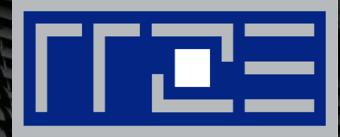


REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Monitoring

Systemausbildung – Grundlagen und Aspekte von
Betriebssystemen und System-nahen Diensten, 29.06.2016
Uwe Scheuerer, RRZE

Agenda

- Wozu Monitoring?
- Unterscheidung
 - Funktionalitäts-Monitoring
 - Performance-Monitoring
- Kriterien
- Datenerhebung
- Abhängigkeiten
- Benachrichtigungen
 - Fehlalarme vermeiden
- Welche Monitoringtools gibt es?
- Icinga und Munin am RRZE



Wozu Monitoring?

- Frühzeitige akute Problemerkennung
- Schnelle Reaktion
- Passende Benachrichtigung

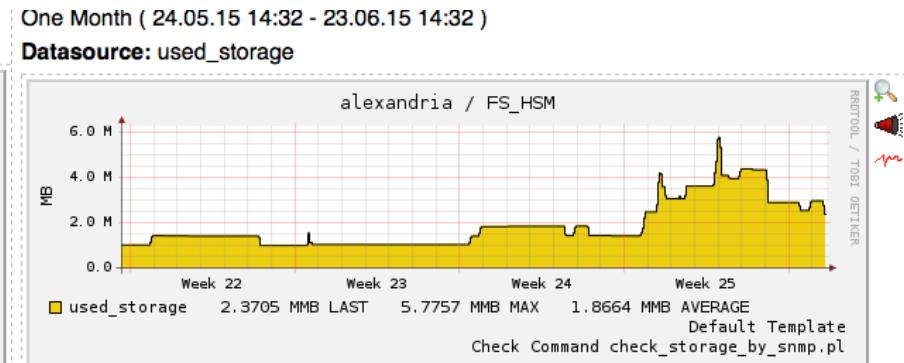
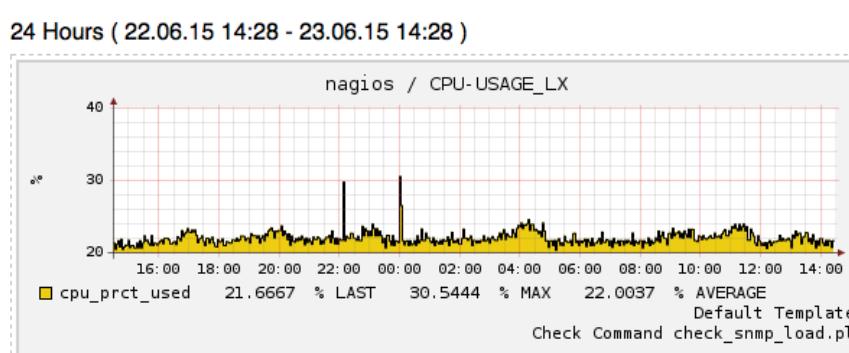
The screenshot shows the Nagios Core interface with the following sections:

- General:** Home, Documentation.
- Current Status:** Tactical Overview, Hosts, Services, Host Groups (Summary, Grid), Service Groups (Summary, Grid), Problems, Services (Unhandled), Hosts (Unhandled), Network Outages, Map, Navvis, Quick Search: nagios.
- Tactical Monitoring Overview:** Last Updated: Tue Jun 23 14:25:09 CEST 2015, Nagios Core® 3.2.3 - www.nagios.org.
- Monitoring Performance:** Service Check Execution: 0.01 / 30.01 / 0.373 sec, Time: 0.00 / 10.27 / 0.588 sec, Host Check Execution Time: 0.01 / 10.02 / 0.067 sec, Host Check Latency: 0.00 / 2.40 / 1.001 sec, # Active Host / Service Checks: 408 / 1672, # Passive Host / Service Checks: 86 / 739.
- Network Outages:** 0 Outages.
- Hosts:** 2 Down, 0 Unreachable, 492 Up, 0 Pending, 2 Acknowledged, 84 Disabled.
- Services:** 24 Critical, 16 Warning, 11 Unknown, 2360 Ok, 0 Pending, 11 Unhandled Problems, 6 Unhandled Problems, 7 on Problem Hosts, 5 Disabled, 7 Disabled, 0 Disabled.
- Monitoring Features:** Flap Detection, Notifications, Event Handlers, Active Checks, Passive Checks. Status: Disabled, Enabled, Enabled, Enabled, Enabled.

Hostgroups		Hosts for backup		Services for alexandria		All host problems		Notifications		Search result host	
Type	Host	Service	Status	Timestamp	Output	Contact	Command				
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 13:00:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 12:50:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 12:30:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 12:20:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 12:10:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 12:00:29	WARNING! SYSTEM usage: 29327/32263 MB (90.90%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:50:29	WARNING! SYSTEM usage: 29324/32263 MB (90.89%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:40:29	WARNING! SYSTEM usage: 29321/32263 MB (90.88%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:30:29	WARNING! SYSTEM usage: 29321/32263 MB (90.88%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:20:29	WARNING! SYSTEM usage: 29321/32263 MB (90.88%)						
Service	zuvdc1.zuv	RAM_WIN	WARNING	2015-06-23 11:18:59	WARNING! Physical usage: 1928/2047 MB (94.19%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:10:29	WARNING! SYSTEM usage: 29320/32263 MB (90.88%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 11:00:29	WARNING! SYSTEM usage: 29321/32263 MB (90.88%)						
Service	zuvdc1.zuv	FS_PART_C_WIN	WARNING	2015-06-23 10:50:29	WARNING! SYSTEM usage: 29309/32263 MB (90.84%)						
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	SSchmitt_email	notify-by-email				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	SSchmitt_sms	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	DGoetz_email	notify-by-email				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	SZenger_email	notify-by-email				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	Rismaier_sms	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	SDoehler_sm	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	AKugler_sms	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	OK	2015-06-23 10:41:59	OK! Physical usage: 1076/2047 MB (52.56%)	SSchmidt_sms	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	CRITICAL	2015-06-23 10:40:59	CRITICAL! Physical usage: 2024/2047 MB (98.88%)	SSchmitt_email	notify-by-email				
Service	zuvdc1.zuv	RAM_WIN	CRITICAL	2015-06-23 10:40:59	CRITICAL! Physical usage: 2024/2047 MB (98.88%)	SSchmitt_sms	notify-by-sms				
Service	zuvdc1.zuv	RAM_WIN	CRITICAL	2015-06-23 10:40:59	CRITICAL! Physical usage: 2024/2047 MB (98.88%)	DGoetz_email	notify-by-email				

Wozu Monitoring?

- Blick auf die Zeit
 - Vergangenheit
 - › Wie hat sich ein System vor dem Problem entwickelt?
 - Zukunft
 - › Wie wird sich das System vermutlich weiterentwickeln?



Unterscheidung

- Je nach gewünschtem Aufgabengebiet kann man Monitoring in zwei grobe Kategorien unterteilen.
- Funktionalitäts-Monitoring
 - Benachrichtigung von Technikern, Kunden und Servicekräften bei
 - › Ausfällen von Hosts
 - › Ausfällen von Services
 - Datenspeicherung nach dem Ex- und Hopp-Prinzip!
Die gesammelten Daten werden hinsichtlich gesetzter Schwellwerte geprüft und melden über unterschiedliche Wege an festgelegte Personen oder Gruppen.

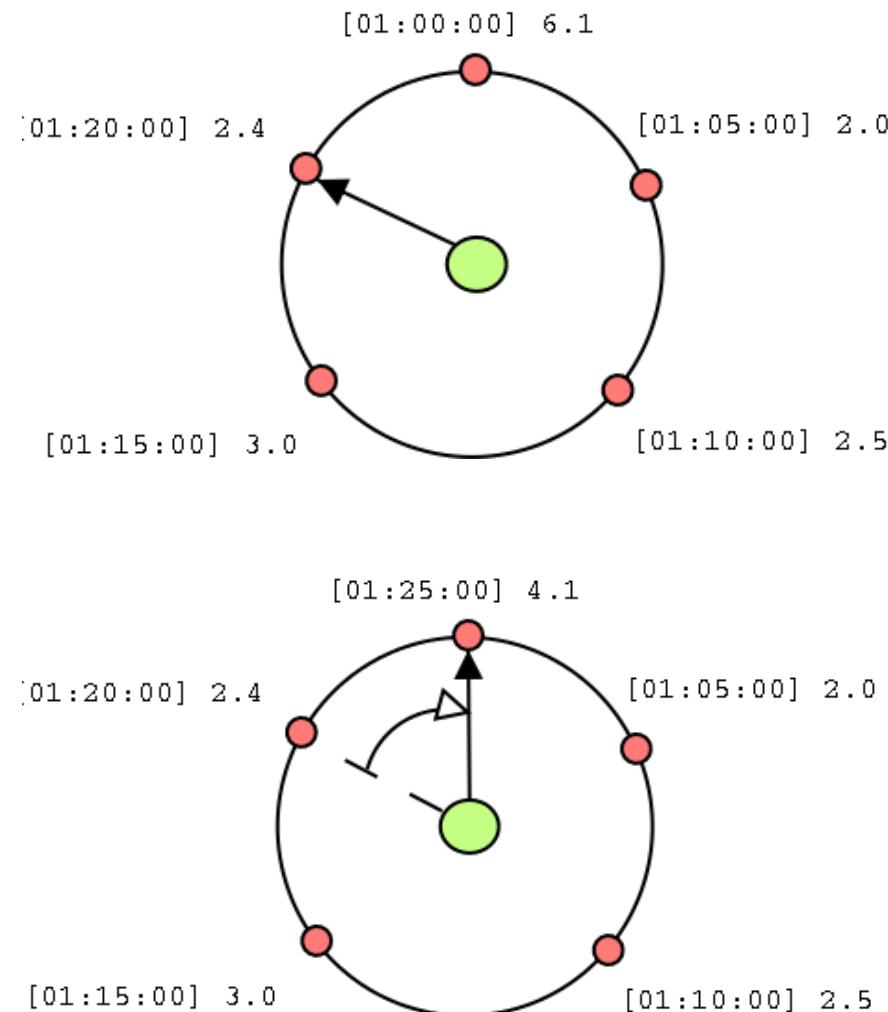
Unterscheidung

■ Performance-Monitoring

- Das Performance-Monitoring sammelt Werte von Host und/oder Diensten und bereitet diese zur Analyse auf. Die gesammelten Daten können entweder bei der Ursachenforschung helfen die zu einem Problem führten oder beispielsweise bei der Vorhersage der zukünftig benötigten Plattenanzahl helfen.
- Hier müssen die gesammelten Daten natürlich langfristig aufgezeichnet und aufbewahrt werden. Zum Beispiel
 - › Antwortzeiten
 - › Auslastungen

Datenspeicherung per RRD

- Die meisten Überwachungstools verwenden zum Speichern der erhobenen Roh-Daten RRD-Files. Dabei wird bereits beim Anlegen festgelegt wie viele Werte gespeichert werden sollen. Wird die maximale Anzahl der Speicherwerte erreicht, wird der erste Wert überschrieben (First in, first out). Durch Kumulierung und verschiedenen Archiven sind Speicherung und Darstellung über einen längeren Zeitraum möglich (Ungenauigkeit beachten!).



Kriterien

- Grundsätzlich bedarf es zu jeder Überwachung einiger Vorüberlegungen:
 - Was muss überwacht werden?
 - Wie kann ich es überwachen (siehe Datenerhebung)?
 - Wichtigkeit
 - Fehlertoleranz (RRD)
 - Wen interessiert das?
 - Wer muss das wissen?
 - Wie schnell MUSS ich reagieren?
 - Wie schnell kann ich reagieren?

Windows-Beispiele:

Hostgroups								Notifications		Search result hosts		All host problem		HostStatus		ServiceStatus		Hostgroups		Services for windows		
		Service		Status		Last check		Duration		Info		Output							Attempt			
Host: cerlangen-web (7 Items)																						
<input type="checkbox"/>		CPU-USAGE_WIN		OK	2015-06-23 20:55:46	3w 4d 20h 32m 7s				OK : CPU load 0%									1 / 3			
<input type="checkbox"/>		FS_PART_C_WIN		WARNING	2015-06-23 20:55:43	3d 1h 36m 51s				WARNING! SYSTEM usage: 540786/571825 ...									3 / 3			
<input type="checkbox"/>		HTTP		OK	2015-06-23 20:56:06	3w 4d 20h 32m 10s				HTTP OK: HTTP/1.1 200 OK - 955 bytes in 0.0...									1 / 3			
<input type="checkbox"/>		PAGEFILE_WIN		OK	2015-06-23 20:56:55	3w 4d 20h 31m 53s				OK! VIRTUAL usage: 5533/49129 MB (11.26%)									1 / 3			
<input type="checkbox"/>		RAM_WIN		OK	2015-06-23 20:56:15	3w 4d 20h 32m 32s				OK! Physical usage: 6508/24565 MB (26.49%)									1 / 3			
<input type="checkbox"/>		RDP		OK	2015-06-23 20:55:35	3w 4d 20h 31m 48s				TCP OK - 0.001 second response time on port ...									1 / 3			
<input type="checkbox"/>		SNMP		OK	2015-06-23 20:56:58	3w 4d 20h 32m 32s				SNMP OK - "Hardware: Intel64 Family 6 Model..."									1 / 3			
Host: clueless-mgmt.zuv (1 Item)																						
<input type="checkbox"/>		HTTPS_PORT		OK	2015-06-23 20:56:47	6w 6h 16m 53s				TCP OK - 0.001 second response time on port ...									1 / 3			
Host: clueless.zuv (5 Items)																						
<input type="checkbox"/>		CPU-USAGE_WIN		OK	2015-06-23 20:56:02	1w 5d 22h 24m 25s				OK : CPU load 0%									1 / 3			
<input type="checkbox"/>		FS_PART_C_WIN		OK	2015-06-23 20:49:50	5w 6d 14h 29m 49s				OK! SYSTEM usage: 63328/139477 MB (45.40%)									1 / 3			
<input type="checkbox"/>		PAGEFILE_WIN		OK	2015-06-23 20:56:30	1w 4d 14h 42m 4s				OK! Virtual usage: 4188/28665 MB (14.61%)									1 / 3			
<input type="checkbox"/>		RAM_WIN		OK	2015-06-23 20:56:32	1w 4d 14h 51m 15s				OK! Physical usage: 3714/14333 MB (25.91%)									1 / 3			
<input type="checkbox"/>		RDP		OK	2015-06-23 20:56:05	5w 6d 14h 39m 47s				TCP OK - 0.000 second response time on port ...									1 / 3			

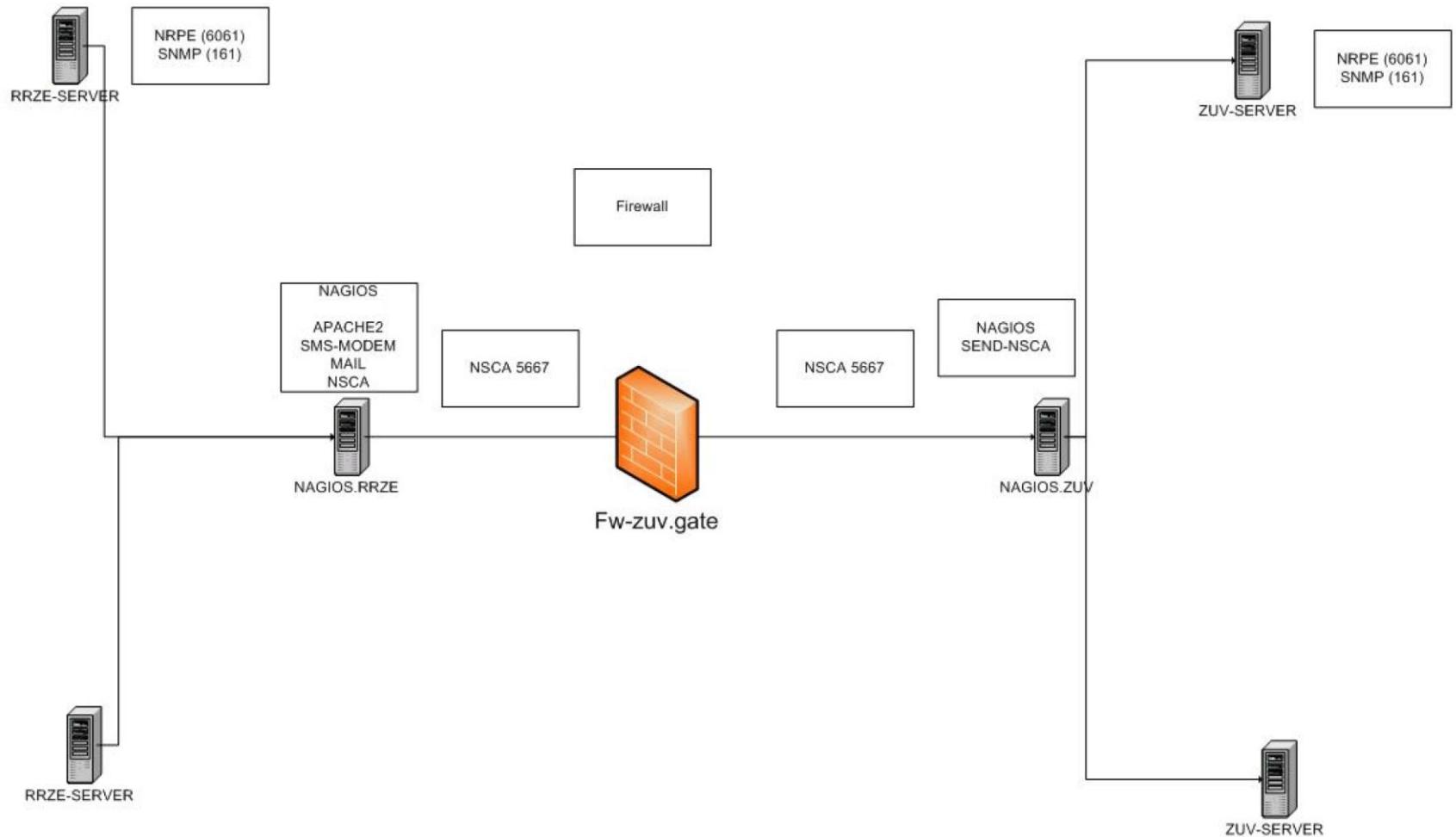
Linux-Beispiele

Service						
	Status	Last check	Duration	Info	Output	Attempt
Host: ak-prod.zuv (10 Items)						
<input checked="" type="checkbox"/>	CPU-USAGE_LX	OK	2015-06-23 20:59:06	10h 55m 52s	CPU used 1.0% (80) : OK	1 / 3
<input checked="" type="checkbox"/>	FS_ROOT_LX	OK	2015-06-23 20:59:41	22w 4d 12h 7m 45s	OK! / usage: 4000/20455 MB (19.56%)	1 / 3
<input checked="" type="checkbox"/>	LOAD_LX	OK	2015-06-23 20:59:38	20w 10h 55m 59s	Load : 0.01 0.07 0.12 : OK	1 / 3
<input checked="" type="checkbox"/>	NTP-TIME	OK	2015-06-23 20:58:48	11w 2h 23m 24s	NTP OK: Offset -0.0002554655075 secs	1 / 3
<input checked="" type="checkbox"/>	RAM_LX	OK	2015-06-23 20:59:42	21w 4d 1h 14m 19s	OK: 30 Prozent RAM sind belegt!	1 / 3
<input checked="" type="checkbox"/>	SNMP	OK	2015-06-23 20:58:50	19w 6d 4h 33m 13s	SNMP OK - Linux ak-prod 3.0.82-0.7-default #...	1 / 3
<input checked="" type="checkbox"/>	SSH	OK	2015-06-23 20:59:17	22w 4d 12h 9m 11s	SSH OK - OpenSSH_6.2 (protocol 2.0)	1 / 3
<input checked="" type="checkbox"/>	SWAP_LX	OK	2015-06-23 20:59:33	6w 5d 10h 56m 6s	OK! Swap usage: 147/4102 MB (3.58%)	1 / 3
<input checked="" type="checkbox"/>	TOTAL PROCESSES_LX	OK	2015-06-23 20:58:50	21w 4d 1h 14m 19s	SNMP OK - 95	1 / 3
<input checked="" type="checkbox"/>	TRAFFIC_ETH0_LX	OK	2015-06-23 20:58:41	1w 4d 18h 36m 30s	eth0:UP (3.0Kbps/2.7Kbps):1 UP: OK	1 / 3
Host: anyrrze1 (8 Items)						
<input checked="" type="checkbox"/>	CPU-USAGE_LX	OK	2015-06-23 20:59:20	10h 57m 57s	CPU used 10.0% (<101) : OK	1 / 3
<input checked="" type="checkbox"/>	DNS	OK	2015-06-23 20:58:33	23w 6d 11h 25m 49s	DNS OK: 0.015 seconds response time. www.g...	1 / 3
<input checked="" type="checkbox"/>	FS_ROOT_LX	OK	2015-06-23 20:58:22	15w 2d 10h 53m 4...	OK! / usage: 4027/134827 MB (2.99%)	1 / 3

Datenerhebung

- Berücksichtigung der Infrastruktur (spezielle geschützte Netze erfordern evtl. „Distributed Monitoring“).
- Je nach dem gewähltem System gibt es unterschiedliche Varianten der Datenerhebung.
 - Sammlung durch einen eigenen Client (Zabbix, Munin,...)
 - Nutzung von Standard-Diensten aus dem Netz (PING, HTTP, SSH,...)
 - Verwendung spezialisierter Dienste (SNMP, NRPE, WMI,...)

Distributed Monitoring



Abhängigkeiten

- Netzstruktur
 - Ausfall von Netzkomponenten
 - Virtualisierung
- Vorgeschaltete Dienste
 - SNMP
 - WMI
 - DNS
- Spezialfälle
 - Hochverfügbarkeit

Benachrichtigungen

- Wer?
 - Spezialisten, Servicekräfte, Kunden
- Wann?
 - 2:00 Uhr nachts, das Handy klingelt
- Wie?
 - E-Mail, SMS, WhatsApp, Web-Ansicht
- Wie Oft?
 - Einmalige Benachrichtigung oder Wiederholung
 - Eskalation (bei längerem Ausfall ohne Reaktion)
- Warum gerade so?
 - Müssen alle Dienste über eine SMS benachrichtigen, oder gibt es günstigere Alternativen?

Fehlalarme vermeiden

- Bei den verwendeten Checks darauf achten, möglichst viele Statusvarianten abzufangen (403 Forbidden-Meldung bei Webservern)
- Serviceabhängigkeiten beachten (Alle SNMP-Checks sind Critical -> SNMP-Ausfall)
- Vernünftige Schwellwerte verwenden (LOAD abhängig von Anzahl der Prozessorkerne)
- Wartungsarbeiten eintragen
- Sinnvolle Checks verwenden (große Festplatten-Belegung in Prozent oder CPU-Last hoch ohne Cachenutzung)
- Sinnvolle Benachrichtigungswerte wählen

Welche Monitoringtools gibt es?

- Funktionalitätsmonitoring
 - Nagios/Icinga (<http://www.icinga.org>),
 - WhatsUP (<http://www.whatsupgold.com>),
 - Zabbix (<http://www.zabbix.com>)
- Performancemonitoring
 - MRTG (<http://oss.oetiker.ch/mrtg/>),
 - Munin (<http://munin-monitoring.org>),
 - Cacti (<http://www.cacti.net>)
- Spezialisten
 - HP Openview
 - Microsoft SCOM (System Center Operations Manager)

RRZE-Veranstaltungskalender & Mailingliste

Kalender abonnieren oder bookmarken

- Alle Infos hierzu stehen auf der Webseite des RRZE unter:
<http://www.rrze.fau.de/news/kalender.shtml>

Mailingliste abonnieren

- Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste [RRZE-Aktuelles](#) gesendet.
- Auch diese Liste kann man abonnieren:
<https://lists.fau.de/mailman/listinfo/rrze-aktuelles>

Themenvorschläge & Anregungen

- Themenvorschläge und Anregungen nehmen wir gerne entgegen!
- Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Systemausbildung)