You will love

Checkmk notifications in 2.4

Tanja Hohenstatt
UX Designer
Checkmk GmbH

The Checkmk notification system is powerful ...

… gives you all the tools you need …

Setup

Notifications   Contact groups   Time periods

Host monitoring rules

Assignment of hosts to contact groups

Delay host notifications

Enable/disable notifications for hosts

Notification period for hosts

Periodic notifications during host problems

Notified events for hosts

Service level of hosts

Service monitoring rules

Assignment of services to contact groups

Delay service notifications

Enable/disable notifications for services

Notification period for services

Periodic notifications during service problems

Notified events for services

Service level of services

Maximum number of check attempts for service

Parameters for Slack, ServiceNow, Opsgenie, …

Other services

Check notification number per contact

Global settings

Really a lot of options…

… but is hard to use

How to Setup Notification Escalation? ✏️

🟦 General   checkmk-v2-1 , notifications

S switch609   5h

Hello

I was wondering if it was possible to setup Notification Esclation.

Let says email gets sent out level 1 support if the issue is not acknowledge after 1 hour it then gets escalated to level 2 support team so on so forth.

⌄ Description

Hi Support,
it is possible disable fallback notification? We receive thousands of fallback emails every day for alerts that do not match the notification rules. We would like to avoid this unnecessary email load because it creates load problems for us. We only need to receive notifications that match the rules

Thanks and BR,

Checkmk
Conference

Make configuring, troubleshooting, and optimizing of notifications easy

Checkmk
Conference

Disclaimer: Early stage concepts

A new way to configure notifications

Checkmk
Conference

Add notification rule

Notification rule   Related   Display   Help   ⬤

Concept - Work in Progress

✕ Cancel   ⬆ Notifications

① Define host/service events

Define any host or service events you want to be notified about.

② Specify host/service conditions

Specify conditions to determine which hosts and which services will be affected by this notification rule.

③ Notification flow

Define when and how you want to be notified.

④ Bulk notifications

To reduce the number of notifications, combine multiple successive notifications for the same contact into a single bulk notification that lists all current problems in, e.g., a single email.

⑤ Review & rule properties

Review your notification rule before applying it. They will take effect right away without "Activate changes".

1 Define host/service events

Define any host or service events you want to be notified about.

Host events....... [Status change ⌄] From [Any ⌄] to [Down ⌄] ×

[⊕ Add event]

Service events... [Status change ⌄] From [OK ⌄] to [Warn ⌄] ×

[Status change ⌄] From [Any ⌄] to [Crit ⌄] ×

[Status change ⌄] From [Any ⌄] to [Unknown ⌄] ×

⊕ Add event

[⬇ **Next step: Specify host/services**]

1 Define host/service events

Define any host or service events you want to be notified about.

Host events....... | Status change ∨ | From | Any ∨ | to | Down ∨ | ×

Select event ... ∧ | ×

- Status change
- Start / End of downtime
- Acknowledgement of problem
- Start / end of flapping state
- Alert handler execution

Service events... | to | Warn ∨ | ×

| to | Crit ∨ | ×

Status change ∨ | From | Any ∨ | to | Unknown ∨ | ×

➕ Add event

⬇ **Next step: Specify host/services**

9

2 **Specify hosts/service conditions** *Concept - Work in Progress*

Specify conditions to determine which hosts and which services will be affected by this notification rule.

∨ **General**

Service level.....   [*Select service level ...* ∨]

Folder...............   [Main ∨]

> **Hosts**

> **Services**

[⬇ **Next step: Notification flow**]   [⬆ **Previous step**]

2 Specify hosts/service conditions

Specify conditions to determine which hosts and which services will be affected by this notification rule.

∨ **General**

Service level...

Folder.............

> **Hosts**

> **Services**

⬇ **Next step:**

∨ **Hosts**

Host tags.......... | Select host tags ∨ | ➕ Add tag condition

Host labels........ ➕ Add label condition

☐ Explicit hosts (Regex)

∨ **Services**

Service labels.... ➕ Add label condition

☐ Explicit services (Regex)

3

Notification flow

Define when and how you want to be notified.

Notify ... [all contacts of the notified object ⌄] (Assign to contact groups)

➕ Add to query

via .... [email ⌄] [*Select email template* ⌄]

if .... [time ⌄] [is ⌄] [time period ⌄] [*Select time period* ⌄] ✕

➕ Add to query

[⬇ **Next step: Bulk notifications**]   [⬆ **Previous step**]

3 # Notification flow

Define when and how you want to be notified.

Notify ... [all contacts of the notified object ∨] (Assign to contact groups)

➕ Add to query

via .... [email ∨] [Select email template ∨]

if .... [time ∨] [is ∨] [time period ∨] [Select time period ∨] ✕

➕ Add to query

[⬇ **Next step: Bulk notifications**]   [⬆ **Previous step**]

Re-usable templates and connections
Contextually edit and create things

Concept - Work in Progress

via .... email ⌄ | Select email template ⌄ | ×

Default (HTML)

Default (ASCII)

✏️ Edit templates

Checkmk
Conference

Re-usable templates and connections
Contextually edit and create things

via .... | Microsoft Teams ⌄ | Select connection ⌄ | ✕

No connections configured

➕ Add connection

Checkmk
Conference

3

Notification flow

Define when and how you want to be notified.

Notify ... [all contacts of the notified object ∨] (Assign to contact groups)

➕ Add to query

via .... [email ∨] [*Select email template* ∨]

if .... [time ∨] [is ∨] [time period ∨] [*Select time period* ∨] ×

➕ Add to query

[⬇ **Next step: Bulk notifications**]   [⬆ **Previous step**]

3

Notification flow

Define when and how you want to be notified.

Notify ... | all contacts of the notified object ∨ | (Assign to contact groups)

➕ Add to query

via .... | email ∨ | *Select email template* ∨

if .... | time ∨ | is ∨ | time period ∨ | *Select time period* ∨ | ×

➕ Add to query

⬇ **Next step: Bulk notifications**   ⬆ **Previous step**

3

Notification flow

Define when and how you want to be notified.

Notify ... [contact group ⌄] [all ⌄]

and ...... [send every ⌄] [5] th notification ×

➕ Add to query

via .... [email ⌄] [Template 1 ⌄]

if .... [time ⌄] [is ⌄] [time period ⌄] [24X7 - Always ⌄] ×

[and ⌄] [number of notification ⌄] [is between ⌄] [5] and [100] ×

➕ Add to query

[⬇ **Next step: Bulk notifications**] [⬆ **Previous step**]

4 Bulk notifications

To reduce the number of notifications, combine multiple successive notifications for the same contact into a single bulk notification that lists all current problems in, e.g., a single email.

Bulk based on ...
- [ ] Folder
- [x] Host
- [ ] Service description
- [ ] Service level
- [ ] Check type
- [ ] Host/Service state
- [ ] Event console contact
- [ ] Event console comment
- [ ] Custom macro

Bulk within .... `0` hour `1` min `0` sec

Max. bulk size ... `1000` notifications per bulk notification

Subject ...... `Check_MK: $COUNT_NOTIFICATIONS$ notifications for $COUNT_HOSTS$ hosts` (Reset to default)

⬇ Next step: Review   ⬆ Previous step

Concept - Work in Progress

⑤ Review & rule properties

Review your notification rule before applying it. They will take effect right away without "Activate changes".

Description .... [   ]

Setting .... ☐ Disable rule

☒ Allow users to deactivate this notification

Comment .... [   ]

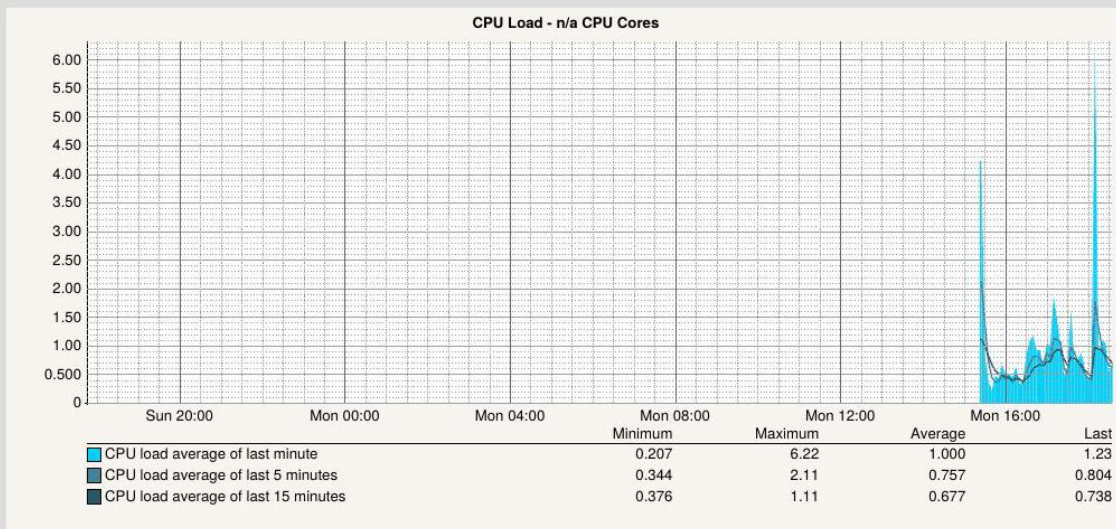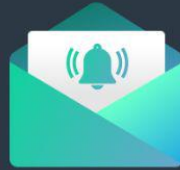Documentation ... [   ]

[✓ **Apply & test notifications**]   [⬆ **Previous step**]

Updates for notification methods

80%

Users are using Checkmk email notifications

Checkmk
Conference

Host	backup44 (Backup-Server 44)
Service	CPU load
Event	OK → CRITICAL
Address	localhost
Date / Time	Mon May 25 18:41:51 CEST 2020
Plugin Output	
Additional Output	
Host Metrics	rta=0.030ms;200.000;500.000;0; pl=0%;40;80;; rtmax=0.043ms;;;; rtmin=0.024ms;;;
Service Metrics	

Graphs

CPU Load - n/a CPU Cores

	Minimum	Maximum	Average	Last
CPU load average of last minute	0.207	6.22	1.000	1.23
CPU load average of last 5 minutes	0.344	2.11	0.757	0.804
CPU load average of last 15 minutes	0.376	1.11	0.677	0.738

checkmk

Host: backup44 (Backup-Server 44)

Service: CPU load

Event: OK → CRIT

View the issue

🔔 **Details**

Date / Time: Mon May 25 18:41:51 CEST 2024

Address: localhost

Focused: Most important info on top

Site: prod

Summary: 15 min load: 6.02 (ok/crit at 4.80/6.00) **CRIT**

Service details:

15 min load per core: 1.40 (4 logical core)
1 min load per core: 2.25 (4 logical core)
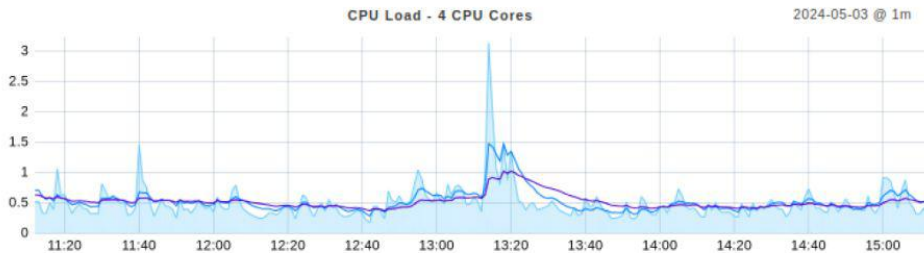5 min load per core: 1.39 (4 logical core)

Graph

CPU Load - 4 CPU Cores   2024-05-03 @ 1m

	Minimum	Maximum	Average	Last
CPU load average of last 15 minutes	0.37	1.02	0.52	0.51
CPU load average of last 5 minutes	0.29	1.48	0.53	0.48
CPU load average of last minute	0.17	3.14	0.5	0.3
Warning of CPU load average of last 15 minutes				20
Critical of CPU load average of last 15 minutes				40

Focused: Most important info on top

Modern look and feel: "New" graphs

Additional details

Host metrics: rta=0.030 ms — rtmax=0.043 ms

Service metrics: offset=0.002 ; 200 ; 500

Notification rule:

→ (#2) Notify all contacts of a host/service via HTML email

Contact groups

- Test
- Main
- Main IT

Service labels

state:bavaria   cmk/os_family:linux

Host tags

Focused: Most important info on top

Modern look and feel: "New" graphs

Traceability: Rule that triggered the notification

Contact groups

- Test
- Main
- Main IT

Service labels

state:bavaria   cmk/os_family:linux

Host tags

checkmk-agent   checkmk-agent icon   ip-v4v6

Checkmk GmbH, Kellerstraße 27, München, Bayern 81667, Germany, +49 89 998209700

Unsubscribe   Manage preferences

Focused: Most important info on top

Modern look and feel: "New" graphs

Traceability: Rule that triggered the notification

Informational: Service labels + Contact groups

Updates for...

A new home
for notifications

Notifications

checkmk

Concept - Work in Progress

| Notifications | Related | Display | Help |

[+] **Add notification rule** [+] **Add email template** 🧪 **Test notifications** 📊 **Analyze recent notifications**

▾ Email templates

#	Actions	Description	Type
0	✏️🖥️🗑️	Default (HTML)	HTML
1	✏️🖥️🗑️	Default (ASCII)	ASCII

▾ Connections

Configured

iLert	4
Jira (Commercial editions only)	1
Microsoft Teams	1
Slack or Mattermost	1

▸ **More connections**

▾ Failed notifications

⚠️ **3**

Failed notifications

▾ Core status of notifications

Site	Core status
central	✅ Notifications enabled
remote1	✅ Notifications enabled
remote2	⚠️ Notifications disabled
remote3	✅ Notifications enabled

▾ Rules to optimize notifications

Monitor

Check notification number per contact	0

Optimize notifications

Business intelligence	0
Delay service notifications	0
Delay host notifications	0
Enable/disable notifications for services	0
Enable/disable notifications for hosts	0
Flap detection settings for services	0
Flap detection settings for hosts	0
Maximum number of check attempts for services	0
Maximum number of check attempts for hosts	0

Global notification rules

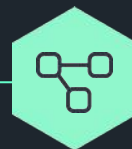| #	Actions	Method	Type	Bulk	Description	Contacts	Conditions
0	⇅✏️🖥️🗑️	email	✅	✅	Notify all contacts of host/service via HTML email	• all contacts of notified object	*(no conditions)*

Same complexity, less complicated

All notification options closer together

Clear and descriptive configuration options

Contextually edit connected options, e.g., time periods
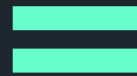
Re-use notification templates and connection

Checkmk
Conference

The notification approach

Your current starting point
Better more than less

Default rule

Contacts	Conditions
• all contacts of the notified object	*(no conditions)*

= **Risking spam + alarm fatigue**

Allowlist your notifications
Proposal for a new paradigm

Principle: "Subscribe" to relevant events, hosts, services

No more "Default" rule: Each rule must be set intentionally

Avoid spam and alarm fatigue

Missing notifications!
Mitigating the risk

Extension of notification analysis:
Which events were generated resulting in NO notification?

Test notifications

"Fallback email address" still exists

Allowlist vs. Blocklist

Allowlist

- Only notify what is defined

- Only specified objects/events are actionable/of interested

- Risk of forgetting an object/event

Blocklist

- Better more than less

- Everything that is being monitored is important, except for specified objects/events

- Risk of spam and alarm fatigue

Checkmk
Conference

We are looking for your feedback & insights!
Soon: Usability tests and interviews around Notifications

To subscribe: **Scan the QR-Code** or visit
lists.checkmk.com and look for
"Checkmk user experience research".

https://lists.checkmk.com/mailman3/postorius/lists/ux-research.lists.checkmk.com/

Checkmk
Conference