SOLUTION NOTE

SEAMLESS CONTROL AND SECURITY FOR HYBRID CLOUD DEPLOYMENTS WITH AMAZON ROUTE 53 AND INFOBLOX

SUMMARY

Amazon Route 53 DNS service offers limited support beyond pure Amazon Web Services (AWS) environments.

These limitations mean enterprises cannot create a single, unified DNS, DHCP and IP address management (DDI) solution to serve their entire enterprise, including their enterprise campus networks and hybrid clouds, with Route 53 alone. Route 53 focuses on only AWS virtual private clouds (VPCs), which limits connectivity, visibility and security when used for non-AWS cloud platforms.

Infoblox integrates its industry-leading DDI platform with AWS and Amazon Route 53 DNS, providing a unified, commercial-, enterprise- and service-provider-grade solution for AWS and hybrid cloud deployments. Infoblox integration with Amazon Route 53 bridges the gap between enterprise IT and cloud teams. It reduces complexity and helps achieve optimal security by providing a single control plane to manage on-premises, private cloud and AWS public cloud deployments, while enhancing security for those deployments. This solution meets the needs of current and future Infoblox customers who are expanding to AWS and are using Amazon Route 53 for DNS.

LACK OF VISIBILITY, AUTOMATION AND CONSISTENCY CAN PLAGUE AMAZON ROUTE 53 DEPLOYMENTS

Amazon Route 53 offers private DNS functionality within AWS VPCs. However, an enterprise using a hybrid cloud faces operational challenges even while using Amazon Route 53 including:

- **Limited DNS:** DNS resolution or responses to queries are isolated within their AWS network, which causes issues when communication is needed outside a particular AWS Private Hosted Zone. To circumvent this problem, IT teams often spin up multiple BIND servers to pass DNS traffic outside the isolated AWS zones. This approach adds complexity and lacks consistency across disparate DNS deployments.
- **No IPAM:** AWS has no IP address management (IPAM) solution and often has limited visibility of virtual instances, which negatively impacts day-to-day management and adds time for auditing and compliance purposes.

BUILDING A UNIFIED DNS AND IPAM SOLUTION WITH AMAZON ROUTE 53

Infoblox DDI for AWS integrates with the Amazon Route 53 DNS service providing a centralized console across AWS and hybrid cloud deployments for visibility, consistent management and security. Without being restricted to Amazon Route 53 Private Hosted Zones, the Infoblox and Amazon Route 53 solution enables reliable hybrid cloud deployments that extend beyond just AWS.

- **Lack of hybrid cloud visibility:** Without a consistent DNS and IPAM solution across the hybrid cloud, enterprise IT must use several tools to access DNS and IP address data. This lack of visibility leads to longer troubleshooting times, reduces the ability to perform network planning, and increases security risks. It also increases inconsistencies in enterprise-wide management of the DNS and IP address space.
- **Limited DNS security:** Route 53 provides limited DNS security and advanced threat detection capability for AWS and hybrid cloud deployments. Data exfiltration using DNS tunneling and malware using DNS are common threats that can cripple IT networks.

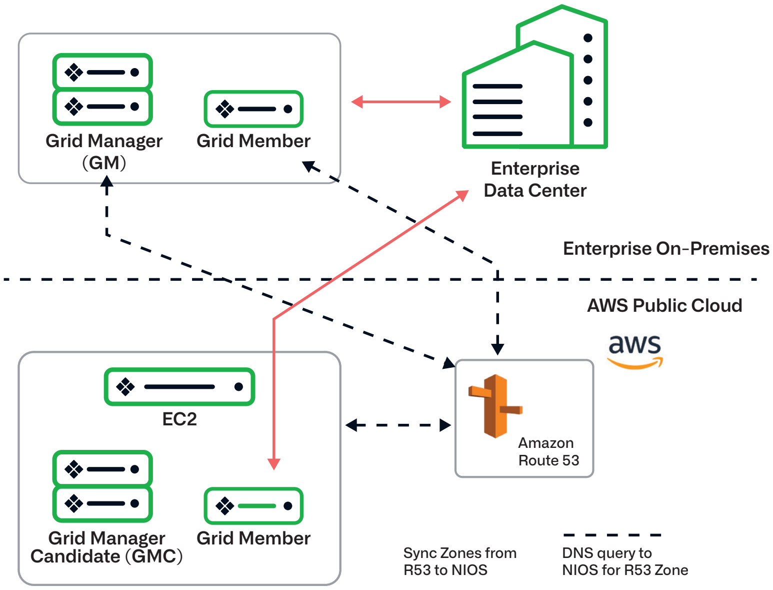


Figure 1: Unified management across a hybrid cloud

Enhance Contextual Visibility across AWS and Hybrid Deployments

Contextual network visibility is critical in today's hybrid multi-cloud environments. Since Route 53 focuses exclusively on AWS virtual resources, visibility is limited only to those public cloud instances. The Infoblox and AWS solution provides automated discovery, enhanced visibility and tracking of VPCs and EC2 instances in a single platform, making it easy to bring public cloud assets under common DNS and IP address management. Infoblox simplifies creating and cleaning up records after instances are destroyed. It detects and includes or excludes network resources using Selective Classless Inter-Domain Routing (CIDR or private IP) vDiscovery to ensure efficient distribution of IP addresses in AWS.

For teams needing to manage and sync multiple accounts in Amazon Route 53, Infoblox saves significant time and AWS usage fees by eliminating vNIOS member deployments in each account and synchronizing all Route 53 hosted zones to the Grid. vDiscovery reduces multiple discovery tasks into a single discovery job across multiple AWS regions and accounts. It also retains account filters to enable region selection and migration of existing vDiscovery jobs without data loss for greater user experience, workload efficiency and admin control.

For federal and other government customers, Infoblox enables further visibility and control by providing Route 53 sync support and vDiscovery for multiple AWS GovCloud regions and accounts. This capability delivers highly available and scalable DNS and connects user requests to AWS Internet applications and customized routing policies for reduced latency.

IT teams can greatly minimize the time needed to audit DNS and IP address information with a consistent view of AWS and non- AWS parameters within a single control plane for compliance, operational and executive reporting.

High Availability, Uptime and Resilience

NIOS allows customers running cloud platform (CP) appliances to configure two NIOS appliances for High Availability (HA) and uptime. HA measures how reliably users can access the system, and whether the system is impacted by planned maintenance or unscheduled downtime. Uptime measures the time a system is operational. With HA, admins can achieve both, and avoid single points of failure in Azure and other public cloud environments, especially for mission-critical applications and workloads.

Stronger DNS Security and Control

In recent years, Distributed Denial of Service (DDoS) attacks on the internet services provider Dyn and other organizations have proven the need for protection against DNS-based threats to minimize costly business disruptions, lost revenue and brand reputation. NIOS adds virtual Advanced DNS Protection (vADP) for AWS public cloud to detect and mitigate the widest range of DNS attacks including volumetric, NXDOMAIN, DNS hijacking and other exploits. With vADP, administrators can quickly detect attacks, maintain DNS integrity, enhance uptime and extend external DNS protection from local on-premises to public cloud environments.

To further harden system security, Infoblox enables vNIOS synchronization with Amazon Route 53 multi-account subset lists to increase security posture and improve control. Administrators can extend Route 53 discovery and sync from a single NIOS instance to a list of multiple accounts in AWS. Administrators can choose between 1) NIOS providing automatic account discovery, or 2) specifying a list of accounts to be discovered and synchronized from Route 53 environments. This capability strengthens security by 1) preventing child accounts from accessing the root; 2) blocking delegate administrator access; 3) inhibiting discovery of all Organizational Unit (OU) accounts; and 4) using Assume-Role permission access. These DNS security provisions fortify critical network services against attack and keep applications available and performing so organization can focus on serving customers and running their business.

Maintain Consistent DDI Platform for Hybrid Cloud

Many organizations deploy a hybrid environment combining on-premises, virtual private, hybrid- and public, multi-cloud infrastructures including AWS. Instead of manual, out-of-date spreadsheets or the complexity of disparate solutions, Infoblox reduces the need to spin up general-purpose DNS servers and enables on-premises to AWS communications, integrating DNS records across multiple platforms within a single control plane to improve consistency and manageability.

Infoblox also supports EC2 R6 instance types, thereby improving performance while lowering the total cost of ownership. Infoblox allows a direct connection to AWS Nitro Systems and the EC2 Serial Console for faster troubleshooting, with better user experience and control. vNIOS further enhances cloud security and control by allowing Elastic Block Store (EBS) encryption for data at rest, data in transit and all volume backups.

Flexible Deployment Options

Infoblox DDI for AWS is tightly integrated with industry-leading on-premises virtual and physical appliances. The comprehensive DDI platform can support AWS public cloud, private cloud environments (e.g., including VMware, OpenStack, Microsoft and others) and traditional networks—or any combination in a hybrid deployment. The unified solution ensures maximum flexibility, scalability and service availability.

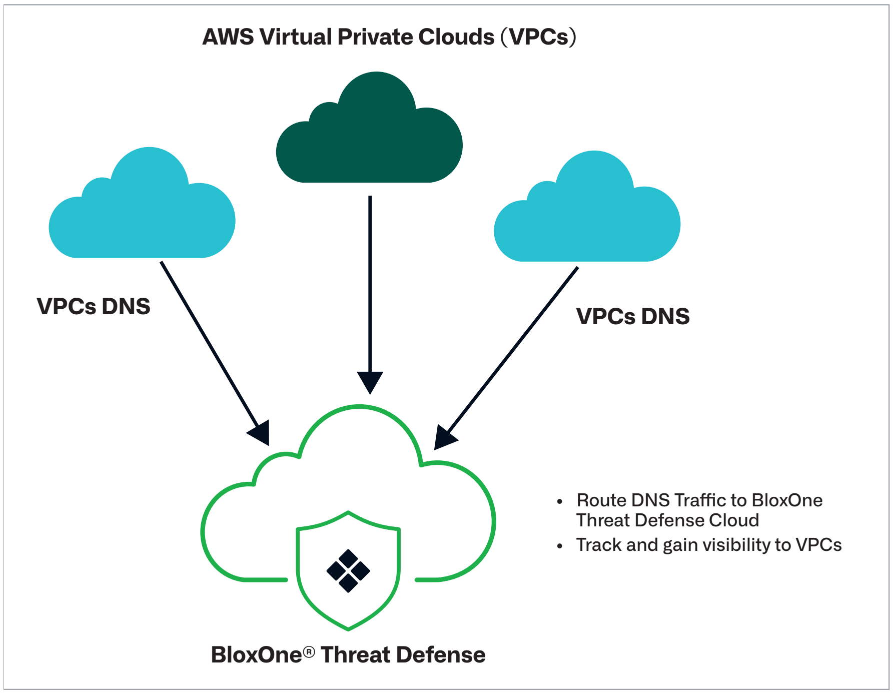
Infoblox offers a full range of deployment options through secure, purpose-built physical and software appliances for small remote and branch offices, medium-sized organizations and large enterprises and services providers with data centers and distributed sites. The Trinzic X6 physical and software appliance platform offers up to 50% better DNS and DHCP performance over prior models. It also includes cost-saving licenses for Cloud Platform API automation, DNS Firewall and DNS Traffic Control global server load balancing. No matter what your organization needs, Infoblox provides the commercial-, enterprise- and service-provider-grade solutions that deliver a consistent, critical network experience with the reliability and flexibility to scale your environment as your business needs require.

Infoblox enables cloud migration by allowing administrators to deploy Network Insight discovery and Reporting and Analytics appliances in AWS public clouds. Network Insight provides integrated Layer-2 and Layer-3 discovery, IPAM sync with devices, end hosts and network ports, switch port management and lifecycle and compliance notification. In addition, the Infoblox Reporting and Analytics solution, built on Splunk, the market- leader in data search, delivers monitoring, visualization and SIEM capabilities. Placing solution-optimizing appliances in AWS supports cloud-first initiatives, simplifies the migration of physical data centers to the cloud, reduces physical data center resources and delivers single- and multi-site visibility into DDI metadata for historic audit/compliance, real time alerting, network performance and capacity planning. As a result, organizations gain complete on-demand visibility, simplify compliance reporting and enable detailed audits of DNS and IP address information for AWS resources across networks and geographic regions.

Extend DNS Layer Security and Threat Detection to AWS

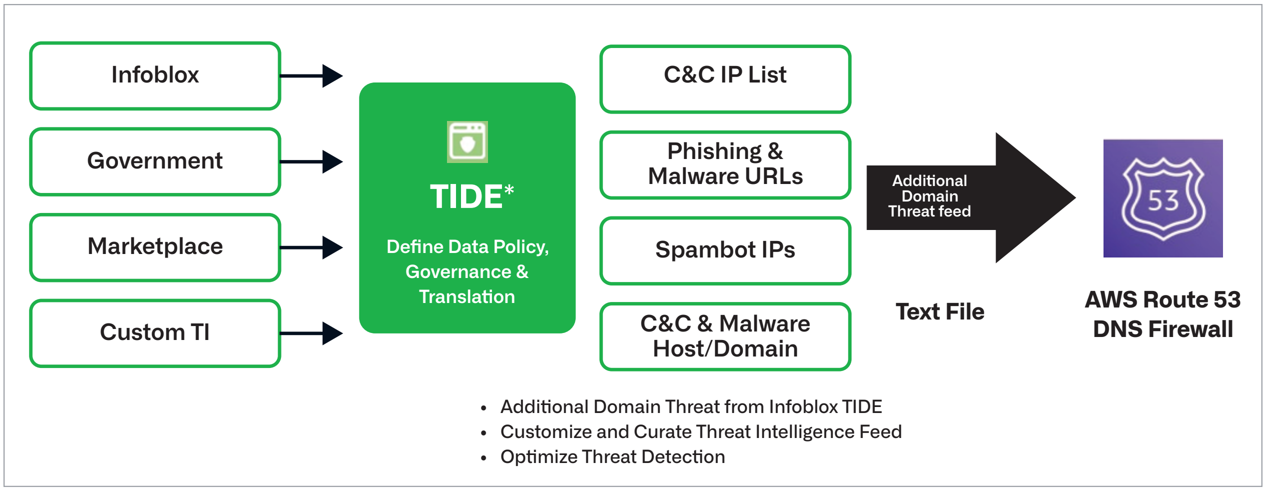
Users can also leverage Infoblox DNS Security, IPAM (IP Address Management) and curated threat intelligence to obtain visibility into AWS VPCs and optimize threat detection for Amazon Route 53 DNS firewall. Implementing Infoblox's BloxOne® Threat Defense as part of a comprehensive strategy significantly reduces the risk of advanced attacks and exploits, and DNS data exfiltration.

Through extensive ecosystem integrations, users can automate response to events detected and use network context to prioritize response. Users can effectively manage and minimize threats in AWS VPCs by routing VPC DNS traffic to BloxOne Threat Defense Cloud, tracking and gaining visibility into cloud instances, and decreasing risk from cyberthreats.



- Route DNS Traffic to BloxOne Threat Defense Cloud
- Track and gain visibility to VPCs

In addition, organizations can leverage Infoblox TIDE (Threat Intel Data Exchange platform) to push indicators of compromise (IOCs) to both Infoblox AWS DNS appliance and the Amazon Route 53 DNS firewall, providing consistent security for all environments and driving accuracy with their choice of threat intel feeds based on their specific need. The access to dozens of additional threat feeds from Infoblox TIDE complements those provided by Route 53 DNS Firewall. The ability to detect and block current threats using a customized "super-feed" uplifts the security stack to improve defense, investigation and response capabilities.



Infoblox

Government

Marketplace

Custom TI

TIDE*

Define Data Policy, Governance & Translation

C&C IP List

Phishing & Malware URLs

Spambot IPs

C&C & Malware Host/Domain

Additional Domain Threat feed

Text File

AWS Route 53 DNS Firewall

- Additional Domain Threat from Infoblox TIDE
- Customize and Curate Threat Intelligence Feed
- Optimize Threat Detection

CONCLUSION

Amazon Route 53’s isolated focus on AWS has management and core network services gaps when managing on-premises and hybrid, multi-cloud infrastructure—including a lack of visibility, inconsistency and security across platforms. Infoblox DDI for AWS eliminates those gaps by leveraging the industry-leading DDI platform and reducing complexity with a single console to manage on-premises, AWS public cloud and critical DNS components. BloxOne Threat Defense provides foundational DNS security to protect hybrid environments with threat detection, response and ecosystem integrations to optimize security performance.

CONTACT US

For more information or to get answers on Infoblox DNS and IPAM and other network services for Amazon Web Services (AWS), connect with your Infoblox account team, see our critical-network integrations or contact us at Infoblox.com.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

© 2024 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20240529v2