

CHECK_MK

CONFERENCE #3



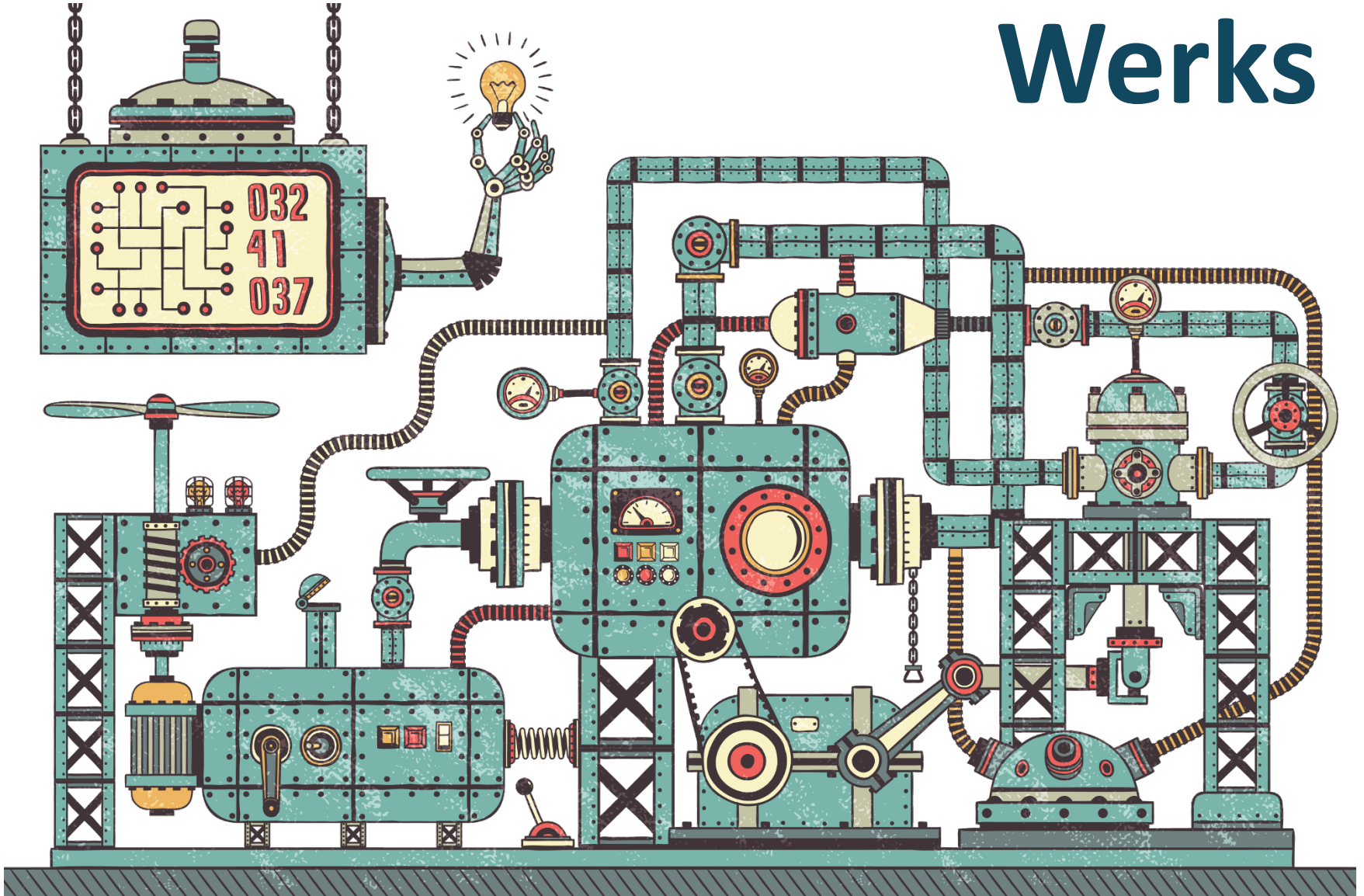
CHECK_MK
CONFERENCE #3

News in the Event Console

Mathias Kettner



Werks



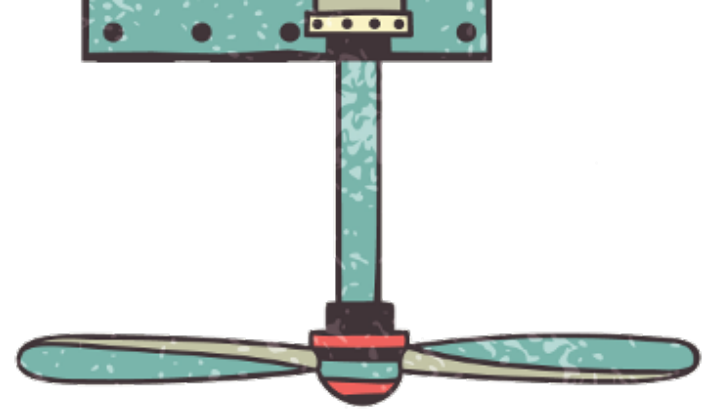
New Feature-Werks

#3720

#4154 #3388 #3887 #3971 #3861 #4151

#4276 #2903 #3717 #2974 #3656 #3262
#4148 #3390 #4132 #3736 #3716 #4166
#3539 #4286 #4277 #2999 #2733 #1306





Werk #3720

Distributed Setups





Situation in 1.2.8

- GUI always accesses the local Event Console
- This limits you to one Event Console!



Problems with this approach

- Does not scale well
- Networking problems may arise
- EC has no information about the hosts



NEW in 1.4.0:

Distributed EC via Livestatus

- GUI accesses ECs via Livestatus
- Livestatus is handled by CMC / Nagios
- CMC / Nagios accesses local EC



Advantages:

- scales better
- no Syslog/SNMP over WAN necessary
- EC has access to host information



Visibility in status GUI



- use host information:
 - information about contact groups



Check_MK-Notifications by EC



- uses host information:
 - correct host name and alias
 - primary IP address
 - WATO folder and host tags
 - contacts and contact groups
 - Host scheduled downtime





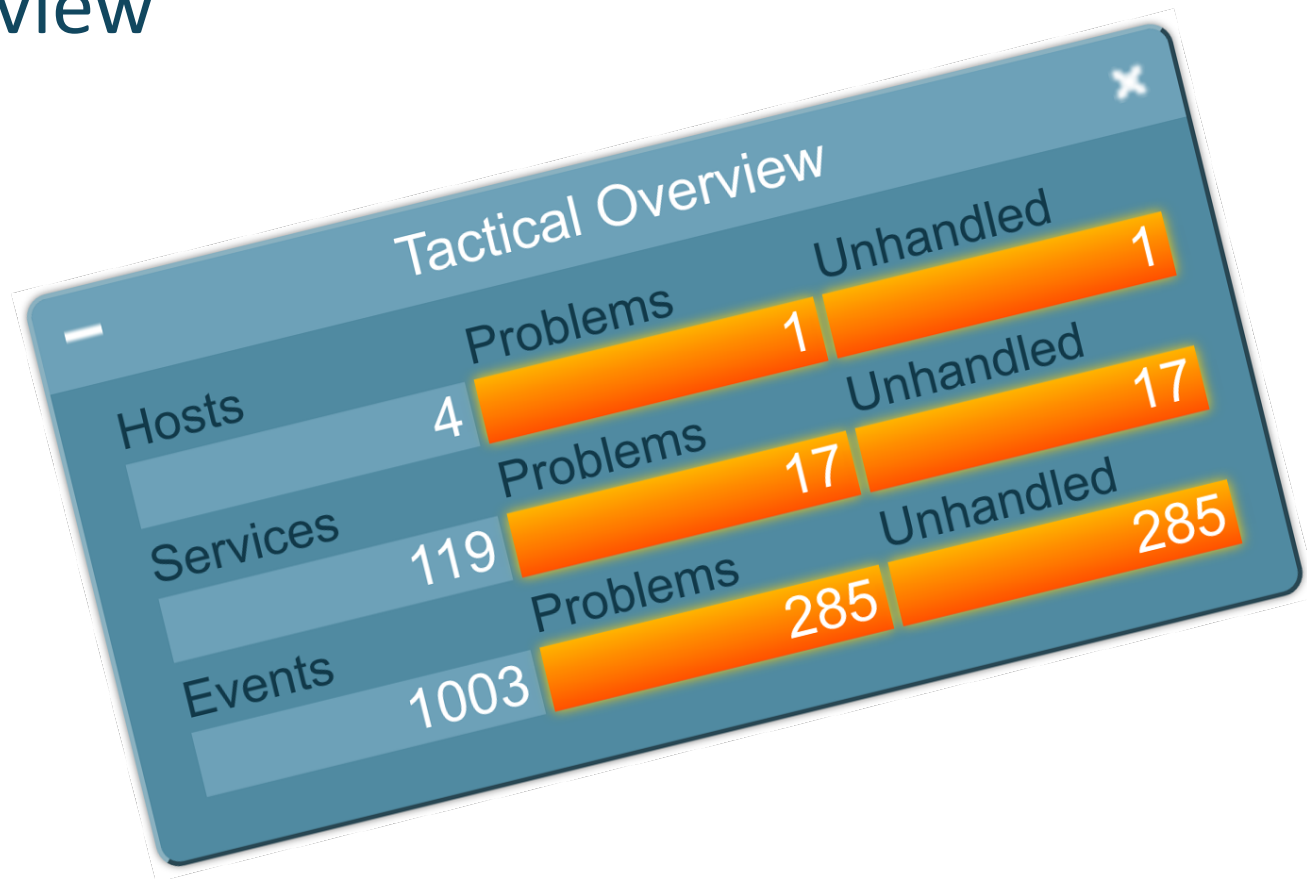
Werk #3971

Tactical Overview



Werk #3971

Events are now being shown in Tactical Overview





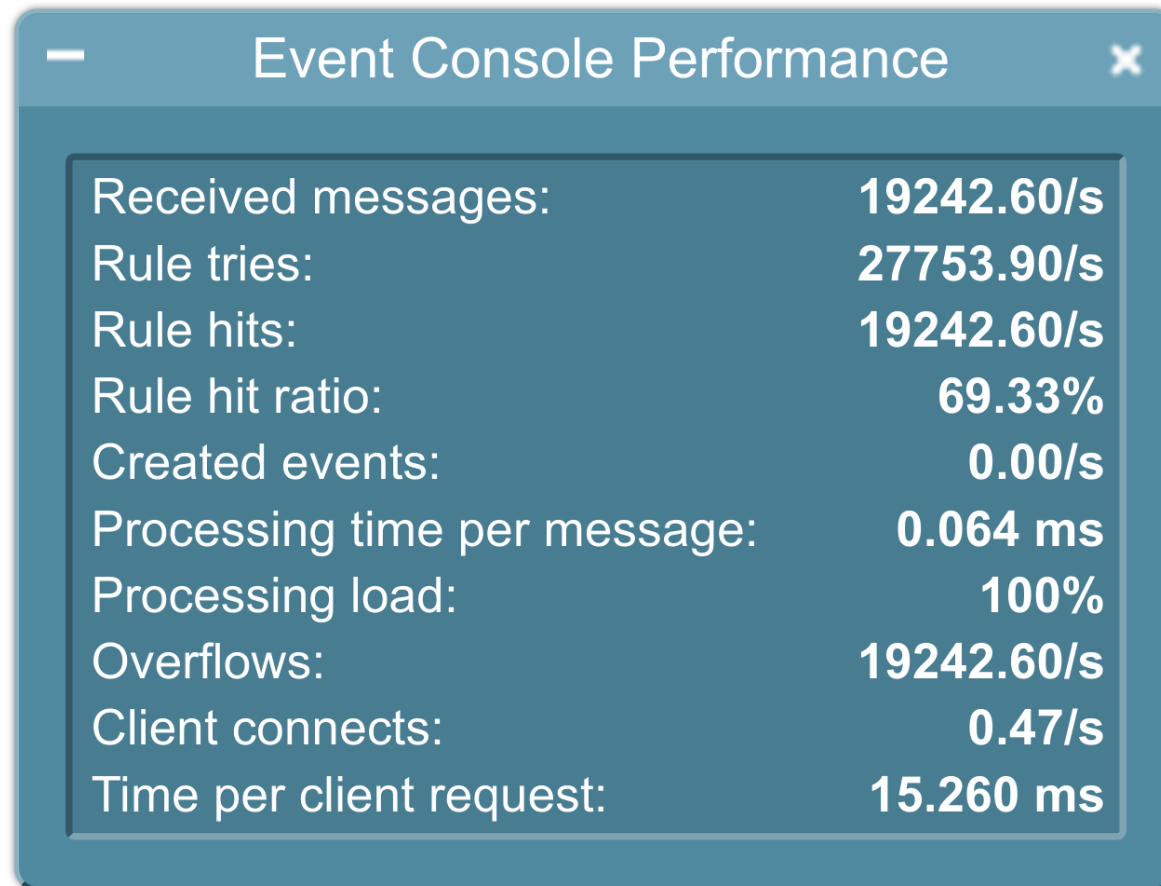
Werk #2309

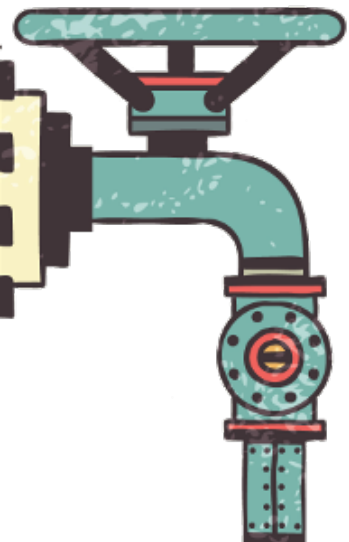
Performance Snapin



Werk #2309

Improved EC Performance snapin





Werk #3388

SNMPv3 Traps



Werk #3388

Event Console can now process SNMPv3 traps

Description

Receive V3 Traps

SNMP credentials

Credentials for SNMPv3 with authentication and privacy (authPriv) ▼

Security Level

authentication and encryption

Authentication protocol

MD5 ▼

Security name

xyz123

Authentication password

.....

Privacy protocol

AES ▼

Privacy pass phrase

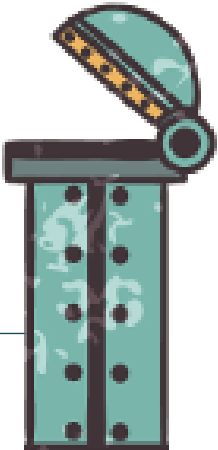
.....



Werk #3539

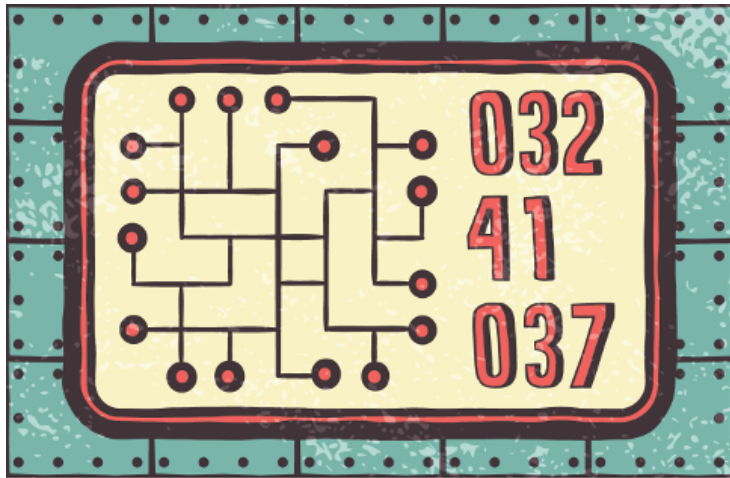
Master Control

Check_MK Conference #3 - News in the Event Console



Notifications switch is now also effective for EC notifications





Werk #2309 Event Simulator



Werk #2309

Added "Service Level" to event simulation

▼ Event Simulator

Message text	Still nothing happened.
Application name	Fooobar-Daemon
Host Name	myhost089
IP Address	1.2.3.4
Syslog Priority	notice ▼
Syslog Facility	user ▼
Service Level	20 - Gold ▼
Simulate for site	beta - Der Master▼





Werk #4166

Archive host's events


Werk #2974






Archive-Icon



Werk #2974

Added short cut icon 'archive this event' to Event Console events view



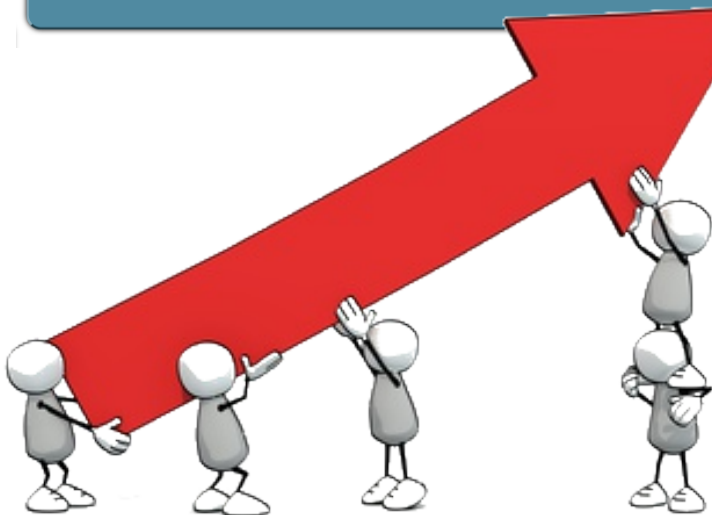
ID	Icons	State	Level	Host	Rule	Application
47		OK	(no Service level)	Klappfisch	alles	wpa_suppl...
1		OK	(no Service level)	Klappfisch	alles	nullmailer
2		OK	(no Service level)	Klappfisch	alles	nullmailer
3		OK	(no Service level)	Klappfisch	alles	nullmailer
4		CRIT	(no Service level)	Klappfisch	alles	nullmailer



Werk #4166

New view command: archive events of a host

Add comment	Comment: <input type="text"/>
	<button>Add comment</button>
Favorites	<button>Add to Favorites</button> <button>Remove from Favorites</button>
Archive events of hosts	<button>Archive events</button>





Werk #3736

Discontinue Counting



Werk #3736

New option for discontinuing counting on open events after configured time



Count until triggered:

Time period for counting:

days

hours

mins

secs

Algorithm:

Interval ▼

☒ Discontinue counting after time has elapsed



Count only for

days

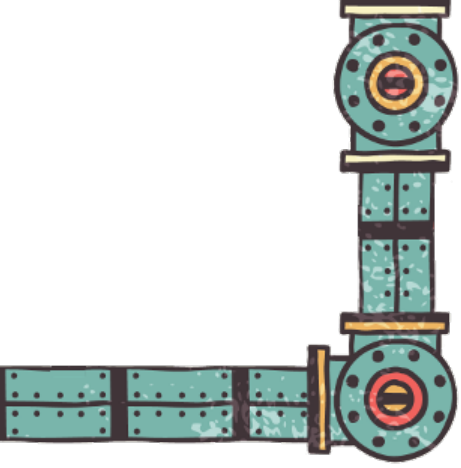
hours

mins

secs

- ☐ Continue counting when event is **acknowledged**
- ☒ Force separate events for different **hosts**
- ☒ Force separate events for different **applications**
- ☒ Force separate events for different **match groups**





Werk #3861

Overflow protection



Design target

Keep EC operational even in abnormal situations, e.g.

- ... one host goes crazy
- ... one type of message floods everything



Werk #3861

Introduced open event limit mechanism for protecting against message storms

- Limits currently open events
- Individual limits:
 - per host
 - per rule
 - total



Possible actions in case of flood (configurable)

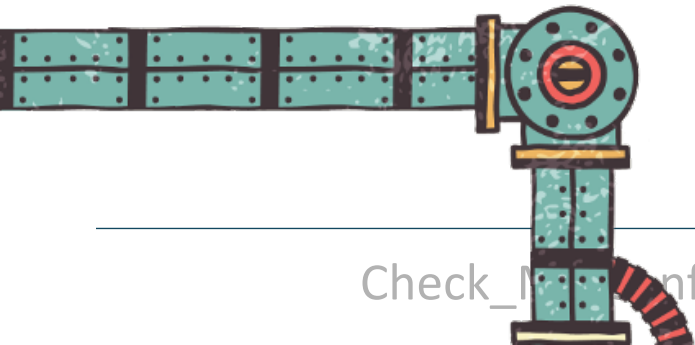
- Stop creating new events
- Create (one last) overflow event
- Notify contacts of bogus host
- Notify „administration“ contacts



Werk #2733

Werk #4151

Event <-> Contact



Werk #2733

Visibility of Event Console events more flexible now

- Choose whether contact groups of host or of rule have precedence
- Also influences notifications

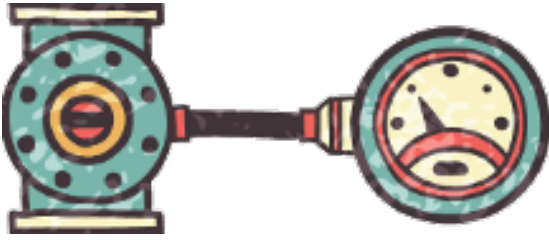


Werk #4151

Use notification fallback also for hosts not known to the monitoring

- In case host not found in monitoring and no contacts in rules
- Makes sure **somebody** gets notified





Further Werks (1)

- #4276** Actions can now access the event macros via environment variables
- #3656** Added support for syslog messages produced by Aristana devices
- #3262** Bulk delete button for custom MIBs now available
- #3390** Events can now be cancelled by the syslog application
- #4132** Monitoring notifications: Add EC_ORIG_HOST to notification context



Further Werks (2)

#3716 New sites now have a default rule pack from the start

#4286 SNMP MIBs of the Event Console can now be packed using MKPs

#4277 Script actions: New event macro ORIG_HOST

#2999 The contact name is now included in Event Console notifications

#1306 Recent event history can now be filtered by extended regular expressions

#3717 Added search to EC settings and structured the options in multiple settings



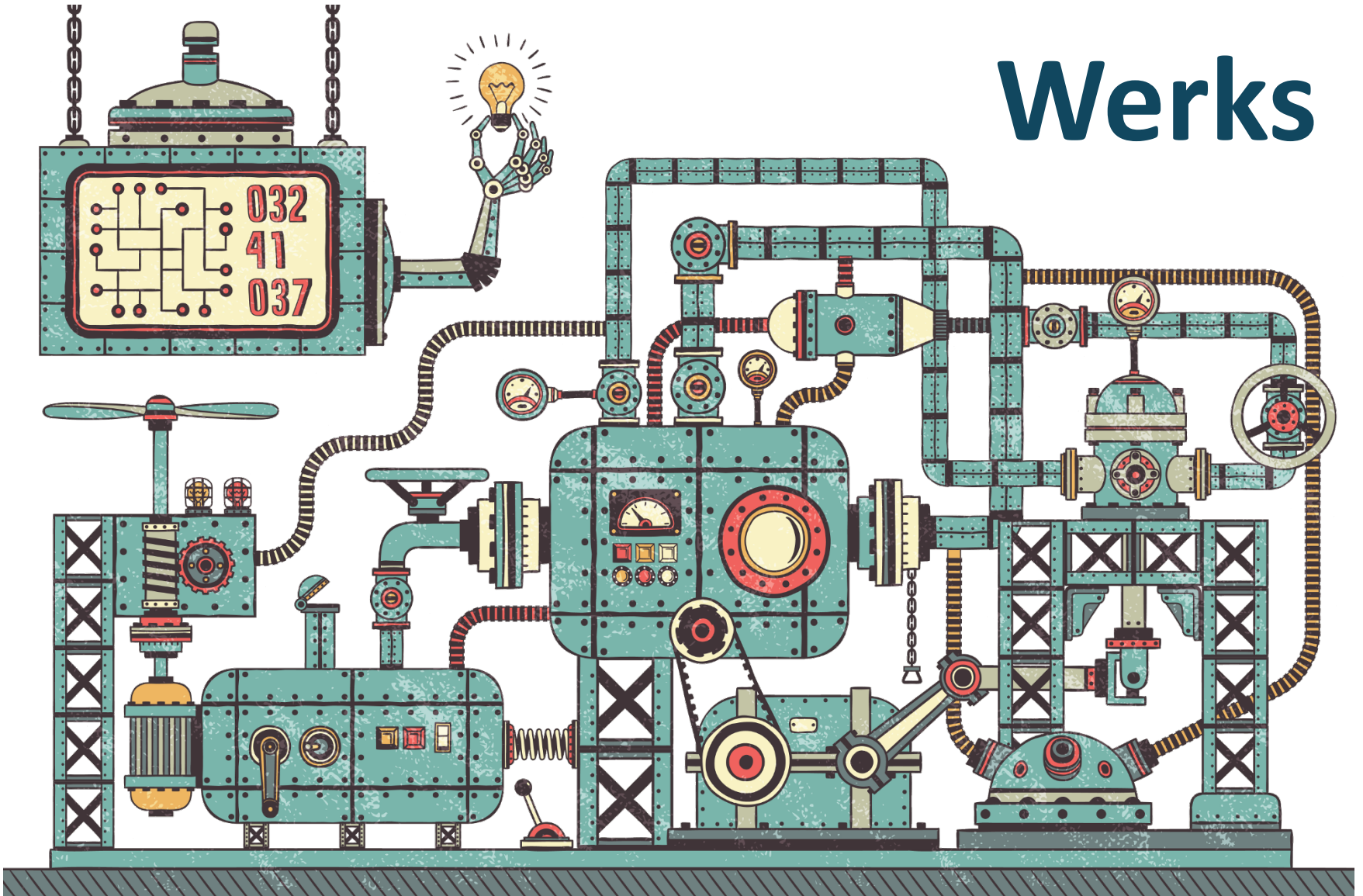
CHECK_MK
CONFERENCE #3

News in the Notification Module

Manfred Brunner



Werks



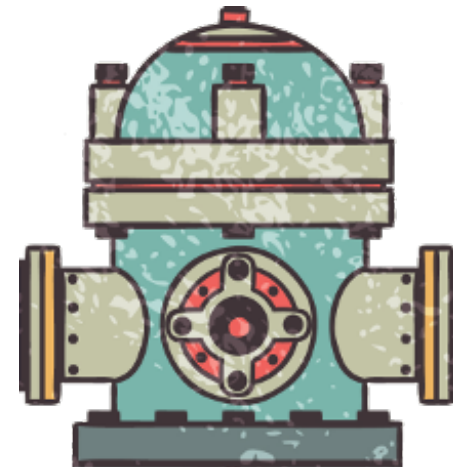
New Feature-Werks

#8637 #8555

#8617 #8330 #8200 # #3972 #3957
#3886 #3532 #3263 #3140 #2935 #2811



Werk #8637 #8555 Notification Spooler



Werk #8367

Check_MK Notification Spooler is always enabled now.

Werk #8555

Enable local asynchronous notification delivery using mknotifyd by default.



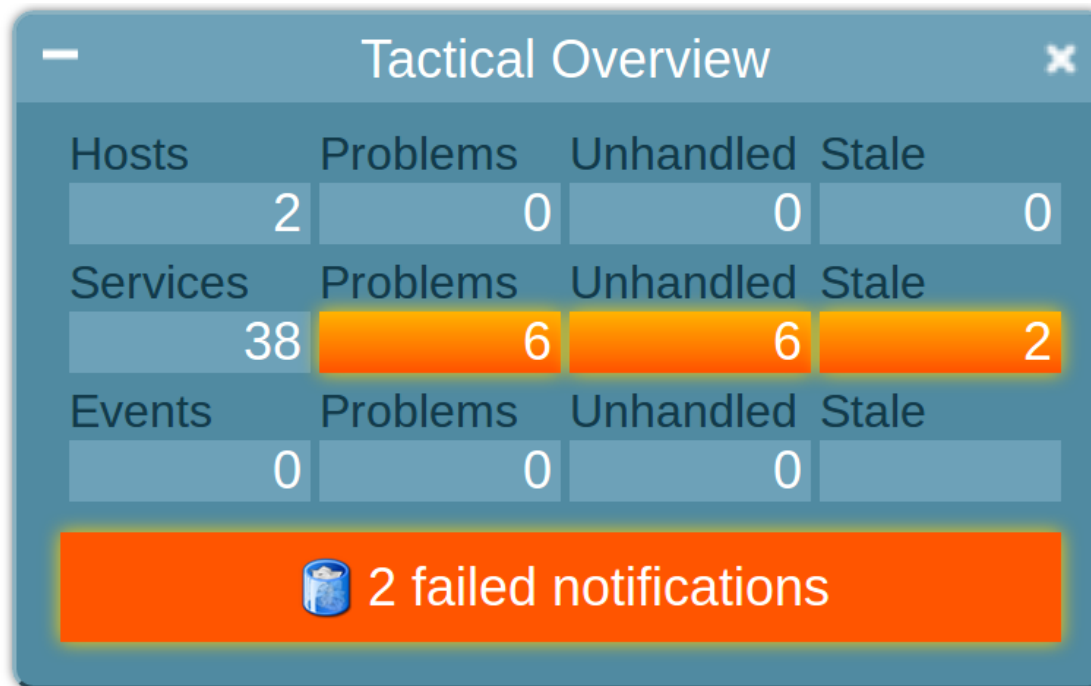
New Standard! Asynchronous delivery

- Every notification will be saved to a spool file
- No jam can build up.
- If the monitoring is stopped the spool files will be retained, later be delivered correctly.





Werk #8330

mknotifyd: now supports concurrent delivery of notifications and passes completion results back to the core.

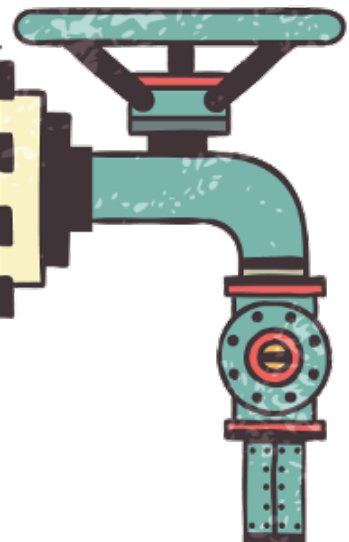


failed_notifications

	Time	Contact	Command	Event	Host	Service	State	Output	Comment
	37.8 s	Manfred	mail	SERVICE NOTIFICATION RESULT	heute	CUPS Queue HP_Officejet_Color_MFP_X585	CRIT	Unhandled exception: Failed to send the mail: /usr/sbin/sendmail is missing	Unhandled exception: Failed to send the mail: /usr/sbin/sendmail is missing
	37.8 s	Manfred	mail	SERVICE NOTIFICATION RESULT	heute	CUPS Queue HP_Officejet_Color_MFP_X585_2	CRIT	Unhandled exception: Failed to send the mail: /usr/sbin/sendmail is missing	Unhandled exception: Failed to send the mail: /usr/sbin/sendmail is missing

```
OMD[heute]:~/var/check_mk/notify/spool$ ll
insgesamt 856
-rw-r--r-- 1 heute heute 4510 Apr 24 10:01 00b0943d-c361-4be9-8fd6-89a25bb4d6c4
-rw-r--r-- 1 heute heute 4535 Apr 24 10:01 02f34446-2c51-4c2c-9f7e-641f37315b92
```





Werk #2811 #3957

Mail body



Werk #2811

You can now configure to add the host/service notes url to the email body.

▼ Notifications

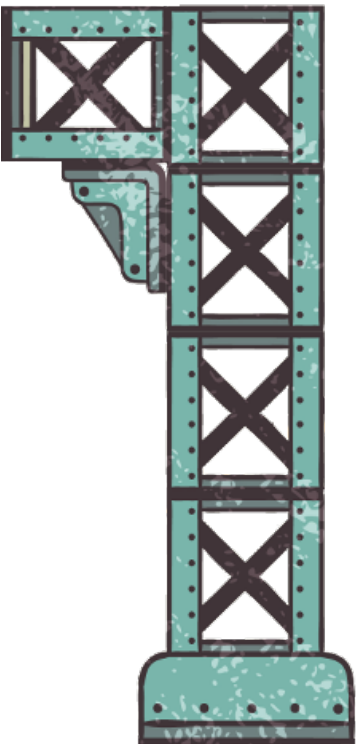
Notes URL for Hosts 1 Notes URL for Services 1

	Actions	Conditions	Value
	   	■ Host name is SRV1	http://www.mein-wiki.intern.com/\$HOSTNAME\$



Werk #3957

Now allows extra HTML section between
body and table




Werk #2811 #3957

▼ Notification Method

Notification Method HTML Email ▼

Call with the following parameters: ▼

- ☐ From: Address
- ☐ Reply-To: Address
- ☐ Subject for host notifications
- ☐ Subject for service notifications
- ☒ Information to be displayed in the email body
 - ☒ IP Address of Host
 - ☒ Absolute Time of Alert
 - ☐ Relative Time of Alert
 - ☒ Additional Plugin Output
 - ☐ Acknowledgement Author
 - ☐ Acknowledgement Comment
 - ☒ Performance Data
 - ☒ Performance Graphs
 - ☒ Custom Host/Service Notes URL
 - ☐ Complete variable list (for testing)
- ☒ Insert HTML section between body and table
 -
- ☐ URL prefix for links to Check_MK
- ☐ Display graphs among each other
- ☐ Notification sort order for bulk notifications
- ☐ Enable synchronous delivery via SMTP





Werk #3972

Bulk notifications



Werk #3972

New feature: bulk notifications based on Event console contacts

▼ Notification Method

Notification Bulking ✕

Time horizon

Bulk up to days hours mins secs

Maximum bulk size

Bulk up to Notifications

Create separate notification bulks based on

☐ Folder

☐ Host

☐ Service description

☐ Service level

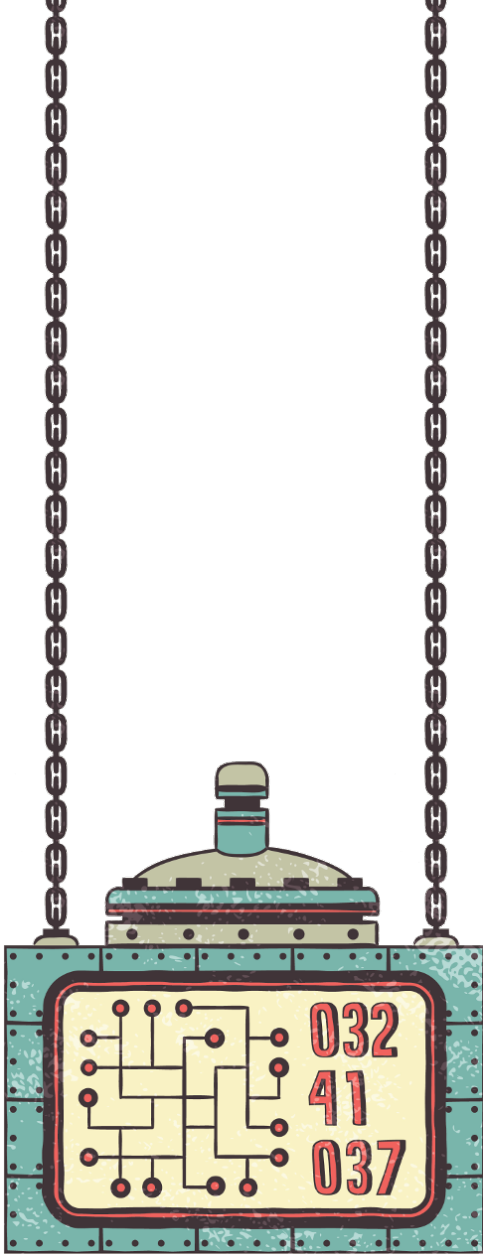
☐ Check type

☐ Host/Service state

☒ Event console contact

Create separate notification bulks for different values of the following custom macros





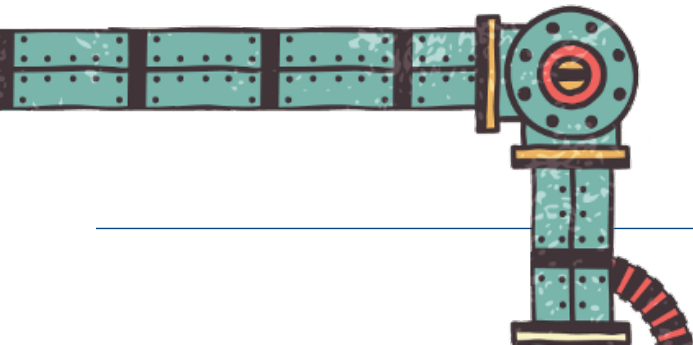
Werk #3532 New conditions



Werk #3532

Rule based notifications:
Three new conditions for service groups matching.

- Exclude Service Groups (Duallist Choice)
- Match Service Groups (Regex)
- Exclude Service Groups (Regex)



Werk #3532

▼ Conditions

Match site ☐

Match folder ☐

Match Host Tags ☐

Match Host Groups ☐

Match only the following hosts ☐

Exclude the following hosts ☐

Match Service Groups ☐

Exclude Service Groups ☒

Match Service Groups (regex) ☒

Exclude Service Groups (regex) ☒

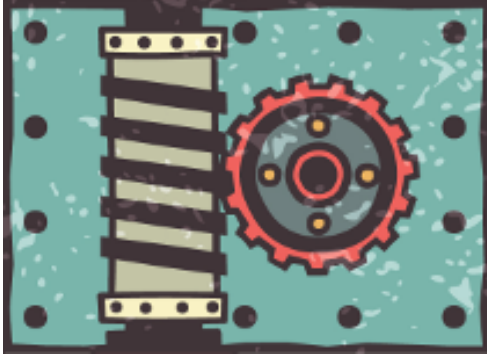
Available > < Selected

All Filesystems ^ v

Match the internal identifier ▼

Match the internal identifier ▼





Werk #2935

Match of Event

Console rules



Werk #2935








A notification can now match multiple Event Console rules.

Match notification comment ☐

Event Console alerts ☒

Match only Event Console alerts ▼

☒ Rule IDs

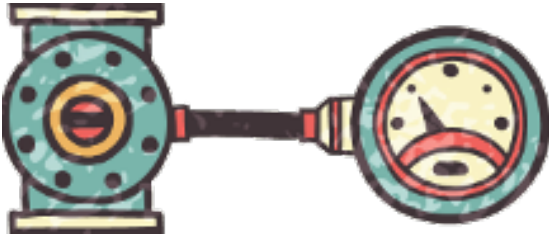
		Rule ID: <input type="text" value="Rule_1"/>
	 	Rule ID: <input type="text" value="Rule_2"/>
		Rule ID: <input type="text" value="Rule_3"/>

☐ Match syslog priority

☐ Match syslog facility

☐ Match event comment





Further Werks (1)

- #8200** Notifications/Alerts: New environment variables
MAXSERVICEATTEMPTS, MAXHOSTATTEMPTS
- #3886** Notifications that do not match any rule are sent to
fallback mail / contacts
- #3263** allow users to restrict by their contact groups
- #3140** mail notification script can now optionally connect
directly to a smtp server instead of using sendmail.



Further Werks (2)

#8617 Alarmspooler: log successful TCP connects

#4286 SNMP MIBs of the Event Console can now be packed using MKPs



CHECK_MK
CONFERENCE #3

Business Intelligence

Marcel Arentz



Rules/Views

#2882

- Reorganizing rules into packs
- Now able to set contacts / permissions
- Share rules between packs



Werk #2882

Business Intelligence

omdadmin (admin) 09:58



Main Menu

New BI Pack

BI Configuration Packs

▶ Actions	ID	Title	Public	Aggregations	Rules	Contact Groups
	default	Default Pack	Yes	1	12	

▼ BI Pack Properties

Pack ID default

Title Default Pack

Permitted Contact Groups Everything▼

Add Contact Group

Public ☒ Allow all users to refer to rules contained in this pack



Werk #2882

▼ Child Node Generation

Nodes that are aggregated by this rule



State of a h

Host: \$HOS



State of a s

Host: \$H

Service: Up



Call a Rule

Rule:

Arguments: \$HOSTNAME\$

applications - Default Pack/Applications
checkmk - Default Pack/Check_MK
filesystem - Default Pack/\$FS\$
filesystems - Default Pack/Disk & Filesystems
general - Default Pack/General State
hardware - Default Pack/Hardware
host - Default Pack/Host \$HOSTNAME\$
logfiles - Default Pack/Logfiles
multipathing - Default Pack/Multipathing
myRule - that/This is my \$HOSTNAME\$
networking - Default Pack/Networking
other - Default Pack/Other
performance - Default Pack/Performance

checkmk - Default Pack/Check_MK ▼

Add child node generator



Rules/Views

#3873

#3955

#3449

- Availability of copying/deactivating of rules
- Renaming of rule ID
- Host alias available in rules



Werk #4460

Business Intelligence - Default Pack - Rules

omdadmin (admin) 10:42



Main Menu

All Packs

Aggregations

New Rule

Unused Rules

Rules

Actions		Level	ID	Parameters	Title	Aggregation	Nodes	Used by	Comment
			host	HOSTNAME	Host \$HOSTNAME\$	worst/1/2	8	Host \$HOSTNAME\$ (host)	
		1	applications	HOSTNAME	Applications	worst	1	Host \$HOSTNAME\$ (host)	
		1	filesystems	HOSTNAME	Disk & Filesystems	worst	4	Host \$HOSTNAME\$ (host)	
		1	general	HOSTNAME	General State	worst	3	Host \$HOSTNAME\$ (host)	
		1	hardware	HOSTNAME	Hardware	worst	1	Host \$HOSTNAME\$ (host)	
		1	logfiles	HOSTNAME	Logfiles	worst	1	Host \$HOSTNAME\$ (host)	
		1	networking	HOSTNAME	Networking	worst	1	Host \$HOSTNAME\$ (host)	
		1	other	HOSTNAME	Other	worst/1/2	1	Host \$HOSTNAME\$ (host)	
		1	performance	HOSTNAME	Performance	worst	1	Host \$HOSTNAME\$ (host)	
		2	filesystem	HOSTNAME FS	\$FSS\$	worst	3	Host \$HOSTNAME\$ (host)	
		2	checkmk	HOSTNAME	Check_MK	worst	1	Host \$HOSTNAME\$ (host)	
		2	multipathing	HOSTNAME	Multipathing	worst	1	Host \$HOSTNAME\$ (host)	



Rules/Views

#3271

- Aggregation of downtimes
- CRIT as default
- Configurable to WARN



Werk #3271

Single Aggregation Host heute 1 row omdadmin (admin) 11:47

Export as PDF Edit View Availability

Links	State	Tree
	WA	▼ Host heute <ul style="list-style-type: none">OK ▼ General State<ul style="list-style-type: none">OK Host status ♦ Packet received via smart PINGOK Uptime ♦ OK - Up since Fri Apr 28 09:07:02 2017 (0d 02:39:24)OK ▼ Performance<ul style="list-style-type: none">OK CPU load ♦ OK - 15 min load 0.35 at 4 Cores (0.09 per Core)OK CPU utilization ♦ OK - user: 5.7%, system: 0.9%, wait: 0.0%, steal: 0.0%, guest: 0.0%, total: 6.6%OK Kernel Context Switches ♦ OK - 1659/sOK Kernel Major Page Faults ♦ OK - 0/sOK Kernel Process Creations ♦ OK - 4/sOK Memory ♦ OK - RAM used: 3.50 GB of 7.82 GB, Swap used: 0.00 B of 2.40 GB, Total virtual memory used: 3.50 GB of 10.21 GB (34.2%),OK Number of threads ♦ OK - 610 threadsWA ▼ Disk & Filesystems<ul style="list-style-type: none">OK Disk IO SUMMARY ♦ OK - Utilization: 0.1%, Read: 1.18 kB/s, Write: 377.70 kB/s, Average Wait: 0.32 ms, Average Read Wait: 2.00 ms, Average Write Wait: 0.32 ms, Latency: 0.07 ms, Average Queue Length: 0.00OK ▶ /OK ▶ /homeWA ▶ /media/sf_macbookWA ▶ /media/sf_seafileOK ▶ /optOK ▶ Networking

WARN



Performance

#3396

#3546

- *Precompile aggregations on demand*
 - new default: ON
- general improved performance
- Especially for single aggregations



Werk #3546

▼ Aggregation Properties

Aggregation Groups Hosts

Rule to call Create nodes based on a host search ▼

Refer to: The found hosts themselves ▼

Agent type: ignore▼

Criticality: ignore▼

Networking Segment: ignore▼

IP Address Family: ignore▼

Host Tags: monitor via SNMP: ignore▼

monitor via Check_MK Agent: is ▼ set

IPv4: ignore▼

IPv6: ignore▼

Host name: All Hosts ▼

Call a Rule▼

Nodes to create: Rule: host - Default Pack/Host \$HOSTNAMES ▼

Arguments: \$HOSTNAMES\$

Disabled ☐ Currently disable this aggregation

Use Hard States ☐ Base state computation on hard states

Aggregation of Downtimes ☐ Escalate downtimes based on aggregated WARN state

Optimization ☒ The aggregation covers data from only one host and its parents.



Performance

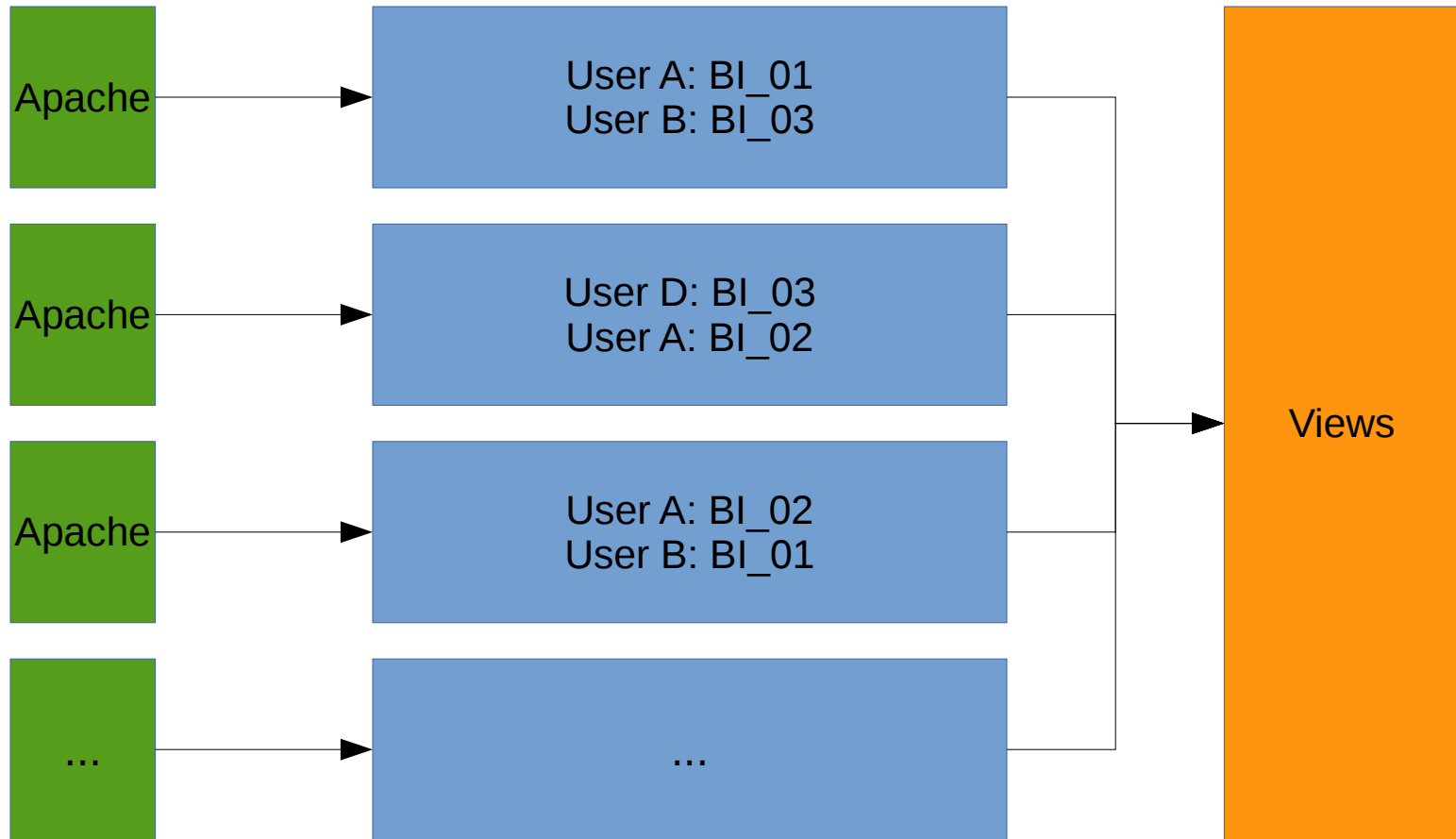
#4002

#4469

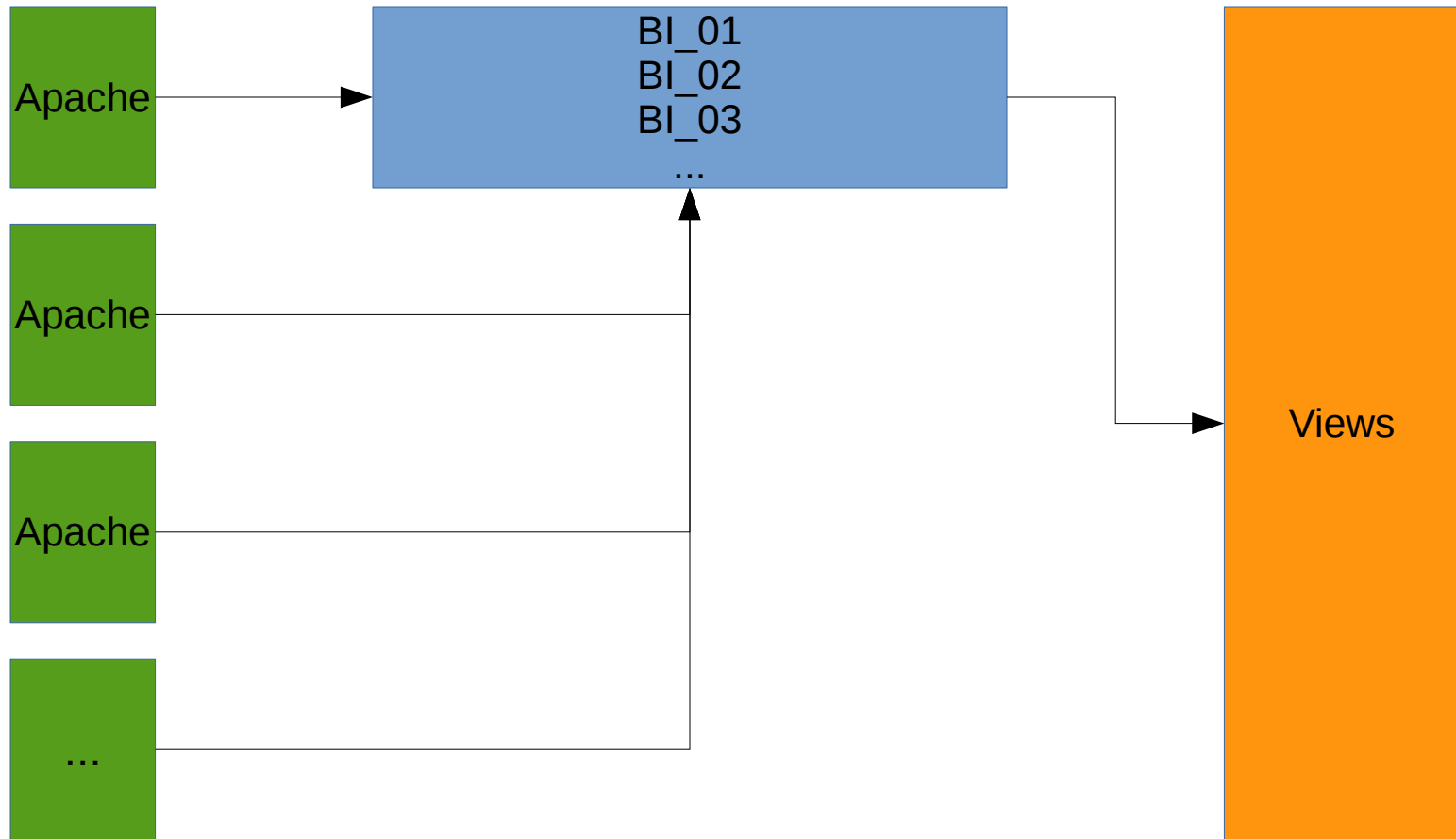
- Major rework of Code
- drastically sped up performance
- Further improvements planned



Werk #4002



Werk #4002



Werk #4002

Old	New
Computation time per apache: 3 aggr: 70 sec	Computation time for 3 aggr: 40 sec (time of slowest)
200 apaches and 8 Cores: $70 * 200 / 8 =$ almost 30 min.	200 apaches and 8 Cores: 40 sec
Computation time per apache: 100 BI's: 20 seconds	Computation time for 100 BI's: 2.5 sec
200 apaches and 8 Cores: $20 * 200 / 8 =$ more than 8 min.	200 apaches and 8 Cores: $20 / 8 = 2.5$ sec



Werk #4469

Old	New
<p>Distributed Monitoring with n sites, 600 aggr and 100ms latency:</p> <ul style="list-style-type: none">- one query for each aggr- ~60 seconds to get the data- plus 3 seconds computation time <p>= 63 sec</p>	<p>Distributed Monitoring with n sites, 600 aggr and 100ms latency:</p> <ul style="list-style-type: none">- evaluate needed data- one query for all the data- 2 sec for parsing the data- plus 3 seconds computation time <p>= around 2+3 sec</p>



CHECK_MK
CONFERENCE #3



Thanks for listening!

YOUR FEEDBACK IS WELCOME