

Netzwerküberwachung mit Nagios & Co.

Kurs 1021

© 2009-2010 OpenSource Training Ralf Spenneberg

Am Bahnhof 3 - 5

48565 Steinfurt

<http://www.opensource-training.de>

<http://www.os-t.de>

Copyright

Die in diesem Kurs zur Verfügung gestellten Folien, Unterlagen und Übungen sind urheberrechtlich geschützt. Wir behalten uns alle Rechte vor, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung ist nicht erlaubt.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit genutzt. Fast alle Hardware- und Softwarebezeichnungen, die in dieser Unterlage erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen.

Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt vorgegangen. Jedoch können Fehler nicht vollständig ausgeschlossen werden. Die Firma OpenSource Training Ralf Spenneberg kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Inhaltsverzeichnis

1	Einführung	7
1.1	Installation	9
1.2	Start	11
1.3	Konfigurationsdateien	15
2	Definition Nagios-Objekte	19
2.1	Host-Definition	21
2.2	Hostgroup-Definition	25
2.3	Verfügbarkeitsprüfung	27
2.4	Service-Definition	29
2.5	Contact-Definition	33
2.6	Command-Definition	35
2.7	Timeperiod-Definition	37
2.8	Template-Definition	39
2.9	Testen der Konfiguration	41
3	Grundlagen	43
3.1	Hard- und Soft-State	43
3.2	Makros	45
3.2.1	Standardmakros	47
3.3	Netzwerktopologie	49
4	Netzwerkbasierete Dienste überwachen	51
4.1	Verfügbare Plugins	51
5	Prüfung lokaler Ressourcen	53
5.1	Plugins	53
5.2	check_by_ssh	55
5.2.1	SSH Konfiguration	57
5.2.2	Nagios-Konfiguration	59
5.3	Nagios Remote Plugin Executor (NRPE)	61
5.3.1	NRPE-Konfiguration	63
5.3.2	Nagios-Konfiguration	65
5.4	Serviceabhängigkeiten	67
6	Benachrichtigungssystem von Nagios	69
6.1	Nachrichtenfilter	69
6.2	Benachrichtigungskommandos	73
6.3	Eskalationsmanagement	75

7	Überwachung mit SNMP	79
7.1	OID und MIB	79
7.2	SNMP und Linux	81
8	Logische Verknüpfungen von Check-Resultaten	83
8.1	Business Process Monitoring	85
9	Passive Tests	87
9.1	Voraussetzungen	88
9.2	Aufbau externer Kommandos	89
9.3	Passive Checks - Resultate verteilen	91
9.4	NSCA Installation	91
9.5	NSCA-Konfiguration	93
10	Windows-Server überwachen	95
10.1	Windows und SNMP	96
10.2	Windows-Dienste zum System-Monitoring	96
10.3	check_nt	99
10.4	NSClient++	101
10.5	NRPE mit NSClient++	105
10.6	OpMon Agent	107
11	Auf Ereignisse automatisiert reagieren	111
11.1	Eventhandler	111
12	Verteiltes Monitoring	113
12.1	OCSP/OCHP einschalten	113
12.2	OCSP/OCHP Kommandos	115
12.3	Aktualität der Testresultate	117
13	Nagios erweitern	119
13.1	Eigene Plugins erstellen	119
13.2	AddOns für Nagios	119
13.3	Grafische Konfigurationswerkzeuge	121
14	Performancedaten erheben	123
14.1	Nagios	123
14.1.1	Template-Dateien	124
14.1.2	Graphen	127
14.2	PNP4Nagios	129

15 Performancedaten mit Munin	131
15.0.1 Übersicht	131
15.0.2 Installation und Konfiguration	133
15.0.3 Manuelle Abfrage	137
15.0.4 Round Robin Datenbanken	139
15.0.5 Plugin-Konfiguration ändern	141
15.0.6 Munin und Nagios	143
Index	145