VINYLDNS COMCAST CASE STUDY

👀 https://opensource.com/article/20/9/open-source-dns

October 2020

COMCAST

AGENDA

1. Intro
2. Background
3. Challenges
4. VinylDNS
5. Scaling VinylDNS for Large Enterprises
6. Results
7. VinylDNS Futures

INTROS

- *WHO ARE WE?*
  - Paul Cleary – Senior Principal Software Engineer @ Comcast
  - Joe Crowe – Senior DNS Engineer @ Comcast
- *WHAT IS VINYLDNS?*
  - Platform for DNS Governance
  - Vendor agnostic, uniform interface for managing diverse DNS systems, including public cloud
  - Single view of data and operations across all your DNS systems
  - Self service DNS with guardrails
  - Gobs of access controls

BACKGROUND

AGILITY

DevOps practices have increased the need for agility

- Immutable infrastructure and frequent deployments require constant changes in DNS records
- DNS changes need to be applied immediately
- Automation cannot wait for a human response

GOVERNANCE

DNS records are some of the most important and sensitive assets in any Company

- DNS manages traffic for thousands of internal applications and services
- Inadvertent DNS changes can cause instability and complete outages
- Malicious DNS change can secretly route traffic to bad actors

CHALLENGES (CIRCA 2015)

1. Existing system was partially automated, partially manual
   1. DNS technicians review some changes, sometimes rejecting them
   2. Some automation applied other changes that met certain criteria
2. Long turn around times (30 minutes – 24 hours)
   1. Tickets are not immediately applied
   2. Sometimes tickets are rejected
   3. **Challenge – automation needs were not being met**
3. Large Scale (100 Million DNS records, 1 Million DNS zones, Thousands of changes per day)
   1. Impossible for DNS technicians to understand the significance of many DNS requests
   2. Approve – possibly apply an errant DNS change
   3. Reject – delay critical infrastructure changes, sometimes in response to an ongoing situation
   4. **Challenge – governance needs were not being met**

VINYLDNS WAS BORN

1. Existing options did not meet both the automation and governance needs
2. Built VinylDNS as an API Gateway to enable safe DNS record management for internal engineering teams
3. The initial governance model was ”Private Zones”, with a “Power User” experience similar to Route 53
    1. DNS Zones can be assigned “ownership” to a group that can manage that zone
    2. DNS record access can be granted outside of the owner group via ACL Rules
        1. *Allow AppTeam1 access to manage www.* for record types A, AAAA, CNAME*
4. REST API enabled simple integration
    1. DNS changes were already “pre-approved” via Security and ACL rules
    2. Changes could be realized as part of automation including Terraform and Ansible

DEMO – PRIVATE (OWNED) ZONES

1. FUTURAMA
    1. bender – a bot, owns bots.planetexpress.com
    2. hermes – accountant, owns finance.planetexpress.com
    3. leela – a VinylDNS sys admin (aka super user)
        1. owns planetexpress.com

SCALING FOR THE ENTERPRISE

1. High Value Domains
   1. Completely lock out VinylDNS from touching certain DNS records
2. ACL Rule model didn’t scale to Millions of Zones
   1. “Shared zone” and “record ownership” model
   2. Reverse zones are often ad-hoc shared space
3. Some DNS changes still require manual review
   1. Manual review workflow for certain DNS changes
4. Ownership of records silently transferred based on organization responsibilities
   1. Global ACLs support overrides for certain DNS records to allow them to be created by one team and managed by others in a more ad-hoc fashion
5. Scheduled Changes
   1. Assign a date/time for a DNS request to be implemented in the future

DEMO - SCALING FEATURES

1. Shared Zones, DNS Requests
2. Manual Review
3. High Value Domains – www.planetexpress.com

VINYLDNS RESULTS

1. Manages much of Comcast’s internal DNS space (not customer DNS space)
   1. Millions DNS records
   2. Hundreds of thousands of DNS Zones
   3. Thousands of DNS changes per day
2. Supports most of Comcast’s engineering teams
   1. Thousands VinylDNS users
   2. 1,000 VinylDNS groups
   3. 99% of all changes implemented in a few seconds
3. One small central DNS admin group for VinylDNS
4. Open sourced in 2018, scale out updates built primarily in 2019

VINYLDNS FUTURES

1. Tighter integration with DNS servers (Zone Management)
2. VinylDNS Admin Experience
3. Other (link to github issues) – pitch for ideas / contribs
    1. Chat - https://gitter.im/vinyldns/vinyldns
    2. Issues - https://github.com/vinyldns/vinyldns/issues
    3. Docs - https://www.vinyldns.io/

COMCAST