Damian Zaremba

TL;DR I like interesting problems, at scale, mostly involving networking.

((Systems + Networking) + Bussiness requirements = Positive bussiness 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 - DevOps Engineer

September 2016 - Present

Working in the network engineering department, dealing with internal systems related to provisioning, monitoring and managing network devices across the globe.

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 OpenLDAP topology, synced with Active Directory entries, using SASL to hand off password authentication
- 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 (level 2, with external QSA assessment)
- 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

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
- Developing Python tooling for streaming SIEM alerts off multiple closed 'black box' security appliances into a single events stream, combined with OSSEC events

- Working with vendors to PoC and implement security appliances, including deploying TAP (Arista 7150 based) infrastructure for data collection/aggregation
- Providing expert level support to the architecture and engineering teams within the Technology department
- Performing reviews on proposed solutions and technical aspects of legal contracts
- Upgrading numerous server roles (including all core infrastructure) to CentOS 6.8 and Puppet 3.x
- Providing security on-call coverage (for both SIEM alerts and as an escalation point for events)
- 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
- Supported the Network team in implementing new internet infrastructure (routing policy, peering points, redundancy testing, design of firewall cluster connectivity to avoid L2 spans in transit layers, confederated BGP etc); this was the implementation of the solution previously designed (see the previous role)
- 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 (team of 3), 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/diagramming existing systems, interviewing candidates for multiple roles (engineers, managers & contractors), providing expert support during service issues/solution design, building software prototypes, working with the teams to establish standards and designing new solutions.

A number of solutions were designed, many of which ended up in production:

- A new internet connectivity segment, removing single providers/devices out of a critical path and improving scalability for the future; this established the first ASN and IP space directly held by the company
- Route based injection for service discovery; a successful PoC and accepted for specific services. No wide rollout due to a lack of equal cost within the main access network
- AWS direct connect for hybrid (test/development) environments; a successful PoC, now supporting multiple teams and production services
- A new '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 2 Kafka clusters deployed, publishing events into a diverse set of backends (ElasticSearch, MySQL, AppDynamics, HDFS, CSV files etc)

Other outcomes include:

- 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 (budgeted for completion Q4 2016)

Some areas of investigation were undertaken:

- Impact of deploying Docker into Production; this was determined to be dependent on an equal cost network due to the impact of differential latencies between access segments on performance
- Real(ish) time event analysis (using Parquet backed tables in Hadoop); the primary driver for this was to power a re-build of the internal A/B/n / MVT testing dashboards
- Datacenter standardisation via logical (vRF) rather than physical role separation

TravelJigsaw Limited (Rentalcars.com) - Linux Systems Administrator

February 2014 - June 2015

Working in a team of 3 sysadmins maintaining, tuning and updating the 1k+ servers that make up the 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 an isolated 3 node (2 HA controllers) OpenStack Havana set-up using NetApp ONTAP storage.
- Designed and implemented a small 'collapsed-core' network - using Cisco technologies
- to provide an isolated R&D network, inside an existing (insecure) corporate network.
- Performed data recovery on R&D servers/data and developed workarounds for internal services during a 4-month long global TECH service failure.
- Developed a testing jig for boards using a raspberry PI with GPIO controlled relays, for automated boot loader re-programming and boot timing on changes.
- Developed and implemented backup/restore procedure for critical data (source code, tickets, build configurations).
- Rearchitected the current 2 server setup (unmonitored, running on raid 0, constrained by disk/CPU) into a 3 node OpenStack setup and re-purposed older servers (removed from service during a transition from CVS to Git) as disposable build agents.
- Implemented configuration management (Puppet), service orchestration (Salt stack) and service/change monitoring (Icinga/Rancid).
- Reduced build times (14 hours to 40min) and implemented a new strategy for multi-component builds.
- Drove continuous deployment methodologies into new product design
- Designed a framework and strategy for increasing confidence in code and speeding up the release cycle.
- Developed software against x86, STM32, and ARM-based platforms, including acting as the control plane for embedded switches/FPGAs/DSPs
- Exposure to proprietary binary based communications protocols and their pitfalls vs open, standards-based communications protocols and their benefits
- Performed maintenance on LFS and Ltib systems for building products
- Debugged and rectified issues in C++/Python/Perl code and shell/Sed/Awk scripting
- Investigated web technologies, updating/deployment methodologies, RFB reverse tunnelling, SELinux, and performance analysis/containment.

- Utilised kernel features to enhance new products (control groups, SELinux, nftables)
- Documented processes for developers (board reprogramming/power up/hardware interfaces)
- Ported numerous internal applications 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-recognised pro audio brands such as MIDAS, Klark Teknik, Turbosound, Behringer, and Bugera.

- Mixed Operations/engineering role covering all levels of the infrastructure.
- Managed 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 Service Desk for ticketing, Pager duty acknowledgements to Icinga acknowledgements 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 around 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 bin log 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 (primarily Ubuntu).
- Packaged and maintained numerous pieces of software into DEB and RPM files for distribution.
- Developed strategies for enforcing change control within a configuration management set-up (gating/testing change sets, peer review, environment isolation).
- Diagnosed multiple issues with an Oracle ESSO deployment.
- Implemented RANCID based backups for network device configurations.
- Implemented LLDP/CDP based network topology diagraming for the discovery of devices within an unknown network.
- Supported the implementation of a new network design (3 DCs, existing offices converted to leased lines, EIGRP backbone, OSFP in office, BGP to the internet and between sites)

Sub 6 Limited - Lead Systems Administrator

October 2011 - August 2012

- Lead the system administration/management 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 and automate the process.
- Introduced continuous integration into the development workflow.
- Rolled out Puppet for configuration management.
- Handled configuration of the switched network.
- Designed and implemented a network topology to 'in-house' all UK DC networking
- Rolled out LDAP and Radius for centralised 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.
- Designed and developed an in-house (customer facing) IP-based FTP access manager.
- Designed and developed a bespoke (customer facing) version manager for 4 x PHP versions.
- Developed a gatekeeper service to display holding pages for clients during a datacenter move.
- Developed numerous custom solutions for clients.

AllGamer, LLC - Freelance systems administrator and developer

November 2010 - September 2011

- Advised on system automation and maintenance.

- Integrated systems into the CRM.
- Assisted in service issue diagnostic and resolution.
- Assisted on service and metric monitoring (Nagios, SNMP, RRDTool, SmokePing).
- Development of community tools.
- Programming of system utilities.

Calyx - Unix/Linux systems administrator

April 2011 - May 2011 (contract)

- Responsible for an RHEL5 RHCS set-up.
- Managed Apache, Tomcat, JBos, Oracle 10G, MySQL.
- Provided on-call support.
- Provided users support in a third line capacity.
- Successfully identified and resolved memory leaks within the application servers.
- Managed Xen and Citrix XenServer deployments.
- Debugged tomcat logs to identify root causes of application issues.
- Implemented process monitoring of background workers to ensure a responsive application.

CloudFlux - Systems Engineer/Developer

October 2010 - May 2011

- Implemented service monitoring and performance graphing.
- Developed a management framework.
- Automated management tasks.
- Managed backups of multiple servers.
- Provided users support in a second/third line capacity.
- Migrated from Xen to KVM.
- Managed a KVM based virtual host.
- Migration of SVN to Git.

UKFast - Linux Engineer

February 2010 - October 2010

- Provided support in a 3rd line capacity.
- Handled technical pre-sales and server set-up.
- Maintained SLAs.
- On-Call/Out of hours work.
- Managing custom platforms, cPanel, Plesk, IIS, Apache, HAProxy, Nginx, LVS.
- Configured and managed multiple Database and File replication solutions.
- Dealt with multiple, geographically redundant sites with solutions spanning across 2 or more.
- Handled network and power issues on a datacenter level.
- Solely responsible for investigating and resolving alerts during out of hours.

Freelancer: Architecture, Infrastructure, Linux Deployment, Network Design, Software Development

November 2008 - Current

End to end management and design of infrastructure, heavily Linux and Network focused.

Provide software development as required in Python (including Django), Perl, PHP, C++ & Ruby. Primary focus on extending open source solutions and API services.

Previously deployed Linux solutions at edge and core, covering small offices up to multi-datacenter setups. Solutions including PXE (kickstart/preseed/Cobbler), Katello, Puppet, SaltStack, asset tracking, lifecycle management, testing, custom Linux distributions and bespoke auditing tools.

Designed networks to specification (cost or functionality), familiar with large layer 2/3 deployments including STP, DTP, LACP protocols, VLAN tagging, trunking, layer 2 protections (ARP, DHCP, BPDU guard), static routing, dynamic routing (RIP,

OSPF, EIGRP, BGP), MPLS (L2 and L3 VPNs, LSPs), QOS, ASA firewalls, ACL management, redundancy, performance optimisation, asynchronous routing, remote troubleshooting, issue diagnostics (layer 1-8) and vendor interaction/management (global).

Re-designed and migrated multiple data centre architectures for hosting providers and global companies including coordination with on-site resources for physical relocation, design constraints, and implementation of redundant core and distribution network services, designing single points of failure out, isolating management connectivity into segregated failure domains (physically, up to a separate BGP mix with different routes), the design of troubleshooting tools for helpdesk staff, auditing equipment, implementation of off-site backup arrangements, low-level migration tools (redirection of network traffic to holding servers, DDOS protection, distributed caching, automated route adjustment tools, automated firewall rule distribution tools), power usage profiling and cost reduction.

Volunteering experience

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, post FOSDEM.
- 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 camp sites, 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
- References available upon request

See Also

- GitHub - damianzaremba
- Last.fm - damianzaremba4
- LinkedIn - damianzaremba
- Website - damianzaremba.co.uk