Neuigkeiten in Check MK

Teil 2

Event Console
Livestatus
Multisite
BI
Check Plugins

24. Oktober 2014

Mathias Kettner
Kellerstr. 29
81667 München
Tel. 089 / 444 09 662

www.mathias-kettner.de

© 2014 Mathias Kettner

Titelbild Image courtesy of Mike Trenchard, Earth Sciences & Image Analysis Laboratory, Johnson Space Center.

ÜBERSICHT

1 Neuigkeiten II
2 EC: Aktionen
3 EC: States
4 Zugriffsrechte für Rollen
5 Timeranges für Graph Search
6 Quicksearch
7 Multisite Virtual Host Trees
8 Kommandos
9 Livestatus und Nagios 4
10 Windows Agent
11 Monitoring von VMware ESX
12 Fibre Channel Checks
13 HW/SW-Inventory

1 Neuigkeiten in Check MK

Alle Rechte an diesen Unterlagen liegen bei Mathias Kettner, Kellerstr. 29, 81667 München. Vervielfältigung oder Reproduktion – auch auszugsweise – nur mit vorheriger schriftlicher Genehmigung. Die Nutzung ist beschränkt auf die Unterrichtsbegleitung für die von Mathias Kettner veranstaltete Schulung und deren spätere persönliche Nutzung durch die Teilnehmer. Insbesondere ist eine Nutzung der Unterlagen für weitere Schulungen oder ähnliche Veranstaltungen untersagt. Diese Unterlagen sind nur original mit Deckblatt, Datumshinweis, in Farbe und auf 200-Gramm Papier. Melden Sie unerlaubte Kopien oder einen anderen Verstoß gegen das Urheberrecht bitte per Telefon unter 089 / 18 90 4210 oder per Email an mk@mathias-kettner.de.

1. Neuigkeiten II

neuigkeitenII

Zweiter Teil der Neuerungen:

- Event Console
- Multisite
- Livestatus
- Windows-Agent
- ESX-Monitoring
- Fibre Channel Checks
- andere Check Plugins

2. EC: Aktionen

cmk_ec_aktionen

Aktionen für der Eventkonsole:

- Verschicken von E-Mails
- Ausführen beliebiger Skripte
- NEU ab 1.2.5i6:
  Weiterleitung an die Rule Based Notifications

Wann:

- wenn ein Event erzeugt wird
- NEU ab 1.2.5i6: wenn ein Event ge-cancelt wird

3. EC: States

cmk_ec_states

Auswahl in Regel unter "Outcome & Action":

- Festes Setzen auf OK, WARN, CRIT, UNKNOWN
- Durch Syslog Severity
- NEU ab 1.2.5i4:
  durch Pattern Matching auf Message Text,
  eigene Patterns für OK, WARN, CRIT

4. Zugriffsrechte für Rollen

new_role_permissions

Neuerungen seit 1.2.5i1 in "Roles & Permissions"

Event Console

- "Roles & Permissions" → "Event Console"
- "See all events = NO":
  Benutzer kann nur Events zu Hosts sehen,
  für die er auch Kontakt ist
- "See events not related to a known host":
  Sichtbarkeit, wenn Host unbekannt ist
- Zusätzlich in Regel "Fallback Contact Groups":
  Kontaktgruppen für unbekannte Hosts

Dashboards

- "Roles & Permissions" → "Dashboards"
- Zugriff auf Dashboard für Rolle erlauben/verbieten
- Default ist "erlauben"
- Einzeln für jedes Dashboard

Eigene Views

- "Roles & Permissions" → "Multisite Views"
- Eigene Views tauchen automatisch auf
- Zugriff für Rolle erlauben/verbieten
- Default ist "erlauben"
- Besitzer des View kann immer zugreifen.

5. Timeranges für Graph Search

new_graph_timerange

Time Ranges im PNP Graph Search

- "Views" → "Addons" → "Search Graphs"
- Icon Displayeinstellungen:
- Auswahl: heute, gestern, diese Woche, letzte Woche, ...
- Beliebige Anfangs- und End-Zeiten

6. Quicksearch

wato_quicksearch

Quicksearch

- Sidebar Snapin
-

- Suche mit Auto-Kompletierung
- ☞ nach Hosts
- ☞ nach Services
- Keyword `s:` ☞ nur nach Services
- Keyword `h:` ☞ nur nach Hosts
- Keyword `sg:` und `hg:` Service- und Hostgruppen
- Neu seit 1.2.5i1: mehrere Kombinationen von Keywords möglich

Alle Rechte an diesen Unterlagen liegen bei Mathias Kettner, Kellerstr. 29, 81667 München. Vervielfältigung oder Reproduktion – auch auszugsweise – nur mit vorheriger schriftlicher Genehmigung. Die Nutzung ist beschränkt auf die Unterrichtsbegleitung für die von Mathias Kettner veranstaltete Schulung und deren spätere persönliche Nutzung durch die Teilnehmer. Insbesondere ist eine Nutzung der Unterlagen für weitere Schulungen oder ähnliche Veranstaltungen untersagt. Diese Unterlagen sind nur original mit Deckblatt, Datumshinweis, in Farbe und auf 200-Gramm Papier. Melden Sie unerlaubte Kopien oder einen anderen Verstoß gegen das Urheberrecht bitte per Telefon unter 089 / 18 90 4210 oder per Email an mk@mathias-kettner.de.

7. Multisite Virtual Host Trees

`multisite_virtualhost_trees`

Virtual Host Trees

- Sidebar Snapin
- Baum basierend auf Host Tags aufbauen
- Bäume konfigurierbar in `global settings` → `Status GUI (Multisite)` → `Virtual Host Trees`
- In Snapin zwischen Bäumen wechseln

8. Kommandos

`multisite_commands`

Sinn von Kommandos

Steuerung des Monitoring, z. B.

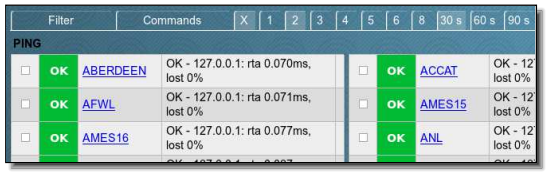
- Bestätigen von Problemen (Acknowledge)
- Setzen von geplanten Wartungszeiten (Downtimes)
- Hinzufügen von Kommentaren
- Tests, etc.
- Kommando bezieht sich auf Objekt (Host, Service, ...)

Filtern / Auswahl

Auswahl der Objekte für ein Kommando:

- Host/Service-Detail aufrufen (Einzeldatensatz)
- In der View filtern

- Checkboxen aktivieren...



- Quicksearch

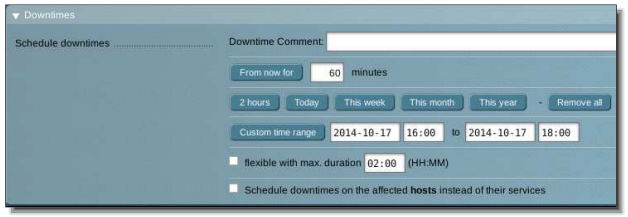
Kommandos

Kommandos auf Services

Neu in 1.2.5i6

- Aktive Checks über Zeit verteilen

Downtimes



Downtimes auf Services

Neu in 1.2.5i6:

- Downtime auf Host statt auf Service setzen

Neu in 1.2.5i6:

- History of scheduled downtimes in den Views

9. Livestatus und Nagios 4

`livestatus_nagios4`

- Neu mit 1.2.5i1:
- Livestatus ist alternativ für Nagios 3 oder 4 kompilierbar
- `setup.sh` erkennt Nagios Version automatisch
- manuell: `configure --with-nagios4`

10. Windows Agent

`new_windows_agent`

MSI-Installer

- Neu in 1.2.5i5
- ausgeliefert mit OMD
- wählt automatisch die richtige Architektur (32/64bit)
- installiert immer in Programme(x86)

Logwatch: Kein Kontext in Logfiles

- Neu in 1.2.5i6
- Option `nocontext` nun auch im Windows Logwatch

Alle Rechte an diesen Unterlagen liegen bei Mathias Kettner, Kellerstr. 29, 81667 München. Vervielfältigung oder Reproduktion – auch auszugsweise – nur mit vorheriger schriftlicher Genehmigung. Die Nutzung ist beschränkt auf die Unterrichtsbegleitung für die von Mathias Kettner veranstaltete Schulung und deren spätere persönliche Nutzung durch die Teilnehmer. Insbesondere ist eine Nutzung der Unterlagen für weitere Schulungen oder ähnliche Veranstaltungen untersagt. Diese Unterlagen sind nur original mit Deckblatt, Datumshinweis, in Farbe und auf 200-Gramm Papier. Melden Sie unerlaubte Kopien oder einen anderen Verstoß gegen das Urheberrecht bitte per Telefon unter 089 / 18 90 4210 oder per Email an mk@mathias-kettner.de.

- Beispiel in `check_mk.ini`:
  `textfile = nocontext C:\tmp\memo.udf`
- sendet nur Logzeilen mit Match, nicht ganzen Kontext

MRPE Include Files

- Neu in 1.2.5i1
- Unterstützung von Include Files für MRPE
- Zusätzliche Konfig-Files in `check_mk.ini` angeben
- `include \\ab = C:\includes\ab-mrpe.cfg`
- enthalten wiederum MRPE Konfiguration
- ausgeführt als anderer Benutzer

Include Files für Plugins/Localchecks

- Neu in 1.2.5i3
- Unterstützung von Include Files für Plugins
- Zusätzliche Konfig-Files in `check_mk.ini` angeben
- `include \\ab = C:\includes\ab-plugin`
- sowohl plugins als auch localchecks
- ausgeführt als anderer Benutzer

andere Neuigkeiten

- Agent liefert erweiterte Prozess-Informationen: kein psperf.bat mehr notwendig
- Performance Counter können mit Namen angegeben werden
- Logwatch kann Unicode Logfiles verarbeiten
- Agent sendet Environment-Variablen an plugins:
- `PLUGINSDIR, LOCALDIR, SPOOLDIR,`
- `MK_CONFIGDIR, REMOTE_HOST`

11. Monitoring von VMware ESX

`cmk_check_esx`

Überwachung von VMware ESX schwierig:

- Kein Agent installierbar seit Version > 3
- SNMP instabil, nicht supported und sehr mager
- stattdessen XML/HTTP basierte API vorhanden

Bestehende Plugins wie `check_vmware_api.pl` sind:

- umständlich zu konfigurieren
- und vor allen: **extrem CPU-fressend**

Check_MK hat nun den `agent_vsphere`:

- in Python implementiert
- läuft als „Data Source Program“
- checks kompletten ESX host in einem Durchlauf
- eigene API-Implementierung → extrem schnell
- Neu in 1.2.5i6: nochmals Steigerung um Faktor 40-200
- direkt konfigurierbar über WATO-Regel

Einrichten des ESX-Monitorings:

1. Monitoring-Benutzer auf VMware einrichten
2. per WATO für alle Hostsystem eine Regel einrichten
   → *Check state of VMWare ESX via vSphere*
3. VMs mit ESX-Namen als Hosts in Check_MK einrichten
4. Check_MK-Agent auf den VMs ist optional

Umfang der aktuellen Implementierung:

- Hardwareüberwachung der Hostsysteme
- CPU und Speicher von Hosts und VMs
- Datastores
- Netzwerkkarten, RAM-Disks, etc.

Hostsystem-Überwachung

Check `esx_vsphere_hostsystem` mit Subchecks:

- CPU
- Memory & Cluster-Memory
- Overall State
- Neu in 1.2.5i6: Maintenance-Mode
- Neu in 1.2.5i3: Multipath-IO Status

Counters

Check `esx_vsphere_counters` mit Subchecks:

- Disk IO (1.2.5i1: auch Latency)
- Network Interfaces
- Uptime
- Neu in 1.2.5i1: Ramdisks

VMs

Check `esx_vsphere_vm` mit Subchecks:

- CPU
- Memory
- Name
- Heartbeat Status
- Neu in 1.2.5i1: Runtime Host
- Neu in 1.2.5i1: Datastores
- Neu in 1.2.5i1: Guest Tool Status

Datastores

Check `esx_vsphere_datastores`:

- Füllstand in % und GB
- uncommitted
- provisioning %

Neu in 1.2.5i6: Lizenzen

Check `esx_vsphere_licenses`:

- Zahl der verbrauchten Lizenzen
- Gesamtzahl der Lizenzen
- Levels für Alarmierung

Sensoren

Check `esx_vsphere_sensors`:

- Hardware-Sensoren
- z.B. Power Supplies

Alle Rechte an diesen Unterlagen liegen bei Mathias Kettner, Kellerstr. 29, 81667 München. Vervielfältigung oder Reproduktion – auch auszugsweise – nur mit vorheriger schriftlicher Genehmigung. Die Nutzung ist beschränkt auf die Unterrichtsbegleitung für die von Mathias Kettner veranstaltete Schulung und deren spätere persönliche Nutzung durch die Teilnehmer. Insbesondere ist eine Nutzung der Unterlagen für weitere Schulungen oder ähnliche Veranstaltungen untersagt. Diese Unterlagen sind nur original mit Deckblatt, Datumshinweis, in Farbe und auf 200-Gramm Papier. Melden Sie unerlaubte Kopien oder einen anderen Verstoß gegen das Urheberrecht bitte per Telefon unter 089 / 18 90 4210 oder per Email an mk@mathias-kettner.de.

12. Fibre Channel Checks

`cmk_brocade_fcport`

Fibre Channel Interfaces

- Bei Brocade Devices
- Aber auch von HP, Dell, etc.
- Monitoring per snmp über Standard IF-MIB
- → if64 check
- passt nicht besonders gut

Brocade Fibre Channel Check

- `brocade_fcport`
- Gibt es schon seit 2011
- Benutzt die FC Switch MIB
- Status, Durchsatz und Fehler auf FC Interfaces
- spezifisch für Fibre Channel
- proprietär für Brocade

`brocade_fcport` Neuigkeiten

- Neu mit 1.2.5i6
- Inventur-Regel auf physikalischen, operationellen und administrativen Status der Interfaces
- Update auf neue Interface-Geschwindigkeiten bis 16Gbit/sec
- Bugfix für ISL-Speed Berechnung

FC Port Check

- Neu in 1.2.5i4: `fc_port` Check
- Benutzt die FibreAlliance/FCMGMT-MIB
- von div. Fibre Channel Devices unterstützt
- Status, Durchsatz und Fehler auf FC Interfaces
- spezifisch für Fibre Channel
- ähnlich dem `brocade_fcport` Check

Brocade und die FibreAlliance MIB

- seit FabricOS 7 wird auch FCMGMT-MIB unterstützt
- → 3 MIBS unterstützt
- → 3 Checks pro Interface möglich
- → potentielle Konflikte
- 1.2.5i5: `fc_port` aus Inventur rausgenommen
- seit 1.2.5i6: cfc˙port wird nur benutzt, wenn `brocade_fcport` nicht unterstützt wird

13. HW/SW-Inventory

`cmk_hwswinventory`

Die Idee

- Agenten liefern bereits Info über Hardware
- Beispiele: Festplatten, Memory
- Diesen kann man nutzen und erweitern mit:
- eigenen Plugins für HW/SW-Informationen
- eigenen Inventurchecks
- eigenen Views in Multisite

Das Inventory liefert

- Hardwareinformationen:
- → BIOS, CPU, Speicher, Controller ...
- Softwareinformationen:
- → Betriebssystem, installierte Pakete ...

Installation auf Linux

❶ Monitoring-Server: `mk_inventory.linux` aus `~/share/check_mk/agents/plugins`
❷ nach `/usr/lib/check_mk_agent/plugins` auf Zielsystem kopieren

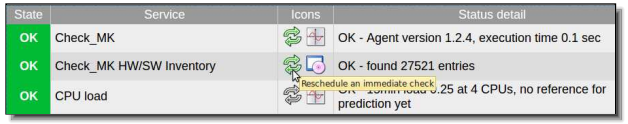
Installation auf Windows

❶ Monitoring-Server: `mk_inventory.ps1` aus `~/share/check_mk/agents/windows/plugins`
❷ nach `\Programme(x86)\check_mk\plugins` auf Zielsystem kopieren
❸ Agent-Service durchstarten

Inventory aktivieren

- WATO → Host and Service Parameters
- Hardware/Software-Inventory
- Regel "Do hardware/software inventory" anlegen

☞ Es wird ein neuer aktiver Check erzeugt



☞ Symbol in Hostansicht verlinkt auf Inventory

Check-Intervall

Problem:

- Daten würden minütlich mit Agenten-Daten geholt
- grosse Datenmenge
- belastet das Zielsystem

☞ will man nicht

Inventur-Intervall

Lösung:

- Check-Plugin sendet Daten nicht jedes Mal
- sondern alle (z.B.) 4 Stunden
- Inventur-Check kann damit umgehen:
- Daten werden zwischengespeichert

Alle Rechte an diesen Unterlagen liegen bei Mathias Kettner, Kellerstr. 29, 81667 München. Vervielfältigung oder Reproduktion – auch auszugsweise – nur mit vorheriger schriftlicher Genehmigung. Die Nutzung ist beschränkt auf die Unterrichtsbegleitung für die von Mathias Kettner veranstaltete Schulung und deren spätere persönliche Nutzung durch die Teilnehmer. Insbesondere ist eine Nutzung der Unterlagen für weitere Schulungen oder ähnliche Veranstaltungen untersagt. Diese Unterlagen sind nur original mit Deckblatt, Datumshinweis, in Farbe und auf 200-Gramm Papier. Melden Sie unerlaubte Kopien oder einen anderen Verstoß gegen das Urheberrecht bitte per Telefon unter 089 / 18 90 4210 oder per Email an mk@mathias-kettner.de.

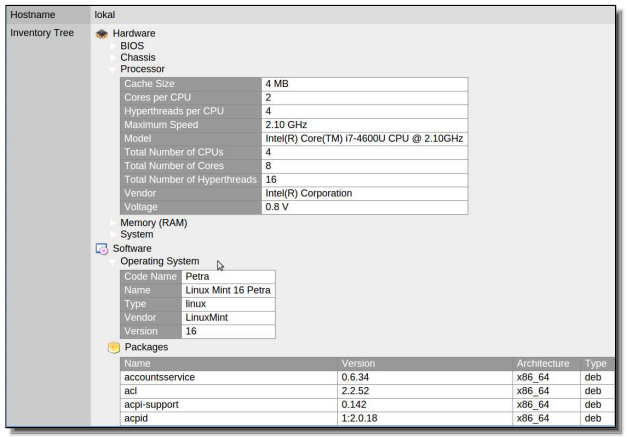
- erst nach (z.B.) 4 Stunden sind die Daten ungültig

Inventur-Plugin Detail

- Gesendete Sektionen haben "persist"-Keyword:

```
<<<lnx_uname:persist(1413748128)>>>
x86_64
3.10.17
```

- zeigt an, bis wann die Sektion gültig ist

Inventur-Checks Detail

- Sektionen mit "persist" Keyword werden gespeichert in `~var/check_mk/persisted/`hostname
- Inventur-Checks liegen in `~share/check_mk/inventory/`sektion
- Verarbeiten Inventur-Sektionen
- Legen prozessierte Daten ab in `~var/check_mk/inventory/`hostname
- diese werden in Multisite angezeigt