University of Notre Dame

DNS use guidelines in AWS

Jan 5, 2015
Version 1.0

Contents

1 Purpose

1.1 Overview

The purpose of this document is to provide information on how to configure DNS for servers in AWS. The document discusses various scenarios and provides examples to aid in understanding how DNS will respond to name queries from various points in the on premise datacenter and AWS infrastructure.

2 DNS Overview

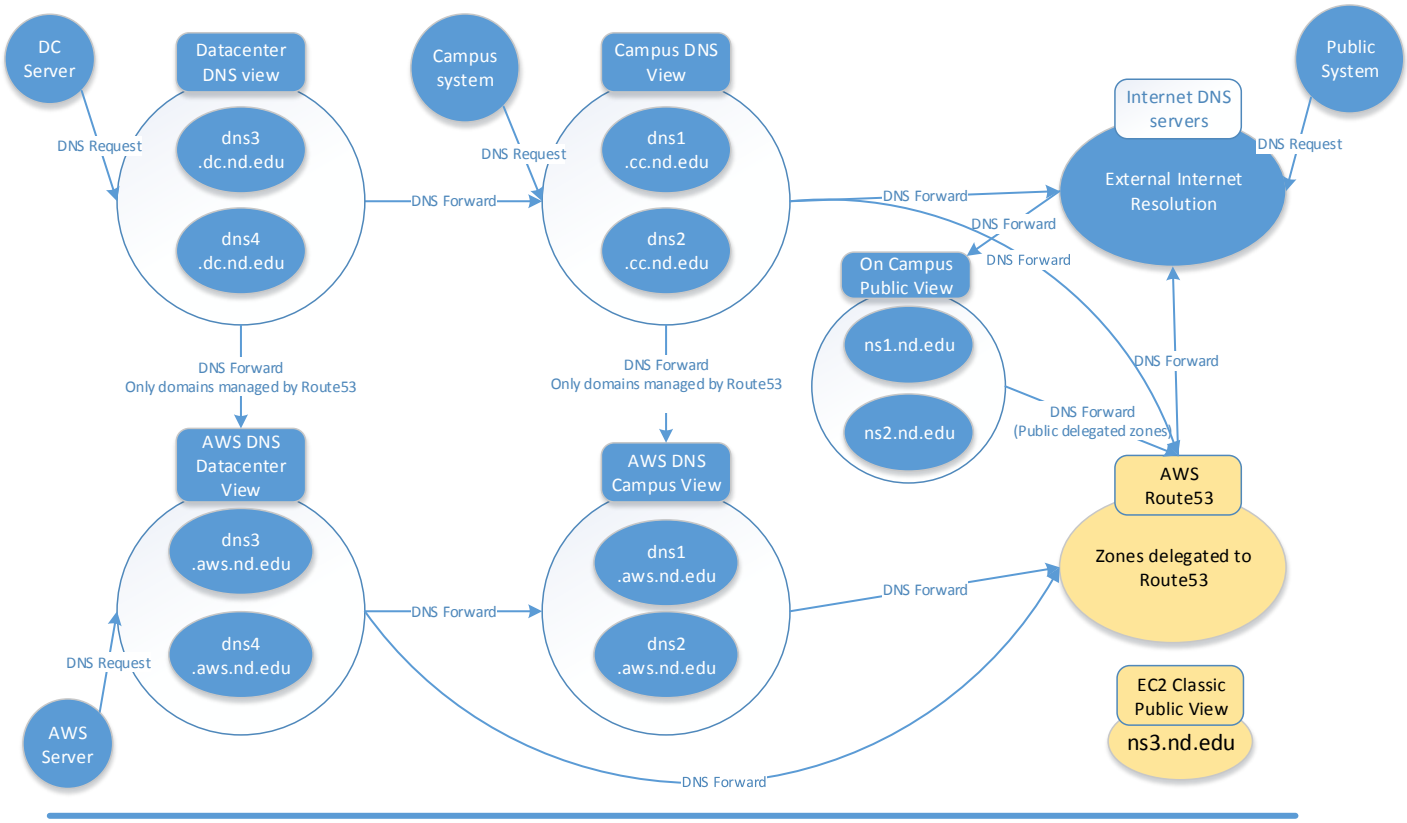
2.1 On Premise DNS

There are currently three views of the DNS name space provided by the on campus DNS system, Datacenter, Campus, and Public. The Datacenter view provides name resolution for privately addressed servers in the main campus datacenters. These addresses can only be resolved by servers that are in the datacenter using the datacenter DNS servers DNS3/4 for resolution. Campus view provides DNS resolution for campus systems and services, both public and private addresses. The Public view is seen by external Internet hosts for domains that are authoritative for nd.edu and not specifically delegated to AWS route53.

2.2 AWS DNS

AWS DNS servers, operated by the OIT, are in the shared services VPC and mimic the datacenter and campus DNS views. There is also a tertiary public view DNS server which is currently in the EC2 classic environment and will be moved to one of the shared services public subnet.

2.3 DNS Logical Diagram



3 Guidance for using DNS

3.1 DNS Management order of preference

1. Manage everything in infoblox unless specific Route53 functions are needed. Point DNS to DNS3/4 in Amazon (Data Center View), this will forward to DNS1/2 (campus view in AWS) to resolve aws.nd.edu, etc. Use a different domain for private and public addresses. If Route53 functions are needed (maybe to use DNS health checks) create a separate domain for these AWS hosts in Route53. Subject to DNS management restrictions. Still point to DNS3/4 in shared services.

2. Manage everything in AWS. If you do this you should put entries in Infoblox to reserve the space as managed in AWS.
    a. If you manage in AWS and use split horizon in AWS, campus can resolve either the private or public but not both.
    b. You will have to manage Route53 from the DCND account with specific permissions on your zone.

3. If completely isolated you can use Route53 directly, but then you lose access to any private addressed services.

3.2 DNS Management Restrictions

- Campus Public IP's cannot go over the tunnel. (Without ugly Nat'ing)
- AWS may have public and private views of the same domain, split horizon. Only one or the other may be visible from a particular view.
- AWS may have public and private domains that do not have the same name. Example, aws.nd.edu should this be strictly private.

4 DNS Scenarios Considered

DC server resolves name in AWS – need private IP returned (server to server com over tunnel)

DC server resolves name in AWS – needs public IP (access via ELB over Internet)

AWS server resolves name in AWS – need private IP returned (ex. Monitoring/logging)

AWS server resolves name in AWS – needs public IP (external ELB)

AWS server resolves name in dc.nd.edu – need private IP returned (database access)

AWS server resolves name in nd.edu – needs public IP (library servers, other public services)

Campus resolves name in AWS – need private IP returned (fat client database access over tunnel)

Campus resolves name in AWS – needs public IP (ELB access to public service)

5 DNS Issues

Do we want to retain the AWS.ND.EDU domain name or change it to something else? Yes.

Should we create a myname-tunnel.nd.edu domain for services that get traffic over the tunnels?

We need to correct DHCP options default domain to be correct (whatever that means), but right now its multi-value which doesn't work. This becomes the domain of the ec2 instance in meta-data.

6 DNS Examples

6.1 Resolving aws.nd.edu

The aws.nd.edu domain maps names to private IPs in the 172.22.0.0/16 range. These addresses are used in the AWS infrastructure VPC architecture. This is the OIT managed "datacenter" in AWS. Servers in AWS that make DNS requests to dns3.aws.nd.edu and dns4.aws.nd.edu (AWS Datacenter View) will resolve these addresses directly. This resolution will also occur for the on campus datacenter view for systems querying dns3.dc.nd.edu and dns4.dc.nd.edu and the campus view for systems querying dns1.cc.nd.edu or dns2.cc.nd.edu.

6.2 Resolving dc.nd.edu

The dc.nd.edu domain maps names to private IPs in the 172.19.x.y range for datacenter subnets. These addresses are used in the on premise datacenters. This is the OIT managed "datacenter" on campus. Servers in the on campus datacenter that make DNS requests to dns3.dc.nd.edu and dns4.dc.nd.edu (Datacenter View) will resolve these addresses directly and always received the private address. This resolution will also occur for the on AWS datacenter view for systems querying dns3.aws.nd.edu and dns4.aws.nd.edu. There is a split horizon view for dc.nd.edu where some hosts will resolve to different addresses based on querying from campus vs. the campus or AWS datacenters. For systems querying

dns1.cc.nd.edu or dns2.cc.nd.edu (Campus view) some dc.nd.edu records will return campus accessible IPs instead of datacenter IPs.

6.3 Resolving identity.nd.edu

The identity.nd.edu is a split horizon domain managed in Route53. It uses Route53 health checks to determine whether to return a campus or AWS public address for public services. Within the AWS and Campus datacenters identity.nd.edu names resolve to AWS datacenter private addresses. In the Campus and Public views identity.nd.edu names resolve to public addresses, for public services.