

.conf2015

Splunk .conf 2015

Gerrit Schmitz

Renjith Nair

Senior System Engineer,
Bosch Software Innovations



splunk®

Copyright © 2015 Splunk Inc.

Agenda

- 1 About Us
- 2 Splunk Architecture @Bosch-SI
- 3 Splunk Monitoring @ Bosch-SI
- 4 Splunk in Bosch IoT Business
- 5 Past and Future Challenges

.conf2015

About Us

splunk®

About Us

- **Gerrit Schmitz**
Senior System Engineer
- **Renjith Nair**
Senior System Engineer

- Combined Splunk Experience of 8 years+

Bosch Software Innovations Worldwide



Bosch Software Innovations

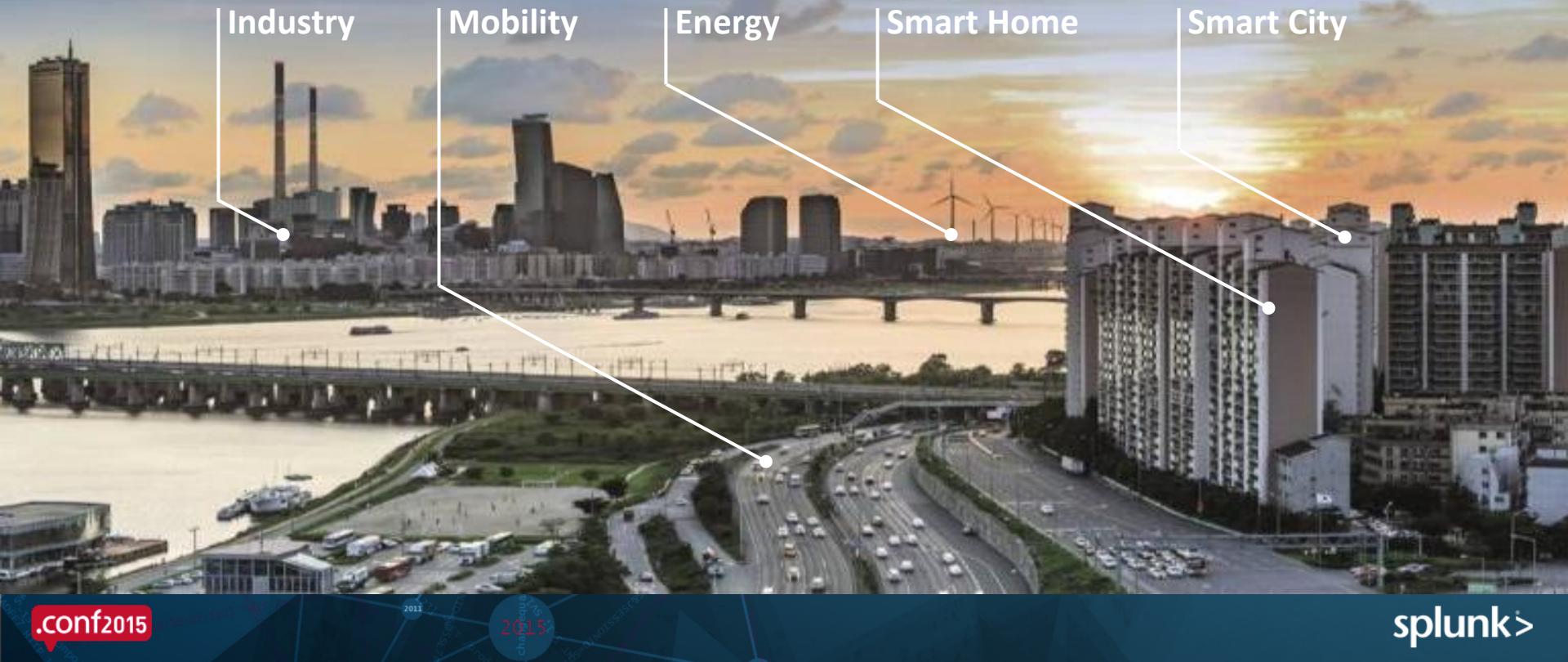
- Software and system services for enterprise solutions in the IoT
- Experience ranges from complex software systems to domain solutions
- 700 associates worldwide



Bosch Software Innovations



IoT Vision – A Connected World



The Things of Bosch



.conf2015



Splunk Architecture @ Bosch SI

splunk®

Splunk Architecture @ Bosch SI



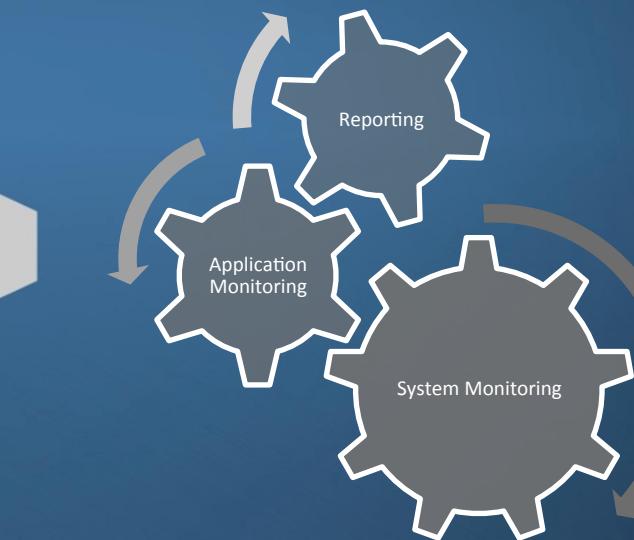
Splunk Architecture @ Bosch SI

- Five Search Heads
 - Seven Indexers
 - Eleven Heavy Forwarders
 - Approximately 150 Universal Forwarders
-
- Two Masters (both Stuttgart)
 - Two Indexer Clusters (stretched)
 - One Search Head Cluster (stretched)

.conf2015

Splunk As A Monitoring Tool

splunk®



OpsMonk

Splunk As A Monitoring Tool

Overview Status ▾ OpsMonAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Overview

Environment Project

Hosts Unavailable 0 Resources Alerts 2 Resources Warnings 1

Recent Alerts

Time	Project	Host	Type	Resource	Severity
09/04/2015 20:25:00	opsmonk	bosch-server	memory	Memory	
09/04/2015 20:25:00	opsmonk	bosch-server	url	http://localhost	
09/04/2015 20:20:00	opsmonk	bosch-server	db	'cs_db'	

Overall Status

Project	Members	Status
opsmonk	12	

Splunk As A Monitoring Tool

Overview Status ▾ OpsMonAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Overview

Environment Project

All *

Hosts Unavailable 0 Resources A

Overall Status		
Project	Members	Status
i-ene-vpp	12	!
i-hcb-smarthome	8	!
i-hcm-amr	5	✓
i-hcm-aplm	5	!
i-hcm-cs-starter	15	✓
i-hcm-misc	11	!

Recent Alerts

Time	Project	Host	Type	Resource	Severity
09/04/2015 20:25:00	opsmonk	bosch-server	memory	Memory	Warning
09/04/2015 20:25:00	opsmonk	bosch-server	url	http://localhost	Warning
09/04/2015 20:20:00	opsmonk	bosch-server	db	'cs_db'	Warning

Splunk As A Monitoring Tool

Alerts

Overview Status ▾ OpsMonkAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Opsmonk Alerts

Project Host Type Priority Acknowledged

opsmonk	bosch-server	memory	All	All
---------	--------------	--------	-----	-----

Click on 'Ack' for acknowledge an alert. Click on any other column of a row for further details

AlertTime	Project	Host	Resource	Type	Priority	Maintenance	Acked	AckedBy	AckedTime
09/09/2015 07:45:00	opsmonk	bosch-server	Memory	memory	!	Off	Ack		

Splunk As A Monitoring Tool

Alerts

Overview Status ▾ OpsMonKAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Opsmon Alerts

Project Host Type Priority Acknowledged

opsmon bosch-server memory All All

Click on 'Ack' for acknowledge an alert. Click on any other column of a row for further details

AlertTime	Project	Host	Resource	Type	Priority	Maintenance	Acked	AckedBy	AckedTime
09/09/2015 07:45:00	opsmon	bosch-server	Memory	memory	!	Off	Yes	Administrator (admin)	09/09/2015 10:40:13

Splunk As A Monitoring Tool

Alerts

Overview Status ▾ OpsMonAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Alert Notification Configuration

Project: opsmonk Host: All Type: All

Resource: All

First Name: Renjith Last Name: Nair

Email *: renjith.nair@bosch-si.com

Sms:

Comments:

* Mandatory fields

Save Search

	Project	Host	Type	Resource	First Name	Last Name	Email	Sms	Comments	
1	opsmonk	All	All	All	Renjith	Nair	renjith.nair@bosch-si.com			X

Splunk As A Monitoring Tool

Maintenance

Overview Status ▾ OpsMonAlerts License Usage Configuration ▾ Maintenance ▾ Search Dashboards OpsMonK

Maintenance

Select type of maintenance:

Project

Select time range: Select on or more projects:

Date time range

Current and future maintenances

Type	Start	End	Resource	Delete
Project	2015-09-09 10:04:21	2015-09-09 12:04:21	opsmonk	X

Splunk As A Monitoring Tool

System Information		Cpu & Memory	Components
Process Status			
Host	Component	Status	
bosch-server	sshd	✓	
URL			
Host	Url	Code	Ping
immvlvm124.innovations.de	http://localhost	000	0.000
Database			
Host	Db	State	ResponseTime
immvlvm124.innovations.de	'cs_db'	FAILED	
Certificates			
Host	Certificate	Expires	DaysLeft
immvlvm124.innovations.de	/pkg/iapspi02/splunk/etc/auth/ca.pem	2016-07-22 01:12:19	318

Splunk As A Monitoring Tool

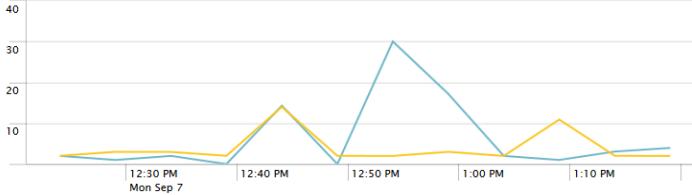
System Information Cpu & Memory Components

Click on a row below for details [CPU table for CPU ; MEM table for Ram]

CPU Load						Memory Usage			
Host	CPU	Usage	lowlait	Idle	Status	Host	Total	Usage	Status
immvilm124.innovations.de	0	3.06	0.00	96.94	✓	immvilm124.innovations.de	8 GB	93	!
immvilm124.innovations.de	1	2.04	0.00	97.96	✓				

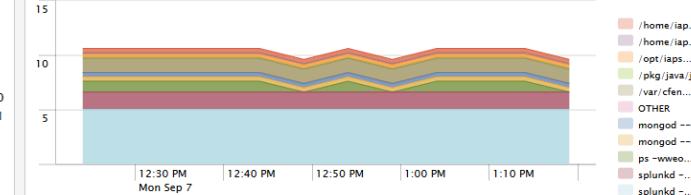
Last 60 minutes

Load Over Time (CPU) for Host : immvilm124.innovations.de



12:30 PM Mon Sep 7 2015

Load Per Process (CPU) for Host : immvilm124.innovations.de



12:30 PM Mon Sep 7 2015

Utilization by Process



12:30 PM Mon Sep 7 2015

Splunk As A Monitoring Tool

System Information Cpu & Memory Components

Host Availability		Last Booted			Total Alerts for Project	
Host	Status	Host	Booted	Status	3	
immvlpvm124.innovations.de		immvlpvm124.innovations.de	2015-04-08 09:50:00			

System Info							
Host	Distribution	Version	Major	Minor	ReleaseName	Timezone	Memory
immvlpvm124.innovations.de	CentOS	6.6	6	6	Final	CEST	8 GB
							Cpu
							2

Recent Alerts For Project					
Time	Host	Type	Resource	Maintenance	
09/04/2015 20:20:00	bosch-server	db	'cs_db'	Off	
09/04/2015 20:25:00	bosch-server	memory	Memory	Off	
09/04/2015 20:25:00	bosch-server	url	http://localhost	Off	

Disk Space					
Host	Filesystem	Mount	Size	Used %	Status
immvlpvm124.innovations.de	/dev/mapper/vg0-lv_app	/app	35G	1	
immvlpvm124.innovations.de	/dev/mapper/vg0-lv_root	/	35G	49	
immvlpvm124.innovations.de	/dev/sda1	/boot	485M	21	
immvlpvm124.innovations.de	tmpfs	/dev/shm	3.9G	7	

.conf2015

Splunk In Bosch IoT Business

splunk®

Bosch IoT Business

eMobility

Driver

- Connected via his mobile phone to an internet portal
- Integrated QR code enables users to start the charging process with a smartphone app

Car / Charging Stations

- Connectivity to internet and charging stations
- Interface for safe and easy billing of the charged electricity

Roaming Platform Provider

- Connects charging infrastructures all over Europe
- Enables easy access to charge stations for electric vehicles

Partners

- Utilities (CPO), Mobility provider (EMP), Automotive supplier (OEM) offering additional services
- Other service partners

Industry 4.0

Machine Operator

- One portal for all applications
- Integration of existing processes and systems
- Comprehensible and accurate accounting of warranty services

Machines

- Real-time compilation of data
- Analysis of machine data to create malfunction prognosis
- Mapping of maintenance processes

Factory

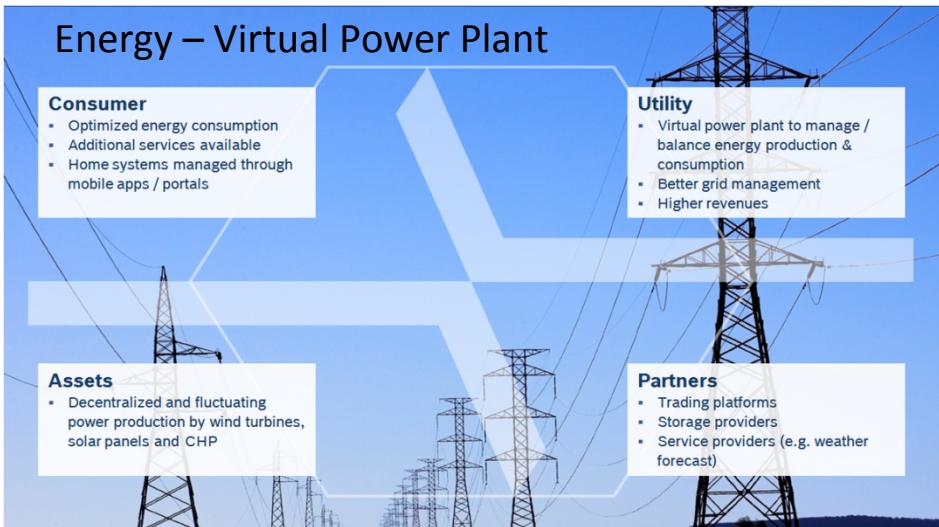
- Maximize uptime
- Efficient use of maximum service-lifetime of spare parts
- Increased productivity

Partners

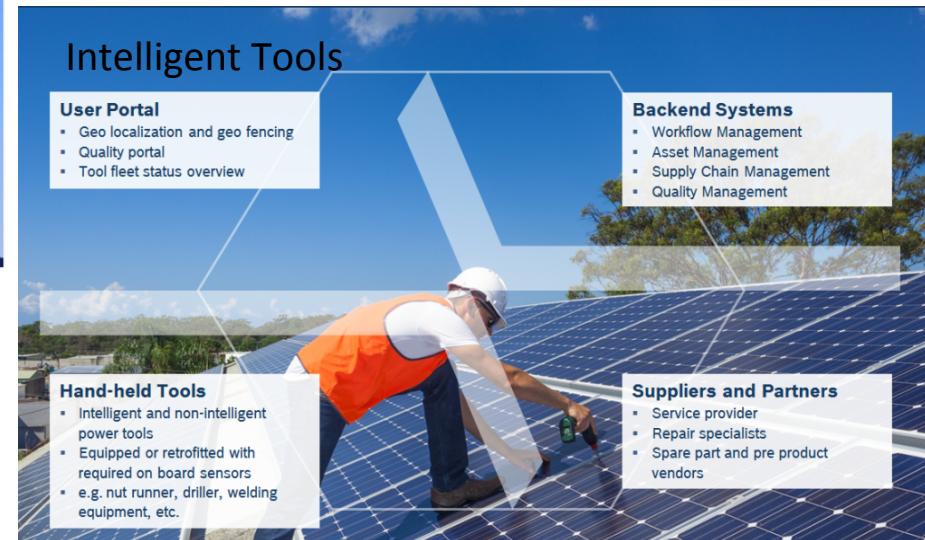
- Optimize service offering
- Revenue through new services
- Increase margins by offering services remotely

Bosch IoT Business

Energy – Virtual Power Plant



Intelligent Tools



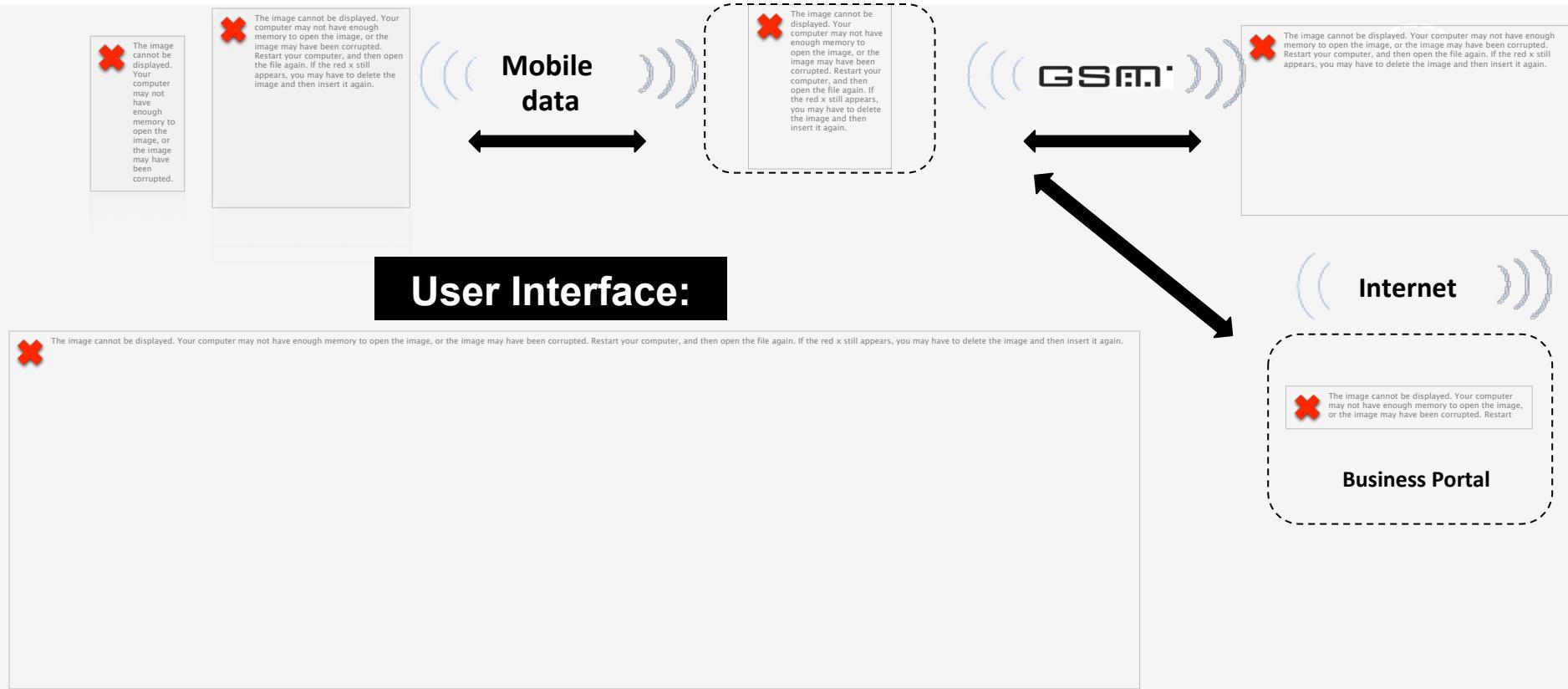
Connected lawn mower Indego

Manage your connected devices
with the touch of a finger

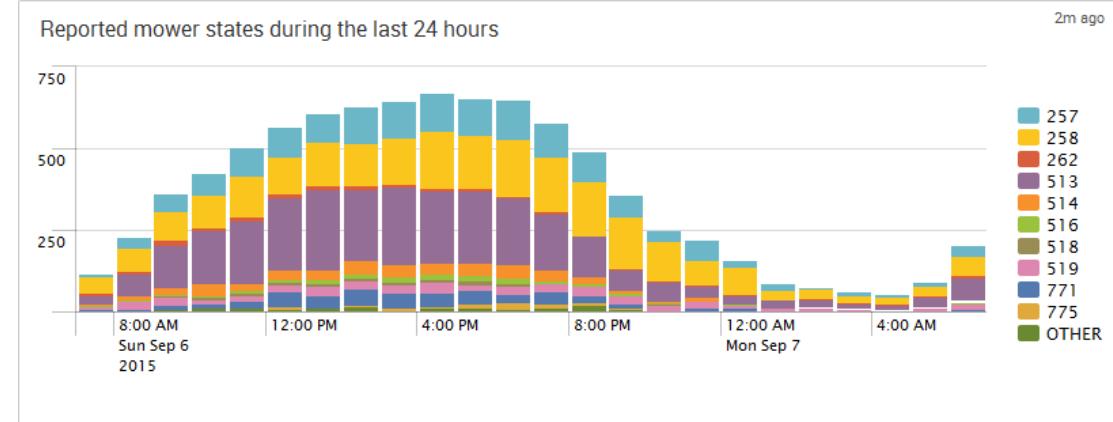
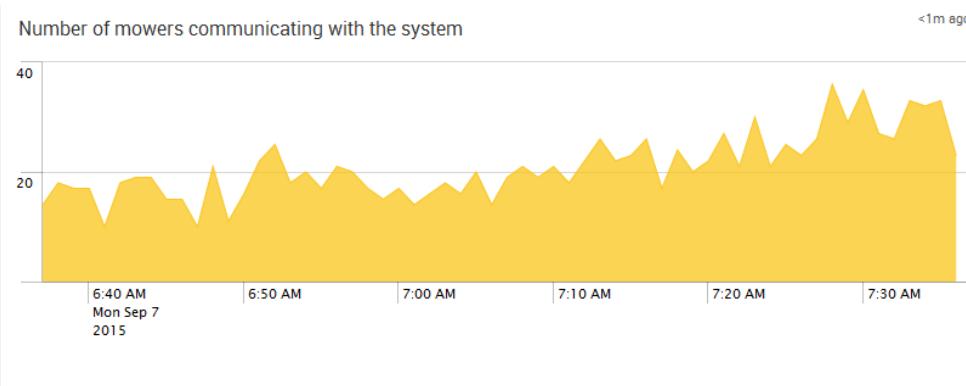
The Bosch Indego is the first robotic lawn mower with a free GSM connection that can be operated simply and conveniently using an app.



Connected lawn mower Indego

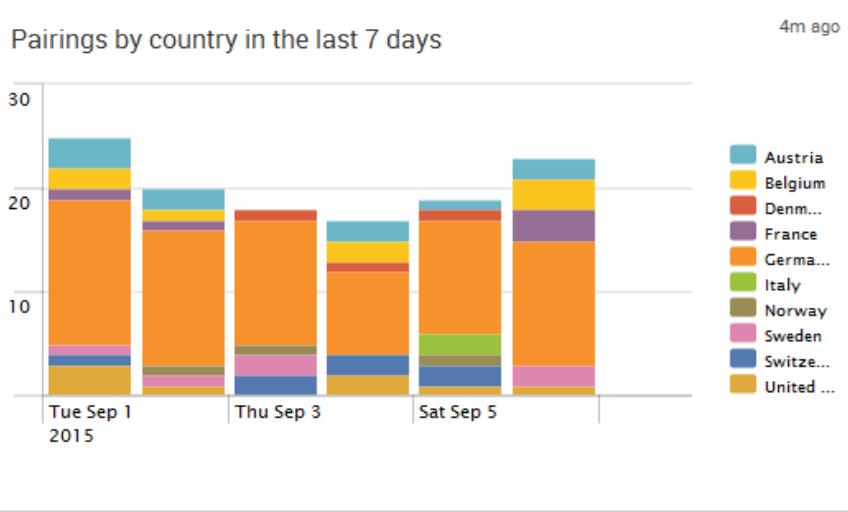


Connected lawn mower Indego



Connected lawn mower Indego

Pairings by country in the last 7 days





BOSCH
Invented for life

.conf2015



Challenges

splunk>

Past Challenges

- **We use our own SSL certificates.**
This is supported, but difficult.
- **We isolate multiple Splunk processes on the same host.**
This is not supported, and also difficult.
- **We run globally distributed Splunk clusters.**
This is not supported, but was quite easy.
- **Our Splunk is completely highly available.**
Including Master and TCP Inputs

If you want to do something similar, we are here to help ☺

Past and Future Challenges

- How could Splunk extract data from an embedded device?
 - Universal forwarder available, but not officially supported for ARM
<https://splunkbase.splunk.com/app/1611/>
 - TCP Input cannot be access protected (safe for client certificates)
 - That leaves the REST Interface
<http://docs.splunk.com/Documentation/Splunk/latest/RESTREF/RESTinput#receivers.2Fsimple>
- Server Authentication: via SSL Certificate
- Client Authentication: via Username/Password
- Client Authorization:
 - edit_tcp permission required
 - Is it a good idea to grant this to a large number of devices?

Future Challenges

To-Do List:

- **Migrating from single-tier to multi-tier storage.**
- **Use roles as distribution lists for alerts.**
Splunk knows the mail addresses from LDAP, why can't we send alerts to a whole role?
- **Limit volume by index – not indexer.**
Seems to require a change in Splunk. So far only alerting works.
- **Automatically provision new tenants.**
- **Integrate more authentication mechanisms (oAuth).**

.conf2015

THANK YOU

Blogging **Internet of Things**
Technology inspiring a connected life

<http://blog.bosch-si.com>
<http://www.bosch-si.com/>

splunk®