Enterprise Networking with Integrated DNS Security and IP Address Management Across Cloud and Multi-Cloud Environments

Executive Summary

Infoblox has partnered with Alkira to offer customers critical networking and security services across the on-premises and cloud environments. Infoblox provides centralized, secure DNS (Domain Name System), IPAM (IP address management), NTP (Network Time Protocol), DHCP (Dynamic Host Configuration Protocol) and DNS security services. The deployment has now been dramatically simplified thanks to integration with Alkira Network Infrastructure-as-a-Service solution.

Challenge

The drive towards digital transformation has taken many organizations in the direction of greater network and IT complexity due to increasingly distributed set of application environments and mobile workforce. As part of transformational efforts, these organizations are moving applications and workloads from the on-premises data centers to single or multiple cloud platforms. One consequence of this upheaval has been increased complexity in DNS, DHCP and IP address management while ensuring consistent and centralized operation of these critical networking services.

Migration to cloud and the increasingly distributed nature of environments also lead to security challenges. Integrated solutions are needed that replace this complexity and vulnerability with simplicity and security.

Infoblox and Alkira Joint Solution

The partnership between Infoblox and Alkira means that organizations can now easily deploy Infoblox inside Alkira Network Infrastructure-as-a-Service and use it to manage DNS, DHCP, IPAM (DDI) and DNS security in hybrid cloud, single cloud and multi-cloud environments. Many organizations are already familiar with the benefits of Infoblox in their on-premises networks. Now they can extend Infoblox instances over various cloud environments using geographically distributed Alkira Cloud Exchange Points (CXPs) for a truly uniform end-to-end networking and security solution.

Infoblox's NIOS DDI runs on patented Grid technology that provides a unified platform for core network services.

- Reliable core network services (DNS, DHCP and IPAM) for connecting all devices, applications, and digital resources across the business
- Simplified management of core network services managed from a common console
- Rich, integrated reporting and analytics capabilities for capacity planning, asset management and control
- DNS-based security to protect against data exfiltration, ransomware, phishing and more

To deploy Infoblox in a single cloud environment, enterprise IT teams often struggle to overcome cloud skills gaps while at the same time working around networking limitations imposed by the rudimentary capabilities of the cloud service providers.

To deploy Infoblox in a multi-cloud environment, separate instances need to be manually deployed and configured for each cloud. Various cloud service providers have different constructs, such as routing tables, subnets, Internet gateways, UDRs and peering, which work in different ways. Managing and operating these disparate constructs becomes increasingly complex and time-consuming task.

Alkira simplifies deployment and integration of Infoblox DDI and DNS security services into the enterprise network running on Alkira Network Infrastructure-as-a-Service solution. Customers can deploy multiple instances of Infoblox virtual appliances into the Alkira Cloud Exchange Points (CXPs) running in AWS, Azure and Google Cloud regions, assign them different roles, and implement cloud or multi-cloud networking design with high availability and high performance using the Anycast capability of Infoblox.

Administrators can choose to join new Infoblox appliances running in Alkira to an existing cluster or create a new cluster. In both cases Infoblox Grid Manager is responsible for controlling the configuration of instances, while Alkira Portal UI is used for their automated deployment in minutes. If a new cluster is created, the Grid Manager can run in Alkira CXP.

Following are key use cases for a joint Infoblox and Alkira solution:

Use Case 1:

DNS-based security and DDoS Protection for the network

More than 90% of malware uses DNS to execute its campaign. In addition, DNS is often used as a pathway for data exfiltration.
Infoblox Threat Defense™, running on Infoblox NIOS appliances, provides DNS-layer security to protect on-premises and cloud environments using threat intelligence and analytics on DNS servers. This helps detect threats early in the lifecycle before it spreads. In addition, DNS, DHCP and IPAM data provides visibility, and critical device and user attribution to speed up incident response. Integrating Infoblox NIOS appliances into the Alkira Cloud Exchange Points (CXPs) allows organizations to apply security controls at the point of network connectivity, closest to the source, thus dramatically reducing overall security exposure.

Use Case 2:

Disaster recovery across multiple cloud regions and multiple clouds

Often organizations leverage multiple cloud regions or multiple clouds to provide higher availability and better quality of experience for user-to-application communication. Infoblox DNS is a key element of such communication. In the event of outage affecting a specific cloud or specific cloud region, Alkira's distributed network infrastructure maintains uninterrupted connectivity for the user-to-application communication. At the same time Alkira's support for Infoblox Anycast DNS, ensures continuous name resolution throughout the outage averting disastrous consequences.

Benefits

Joint Solution Components

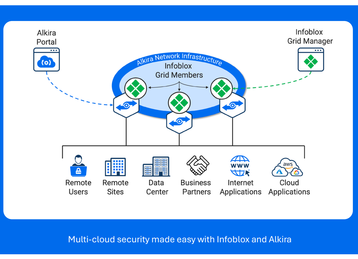
- ✓ Alkira Network Infrastructure-as-a-Service
- ✓ Alkira Cloud Exchange Points (CXPs)
- ✓ Infoblox NIOS DDI
- ✓ Infoblox Threat Defense Business On-premises (running on NIOS appliances)
- ✓ Advanced DNS Protection

Solution Benefits

- ✓ Uniform and simplified deployment of DDI services across cloud and multi-cloud environments
- ✓ Strong DNS-level cloud security
- ✓ Consolidated DNS, DHCP and IPAM management
- ✓ Global scale
- ✓ Unprecedented agility
- ✓ High availability and resiliency

An organization's DNS is essential for mission-critical network connectivity. In the event of a DDoS attack that affects DNS services, losses can be huge. Infoblox Advanced DNS Protection (ADP) offers protection against the widest range of DNS DDoS attacks, maintaining uptime for an organization.

The combination of Infoblox Threat Defense on-premises appliance and Infoblox NIOS virtual appliance integrated into the Alkira Cloud Exchange Points (CXPs) offer an end-to-end solution for securing communication across hybrid cloud, single cloud and multi-cloud environments.



Multi-cloud security made easy with Infoblox and Alkira

About Alkira

Alkira is the leader in Network Infrastructure-as-a-Service. Our solution offers enterprise-grade network capabilities, eliminates network complexity, accelerates cloud and AI initiatives, and reduces overall costs. It allows organizations to design and deploy networks connecting and securing users, sites, and clouds within minutes. Alkira's solution is trusted by Fortune 500 enterprises and leading system integrators.

Learn more at alkira.com

About Infoblox

Infoblox unites networking, security and cloud to form a platform for operations that's as resilient as it is agile. Trusted by 13,000+ customers, including 92 of the Fortune 100, we seamlessly integrate, secure and automate critical network services so businesses can move fast without compromise.

Learn more at https://www.infoblox.com