Who is Karsten?

- CTO, Netic A/S

- Splunk Deployment Architect

Agenda:

- Netic
- Splunk
- Use Cases in FMK
- Q&A

a NoSQL database with benefits :)

Karsten Thygesen
karthy@netic.dk

Netic A/S

- Netic
  - Founded in 2002
  - Private funded
  - HQ in Aalborg
  - 20 employees
  - Multiple datacenters
- Business Areas
  - Hosting
  - **Operations**
  - Consultancy, Infrastructure
  - SW Development
  - Splunk
- References
  - Fælles Medicinkort
  - National Service Platform
  - Sundhedsdatan et-tet
  - vaccinations-registret
  - Nemhandel-registret
  - Debitorregistret

Splunk=Engine for Machine Data

Collect and Index

Any log files
Custom applications
Web servers
User clickstream
Social platforms
Servers/Hypervisors/VM's
Configs
Telecoms devices
Storage devices
Network devices
Security devices
Firewalls, IDS
Databases
Web services
System metrics
GPS
DNS, DHCP
AAA logs
Proxy servers
Scripts
Sensors

Splunk IT

~~Connectors~~ ~~Schemas~~
~~Databases~~ ~~Limits~~

Identification

Jun 12 11:38:19 server sshd[13375]: error: PAM authentication error user=karthy srcip=62.116.207.26

Jun 12 11:38:21 server sshd[13375]: error: PAM authentication error user=karthy srcip=129.42.38.1

Common Uses and Maturity

Business Insights	Value
Operational Visibility	Service
Proactive Monitoring	Proactive
Search + Investigate	Reactive

splunk> POWERED

Differentiate

- RealTime Architecture
- Universal Machine Data platform
- Schema on the fly
- Fast time to Value
- Agile Reporting and Analytics
- Scales from Deskto to Enterprise
- Passionate and Vibrant community

Our Solution

- App Development
- App Management
- IT Operations
- Security & Compliance
- Web Intelligence
- Business Analytics

Developer Framework

splunk>

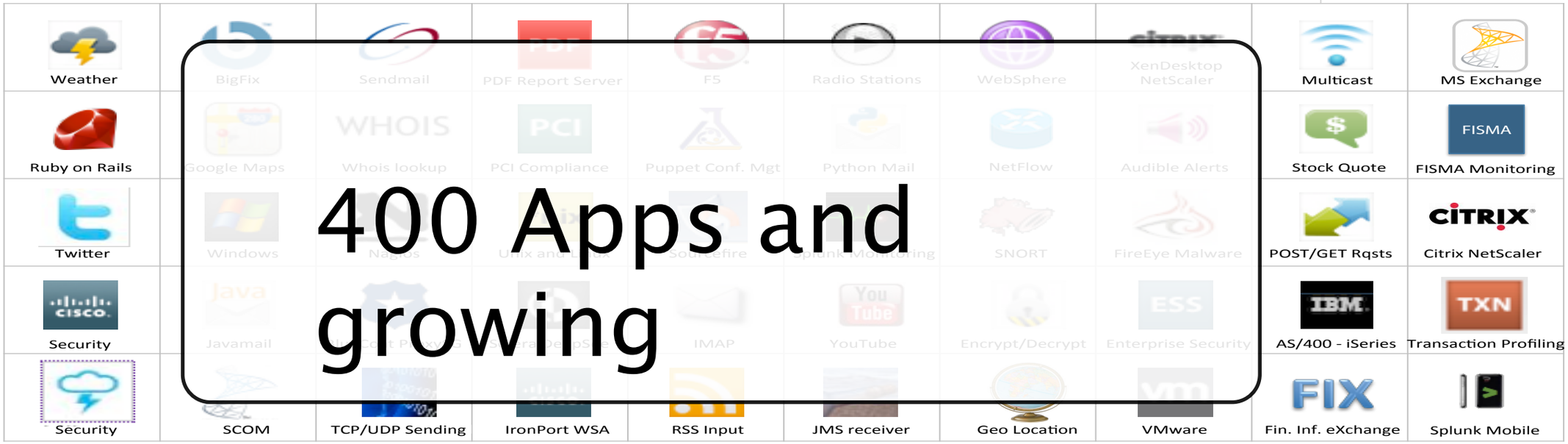
Splunk Apps Let You Do More

Community

Technology Partners

Developers

Splunk Built



400 Apps and growing

DEVELOPER FRAMEWORK

splunk>

Splunk for Exchange

splunk> POWERED Microsoft® Exchange Server

Karsten Thygesen | App | Manager | Alerts | Jobs | Logout

Home | Search | Operations | Message Tracking | Client Behavior | Capacity Planning | Help | About

Overview | Actions

search | Last 24 hours

DNSBL Reputation

Every 4 hours, the Splunk App for Microsoft Exchange checks a variety of DNSBL servers to see if the outbound mail servers (listed in reputation.conf) are listed. Click through to see which servers are actually listing your outbound mail servers.

DNSBL Reputation:

Service Availability

This chart shows systems that are not running services that they are meant to be running given their role.

	Name	Service
1	# Problem Services	0

Non-Reporting Servers

This table shows the Microsoft Exchange hosts that have not reported within 30 minutes. This may indicate a problem with data collection on that host.

	host	Idle Time
1	# Problem Servers	0

Source Types

« prev 1 2 next »

	sourcetype	Events
1	MSExchange:2010:Folder-Usage	58079896
2	MSWindows:2008R2:IIS	37618247
3	MSExchange:2010:MessageTracking	1647991
4	MSExchange:2010:Mailbox-Usage	745873
5	MSExchange:2010:Topology	171334
6	MSExchange:Reputation	136240
7	MSExchange:2010:DatabaseRedundancyStatus	133967
8	MSExchange:2010:Usage	68395
9	MSExchange:2010:ServerQueues	67990
10	MSExchange:2010:DatabasereplicationHealth	67935

Message Rate

Msgs/Hour

Hosts

	host	Events
1	ex02.mshosting.local	8545612
2	ex01.mshosting.local	2776738
3	cas01.mshosting.local	1158104

Active Directory

splunk> POWERED

Windows Server Active Directory

Karsten Thygesen | App | Manager | Alerts | Jobs | Logout

Home | Search | Operations | Security | Change Mgmt | Help | About

Topology Report | Actions

Active Directory Topology Report

Last 60 minutes

This dashboard gives you a topology report for the entire Active Directory infrastructure being monitored.

Forest	Site	Domain	Server
mshosting.local	Aalborg	mshosting.local	ad01.mshosting.local ad02.mshosting.local

Forest: mshosting.local (Windows2008R2Forest), Domain: MSHOSTING\mshosting.local (Windows2008R2Domain)

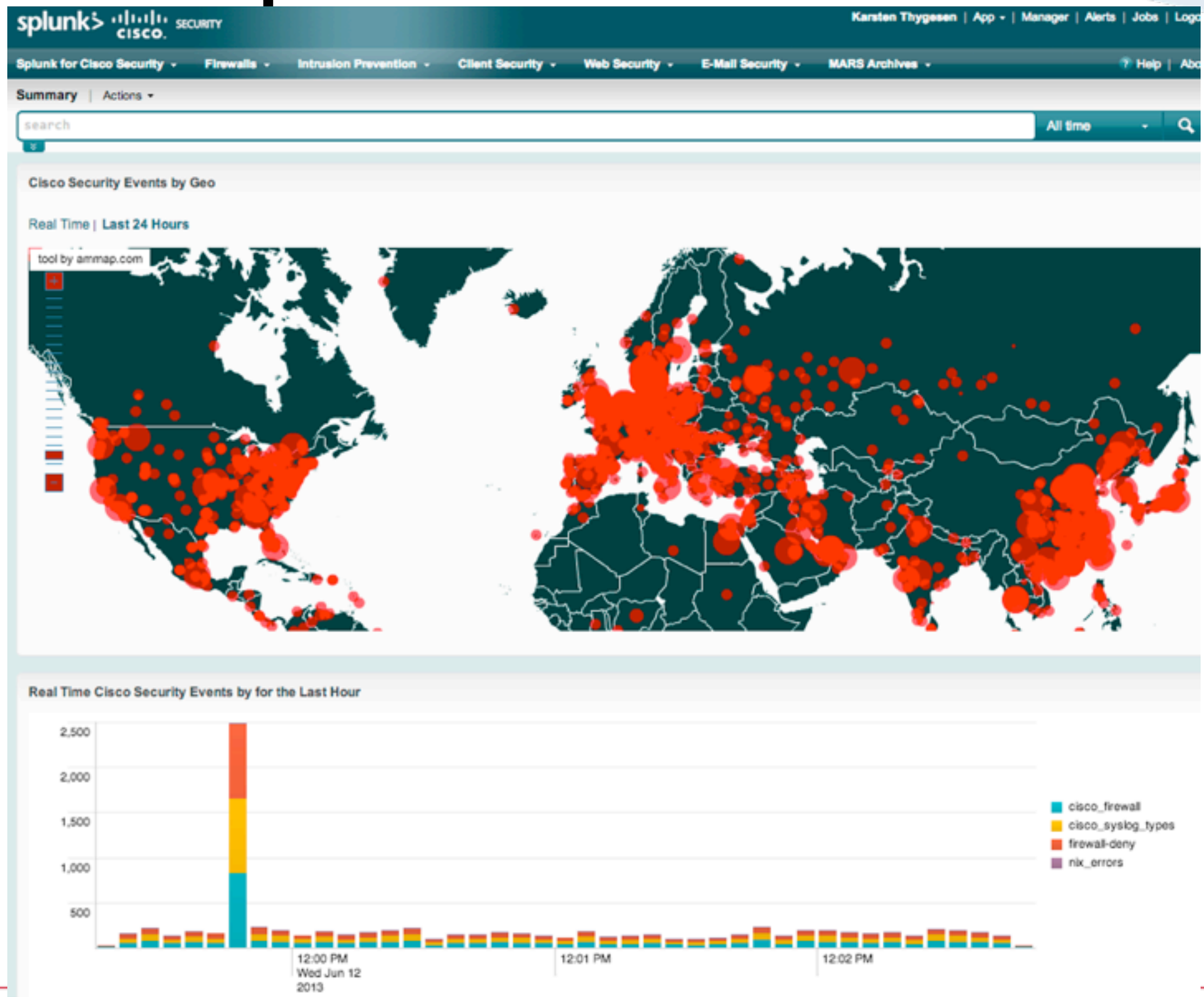
Show 10 entries

Search:

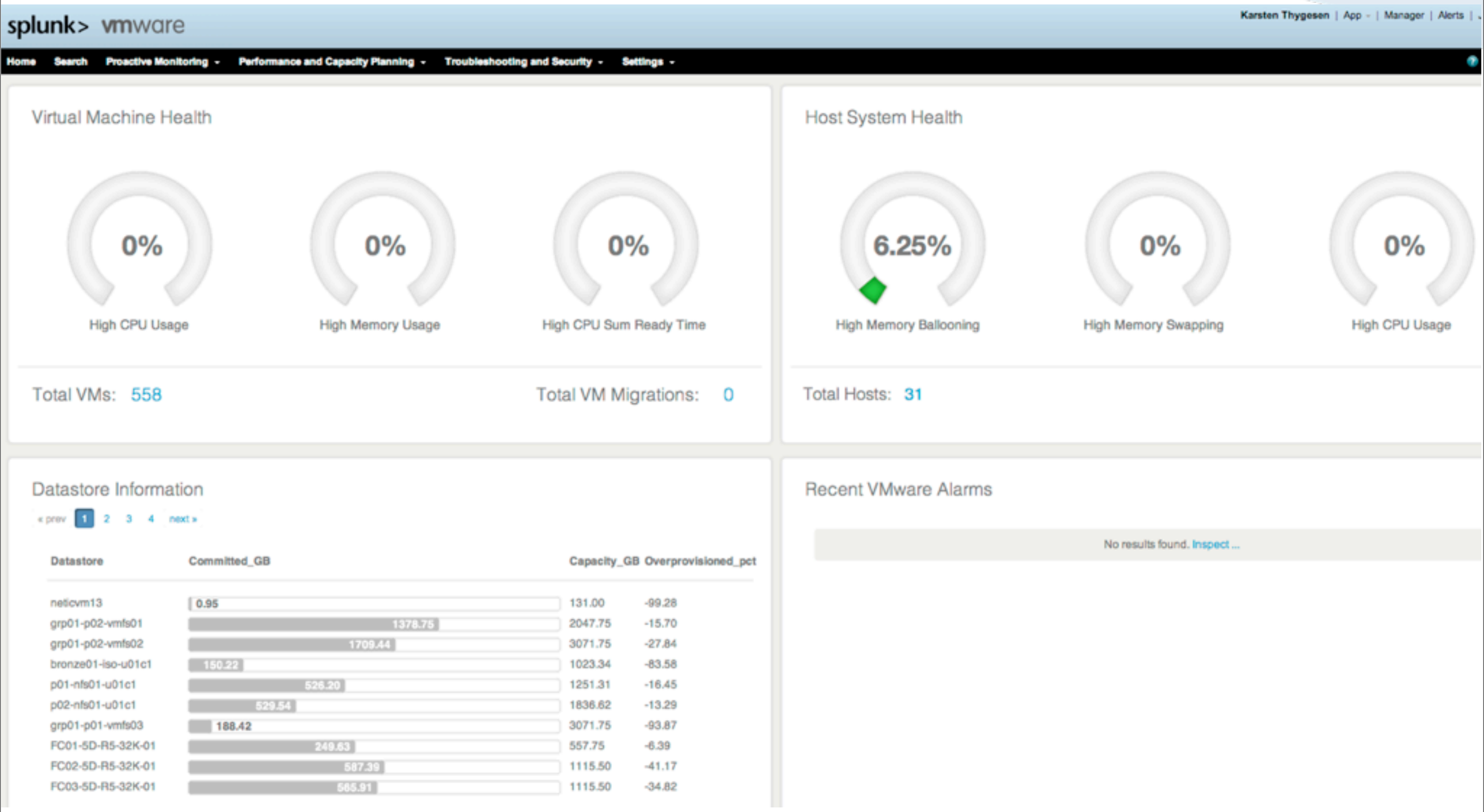
Host	Site	Operating System	Version	Master Roles	DSA Options	Services	DNS Registration	SYSVOL Shared
ad01.mshosting.local	Aalborg	Windows Server 2008 R2 Standard	6.1 (7601)	S D P R I				
ad02.mshosting.local	Aalborg	Windows Server 2008 R2 Standard	6.1 (7601)					

Showing 1 to 2 of 2 entries

Splunk for Cisco



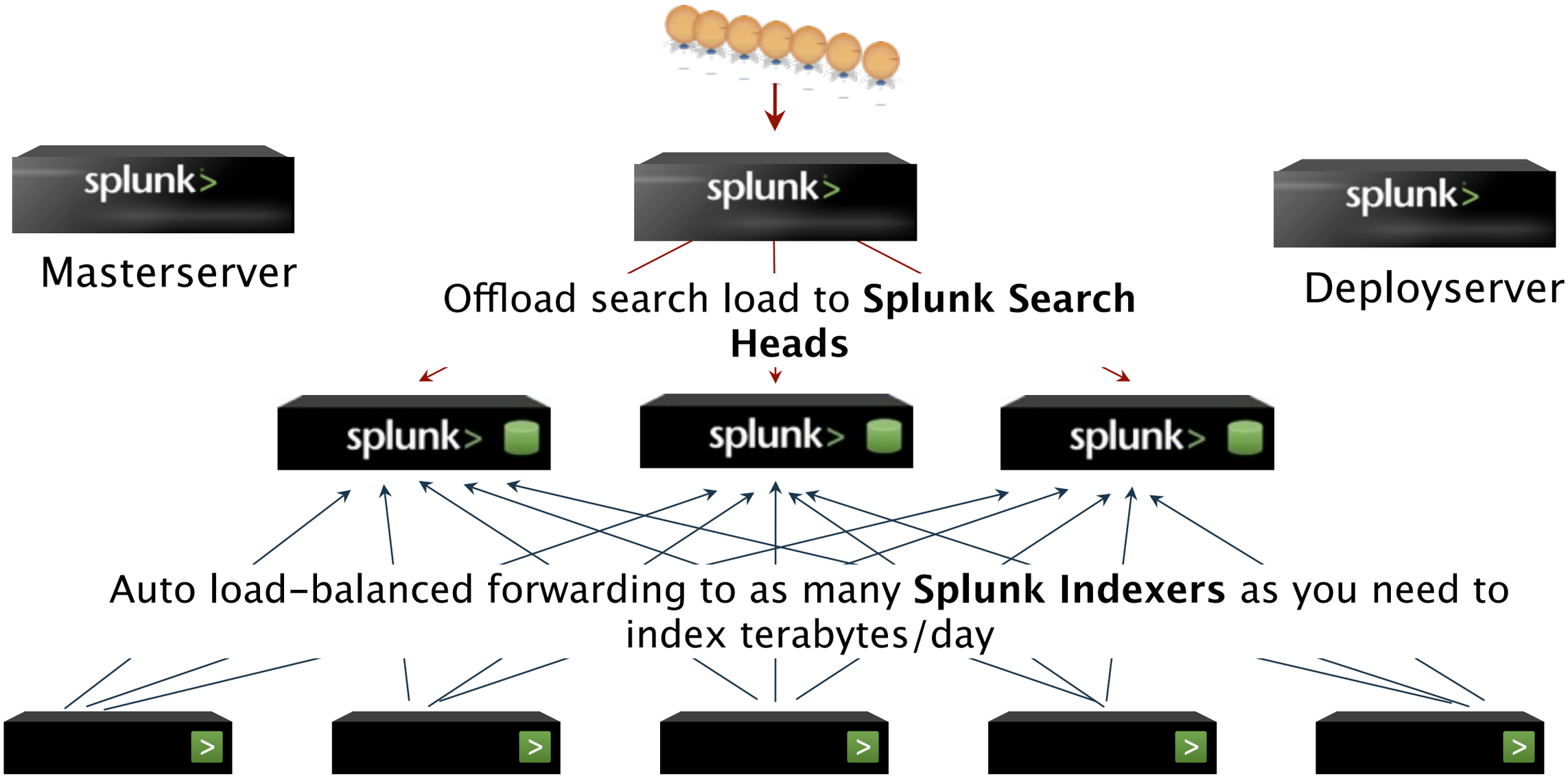
Splunk for VMWare



Custom Apps


splunk> Trifork FMK
Karsten Thygesen | App | Manager | Alerts | Jobs | Logout
Dashboards | Staging Dashboards | Opfølgning | Reports | Form searches | Search views | Searches | Unclassified
Help | About
wall view
Print | Schedule PDF Delivery | Generate PDF | Edit: On Off
kald pr. min seneste 4 timer
12m ago
909
808
707
606
505
404
303
202
101
time
today
last_week
View results
Kald pr. min (1min sampling, 1 min window)
real-time
0
200
400
600
800
1,000
1,200
597
View results
System fejl (sidste 8 timer)
13m ago
PEMException
SAXParseException
SocketTi...xception
Fejl
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
Antal
View results
95 percentil zxtm_internal_timing (5min sampling)
3m ago
Svartid (sec)
3
2
1
9:00 AM
Wed Jun 12
2013
10:00 AM
11:00 AM
null
perc90_Other
average_Other
perc90_l...eceptcall
average_...eceptcall
View results
FMK_requst pr min pr host (2 min sampling, 4 t window)
13m ago
400
200
8:00 AM
Wed Jun 12
2013
9:00 AM
10:00 AM
11:00 AM
_time
prod01...etic.dk
prod02...etic.dk
prod03...etic.dk
prod04...etic.dk
View results
Max requests/min fordelt på uger (2 min sampling)
14h ago
Max requests / min
1,500
1,000
500
15 16 17 18 19 20 21 22 23 24
Uge
max(count2)
View results
Antal Applikationsfejl
13m ago
Sidste 24 Timer
30 dages gennemsnit
Antal
100
10
113
118
120
121
130
134
139
212
Fejlkode
%-del af langsomme kald
3m ago
100
75
50
25
8:00 AM
Wed Jun 12
2013
9:00 AM
10:00 AM
11:00 AM
_time
AttachOrDetachPrescr
CreateDM
CreatePrescript
GetDM
GetMC
GetMCPDF
GetMCVersion
NULL
OTHER
SetReviewed
UpdateDM
UpdateMC

Massive Linear Scalability to Tens of



FMK – Fælles Medicin Kort (Common Medicine card)

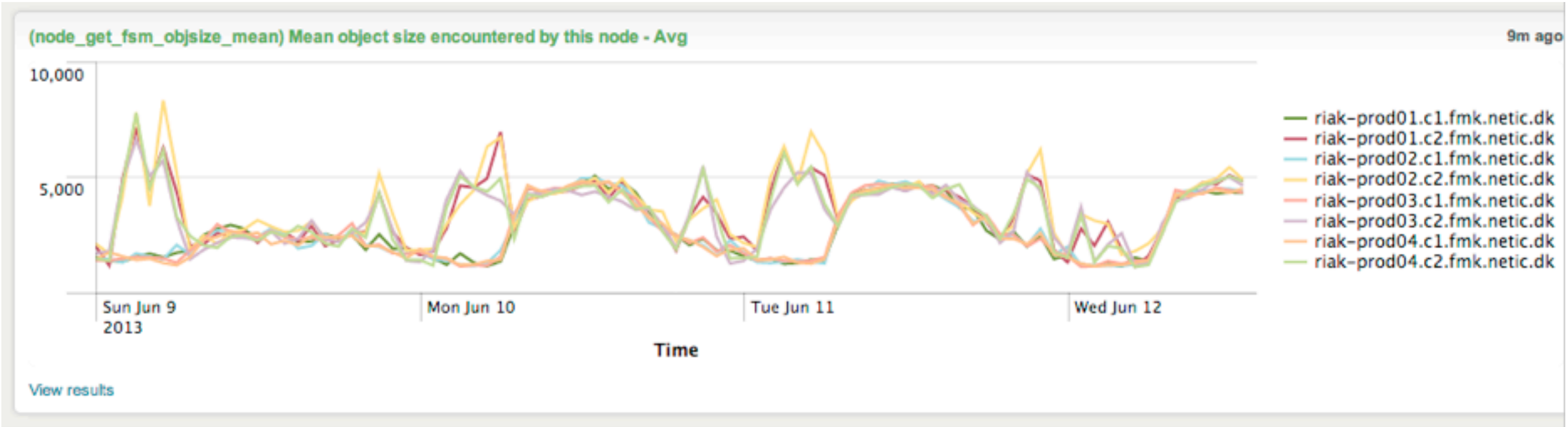
- Record of danish citizens medicin usage
- Nominated “digitaliseringsprisen” in 2011
- Total of ~130 servers in two datacenters
- One of the first “real” systems to use NoSQL (Riak)
- Developed by Trifork, Operations by Netic

FMK Use Cases

- Usage statistics
  - –Group by usertype, location, EPJ system, time of day/week...
- Performance
  - –Avg/95-percentile responsetime by call type, by client, by anything
  - –Pinpoint bad user experience
  - –SLA reporting

FMK Use Cases

- Riak statistics
  - –Siblings
  - –Object Sizes
  - –Responsetimes
  - –Read/Write ratio
  - –Compact frequency
  - –Replication
  - –Traffic/Trends



FMK Use Cases

- Operational Insight
  - –Wallview by operations
    - improved “guts feeling”
    - Reduce incident
    - Discover problems early
  - –Wallview by developers
    - Instant feedback of changes
    - Tight monitoring of new releases (deployments)
    - Seriously reduce time to understand and fix problems
  - –Wallview by Owner

FMK Use Cases

- Changes Culture
  - To describe an observed problem, we communicate Splunk searches
  - Development very close to operation but complies to segregation of duties
  - Better understanding both ways
  - More focus on enhanced logging and session tracing
  - Almost all reporting is dashboards in Splunk

karthy@netic.dk