NEW CHALLENGES AT PALANTIR

MONITORING THE COFFEE

JARED LEDVINA

- Cloud Operations Engineer at Palantir Technologies
- 2015 Computer Network and System Administration (CNSA) Graduate from Michigan Technological University
- Ham Radio Callsign: KK6YJA
- Student Pilot at Michigan Flyers
- Lead Maintainer for the Sensu Ansible repos

DISCLAIMER

- This presentation was prepared or accomplished by Jared Ledvina in his personal capacity. The opinions expressed in this article are the author's own and do not reflect the view of the Palantir Technologies.
- Any republishing of any or all of the content contained within this presentation is strictly forbidden unless explicit permission is granted by Jared Ledvina.

WHY AM I TALKING TO YOU?

- Palantir continues to experience rapid growth
- We've deployed some incredible technologies
- We've learned some hard lessons

WHAT IS PALANTIR?

PALANTIR IS…

- a silicon valley software company.
- headquartered in Palo Alto, CA with offices all over the world.
- building software to make people better at their most important work.
- helping investigators uncover human trafficking rings, find exploited children, and unravel complex financial crimes.
- continuing to rapidly expand our cloud footprint.

WHERE WE'VE COME SINCE LAST TIME

OVER THE LAST 8 MONTHS…

- We've grown from 8,100 instances in production to 12,500
- We've surpassed the 50% mark for hosts running CentOS 7
- We support 13 AWS Regions
- Overhauled our Configuration Management and Monitoring platforms

CONFIGURATION MANAGEMENT

CONFIGURATION MANAGEMENT UPGRADES

- Upgraded from Puppet 3.8.2 to 5.5.1
- Upgraded from Hiera 1 to 5
- Reduced our PuppetDB RDS usage by 50%
- Deployed automatic baseline unit tests to all of our Puppet modules
- 4,900+ commits since last year

MONITORING UPGRADES

- Re-architected and deployed to production Sensu as a monitoring platform
- Completely deprecated our self-hosted metric solution with DataDog
- Designed our self-healing framework to significantly knock back manual work

DATADOG

DATADOG AND OUR DATA DRIVEN APPROACH

- Fully decommissioned our internal OpenTSDB & Grafana setup
- Migrated all critical custom collectors into the DataDog Agent
- Never before seen cross team collaboration during incidents
- Ability to measure true performance impact of changes
- Fundamentally changing the way we approach production rollouts

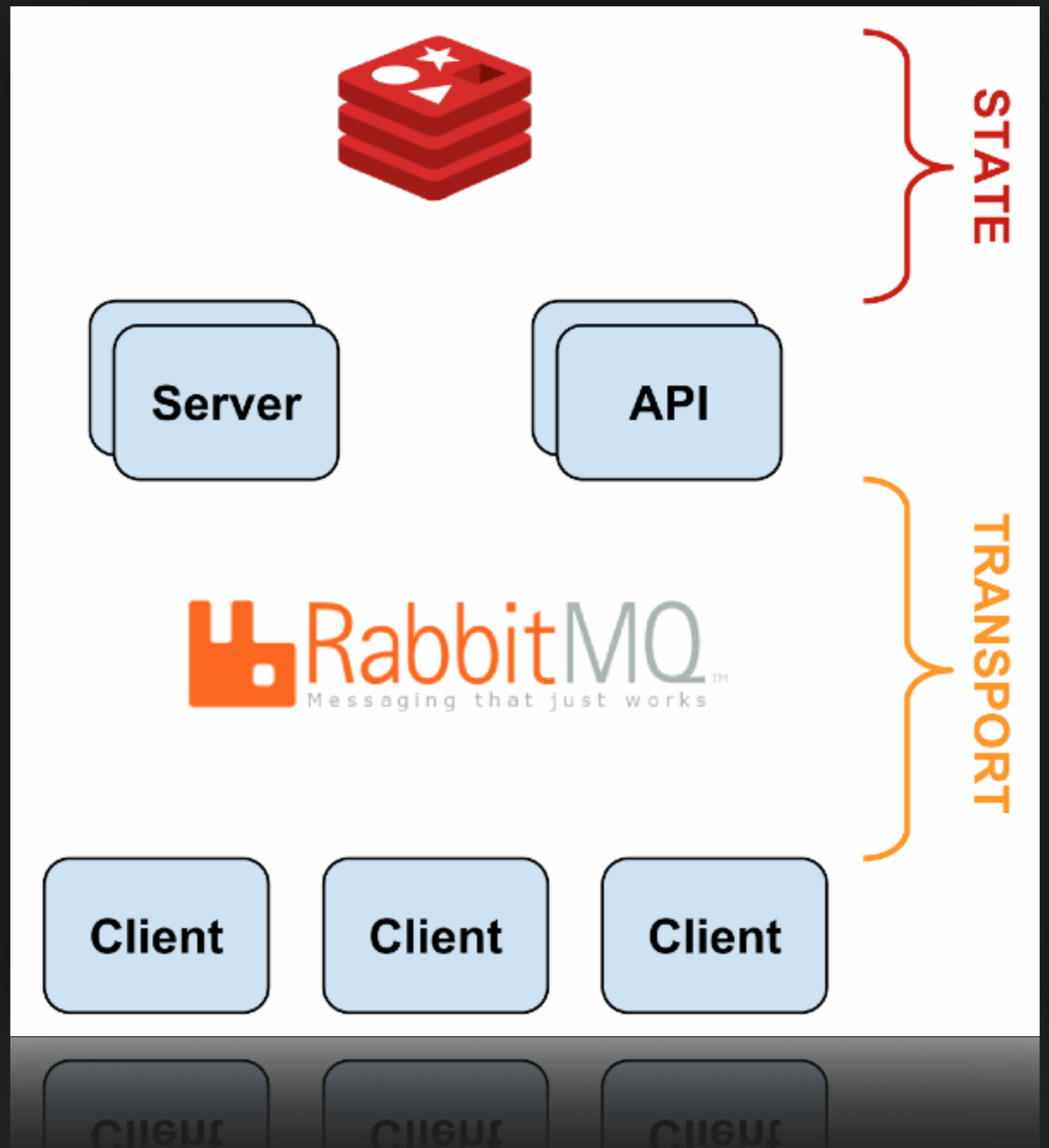
SENSU

WHAT IS SENSU?

- “Sensu is an infrastructure and application monitoring and telemetry solution. Sensu provides a framework for monitoring infrastructure, service & application health, and business KPIs. Sensu is specifically designed to solve monitoring challenges introduced by modern infrastructure platforms with a mix of static, dynamic, and ephemeral infrastructure at scale (i.e. public, private, and hybrid clouds).”
- tl;dr - It’s pretty badass and powerful

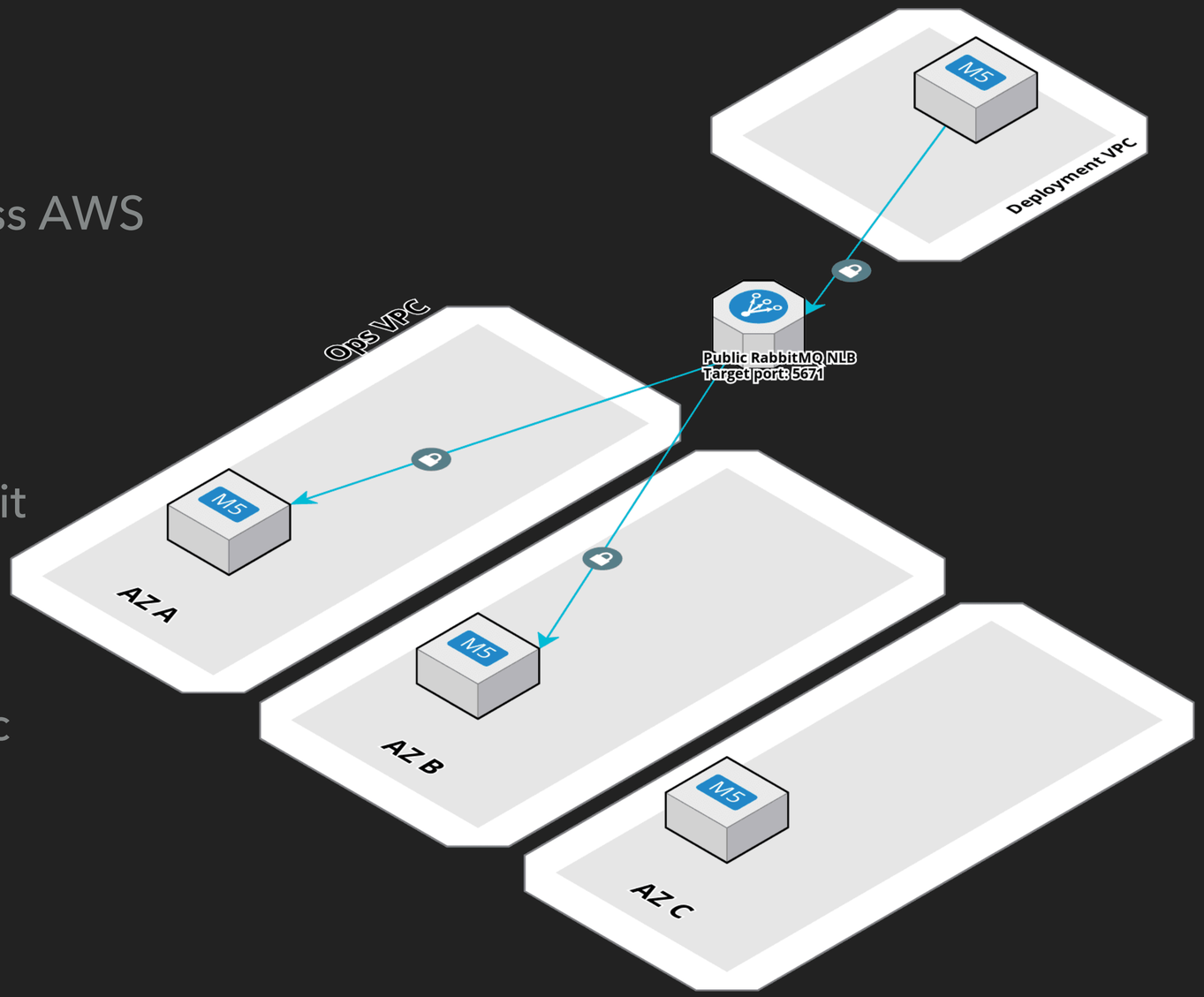
SENSU COMPONENTS

- Sensu Client
- Sensu Server
- Sensu API
- Uchiwa
- RabbitMQ
- Redis



HOW WE DEPLOY SENSU TODAY

- Three ‘full stack’ instances spread across AWS AZ’s.
- c5.xlarge’s w/ 100GiB EBS storage
- AWS Elasticache w/ encryption in transit
- Ingress AWS NLB
- Processing around 1,000 messages/sec
- Very spiky workload



SENSU ADVANTAGES

- Built upon solid open source technologies
- Easily configurable in a highly available cluster
- Responsive JSON REST API
- Incredibly flexible to be configured to your organizations needs
- Able to monitoring everything and more

SECURING SENSU

- Leverage in-transit encryption w/ TLS 1.2 & CIPHER HERE
- Enable RabbitMQ's 'verify_peer' for client certificate validation
- Disable TCP/UDP client sockets, enable authentication on HTTP endpoints
- Enable 'safe_mode'
- Configure 'client_signature' by default
- Lock down Sensu API access and proxy connections w/ auth and TLS
- Enable encryption in transit for Redis communication

THE SENSU ADVANTAGE

- Uchiwa provides incredible power regex based searches across alerts
- Handlers and filters easily support mimicking Nagios's alert strategies
- Leveraging occurrences and dependancies to cut back on alert fatigue
- Clients register themselves and begin reporting within seconds of coming online

WHERE WE GO FROM HERE

FORWARD LOOKING

- Migration from FreeIPA 3.0.0 to 4.5.2
- Continuating to deprecate CentOS 6 instances
- Overhauling our patching cycle to reduce manual interaction
- Deploying basic auto-remediation for nearly all monitoring checks
- Decentralizing components to reduce outage impacts

THANKS FOR COMING!

- keybase.io/jledvina
- jaredledvina@gmail.com
- https://github.com/jaredledvina
- https://palantir.com/careers


QUESTIONS?