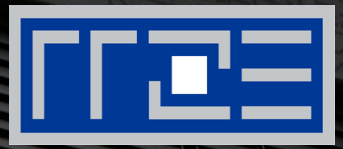
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Systemüberwachung / Monitoring

Systemausbildung − Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten

Uwe Scheuerer, RRZE, 24.06.2015

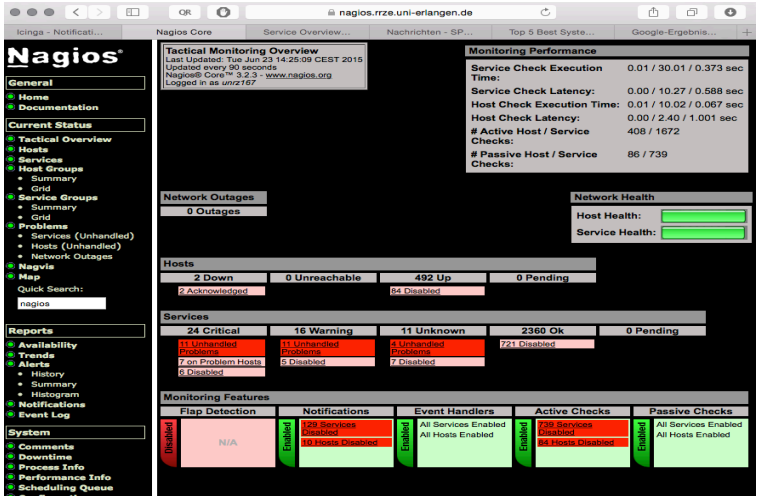
FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

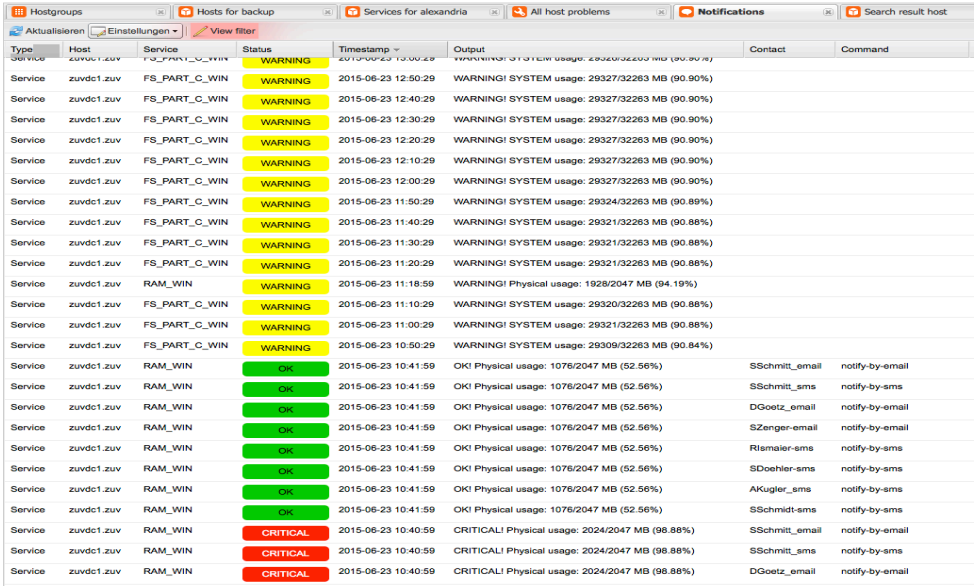
Agenda

- Wozu Monitoring?
- Unterscheidung
  - Funktionalitäts-Monitoring
  - Performance-Monitoring
- Kriterien
- Datenerhebung
- Abhängigkeiten
- Benachrichtigungen
  - Fehlalarme vermeiden
- Ein paar Monitoringtools
- Icinga und Munin am RRZE

Wozu Monitoring?

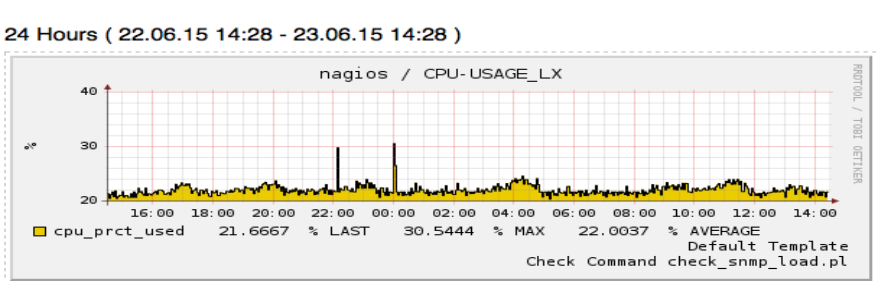
- Zeitnahe akute Problemerkennung
  - Schnelle Reaktion
  - Passende Benachrichtigung

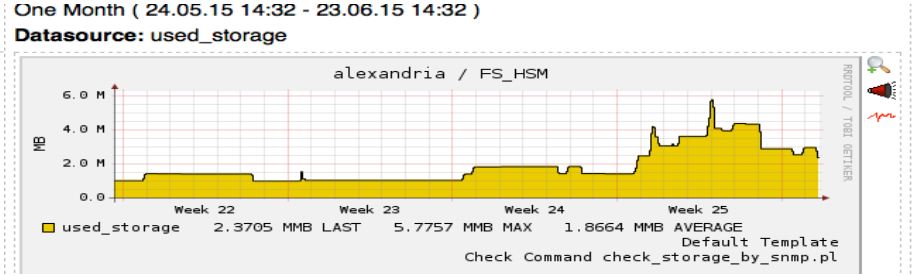




Wozu Monitoring?

- 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 Administratoren, Kunden und Servicekräften bei
    - Ausfällen von Hosts
    - Ausfällen von Services

Funktionalitäts-Monitoring

- Die gesammelten Daten werden hinsichtlich gesetzter Schwellwerte geprüft
- Warnmeldungen werden über unterschiedliche Wege an festgelegte Personen oder Gruppen gesendet.
- Eine dauerhafte Speicherung der Rohdaten ist nicht zwingend notwendig
- Die aktuellen Werte werden meist in einfachen Dateien gespeichert

Performance-Monitoring

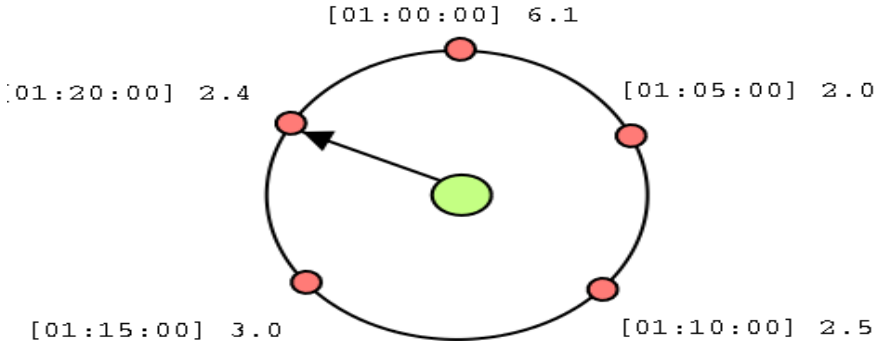
- Das Performance-Monitoring sammelt Werte von Host und/oder Diensten und bereitet diese zur Analyse auf
- Verwendung der gesammelten Daten zur Ursachenforschung bei Problemen
- Hilfe zur Vorhersage der zukünftig benötigten Ressourcen (Platten, Speicher, etc.)

Performance-Monitoring

- Die gesammelten Daten müssen langfristig aufgezeichnet und aufbewahrt werden. Zum Beispiel
  - Latenzzeiten (RTT, HTTP-Requests...)
  - Auslastungen (RAM, CACHE, CPU...)
  - Anzahl verschickter SMs

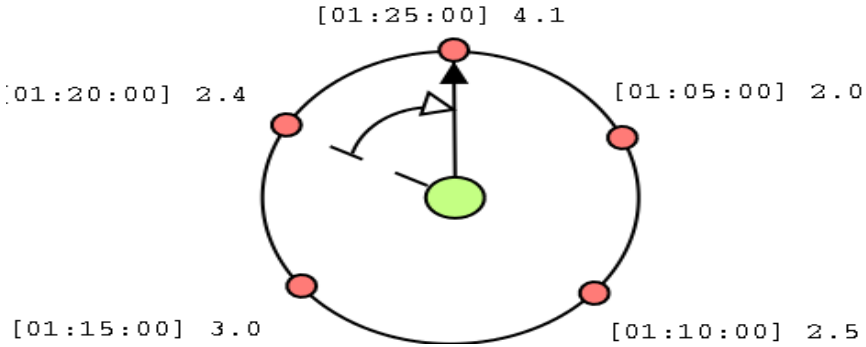
Datenspeicherung per RRD

- Die meisten Überwachungstools verwenden zum Speichern der erhobenen Roh-Daten RRD-Files. Dabei werden bereits beim Anlegen festgelegt wie viele Werte gespeichert werden sollen.



Datenspeicherung per RRD 2

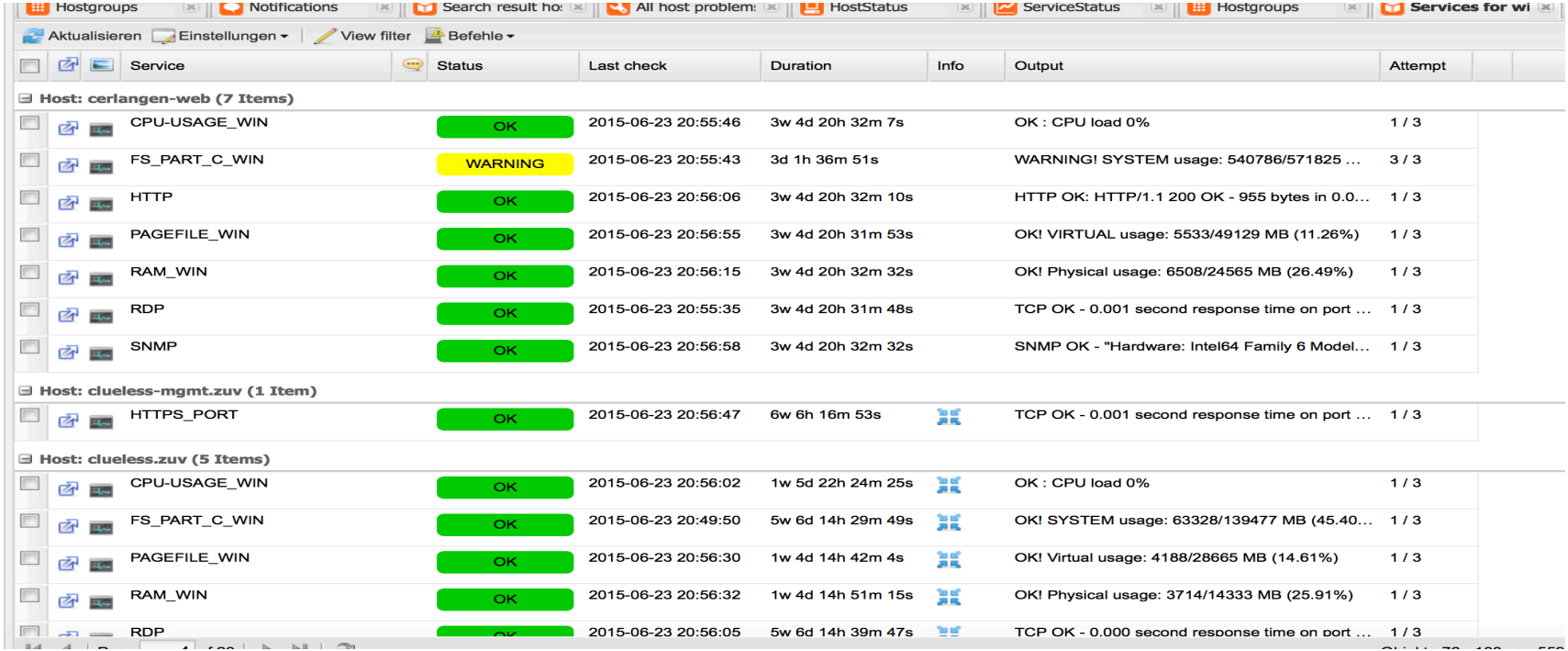
- Ist die maximale Anzahl der Speicherwerte erreicht, wird der erste Wert überschrieben (First in, first out). Durch Kummulierung und der Verwendung verschiedener Archiven sind Speicherung und Darstellung über einen längeren Zeitraum möglich (Ungenauigkeit beachten!).



Kriterien

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

Windows-Beispiele:

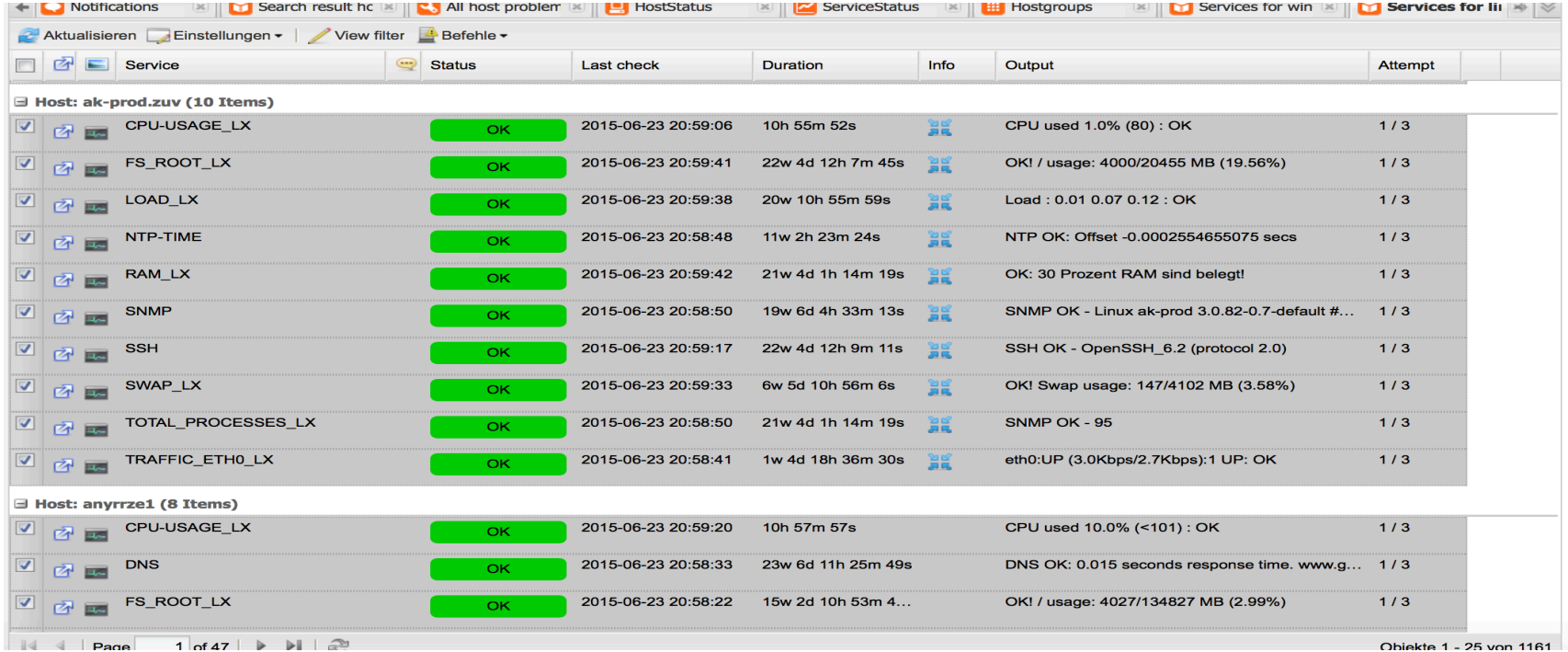


Hostgroups | Notifications | Search result ho: | All host problem: | HostStatus | ServiceStatus | Hostgroups | Services for wi

Aktualisieren | Einstellungen | View filter | Befehle

Service	Status	Last check	Duration	Info	Output	Attempt
Host: cerlangen-web (7 Items)						
CPU-USAGE_WIN	OK	2015-06-23 20:55:46	3w 4d 20h 32m 7s		OK : CPU load 0%	1 / 3
FS_PART_C_WIN	WARNING	2015-06-23 20:55:43	3d 1h 36m 51s		WARNING! SYSTEM usage: 540786/571825 ...	3 / 3
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
PAGEFILE_WIN	OK	2015-06-23 20:56:55	3w 4d 20h 31m 53s		OK! VIRTUAL usage: 5533/49129 MB (11.26%)	1 / 3
RAM_WIN	OK	2015-06-23 20:56:15	3w 4d 20h 32m 32s		OK! Physical usage: 6508/24565 MB (26.49%)	1 / 3
RDP	OK	2015-06-23 20:55:35	3w 4d 20h 31m 48s		TCP OK - 0.001 second response time on port ...	1 / 3
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)						
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)						
CPU-USAGE_WIN	OK	2015-06-23 20:56:02	1w 5d 22h 24m 25s		OK : CPU load 0%	1 / 3
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
PAGEFILE_WIN	OK	2015-06-23 20:56:30	1w 4d 14h 42m 4s		OK! Virtual usage: 4188/28665 MB (14.61%)	1 / 3
RAM_WIN	OK	2015-06-23 20:56:32	1w 4d 14h 51m 15s		OK! Physical usage: 3714/14333 MB (25.91%)	1 / 3
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

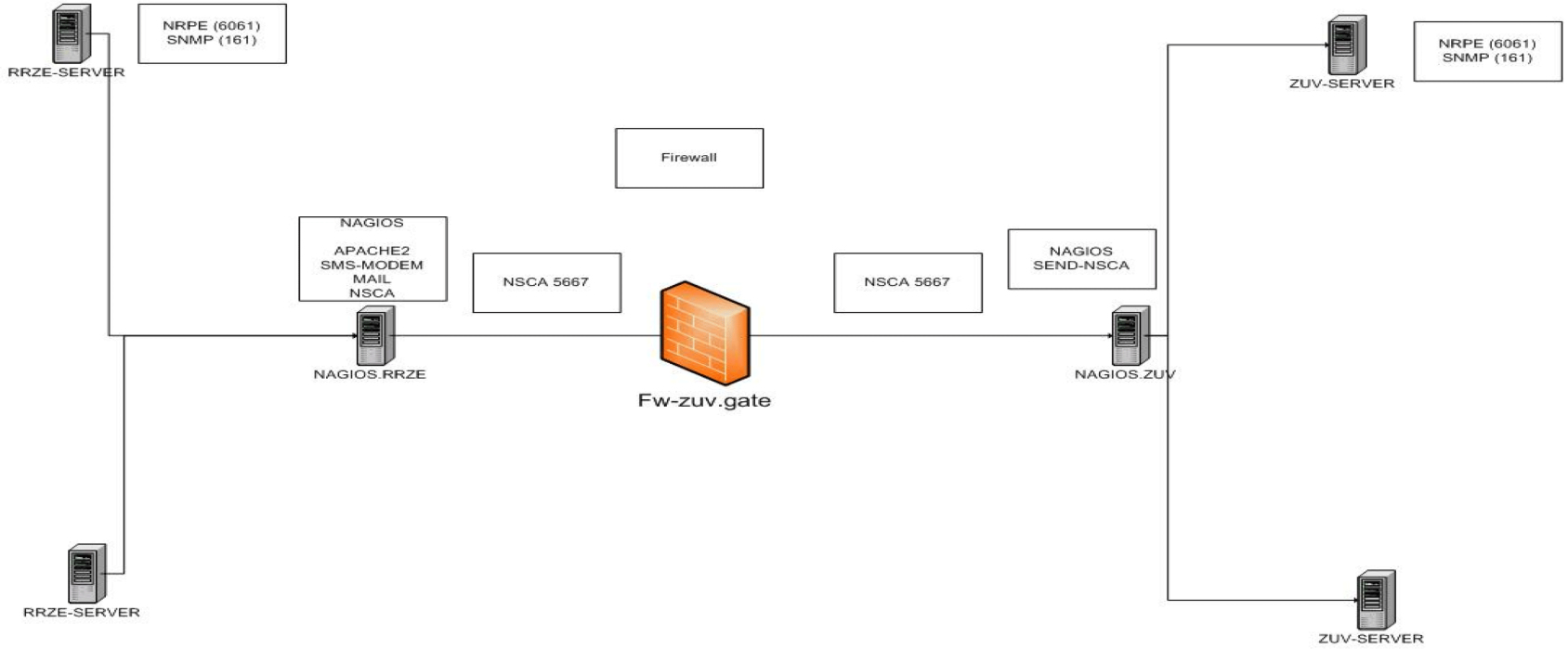


Service	Status	Last check	Duration	Info	Output	Attempt
Host: ak-prod.zuv (10 Items)						
CPU-USAGE_LX	OK	2015-06-23 20:59:06	10h 55m 52s		CPU used 1.0% (80) : OK	1 / 3
FS_ROOT_LX	OK	2015-06-23 20:59:41	22w 4d 12h 7m 45s		OK! / usage: 4000/20455 MB (19.56%)	1 / 3
LOAD_LX	OK	2015-06-23 20:59:38	20w 10h 55m 59s		Load : 0.01 0.07 0.12 : OK	1 / 3
NTP-TIME	OK	2015-06-23 20:58:48	11w 2h 23m 24s		NTP OK: Offset -0.0002554655075 secs	1 / 3
RAM_LX	OK	2015-06-23 20:59:42	21w 4d 1h 14m 19s		OK: 30 Prozent RAM sind belegt!	1 / 3
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
SSH	OK	2015-06-23 20:59:17	22w 4d 12h 9m 11s		SSH OK - OpenSSH_6.2 (protocol 2.0)	1 / 3
SWAP_LX	OK	2015-06-23 20:59:33	6w 5d 10h 56m 6s		OK! Swap usage: 147/4102 MB (3.58%)	1 / 3
TOTAL_PROCESSES_LX	OK	2015-06-23 20:58:50	21w 4d 1h 14m 19s		SNMP OK - 95	1 / 3
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)						
CPU-USAGE_LX	OK	2015-06-23 20:59:20	10h 57m 57s		CPU used 10.0% (<101) : OK	1 / 3
DNS	OK	2015-06-23 20:58:33	23w 6d 11h 25m 49s		DNS OK: 0.015 seconds response time. www.g...	1 / 3
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

- 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, SNMP,...)
  - Verwendung spezialisierter Dienste (NRPE, WMI,...)
- Berücksichtigung der Infrastruktur (spezielle geschützte Netze erfordern evtl. „Distributed Monitoring“).

Distributed Monitoring



Abhängigkeiten

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

Abhängigkeiten

- Hochverfügbarkeit
  - Erfordert mehrfache Überwachung
    - Host und Dienst-Verfügbarkeit auf den echten Servern
    - Host und Dienst-Verfügbarkeit auf der Cluster-Adresse
- Komplexere Systeme:
  - Abhängigkeiten zwischen unterschiedlichen Host
  - Voneinander abhängige Applikationen oder Services

Benachrichtigungen

- Wer?
  - Spezialisten, Servicekräfte, Kunden
- Wann?
  - 2:00 Uhr nachts, das Handy klingelt
- Wie?
  - E-Mail, SMS, WhatsApp, Web-Ansicht

Benachrichtungen

- 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 Prozessorkernen)

Fehlalarme vermeiden

- Wartungsarbeiten eintragen
- Sinnvolle Checks verwenden (große Festplatten Belegung in Prozent)
- Sinnvolle Benachrichtigungswerte wählen

Beispiele für Funktionalitäts-Monitoring

- Nagios/Icinga www.icinga.org
- WhatsUP www.whatsupgold.com
- Zabbix www.zabbix.com

Beispiele Performance-Monitoring

- MRTG http://oss.oetiker.ch/mrtg/
- Munin http://munin-monitoring.org
- Cacti www.cacti.net

Herstellerspezifische Tools

- HP OpenOne
  - support.openview.hp.com/downloads.jsp
- Microsoft SCOM (System Center Operations Manager)
  - technet.microsoft.com/de-de/systemcenter/bb497976.aspx

ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge zur „Systemausbildung

29.04.2015 − Geschichte der Betriebssysteme
06.05.2015 − Unixoide Betriebssysteme (Unix, Linux, OS X)
13.05.2015 − Windows-Betriebssysteme
20.05.2015 − Benutzerverwaltung: LDAP
27.05.2015 − Benutzerverwaltung: MS Active Directory
03.06.2015 − Storage / Filesysteme
10.06.2015 − Virtualisierung
17.06.2015 − Backup / Archiv
24.06.2015 − Systemüberwachung, Monitoring
01.07.2015 − High Performance Computing
08.07.2015 − IT-Sicherheit

- Immer mittwochs (ab 14 c.t.),
- Raum 2.049 im RRZE

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
- Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
- stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

http://www.rrze.fau.de/news/systemausbildung.shtml

RRZE-Veranstaltungskalender & Mailinglisten

- 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)