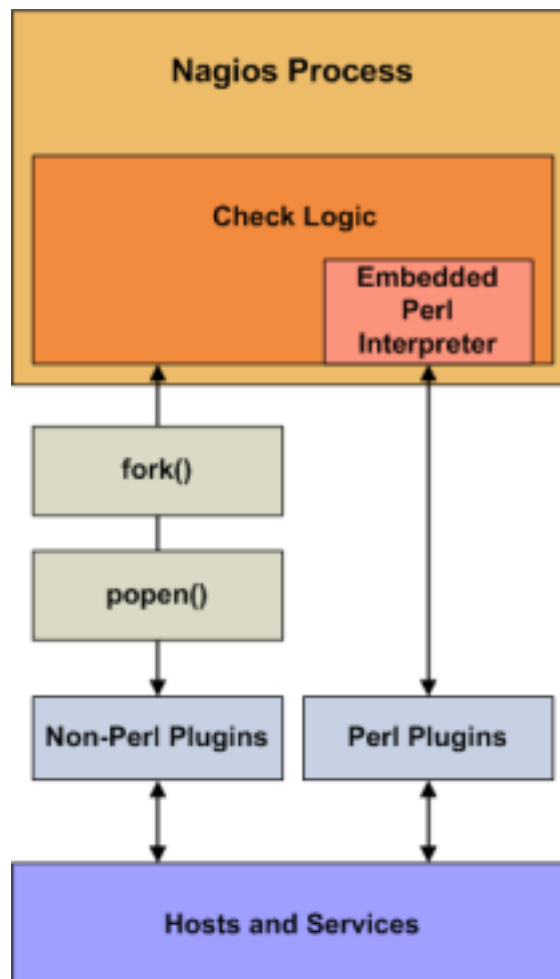
1. You schedule downtime for host A from 7:30pm-9:30pm on a Monday
2. You bring the server down about 7:45pm Monday evening to start a hard drive upgrade
3. After wasting an hour and a half battling with SCSI errors and driver incompatibilities, you finally get the machine to boot up
4. At 9:15 you realize that one of your partitions is either hosed or doesn't seem to exist anywhere on the drive
5. Knowing you're in for a long night, you go back and schedule additional downtime for host A from 9:20pm Monday evening to 1:30am Tuesday Morning.

If you schedule overlapping periods of downtime for a host or service (in this case the periods were 7:40pm-9:30pm and 9:20pm-1:30am), Nagios will wait until the last period of scheduled downtime is over before it allows notifications to be sent out for that host or service. In this example notifications would be suppressed for host A until 1:30am Tuesday morning.

## Chapter 50

# Using The Embedded Perl Interpreter

### 50.1 Introduction



Nagios can be compiled with support for an embedded Perl interpreter. This allows Nagios to execute Perl plugins much more efficiently than it otherwise would, so it may be of interest to you if you rely heavily on plugins written in Perl.

Without the embedded Perl interpreter, Nagios executes Perl (and non-Perl) plugins by forking and executing the plugins as an external command. When the embedded Perl interpreter is used, Nagios can execute Perl plugins by simply making a library call.

---

**Tip**

The embedded Perl interpreter works with all Perl scripts that Nagios executes - not just plugins. This documentation discusses the embedded Perl interpreter in relation to plugins used for host and service checks, but it applies just the same to other types of Perl scripts you may be using for other types of commands (e.g. notification scripts, event handler scripts, etc.).

---

Stephen Davies contributed the original embedded Perl interpreter code several years back. Stanley Hopcroft has been the primary person helping to improve the embedded Perl interpreter code quite a bit and has commented on the advantages/disadvantages of using it. He has also given several helpful hints on creating Perl plugins that work properly with the embedded interpreter.

It should be noted that "ePN", as used in this documentation, refers to embedded Perl Nagios, or if you prefer, Nagios compiled with an embedded Perl interpreter.

## 50.2 Advantages

Some advantages of ePN (embedded Perl Nagios) include:

- Nagios will spend much less time running your Perl plugins because it no longer forks to execute the plugin (each time loading the Perl interpreter). Instead, it executes your plugin by making a library call.
- It greatly reduces the system impact of Perl plugins and/or allows you to run more checks with Perl plugin than you otherwise would be able to. In other words, you have less incentive to write plugins in other languages such as C/C++, or Expect/TCL, that are generally recognised to have development times at least an order of magnitude slower than Perl (although they do run about ten times faster also - TCL being an exception).
- If you are not a C programmer, then you can still get a huge amount of mileage out of Nagios by letting Perl do all the heavy lifting without having Nagios slow right down. Note however, that the ePN will not speed up your plugin (apart from eliminating the interpreter load time). If you want fast plugins then consider Perl XSUBs (XS), or C after you are sure that your Perl is tuned and that you have a suitable algorithm (Benchmark.pm is invaluable for comparing the performance of Perl language elements).
- Using the ePN is an excellent opportunity to learn more about Perl.

## 50.3 Disadvantages

The disadvantages of ePN (embedded Perl Nagios) are much the same as Apache mod\_perl (i.e. Apache with an embedded interpreter) compared to a plain Apache:

- A Perl program that works fine with plain Nagios may not work with the ePN. You may have to modify your plugins to get them to work.
  - Perl plugins are harder to debug under an ePN than under a plain Nagios.
  - Your ePN will have a larger SIZE (memory footprint) than a plain Nagios.
  - Some Perl constructs cannot be used or may behave differently than what you would expect.
  - You may have to be aware of 'more than one way to do it' and choose a way that seems less attractive or obvious.
  - You will need greater Perl knowledge (but nothing very esoteric or stuff about Perl internals - unless your plugin uses XSUBS).
-

## 50.4 Using The Embedded Perl Interpreter

If you want to use the embedded Perl interpreter to run your Perl plugins and scripts, here's what you'll need to do:

1. Compile Nagios with support for the embedded Perl interpreter (see instructions below).
2. Enable the `enable_embedded_perl` option in the main configuration file.
3. Set the `use_embedded_perl_implicitly` option to fit your needs. This option determines whether or not the Perl interpreter should be used by default for individual Perl plugins and scripts.
4. Optionally enable or disable certain Perl plugins and scripts from being run using the embedded Perl interpreter. This can be useful if certain Perl scripts have problems being running under the Perl interpreter. See instructions below for more information on doing this.

## 50.5 Compiling Nagios With Embedded Perl

If you want to use the embedded Perl interpreter, you'll first need to compile Nagios with support for it. To do this, simply run the configure script with the addition of the `--enable-embedded-perl` option. If you want the embedded interpreter to cache internally compiled scripts, add the `--with-perlcache` option as well. Example:

```
linux:~ # ./configure --enable-embedded-perl --with-perlcache otheroptions...
```

Once you've rerun the configure script with the new options, make sure to recompile Nagios.

## 50.6 Plugin-Specific Use of the Perl Interpreter

Beginning with Nagios 3, you can specify which Perl plugins or scripts should or should not be run under the embedded Perl interpreter. This is particularly useful if you have troublesome Perl scripts which do not work well with the Perl interpreter.

To explicitly tell Nagios whether or not to use the embedded Perl interpreter for a particular perl script, add one of the following entries to your Perl script/plugin...

To tell Nagios to use the Perl interpreter for a particular script, add this line to the Perl script:

```
nagios: +epn
```

To tell Nagios to NOT use the embedded Perl interpreter for a particular script, add this line to the Perl script:

```
nagios: -epn
```

Either line must be located within the first 10 lines of a script for Nagios to detect it.

---

### Tip

If you do not explicitly use the method above to tell Nagios whether an individual plugin can be run under the Perl interpreter, Nagios will make will a decision for you. This decision process is controlled by the `use_embedded_perl_implicitly` variable. If the value is set to 1, all Perl plugins/scripts (that do not explicitly enable/disable the ePN) will be run under the Perl interpreter. If the value is 0, they will NOT be run under the Perl interpreter.

---

## 50.7 Developing Plugins For Use With Embedded Perl

Information on developing plugins for use with the embedded Perl interpreter can be found [here](#).

---

## Chapter 51

# Adaptive Monitoring

### 51.1 Introduction

Nagios allows you to change certain commands and host and service check attributes during runtime. I'll refer to this feature as 'adaptive monitoring'. Please note that the adaptive monitoring features found in Nagios will probably not be of much use to 99% of users, but they do allow you to do some neat things.

### 51.2 What Can Be Changed?

The following service check attributes can be changed during runtime:

- Check command (and command arguments)
- Check interval
- Max check attempts
- Check timeperiod
- Event handler command (and command arguments)

The following host check attributes can be changed during runtime:

- Check command (and command arguments)
- Check interval
- Max check attempts
- Check timeperiod
- Event handler command (and command arguments)

The following global attributes can be changed during runtime:

- Global host event handler command (and command arguments)
  - Global service event handler command (and command arguments)
-



## 51.3 External Commands For Adaptive Monitoring

In order to change global or host- or service-specific attributes during runtime, you must submit the appropriate **external command** to Nagios via the **external command file**. The table below lists the different attributes that may be changed during runtime, along with the external command to accomplish the job.

A full listing of external commands that can be used for adaptive monitoring (along with examples of how to use them) can be found online at the following URL: <http://www.nagios.org/developerinfo/externalcommands/>

---

### Note

- When changing check commands, check timeperiods, or event handler commands, it is important to note that the new values for these options must have been defined before Nagios was started. Any request to change a command or timeperiod to one which had not been defined when Nagios was started is ignored.
  - You can specify command arguments along with the actual command name - just separate individual arguments from the command name (and from each other) using bang (!) characters. More information on how arguments in command definitions are processed during runtime can be found in the documentation on **macros**.
-

## Chapter 52

# Predictive Dependency Checks

### 52.1 Introduction

Host and service **dependencies** can be defined to allow you greater control over when checks are executed and when notifications are sent out. As dependencies are used to control basic aspects of the monitoring process, it is crucial to ensure that status information used in the dependency logic is as up to date as possible.

Nagios allows you to enable predictive dependency checks for hosts and services to ensure that the dependency logic will have the most up-to-date status information when it comes to making decisions about whether to send out notifications or allow active checks of a host or service.

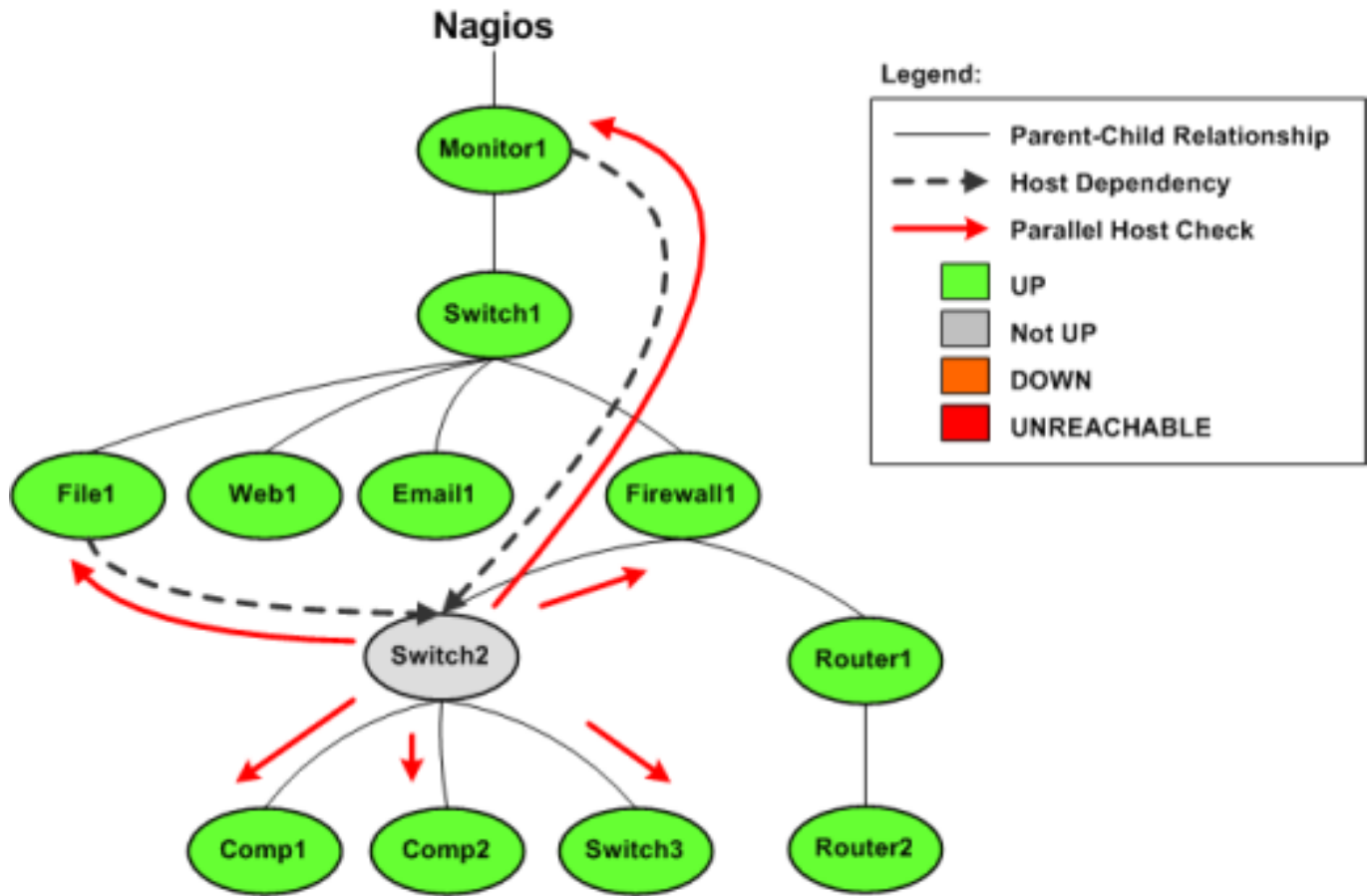
### 52.2 How Do Predictive Checks Work?

The image below shows a basic diagram of hosts that are being monitored by Nagios, along with their parent/child relationships and dependencies.

The *Switch2* host in this example has just changed state from an UP state to a problem state. Nagios needs to determine whether the host is DOWN or UNREACHABLE, so it will launch parallel checks of *Switch2*'s immediate parents (*Firewall1*) and children (*Comp1*, *Comp2*, and *Switch3*). This is a normal function of the **host reachability** logic.

You will also notice that *Switch2* is depending on *Monitor1* and *File1* for either notifications or check execution (which one is unimportant in this example). If predictive host dependency checks are enabled, Nagios will launch parallel checks of *Monitor1* and *File1* at the same time it launches checks of *Switch2*'s immediate parents and children. Nagios does this because it knows that it will have to test the dependency logic in the near future (e.g. for purposes of notification) and it wants to make sure it has the most current status information for the hosts that take part in the dependency.

---



That's how predictive dependency checks work. Simple, eh?

#### Note

Predictive service dependency checks work in a similar manner to what is described above. Except, of course, they deal with services instead of hosts.

## 52.3 Enabling Predictive Checks

Predictive dependency checks involve rather little overhead, so I would recommend that you enable them. In most cases, the benefits of having accurate information for the dependency logic outweighs the extra overhead imposed by these checks.

Enabling predictive dependency checks is easy:

- Predictive host dependency checks are controlled by the `enable_predictive_host_dependency_checks` option.
- Predictive service dependency checks are controlled by the `enable_predictive_service_dependency_checks` option.

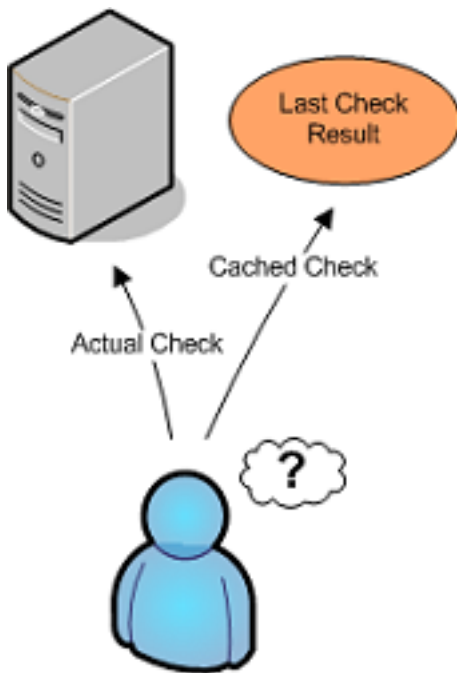
## 52.4 Cached Checks

Predictive dependency checks are on-demand checks and are therefore subject to the rules of **cached checks**. Cached checks can provide you with performance improvements by allowing Nagios to forgo running an actual host or service check if it can use a relatively recent check result instead. More information on cached checks can be found [here](#).

## Chapter 53

# Cached Checks

### 53.1 Introduction



The performance of Nagios' monitoring logic can be significantly improved by implementing the use of cached checks. Cached checks allow Nagios to forgo executing a host or service check command if it determines a relatively recent check result will do instead.

### 53.2 For On-Demand Checks Only

Regularly scheduled host and service checks will not see a performance improvement with use of cached checks. Cached checks are only useful for improving the performance of on-demand host and service checks. Scheduled checks help to ensure that host and service states are updated regularly, which may result in a greater possibility their results can be used as cached checks in the future.

For reference, on-demand host checks occur...

- When a service associated with the host changes state.
- As needed as part of the **host reachability** logic.

- As needed for **predictive host dependency checks**.

And on-demand service checks occur...

- As needed for **predictive service dependency checks**.

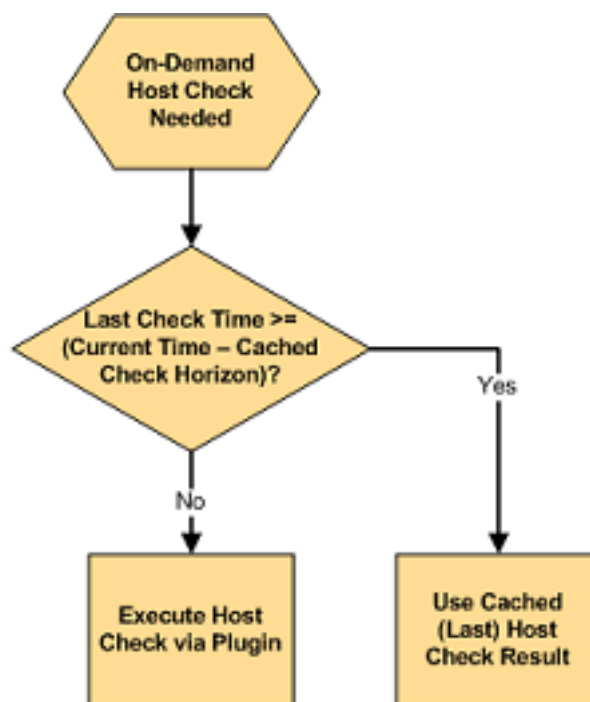
---

**Note**

Unless you make use of service dependencies, Nagios will not be able to use cached check results to improve the performance of service checks. Don't worry about that - its normal. Cached host checks are where the big performance improvements lie, and everyone should see a benefit there.

---

### 53.3 How Caching Works



When Nagios needs to perform an on-demand host or service check, it will make a determination as to whether it can use a cached check result or if it needs to perform an actual check by executing a plugin. It does this by checking to see if the last check of the host or service occurred within the last X minutes, where X is the cached host or service check horizon.

If the last check was performed within the timeframe specified by the cached check horizon variable, Nagios will use the result of the last host or service check and will not execute a new check. If the host or service has not yet been checked, or if the last check falls outside of the cached check horizon timeframe, Nagios will execute a new host or service check by running a plugin.

### 53.4 What This Really Means

Nagios performs on-demand checks because it needs to know the current state of a host or service at that exact moment in time. Utilizing cached checks allows you to make Nagios think that recent check results are 'good enough' for determining the current state of hosts, and that it doesn't need to go out and actually re-check the status of that host or service.

The cached check horizon tells Nagios how recent check results must be in order to reliably reflect the current state of a host or service. For example, with a cached check horizon of 30 seconds, you are telling Nagios that if a host's state was checked sometime in the last 30 seconds, the result of that check should still be considered the current state of the host.

---

The number of cached check results that Nagios can use versus the number of on-demand checks it has to actually execute can be considered the cached check ‘hit’ rate. By increasing the cached check horizon to equal the regular check interval of a host, you could theoretically achieve a cache hit rate of 100%. In that case all on-demand checks of that host would use cached check results. What a performance improvement! But is it really? Probably not.

The reliability of cached check result information decreases over time. Higher cache hit rates require that previous check results are considered ‘valid’ for longer periods of time. Things can change quickly in any network scenario, and there’s no guarantee that a server that was functioning properly 30 seconds ago isn’t on fire right now. There’s the tradeoff - reliability versus speed. If you have a large cached check horizon, you risk having unreliable check result values being used in the monitoring logic.

Nagios will eventually determine the correct state of all hosts and services, so even if cached check results prove to unreliably represent their true value, Nagios will only work with incorrect information for a short period of time. Even short periods of unreliable status information can prove to be a nuisance for admins, as they may receive notifications about problems which no longer exist.

There is no standard cached check horizon or cache hit rate that will be acceptable to every Nagios users. Some people will want a short horizon timeframe and a low cache hit rate, while others will want a larger horizon timeframe and a larger cache hit rate (with a low reliability rate). Some users may even want to disable cached checks altogether to obtain a 100% reliability rate. Testing different horizon timeframes, and their effect on the reliability of status information, is the only way that an individual user will find the ‘right’ value for their situation. More information on this is discussed below.

## 53.5 Configuration Variables

The following variables determine the timeframes in which a previous host or service check result may be used as a cached host or service check result:

- The `cached_host_check_horizon` variable controls cached host checks.
- The `cached_service_check_horizon` variable controls cached service checks.

## 53.6 Optimizing Cache Effectiveness

In order to make the most effective use of cached checks, you should:

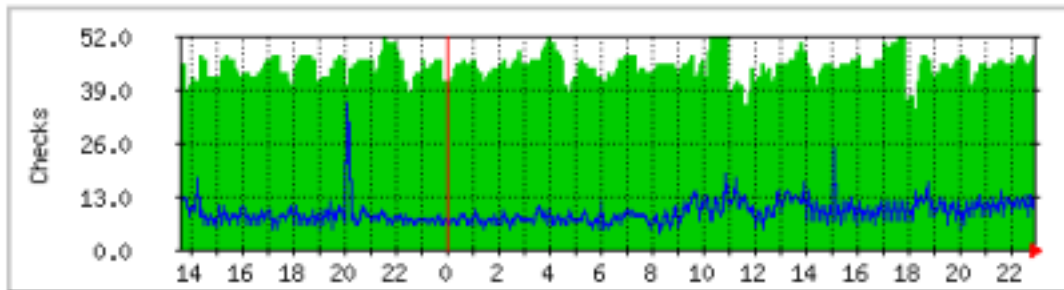
- Schedule regular checks of your hosts
- Use MRTG to graph statistics for 1) on-demand checks and 2) cached checks
- Adjust cached check horizon variables to fit your needs

You can schedule regular checks of your hosts by specifying a value greater than 0 for `check_interval` option in your **host definitions**. If you do this, make sure that you set the `max_check_attempts` option to a value greater than 1, or it will cause a big performance hit. This potential performance hit is describe in detail [here](#).

---

## Active Host Checks

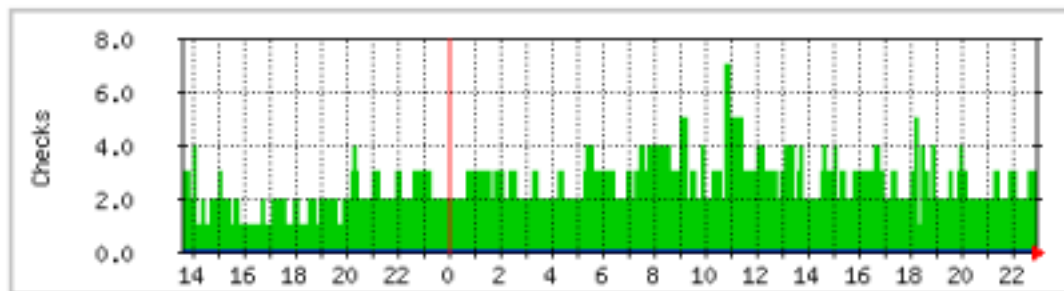
'Daily' Graph (5 Minute Average)



Max Scheduled Checks: 52.0    Average Scheduled Checks: 44.0    Current Scheduled Checks: 47.0  
Max On-Demand Checks: 35.0    Average On-Demand Checks: 9.0    Current On-Demand Checks: 14.0

## Cached Host Checks

'Daily' Graph (5 Minute Average)



Max Host Checks: 7.0    Average Host Checks: 2.0    Current Host Checks: 3.0

A good way to determine the proper value for the cached check horizon options is to compare how many on-demand checks Nagios has to actually run versus how many it can use cached values for. The [nagiosstats](#) utility can produce information on cached checks, which can then be [graphed with MRTG](#). Example MRTG graphs that show cached vs. actual on-demand checks are shown to the right.

The monitoring installation which produced the graphs above had:

- A total of 44 hosts, all of which were checked at regular intervals
- An average (regularly scheduled) host check interval of 5 minutes
- A [cached\\_host\\_check\\_horizon](#) of 15 seconds

The first MRTG graph shows how many regularly scheduled host checks compared to how many cached host checks have occurred. In this example, an average of 53 host checks occur every five minutes. 9 of these (17%) are on-demand checks.

The second MRTG graph shows how many cached host checks have occurred over time. In this example an average of 2 cached host checks occurs every five minutes.

Remember, cached checks are only available for on-demand checks. Based on the 5 minute averages from the graphs, we see that Nagios is able to use cached host check results every 2 out of 9 times an on-demand check has to be run. That may not seem much, but these graphs represent a small monitoring environment. Consider that 2 out of 9 is 22% and you can start to see how this could significantly help improve host check performance in large environments. That percentage could be higher if the cached host check horizon variable value was increased, but that would reduce the reliability of the cached host state information.

Once you've had a few hours or days worth of MRTG graphs, you should see how many host and service checks were done by executing plugins versus those that used cached check results. Use that information to adjust the cached check horizon variables

appropriately for your situation. Continue to monitor the MRTG graphs over time to see how changing the horizon variables affected cached check statistics. Rinse and repeat as necessary.



## Chapter 54

# Passive Host State Translation

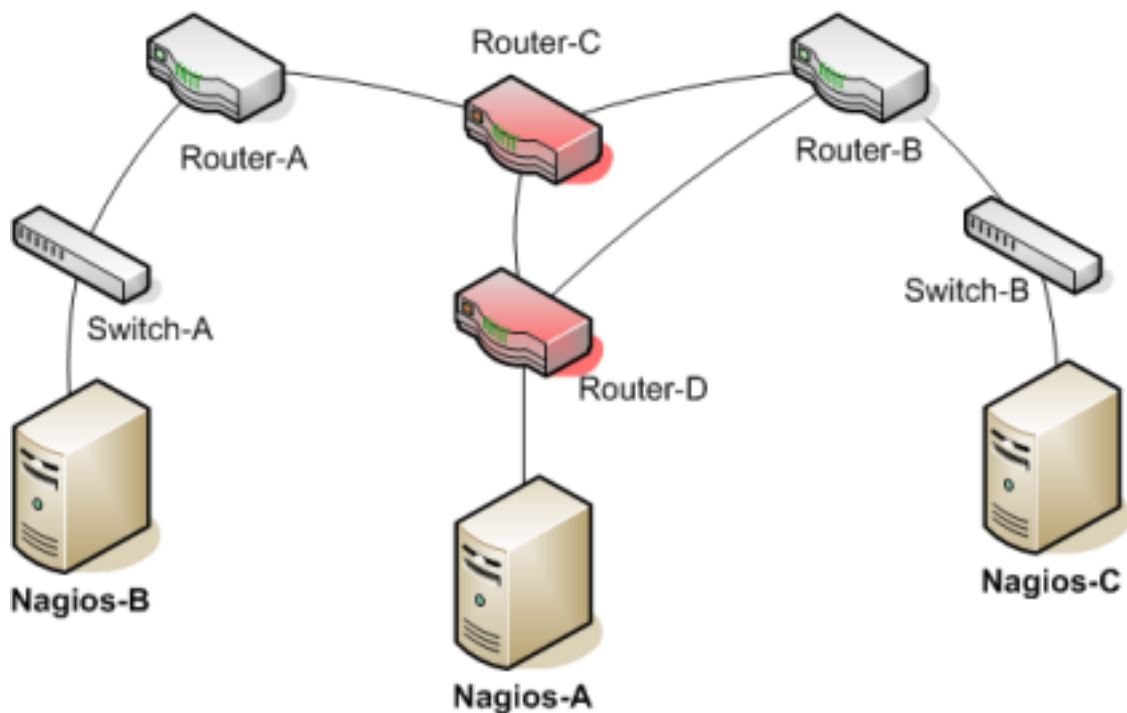
### 54.1 Introduction

When Nagios receives passive host checks from remote sources (i.e other Nagios instances in distributed or failover setups), the host state reported by the remote source may not accurately reflect the state of the host from Nagios' view. As distributed and failover monitoring installations are fairly common, it is important to provide a mechanism for ensuring accurate host states between different instances of Nagios.

### 54.2 Different World Views

The image below shows a simplified view of a failover monitoring setup.

- *Nagios-A* is the primary monitoring server, and is actively monitoring all switches and routers.
- *Nagios-B* and *Nagios-C* are backup monitoring servers, and are receiving passive check results from *Nagios-A*
- Both *Router-C* and *Router-D* have suffered failures and are offline.



What states are *Router-C* and *Router-D* currently in? The answer depends on which Nagios instance you ask.

- *Nagios-A* sees *Router-D* as DOWN and *Router-C* as UNREACHABLE
- *Nagios-B* should see *Router-C* as DOWN and *Router-D* as UNREACHABLE
- *Nagios-C* should see both routers as being DOWN.

Each Nagios instance has a different view of the network. The backup monitoring servers should not blindly accept passive host states from the primary monitoring server, or they will have incorrect information on the current state of the network.

Without translating passive host check results from the primary monitoring server (*Nagios-A*), *Nagios-C* would see *Router-D* as UNREACHABLE, when it is really DOWN based on its viewpoint. Similarly, the DOWN/UNREACHABLE states (from the viewpoint of *Nagios-A*) for *Router-C* and *Router-D* should be flipped from the viewpoint of *Nagios-B*.

---

**Note**

There may be some situations where you do not want Nagios to translate DOWN/UNREACHABLE states from remote sources to their 'correct' state from the viewpoint of the local Nagios instance. For example, in distributed monitoring environments you may want the central Nagios instance to know how distributed instances see their respective portions of the network.

---

## 54.3 Enabling State Translation

By default, Nagios will not automatically translate DOWN/UNREACHABLE states from passive check results. You will need to enable this feature if you need and want it.

The automatic translation of passive host check states is controlled by the `translate_passive_host_checks` variable. Enable it and Nagios will automatically translate DOWN and UNREACHABLE states from remote sources to their correct state for the local instance of Nagios.

## Chapter 55

# Service and Host Check Scheduling

### 55.1    **TODO**

This documentation is being rewritten for Nagios 3. Stay tuned for more information in a later beta release...

## Chapter 56

# Custom CGI Headers and Footers

### 56.1 Introduction

If you're doing custom installs of Nagios for clients, you may want to have a custom header and/or footer displayed in the output of the **CGIs**. This is particularly useful for displaying support contact information, etc. to the end user.

It is important to note that, unless they are executable, custom header and footer files are not pre-processed in any way before they are displayed. The contents of the header and footer include files are simply read and displayed in the CGI output. That means they can only contain information a web browser can understand (HTML, JavaScript, etc.).

If the custom header and footer files are executable, then the files are executed and their output returned to the user, so they should output valid HTML. Using this you can run your own custom designed CGI to insert data into the nagios display. This has been used to insert graphs from rrdtool using ddraw and command menus into the nagios display pane. The executable customer header and footer files are run with the same CGI environment as the main nagios CGI, so your files can parse the query information, authenticated user information, etc. to produce appropriate output.

### 56.2 How Does It Work?

You can include custom headers and footers in the output of the CGIs by dropping some appropriately named HTML files in the `ssi/` subdirectory of the Nagios HTML directory (i.e. `/usr/local/nagios/share/ssi`).

Custom headers are included immediately after the `<BODY>>` tag in the CGI output, while custom footers are included immediately before the closing `</BODY>` tag.

There are two types of customer headers and footers:

- Global headers/footers. These files should be named `common-header.ssi` and `common-footer.ssi`, respectively. If these files exist, they will be included in the output of all CGIs.
- CGI-specific headers/footers. These files should be named in the format `CGINAME-header.ssi` and `CGINAME-footer.ssi`, where `CGINAME` is the physical name of the CGI without the `.cgi` extension. For example, the header and footer files for the **alert summary CGI** (`summary.cgi`) would be named `summary-header.ssi` and `summary-footer.ssi`, respectively.

You are not required to use any custom headers or footers. You can use only a global header if you wish. You can use only CGI-specific headers and a global footer if you wish. Whatever you want. Really.

---



```

~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
 ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
 ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
 ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
 ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~hosttemplate1
 ~ ~ ~ ~ ~ ~ ~ }

 ~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
 ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~3
 ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ hosttemplate1
 ~ ~ ~ ~ ~ ~ ~ }

```

You'll note that the definition for host *bighost1* has been defined as having *hosttemplate1* as its template name. The definition for host *bighost2* is using the definition of *bighost1* as its template object. Once Nagios processes this data, the resulting definition of host *bighost2* would be equivalent to this definition:

```

~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
 ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
 ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
 ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~3
 ~ ~ ~ ~ ~ ~ ~ }

```

You can see that the `check_command` and `notification_options` variables were inherited from the template object (where host *bighost1* was defined). However, the `host_name` and `max_check_attempts` variables were not inherited from the template object because they were defined locally. Remember, locally defined variables override variables that would normally be inherited from a template object. That should be a fairly easy concept to understand.

---

#### Tip

If you would like local string variables to be appended to inherited string values, you can do so. Read more about how to accomplish this [below](#).

---

## 57.4 Inheritance Chaining

Objects can inherit properties/variables from multiple levels of template objects. Take the following example:

```

~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
 ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
 ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
 ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
 ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~hosttemplate1
 ~ ~ ~ ~ ~ ~ ~ }

 ~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
 ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~3
 ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ hosttemplate1
 ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~hosttemplate2
 ~ ~ ~ ~ ~ ~ ~ }

 ~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost3
 ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ hosttemplate2
 ~ ~ ~ ~ ~ ~ ~ }

```

You'll notice that the definition of host *bighost3* inherits variables from the definition of host *bighost2*, which in turn inherits variables from the definition of host *bighost1*. Once Nagios processes this configuration data, the resulting host definitions are equivalent to the following:

```
~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~3
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost3
~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~3
~ ~ ~ ~ ~ ~ ~ ~ }
```

There is no inherent limit on how 'deep' inheritance can go, but you'll probably want to limit yourself to at most a few levels in order to maintain sanity.

## 57.5 Using Incomplete Object Definitions as Templates

It is possible to use incomplete object definitions as templates for use by other object definitions. By "incomplete" definition, I mean that all required variables in the object have not been supplied in the object definition. It may sound odd to use incomplete definitions as templates, but it is in fact recommended that you use them. Why? Well, they can serve as a set of defaults for use in all other object definitions. Take the following example:

```
~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
~ ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~ ~generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ register ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~0
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
~ ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ ~ generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ ~ 192.168.1.4
~ ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ ~ generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ }
```

Notice that the first host definition is incomplete because it is missing the required `host_name` variable. We don't need to supply a host name because we just want to use this definition as a generic host template. In order to prevent this definition from being registered with Nagios as a normal host, we set the `register` variable to 0.

The definitions of hosts *bighost1* and *bighost2* inherit their values from the generic host definition. The only variable we've chosen to override is the address variable. This means that both hosts will have the exact same properties, except for their `host_name` and `address` variables. Once Nagios processes the config data in the example, the resulting host definitions would be equivalent to specifying the following:

```
~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
 ~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
 ~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
 ~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
 ~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
 ~ ~ ~ ~ ~ ~ ~ ~ }

 ~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost2
 ~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ 192.168.1.4
 ~ ~ ~ ~ ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ check-host-alive
 ~ ~ ~ ~ ~ ~ ~ ~ notification_options ~ ~d,u,r
 ~ ~ ~ ~ ~ ~ ~ ~ max_check_attempts ~ ~ ~5
 ~ ~ ~ ~ ~ ~ ~ ~ }
```

At the very least, using a template definition for default variables will save you a lot of typing. It'll also save you a lot of headaches later if you want to change the default values of variables for a large number of hosts.

## 57.6 Custom Object Variables

Any **custom object variables** that you define in your host, service, or contact definition templates will be inherited just like other standard variables. Take the following example:

```
~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ ~ _customvar1 ~ ~ ~ ~ ~ somevalue ~; <-- Custom host variable
 ~ ~ ~ ~ ~ ~ ~ ~ _snmp_community ~ ~ ~ ~ ~ public ~; <-- Custom host variable
 ~ ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~ ~generichosttemplate
 ~ ~ ~ ~ ~ ~ ~ ~ register ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~0
 ~ ~ ~ ~ ~ ~ ~ ~ }

 ~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
 ~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
 ~ ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ ~ generichosttemplate
 ~ ~ ~ ~ ~ ~ ~ ~ }
```

The host *bighost1* will inherit the custom host variables `_customvar1` and `_snmp_community`, as well as their respective values, from the *generichosttemplate* definition. The effective result is a definition for *bighost1* that looks like this:

```
~ ~ ~ ~ define host{
 ~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ bighost1
 ~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
 ~ ~ ~ ~ ~ ~ ~ ~ _customvar1 ~ ~ ~ ~ ~ somevalue
 ~ ~ ~ ~ ~ ~ ~ ~ _snmp_community ~ ~ ~ ~ ~ public
 ~ ~ ~ ~ ~ ~ ~ ~ }
```

## 57.7 Cancelling Inheritance of String Values

In some cases you may not want your host, service, or contact definitions to inherit values of string variables from the templates they reference. If this is the case, you can specify **'null'** (without quotes) as the value of the variable that you do not want to inherit. Take the following example:



```

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ event_handler ~ ~ ~ ~ ~ my-event-handler-command
~ ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~ ~generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ register ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~0
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ bighost1
~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
~ ~ ~ ~ ~ ~ ~ ~ event_handler ~ null
~ ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ ~ generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ }

```

In this case, the host *bighost1* will not inherit the value of the `event_handler` variable that is defined in the *generichosttemplate*. The resulting effective definition of *bighost1* is the following:

```

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ bighost1
~ ~ ~ ~ ~ ~ ~ ~ address ~ ~ ~ ~ ~ ~ ~ ~ 192.168.1.3
~ ~ ~ ~ ~ ~ ~ ~ }

```

## 57.8 Additive Inheritance of String Values

Nagios gives preference to local variables instead of values inherited from templates. In most cases local variable values override those that are defined in templates. In some cases it makes sense to allow Nagios to use the values of inherited and local variables together.

This "additive inheritance" can be accomplished by prepending the local variable value with a plus sign (+). This feature is only available for standard (non-custom) variables that contain string values. Take the following example:

```

define host{
~ ~ ~ ~ ~ ~ ~ ~ hostgroups ~ ~ ~ ~ ~ ~ ~ ~ ~all-servers
~ ~ ~ ~ ~ ~ ~ ~ name ~ ~ ~ ~ ~ ~ ~ ~ ~generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ register ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~0
~ ~ ~ ~ ~ ~ ~ ~ }

~ ~ ~ ~ define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ linuxserver1
~ ~ ~ ~ ~ ~ ~ ~ hostgroups ~ ~ ~ ~ ~ ~ ~ ~ ~+linux-servers,web-servers
~ ~ ~ ~ ~ ~ ~ ~ use ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~generichosttemplate
~ ~ ~ ~ ~ ~ ~ ~ }

```

In this case, the host *linuxserver1* will append the value of its local `hostgroups` variable to that from *generichosttemplate*. The resulting effective definition of *linuxserver1* is the following:

```

define host{
~ ~ ~ ~ ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ linuxserver1
~ ~ ~ ~ ~ ~ ~ ~ hostgroups ~ ~ ~ ~ ~ ~ ~ ~ ~all-servers,linux-servers,web-servers
~ ~ ~ ~ ~ ~ ~ ~ }

```

## 57.9 Implied Inheritance

Normally you have to either explicitly specify the value of a required variable in an object definition or inherit it from a template. There are a few exceptions to this rule, where Nagios will assume that you want to use a value that instead comes from a related object. For example, the values of some service variables will be copied from the host the service is associated with if you don't otherwise specify them.

The following table lists the object variables that will be implicitly inherited from related objects if you don't explicitly specify their value in your object definition or inherit them from a template.

| Object Type                | Object Variable              | Implied Source                                                    |
|----------------------------|------------------------------|-------------------------------------------------------------------|
| <b>Services</b>            | <i>contact_groups</i>        | <i>contact_groups</i> in the associated host definition           |
|                            | <i>notification_interval</i> | <i>notification_interval</i> in the associated host definition    |
|                            | <i>notification_period</i>   | <i>notification_period</i> in the associated host definition      |
| <b>Host Escalations</b>    | <i>contact_groups</i>        | <i>contact_groups</i> in the associated host definition           |
|                            | <i>notification_interval</i> | <i>notification_interval</i> in the associated host definition    |
|                            | <i>escalation_period</i>     | <i>notification_period</i> in the associated host definition      |
| <b>Service Escalations</b> | <i>contact_groups</i>        | <i>contact_groups</i> in the associated service definition        |
|                            | <i>notification_interval</i> | <i>notification_interval</i> in the associated service definition |
|                            | <i>escalation_period</i>     | <i>notification_period</i> in the associated service definition   |

## 57.10 Implied/Additive Inheritance in Escalations

Service and host escalation definitions can make use of a special rule that combines the features of implied and additive inheritance. If escalations 1) do not inherit the values of their `contact_groups` or `contacts` directives from another escalation template and 2) their `contact_groups` or `contacts` directives begin with a plus sign (+), then the values of their corresponding host or service definition's `contact_groups` or `contacts` directives will be used in the additive inheritance logic.

Confused? Here's an example:

```
define host{
 ~ ~ ~ ~ name ~ ~ ~ ~ ~linux-server
 ~ ~ ~ ~ contact_groups ~linux-admins
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }

define hostescalation{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~linux-server
 ~ ~ ~ ~ contact_groups ~+management
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```

This is a much simpler equivalent to:

```
define hostescalation{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~linux-server
 ~ ~ ~ ~ contact_groups ~linux-admins,management
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```



inheritance sources can themselves inherit variables/values from one or more other sources, it can get tricky to figure out what variable/value pairs take precedence.

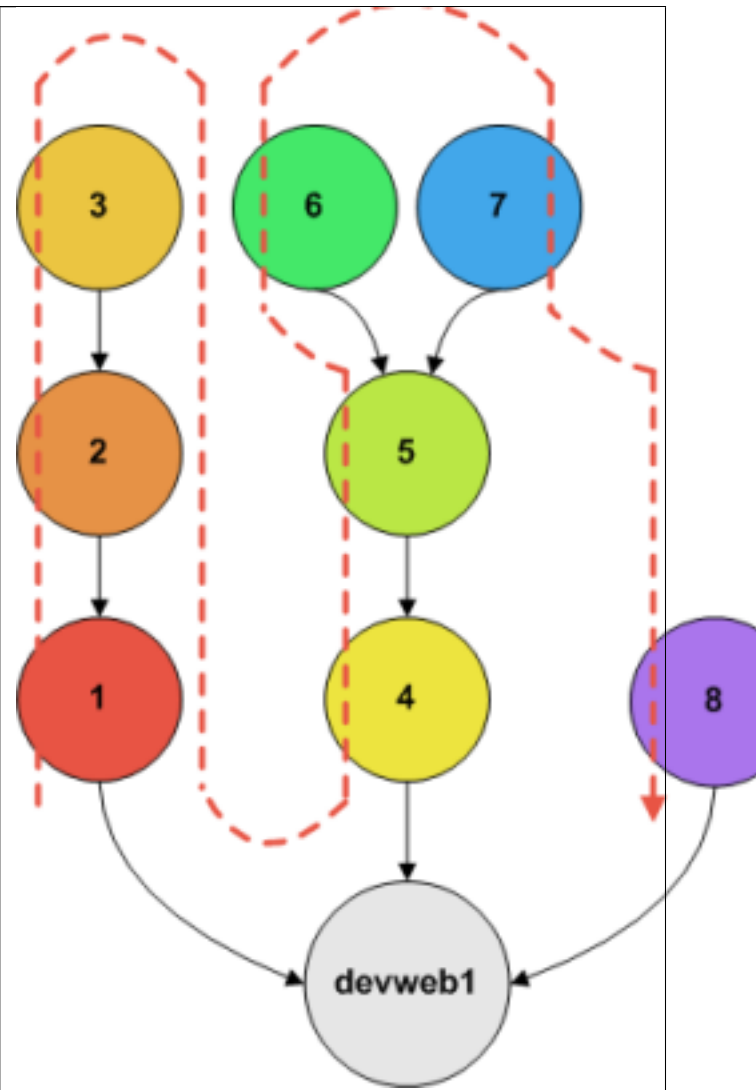
Consider the following host definition that references three templates:

# Development web server

```
define host{
 ~ ~ ~ ~ use ~ ~ ~ ~1, 4, 8
 ~ ~ ~ ~ host_name ~devweb1
 ...
 ~ ~ ~ ~ }
```

If some of those referenced templates themselves inherit variables/values from one or more other templates, the precedence rules are shown to the right.

Testing, trial, and error will help you better understand exactly how things work in complex inheritance situations like this. :-)



## Chapter 58

# Time-Saving Tricks For Object Definitions

## **Abstract**

or..."How To Preserve Your Sanity"

## 58.1 Introduction

This documentation attempts to explain how you can exploit the (somewhat) hidden features of **template-based object definitions** to save your sanity. How so, you ask? Several types of objects allow you to specify multiple host names and/or hostgroup names in definitions, allowing you to "copy" the object definition to multiple hosts or services. I'll cover each type of object that supports these features separately. For starters, the object types which support this time-saving feature are as follows:

- **Services**
- **Service escalations**
- **Service dependencies**
- **Host escalations**
- **Host dependencies**
- **Hostgroups**

Object types that are not listed above (i.e. timeperiods, commands, etc.) do not support the features I'm about to describe.

## 58.2 Regular Expression Matching

The examples I give below use 'standard' matching of object names. If you wish, you can enable regular expression matching for object names by using the **use\_regexp\_matching** config option. By default, regular expression matching will only be used in object names that contain \*, ?, +, or \.. If you want regular expression matching to be used on all object names, enable the **use\_true\_regexp\_matching** config option. Regular expressions can be used in any of the fields used in the examples below (host names, hostgroup names, service names, and servicegroup names).

---

### Note

Be careful when enabling regular expression matching - you may have to change your config file, since some directives that you might not want to be interpreted as a regular expression just might be ! Any problems should become evident once you verify your configuration.

---

## 58.3 Service Definitions

### 58.3.1 Multiple Hosts:

If you want to create identical **services** that are assigned to multiple hosts, you can specify multiple hosts in the `host_name` directive. The definition below would create a service called **SOMESERVICE** on hosts **HOST1** through **HOSTN**. All the instances of the **SOMESERVICE** service would be identical (i.e. have the same check command, max check attempts, notification period, etc.).

```
define service{
 host_name HOST1,HOST2,HOST3,...,HOSTN
 service_description SOMESERVICE
 other service directives ...
}
```

### 58.3.2 All Hosts In Multiple Hostgroups:

If you want to create identical services that are assigned to all hosts in one or more hostgroups, you can do so by creating a single service definition. How ? The `hostgroup_name` directive allows you to specify the name of one or more hostgroups that the service should be created for. The definition below would create a service called `SOMESERVICE` on all hosts that are members of hostgroups `HOSTGROUP1` through `HOSTGROUPN`. All the instances of the `SOMESERVICE` service would be identical (i.e. have the same check command, max check attempts, notification period, etc.).

```
define service{
 hostgroup_name HOSTGROUP1,HOSTGROUP2,...,HOSTGROUPN
 service_description SOMESERVICE
 other service directives ...
}
```

### 58.3.3 All Hosts:

If you want to create identical services that are assigned to all hosts that are defined in your configuration files, you can use a wildcard in the `host_name` directive. The definition below would create a service called `SOMESERVICE` on all hosts that are defined in your configuration files. All the instances of the `SOMESERVICE` service would be identical (i.e. have the same check command, max check attempts, notification period, etc.).

```
define service{
 host_name *
 service_description SOMESERVICE
 other service directives ...
}
```

### 58.3.4 Excluding Hosts:

If you want to create identical services on numerous hosts or hostgroups, but would like to exclude some hosts from the definition, this can be accomplished by preceding the host or hostgroup with a `!` symbol.

```
define service{
 host_name HOST1,HOST2,!HOST3,!HOST4,...,HOSTN
 hostgroup_name HOSTGROUP1,HOSTGROUP2,!HOSTGROUP3,!HOSTGROUP4,...,HOSTGROUPN
 service_description SOMESERVICE
 other service directives ...
}
```

## 58.4 Service Escalation Definitions

### 58.4.1 Multiple Hosts:

If you want to create **service escalations** for services of the same name/description that are assigned to multiple hosts, you can specify multiple hosts in the `host_name` directive. The definition below would create a service escalation for services called `SOMESERVICE` on hosts `HOST1` through `HOSTN`. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define serviceescalation{
 host_name HOST1,HOST2,HOST3,...,HOSTN
 service_description SOMESERVICE
 other escalation directives ...
}
```



### 58.4.2 All Hosts In Multiple Hostgroups:

If you want to create service escalations for services of the same name/description that are assigned to all hosts in in one or more hostgroups, you can do use the `hostgroup_name` directive. The definition below would create a service escalation for services called `SOMESERVICE` on all hosts that are members of hostgroups `HOSTGROUP1` through `HOSTGROUPN`. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define serviceescalation{
 hostgroup_name HOSTGROUP1,HOSTGROUP2,...,HOSTGROUPN
 service_description SOMESERVICE
 other_escalation_directives ...
}
```

### 58.4.3 All Hosts:

If you want to create identical service escalations for services of the same name/description that are assigned to all hosts that are defined in your configuration files, you can use a wildcard in the `host_name` directive. The definition below would create a service escalation for all services called `SOMESERVICE` on all hosts that are defined in your configuration files. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define serviceescalation{
 host_name *
 service_description SOMESERVICE
 other_escalation_directives ...
}
```

### 58.4.4 Excluding Hosts:

If you want to create identical services escalations for services on numerous hosts or hostgroups, but would like to exclude some hosts from the definition, this can be accomplished by preceding the host or hostgroup with a `!` symbol.

```
define serviceescalation{
 host_name HOST1,HOST2,!HOST3,!HOST4,...,HOSTN
 hostgroup_name HOSTGROUP1,HOSTGROUP2,!HOSTGROUP3,!HOSTGROUP4,...,HOSTGROUPN
 service_description SOMESERVICE
 other_escalation_directives ...
}
```

### 58.4.5 All Services On Same Host:

If you want to create **service escalations** for all services assigned to a particular host, you can use a wildcard in the `service_description` directive. The definition below would create a service escalation for all services on host `HOST1`. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

If you feel like being particularly adventurous, you can specify a wildcard in both the `host_name` and `service_description` directives. Doing so would create a service escalation for all services that you've defined in your configuration files.

```
define serviceescalation{
 host_name HOST1
 service_description *
 other_escalation_directives ...
}
```

### 58.4.6 Multiple Services On Same Host:

If you want to create **service escalations** for all multiple services assigned to a particular host, you can use a specify more than one service description in the `service_description` directive. The definition below would create a service escalation for services SERVICE1 through SERVICEN on host HOST1. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define serviceescalation{
 host_name HOST1
 service_description SERVICE1,SERVICE2,...,SERVICEN
 other_escalation_directives ...
}
```

### 58.4.7 All Services In Multiple Servicegroups:

If you want to create service escalations for all services that belong in one or more servicegroups, you can do use the `servicegroup_name` directive. The definition below would create service escalations for all services that are members of servicegroups SERVICEGROUP1 through SERVICEGROUPN. All the instances of the service escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define serviceescalation{
 servicegroup_name SERVICEGROUP1,SERVICEGROUP2,...,SERVICEGROUPN
 other_escalation_directives ...
}
```

## 58.5 Service Dependency Definitions

### 58.5.1 Multiple Hosts:

If you want to create **service dependencies** for services of the same name/description that are assigned to multiple hosts, you can specify multiple hosts in the `host_name` and or `dependent_host_name` directives. In the example below, service SERVICE2 on hosts HOST3 and HOST4 would be dependent on service SERVICE1 on hosts HOST1 and HOST2. All the instances of the service dependencies would be identical except for the host names (i.e. have the same notification failure criteria, etc.).

```
define servicedependency{
 host_name HOST1,HOST2
 service_description SERVICE1
 dependent_host_name HOST3,HOST4
 dependent_service_description SERVICE2
 other_dependency_directives ...
}
```

### 58.5.2 All Hosts In Multiple Hostgroups:

If you want to create service dependencies for services of the same name/description that are assigned to all hosts in in one or more hostgroups, you can do use the `hostgroup_name` and/or `dependent_hostgroup_name` directives. In the example below, service SERVICE2 on all hosts in hostgroups HOSTGROUP3 and HOSTGROUP4 would be dependent on service SERVICE1 on all hosts in hostgroups HOSTGROUP1 and HOSTGROUP2. Assuming there were five hosts in each of the hostgroups, this definition would be equivalent to creating 100 single service dependency definitions ! All the instances of the service dependency would be identical except for the host names (i.e. have the same notification failure criteria, etc.).

```
define servicedependency{
 hostgroup_name HOSTGROUP1,HOSTGROUP2
 service_description SERVICE1
 dependent_hostgroup_name HOSTGROUP3,HOSTGROUP4
 dependent_service_description SERVICE2
 other dependency directives ...
}
```

### 58.5.3 All Services On A Host:

If you want to create service dependencies for all services assigned to a particular host, you can use a wildcard in the `service_description` and/or `dependent_service_description` directives. In the example below, all services on host HOST2 would be dependent on all services on host HOST1. All the instances of the service dependencies would be identical (i.e. have the same notification failure criteria, etc.).

```
define servicedependency{
 host_name HOST1
 service_description *
 dependent_host_name HOST2
 dependent_service_description *
 other dependency directives ...
}
```

### 58.5.4 Multiple Services On A Host:

If you want to create service dependencies for multiple services assigned to a particular host, you can specify more than one service description in the `service_description` and/or `dependent_service_description` directives as follows:

```
define servicedependency{
 host_name HOST1
 service_description SERVICE1,SERVICE2,...,SERVICEN
 dependent_host_name HOST2
 dependent_service_description SERVICE1,SERVICE2,...,SERVICEN
 other dependency directives ...
}
```

### 58.5.5 All Services In Multiple Servicegroups:

If you want to create service dependencies for all services that belong in one or more servicegroups, you can do use the `servicegroup_name` and/or `dependent_servicegroup_name` directive as follows:

```
define servicedependency{
 servicegroup_name SERVICEGROUP1,SERVICEGROUP2,...,SERVICEGROUPN
 dependent_servicegroup_name SERVICEGROUP3,SERVICEGROUP4,...SERVICEGROUPN
 other dependency directives ...
}
```

### 58.5.6 Same Host Dependencies:

If you want to create service dependencies for multiple services that are dependent on services on the same host, leave the `dependent_host_name` and `dependent_hostgroup_name` directives empty. The example below assumes that hosts HOST1 and HOST2 have at least the following four services associated with them: SERVICE1, SERVICE2, SERVICE3, and SERVICE4. In this example, SERVICE3 and SERVICE4 on HOST1 will be dependent on both SERVICE1 and SERVICE2 on HOST1. Similiarly, SERVICE3 and SERVICE4 on HOST2 will be dependent on both SERVICE1 and SERVICE2 on HOST2.

```
define servicedependency{
 host_name HOST1,HOST2
 service_description SERVICE1,SERVICE2
 dependent_service_description SERVICE3,SERVICE4
 other dependency directives ...
}
```

## 58.6 Host Escalation Definitions

### 58.6.1 Multiple Hosts:

If you want to create **host escalations** for multiple hosts, you can specify multiple hosts in the `host_name` directive. The definition below would create a host escalation for hosts HOST1 through HOSTN. All the instances of the host escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define hostescalation{
 host_name HOST1,HOST2,HOST3,...,HOSTN
 other escalation directives ...
}
```

### 58.6.2 All Hosts In Multiple Hostgroups:

If you want to create host escalations for all hosts in in one or more hostgroups, you can do use the `hostgroup_name` directive. The definition below would create a host escalation on all hosts that are members of hostgroups HOSTGROUP1 through HOSTGROUPN. All the instances of the host escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define hostescalation{
 hostgroup_name HOSTGROUP1,HOSTGROUP2,...,HOSTGROUPN
 other escalation directives ...
}
```

### 58.6.3 All Hosts:

If you want to create identical host escalations for all hosts that are defined in your configuration files, you can use a wildcard in the `host_name` directive. The definition below would create a hosts escalation for all hosts that are defined in your configuration files. All the instances of the host escalation would be identical (i.e. have the same contact groups, notification interval, etc.).

```
define hostescalation{
 host_name *
 other escalation directives ...
}
```

### 58.6.4 Excluding Hosts:

If you want to create identical host escalations on numerous hosts or hostgroups, but would like to exclude some hosts from the definition, this can be accomplished by preceding the host or hostgroup with a `!` symbol.

```
define hostescalation{
 host_name HOST1,HOST2,!HOST3,!HOST4,...,HOSTN
 hostgroup_name HOSTGROUP1,HOSTGROUP2,!HOSTGROUP3,!HOSTGROUP4,...,HOSTGROUPN
 other escalation directives ...
}
```

## 58.7 Host Dependency Definitions

### 58.7.1 Multiple Hosts:

If you want to create **host dependencies** for multiple hosts, you can specify multiple hosts in the `host_name` and/or `dependent_host_name` directives. The definition below would be equivalent to creating six separate host dependencies. In the example above, hosts HOST3, HOST4 and HOST5 would be dependent upon both HOST1 and HOST2. All the instances of the host dependencies would be identical except for the host names (i.e. have the same notification failure criteria, etc.).

```
define hostdependency{
 host_name HOST1,HOST2
 dependent_host_name HOST3,HOST4,HOST5
 other dependency directives ...
}
```

### 58.7.2 All Hosts In Multiple Hostgroups:

If you want to create host escalations for all hosts in in one or more hostgroups, you can do use the `hostgroup_name` and `/or dependent_hostgroup_name` directives. In the example below, all hosts in hostgroups `HOSTGROUP3` and `HOSTGROUP4` would be dependent on all hosts in hostgroups `HOSTGROUP1` and `HOSTGROUP2`. All the instances of the host dependencies would be identical except for host names (i.e. have the same notification failure criteria, etc.).

```
define hostdependency{
 hostgroup_name HOSTGROUP1,HOSTGROUP2
 dependent_hostgroup_name HOSTGROUP3,HOSTGROUP4
 other dependency directives ...
}
```

## 58.8 Hostgroups

### 58.8.1 All Hosts:

If you want to create a hostgroup that has all hosts that are defined in your configuration files as members, you can use a wildcard in the `members` directive. The definition below would create a hostgroup called `HOSTGROUP1` that has all all hosts that are defined in your configuration files as members.

```
define hostgroup{
 hostgroup_name HOSTGROUP1
 members *
 other hostgroup directives ...
}
```

## **Part VII**

# **Security and Performance Tuning**

## Chapter 59

# Security Considerations

### 59.1 Introduction



This is intended to be a brief overview of some things you should keep in mind when installing Nagios, so as set it up in a secure manner.

Your monitoring box should be viewed as a backdoor into your other systems. In many cases, the Nagios server might be allowed access through firewalls in order to monitor remote servers. In most all cases, it is allowed to query those remote servers for various information. Monitoring servers are always given a certain level of trust in order to query remote systems. This presents a potential attacker with an attractive backdoor to your systems. An attacker might have an easier time getting into your other systems if they compromise the monitoring server first. This is particularly true if you are making use of shared SSH keys in order to monitor remote systems.

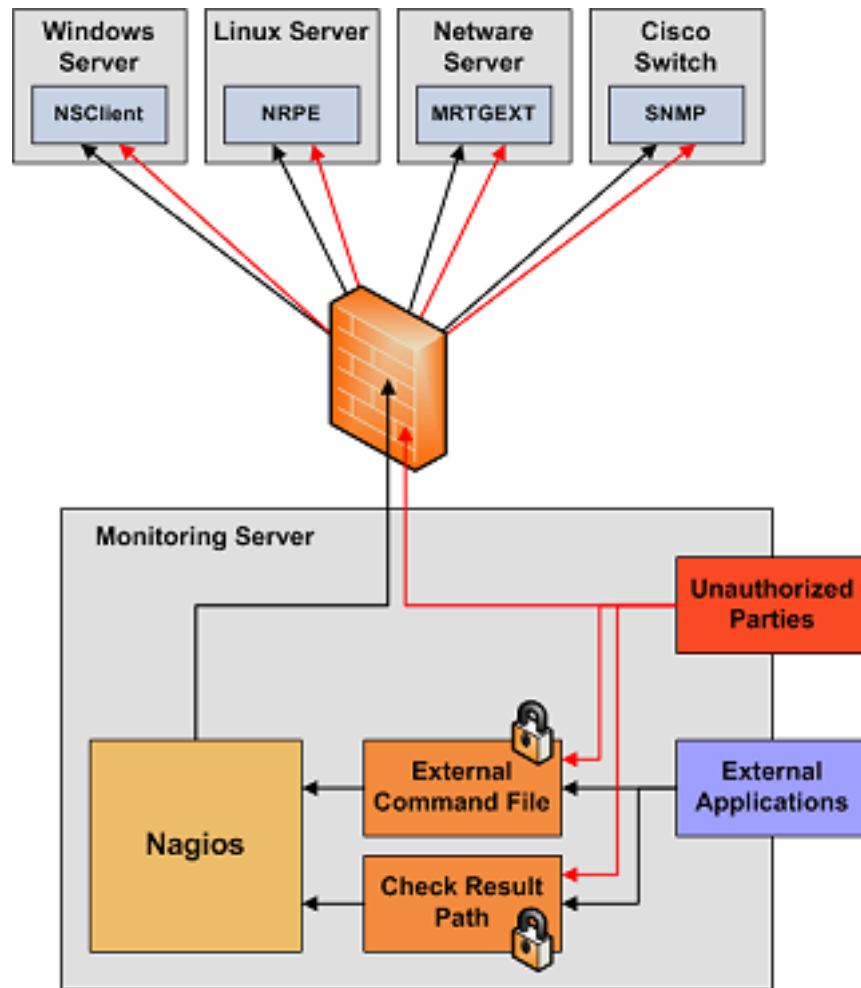
If an intruder has the ability to submit check results or external commands to the Nagios daemon, they have the potential to submit bogus monitoring data, drive you nuts you with bogus notifications, or cause event handler scripts to be triggered. If you have event handler scripts that restart services, cycle power, etc. this could be particularly problematic.

Another area of concern is the ability for intruders to sniff monitoring data (status information) as it comes across the wire. If communication channels are not encrypted, attackers can gain valuable information by watching your monitoring information. Take as an example the following situation: An attacker captures monitoring data on the wire over a period of time and analyzes the typical CPU and disk load usage of your systems, along with the number of users that are typically logged into them. The attacker is then able to determine the best time to compromise a system and use its resources (CPU, etc.) without being noticed.

Here are some tips to help ensure that you keep your systems secure when implementing a Nagios-based monitoring solution...

### 59.2 Best Practices

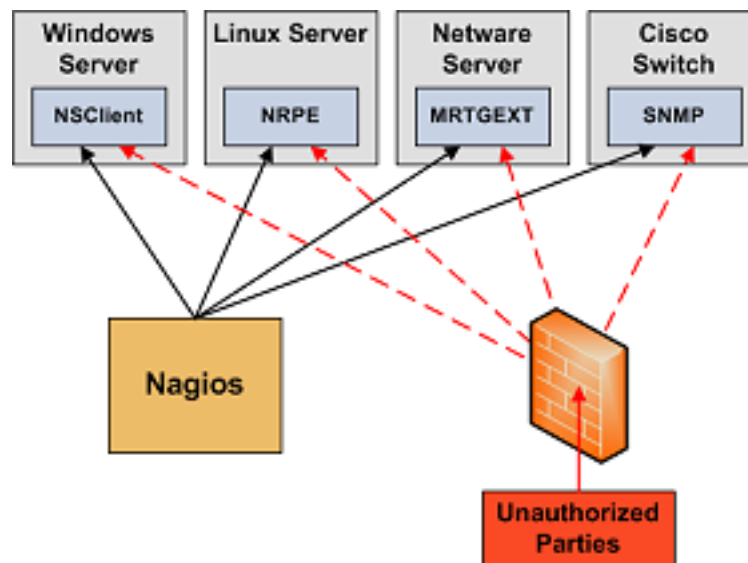
1. **Use a Dedicated Monitoring Box.** I would recommend that you install Nagios on a server that is dedicated to monitoring (and possibly other admin tasks). Protect your monitoring server as if it were one of the most important servers on your network. Keep running services to a minimum and lock down access to it via TCP wrappers, firewalls, etc. Since the Nagios server is allowed to talk to your servers and may be able to poke through your firewalls, allowing users access to your monitoring server can be a security risk. Remember, its always easier to gain root access through a system security hole if you have a local account on a box.



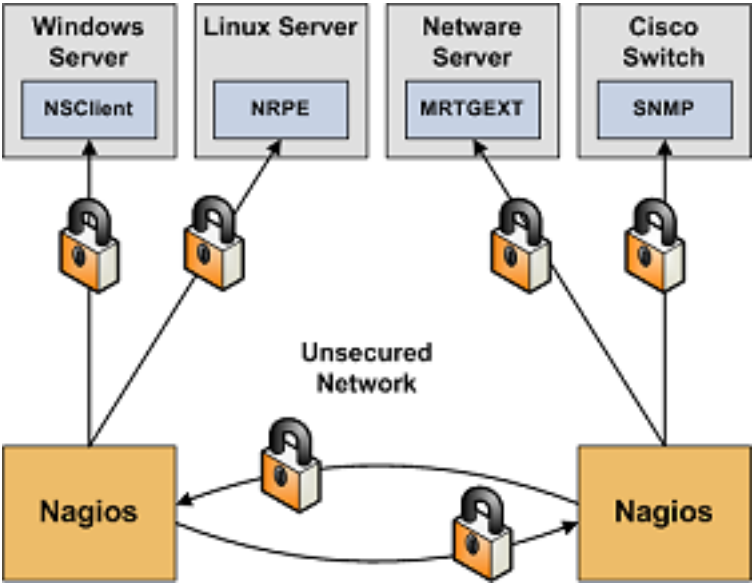
2. **Don't Run Nagios As Root.** Nagios doesn't need to run as root, so don't do it. You can tell Nagios to drop privileges after startup and run as another user/group by using the `nagios_user` and `nagios_group` directives in the main config file. If you need to execute event handlers or plugins which require root access, you might want to try using `sudo`.
3. **Lock Down The Check Result Directory.** Make sure that only the nagios user is able to read/write in the `check result path`. If users other than nagios (or root) are able to write to this directory, they could send fake host/service check results to the Nagios daemon. This could result in annoyances (bogus notifications) or security problems (event handlers being kicked off).
4. **Lock Down The External Command File.** If you enable `External Commands` external commands, make sure you set proper permissions on the `/usr/local/nagios/var/rw` directory. You only want the Nagios user (usually nagios) and the web server user (usually nobody, httpd, apache2, or www-data) to have permissions to write to the command file. If you've installed Nagios on a machine that is dedicated to monitoring and admin tasks and is not used for public accounts, that should be fine. If you've installed it on a public or multi-user machine (not recommended), allowing the web server user to have write access to the command file can be a security problem. After all, you don't want just any user on your system controlling Nagios through the external command file. In this case, I would suggest only granting write access on the command file to the nagios user and using something like `CGIWrap` to run the CGIs as the nagios user instead of nobody.
5. **Require Authentication In The CGIs.** I would strongly suggest requiring authentication for accessing the CGIs. Once you do that, read the documentation on the default rights that authenticated contacts have, and only authorize specific contacts for additional rights as necessary. Instructions on setting up authentication and configuring authorization rights can be found [Authentication and Authorization in The CGI](#) here. If you disable the CGI authentication features using the `use_authentication` directive in the CGI config file, the `command CGI` will refuse to write any commands to the `external command file`. After all, you don't want the world to be able to control Nagios do you?



6. **Implement Enhanced CGI Security Measures.** I would strongly suggest that you consider implementing enhanced security measures for the CGIs as described [here](#). These measures can help ensure that the username/password you use to access the Nagios web interface are not intercepted by third parties.
7. **Use Full Paths In Command Definitions.** When you define commands, make sure you specify the full path (not a relative one) to any scripts or binaries you're executing.
8. **Hide Sensitive Information With \$USERn\$ Macros.** The CGIs read the [Main Configuration File Options](#) main config file and [Object Configuration Overview](#) Object config file(s), so you don't want to keep any sensitive information (usernames, passwords, etc) in there. If you need to specify a username and/or password in a command definition use a \$USERn\$ [Understanding Macros and How They Work](#) macro to hide it. \$USERn\$ macros are defined in one or more [resource files](#). The CGIs will not attempt to read the contents of resource files, so you can set more restrictive permissions (600 or 660) on them. See the sample `resource.cfg` file in the base of the Nagios distribution for an example of how to define \$USERn\$ macros.
9. **Strip Dangerous Characters From Macros.** Use the [illegal\\_macro\\_output\\_chars](#) directive to strip dangerous characters from the \$HOSTOUTPUT\$, \$SERVICEOUTPUT\$, \$HOSTPERFDATA\$, and \$SERVICEPERFDATA\$ macros before they're used in notifications, etc. Dangerous characters can be anything that might be interpreted by the shell, thereby opening a security hole. An example of this is the presence of backtick ( ` ) characters in the \$HOSTOUTPUT\$, \$SERVICEOUTPUT\$, \$HOSTPERFDATA\$, and/or \$SERVICEPERFDATA\$ macros, which could allow an attacker to execute an arbitrary command as the nagios user (one good reason not to run Nagios as the root user).
10. **Secure Access to Remote Agents.** Make sure you lock down access to agents (NRPE, NSClient, SNMP, etc.) on remote systems using firewalls, access lists, etc. You don't want everyone to be able to query your systems for status information. This information could be used by an attacker to execute remote event handler scripts or to determine the best times to go unnoticed.



11. **Secure Communication Channels.** Make sure you encrypt communication channels between different Nagios installations and between your Nagios servers and your monitoring agents whenever possible. You don't want someone to be able to sniff status information going across your network. This information could be used by an attacker to determine the best times to go unnoticed.



## Chapter 60

# Enhanced CGI Security and Authentication

### 60.1 Introduction



This is intended to be an introduction for implementation of stronger authentication and server security focused around the CGI web interface.

There are many ways to enhance the security of your monitoring server and Nagios environment. This should not be taken as the end all approach to security. Instead, think of it as an introduction to some of the techniques you can use to tighten the security of your system. As always, you should do your research and use the best techniques available. Treat your monitoring server as it were the most important server in your network and you shall be rewarded.

### 60.2 Additional Techniques

- **Stronger Authentication using Digest Authentication.** If you have followed the [quickstart guides](#), chances are that you are using Apache's [Basic Authentication](#). Basic Authentication will send your username and password in "clear text" with every http request. Consider using a more secure method of authentication such as [Digest Authentication](#) which creates a MD5 Hash of your username and password to send with each request.
- **Forcing TLS/SSL for all Web Communication.** Apache provides [TLS/SSL](#) through the [mod\\_ssl](#) module. TLS/SSL provides a secure tunnel between the client and server that prevents eavesdropping and tampering using strong publickey/privatekey cryptography.
- **Locking Down Apache Using Access Controls.** Consider locking down access to the Nagios box to your IP address, IP address range, or IP subnet. If you require access outside your network you could use VPN or SSH Tunnels. This is a easy and strong to limit access to HTTP/HTTPS on your system.

#### 60.2.1 Implementing Digest Authentication

The implementation of Digest Authentication is simple. You will have to create the new type of password file using the ['htdigest'](#) tool, then modify the Apache configuration for nagios (typically `/etc/httpd/conf.d/nagios.conf`).

Create a new passwords file using the **'htdigest'** tool. The difference that you will notice if you are familiar with **'htpasswd'** tools is the requirement to supply a **'realm'** argument. Where **'realm'** in this case refers to the value of the **'AuthName'** directive in the Apache configuration.

```
linux:~ # htdigest -c /usr/local/nagios/etc/.digest_pw "Nagios Access" nagiosadmin
```

Next, edit the Apache configuration file for Nagios (typically `/etc/httpd/conf.d/nagios.conf`) using the following example.

```
BEGIN APACHE CONFIG SNIPPET - NAGIOS.CONF
ScriptAlias /nagios/cgi-bin "/usr/local/nagios/sbin"
<Directory "/usr/local/nagios/sbin">
 Options ExecCGI
 AllowOverride None
 Order allow,deny
 Allow from all
 AuthType Digest
 AuthName "Nagios Access"
 AuthUserFile /usr/local/nagios/etc/.digest_pw
 Require valid-user
</Directory>

Alias /nagios "/usr/local/nagios/share"
<Directory "/usr/local/nagios/share">
 Options None
 AllowOverride None
 Order allow,deny
 Allow from all
 AuthType Digest
 AuthName "Nagios Access"
 AuthUserFile /usr/local/nagios/etc/.digest_pw
 Require valid-user
</Directory>
END APACHE CONFIG SNIPPETS
```

Then, restart the Apache service so the new settings can take effect.

```
linux:~ # /etc/init.d/httpd restart
```

## 60.2.2 Implementing Forced TLS/SSL

Make sure you've installed Apache and OpenSSL. By default you should have **mod\_ssl** support if you are still having trouble you may find help reading Apache's [TLS/SSL Encryption Documentation](#).

Next, verify that TLS/SSL support is working by visiting your Nagios Web Interface using HTTPS (`https://your.domain/nagios`). If it is working you can continue on to the next steps that will force using HTTPS and block all HTTP requests for the Nagios Web Interface. If you are having trouble visit Apache's [TLS/SSL Encryption Documentation](#) and [Google](#) for troubleshooting your specific Apache installation. Next, edit the Apache configuration file for Nagios (typically `/etc/httpd/conf.d/nagios.conf`) by adding the **SSLRequireSSL** directive to both the **sbin** and **share** directories.

```
BEGIN APACHE CONFIG SNIPPET - NAGIOS.CONF
ScriptAlias /nagios/cgi-bin "/usr/local/nagios/sbin"
<Directory "/usr/local/nagios/sbin">
 ...
 SSLRequireSSL
 ...
</Directory>

Alias /nagios "/usr/local/nagios/share"
<Directory "/usr/local/nagios/share">
```

```
...
 SSLRequireSSL
...
</Directory>
END APACHE CONFIG SNIPPETS
```

Restart the Apache service so the new settings can take effect.

```
linux:~ # /etc/init.d/httpd restart
```

### 60.2.3 Implementing IP subnet lockdown

The following example will show how to lock down Nagios CGIs to a specific IP address, IP address range, or IP subnet using Apache's [access controls](#). Edit the Apache configuration file for Nagios (typically `/etc/httpd/conf.d/nagios.conf`) by using the Allow, Deny, and Order directives using the following as an example.

```
BEGIN APACHE CONFIG SNIPPET - NAGIOS.CONF
ScriptAlias /nagios/cgi-bin "/usr/local/nagios/sbin"
<Directory "/usr/local/nagios/sbin">
 ...
 AllowOverride None
 Order deny,allow
 Deny from all
 Allow from 127.0.0.1 10.0.0.25 # Allow single IP addresses
 Allow from 10.0.0.0/255.255.255.0 # Allow network/netmask pair
 Allow from 10.0.0.0/24 # Allow network/nnn CIDR spec
 ...
</Directory>

Alias /nagios "/usr/local/nagios/share"
<Directory "/usr/local/nagios/share">
 ...
 AllowOverride None
 Order deny,allow
 Deny from all
 Allow from 127.0.0.1 10.0.0.25 # Allow single IP addresses
 Allow from 10.0.0.0/255.255.255.0 # Allow network/netmask pair
 Allow from 10.0.0.0/24 # Allow network/nnn CIDR spec
 ...
</Directory>
END APACHE CONFIG SNIPPET
```

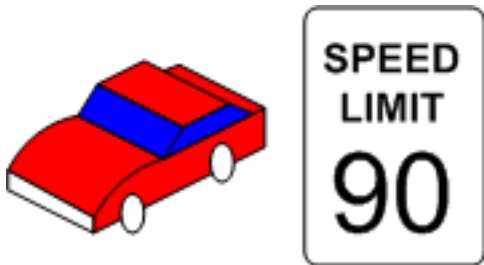
## 60.3 Important Notes

- **Digest Authentication sends data in the clear but not your username and password.**
- **Digest Authentication is not as universally supported as Basic Authentication.**
- **TLS/SSL has potential for ‘[man-in-the-middle attacks](#)’.** MITM attacks are vulnerable if an attacker is able to insert itself between the server and client such as in a Phishing attack, ISP monitoring, or corporate LAN firewall certificate resigning. So read up on certificate verification!
- **Apache access controls only protect the HTTP/HTTPS protocols.** Look into [IPtables](#) for strong system wide firewall control.
- **Most importantly, Security is a moving target so stay informed and do research!** Perhaps by listening to a Podcast such as "[Security Now!](#)".

## Chapter 61

# Tuning Nagios For Maximum Performance

### 61.1 Introduction



So you've finally got Nagios up and running and you want to know how you can tweak it a bit. Tuning Nagios to increase performance can be necessary when you start monitoring a large number (> 1,000) of hosts and services. Here are a few things to look at for optimizing Nagios...

### 61.2 Optimization Tips:

1. Graph performance statistics with MRTG. In order to keep track of how well your Nagios installation handles load over time and how your configuration changes affect it, you should be graphing several important statistics with MRTG. This is really, really, really useful when it comes to tuning the performance of a Nagios installation. Really. Information on how to do this can be found [Graphing Performance Info With MRTG](#)here.
2. Use large installation tweaks. Enabling the `use_large_installation_tweaks` option may provide you with better performance. Read more about what this option does [Large Installation Tweaks](#)here.
3. Disable environment macros. Macros are normally made available to check, notification, event handler, etc. commands as environment variables. This can be a problem in a large Nagios installation, as it consumes some additional memory and (more importantly) more CPU. If your scripts don't need to access the macros as environment variables (e.g. you pass all necessary macros on the command line), you don't need this feature. You can prevent macros from being made available as environment variables by using the `enable_environment_macros` option.
4. Check Result Reaper Frequency. The `check_result_reaper_frequency` variable determines how often Nagios should check for host and service check results that need to be processed. The maximum amount of time it can spend processing those results is determined by the max reaper time (see below). If your reaper frequency is too high (too infrequent), you might see high latencies for host and service checks.
5. Max Reaper Time. The `max_check_result_reaper_time` variables determines the maximum amount of time the Nagios daemon can spend processing the results of host and service checks before moving on to other things - like executing new host and service checks. Too high of a value can result in large latencies for your host and service checks. Too low of a value can have the same effect. If you're experiencing high latencies, adjust this variable and see what effect it has. Again, you should be [Graphing Performance Info With MRTG](#)graphing statistics in order to make this determination.

6. Adjust buffer slots. You may need to adjust the value of the `external_command_buffer_slots` option. Graphing buffer slot statistics with [Graphing Performance Info With MRTGMRTG](#) (see above) is critical in determining what values you should use for this option.
  7. Check service latencies to determine best value for maximum concurrent checks. Nagios can restrict the number of maximum concurrently executing service checks to the value you specify with the `max_concurrent_checks` option. This is good because it gives you some control over how much load Nagios will impose on your monitoring host, but it can also slow things down. If you are seeing high latency values (> 10 or 15 seconds) for the majority of your service checks (via the `extinfo` CGI), you are probably starving Nagios of the checks it needs. That's not Nagios's fault - it's yours. Under ideal conditions, all service checks would have a latency of 0, meaning they were executed at the exact time that they were scheduled to be executed. However, it is normal for some checks to have small latency values. I would recommend taking the minimum number of maximum concurrent checks reported when running Nagios with the `-s` command line argument and doubling it. Keep increasing it until the average check latency for your services is fairly low. More information on service check scheduling can be found [Service and Host Check Scheduling](#) here.
  8. Use passive checks when possible. The overhead needed to process the results of `Passive Checks` passive service checks is much lower than that of 'normal' active checks, so make use of that piece of info if you're monitoring a slew of services. It should be noted that passive service checks are only really useful if you have some external application doing some type of monitoring or reporting, so if you're having Nagios do all the work, this won't help things.
  9. Avoid using interpreted plugins. One thing that will significantly reduce the load on your monitoring host is the use of compiled (C/C++, etc.) plugins rather than interpreted script (Perl, etc) plugins. While Perl scripts and such are easy to write and work well, the fact that they are compiled/interpreted at every execution instance can significantly increase the load on your monitoring host if you have a lot of service checks. If you want to use Perl plugins, consider compiling them into true executables using `perlcc(1)` (a utility which is part of the standard Perl distribution) or compiling Nagios with an embedded Perl interpreter (see below).
  10. Use the embedded Perl interpreter. If you're using a lot of Perl scripts for service checks, etc., you will probably find that compiling the `embedded Perl interpreter` into the Nagios binary will speed things up.
  11. Optimize host check commands. If you're checking host states using the `check_ping` plugin you'll find that host checks will be performed much faster if you break up the checks. Instead of specifying a `max_attempts` value of 1 in the host definition and having the `check_ping` plugin send 10 ICMP packets to the host, it would be much faster to set the `max_attempts` value to 10 and only send out 1 ICMP packet each time. This is due to the fact that Nagios can often determine the status of a host after executing the plugin once, so you want to make the first check as fast as possible. This method does have its pitfalls in some situations (i.e. hosts that are slow to respond may be assumed to be down), but you'll see faster host checks if you use it. Another option would be to use a faster plugin (i.e. `check_fping`) as the `host_check_command` instead of `check_ping`.
  12. Schedule regular host checks. Scheduling regular checks of hosts can actually help performance in Nagios. This is due to the way the `Cached Checks` cached check logic works (see below). Prior to Nagios 3, regularly scheduled host checks used to result in a big performance hit. This is no longer the case, as host checks are run in parallel - just like service checks. To schedule regular checks of a host, set the `check_interval` directive in the `host definition` to something greater than 0.
  13. Enable cached host checks. Beginning in Nagios 3, on-demand host checks can benefit from caching. On-demand host checks are performed whenever Nagios detects a service state change. These on-demand checks are executed because Nagios wants to know if the host associated with the service changed state. By enabling cached host checks, you can optimize performance. In some cases, Nagios may be able to use the old/cached state of the host, rather than actually executing a host check command. This can speed things up and reduce load on monitoring server. In order for cached checks to be effective, you need to schedule regular checks of your hosts (see above). More information on cached checks can be found [Cached Checks](#) here.
  14. Don't use aggressive host checking. Unless you're having problems with Nagios recognizing host recoveries, I would recommend not enabling the `use_aggressive_host_checking` option. With this option turned off host checks will execute much faster, resulting in speedier processing of service check results. However, host recoveries can be missed under certain circumstances when this is turned off. For example, if a host recovers and all of the services associated with that host stay in non-OK states (and don't "wobble" between different non-OK states), Nagios may miss the fact that the host has recovered. A few people may need to enable this option, but the majority don't and I would recommend not using it unless you find it necessary...
-

- 
15. External command optimizations. If you're processing a lot of external commands (i.e. passive checks in a [Distributed Monitoring](#) distributed setup, you'll probably want to set the `command_check_interval` variable to -1. This will cause Nagios to check for external commands as often as possible. You should also consider increasing the number of available [external command buffer slots](#). Buffers slots are used to hold external commands that have been read from the [external command file](#) (by a separate thread) before they are processed by the Nagios daemon. If your Nagios daemon is receiving a lot of passive checks or external commands, you could end up in a situation where the buffers are always full. This results in child processes (external scripts, NSCA daemon, etc.) blocking when they attempt to write to the external command file. I would highly recommend that you graph external command buffer slot usage using MRTG and the `nagiosstats` utility as described [Graphing Performance Info With MRTG](#) here, so you understand the typical external command buffer usage of your Nagios installation.
16. Optimize hardware for maximum performance.

---

**Note**

Hardware performance shouldn't be an issue unless:

- (a) you're monitoring thousands of services
  - (b) you're doing a lot of post-processing of performance data, etc. Your system configuration and your hardware setup are going to directly affect how your operating system performs, so they'll affect how Nagios performs. The most common hardware optimization you can make is with your hard drives. CPU and memory speed are obviously factors that affect performance, but disk access is going to be your biggest bottleneck. Don't store plugins, the status log, etc on slow drives (i.e. old IDE drives or NFS mounts). If you've got them, use UltraSCSI drives or fast IDE drives. An important note for IDE/Linux users is that many Linux installations do not attempt to optimize disk access. If you don't change the disk access parameters (by using a utility like `hdparm`), you'll loose out on a lot of the speedy features of the new IDE drives.
-



## Chapter 62

# Fast Startup Options

### 62.1 Introduction

There are a few things you can do that can decrease the amount of time it take Nagios to startup (or restart). These speedups involve easing some of the burden involved in processing your configuration files.

Using these techniques is particularly useful when you have one or more of the following:

- Large configurations
- Complex configurations (heavy use of template features)
- Installations where frequent restarts are necessary

### 62.2 Background

Whenever Nagios starts/restarts it has to process your configuration files before it can get down to the business of monitoring. This configuration startup process involves a number of steps:

- Reading the config files
- Resolving template definitions
- "Recombobulating" your objects (my term for the various types of work that occurs)
- Duplicating object definitions
- Inheriting object properties
- Sorting your object definitions
- Verifying object relationship integrity
- Checking for circular paths
- and more...

Some of these steps can be quite time-consuming when you have large or complex configurations. Is there a way to speed any of these steps up? Yes!

---

Whoa! From 68 seconds to just 5 seconds? Yep, read on for how to do it.

## 62.4 Pre-Caching Object Configuration

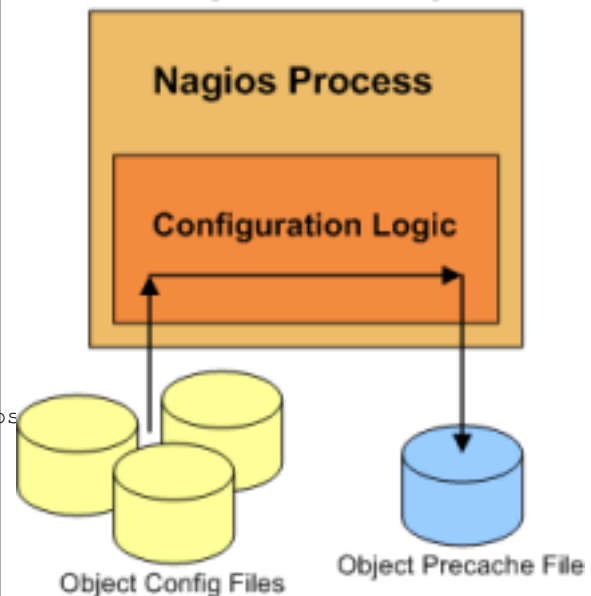
Nagios can spend quite a bit of time parsing your config files, especially if you make use of the template features such as inheritance, etc. In order to reduce the time it takes to parse your config, you can have Nagios pre-process and pre-cache your config files for future use.

When you run nagios with the `-p` command line option, Nagios will read your config files in, process them, and save them to a pre-cached object config file (specified by the `precached_object_file` directive). This pre-cached config file will contain pre-processed configuration entries that are easier/faster for Nagios to process in the future. You must use the `-p` command line option along with either the `-v` or `-s` command line options, as shown below. This ensures that your configuration is verified before the precached file is created.

```
linux:~ # <:b>/usr/local/nagios/bin/ ↵
nagios -pv /usr/local/nagios/etc/nagios
```

The size of your precached config file will most likely be significantly larger than the sum of the sizes of your object config files. This is normal and by design.

### Generating Cached Configuration



Once the precached object configuration file have been created, you can start Nagios and tell it to use the precached config file instead of your object config file(s) by using the `-u` command line option.

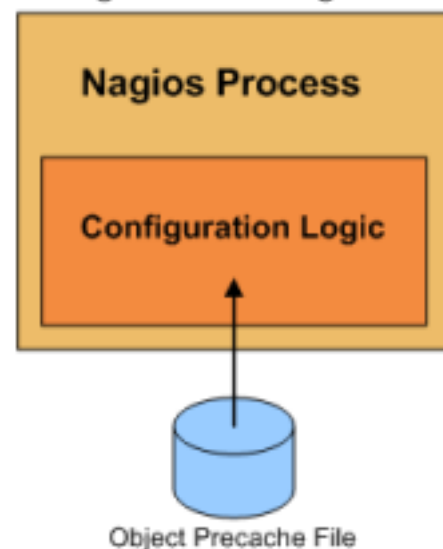
```
linux:~ # <:b>/usr/local/nagios/bin/ ↵
nagios -ud /usr/local/nagios/etc/nagios
```



#### Important

If you modify your configuration files, you will need to re-verify and re-cache your configuration files before restarting Nagios. If you don't re-generate the precached object file, Nagios will continue to use your old configuration because it is now reading from the precached file, rather than your source configuration files.

### Using Cached Configuration



## 62.5 Skipping Circular Path Tests

The second (and most time-intensive) portion of the configuration startup phase is the circular path check. In the example above, it took nearly a minute to perform this step of the configuration verification.

What is the circular path check and why does it take so long? The circular patch check is designed to ensure that you don't define any circular paths in your host, host dependency, or service dependency definitions. If a circular path existed in your config files, Nagios could end up in a deadlock situation. The most likely reason for the check taking so long is that I'm not using an efficient

algorithm. A much more efficient algorithm for detecting circular paths would be most welcomed. Hint: That means all you CompSci graduate students who have been emailing me about doing your thesis on Nagios can contribute some code back. :-)

If you want to skip the circular path check when Nagios starts, you can add the `-x` command line option like this:

```
linux:~ # /usr/local/nagios/bin/nagios -xd /usr/local/nagios/etc/nagios.cfg
```

**Important**

It is of utmost importance that you verify your configuration before starting/restarting Nagios when skipping circular path checks. Failure to do so could lead to deadlocks in the Nagios logic. You have been warned.

## 62.6 Putting It All Together

Follow these steps if you want to make use of potential speedups from pre-caching your configuration and skipping circular path checks.

1. Verify your configuration and create the precache file with the following command:

```
linux:~ # /usr/local/nagios/bin/nagios -vp /usr/local/nagios/etc/nagios.cfg
```

2. Stop Nagios if it is currently running.
3. Start Nagios like so to use the precached config file and skip circular path checks:

```
linux:~ # /usr/local/nagios/bin/nagios -uxd /usr/local/nagios/etc/nagios.cfg
```

4. When you modify your original configuration files in the future and need to restart Nagios to make those changes take place, repeat step 1 to re-verify your config and regenerate your cached config file. Once that is done you can restart Nagios through the web interface or by sending a SIGHUP signal. If you don't re-generate the precached object file, Nagios will continue to use your old configuration because it is now reading from the precached file, rather than your source configuration files.
5. That's it! Enjoy the increased startup speed.

## Chapter 63

# Large Installation Tweaks

### 63.1 Introduction

Users with large Nagios installations may benefit from the `use_large_installation_tweaks` configuration option. Enabling this option allows the Nagios daemon to take certain shortcuts which result in lower system load and better performance.

### 63.2 Effects

When you enable the `use_large_installation_tweaks` option in your main Nagios config file, several changes are made to the way the Nagios daemon operates:

1. No Summary Macros In Environment Variables - The `summary_macros` will not be available to you as environment variables. Calculating the values of these macros can be quite time-intensive in large configurations, so they are not available as environment variables when use this option. Summary macros will still be available as regular macros if you pass them to to your scripts as arguments.
  2. Different Memory Cleanup - Normally Nagios will free all allocated memory in child processes before they exit. This is probably best practice, but is likely unnecessary in most installations, as most OSes will take care of freeing allocated memory when processes exit. The OS tends to free allocated memory faster than can be done within Nagios itself, so Nagios won't attempt to free memory in child processes if you enable this option.
  3. Checks `fork()` Less - Normally Nagios will `fork()` twice when it executes host and service checks. This is done to (1) ensure a high level of resistance against plugins that go awry and segfault and (2) make the OS deal with cleaning up the grandchild process once it exits. The extra `fork()` is not really necessary, so it is skipped when you enable this option. As a result, Nagios will itself clean up child processes that exit (instead of leaving that job to the OS). This feature should result in significant load savings on your Nagios installation.
-

## Chapter 64

# Using The Nagiostats Utility

### 64.1 Introduction

A utility called **nagiostats** is included in the Nagios distribution. It is compiled and installed along with the main Nagios daemon. The **nagiostats** utility allows you to obtain various information about a running Nagios process that can be very helpful in **Tuning Nagios For Maximum Performance** tuning performance. You can obtain information either in human-readable or MRTG-compatible format.

### 64.2 Usage Information

You can run the **nagiostats** utility with the `--help` option to get usage information.

### 64.3 Human-Readable Output

To obtain human-readable information on the performance of a running Nagios process, run the **nagiostats** utility with the `-c` command line argument to specify your main configuration file location like such: `[nagios@lanman ~]# /usr/local/nagios`  
`-c /usr/local/nagios/etc/nagios.cfg`

```
Nagios Stats 3.0prealpha-05202006
Copyright (c) 2003-2007 Ethan Galstad (www.nagios.org)
Last Modified: 05-20-2006
License: GPL

CURRENT STATUS DATA

Status File: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ /usr/local/nagios/var/status.dat
Status File Age: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~0d 0h 0m 9s
Status File Version: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~3.0prealpha-05202006

Program Running Time: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 0d 5h 20m 39s
Nagios PID: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 10119
Used/High/Total Command Buffers: ~ ~ ~ ~0 / 0 / 64
Used/High/Total Check Result Buffers: ~ 0 / 7 / 512

Total Services: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 95
Services Checked: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 94
Services Scheduled: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 91
Services Actively Checked: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 94
Services Passively Checked: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ 1
```



## Chapter 65

# Graphing Performance Info With MRTG

### 65.1 Introduction

The [Using The Nagiosstats Utility](#) `nagiosstats` utility allows you to graph various Nagios performance statistics over time using [MRTG](#). This is important because it can help you:

- Ensure Nagios is operating efficiently
- Locate problem areas in the monitoring process
- Observe the performance impacts of changes in your Nagios configuration

### 65.2 Sample MRTG Configuration

Sample MRTG configuration file snippets for graphing various Nagios performance statistics can be found in the `mrtg.cfg` file located in the `sample-config/` subdirectory of the Nagios distribution. You can create graphs of other performance information if you'd like - the samples just provide you with a good starting point.

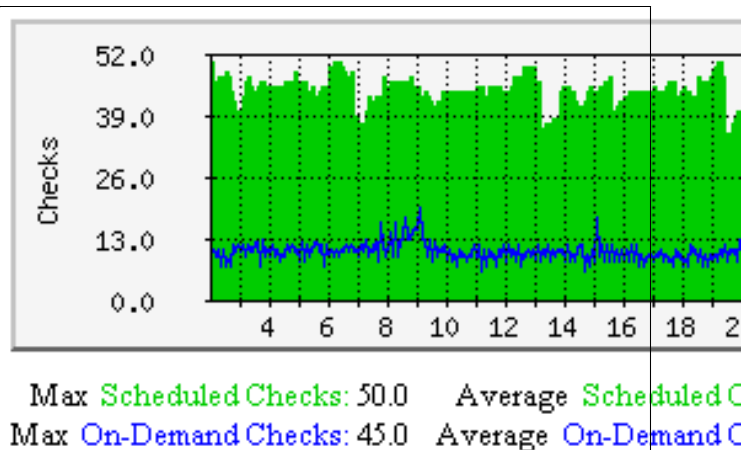
Once you copy these sample entries into your MRTG config file (`/etc/mrtg/mrtg.cfg`) you should have some new graphs the next time MRTG runs.

### 65.3 Example Graphs

I'll describe what a few of the sample MRTG graphs mean and what they can be used for...

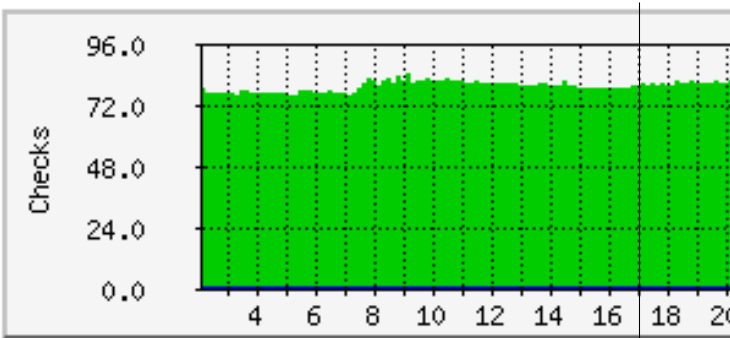
Active Host Checks - This graph shows how many active host checks (regularly scheduled and on-demand) have occurred over time. Useful for understanding:

- [Host Checks](#) Host checks
- [Read more](#) Predictive host dependency checks
- [Cached Checks](#) Cached checks

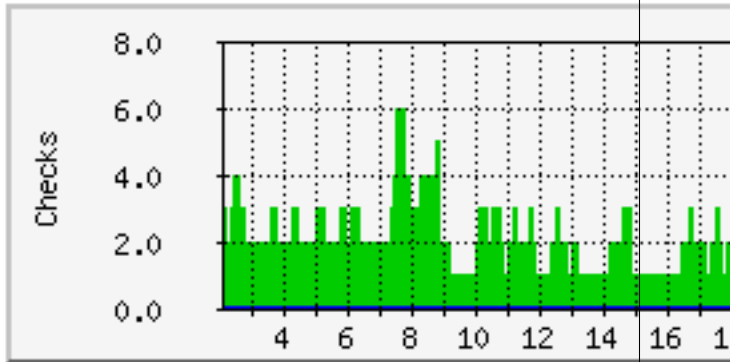




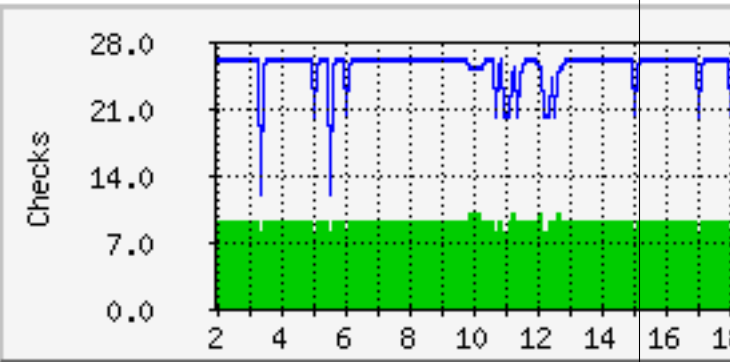
|                                                                                                                                                                                                                                                                                                                                                                       |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <p>Active Service Checks - This graph shows how may active service checks (regularly scheduled and on-demand) have occurred over time. Useful for understanding:</p> <ul style="list-style-type: none"><li>• <b>Service Checks</b>Service checks</li><li>• <b>Read more</b>Predictive service dependency checks</li><li>• <b>Cached Checks</b>Cached checks</li></ul> |  |
| <p>Cached Host and Service Checks - This graph shows how may cached host and service checks have occurred over time. Useful for understanding:</p> <ul style="list-style-type: none"><li>• <b>Cached Checks</b>Cached checks</li><li>• <b>Read more</b>Predictive host and service dependency checks</li></ul>                                                        |  |
| <p>Passive Host and Service Checks - This graph shows how may passive host and service checks have occurred over time. Useful for understanding:</p> <ul style="list-style-type: none"><li>• <b>Passive Checks</b>Passive checks</li></ul>                                                                                                                            |  |



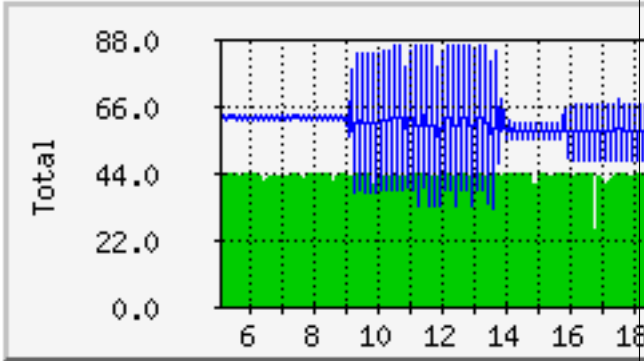
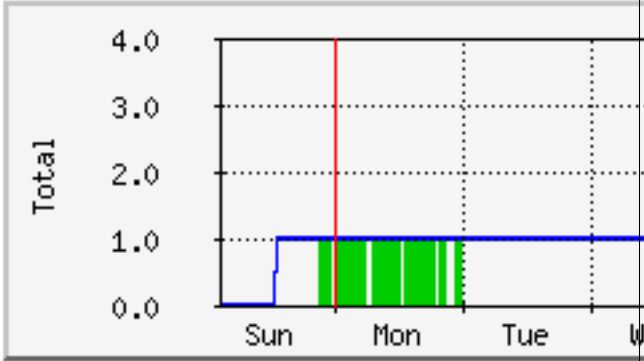
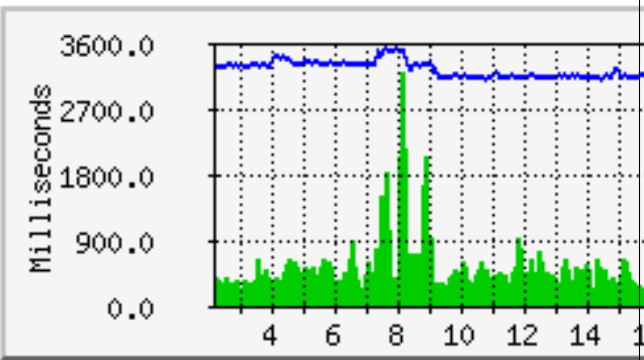
Max **Scheduled Checks**: 93.0    Average **Scheduled Checks**: 72.0  
Max **On-Demand Checks**: 0.0    Average **On-Demand Checks**: 0.0

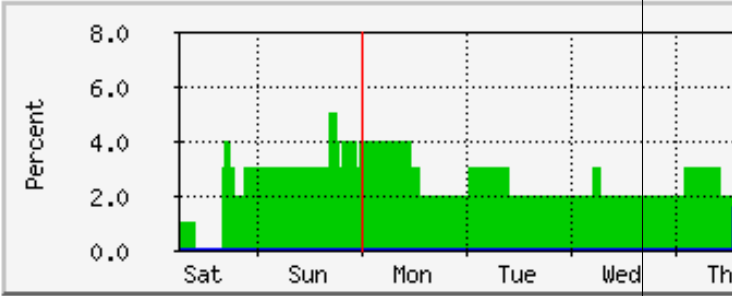
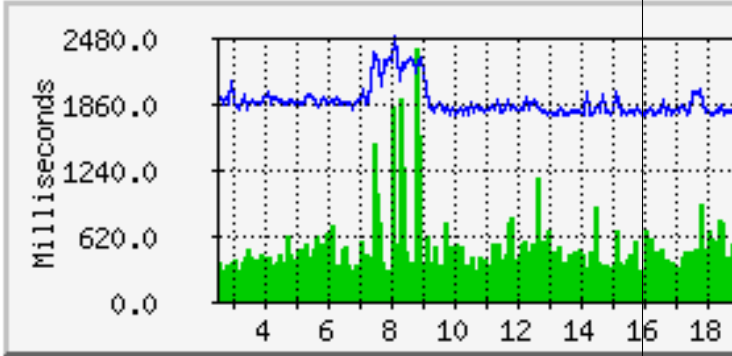
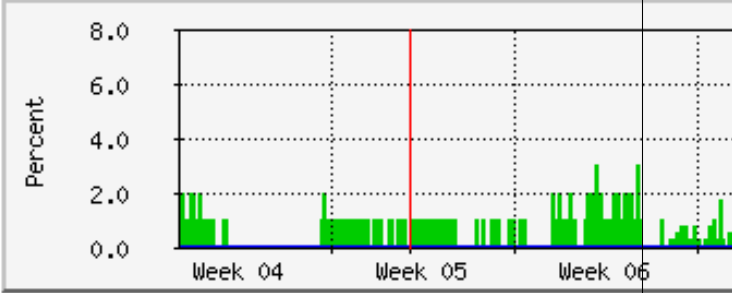
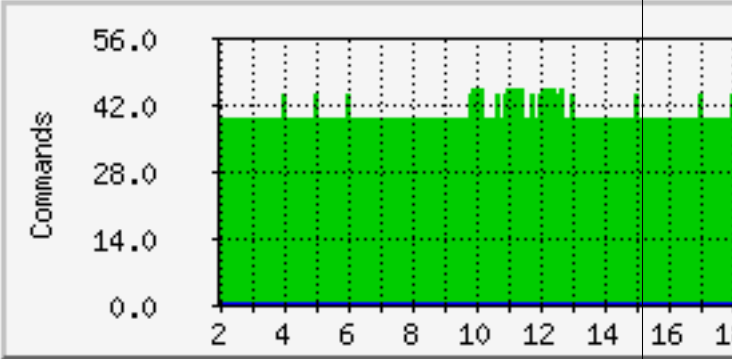


Max **Host Checks**: 6.0    Average **Host Checks**: 2.0  
Max **Service Checks**: 0.0    Average **Service Checks**: 0.0

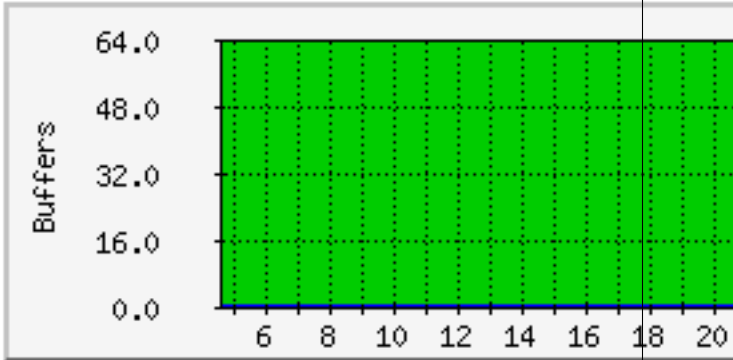


Max **Host Checks**: 10.0    Average **Host Checks**: 10.0  
Max **Service Checks**: 26.0    Average **Service Checks**: 10.0

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><p>Hosts/Services Actively Checked - This graph shows how many (of the total number of) hosts and services were last checked actively over time. Useful for understanding:</p><ul style="list-style-type: none"><li>• <b>Active Checks</b>Active checks</li></ul></div>                                                                                                                                                                                                                                                                                                                                                            | <div><p>This graph displays the number of hosts and services actively checked over a 24-hour period. The y-axis, labeled 'Total', ranges from 0.0 to 88.0 in increments of 22.0. The x-axis shows hours from 6 to 20. A green area at the bottom represents the number of active services, which fluctuates between approximately 22 and 44. A blue line represents the total number of active checks, which stays around 66 but shows significant spikes, reaching nearly 88 between hours 10 and 14.</p><p>Max <b>Hosts</b>: 44.0    Average <b>Hosts</b>: 42.0    Current <b>Hosts</b>: 44.0<br/>Max <b>Services</b>: 85.0    Average <b>Services</b>: 60.0    Current <b>Services</b>: 44.0</p></div> |
| <div><p>Hosts/Services Passively Checked - This graph shows how many (of the total number of) hosts and services were last checked passively over time. Useful for understanding:</p><ul style="list-style-type: none"><li>• <b>Passive Checks</b>Passive checks</li></ul></div>                                                                                                                                                                                                                                                                                                                                                        | <div><p>This graph shows the number of passively checked hosts and services over time. The y-axis, labeled 'Total', ranges from 0.0 to 4.0 in increments of 1.0. The x-axis shows days of the week: Sun, Mon, Tue, Wed. A green area at the bottom represents passive services, which are mostly zero but show small spikes to 1.0 on Sunday and Monday. A blue line represents the total passive checks, which is mostly at 0.0 but has a single spike to 1.0 on Sunday.</p><p>Max <b>Hosts</b>: 1.0    Average <b>Hosts</b>: 0.0    Current <b>Hosts</b>: 0.0<br/>Max <b>Services</b>: 1.0    Average <b>Services</b>: 1.0    Current <b>Services</b>: 1.0</p></div>                                   |
| <div><p>Average Service Check Latency and Execution Time - This graph shows average service check latency and execution times over time. Useful for understanding:</p><ul style="list-style-type: none"><li>• <b>Service Checks</b>Service checks</li><li>• <b>Tuning Nagios For Maximum Performance</b>Performance tuning</li></ul><p>Consistently high latencies can be an indication that one of more of the following variables need tweaking:</p><ul style="list-style-type: none"><li>• <b>max_concurrent_checks</b></li><li>• <b>check_result_reaper_frequency</b></li><li>• <b>max_check_result_reaper_time</b></li></ul></div> | <div><p>This graph illustrates the average latency and execution time for service checks in milliseconds. The y-axis, labeled 'Milliseconds', ranges from 0.0 to 3600.0 in increments of 900.0. The x-axis shows hours from 4 to 18. A green area at the bottom represents the average execution time, which is mostly below 900ms but has a large spike reaching nearly 3600ms around hour 8. A blue line represents the average latency, which remains relatively stable around 3200ms.</p><p>Max <b>Latency</b>: 3203.0    Average <b>Latency</b>: 3203.0<br/>Max <b>Execution Time</b>: 3498.0    Average <b>Execution Time</b>: 3498.0</p></div>                                                   |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Average Service State Change - This graph shows the average percent state change (a measure of volatility) for services over time, broken down by services that were last checked either actively or passively. Useful for understanding:</p> <ul style="list-style-type: none"><li>Detection and Handling of State FlappingFlap detection</li></ul>                                                                                                                                                                                                                        |  <p>Max Active Check % Change: 5.0    Average Active Check %<br/>Max Passive Check % Change: 3.0    Average Passive Check %</p>   |
| <p>Average Host Check Latency and Execution Time - This graph shows average host check latency and execution times over time. Useful for understanding:</p> <ul style="list-style-type: none"><li>Host ChecksHost checks</li><li>Tuning Nagios For Maximum PerformancePerformance tuning</li></ul> <p>Consistently high latencies can be an indication that one of more of the following variables need tweaking:</p> <ul style="list-style-type: none"><li>max_concurrent_checks</li><li>check_result_reaper_frequency</li><li>max_check_result_reaper_time</li></ul>         |  <p>Max Latency: 2373.0    Average Latency<br/>Max Execution Time: 2480.0    Average Execution Time</p>                          |
| <p>Average Host State Change - This graph shows the average percent state change (a measure of volatility) for hosts over time, broken down by hosts that were last checked either actively or passively. Useful for understanding:</p> <ul style="list-style-type: none"><li>Detection and Handling of State FlappingFlap detection&gt;</li></ul>                                                                                                                                                                                                                             |  <p>Max Active Check % Change: 7.0    Average Active Check %<br/>Max Passive Check % Change: 0.0    Average Passive Check %</p> |
| <p>External Commands - This graph shows how many external commands have been processed by the Nagios daemon over time. Unless you're processing a large number of external commands (as in the case with distributed monitoring setups), this graph may appear mostly empty. Monitoring external commands can be useful for understanding the impacts of:</p> <ul style="list-style-type: none"><li>Passive ChecksPassive checks</li><li>Distributed MonitoringDistributed monitoring</li><li>Redundant and Failover Network MonitoringRedundant/failover monitoring</li></ul> |  <p>Max Commands: 54.0    Average Commands: 40.0</p>                                                                            |

External Command Buffers - This graph shows how many external command buffer slots are in use over time. If the number of used buffers is near the number of available buffers on a regular basis, it is likely you need to increase the available **external command buffer slots**. Each buffer slot can hold one external command. Buffers are used for temporarily holding external commands from the time they are read from the **external command file** to the time they are processed by the Nagios daemon.



|                 |                     |                     |
|-----------------|---------------------|---------------------|
| Max Avail: 64.0 | Average Avail: 64.0 | Current Avail: 64.0 |
| Max Used: 29.0  | Average Used: 0.0   | Current Used: 0.0   |

## **Part VIII**

# **Integration With Other Software**

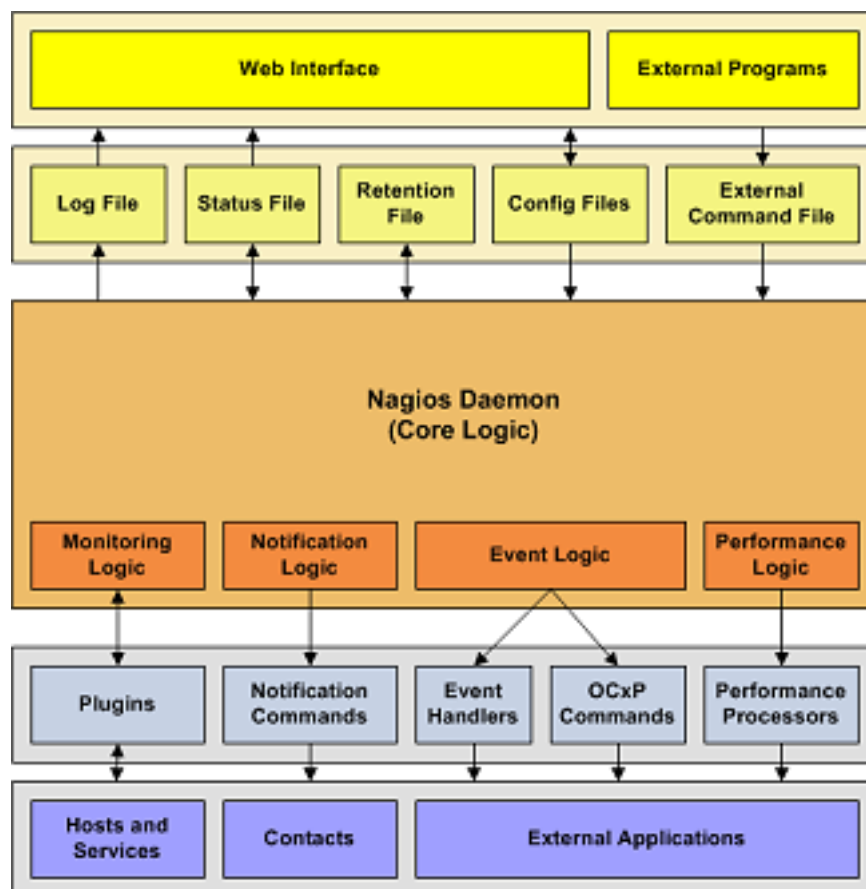
## Chapter 66

# Integration Overview

### 66.1 Introduction

One of the reasons that Nagios is such a popular monitoring application is the fact that it can be easily integrated in your existing infrastructure. There are several methods of integrating Nagios with the management software you're already using and you can monitor almost any type of new or custom hardware, service, or application that you might have.

### 66.2 Integration Points



To monitor new hardware, services, or applications, check out the docs on:

- [Nagios Plugins](#)
- [Nagios Plugin API](#)
- [Passive Checks](#)
- [Event Handlers](#)

To get data into Nagios from external applications, check out the docs on:

- [Passive Checks](#)
- [External Commands](#)

To send status, performance, or notification information from Nagios to external applications, check out the docs on:

- [Event Handlers](#)
- [OCSP](#) and [OCHP](#) Commands
- [Performance Data](#)
- [Notifications](#)

## 66.3 Integration Examples

I've documented some examples on how to integrate Nagios with external applications:

- [TCP Wrappers Integration](#) (security alerts)
  - [SNMP Trap Integration](#) (Arcserve backup job status)
-

## Chapter 67

# SNMP Trap Integration

### 67.1 Introduction

---

**Note**

Nagios is not designed to be a replacement for a full-blown `SNMP` management application like HP OpenView or [OpenNMS](#). However, you can set things up so that `SNMP` traps received by a host on your network can generate alerts in Nagios.

---

As if designed to make the Gods of Hypocrisy die of laughter, `SNMP` is anything but simple. Translating `SNMP` traps and getting them into Nagios (as passive check results) can be a bit tedious. To make this task easier, I suggest you check out Alex Burger's `SNMP` Trap Translator project located at <http://www.snmpptt.org>. When combined with Net-SNMP, SNMPTT provides an enhanced trap handling system that can be integrated with Nagios.

Yep, that's all.

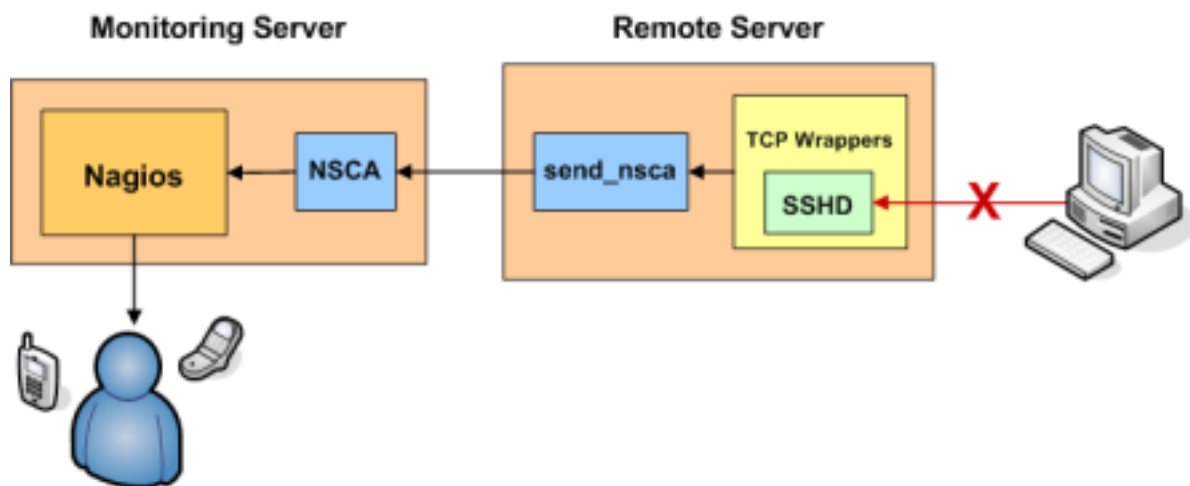
---



## Chapter 68

# TCP Wrappers Integration

### 68.1 Introduction



This document explains how to easily generate alerts in Nagios for connection attempts that are rejected by TCP wrappers. For example, if an unauthorized host attempts to connect to your SSH server, you can receive an alert in Nagios that contains the name of the host that was rejected. If you implement this on your Linux/Unix boxes, you'll be surprised how many port scans you can detect across your network.

These directions assume:

1. You are already familiar with **Passive Checks** and how they work.
2. You are already familiar with **Volatile Services** and how they work.
3. The host which you are generating alerts for (i.e. the host you are using TCP wrappers on) is a remote host (called firestorm in this example). If you want to generate alerts on the same host that Nagios is running you will need to make a few modifications to the examples I provide.
4. You have installed the **NSCA daemon** on your monitoring server and the NSCA client (**send\_nsca**) on the remote machine that you are generating TCP wrapper alerts from.

### 68.2 Defining A Service

If you haven't done so already, create a **host definition** for the remote host (firestorm).

Next, define a service in one of your **object configuration files** for the TCP wrapper alerts on host firestorm. The service definition might look something like this:

```
define service{
 ~ ~ ~ ~ host_name ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ firestorm
 ~ ~ ~ ~ service_description ~ ~ ~ ~ ~ TCP Wrappers
 ~ ~ ~ ~ is_volatile ~ ~ ~ ~ ~ ~ ~ ~ ~ 1
 ~ ~ ~ ~ active_checks_enabled ~ ~ ~ ~ ~ 0
 ~ ~ ~ ~ passive_checks_enabled ~ ~ ~ ~ ~1
 ~ ~ ~ ~ max_check_attempts ~ ~ ~ ~ ~ ~1
 ~ ~ ~ ~ check_command ~ ~ ~ ~ ~ ~ ~ ~ check_none
 ~ ~ ~ ~ ...
 ~ ~ ~ ~ }
```

There are some important things to note about the above service definition:

1. The volatile option enabled. We want this option enabled because we want a notification to be generated for every alert that comes in.
2. Active checks of the service as disabled, while passive checks are enabled. This means that the service will never be actively checked by Nagios - all alert information will have to be received passively from an external source.
3. The `max_check_attempts` value is set to 1. This guarantees you will get a notification when the first alert is generated.

## 68.3 Configuring TCP Wrappers

Now you're going to have to modify the `/etc/hosts.deny` file on firestorm. In order to have the TCP wrappers send an alert to the monitoring host whenever a connection attempt is denied, you'll have to add a line similar to the following:

```
ALL: ALL: RFC931: twist (/usr/local/nagios/libexec/eventhandlers/handle_tcp_wrapper %h %d)&
```

This line assumes that there is a script called `handle_tcp_wrapper` in the `/usr/local/nagios/libexec/eventhandlers/` directory on firestorm. We'll write that script next.

## 68.4 Writing The Script

The last thing you need to do is write the `handle_tcp_wrapper` script on firestorm that will send the alert back to the Nagios server. It might look something like this:

```
#!/bin/sh
/usr/local/nagios/libexec/eventhandlers/submit_check_result firestorm "TCP Wrappers" 2 " ←
Denied $2-$1" > /dev/null 2> /dev/null
```

Notice that the **handle\_tcp\_wrapper** script calls the **submit\_check\_result** script to actually send the alert back to the monitoring host. Assuming your Nagios server is called monitor, the **submit\_check\_result** script might look like this:

```
#!/bin/sh
Arguments
$1 = name of host in service definition
$2 = name/description of service in service definition
$3 = return code
$4 = outputs

/bin/echo -e "$1\t$2\t$3\t$4\n" | /usr/local/nagios/bin/send_nsca monitor -c /usr/local/ ←
nagios/etc/send_nsca.cfg
```

## 68.5 Finishing Up

You've now configured everything you need to, so all you have to do is restart the `inetd` process on `firestorm` and restart Nagios on your monitoring server. That's it! When the TCP wrappers on `firestorm` deny a connection attempt, you should be getting alerts in Nagios. The plugin output for the alert will look something like the following: `Denied sshd2-sdn-ar-002mm-innP321.dialsprint.net`

---

## **Part IX**

# **Nagios Addons**

## Chapter 69

# Nagios Addons

### 69.1 Introduction

There are a lot of ‘addon’ software packages that are available for Nagios. Addons can be used to extend Nagios’ functionality or integrate Nagios with other applications.

Addons are available for:

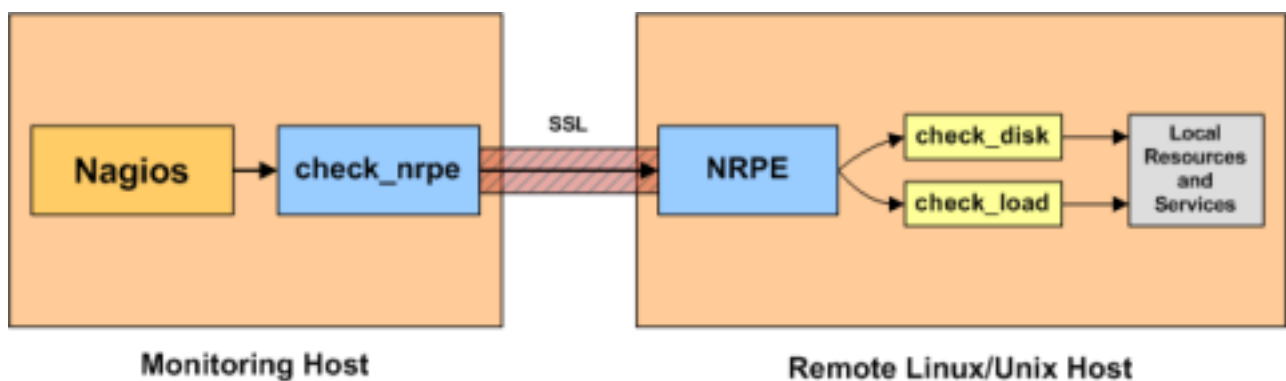
- Managing the config files through a web interface
- Monitoring remote hosts (\*NIX, Windows, etc.)
- Submitting passive checks from remote hosts
- Simplifying/extending the notification logic
- ...and much more

You can find many addons for Nagios by visiting:

- [Nagios.org](http://Nagios.org)
- [SourceForge.net](http://SourceForge.net)
- [NagiosExchange.org](http://NagiosExchange.org)

I’ll give a brief introduction to a few of the addons that I’ve developed for Nagios...

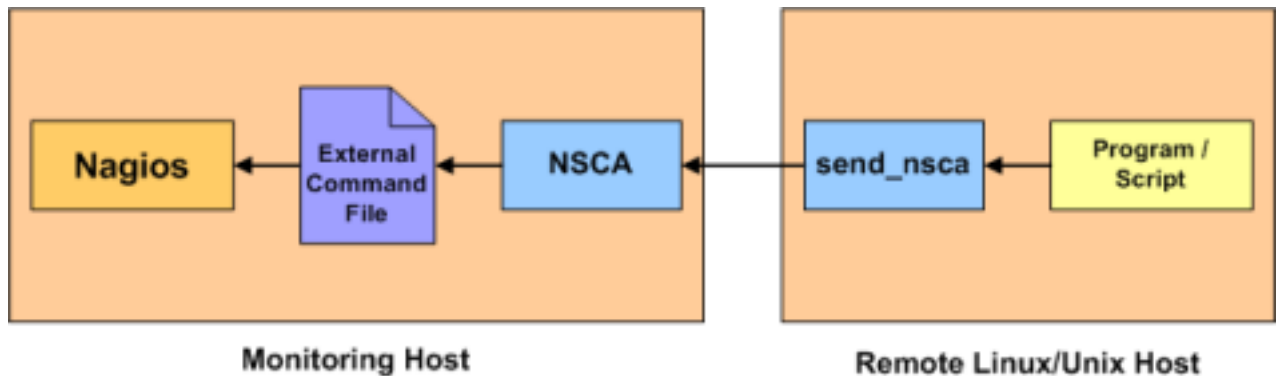
### 69.2 NRPE



NRPE is an addon that allows you to execute **Nagios Plugins** on remote Linux/Unix hosts. This is useful if you need to monitor local resources/attributes like disk usage, CPU load, memory usage, etc. on a remote host. Similiar functionality can be accomplished by using the **check\_by\_ssh** plugin, although it can impose a higher CPU load on the monitoring machine - especially if you are monitoring hundreds or thousands of hosts.

The NRPE addon and documentation can be found at <http://www.nagios.org/>.

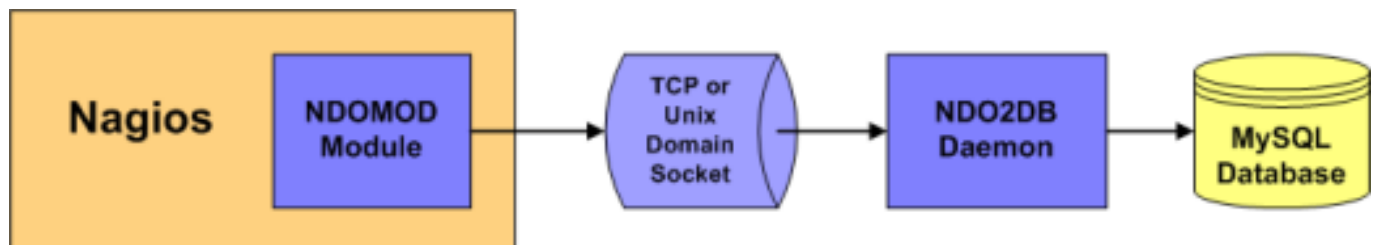
### 69.3 NSCA



NSCA is an addon that allows you to send **Passive Checks** results from remote Linux/Unix hosts to the Nagios daemon running on the monitoring server. This is very useful in **Distributed Monitoring** and **Redundant and Failover Network Monitoring** setups.

The NRPE addon and documentation can be found at <http://www.nagios.org/>.

### 69.4 NDOUtils



NDOUtils is an addon that allows you to store all status information from Nagios in a MySQL database. Multiple instances of Nagios can all store their information in a central database for centralized reporting. This will likely serve as the basis for a new PHP-based web interface for Nagios in the future.

The NDOUtils addon and documentation can be found at <http://www.nagios.org/>.

# **Part X**

# **Development**

---

## Chapter 70

# Nagios Plugin API

### 70.1 Other Resources

If you're looking at writing your own plugins for Nagios, please make sure to visit these other resources:

- The official [Nagios plugin project website](#)
- The official [Nagios plugin development guidelines](#)

### 70.2 Plugin Overview

Scripts and executables must do two things (at a minimum) in order to function as Nagios plugins:

- Exit with one of several possible return values
- Return at least one line of text output to `STDOUT`

The inner workings of your plugin are unimportant to Nagios. Your plugin could check the status of a TCP port, run a database query, check disk free space, or do whatever else it needs to check something. The details will depend on what needs to be checked - that's up to you.

### 70.3 Return Code

Nagios determines the status of a host or service by evaluating the return code from plugins. The following tables shows a list of valid return codes, along with their corresponding service or host states.

| Plugin Return Code | Service State | Host State              |
|--------------------|---------------|-------------------------|
| 0                  | OK            | UP                      |
| 1                  | WARNING       | UP or DOWN/UNREACHABLE* |
| 2                  | CRITICAL      | DOWN/UNREACHABLE        |
| 3                  | UNKNOWN       | DOWN/UNREACHABLE        |

---

**Note**

If the `use_aggressive_host_checking` option is enabled, return codes of 1 will result in a host state of DOWN or UNREACHABLE. Otherwise return codes of 1 will result in a host state of UP. The process by which Nagios determines whether or not a host is DOWN or UNREACHABLE is discussed [here](#).

---



## 70.4 Plugin Output Spec

At a minimum, plugins should return at least one of text output. Beginning with Nagios 3, plugins can optionally return multiple lines of output. Plugins may also return optional performance data that can be processed by external applications. The basic format for plugin output is shown below:

```
TEXT OUTPUT | OPTIONAL PERFDATA LONG TEXT LINE 1 LONG TEXT LINE 2...LONG TEXT LINE N | PERFDATA
LINE 2 PERFDATA LINE 3...PERFDATA LINE N
```

The performance data (shown in orange) is optional. If a plugin returns performance data in its output, it must separate the performance data from the other text output using a pipe (|) symbol. Additional lines of long text output (shown in blue) are also optional.

## 70.5 Plugin Output Examples

Let's see some examples of possible plugin output...

### Case 1: One line of output (text only)

Assume we have a plugin that returns one line of output that looks like this:

```
DISK OK - free space: / 3326 MB (56%);
```

If this plugin was used to perform a service check, the entire line of output will be stored in the **\$SERVICEOUTPUT\$** macro.

### Case 2: One line of output (text and perfdata)

A plugin can return optional performance data for use by external applications. To do this, the performance data must be separated from the text output with a pipe (|) symbol like such:

```
DISK OK - free space: / 3326 MB (56%);
```

```
~|~
```

```
/=2643MB;5948;5958;0;5968
```

If this plugin was used to perform a service check, the red portion of output (left of the pipe separator) will be stored in the **\$SERVICEOUTPUT\$** macro and the orange portion of output (right of the pipe separator) will be stored in the **\$SERVICEPERFDATA\$** macro.

### Case 3: Multiple lines of output (text and perfdata)

A plugin optionally return multiple lines of both text output and perfdata, like such:

```
DISK OK - free space: / 3326 MB (56%);~|~/=2643MB;5948;5958;0;5968/ 15272 MB (77%);/boot 68 MB (69%);/home 69357 MB (27%);/var/log 819 MB (84%);~|~/boot=68MB;88;93;0;98/home=69357 MB;253404;253409;0;253414 /var/log=818MB;970;975;0;980
```

If this plugin was used to perform a service check, the red portion of first line of output (left of the pipe separator) will be stored in the **\$SERVICEOUTPUT\$** macro. The orange portions of the first and subsequent lines are concatenated (with spaces) are stored in the **\$SERVICEPERFDATA\$** macro. The blue portions of the 2nd - 5th lines of output will be concatenated (with escaped newlines) and stored in **\$LONGSERVICEOUTPUT\$** the macro.

The final contents of each macro are listed below:

| Macro                 | Value                                                                 |
|-----------------------|-----------------------------------------------------------------------|
| \$SERVICEOUTPUT\$     | DISK OK - free space: / 3326 MB (56%);                                |
| \$SERVICEPERFDATA\$   | /=2643MB;5948;5958;0;5968 /boot=68MB;88;93;0;98 /home=69357           |
| \$LONGSERVICEOUTPUT\$ | / 15272 MB (77%);<br>/n/boot 68 MB (69%);<br>/n/var/log 819 MB (84%); |

With regards to multiple lines of output, you have the following options for returning performance data:

- You can choose to return no performance data whatsoever
- You can return performance data on the first line only
- You can return performance data only in subsequent lines (after the first)
- You can return performance data in both the first line and subsequent lines (as shown above)

## 70.6 Plugin Output Length Restrictions

Nagios will only read the first 4 KB of data that a plugin returns. This is done in order to prevent runaway plugins from dumping megs or gigs of data back to Nagios. This 4 KB output limit is fairly easy to change if you need. Simply edit the value of the `MAX_PLUGIN_OUTPUT_LENGTH` definition in the `include/nagios.h.in` file of the source code distribution and recompile Nagios. There's nothing else you need to change!

## 70.7 Examples

If you're looking for some example plugins to study, I would recommend that you download the official Nagios plugins and look through the code for various C, Perl, and shell script plugins. Information on obtaining the official Nagios plugins can be found [here](#).

## 70.8 Perl Plugins

Nagios features an optional **embedded Perl interpreter** which can speed up the execution of Perl plugins. More information on developing Perl plugins for use with the embedded Perl interpreter can be found [here](#).

---

## Chapter 71

# Developing Plugins For Use With Embedded Perl

### 71.1 Introduction

Stanley Hopcroft has worked with the embedded Perl interpreter quite a bit and has commented on the advantages/disadvantages of using it. He has also given several helpful hints on creating Perl plugins that work properly with the embedded interpreter. The majority of this documentation comes from his comments.

It should be noted that 'ePN', as used in this documentation, refers to embedded Perl Nagios, or if you prefer, Nagios compiled with an embedded Perl interpreter.

### 71.2 Target Audience

- Average Perl developers; those with an appreciation of the languages powerful features without knowledge of internals or an in depth knowledge of those features.
- Those with a utilitarian appreciation rather than a great depth of understanding.
- If you are happy with Perl objects, name management, data structures, and the debugger, that's probably sufficient.

### 71.3 Things you should do when developing a Perl Plugin (ePN or not)

- Always always generate some output
  - Use 'use utils' and import the stuff it exports (\$TIMEOUT %ERRORS &print\_revision &support)
  - Have a look at how the standard Perl plugins do their stuff e.g.
    - Always exit with \$ERRORS{CRITICAL}, \$ERRORS{OK}, etc.
    - Use getopt to read command line arguments
    - Manage timeouts
    - Call print\_usage (supplied by you) when there are no command line arguments
    - Use standard switch names (eg H 'host', V 'version')
-

## 71.4 Things you must do to develop a Perl plugin for ePN

1. <DATA> can not be used; use here documents instead e.g.

```
my $data = <<DATA;
portmapper 100000
portmap 100000
sunrpc 100000
rpcbind 100000
rstatd 100001
rstat 100001
rup 100001
..
DATA

%prognum = map { my($a, $b) = split; ($a, $b) } split(/\n/, $data) ;
```

2. BEGIN blocks will not work as you expect. May be best to avoid.
3. Ensure that it is squeaky clean at compile time i.e.
  - use strict
  - use perl -w (other switches [T notably] may not help)
  - use perl -c
4. Avoid lexical variables (my) with global scope as a means of passing variable data into subroutines. In fact this is fatal if the subroutine is called by the plugin more than once when the check is run. Such subroutines act as 'closures' that lock the global lexicals first value into subsequent calls of the subroutine. If however, your global is read-only (a complicated structure for example) this is not a problem. What Bekman **recommends you do instead**, is any of the following:
  - make the subroutine anonymous and call it via a code ref e.g.

| turn this                                                      | into                                   |
|----------------------------------------------------------------|----------------------------------------|
| my \$x = 1 ;                                                   | my \$x = 1 ;                           |
| sub a { .. Process \$x ... }                                   | \$a_cr = sub { ... Process \$x ... } ; |
| .                                                              | .                                      |
| .                                                              | .                                      |
| a ;                                                            | &\$a_cr ;                              |
| \$x = 2                                                        | \$x = 2 ;                              |
| a ;                                                            | &\$a_cr ;                              |
| # anon closures <u>always</u> rebind the current lexical value |                                        |

- put the global lexical and the subroutine using it in their own package (as an object or a module)
  - pass info to subs as references or aliases (\$lex\_var or \$\_[n])
  - replace lexicals with package globals and exclude them from 'use strict' objections with 'use vars qw(global1 global2 ..)'
5. Be aware of where you can get more information.

Useful information can be had from the usual suspects (the O'Reilly books, plus Damien Conways 'Object Oriented Perl') but for the really useful stuff in the right context start at Stas Bekman's mod\_perl guide at <http://perl.apache.org/guide/>.

This wonderful book sized document has nothing whatsoever about Nagios, but all about writing Perl programs for the embedded Perl interpreter in Apache (ie Doug MacEacherns mod\_perl).

The perlembed manpage is essential for context and encouragement.

On the basis that Lincoln Stein and Doug MacEachern know a thing or two about Perl and embedding Perl, their book 'Writing Apache Modules with Perl and C' is almost certainly worth looking at.

6. Be aware that your plugin may return strange values with an ePN and that this is likely to be caused by the problem in item #4 above
7. Be prepared to debug via:
  - having a test ePN and
  - adding print statements to your plugin to display variable values to STDERR (can't use STDOUT)
  - adding print statements to p1.pl to display what ePN thinks your plugin is before it tries to run it (vi)
  - running the ePN in foreground mode (probably in conjunction with the former recommendations)
  - use the 'Deparse' module on your plugin to see how the parser has optimised it and what the interpreter will actually get. (see 'Constants in Perl' by Sean M. Burke, The Perl Journal, Fall 2001)

```
perl -MO::Deparse <your_program>
```

8. Be aware of what ePN is transforming your plugin too, and if all else fails try and debug the transformed version. As you can see below p1.pl rewrites your plugin as a subroutine called 'hndlr' in the package named 'Embed::<something\_related>'. Your plugin may be expecting command line arguments in @ARGV so p1.pl also assigns @\_ to @ARGV. This in turn gets 'eval' ed and if the eval raises an error (any parse error and run error), the plugin gets chucked out. The following output shows how a test ePN transformed the **check\_rpc** plugin before attempting to execute it. Most of the code from the actual plugin is not shown, as we are interested in only the transformations that the ePN has made to the plugin). For clarity, transformations are shown in red:

```
~ ~ ~ ~ ~ ~ ~ package main;
~ ~ ~ ~ ~ ~ ~ use subs 'CORE::GLOBAL::exit';
~ ~ ~ ~ ~ ~ ~ sub CORE::GLOBAL::exit { die "ExitTrap: $_[0]
(Embed::check_5frpc)"; }
~ ~ ~ ~ ~ ~ ~ package Embed::check_5frpc; sub hndlr { shift(@_);
@ARGV=@_;
#! /usr/bin/perl -w
#
check_rpc plugin for Nagios
#
usage:
~ ~check_rpc host service
#
Check if an rpc service is registered and running
using rpcinfo - $proto $host $prognum 2>&1 |";
#
Use these hosts.cfg entries as examples
#
command[check_nfs]=/some/path/libexec/check_rpc $HOSTADDRESS$ nfs
service[check_nfs]=NFS;24x7;3;5;5;unix-admin;60;24x7;1;1;1;;check_rpc
#
initial version: 3 May 2000 by Truongchinh Nguyen and Karl DeBisschop
current status: $Revision: 1.19 $
#
Copyright Notice: GPL
#
... rest of plugin code goes here (it was removed for brevity) ...
}
```

9. Don't use 'use diagnostics' in a plugin run by your production ePN. I think it causes\_\_all\_\_ the Perl plugins to return CRITICAL.
10. Consider using a mini embedded Perl C program to check your plugin. This is not sufficient to guarantee your plugin will perform Ok with an ePN but if the plugin fails this test it will certainly fail with your ePN. [ A sample mini ePN is included in the contrib/ directory of the Nagios distribution for use in testing Perl plugins. Change to the contrib/ directory and type **make mini\_epn** to compile it. It must be executed from the same directory that the p1.pl file resides in (this file is distributed with Nagios). ]