US Navy
PEO Digital
OTP ORE
Domain Naming Service Plan

PWS 3.4.11.1

17 April 2023

2 TWELVE Solutions
241 18th Street, Suite 203
Arlington, VA 22202

www.2TWELVEsolutions.com

Overview

In order to integrate modern solutions into a global enterprise, key foundational elements, such as a modern, high availability Domain Name System (DNS) must be in place to support modern, cloud-native, solutions. This includes DNS visibility and monitoring capabilities, which provide critical metrics and oversight for the TCP/IP network.

The DNS is a critical function for all types of application access. As such, DNS failures can have a cascading effect on the performance and access of all other systems and services. When a system fails, one of the first checks is to verify that DNS is operational. **From an availability perspective, it is recommended to keep strongly dependent resources - such as DNS, domain controllers - as logically close (flattening network subnets, domains, etc.) as possible to the workloads that depend on them**.

This DNS plan supports cloud tolerant, cloud ready, and cloud native systems across multiple cloud environments. Additionally, this plan implements DNSsec, which integrates security components into the naming services. This plan is informed by the Navy state configuration data, as well as DNS implementations developed Triton Lab for the prototype during the OTA. With the scarce number of routable IPv4 addresses, it is important a modern design include a DNS that resolves IPv6. These design implementations included DNS to support Hybrid on-premise to cloud, cloud to cloud, and monolithic applications to containers/microservices. **The target state DNS should be decoupled to service multiple states of the hybrid ranging from Cloud tolerant, ready and native**. The recommendations provide the foundation that must be in place at a minimum to be able to adopt the target endstate DNS design that can support current hybrid cloud environments (Azure, and AWS) and microservices architectures.

Critical Design elements

- Zones and physical/logical DNS locations, routing and load balancing
    - For High Availability (HA), DNS servers should be replicated across multiple logical cloud zones
    - Modern platforms generally replicate and synchronize “n+2” systems for HA
    - Must handle the organization's load, security, and scalability requirements
        - DNSsec
        - Scalability
    - Multiple routing pathways and load balancing systems are critical
- Time to live policies and caching
    - The shorter it is, more traffic shaping options are available
    - General recommendations for stable DNS (no frequent updates) is 1 hour. If making DNS updates, lower the TTL to 5min (300s) at least a day in advance. After changes are made operations can revert to TTL of 1 hour
- Monitoring and management
    - Log collection and monitoring tools to track the health and performance
- Naming Conventions
    - Plan will provide name services for ORE.NAVY.MIL and subdomains. Can support custom domains and subdomains.
    - Rapidly provide services under ORE.NAVY.MIL subdomain, such as www.project.ABC.ORE.NAVY.MIL

Initial DNS Architecture Plan

Automation is critical for both resiliency and performance of the modern DNS, the ORE DNS plan includes IaC templates to deploy HA DNS for Triton Lab platform for ORE cloud native application. The template will create three stateless cloud compute instances running BIND DNS across multiple availability zones for resiliency, along with one stateless cloud compute instance to handle DNS layer 4 Load Balancing and one elastic file system for HA DNS data storage.

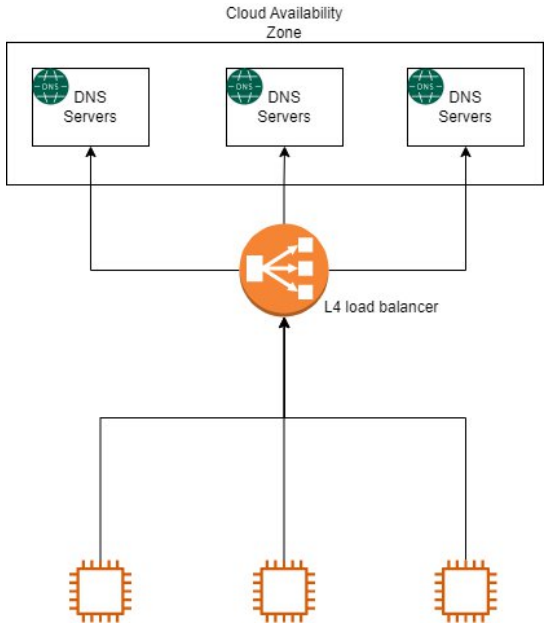
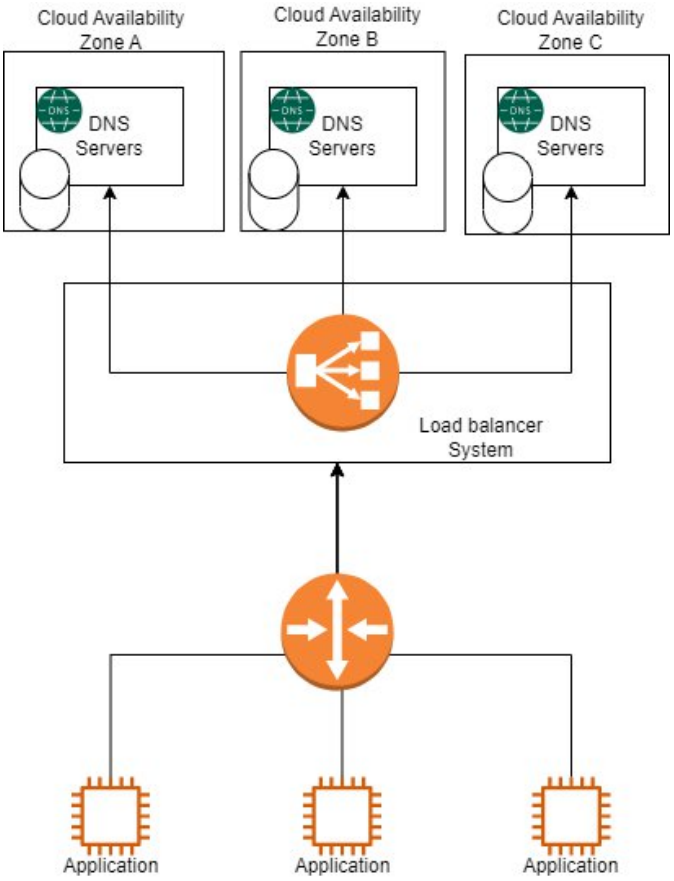


Figure 1: Base High Availability Cloud DNS system

Resilience for Enterprise Scale

To increase service resilience, this architecture can be adjusted and replicated across multiple network regions and zones to ensure endpoints can reach DNS services. The load balancing and networking system should also provide multiple routing pathways to ensure connection as shown in the diagram below.



DNS Security (DNSSec)

DNSSEC is required to meet government compliance objectives. The implementation of DNSSEC is intended to protect the reputation of government domains and prevent attacks on DNS infrastructure. *OMB M-08-23: Securing the Federal Government's Domain Name System Infrastructure*[i] directs government entities to secure the .gov/.mil and all second level TLDs (Navy.mil using DNSSEC).

Within Triton lab, the OTA team prototyped the impact of sublevel domains to the TLD. This design approach requires integration and management for the object records and its impact to integrated AD as current NMCI design. Locality, ownership, access, and current state resource records need to be understood. The security design tradeoffs for a target state should balance the exposure of AD to the cloud, ensuring there are no open inbound ports proliferating copies and replicas of sensitive AD data to the external cloud infrastructure. This design will enable organizations to authenticate users against on-premises AD.

Implementing DNSSEC involves a series of steps, including generating keys, configuring zones, signing zones, and publishing keys.

Generate Keys:

There are different tools available to generate DNSSEC keys. One popular tool is called dnssec-keygen, which is included in the BIND DNS server software. This DNS Plan intends to generate keys with the following script:

```
dnssec-keygen -a RSASHA256 -b 2048 -n ZONE example.com
```

Configure Zones:

The DNSSEC-related resource records must be configured to the zone file. These include the DNSKEY record, which contains the public key, and the DS record, which is used to publish the public key in the parent zone. Sample configuration below:

```
$ORIGIN example.com.
$TTL 3600
@   IN  SOA ns1.example.com. admin.example.com. (
            2021040501 ; serial
            3600       ; refresh
            1800       ; retry
            604800     ; expire
            3600       ; minimum
            )
    IN  NS  ns1.example.com.
    IN  NS  ns2.example.com.
    IN  A   192.0.2.1
; DNSSEC-related resource records
    IN  DNSKEY  (...)
    IN  DS      (...)
```

Sign Zones:

To sign zones, the plan is to leverage the dnssec-signzone command included in the BIND DNS server software. General example below:

```
dnssec-signzone -A -N INCREMENT -o example.com -t example.com.signed
example.com Kexample.com.+008+12345.private
```

Publish Keys:

To publish the public key in the parent zone, this plan creates a DS record for the signed zone and submit it to the parent zone administrator. The DS record contains a hash of the public key, along with metadata. General record template below:

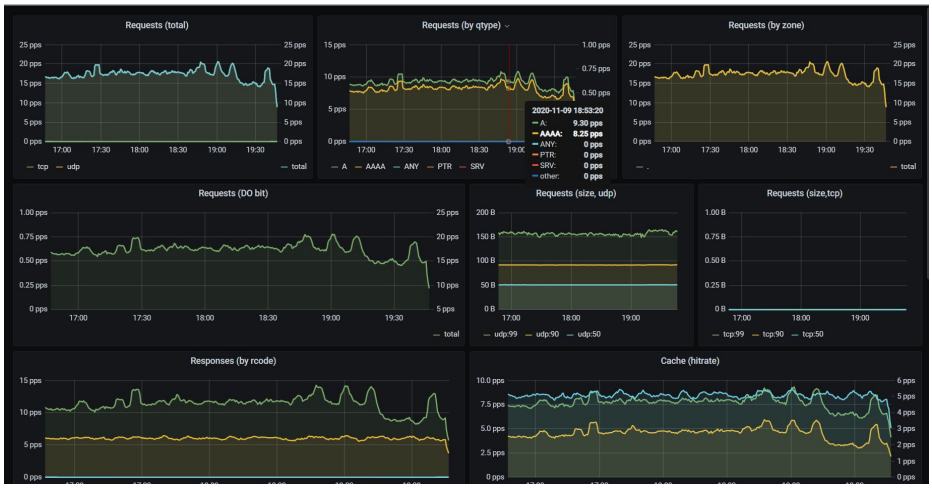
```
example.com. IN DS 12345 8 2 ABCDEF...
```

Monitoring and Oversight

The DNS plan includes logging and monitoring for DNS performance and managing cases such as spike in NXDOMAIN responses. This will allow operations to have granular alerting and visibility into performance issues related to DNS and allow the organization to identify and resolve access degradation issues early on. Metrics as shown in the example figure below can identify trends, such as domains that have increased traffic or domains that are erroneously accessed. **With this type of insight, operations teams can set quality of service (QoS) levels for the identified domains to prioritize and increase bandwidth or de-prioritize and rate-limit as appropriate.** The data can also trigger alerts so responsive actions can be applied before major issues arise or to support investigation or discovery efforts.

The screenshot below shows a designed and implemented prototype built in Triton Lab to demonstrate a Hybrid DNS monitoring that meets the recommendations above.

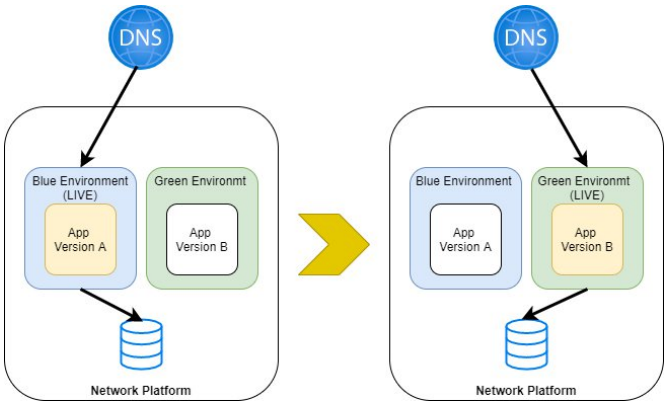
Figure 1 - DNS Metrics



Benefits: Blue/Green Deployments

Blue-green deployment is a technique that reduces downtime and risk by running two identical production environments called Blue and Green. **The fundamental idea behind blue/green deployment is to shift traffic between two identical environments that are running different versions of your application**.

The blue environment represents the current application version serving production traffic. **In parallel,** the green environment is staged running a different version of your application. Once the green environment completes and passes testing, production traffic is redirected from blue to green.



At any time, only one of the environments is live, with the live environment serving all production traffic. In the left example above, Blue is currently live and Green is idle. After a new version (patch, update, etc) of your software is ready, the deployment and the final testing takes place in the environment that is not live (green in this example). **The DNS is fundamental for blue/green deployments, directing traffic by simply updating DNS records**. **Once deployed and fully tested the software in Green, the DNS routes incoming requests to the Green environment instead of Blue. Green is now live, and Blue is idle.**

This technique can eliminate downtime due to app deployment, reduce risk with the option to roll back to the last version in the Blue environment, and fits well with CI/CD workflows, in many cases limiting their complexity. Deployment automation would have to consider fewer dependencies on an existing environment, state, or configuration.

In addition to a highly available DNS system, Blue Green deployments require a fully automated platform (hypervisor, OS, shared services, applications, and devops pipelines) ensuring the infrastructure and shared services are immutable. All resources within the Triton lab Platform are provisioned and orchestrated by Infrastructure as Code (IaC) frameworks. This provides a degree of immutability and idempotency that allows us to employ continuous integration and continuous delivery at all levels from infrastructure.

This immutability provides the ability to do canary or blue/green deployments and allows Triton Platform to treat all facets of the platform as “cattle” versus “pets.”

Integrated Systems and Dependencies

It is imperative that the Navy remove WINS and LMhost name resolution pathways from the network as seen in other site visits and highlighted in the Pentagon RCA. This can be done via reconciliation and cleanup. The ORE team recommends the DNS design provided which supports on-premise, Linux, containers, and cloud services. If not considering DNS/name resolution within AD/DNS structure, everything will flow through the future DDI solution, which can create resource bottlenecks.

Top level tasks and Dependencies

The target AD design, must account for the current state and must determine the number of forests that the Navy requires.

The plan must provide the design (logical architecture) of the domains, DNS infrastructure, and organizational units (OUs). This includes the location of AD DS sites, the AD DS domain controllers within each site, and the site links and site link bridges that support AD DS replication. The implementation plan must account for the storage/compute requirements, as well as testing, rollback, and user/group/profile management.

Based on the 2020 Pentagon RCA, the current DCs supporting the capital region are undersized. The DC at WYND must be resized and provided the necessary compute, storage, and networking resources to support the approximately 60,000 users.

Additionally, there are a number of AD and Name resolution dependencies that the vendor must address included below.

- Reconciliation and replication of zones
- Forwarding and reverse address lookups
- Subnetting and what endpoints are tied to each.
- Access: enterprise admin and domain admin rights required to truly evaluate current design

Appendix A: DNSSEC

DNSSEC is required to meet government compliance objectives. The implementation of DNSSEC is intended to protect the reputation of government domains and prevent attacks on DNS infrastructure. *OMB M-08-23: Securing the Federal Government's Domain Name System Infrastructure*[ii] directs government entities to secure the .gov/.mil and all second level TLDs (Navy.mil using DNSSEC). The authoritative source, NIST SP 800-53 rev 4/5, includes SC-20: SECURE NAME/ADDRESS RESOLUTION SERVICE[iii], which recommends implementation of DNSSEC for DNS server implementations for low, moderate and high baselines.

The design of DNS is inherently prone to spoofing and man in the middle (MITM) attacks. DNSSEC provides security enhancements to DNS components that enable DNS data to be cryptographically signed and verified using PKI. With DNSSEC, a DNS server can validate responses that it receives as genuine. By validating DNS responses, DNS servers and clients are protected against DNS spoofing.

Spoofing or MITM of government DNS servers has generally been a low threat. The predominant number of authoritative DNS servers, services that rely on those DNS servers, and users of said services reside behind the protected perimeters of government networks. As a result, there is little opportunity for adversaries to discover and exploit DNS traffic. This premise is rapidly changing, however. Government entities and users are now major consumers of cloud and externally managed and hosted services. This in turn has required operations to make more DNS zones available over the Internet for either interoperability reasons with the external service providers or ease of use for remote users such as enabling VPN-less access.

VPN-less access or the proliferation of on and off VPN access to organizational resources increases the threat profile. Before COVID, VPN was implemented as always-on, and all network traffic – including DNS traffic – goes over the VPN. But in order reduce bottlenecks on the VPN, government entities have shifted to an as-needed VPN implementation. **This opens up the opportunity for users to encounter domain spoofing attacks when accessing HTTP content**. When the user enters "outlook.com" into the URL bar of the browser, if DNS is spoofed, it could resolve a non-Microsoft IP and redirect to https://notoutlook.ru. All the redirection, federation, protocol upgrade schemes occurring on dynamic web applications make it hard for users to notice such changes.

These type of use cases are the new normal. Government entities will consume more externally hosted services. Users will be off network more consistently. Government managed services will be hosted in multiple collocation facilities and/or cloud IaaS across multiple regions and availability zones. In the end it will not be possible to keep authoritative DNS servers only behind the protected perimeters. DNS implementations will need to horizontally scale to meet the performance needs of the dependent applications at those locations. Therefore, DNSSEC will be necessary sooner than later to meet the demand and overcome the increased threat. **DNSSEC will need to be successfully implemented in order to achieve compliance mandates.**

---

[i] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf
[ii] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf
[iii] https://nvd.nist.gov/800-53/Rev4/control/SC-20