

BMC and Prometheus

In 5 min


by Christian "bluecmd" Svensson 2018-08-09



What is a BMC?

- Baseboard Management Controller
- Allows remote administrative actions such as power on, power off, emulate USB devices, flashing firmware, etc.
- Vendors call it differently things, iLO/iDRAC/IPMI/etc.
- It's a server in the server that is always on
 - Example: ARM926, 400MHz, 256MB RAM

What is inside the BMC?

- Modern software 
- From a server that was **designed** in 2015 and manufactured in 2016, this is what we have:

```
# uname -a
```

```
Linux QCT7Cxxxx3F0 2.6.28.10-ami #1 Mon Jan 4 20:54:46 CST 2016 armv5tejl unknown
```

```
# busybox
```

```
BusyBox v1.13.2 (2016-01-14 20:11:32 CST) multi-call binary
```

```
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
```

What is inside the BMC?

- GPL code

```
# grep --text GPL /lib/modules/2.6.28.10-ami/misc/iUSB.ko  
license=GPLdescription=iUSB moduleauthor=redacted  
<x@ami.com>depends=usbe,helpervermagic=2.6.28.10-ami
```

Request for source code still pending....

Cool story, but what's the Prometheus hook?

- Always on metrics!

ipmitool sensors

P0 Temp	29.000	degrees C	ok	na	na	na	na	91.000	na
P1 Temp	30.000	degrees C	ok	na	na	na	na	91.000	na
P0 DTSmax	95.000	degrees C	ok	na	na	na	na	na	na
P1 DTSmax	95.000	degrees C	ok	na	na	na	na	na	na
P5V	5.058	Volts	ok	na	4.501	na	na	5.493	na
P12V	12.420	Volts	ok	na	11.340	na	na	13.200	na
Inlet Temp	31.000	degrees C	ok	na	na	na	na	40.000	na
Outlet Temp	29.000	degrees C	ok	na	na	na	na	80.000	na
PCH Temp	40.000	degrees C	ok	na	na	na	na	66.000	na
SYS FAN0	2200.000	RPM	ok	na	500.000	na	na	9000.000	na
SYS FAN1	2200.000	RPM	ok	na	500.000	na	na	9000.000	na

What is IPMI?

- Defined in "Intelligent Platform Management Interface Specification (Second Generation v2.0)"
- 644 pages
- Probably a good protocol, dunno, too long - didn't read
 - Has custom undocumented vendor/OEM commands that look like this:
 - `ipmitool raw 0x32 0xaa 0x00 # Mysterious CD-ROM drive appears on the host` `⌘_(ツ)_/`
 - Bonus: does RPC calls over an interface called **keyboard controller style** (KCS)

Scary, let's use node_exporter

- Problem: You don't have root access
- Solution: Ignore that, get root

```
# whoami  
root
```

How to root the BMC

1.



Get the IP of the
BMC

2.



Gain root

Scary, let's use the node exporter

```
# cd go/src/github.com/prometheus/node_exporter  
# patch -p1 < bmc-metrics.patch  
# GOARCH=arm GOARM=5 go build  
# # copy to bmc  
# ./node_exporter
```


node_server_powered_on

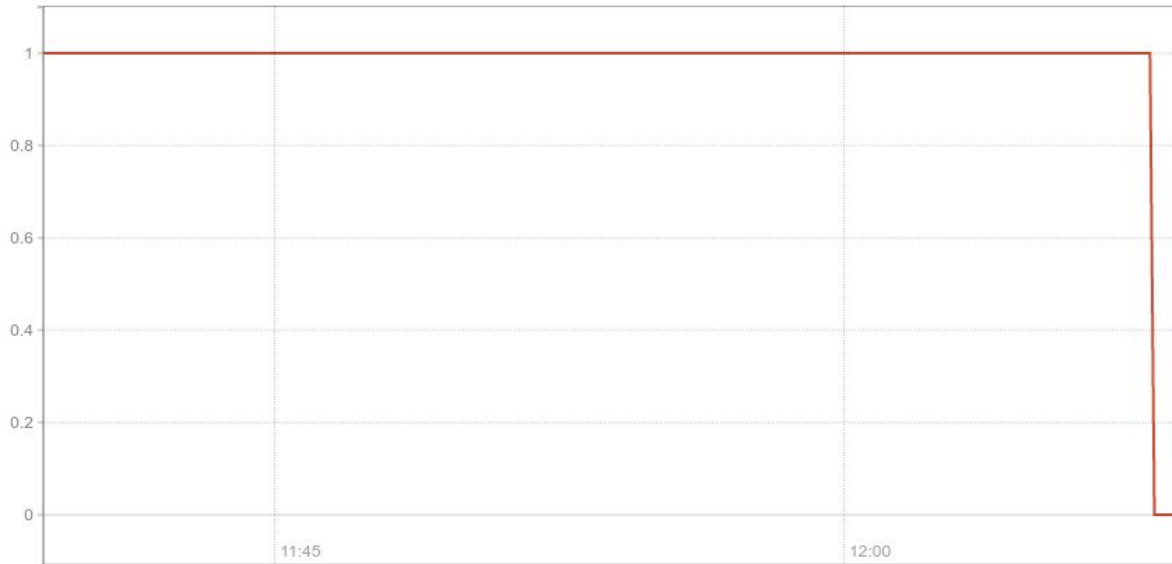
Load time: 138ms
Resolution: 7s
Total time series: 1

Execute

- insert metric at cursor -

Graph Console

- 30m  +  Until  Res. (s) stacked



node_server_powered_on(instance="r1a0-bmc:9100" job="bmc")

u-bmc

u-bmc is the working name for a project to replace the BMC software with an open source and de-bloated version using modern technologies, like Prometheus' exposition format, where it makes sense.

Still very early, have no fancy web page yet, but I'd love to hear from you if you want to contribute.

Thanks!

@bluecmd on github/twitter/etc

For a recorded "live" demo:

<https://asciinema.org/a/GSv8ASBcHizDsc1mNvKCYyyqg>