

Damian Zaremba

I like interesting problems, at scale, mostly involving networking.

((Systems + Networking) + Business requirements = Positive business impact) == <3

Summary

Linux/network focused sysadmin constantly looking to improve service and run at the edge of technology.

Passionate about networking, architecture, solution design, automation, testing, Linux, open source, micro optimisations, monitoring, metrics and graphing.

Driven to impact change where required and deliver things done efficiently and effectively.

Employment History

Booking.com - Network Engineer

September 2016 - Present

Focused on the design, engineering and management of AS43996 & AS202196, powering Booking.com globally.

Responsibilities included:

- Management of the global routing policies
- Extending/managing peering relationships and transit selections
- Hardware upgrades and maintenance in a non-stop manner
- Deployment of new POPs
- Ensuring adequate capacity and redundancy
- Testing and implementing new technologies as required (EVPN, IPFIX etc)
- Developing tooling and processes required to manage the global deployment
- Supporting network tooling and authentication services for all network teams within Booking.com
- Participating in the on-call rotation covering all production networks
- LIR administration

Achievements included:

- Management of all network tooling services in Puppet
- Port of existing IPFIX/Netflow v5 decoders into Go reducing resource usage and custom code significantly
- Peer/IX selection/management tooling using flow and latency data for business/data focused decisions
- Internal tooling integration with PeeringDB
- Implementation of real-time TCP latency monitoring tooling
- Implementation of POP performance measurement tooling (deployed to customer/partner facing apps)
- Introduction of Kafka and Hadoop technologies for data processing
- Introduction of OpenBMP and RPKI validators to aid troubleshooting/leak prevention
- Development of Ansible based configuration management with integration into existing data sources
- Automation of manual processes (lab router firmware version changes, dashboard creation, route filter management etc)
- First internal team to have IPv6 enabled management for all devices
- Improvements to the GeoDNS backend including EDNS0 support

As an extension to this role, I also provide design/engineering support to and act as an escalation point for BookingGo (Rentalcars.com) teams on an ad-hoc basis, including on the integration of infrastructure.

TravelJigsaw Limited (Rentalcars.com) - Principal Security Engineer

November 2015 - September 2016

Focused on improving all technical aspects of the security landscape.

Worked closely with Legal, Finance, Technology and Security teams in the business to deliver security objectives.

A number of large undertakings were completed successfully including:

- Achieving a ~65% reduction in external facing vulnerabilities, while observing a ~44% increase in assets.
- Deploying an internal certificate authority and root certificates (ca-bundle + JKS files) to 800+ servers
- Developing tooling in Puppet for firewall rule management and deployed restrictive iptables rules to 800+ servers
- Deploying OpenLDAP using SSSD & pam_access to 800+ servers for centralised authentication and access control
- Building tooling around Nexpose, Serverspec & Test Kitchen for integration into a CI pipeline
- Deploying an OSSEC setup to 800+ servers
- Implementing internal vulnerability scanning of ~2000 assets.
- Rebuilding the entire PCI DSS environment with minimal business impact and 100% removal of vulnerabilities, including conformance to PCI DSS (with QSA signoff)
- Developing CSP/HPKP functionality and servlet filters for external facing applications, including reporting functionality to assess the impact of policy/filter changes
- Developing tooling for automated server patching (including staged rollouts + reporting)
- Developing tooling for rotating encryption keys on 10+ million data entries in a fast and minimally impactful manner
- Deploying a horizontally scalable (Anycast + Resilient ECMP based) load balancing implementation using HAProxy to support migrating all external traffic to use TLS
- Provided expert support to other teams in the business, ensuring their designs were both secure and scalable

More day to day operational items included:

- Introducing hiera-eyaml (using the GPG backend) and node_encrypt into Puppet (3.x), for improved configuration secrets handling
- Deploying SELinux in targeted mode to all 'critical infrastructure' (including in PCI/PII zones and core infrastructure)
- Developing security tooling with appropriate access controls for common activities such as managing OSSEC alerts, reporting on user access and changing on-call settings
- Developing Python tooling for handling inventory changes in 'black box' security appliances
- Performing reviews on proposed solutions and technical aspects of legal contracts
- Providing security on-call coverage
- Standardising firewall rules across multiple Juniper SRX clusters
- Working with external and internal auditors to improve controls and ensure (SoX, PCI DSS, DPA, Privacy Shield) compliance
- Developing tooling for server patching in a controlled manner, targeting both CentOS and VMWare ESXi (4.x / 5.x); Successfully upgraded 100+ VMWare hosts, 800+ CentOS 6.x servers
- Developing abstractions in puppet for managing pam_access and sudo (group) based access rules, with inheritance
- Interviewing candidates for engineering and development roles
- Drafting a roadmap and key milestones for security enhancements

TravelJigsaw Limited (Rentalcars.com) - Technical Architect

June 2015 - November 2015

As a founding member of the architecture team, my initial focus was a review of the core systems, potential contention/failure points and a roadmap for core infrastructure.

The work was varied and included documenting existing systems, interviewing candidates for multiple roles, providing expert support during service issues/solution design, building software prototypes, working with the teams to establish standards and designing new solutions.

As the only infrastructure focused member of the team, a lot of alignment and collaboration with the 2 software architects was undertaken during this time.

Some key solutions that were designed and placed into production included:

- Internet connectivity, resolving redundancy issues and providing future scalability; this established the first ASN and IP space directly held by the company
- AWS direct connect for hybrid (test/development) environments; a successful PoC, now supporting multiple teams and production services
- ‘Event backbone’ using Apache Flume and Kafka with custom consumers written in Java; a successful PoC handling millions of events a minute. This is now the standard way to transmit/consume events within the company and has a diverse set of backends (ElasticSearch, MySQL, AppDynamics, HDFS etc)

Other outcomes included:

- An 18-month roadmap/improvement plan for the network
- Numerous risks identified within the technology landscape and prioritised for resolution with the engineering teams
- Implementation of Bamboo for CI, including multiple example jobs and Java-based plugins
- Implementation of Artifactory Pro for internal binary sharing (integrated into Bamboo and internal deployment systems)
- Updated design for a multistage Clos architecture within the DCs with the budget accepted

TravelJigsaw Limited (Rentalcars.com) - Linux Systems Administrator

February 2014 - June 2015

Working in a team of 3 DBAs, 3 Sysadmins and a Network operations engineer scaling out and managing the 1k+ of servers that make up the Rentalcars.com infrastructure.

- Managed/deployed a heterogeneous infrastructure consisting of bare metal rack mount and blade servers (HP/Dell) alongside VMWare ESX, KVM, Docker and EC2 based instances
- Refactored a Puppet 2.x setup into a Puppet 3.x setup using the latest language standards and the principle of state convergence on the first run
- Supported the internal tools written in Python/Ruby including the Django-based asset management tool
- Provided out of hours support to the business via an on-call rota
- Introduced CI to operations for RPM builds and puppet testing
- Re-designed the core network to be a fabric-based setup, based on a multi-stage Clos architecture
- Coordinated with data centre and network teams to ensure changes are completed as required by the business
- Deployed anti-virus scanning and DKIM signing of outbound messages using Exim routers to ensure external facing email meets validation/verification levels requested by the business
- Developed multiple fabric based scripts for real-time auditing and remediation of servers (firmware versions, log file cleanup etc)
- Built a PoC SaltStack deployment
- Performed troubleshooting on multiple issues of PHP-FPM, Tomcat, Java 7/8, Nginx, Apache & F5 setups
- Championed the use of upstream packages and versions of core software
- Worked closely with development teams to test new software and build a path to production
- Developed kickstart files and custom initrd files for server installation (including automated firmware updates)
- Developed acceptance tests for hardware using PyUnit and Fabric
- Interviewed candidates for junior sysadmin positions and devised training plans for them within the company
- Devised tests for and interviewed candidates for senior engineering positions

A part of this role involved building the initial infrastructure for Car+Driver (Rideways.com); a startup within the company. This was accomplished using:

- AWS EC2/S3/RDS/Cloudfront/Cloudformation/ElastiCache
- Python (troposphere) based CloudFormation generation
- Python (boto) based deployment scripts, for CloudFormation and CodeDeploy
- Packer + Puppet (masterless) based AMI creation
- Github + Bamboo + Jira for CI/CD

MUSIC Group - Software Engineer (RnD - Midas/Klark Teknik)

July 2013 - February 2014

Working on new Midas/Klark Teknik products and supporting internal R&D infrastructure.

- Deployed a 3 node OpenStack setup using NetApp ONTAP storage
- Designed and implemented a small ‘collapsed-core’ network to provide an isolated R&D network, inside an existing (insecure) corporate network
- Performed data recovery for R&D and developed workarounds for internal services during a 4-month long global technology failure
- Developed a testing jig for development boards to enable automated boot loader re-programming and boot timing on changes
- Developed and implemented backup/restore procedures using AWS Glacier
- Implemented configuration management (Puppet, Saltstack) and service/change monitoring (Icinga/Rancid)
- Reduced build times and implemented a new strategy for component-based builds
- Designed a framework for increasing confidence in code and speeding up the release cycle
- Developed software against x86, STM32 and ARM based platforms
- Performed maintenance on LFS and Ltib systems for building products
- Debugged and rectified issues in C++/Python/Perl code and shell/Sed/Awk scripting
- Utilised kernel features to enhance new products (control groups, SELinux, nftables)
- Documented processes for developers (board reprogramming/bootup)
- Ported numerous internal apps from x86 to ARM
- Managed Atlassian developer tools (Jira, Stash, Bamboo, Fisheye)

MUSIC Group - Systems Engineer (Global Enterprise Engineering)

October 2012 - July 2013

Supporting world-recognized pro audio brands such as MIDAS, Klark Teknik, Turbosound, Behringer and Bugera.

- Mixed Operations/engineering role covering all levels of the infrastructure
- Managing a complex heterogeneous infrastructure based upon VMware
- Implementing service monitoring and metric collection systems (MRTG, Smokeping, Icinga, Graphite, PRTG)
- Troubleshooting layer 2/3 network issues across multiple sites (combination of P2P MPLS links (L2 & 3), MPLS cloud and GRE tunnels connected via a mix of OSPF and static routes)
- Developed custom integration (Icinga to ServiceDesk for ticketing, Pagerduty ack’s to Icinga ack’s for alerts), plugins (VMware hardware checking, Oracle ESSO transaction level checking) and templates (network devices, server roles etc) for monitoring systems
- Developed a custom roster system based on email DL’s for Openfire, based on business requirements
- Developed numerous scripts for auditing and policy enforcement purposes
- Automated manual tasks to increase reliability
- Maintained binlog based replication on multiple MySQL clusters
- Dealt with multiple outages relating to VMware/DNS/Network/Disk availability
- Developed strategies for operating system deployment and management globally
- Packaged and maintained numerous pieces of software into DEB and RPM files for distribution
- Developed strategies for enforcing change control within a configuration management setup (gating/testing changesets, peer review, environment isolation)
- Diagnosed multiple issues with an Oracle ESSO deployment
- Implemented RANCID based backups for network device configs

Sub 6 Limited - Lead Systems Administrator

October 2011 - August 2012

- Lead the sysadmin side of the UK/US based managed hosting companies
- Handled escalated issues, complex solutions, monitoring and reporting requirements

- Integrated multiple services into the asset management system to cut down on manual steps
- Introduced continuous integration into the development workflows
- Rolled out Puppet for configuration management
- Managed configuration of the switched network
- Rolled out LDAP and Radius for centralized authentication
- Developed custom features for Kayako and WHMCS
- Introduced Graphite and exposed monitoring metrics to clients
- Increased security across the entire platform (PBX, DNS, Billing, client servers)
- Implemented rolling password changes on a twice weekly basis
- Built a custom IP based FTP access manager
- Developed patching policies around a rolling release cycle
- Built a custom version manager for 4 PHP versions which enabled clients to run applications with different requirements on the same server
- Built a custom gatekeeper service to display holding pages for clients during a datacenter move which served media via Nginx for thousands of IP addresses.
- Developed numerous custom solutions for clients based on Linux systems

Volunteering experience

ClueBot NG Maintainer

2012 - Present

- Heavily used anti-vandalism Wikipedia bot with over 4.8 million edits
- Monitor ClueBot NG to ensure active reversion of vandalism
- Perform code fixes and improvements to reduce errors
- Interact with the community during issues and suggested improvements

FOSDEM volunteer

January 31st 2014 - 2nd February 2014

- Assisted with the build-out for FOSDEM, prior to the event
- Assisted with the clean up of the ULB in Brussels
- Assisted with any misc tasks as required during the conference, based on organiser requirements
- Assisted with the initial video editing for Saturday's raw footage
- Moderated multiple talks (keynotes/main tracks) in the Jason building (1400 seat capacity)
- Worked with a multinational team of volunteers (50+) to help deliver 512 talks over 22 rooms in 2 days

The Scout Association

December 2006 - January 2014

- Assistant Scout Leader
- Assist with program creation and delivery
- Teach new skills
- Perform building and equipment maintenance
- Ensure meetings take place safely
- Activity instructor for climbing
- Completed training for first aid, climbing, safeguarding and leadership
- Assist local campsites, district, county, and groups at large events

Professional certifications (current)

- Red Hat Certified Engineer - 150-017-028
- Red Hat Certified System Administrator - 150-017-028

Misc

- UK passport/driving licence
- Available out of hours
- Based in Amsterdam, Netherlands
- Diver, Climber, Explorer

See Also

- [GitHub](#) - damianzaremba
- [Last.fm](#) - damianzaremba4
- [LinkedIn](#) - damianzaremba
- [Website](#) - damianzaremba.co.uk