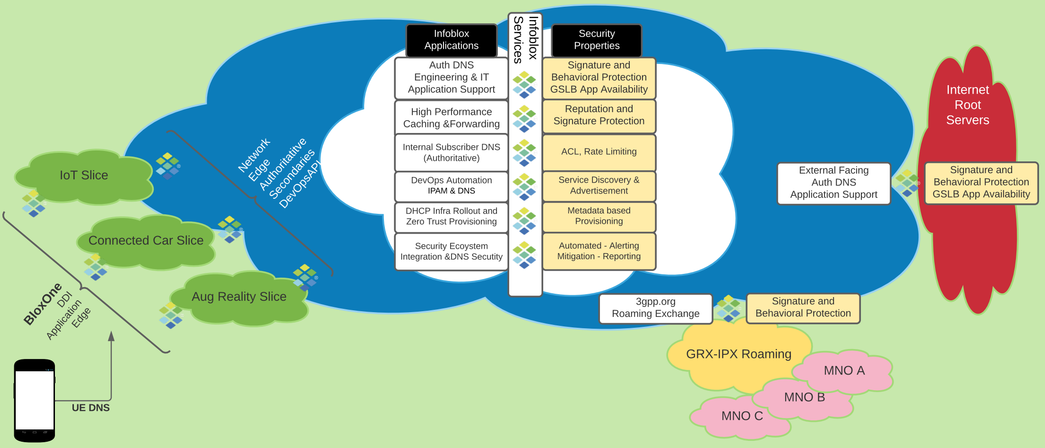
# Infoblox DNS Best Practice for Service Providers

The key aspects outlined in this document have multiple overlapping practices. Network topology and system architecture cannot be discussed without considering security and risk reduction. Naming conventions and name space architecture are relevant to network configuration and security, especially when considering the roaming services. Too often automation is overlooked or considered to be “mandatory” with no consideration of integration points, metadata discontinuity and functional requirements for infrastructure automation. Choosing a unified end to end DNS solution from core to edge and far edge across all network slices provides the most redundant, recoverable and reliable solution available.




### DNS Best Practices

**Position user plane DNS high speed Gi caching** on separate servers as close to the customer as geographically possible.
**Provide Geo-Redundancy to avoid single point of failure** in addition to redundant hardware in the VNF. Geo-Redundancy and local survivability should be considered for each service point. Multiple Anycast groups provide the best redundancy for DNS caching.
**Multimaster DNS** provides the protocol level redundancy required by authoritative DNS.
**Deliver authoritative and caching DNS by dedicated servers.** Authoritative and caching servers have different traffic profiles and different security exposure. Separate authoritative DNS from packet core (3GPP TS33.310, 33.210, GSMA PRD IR.67). It is also recommended to separate the user plane that carries DNS queries from DNS management traffic using an out of band secure management network.
**Separate user plane/data plane & management** traffic for all DNS by enabling out of band management for the Grid VPN to guarantee management traffic is separate from user plane to avoid security risks and traffic bottlenecks during security and incident management.
**Hybrid Public/Private Cloud deployments** provide platform diversity as well as Geo-Redundancy and local survivability.
**BloxOne DDI SaaS based DNS** provides Zero Touch Provisioning at web scale using a container based deployment model and can be monetized for enterprise and other commercial deployments.

### Security Considerations

**Restrict caching DNS service** to “subscribers only” to avoid acting as an open resolver to the Internet. ACLs must be set appropriately to ensure only valid users or applications are accessing DNS infrastructure. Enabling RPZ, ADP, Threat Insight for Data Exfiltration, provides best in class DNS security.
**Protect the DNS server and all the underlying protocols** required to deliver DNS services (UDP/TCP/NTP/OSPF/BGP etc.) against security threats. By enabling and tuning Infoblox Advanced DNS Protection “Threat Protect”.
**Implement Role Based Access Control** such that access rights are aligned with the tasks to be executed using a least permissions model.
**Discover unknown devices deployed in the network** and provide those details to IPAM (IP Address Management) with Infoblox Discovery.
**Secure DNS service for GRX/IPX (Behavioral and Signature-based protection).** Enabling “Threat Defense, Threat Protect and Threat Insight” for Reputation, Signature and Behavioral threat mitigation improves security posture & reduces overall attack surface exposed to the Internet and internally.
**Increase visibility** into which devices are making requests to connect to malicious destinations and malware infestation command and control.
**Improve security with DHCP Fingerprinting** to confidently identify devices and apply DHCP filters and controls to allow only legitimate leases and deny nefarious lease requests. Configure DHCP option name spaces to support ONLY the devices that should be allowed to request DHCP addresses. Option spaces ensure the correct strings are sent and identify individual devices.

### DevOps and Automation Considerations

**Use Authoritative IPAM for contextual information** to collect all data into a single source of truth with one database/UI/API. Use discovery to find devices and update IPAM to validate endpoints and address allocations.
**Leverage detailed customizable protocol reporting** to collect all data required to manage capacity, identify anomalies, and track baseline production information daily. Thresholds can be set to send outbound API and alerting for security ecosystem and automation.
**Use Infoblox Grid technology** to make DNS resource record updates without affecting service uptime, all updates and administrative commands are sent across secure encrypted communications. Protocol and management communications should not be sent clear text i.e. zone transfers or control plane messaging.
**Provide automated IPAM** provisioning wherever possible including IaaS, CaaS, PaaS environments and use metadata tagging to identify functional and network hierarchical information and context (Core, RAN, ORAN, etc.)
**Discover unknown devices deployed in the network** and provide those details to IPAM (IP Address Management) with Infoblox Discovery. Gleaning visibility and trending of all DNS/DHCP/IP activity on the network can be done with Infoblox’s Reporting & Analytics solutions.
**IPAM Redundant API** must be considered to maintain operations of the distributed MANO and CNFM/VNFM functions.

## Key Network Topology and System Architecture Considerations

The best practice recommends authoritative and caching DNS services be provided by dedicated/separate servers. Additionally separate authoritative DNS servers should be maintained for node selection for packet core and GRX/IPX Roaming. It is also recommended to separate the user plane that carries DNS queries from DNS management traffic using an out of band secure management network. Anycast deployment should be used to optimize DNS performance, improve service redundancy, and service availability which also simplifies horizontal DNS server scaling. It is recommended to position Gi DNS caching infrastructure as close to 4G/5G subscribers as geographically possible to improve the user experience and application performance. Basic service architecture paradigms to architect and implement local and regional redundancy for disaster recovery (DR) are always required and should not be neglected. It is essential to restrict user plane caching DNS services to 4G/5G subscribers only. This approach avoids DNS caching servers acting as an open resolver to the Internet which can be used in DNS amplification and DNS reflection attacks “weaponizing” infrastructure against internal and external targets.

Infoblox has identified capacity planning as one of the major challenges for service providers from a both a cost and design perspective. Infoblox FLEX model provides a unique approach which allows architects to first consider best placement of the service without the need to incur more software cost. FLEX uses a consumption based cost model so that architects can choose to deploy centrally with large VMs or distributed with small VMs using “Best Fit” for each deployment. Unlike legacy models, architects are not constrained with capacity planning for 5 year deployments, and customers can pay as you grow eliminating large up front cost for infrastructure. This model can also be used for monetized DNS services such as parental control, security policy or Safe Browsing Managed Services. (Hybrid cloud architectures are given special attention at the end of this document.)

## Key Risk Reduction and Security Automation

Securing DNS is critical to maintaining stability of the infrastructure and protect users and services. It is important that all DNS administrators should be trained/certified to the level required for their role. Defining granular administrator rights by implementing Role Based Access Control (RBAC) such that access rights are aligned with the tasks and roles to be executed is mandatory. Integration with AAA systems controlled by separate administrative information assurance teams is recommended for separation of duties shared privilege model. Auditing all configuration changes on a per user basis is recommended to limit the possibility of changes without an appropriate level of authority. Extra security consideration for devices communicating with the GRX/IPX infrastructure should be incorporated, deploying DDoS signature-based protection is highly recommended. Behavioral detection of DNS anomalies provides rapid detection of emerging threats and more advanced DNS attacks. Roaming interfaces should ALWAYS be treated as untrusted. Namespace separation should be done relative to the roaming authoritative zones and the internal 5GC zones of the service provider. While it is mandatory that the “3gppnetwork.org” domain be used for roaming, this is not a requirement for internal 5GC DNS. A private zone such as “<carriername>.com” should be used for internal name resolution for network node selection.

Infoblox integration with the security ecosystem leverages automated outbound API actions based on security events or system threshold alerts. Automated actions provide mitigation for various attack and malware traffic. Infoblox recommends integration with DNS logging and CEF event status with SIEM and TIP infrastructure to create automated work-flows for service tickets and event management. BloxOne Threat Defense suite of security products targets DNS as a first line of defense against malware and nefarious command and control domains. Through ecosystem data sharing of threat intel the DNS and threat intel feeds provide updated IOCs to improve security posture. Additionally, Infoblox “Threat Protect” can provide signature based detection of threats against the infrastructure, allowing DNS to respond even under volumetric and targeted attacks.
Infoblox Security Ecosystem Documentation: https://www.infoblox.com/products/cybersecurity-ecosystem/

## API Advantages for Automated DDI in MANO/CNF/VNF

**API for IPAM and DNS Automation:** API Redundancy must be considered to maintain operations of the distributed MANO and CNFM/VNFM functions. Programmatic network and IP Address allocation is critical for all automation tasks and DNS resource records for service advertisements. Infoblox API capabilities allow DevOps to take advantage of DNS service advertisement for new applications as workloads are created, such as MEC for both Application and Network Edge. Infoblox API allows creation of workflows for self service functions of the namespace and network or address allocation. This reduces workload on operations teams and prevents human error through built in error checking and prevention. Address allocation may be accomplished with DHCP or orchestration functions through the use of metadata tags to identify routable address space based on location, infrastructure tier and function. Through a well organized addressing schema, automation tasks become simpler through standardized naming conventions for easier programmatic call flows. Infoblox recommends a tiered hierarchy with functional and location based metadata tags and DNS naming conventions.
Example Tagging:
- Hierarchal: Core, Distro, Access, Edge
- Location: National, Regional, Locale, Site
- Functional: ORan, MSO, 5GC, Gn, Gx, Gi
- Cloud: Private, Public1 Public2

Infoblox API Documentation: https://www.infoblox.com/wp-content/uploads/infoblox-deployment-infoblox-rest-api.pdf

## Best Practice for DNS Architecture for Hybrid Clouds

Infoblox Grid provides integrated and automated management functions for deploying DNS, DHCP and IPAM (DDI) in hybrid cloud environments. Infoblox uses secure encrypted communication for management functions, all data replication, discovery and API functions. Deploying and extending the Infoblox Grid using public cloud provides additional benefits such as centralized management with redundancy and high availability across public and private cloud platforms.
Infoblox recommends the following best practices architecture for hybrid cloud deployments:

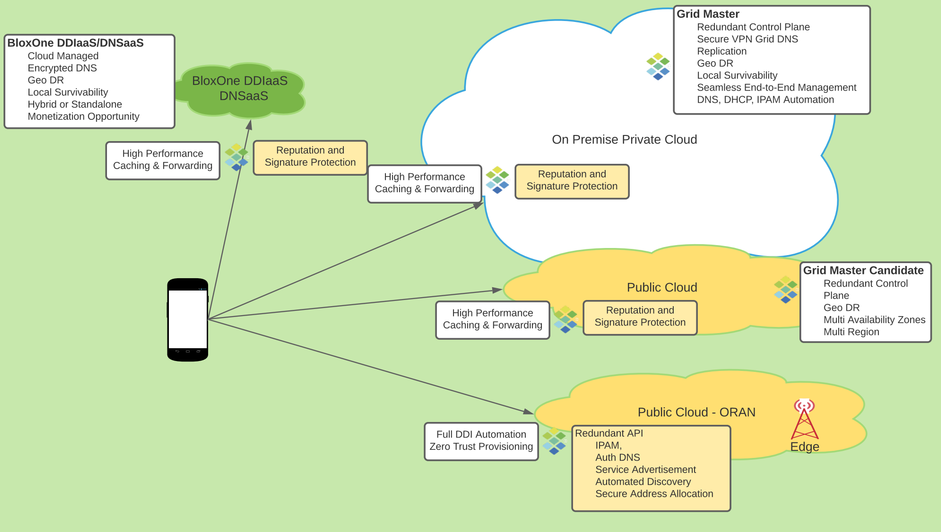
- Grid Master on-premises, centralized management for all grid members
- Grid Master Candidate deployed as on public cloud in shared service VPC for platform and geo-redundancy
- Primary DNS server on-premise, serving DNS for on-premise clients
- “Cloud Network Automation” by Infoblox provides visibility of public cloud resources for automated inventory and IPAM integration
- Secondary DNS server on public cloud in shared service VPC, serving DNS for public cloud Guest and Provider VMs
- Additional appliance deployed for DNS in separate region for fault tolerance/disaster recovery
- Grid members running on public cloud can be deployed in availability sets or multiple availability zones for maximum uptime
- Integrated reporting for automated visibility and reporting on all workloads

Use of multiple regions available from public cloud providers allows distribution of VMs and network services globally, providing fault tolerance for large-scale outages or disasters. Deploying DDI services, as well as Grid Master Candidates across these multiple regions provides maximum availability, including management functions and API. Deploying DNS servers in multiple regions and setting them up as name server groups allows the DNS service to continue uninterrupted during a regional outage. Instances deployed in a single Availability Zone might end up on a single hardware cluster. If that hardware cluster experiences an outage, this can result in a service impact on multiple DNS instances. Create your cloud virtual networks using IP address space that does not overlap with the address space you use on premise. This will allow for the simplest and most consistent IP address management schema.If you are unable to avoid overlapping address space, Infoblox IPAM can still be used to manage these spaces using “Network Views”. A hub and spoke design for cloud deployments allows critical services to be accessed from all networks where they are required. It can reduce costs by centralizing these core services into a “shared services” VPC. The hub and spoke design also facilitates control of traffic flow since all traffic is routed through the shared services/transit virtual network.

**API for IPAM and DNS Automation:** Redundant API must be considered to maintain operations of the distributed MANO and CNFM/VNFM functions, dynamic network and IP address allocation is critical for all automation tasks and DNS names for service advertisements. Address allocation can be accomplished with DHCP or orchestration functions through the use of metadata tags to identify routable address space based on location, infrastructure tier and function. Through a well organized addressing schema, automation tasks become simpler through standardized naming conventions for easier programmatic call flows. Infoblox recommends a tiered hierarchy with functional and location based metadata tags and DNS naming conventions.

Example Tagging:
- Hierarchical: Core, Distro, Access, Edge
- Location: National, Regional, Locale, Site
- Functional: ORan, MSO, EPC, 5GC, Gn, Gx, Gi
- Cloud: Private, Public1 Public2

**DDIaaS/DNSaaS:** Infoblox recommends the BloxOne platform for Application Edge, Managed Edge, Private 4G/5G deployments. The BloxOne Platform is cloud managed and provides full DDI functions complete with all the advantages of a public cloud deployment. The BloxOne solution provides local breakout functions and insures maximum service availability either standalone or in conjunction with other deployment models such as on premise or hybrid.




**For more details related to best practices discussed above you may reveiw the following documents.**
**Your Infoblox account team is available to support you and provide detailed design recommendations for any DDI use case large or small.**

**Infoblox Cloud Platform Integration Documentation:** https://www.infoblox.com/wp-content/uploads/infoblox-datasheet-infoblox-cloud-platform-appliances.pdf
**Infoblox Hybrid Cloud Deployment Documentation:** https://www.infoblox.com/products/multi-cloud-deployments/
**Infoblox Security Ecosystem Documentation:** https://www.infoblox.com/products/cybersecurity-ecosystem/
**Infoblox API Documentation:** https://www.infoblox.com/wp-content/uploads/infoblox-deployment-infoblox-rest-api.pdf