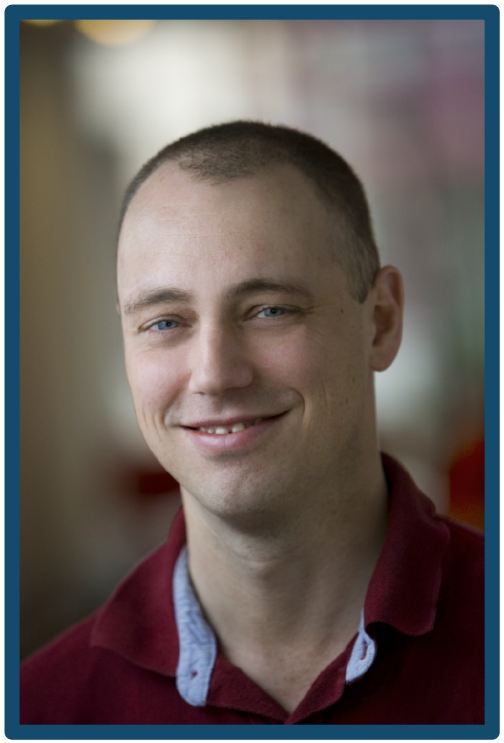
Introduction to op5 Monitor 7.0

A brief overview

This webinar will start in a few minutes

Who are we



Product Manager
Peter Andersson

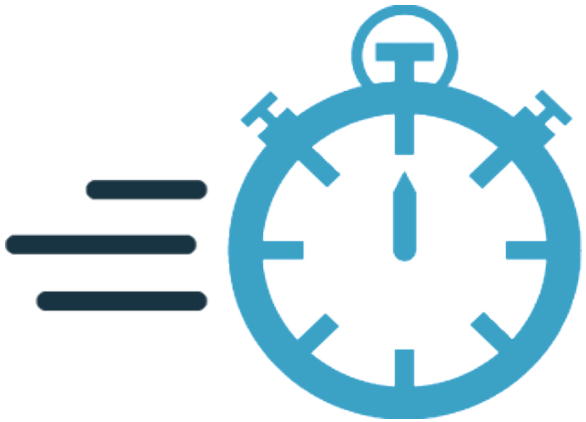
Digital Marketing & Web Manager
Andreas Månsson

CTO
Jan Josephson

op5

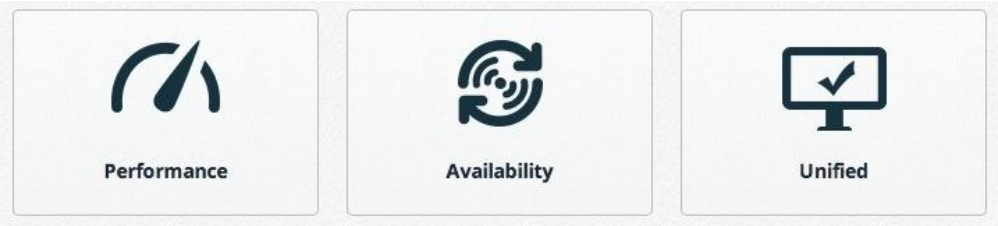
Agenda for today

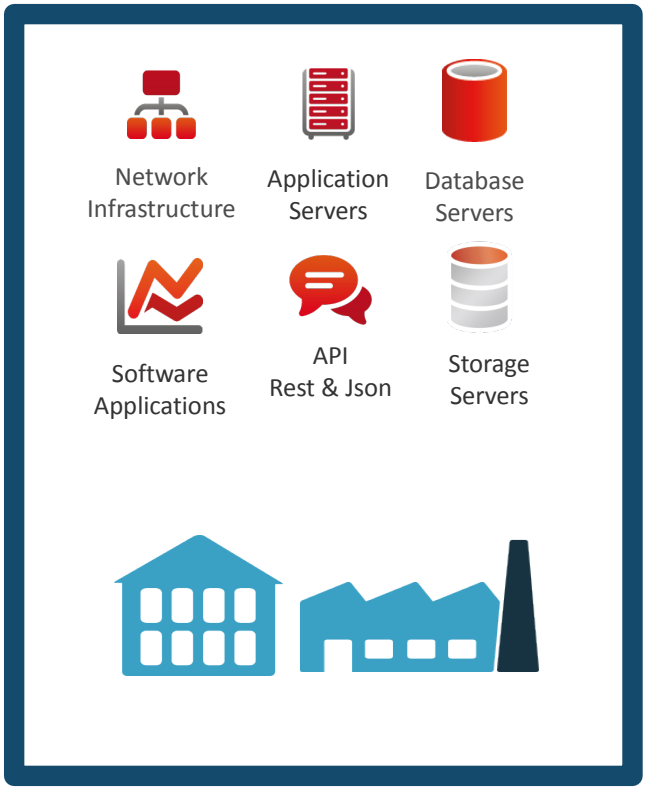
- Hybrid IT is the winner
- Logserver - Logger
- Features
  - Faster filtering capabilities
  - Enhancement to “Test this button”
- Plugins
- op5 Mobile App iOS
- Q/A



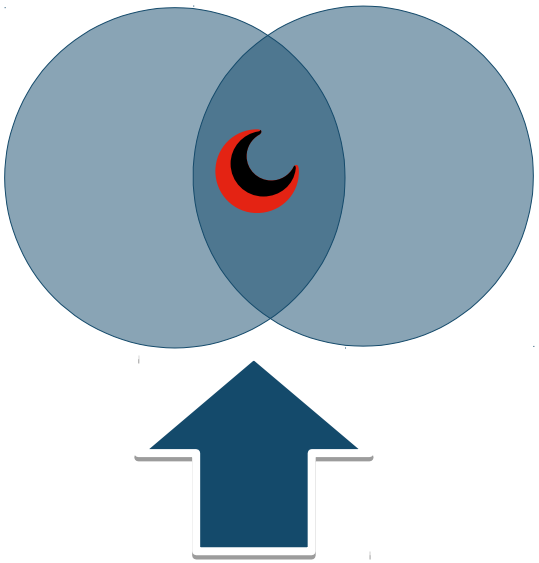
Hybrid IT is the winner

Hybrid IT is the winner!





Enterprise IT



We enable a controlled evolution to the hybrid cloud for Enterprise IT

"Ix, Px, Sx, DBx etc…as a Service

op5

It looks simple and cool....

HealthCare.gov | Learn | Get Insurance | Log in | Español

Individuals & Families | Small Businesses | All Topics | Search | Search

Still need health coverage?

FIND OUT IF YOU QUALIFY

for a Special Enrollment Period or Medicaid/CHIP

- Report income or life changes
- See plans and prices
- Small businesses: Apply any time
- Learn about fees & exemptions

Health Insurance Marketplace

HEALTHCARE.GOV BLOG

- 28 AUG Scheduled downtime to improve HealthCare.gov
- 22 AUG Help your kids start the school year strong with health coverage
- 21 AUG Making an appointment

TOP CONTENT

- Getting coverage outside Open Enrollment
- Using your new insurance coverage
- Using your new Medicaid or CHIP coverage

CONNECT WITH US

- Share Your Story
- Watch Videos
- Questions? Call 1-800-318-2596

QUICK INFORMATION

For Partners | Regulatory and Policy Information
For the Media | About the Affordable Care Act
For States | For Businesses

RESOURCES IN OTHER LANGUAGES

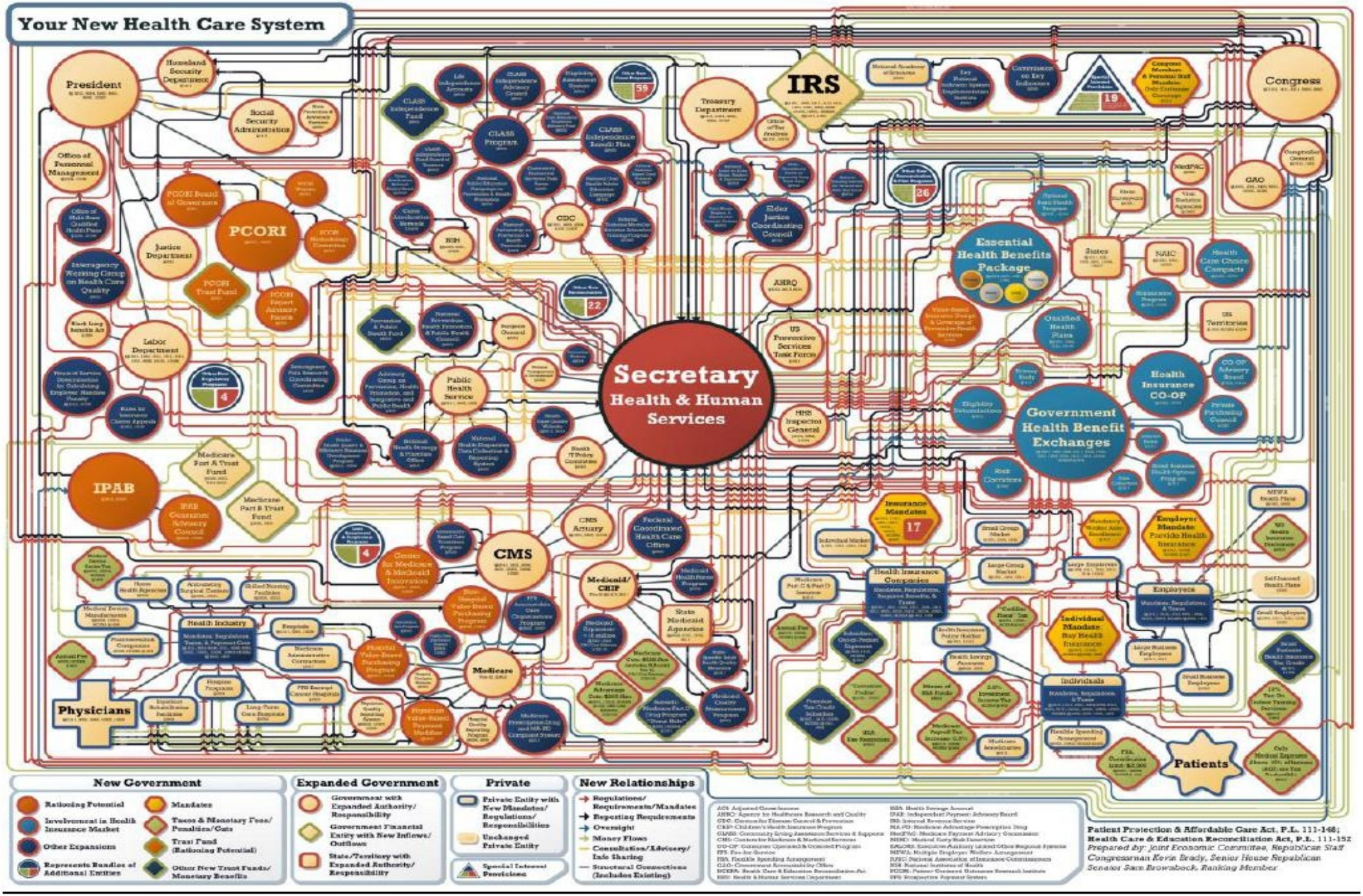
中文 (Chinese) | Kreyòl (French Creole)
한국어 (Korean) | Polski (Polish)
Português (Portuguese) | Español (Spanish)

GET EMAIL UPDATES

Email Address

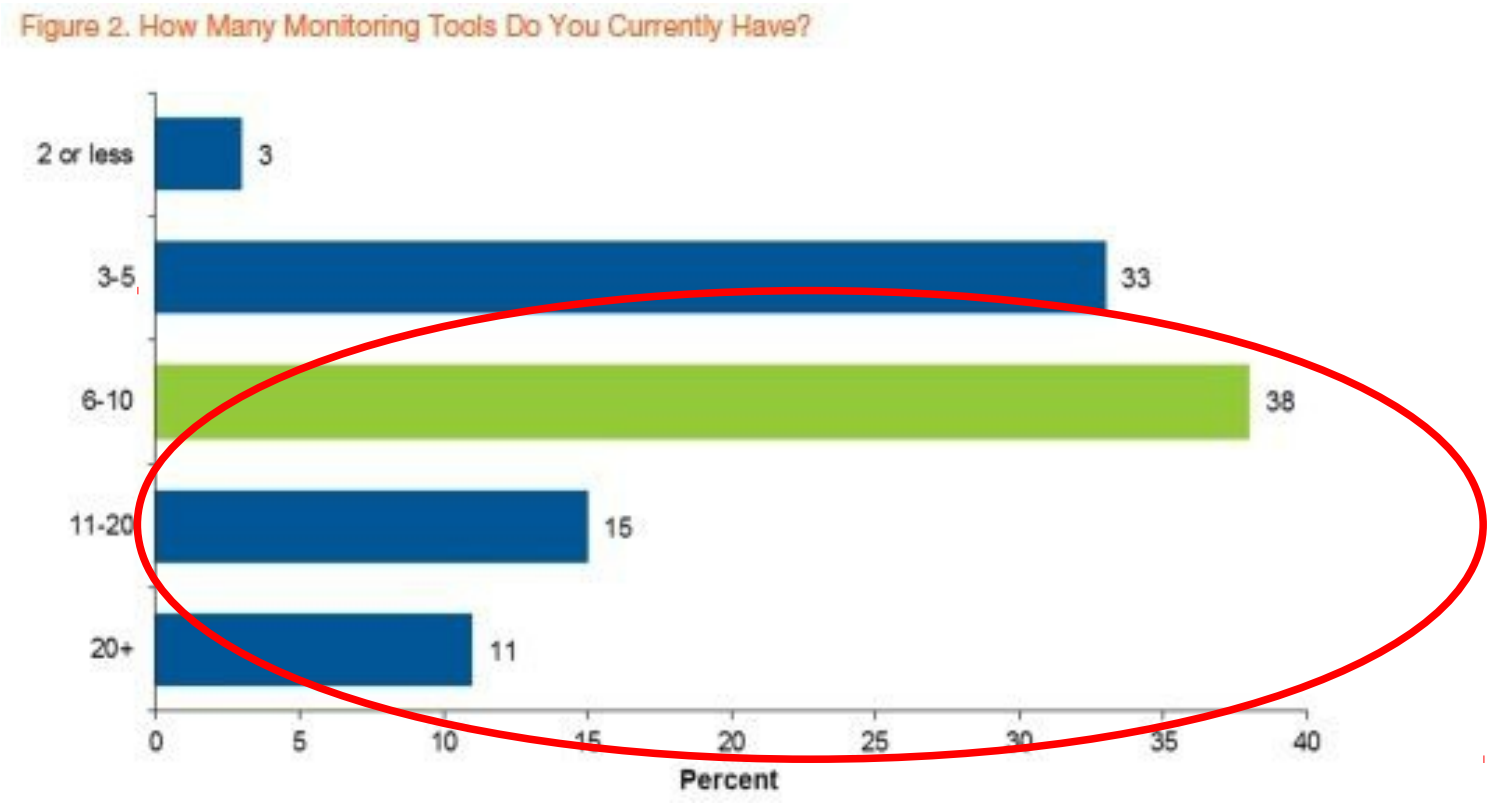
op5

But under the hood….



op5

What do enterprise IT do about it?



- More then 60% of the companies have six or more then 20 different monitoring tools installed in parallel!

op5

op5

op5

Gartner Top Recommendations!

Analyst(s): Jonah Kowall, Colin Fletcher

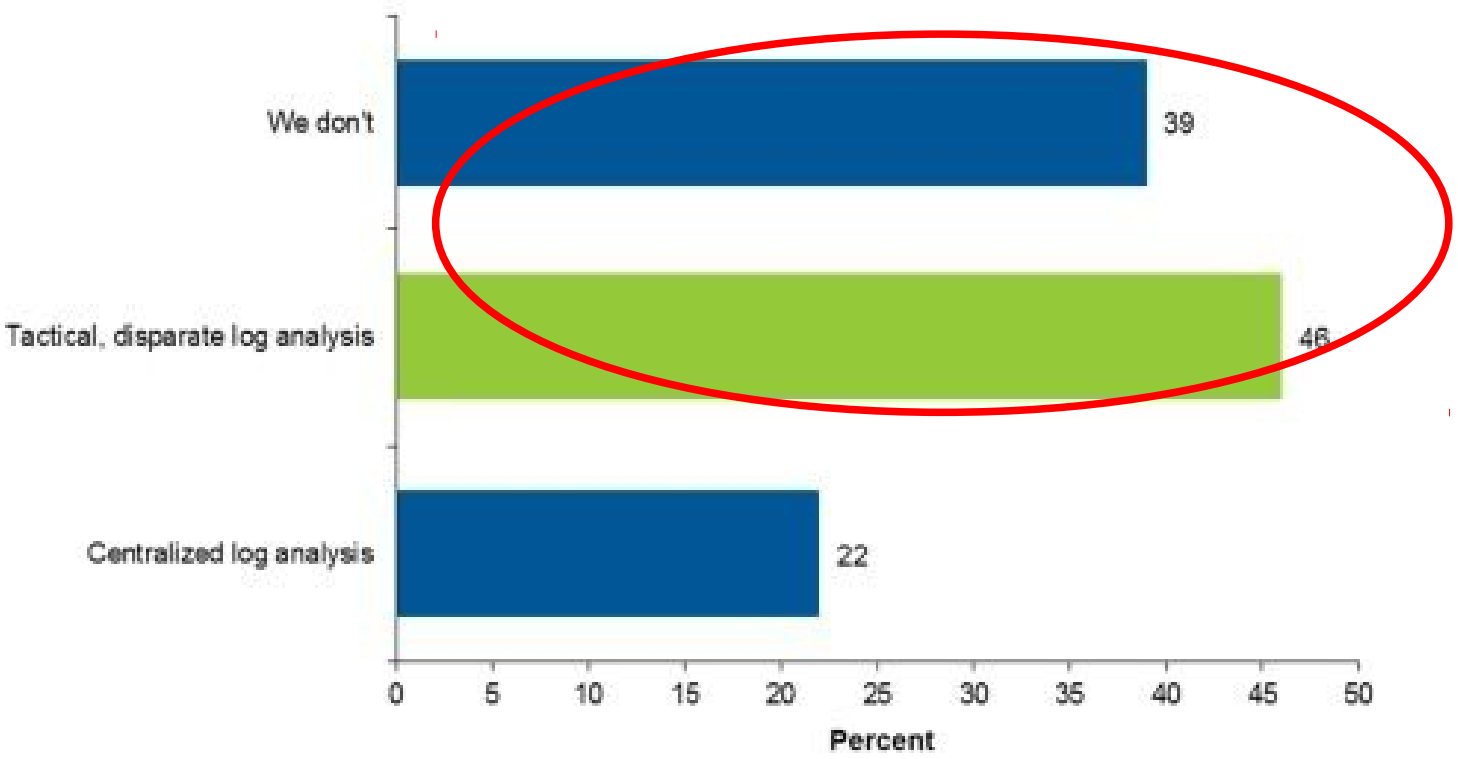
Enterprise I&O teams should combine unified monitoring and log analytics technologies to build a simpler, faster and cost-effective approach to managing the availability of today's highly complex and dynamic environments.

op5

Logs provide unparalleled details on what went wrong
CHECK
mph
40
20
20
0

op5

8 out of 10 of Enterprises lacks the use of continued centralized Log Analysis!

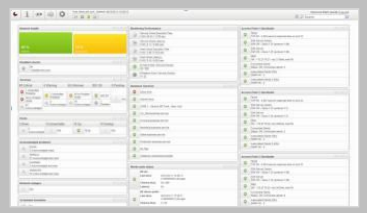


Gartner

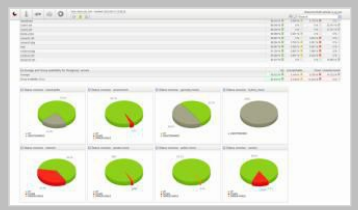
- Implement unified monitoring and log analysis tools to support availability management and goals.
- Implement log analysis to support IT and security operations, foster collaboration across teams, and improve tactical troubleshooting.

op5

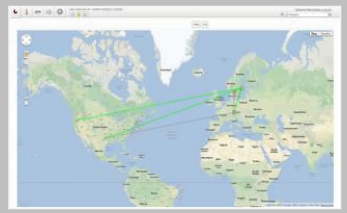
Unified Monitoring including details



Dashboards



Graphs & Reports



Mapping

API

Smart Filters

Event Correlation

Collection Tier

Agent based

Application Servers

Database Servers

Storage Servers

Agent less

Application Servers

Database Servers

Storage Servers

Network Infrastructure

API Rest & Json

Traps & Logs

Software Applications

Cloud Services

Connectivity Providers

op5

Introducing op5 Monitor 7.0

op5 Monitor 7.0

Integrated Logserver

Logger

Logger

- op5 Monitor can now act as a logserver
- Key features
  - Same GUI as Monitor
    - No need to change tool
    - Enrich alerts with logdata
  - New listview type log_messages - possible to use smart filters to create custom views
  - API support for easy and secure integration
  - Same athenticate mechanisms as in op5 Monitor, like LDAP/AD
  - Log reports using smart filters

op5

Screenshots op5 Logger

op5 Monitor » List view - Mozilla Firefox

https://vakttornet/monitor/index.php/listview?q=[log_messages] all

Monitor Admin at vakttornet.mynet | Log out

Search

List view | Log_messages | Count: 34071 | Run query on archive

Severity	Facility	Receive time	Message time	Event ID	Source IP address	Ident	Host	PID	Message
6: info	2: mail	2014-09-10 14:56:57	2014-09-10 14:56:57	0	10.1.1.47	dovecot	mail	0	imap-login: Disconnected (no auth atte handshaking: Disconnected
4: warning	2: mail	2014-09-10 14:56:57	2014-09-10 14:56:57	0	10.1.1.47	dovecot	mail	0	imap-login: Warning: SSL: where=0x10 [10.1.1.87]
3: error	3: daemon	2014-09-10 14:56:57	2014-09-10 14:56:57	0	127.0.0.1	nsca	vakttornet	21742	Received invalid packet type/version fr wrong password or crypto algorithm?
4: warning	2: mail	2014-09-10 14:56:57	2014-09-10 14:56:57	0	10.1.1.47	dovecot	mail	0	imap-login: Warning: SSL: where=0x20 [10.1.1.87]
6: info	10: authpriv	2014-09-10 14:56:56	2014-09-10 14:56:56	0	127.0.0.1	sshd	vakttornet	21738	Did not receive identification string fron
3: error	3: daemon	2014-09-10 14:56:52	2014-09-10 14:56:52	0	127.0.0.1	nsca	vakttornet	21724	Received invalid packet type/version from client - possibly due to client using wrong password or crypto algorithm?
6: info	10: authpriv	2014-09-10 14:56:51	2014-09-10 14:56:51	0	127.0.0.1	sshd	vakttornet	21722	Did not receive identification string from ::1
3: error	3: daemon	2014-09-10 14:56:47	2014-09-10 14:56:47	0	127.0.0.1	nsca	vakttornet	21699	Received invalid packet type/version from client - possibly due to client using wrong password or crypto algorithm?
6: info	10: authpriv	2014-09-10 14:56:46	2014-09-10 14:56:46	0	127.0.0.1	sshd	vakttornet	21691	Did not receive identification string from ::1
3: error	3: daemon	2014-09-10 14:56:42	2014-09-10 14:56:42	0	127.0.0.1	nsca	vakttornet	21679	Received invalid packet type/version from client - possibly due to client using wrong password or crypto algorithm?
5: notice	10: authpriv	2014-09-10 14:56:41	2014-09-10 14:56:41	0	10.1.1.254	sudo	10.1.1.254	0	_nrpe : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/root/scripts /check_openvpn_user.pl -S /tmp/openvpn-status.log -u raspberrypilcd
6: info	10: authpriv	2014-09-10 14:56:41	2014-09-10 14:56:41	0	127.0.0.1	sshd	vakttornet	21677	Did not receive identification string from ::1
6: info	3: daemon	2014-09-10 14:56:39	2014-09-10 14:56:39	0	127.0.0.1	xinetd	vakttornet	6367	START: livestatus pid=21664 from=::ffff:10.8.0.6
6: info	3: daemon	2014-09-10 14:56:39	2014-09-10 14:56:39	0	127.0.0.1	xinetd	vakttornet	6367	EXIT: livestatus status=0 pid=21652 duration=1(sec)
6: info	3: daemon	2014-09-10 14:56:39	2014-09-10 14:56:39	0	127.0.0.1	xinetd	vakttornet	6367	START: livestatus pid=21667 from=::ffff:10.8.0.6
6: info	3: daemon	2014-09-10 14:56:39	2014-09-10 14:56:39	0	127.0.0.1	xinetd	vakttornet	6367	EXIT: livestatus status=0 pid=21664 duration=0(sec)
6: info	3: daemon	2014-09-10 14:56:39	2014-09-10 14:56:39	0	127.0.0.1	xinetd	vakttornet	6367	EXIT: livestatus status=0 pid=21667 duration=0(sec)

Run query on archive

Query: [log_messages] all

Start time

yesterday

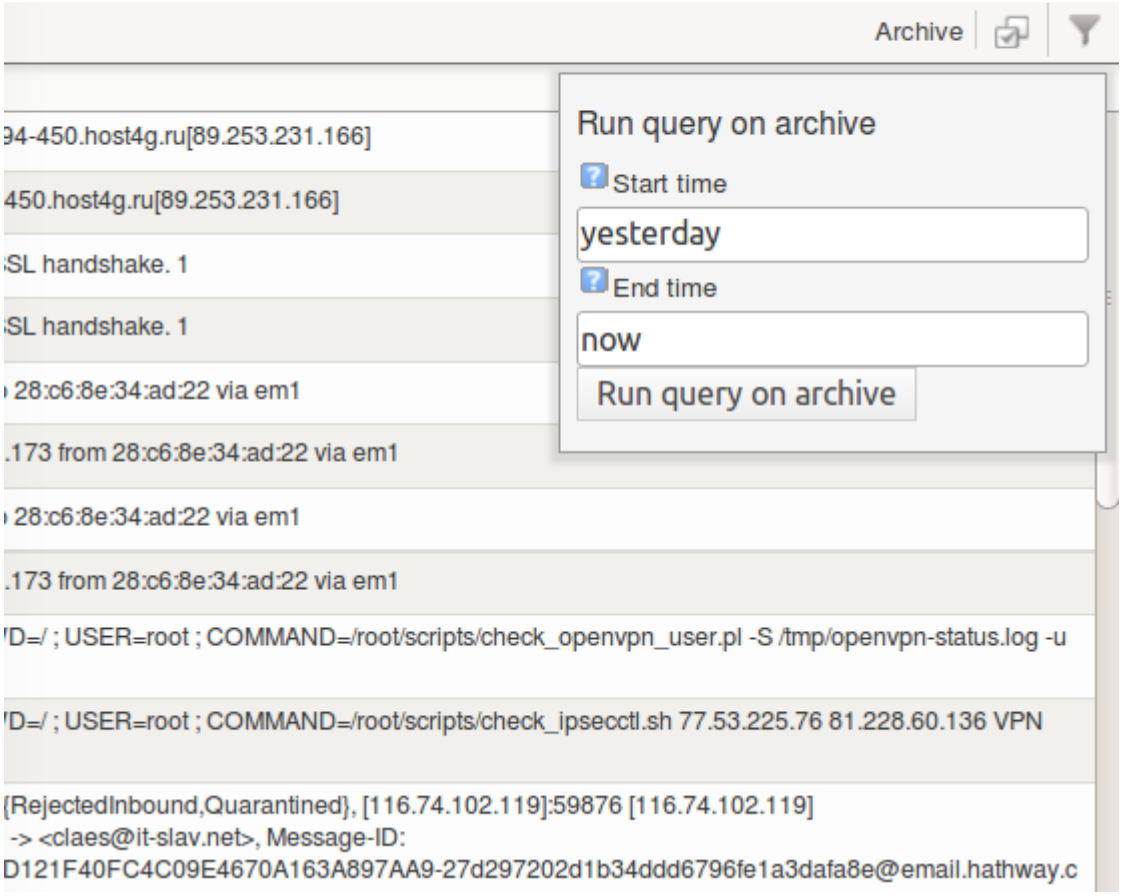
End time

now

Run query on archive

op5 Logger queries

- Logger queries
  - “Human” timestamp
  - Runs on active filter



op5 Logger report

op5 Monitor » Log archive search - Mozilla Firefox

https://vakttornet/monitor/index.php/logger/generate?start_time=today+00%3A00&end_time=now&query=[log_messages]+all

Monitor Admin at vakttornet.mynet | Log out

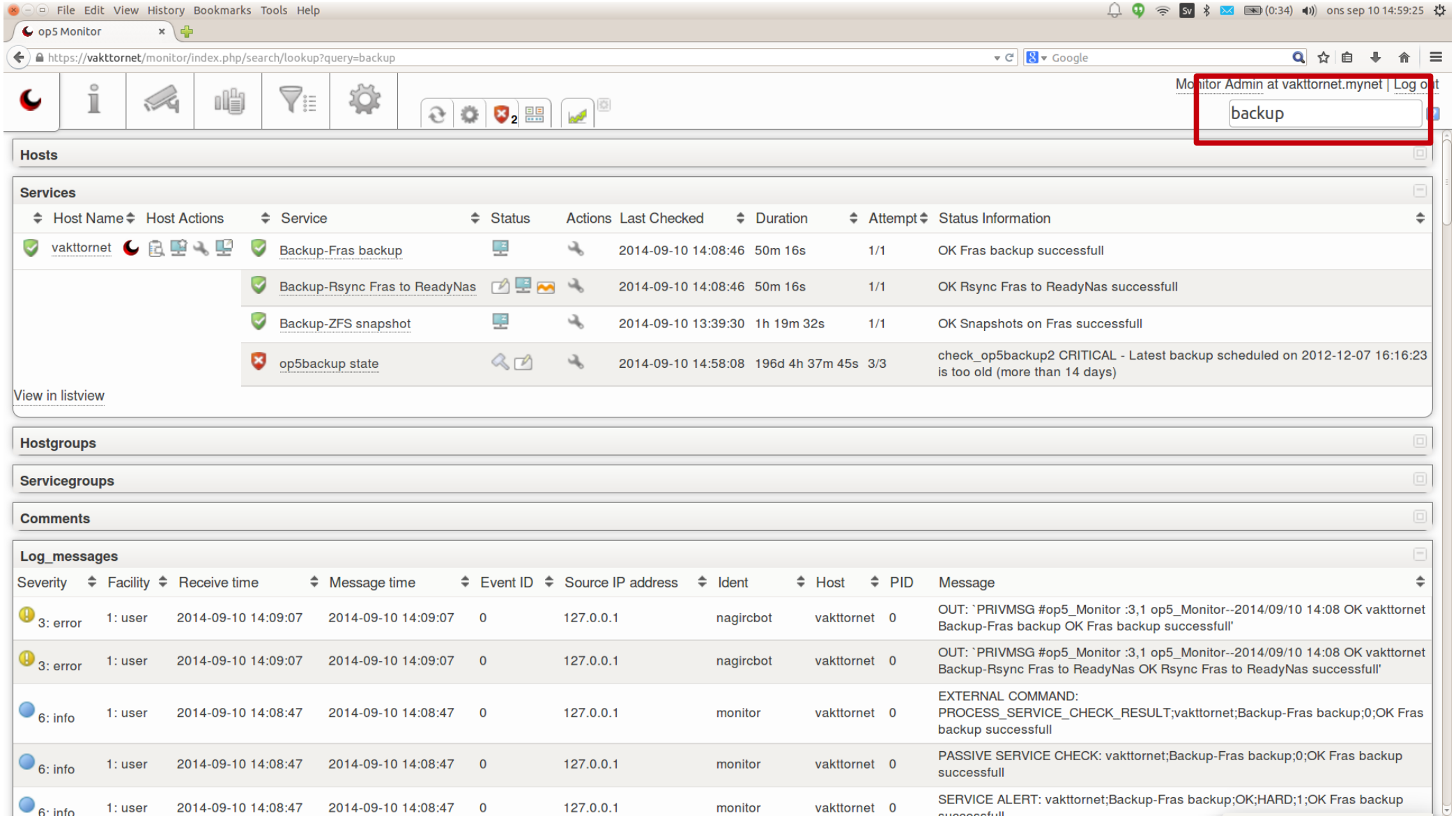
Search

Log archive search

Reporting period: From **2014-09-10 00:00:00** to **2014-09-10 15:00:13**

Source IP address	Receive time	Facility	Severity	Message time	Host	Ident	PID	Event	Message
127.0.0.1	2014-09-10 08:55:52	syslog	notice	2014-09-10 08:55:52	vakttornet	syslog-ng	1216	0	syslog-ng starting up; version='3.3.7'
127.0.0.1	2014-09-10 08:55:52	user	info	2014-09-10 08:55:52	vakttornet	yum	29541	0	Installed: op5-syslog-ng-4.0.0-op5.1.el6.x86_64
127.0.0.1	2014-09-10 08:55:53	user	info	2014-09-10 08:55:53	vakttornet	yum	29541	0	Installed: op5-logserver-gui-7.0.4-op5.1.el6.noarch
127.0.0.1	2014-09-10 08:55:54	authpriv	info	2014-09-10 08:55:54	vakttornet	sshd	1258	0	Did not receive identification string from ::1
127.0.0.1	2014-09-10 08:55:54	daemon	error	2014-09-10 08:55:54	vakttornet	nsca	1259	0	Received invalid packet type/version from client - possibly due to client using wrong password or crypto algorithm?
127.0.0.1	2014-09-10 08:55:54	authpriv	notice	2014-09-10 08:55:54	vakttornet	sudo	0	0	nobody : TTY=unknown ; PWD=/ ; USER=monitor ; COMMAND=/usr/bin/mon check latency service
127.0.0.1	2014-09-10 08:55:55	user	info	2014-09-10 08:55:55	vakttornet	python	0	0	op5keepalived reporting in. pid = 1273; session id = 1272;
127.0.0.1	2014-09-10 08:55:55	user	info	2014-09-10 08:55:55	vakttornet	yum	29541	0	Installed: op5-logger-backup-7.0.0-op5.1.el6.x86_64
127.0.0.1	2014-09-10 08:55:55	user	info	2014-09-10 08:55:55	vakttornet	yum	29541	0	Updated: op5kad-0.0.7-op5.1.x86_64
127.0.0.1	2014-09-10 08:55:56	user	info	2014-09-10 08:55:56	vakttornet	monitor	0	0	livestatus: Socket thread has terminated
	2014-09-10			2014-09-10					

Direct search



Information sources

Active checks

- "Normal way"
- Scheduled by op5 Monitor
- Example
  - SNMP get
  - check_http
  - CPU load via agent
  - WMI

Passive checks

- External scheduler
- Example
  - Backup job
  - Plugin that take looong time to run

Log messages

- Windows logs
- Debug
- Alert Enrichment
- Regulations like PCI
- Examples
  - Transaction
  - Application data
  - Firewall info
  - Security information

SNMPtraps

- Communication equipement
- Common appliance
- "Standard"
- Example
  - Routers
  - Switches
  - Printers
  - PBX

op5

API improvements

External Commands

- Ack. Hostproblem
- Ack. Service problems
- Schedule downtime
- Passive check result host
- Passive check result service
- Schedule host check
- Schedule service check
- Example
  - Mobile clients
  - 3rd party ticket handling

Filter

- Query
- Listviews
- (incl.traps and log messages)
- Count

Status

- Host, service, notifications etc.
- Host group, service group
- Example
  - External view
  - Visualisation
  - Ticket handling
  - Customer portal

op5 Monitor

REST/API

Configuration

- Input
- Output
- Change
- Example
  - CMDB's
  - Inventory
  - Mass-update, delete, change

API

XML, JSON, HTML

Report

- Report data
- Example
  - Ticket handling systems
  - 3rd party clients
  - Report tool

op5

Current op5 Logserver

- **Fully supported**
- We recommend trying the new Logger version in parallel with your old system and contact us when you are ready to upgrade.
- You cannot seamless upgrade your standalone current op5 Logserver to op5 Logger

- Contact us for a technical assistance if you want help with migration to op5 Logger

op5

Example, logger integration

Root cause analysis

Host Name	Host Actions	Service	Status	Actions	Last Checked	Duration	Attempt	Status Information	Logger
aftonbladet.se		HTTP Server			2014-09-05 11:37:21	1d 21h 12m 24s	1/3	HTTP OK: HTTP/1.1 301 Moved Permanently - 216 bytes in 0.017 second response time	Logger
dn.se		HTTP Server			2014-09-05 11:37:48	1d 21h 11m 57s	1/3	HTTP OK: HTTP/1.0 301 Moved Permanently - 116 bytes in 0.028 second response time	Logger
monitor		CPU - IO wait			2014-09-05 11:35:58	3d 18h 3m 50s	1/3	CPU OK : iowait 0.00%	Logger
		CPU - Idle			2014-09-05 11:37:12	7m 33s	1/3	CPU OK : idle 58.95%	Logger
		CPU - System usage			2014-09-05 11:37:54	24d 21h 21m 59s	1/3	CPU OK : system 10.00%	Logger
		Critical Syslog messages			2014-09-05 11:35:43	2h 14m 2s	1/3	FILTER OK - Log filter contains 0 logs	Logger
		Cron process			2014-09-05 11:38:15	24d 21h 21m 51s	1/3	PROCS OK: 1 process with command name 'crond'	Logger
		Dell open manage			2014-09-05 11:38:56	25d 22m 18s	3/3	ERROR: Alarm signal (Nagios time-out)	Logger
		Dell open manage global			2014-09-05 11:38:33	25d 22m 23s	3/3	ERROR: Alarm signal (Nagios time-out)	Logger

List view | Log_messages | Count: 112437 | Run query on archive

Severity	Facility	Receive time	Message time	Event ID	Source IP address	Ident	Host	PID	Message
5: notice	10: authpriv	2014-09-05 11:37:19	2014-09-05 11:37:19	0	127.0.0.1	dell-openmanage	maint70head	0	Dell Open Manage crashed
5: notice	10: authpriv	2014-09-05 11:36:47	2014-09-05 11:36:47	0	127.0.0.1	sudo	maint70head	0	nobody : TTY=unknown ; PWD=/ ; USER=monitor ; COMMAND=/usr /bin/mon check latency service
5: notice	10: authpriv	2014-09-05 11:36:40	2014-09-05 11:36:40	0	127.0.0.1	sudo	maint70head	0	nobody : TTY=unknown ; PWD=/ ; USER=monitor ; COMMAND=/usr /bin/mon check exectime service

op5

Features

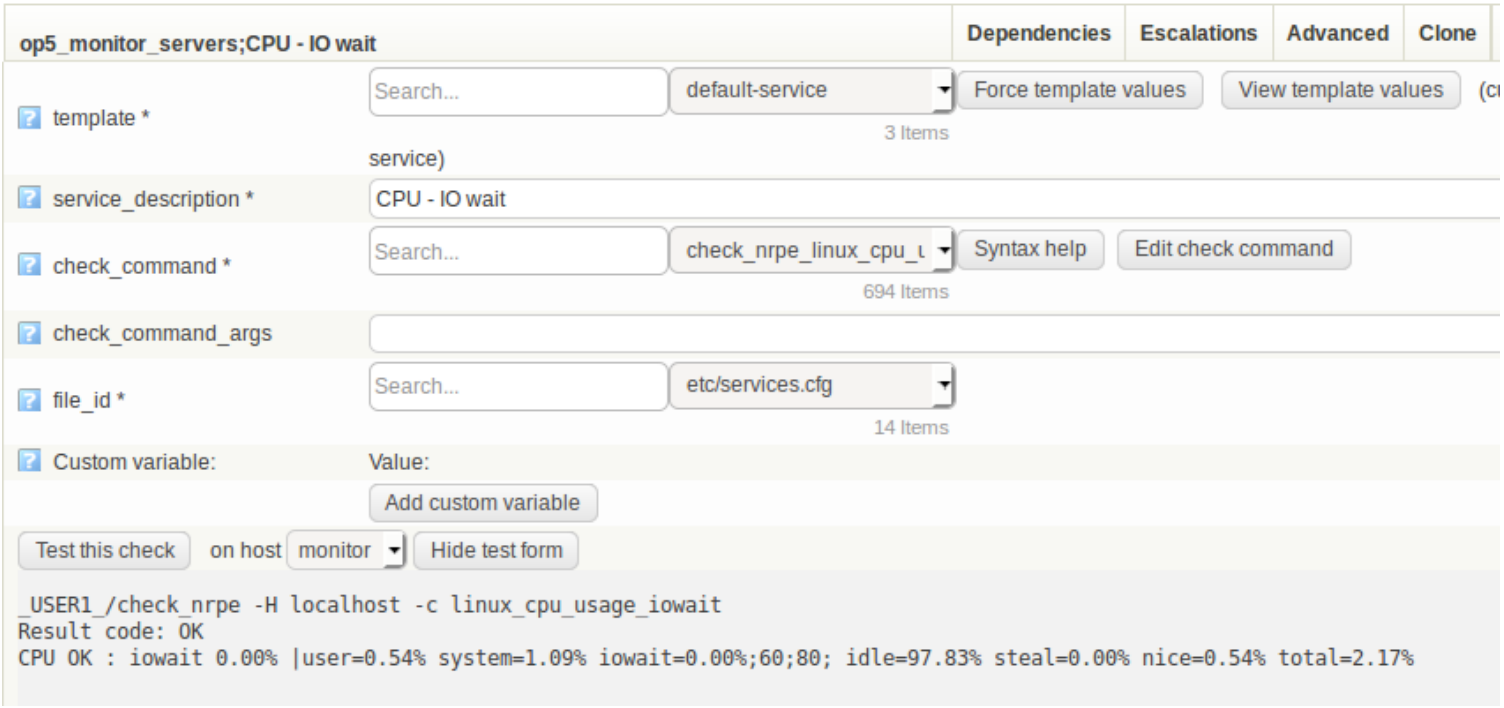
Features

- Faster filtering in dialogue boxes.
  - Tests show that it can handle more then 100 000 objects
- Easier to define time-based filters.
- Possibility to show long plugin output in csv reports.
- Security enhancements in PNP and Nagvis by protecting cookies better.
- Manuals moved to online to ensuring the latest version is available

op5

Features

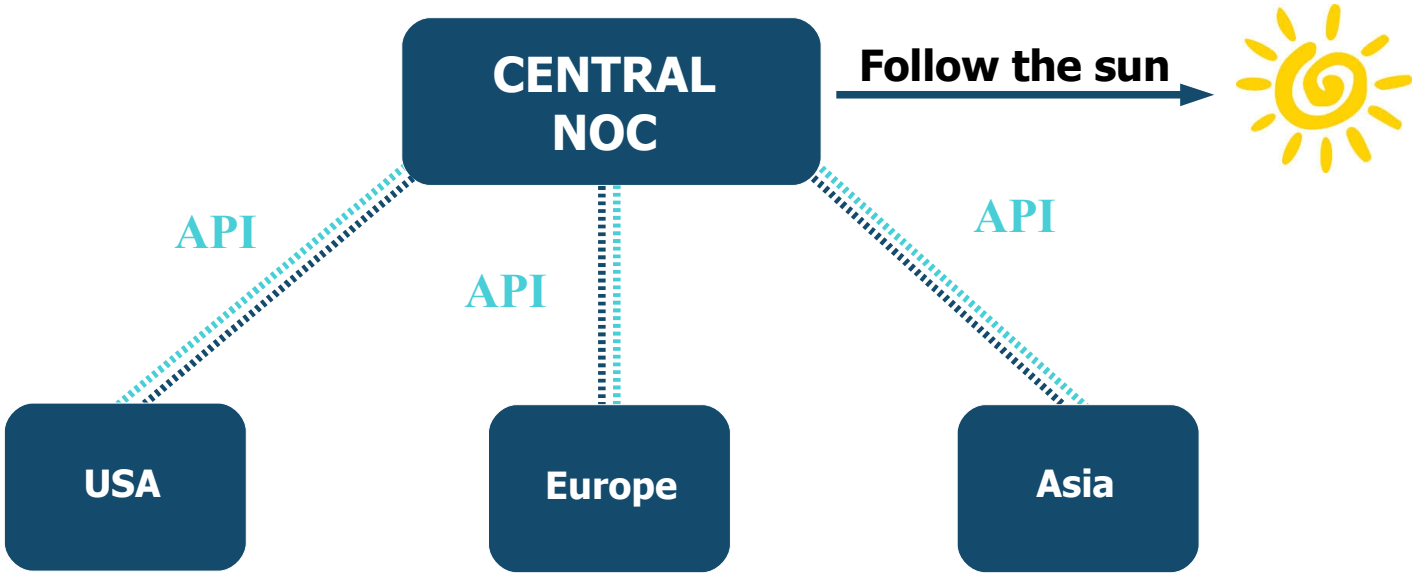
- Enhancement to “Test this button”
  - Added the possibility to select which host to use if the service is on a hostgroup.
  - Made it easier to re-try the execution.



Plugins

op5 HTTP API Plugin

- A plugin to easily query the op5 HTTP API on the same or a remote op5 Monitor host.
  - Makes it possible to have one central monitor system that gathers information from others via the API.
  - In combination with list filters very powerful possibilities arises, like:



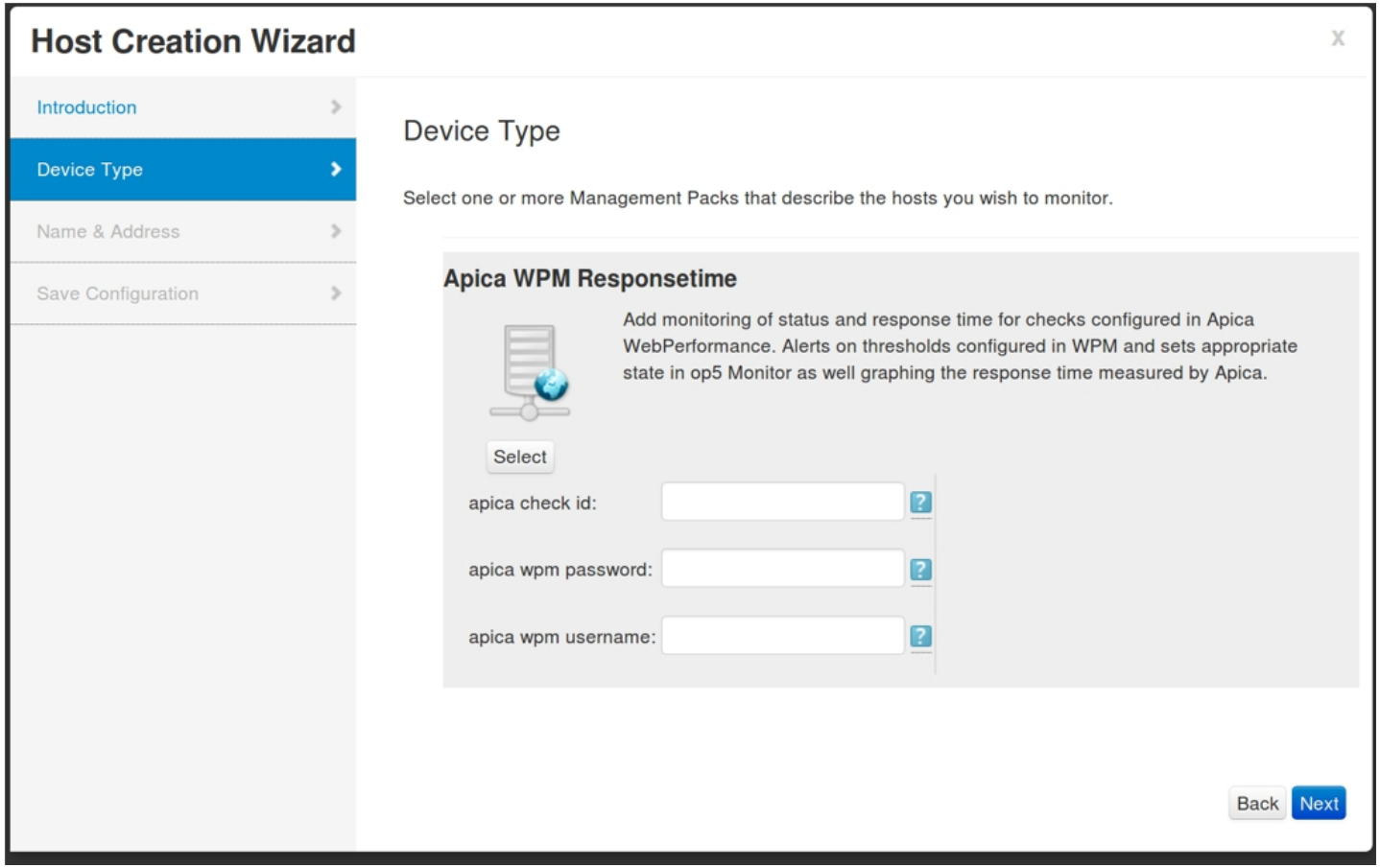
- Core Net **US**
- Core DB **US**
- Core APP **US**

- Core Net **EU**
- Core DB **EU**
- Core APP **EU**

- Core Net **AS**
- Core DB **AS**
- Core APP **AS**

Apica Plug-in

- New plugin: check_apica_responsetime
- Corresponding management pack to monitor status and response time for checks configured in Apica WebPerformance.



op5 Mobile App

op5 Mobile App

- App for IOS (7.x) & Android (4.x)
  - Check the IT environment whenever, wherever

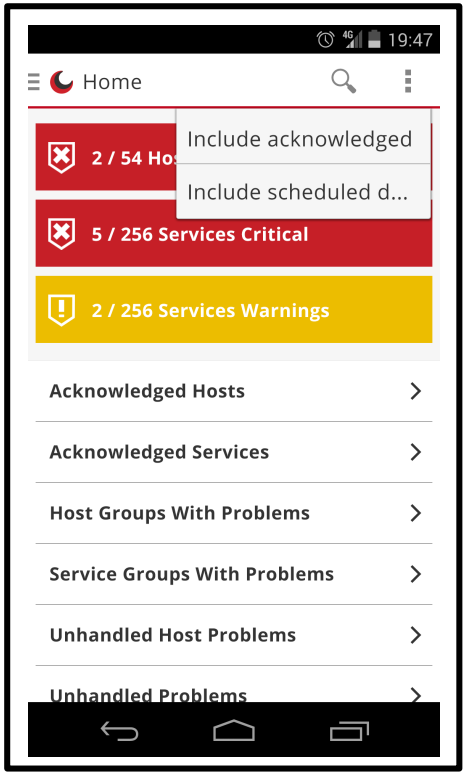
- Main features:
  - All communication goes over secure API
    - All major solution today generally availible are built upon the old unsecured CGI
  - Full support for Listview
    - Host, services, status etc
  - Clear colour marks for status
    - Direct links to problem
    - Acknowledge in app

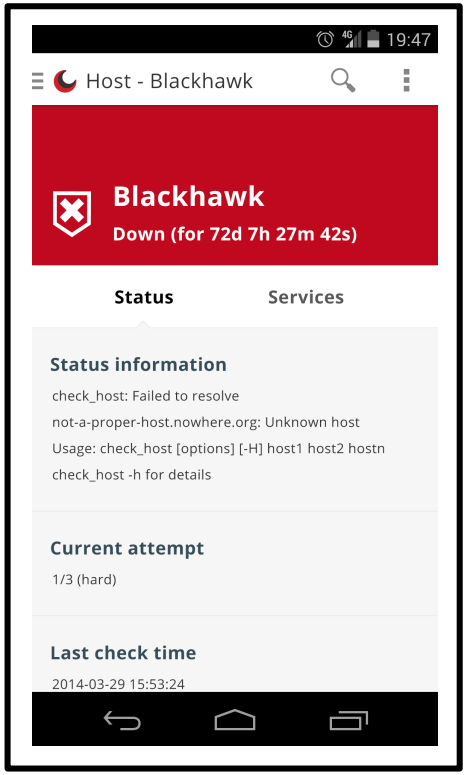
App Store

Google play

op5

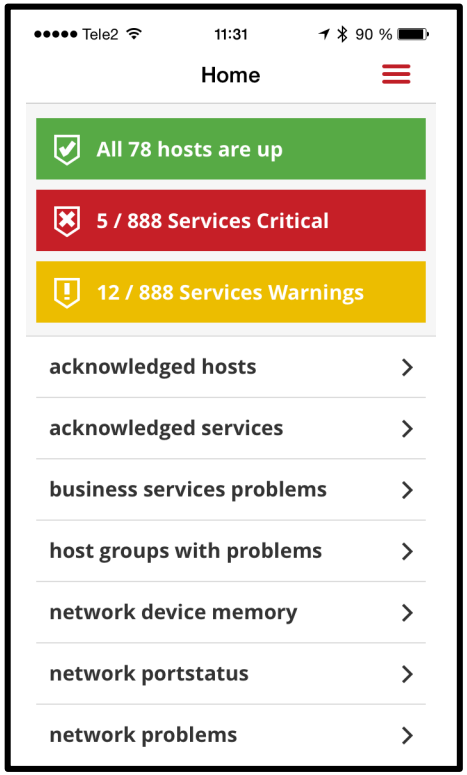
op5 Mobile App

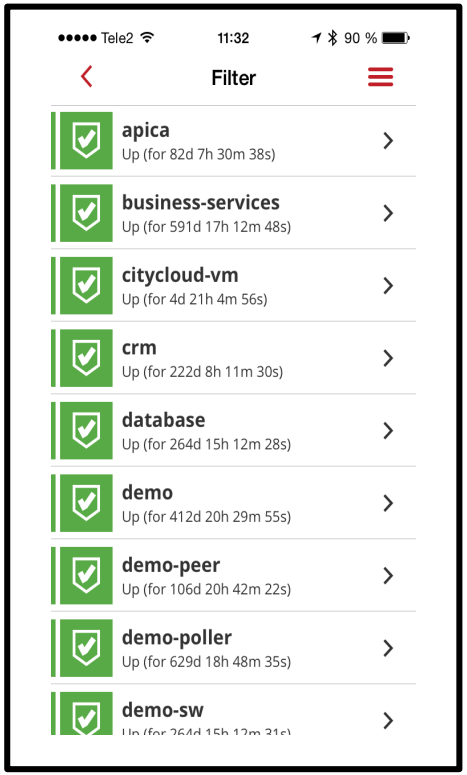




- Screenshots Android

- Screenshots iPhone





op5

Q/A

Knowledge base

Visit our Knowledge Base

Visit our Knowledge base: https://kb.op5.com

You will find manuals, how-to´s, management packs, tips and tricks and many other interesting spaces to browse through.

Get in touch

Get in touch with us

info@op5.com

cr@op5.com

Please contact us for a one-to-one demo or if you have a question