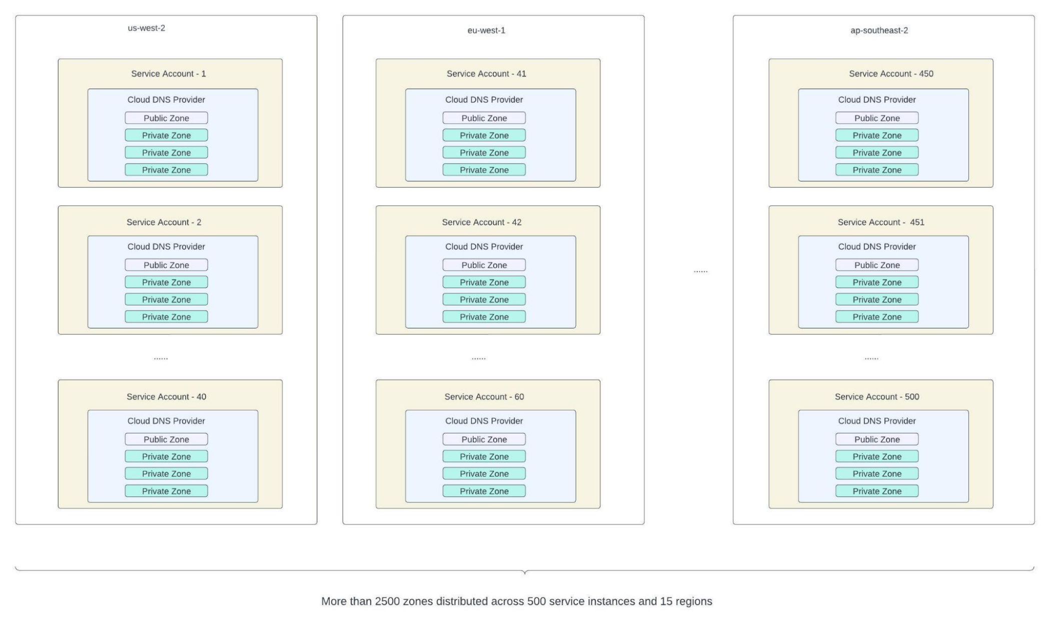
Cloud DNS Monitoring in Large Scale

Sidan Qi (sidan.qi@salesforce.com)
Sile Yang (sile.yang@salesforce.com)

Feb 9th 2024
OARC 42 workshop,
Charlotte, NC, USA

DNS Monitoring Overview
- Managing Scale and Distribution

- Private DNS System
  - Only associated virtual private cloud (VPC) can query private DNS
  - DNSSEC validation enabled on VPC
- Manages more than **2500** DNS zones
  - 500 service accounts
  - 15 Regions Globally
  - Up to 10,000 records per zone



us-west-2

Service Account - 1
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

Service Account - 2
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

......

Service Account - 40
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

eu-west-1

Service Account - 41
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

Service Account - 42
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

......

Service Account - 60
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

......

ap-southeast-2

Service Account - 450
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

Service Account - 451
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

......

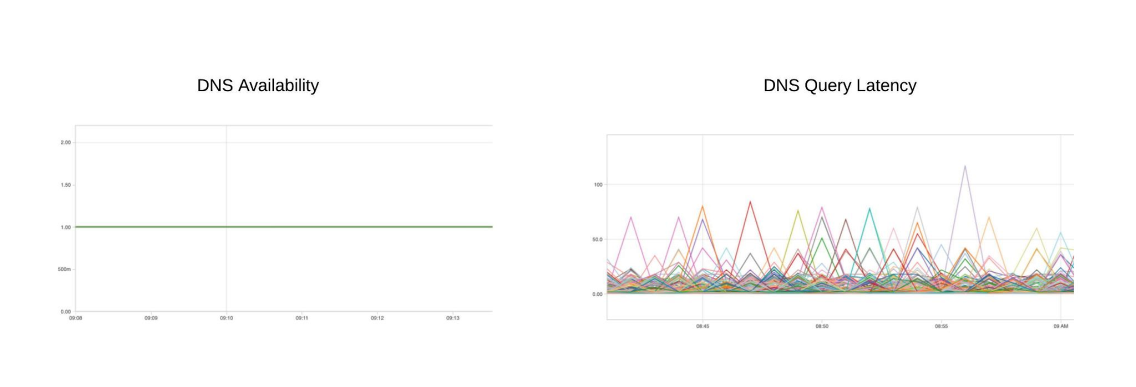
Service Account - 500
Cloud DNS Provider
Public Zone
Private Zone
Private Zone
Private Zone

More than 2500 zones distributed across 500 service instances and 15 regions

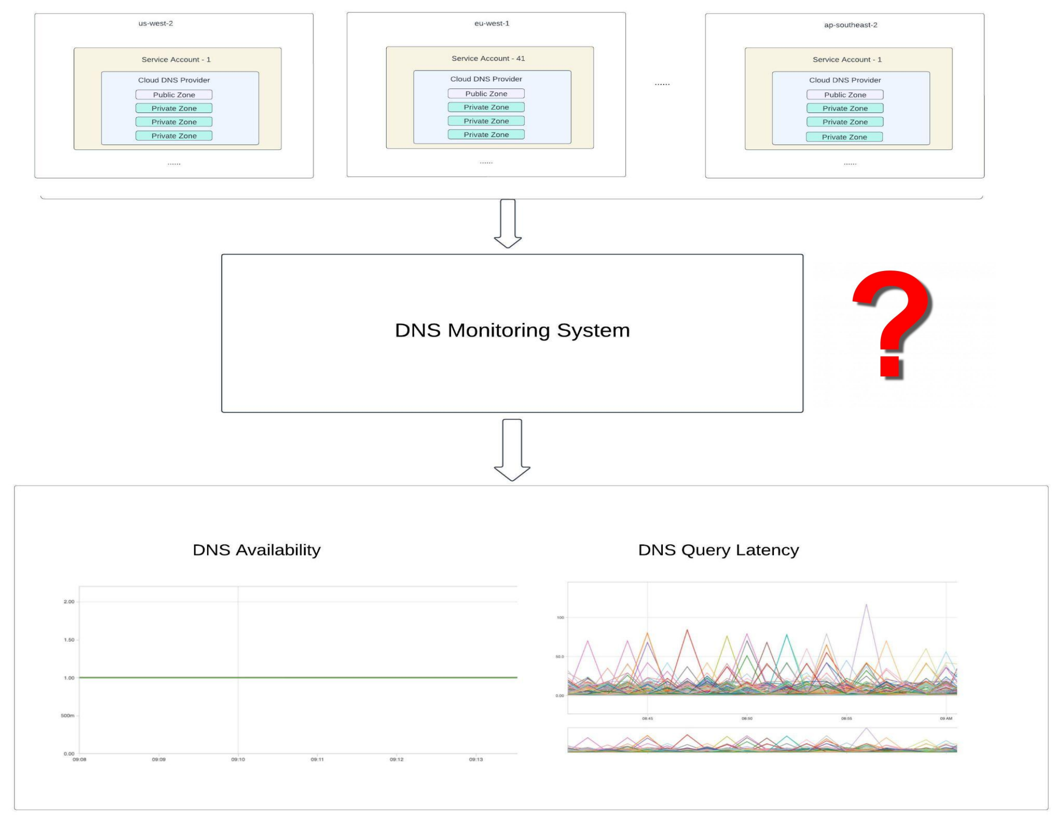
DNS Monitoring Overview

- Key Metrics in DNS Monitoring

- DNS Availability
  - Zone Resolution - checking the accuracy of query results
  - Zone Delegation - verifying that name servers are properly configured for **public zones**
  - Zone-VPC Association - checking whether specific vpcs associated with **private zones**
- Query latency
  - Response Time - measures the time it takes for a DNS query to be completed

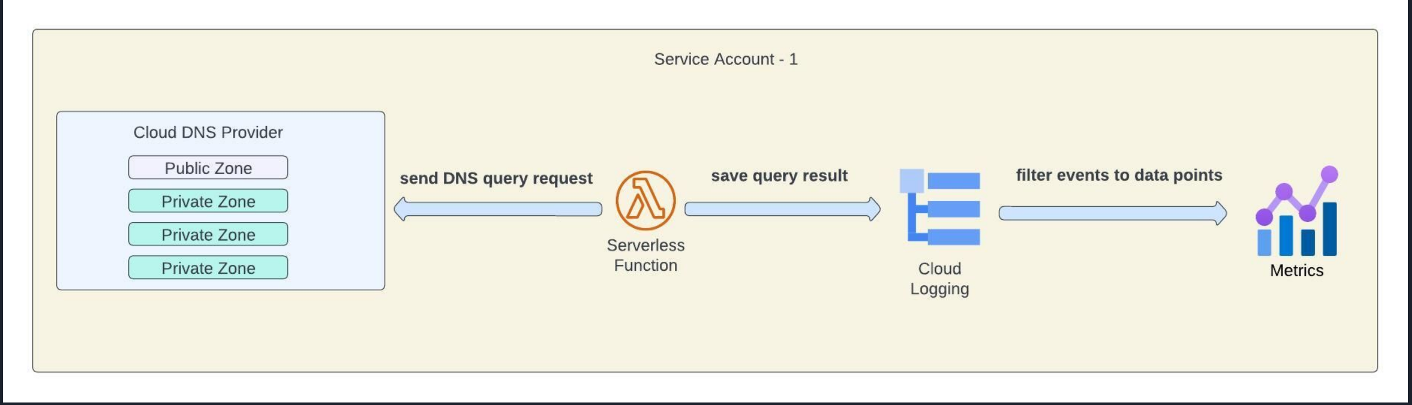


DNS Monitoring System overview



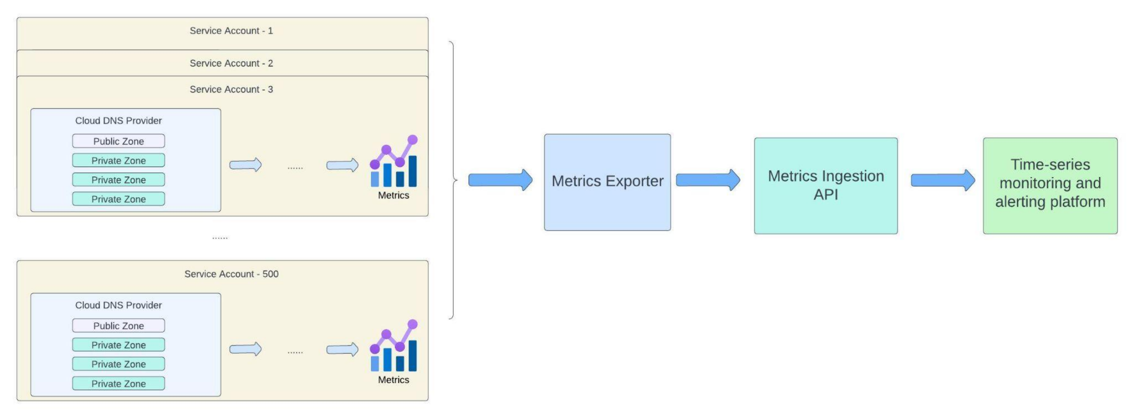
DNS Monitoring System overview
-   Synthetic Monitoring

1. Serverless function (e.g. AWS Lambda) sends DNS query request to each hosted zone
2. Serverless function log the query result and query response time to cloud logging system
3. From cloud logging system, filter every event to data point
   a. Successful query → 1 , Failed query → 0
   b. Query response time
4. Finally, data points are aggregated to metrics



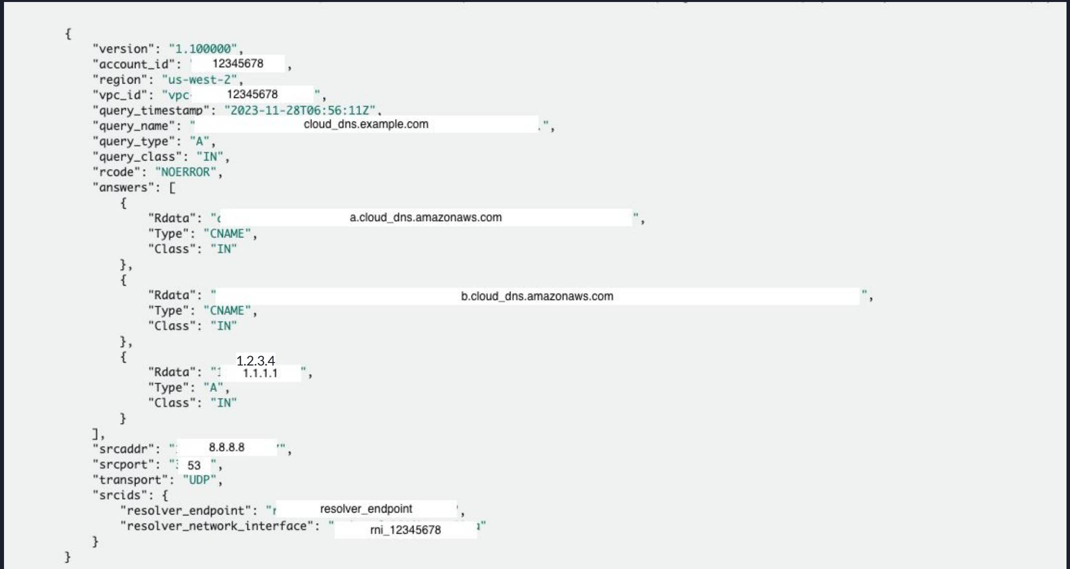
DNS Monitoring System overview
- Export the metrics

- Metrics Exporter - Collects Metrics from all service accounts and send metrics to ingestion API
- Metrics Ingestion API - Sends JSON messages and metrics to monitoring platform
- Time-series Monitoring and Alerting Platform - Generates monitoring dashboard



DNS Monitoring Enhancement
- Cloud Provider's DNS Query Logging

- DNS Query Logging enables users to log information about the DNS queries that Cloud DNS provider receives
- DNS Query Logging monitors real user query while the synthetic DNS monitoring system is based on the **simulation** of the user traffic



```
{
    "version": "1.100000",
    "account_id": "12345678",
    "region": "us-west-2",
    "vpc_id": "vpc-12345678",
    "query_timestamp": "2023-11-28T06:56:11Z",
    "query_name": "cloud_dns.example.com.",
    "query_type": "A",
    "query_class": "IN",
    "rcode": "NOERROR",
    "answers": [
        {
            "Rdata": "a.cloud_dns.amazonaws.com",
            "Type": "CNAME",
            "Class": "IN"
        },
        {
            "Rdata": "b.cloud_dns.amazonaws.com",
            "Type": "CNAME",
            "Class": "IN"
        },
        {
                     1.2.3.4
            "Rdata": "1.1.1.1",
            "Type": "A",
            "Class": "IN"
        }
    ],
    "srcaddr": "8.8.8.8",
    "srcport": "53",
    "transport": "UDP",
    "srcids": {
        "resolver_endpoint": "resolver_endpoint",
        "resolver_network_interface": "rni_12345678"
    }
}
```

DNS Monitoring Enhancement
- Cloud Provider’s DNS Query Logging

- Benefits of Enabling Query Logging
  - Enhanced Resolution Monitoring
    - Enables detailed tracking of DNS query resolutions originating from Virtual Private Cloud (VPC) environments for private DNS
  - Improved Cost Management
    - Provides critical insights into the volume of DNS queries made which are charged by cloud provider

DNS Monitoring - Limitations & Challenges

- Current monitoring system only covers the zone resolution and delegation. Many other DNS health metrics like DNSSEC, propagation time, and resolution path are not covered.
- Current monitoring system is not sensitive enough to inside traffic/request burst.
- Cloud provides impose strict rate limit, causing problems for applications that issue high-volume of DNS requests.

DNS Monitoring - Learnings

- Trade-off among the amount of monitoring, operational cost, system performance, …
- Leverage multiple cloud-based built-in tools (i.e. CloudWatch in AWS). These tools save us a lot of work and time.
- Decentralizing DNS infrastructure requires a distributed DNS monitoring system - this way helps us to deal with rate limit challenge.
- Build an automated system in large scale - use cloud-based approaches (i.e. Infra as Code, Metrics Exporter..) to implement a easy-to-build and easy-to-maintain monitoring system.
- Integrate the use of capacity forecasting system

Questions/Comments?

Topic Summary

- Our Cloud DNS infrastructure manages over 2,500 zones across 15 regions globally, with each zone capable of hosting up to 10,000 records.
- The primary metrics for our monitoring focus are DNS Availability and Query Latency.
- Our DNS proactive monitoring system utilizes a suite of cloud-based tools, including serverless functions, cloud logging systems, and metrics filters.
- The query logging feature offered by DNS cloud providers significantly improves resolution monitoring for private DNS and facilitates efficient cost management.
- Build a monitoring system in large scale is a trade-off among monitoring amount, cost, performance, rate limit.
- Take advantage of public cloud provides: built-in tools, open-source communities..

Thank you