How an Enterprise Manages Very Large Number of DNS Records

Han Zhang, Pallavi Aras
Salesforce

How Do You Use DNS?

- Who make DNS changes in your company?
  - DNS admins/teams
  - Various operational teams
  - Automation tools
- How many zones do you manage?
- How many records do you manage?
- How dynamic are the records/zones?
- Do you use single DNS provider or multiple providers for the zones?
- How many accounts do you manage on all the providers?

When It Becomes Complicated

- How about tens of millions of records in thousands of zones hosted on multiple DNS providers?
  - Manual change is not possible
  - All the teams and tools need to know on which DNS providers the zones are hosted
  - Different providers have different Rest API specifications
  - How about we add new zones?
  - How about we migrate zones between DNS providers?

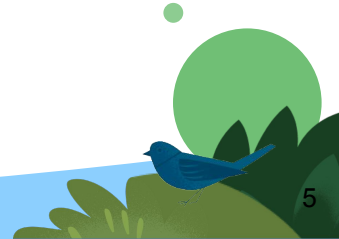
Tools for Managing DNS across Multiple Providers

- OctoDNS
  - Infrastructure as code
- Netflix denominator
  - CLI tool
- ExternalDNS
  - Manage DNS records for Kubernetes

What Do We Need?

A DNS provider agnostic Rest API endpoint

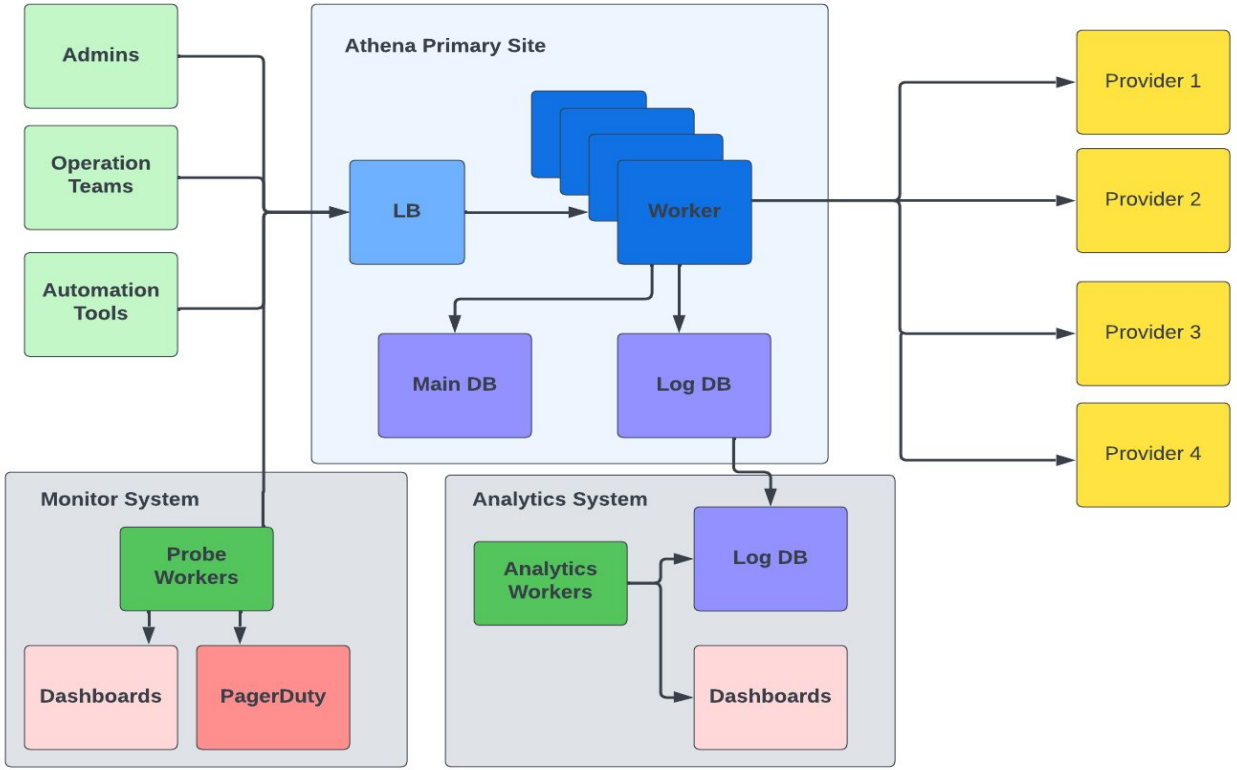
- Hide the details of providers
- Provide a standard interface to make DNS changes
- Provide standard responses to the users
- High availability
- High scalability
- Easy account management



Athena - A DNS provider agnostic Rest API endpoint

- Hosted on a cloud platform
- Highly available
- Highly scalable
- Tens of millions of records
- Thousands of zones
- Multiple DNS providers
- Users are admins, operational teams, application code, automation tools
- Handles over 1 million create/update/delete requests per day
- Has been used in production for 4 years

Athena Ecosystem



How to Manage the Zone Vendor Mappings

- A microservice pulls zone list from DNS providers
- Mapping can also be added manually using Rest API calls
- In Athena DB:

```
{
        "zone": "example.com.",
        "primaryVendors": [ "providerA"]
}
```

Account Management

- 20 teams, 20 engineers on each team, 10 providers
- Total number of accounts to manage
  - Without Athena: 20*20*10 = 4,000 accounts
  - With Athena:
    - Single account for each team on each provider: 200 accounts
    - Each engineer has an Athena account: 20*20 = 400 accounts
    - Total: 600 accounts 15% of 4,000 accounts
- When an engineer leaves the company
  - Without Athena: 10 accounts need to be removed from all the providers
  - With Athena: a single account needs to be removed
- "providerAccount":

  { "provider1": "account1",

  "provider2": "account2"}

Communicate with Athena

- Curl command
- Postman, etc
- We developed a CLI toolkit
  - toolkit --prod --update add cname foo.example.com bar.example.com

Future Work

- Support atomic transaction
  - Multiple domains need to be CRUD together
  - A zone is hosted on two providers, both serve as primary
  - Two-phase commit and SAGA
- Fine-grained access control
  - Type-level access control
  - Record-level access control
- More Authentication Methods
  - mTLS

Questions?