

WHITEPAPER

BEST PRACTICES ARCHITECTURE FOR INFOBLOX UNIVERSAL DDI™

A PRACTICAL LOOK AT DEPLOYING DHCP, DNS
AND DNS FILTERING IN DISTRIBUTED, HYBRID
AND MULTI-CLOUD ENVIRONMENTS

By Infoblox's Technical Marketing Team



TABLE OF CONTENT

ABSTRACT	3
THE COMPANY	3
BENEFITS OF CLOUD-FIRST ARCHITECTURES.....	4
SERVICE AND SERVER GLOSSARY.....	4
Management Plane	4
DNS	6
External Authoritative DNS	6
Internal DNS.....	7
<i>DNS Traffic Control</i>	8
Forwarding.....	8
Recursive DNS	8
DNS as a Cyberattack Vector	9
Content Filters.....	9
DHCP	9
DDNS	10
Authoritative IPAM	10
IPAM Realms.....	11
Asset Insights.....	11
<i>Why Is Asset Discovery Important?</i>	11
NIOS.....	12
NIOS-X.....	12
NIOS-X as a Service	13
Third-Party Integrations	14
Automation.....	15
ARCHITECTURE.....	15
Headquarters.....	15
Cloud	17
Branch Locations.....	17
Small-Footprint Locations (Storefronts).....	17

ABSTRACT

This reference architecture focuses on the conceptual best practices for the delivery of the critical network services Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) and IP address management (IPAM) in distributed environments, such as hybrid, cloud or multi-cloud. This document focuses on Infoblox's software-as-a-service (SaaS) offerings, or Infoblox Universal DDI (DNS, DHCP and IPAM), which is specialized for lightweight, scalable and flexible deployments. Concepts covered in this document include:

- Managing highly distributed environments across multiple clouds and locations
- Deciding which delivery method(s) of protocol services best suits your environment (NIOS, NIOS-X, NIOS-X-as-a-Service)
- Leveraging DNS to improve security in distributed environments
- Integrating existing tools with Infoblox to improve efficiency and cost savings in distributed environments
- Improving security, taking inventory of assets and maintaining good on-premises and cloud hygiene with Infoblox Asset Insights™
- Utilizing automation to improve workflows and speed up the provisioning of new DDI objects required in day-to-day operations

To better present these concepts, a case study will be covered in this document. The fictional company ACME-Mart, a large, global retailer, will be implementing its DDI architecture to help satisfy its requirements for its highly distributed, multi-cloud environment utilizing industry best practices for DDI. ACME-Mart will also be integrating its existing security information and event management (SIEM), IT service management (ITSM) and other network and security tools to improve the return on investment (ROI) and time to value (TTV) of Infoblox and their integrated network and security tools.

While reading this paper, readers are encouraged to use ACME-Mart's architecture as a benchmark and reference for evaluating improvements to their own DDI strategy. Are there potential improvements that could be made to your own organization's DDI infrastructure's resiliency, performance, security, ease of deployment and disaster recovery?

An additional white paper covering an alternative deployment method and architecture which includes Network Identity Operating System (NIOS) has been published on our website, titled [Infoblox® Reference Architecture and Best Practices for NIOS DDI](#).

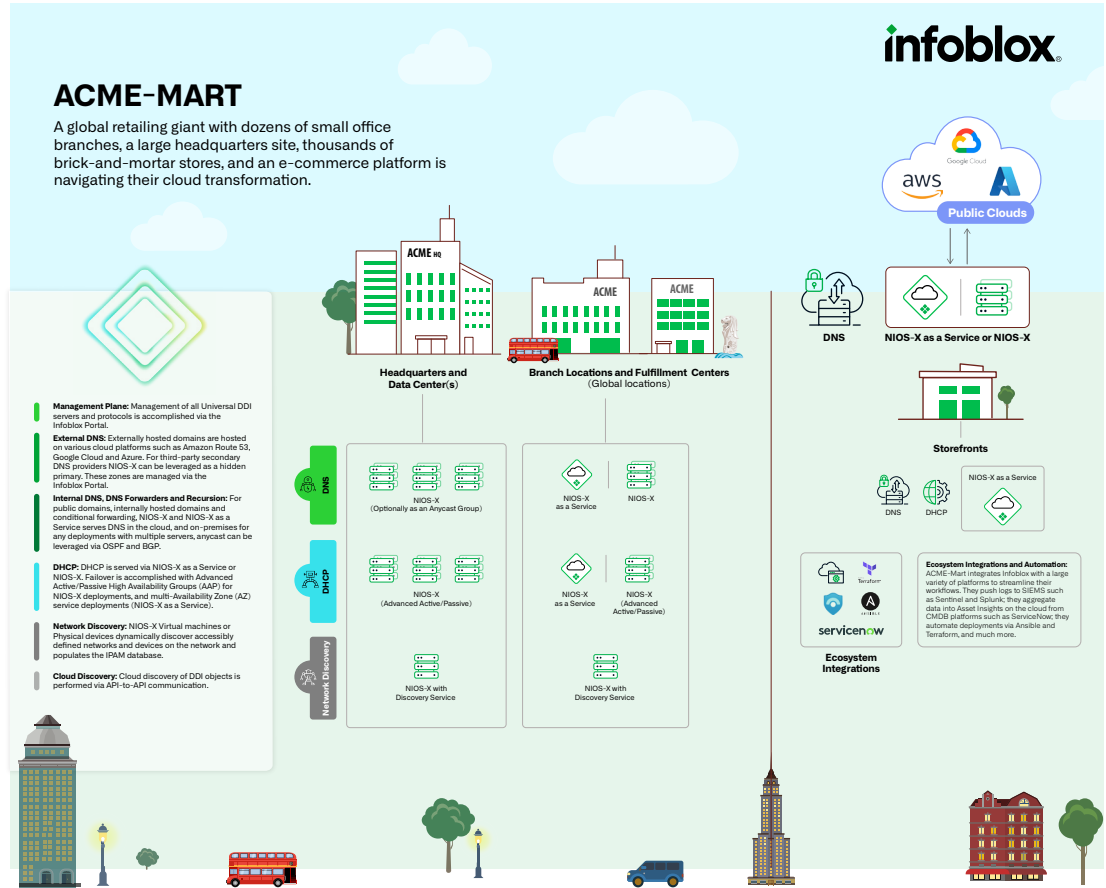
THE COMPANY

ACME-Mart is a global retail giant, serving millions of customers daily across diverse regions. A household name, ACME-Mart offers a wide variety of consumer goods, from groceries and household essentials to electronics and apparel. With a strong emphasis on convenience and affordability, ACME-Mart thrives on its extensive network of stores, an e-commerce platform and distribution centers, ensuring seamless accessibility for customers worldwide.

In response to rapid technological advancements and the increasing demands of a cloud-first market, ACME-Mart has embarked on an ambitious initiative to modernize its network infrastructure. The company recognizes that its existing traditional data center model is no longer sufficient to support the agility, scalability and resilience required for a fast-paced retail environment. As a result, ACME-Mart has committed to a cloud-first approach, leveraging a multi-cloud architecture to enhance efficiency and streamline operations.

With dozens of small office branches, a large headquarters and thousands of brick-and-mortar locations, ACME-Mart's network is vast and complex. Every store, office and corporate hub depends on reliable critical network services, such as DNS and DHCP, to maintain seamless connectivity. Transitioning to a cloud-first model will allow ACME-Mart to optimize its network performance, bolster security and improve flexibility, ultimately enabling enhanced customer experience and business operations.

Through this transformation, ACME-Mart aims to create a more robust, scalable and distributed environment that supports its global expansion and innovation initiatives. By moving away from traditional data centers, the company will reduce infrastructure costs, improve disaster recovery capabilities and take full advantage of modern cloud technologies to stay ahead in the competitive retail landscape.



BENEFITS OF CLOUD-FIRST ARCHITECTURES

A cloud-first approach offers significant advantages by ensuring scalability, allowing businesses to easily adjust resources based on demand without the limitations of physical infrastructure. It provides unmatched flexibility, enabling organizations to quickly deploy, update and adapt applications to evolving needs. The lightweight nature of cloud solutions reduces dependency on bulky hardware, cutting costs and improving efficiency. By breaking down traditional data silos, cloud technologies foster seamless collaboration, ensuring that teams can share information effortlessly across departments. Ultimately, embracing a cloud-first strategy enhances agility, fosters innovation and supports a more streamlined, responsive operational model.

SERVICE AND SERVER GLOSSARY

MANAGEMENT PLANE

The Universal DDI product has a variety of useful capabilities, including the unique capability to act as a management plane for multiple DDI platforms, including its own native NIOS-X and NIOS-X as a Service servers. Via secure APIs, the Infoblox Portal integrates with a variety of platforms, such as:

- NIOS (Infoblox)
- Microsoft DNS and DHCP Servers
- Amazon Route 53
- Azure DNS
- Google Cloud DNS
- CrowdStrike
- ServiceNow

This list is not all encompassing as more platforms are being added at a regular cadence.

The Infoblox Portal is the one-stop shop for managing Infoblox DDI, Infoblox Threat Defense™ and all other integrated DDI platforms. The portal is hosted in the cloud and, therefore, has all the benefits of cloud-based applications. Management of the platform thus has the shared security model that is maintained by cloud providers. The hosting cloud protects the physical infrastructure and the user administers access to the objects hosted in the cloud. The portal contains useful role-based access controls (RBACs).

While this document does not fully cover the nuances of RBAC in the Infoblox Portal, users can be assigned to a variety of roles that contain permissions to create, read, update or delete objects and access views. Access views are an extension of RBAC, which allows for even further granular control over the Infoblox Platform's permissions. With access views, users may be assigned to specific DDI objects, where they can create, read, update or delete objects based on their permissions; access views allow for self-service of DDI objects that they may be assigned to, or to improve visibility. See Figure 2 for an example diagram of access view usage.

ACME-Mart looks to manage their entire diverse DNS, DHCP and IPAM portfolio with the Infoblox Portal.

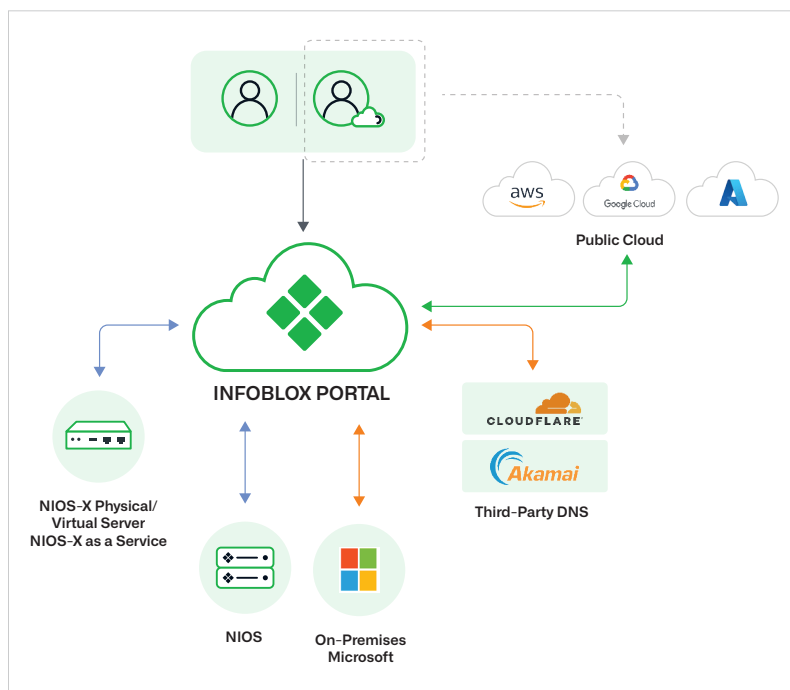


Figure 1. The Infoblox Portal allows for the integration and management of diverse DDI platforms in a consistent workspace

ACME-Mart's DDI team also grants Infoblox Portal access to other teams via access views so they can manage specific DNS zones and specific IPAM objects as needed by their daily processes.

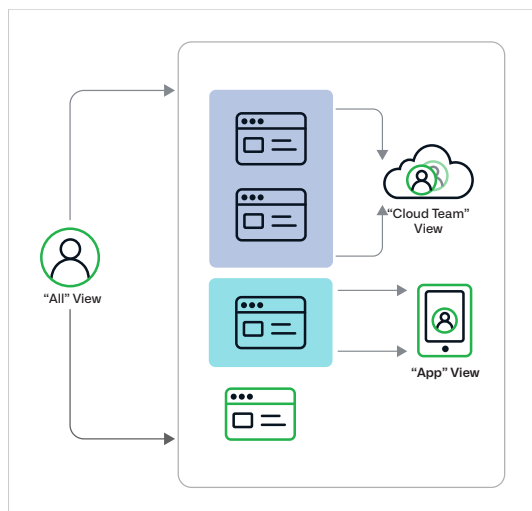


Figure 2. The Infoblox Portal contains access views, which allow specific users to create, read, update or delete specific objects. In the diagram, users assigned to the “All” view have full access to all licensed features and can perform operations on all objects in the tenant. The “All” view user is similar to a global administrator, which is common in various software platforms. The “Cloud Team” view and “App” view users only have the ability to read or interact with objects in their access views.

By using the Infoblox Portal as their primary DDI management plane, ACME-Mart simplifies their workflows, breaks down cross-team silos and reduces both the training and expertise required to administer each unique platform.

DNS

DNS is a hierarchical naming system built on a distributed database of internet- or private network-connected resources. DNS can be seen as the foundation of the internet, providing the ability to resolve human-readable domain names to numerical identifiers known as IP addresses, which in turn allows clients to communicate to specific resources. A crucially important network service, DNS enables virtually all internet communication. Without DNS, clients would need to input the IP address of each individual server they wanted to reach when navigating the internet. In almost all situations, navigation on the internet simply does not work without DNS. Due to the criticality of this protocol, reliable, secure and consistent DNS is imperative for modern business processes.

DNS servers can be configured to authoritatively host private or public zones, conditionally forward to other DNS servers for domains that they are authoritative for, recursively resolve domains or some combination of roles. With that said, it presents security risks to have an internet-accessible DNS server that provides both authoritative and recursive services, so that is generally avoided. However, for DNS servers that are only accessible internally, it is common to combine both authoritative and recursive roles.

External Authoritative DNS

External authoritative DNS servers (often called simply external DNS) support the ability for the public to resolve domain names. This resolution is critical for organizations in order to send emails to their email addresses, reach their web servers or access any other services they make available to the internet. The Infoblox Portal has the ability to manage a variety of platforms that host external DNS zones, including cloud-native DNS services (e.g., Route 53), DNS services hosted by content delivery network (CDN) providers, including Cloudflare and Akamai, and Infoblox’s NIOS. Depending on the use case, a combination of external DNS providers may be used.

One option for hosting external authoritative DNS service is Infoblox NIOS. When leveraging NIOS to provide external authoritative DNS services, Infoblox recommends a hidden primary in a Virtual Router Redundancy Protocol (VRRP) high availability (HA) pair, which provides zone data

to any number of secondaries, including NIOS appliances running Advanced DNS Protection (ADP). It is important to note that for any Domain Name System Security Extensions (DNSSEC)-signed zones, the Grid Manager must be the primary. Secondaries to the NIOS primary may also include third-party DNS providers. When deploying NIOS instances, companies should consider the appropriate sizing for their NIOS servers, based on the volume of queries they are expecting and the amount of DNS data the appliances will host. Anycast may also be leveraged to position multiple DNS servers behind a single IP address, which improves the resiliency and availability of the DNS protocol.

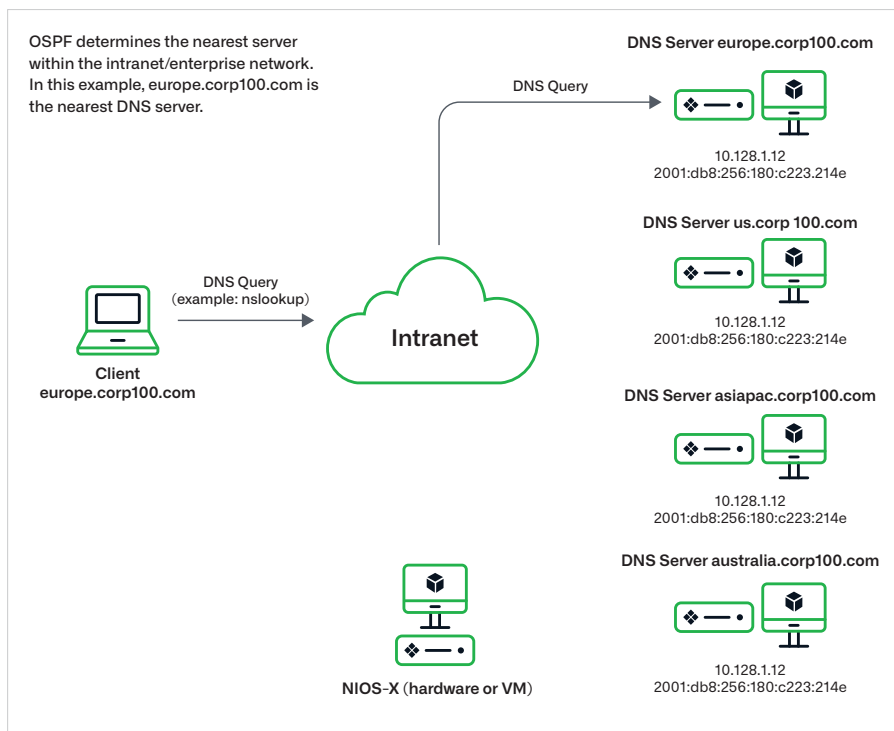


Figure 3. An example of DNS servers in an anycast configuration. Each DNS server in the anycast group leverages the same IP. When a client attempts to resolve a domain, they will resolve the query via the nearest DNS server, or, if that DNS server is experiencing a service outage, they will receive the next closest server.

Due to the risk of publicly hosting DNS zones, companies must maintain proper protection for the DNS infrastructure against attacks such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. The NIOS platform supports ADP, which can help mitigate these types of attacks.

ACME-Mart manages their external DNS zones via the Infoblox Portal and hosts the zones on a variety of platforms, including Akamai, Cloudflare and cloud providers, such as AWS, Azure and Google Cloud.

Internal DNS

Internal DNS is for resolution of domain names that are not publicly reachable. In the cloud, internal domains may be associated with a virtual private cloud (VPC) or virtual network (VNet). Cloud workloads often leverage internal DNS to do a variety of integral tasks, such as accessing a cloud database or another cloud-hosted server to accomplish a workflow. On-premises DNS servers host internal domains that allow for business processes to run without a hitch; this could be users accessing their email or an internal company website.

Infoblox provides the ability to authoritatively serve internal domains in a variety of ways: NIOS, NIOS-X or NIOS-X as a Service. In addition to serving internal domains, Infoblox can also manage internal domains hosted on integrated platforms via the Infoblox Portal.

ACME-Mart manages all of their internal DNS records via the Infoblox Portal. To serve DNS records, they host internal domains via a variety of servers depending on the case. For specifics on which type of DNS server fits each type of use case view the sections under [Architecture](#).

DNS Traffic Control

For NIOS, NIOS-X and NIOS-X as a Service DNS servers, Infoblox has a tool known as DNS Traffic Control (DTC) which provides a variety of ways to manage how traffic is routed via intelligent DNS responses. DTC provides the right answer to the right client at the right time. For example, when clients from different subnets need to resolve the same domain name, a DTC Topology policy can be used to route clients to the nearest available instance of an application or service to minimize latency. DTC also includes the ability to perform health checks against resource targets and take that information into account when choosing the best answer for a client. This allows for automated failover from unavailable resources to ones that are healthy. In addition to Topology policies, Ratio, Round Robin and Global Availability (i.e., ordered list) load balancing methods are also available to optimize application uptime and performance.

Forwarding

Forwarding is the process of one DNS server sending a recursive query to another DNS server for resolution. There are two different ways to forward DNS queries, forwarding only for specific zones (commonly known as conditional forwarding) and default forwarding, which sends all queries that cannot be resolved on the server to another set of servers. A common architectural practice is to have DNS servers located in a demilitarized zone (DMZ) that receives all internet-bound queries from the internal DNS servers. DNS servers performing that function on-premises are generally known as local forwarders or caching forwarders. Forwarding name servers cache DNS data, which in turn reduces the amount of traffic and improves DNS query response times.

In situations where cloud-hosted clients need to resolve internal domains hosted on-premises or in another cloud, or if an on-premises client needs to resolve a domain hosted in the cloud, conditional forwarding can be leveraged to enable this communication. Conditional forwarders have a variety of names depending on the cloud provider (for example, in AWS they are called inbound and outbound endpoints). Universal DDI offers the ability to manage these conditional forwarders and their rules.

ACME-Mart leverages Universal DDI to manage their conditional forwarders. Conditional forwarding is possible via forwarding rules on NIOS, NIOS-X and NIOS-X as a Service protocol servers for clients resolving domains that are hosted in public clouds, or for cloud-to-cloud communication (i.e., AWS to Azure).

Recursive DNS

Recursive DNS is required whenever a client (also known as a stub resolver) queries a DNS server to resolve a domain name that the DNS server cannot resolve from its local cache or DNS data that it's authoritative for. Infoblox NIOS-X, NIOS-X as a Service and NIOS all have the ability to recursively resolve domain names by either sending a query to a root server, a public resolver or to Infoblox Threat Defense, which recursively resolves domain names and also acts as a DNS firewall by means of user-defined policies; more about this in the section titled [DNS as a Cyberattack Vector](#).

ACME-Mart leverages NIOS, NIOS-X and NIOS-X as a Service in conjunction with Infoblox Threat Defense to both block malicious domains and recursively resolve DNS queries for domains not hosted internally or externally, by ACME-Mart.

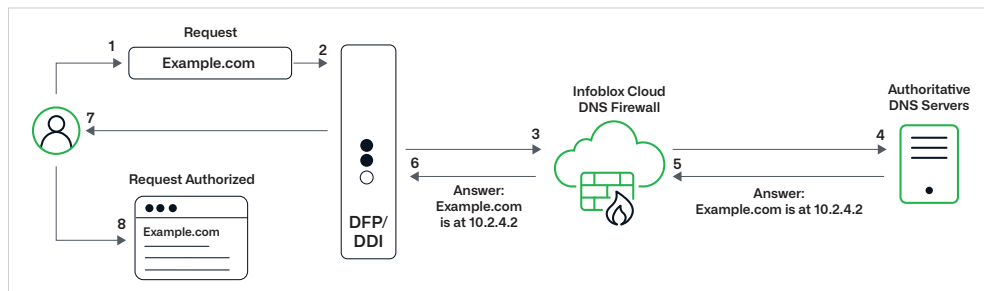


Figure 4. NIOS-X and Threat Defense performing recursion for a public domain resolution

DNS as a Cyberattack Vector

As with nearly everything on the internet, malicious actors have found ways to exploit the DNS protocol in a multitude of ways. Thankfully, Infoblox has tools that can assist with protecting against malicious actors when they target an organization's DNS infrastructure. Some DNS attacks Infoblox can help protect against include:

- **DNS Data Exfiltration and DNS Data Infiltration:** DNS data exfiltration and DNS data infiltration are forms of DNS tunneling which can be utilized by malicious actors to break down sensitive information, such as customer records or credit card information, into small packets which can be sent over DNS. Data can be either infiltrated or exfiltrated.
- **DoS/DDoS:** A DoS attack floods a DNS server with excessive requests from a single source, disrupting service. A DDoS attack amplifies this by using multiple sources, such as a botnet, making remediation harder. Both aim to overwhelm and disable targets
- **Command and Control (C2):** C2 leverages DNS to remotely control a compromised system. This can lead to data exfiltration, data infiltration or using the target system in a DDoS attack.
- **Phishing:** Phishing is a cyberattack technique where attackers impersonate legitimate entities, such as a website, to trick individuals into revealing sensitive information or downloading malicious software. To enhance their deception, phishers often exploit the DNS by registering lookalike domain names that mimic trusted sources.

This list is not all inclusive. However, this highlights how malicious actors often target DNS as an attack vector. Infoblox conducts extensive threat research to maintain multiple threat indicator feeds to protect against zero-day threats and known malicious domains. These feeds can be attached to a security policy or downloaded to an on-premises DNS firewall to both block and log attacks.

Content Filters

When certain types of online content are restricted at a given location, it's necessary to implement a method for blocking domains that provide such material. Infoblox offers the ability to block these domains via content filters that include a wide variety of content types. From pornography to social media, blocking these domains at a DNS level offers a simple, yet effective way to enforce company policies.

DHCP

DHCP is a critical network service and essential to nearly every network. When properly configured, it ensures seamless connectivity by offering unused IP addresses to clients, which enables network communication, prevents IP conflicts and provides clients with important information, such as the IP address of a DNS server and a router via DHCP options. DHCP allows devices to join and switch networks without requiring clients to manually input their IPs. Without DHCP, clients would need to input IP addresses manually, which would be impractical.

Given the criticality of DHCP, network architecture must prioritize effective, highly available and resilient design. Therefore, implementing DHCP failover is not optional—it's a requirement. With Universal DDI, administrators can group DHCP servers to serve clients' IP addresses, called a DHCP HA group, providing DHCP failover. With certain DHCP HA configurations, the capacity of these servers expands. With all DHCP HA configurations, if a server in an HA group “fails,” the DHCP service can continue while the other server recovers. When considering DHCP servers, NIOS-X, NIOS-X as a Service and NIOS all offer DHCP failover in a variety of forms. Refer to the section titled [Architecture](#) for more information on which server best suits which environment.

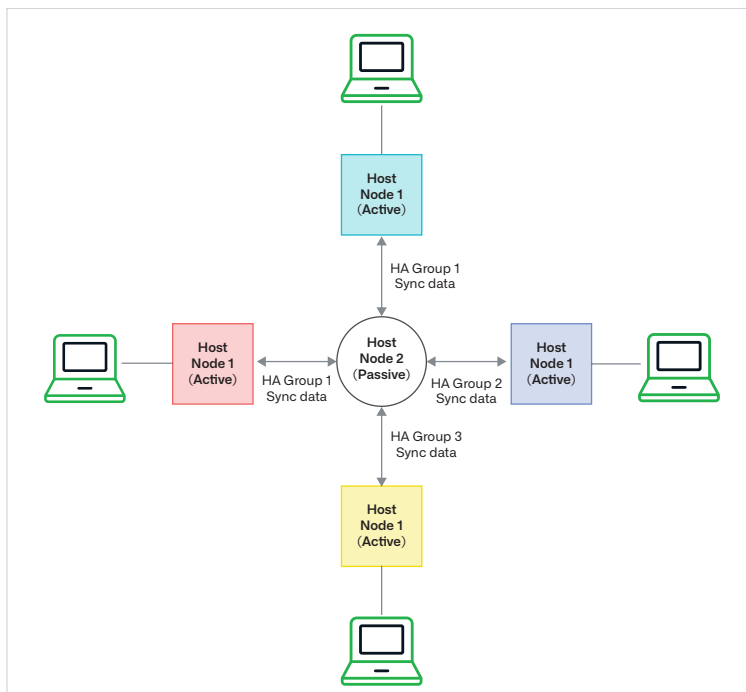


Figure 5. Clients access a DHCP HA group in an Advanced Active/Passive configuration. This DHCP HA configuration is asynchronous and provides effective DHCP failover.

In the cloud, the local DHCP service is managed by each respective cloud provider. All cloud providers do not allow you to replace their built-in DHCP service with your own. Cloud administrators are given limited control for each built-in DHCP service; however, some parameters may be configured, for example, administrators may configure the DNS server clients will communicate with when acquiring a DHCP lease. Due to this, when planning DDI architecture in the cloud, DHCP servers are not required.

DDNS

Dynamic DNS (DDNS) is the ability of DHCP servers to update DNS records when a client requests them to do so. This simplifies DNS administration and ensures that users and applications can always reach the correct destination, even if the IP address changes. Infoblox offers the ability to utilize DDNS regardless of the server serving DHCP.

AUTHORITATIVE IPAM

Authoritative IPAM acts as a single source of truth for all IP-related network data. It accurately reflects a clear view of an organization's network, providing contextual visibility into IP addresses, subnets and virtual local area networks (VLANs). IP conflicts, duplication and misrouting often result from manual processes or fragmented tools, especially in hybrid and multi-cloud environments, which can lead to network outages and escalations. Authoritative IPAM is the only way to avoid these outcomes. It ensures accuracy by comparing IPAM database records with the actual network state to detect discrepancies or overlaps.

Beyond just IP address and subnet information, authoritative IPAM identifies a wealth of endpoint data. It reveals details like device type (e.g., router, switch, firewall or host), model, operating system, vendor and location. You will know when the asset joined or left the network, and a precise location of where it is connected. No matter how complicated or distributed the hybrid, multi-cloud environment is, you will gain a clear, near-real-time summary and detailed visibility of everything on your network.

In Universal DDI, authoritative IPAM is managed centrally by consolidating data from multiple discovery sources across on-premises and cloud environments. Universal Asset Insights aggregates and normalizes IP address information from these discovery sources into a unified view. This centralized approach enables consistent IP address allocation, identifies overlaps between networks and shows them in a flat view for clear visibility.

IPAM Realms

Infoblox Universal DDI offers a feature named IPAM Realms, which is a way to logically segment or isolate IP blocks, providing the ability to plan and enforce IP usage across multiple IPAM tools. IP blocks in a realm can be defined as a few different things:

- **Delegated:** IP blocks can be delegated to specific IPAM tools, making them authoritative for the segment of IPs that have been defined and preventing other IPAM tools from creating blocks that overlap.
- **Reserved:** IP blocks that are reserved may not be used by IPAM tools in the realm. This is useful in various situations, for example, where certain IPs are in use by on-premises networks.
- **Overlapping:** Overlapping blocks are IP blocks that are OK to be overlapped. For example, a network that is behind a Network Address Translation (NAT) gateway.

IPAM tools that are joined to a realm will follow the structure as defined by the aforementioned blocks. This allows for better planning and enforcement of IP address usage across diverse systems, which helps avoid conflicts, overlaps and potential IP-related outages.

Asset Insights

Universal Asset Insights offers a centralized view of aggregated and normalized asset data from multiple discovery sources: NIOS Network Insights, NIOS-X (VM Probe), cloud environments and integrated platforms. As part of Universal DDI, it consolidates this diverse asset data in one place and offers multiple ways to view it for better clarity and usability:

- **Asset Inventory** acts as the centralized console to view all the discovered assets, which further allows users to apply filters for customized results and allows them to export to a CSV file for further analysis or reporting.
- **Assets Workspace** (asset-centric view) has AI applied to the discovered assets to determine if assets are fully utilized or vulnerable to attacks. The workspace includes multiple monitors that organize assets by classification, type, missing records and assets by location, making it easier to focus on what matters most.
- **DDI Workspace** focuses on showing trends in networks and DDI protocol services, which includes DHCP range and subnet utilization, overlapping IP blocks, dangling and abandoned records.

Why Is Asset Discovery Important?

Discovery helps businesses identify and locate all the assets connected to their network, whether on-premises or in the cloud. Without discovery, organizations may overlook the hidden, underutilized or vulnerable assets, which could put security at risk or waste resources. Asset discovery gives you visibility into what is running, where it is connected and how it is being used. It helps you make smarter choices, plan better and deal with challenges more quickly.

To ensure full visibility and secure operation of discovery processes, architect your discovery infrastructure with the following in mind:

- Cloud discovery works by using built-in cloud APIs to collect details about your network, compute, storage and other resources from all accounts and regions.
 - » Use identity and access management (IAM) roles to control access when setting up discovery to keep it secure and robust.
 - » Use multi-account organizational-level discovery wherever possible and not just individual accounts, to reduce management overhead and ensure full visibility.
 - » Use CloudFormation templates to quickly deploy Infoblox's cloud discovery integration for automated asset visibility.
- On-premises discovery services should not be run on the same server as other protocol services like DNS or DHCP.
 - » The architecture supports common network protocols, like Simple Network Management Protocol (SNMP), Secure Shell (SSH) and Command-Line Interface (CLI), to gather detailed information about each asset it finds.
 - » Ensure network ranges that need to be discovered are identified in advance and the necessary credentials (e.g., SNMP, SSH and CLI) are available ahead of time for smooth and comprehensive asset discovery.
 - » Administrators should consider network boundaries, such as firewalls, when deploying discovery nodes. NIOS-X discovery probes scan and transmit data over specific ports, depending on the scanning techniques used.
 - » If networks being discovered are in multiple geographical locations or large quantities of IPs are being scanned, multiple NIOS-X servers should be leveraged to reduce scan times and reduce the load on network bandwidth.

NIOS

NIOS is the traditional form factor of Infoblox DDI, best for external DNS, private cloud and local-only deployments. The NIOS platform utilizes Infoblox's patented Grid technology, which provides a unified platform for critical network services. An Infoblox Grid consists of at least one Grid Manager, with a variety of other Grid Members. One or more Grid Members can act as a Grid Manager Candidate if a Grid Manager has an outage. Managing this platform can be performed via the Grid Manager's graphical user interface (GUI). Or, if a NIOS grid is running versions 9.0.4 or above, it can be joined to the Infoblox Platform for full management via the Infoblox Portal. Versions 9.0.3 or previous can share data with the Infoblox Portal via the NIOS Grid Connector but is read-only with certain limitations, such as the inability to see active leases. One important note, when managing NIOS from the Infoblox Portal, software updates are still a manual process, unlike NIOS-X and NIOS-X as a Service.

NIOS operates a variety of services as determined by administrators, such as DNS, DHCP, Network Time Protocol (NTP) and others. Certain models, such as network discovery (ND), are capable of only one type of service: in the case of ND, discovery. The model type also determines the leases per second (LPS) and queries per second (QPS) capabilities of a NIOS device. For more information on sizing and NIOS models, reach out to your Infoblox representative as this topic is not within the scope of this document.

NIOS-X

NIOS-X is a physical or virtual server that provides one or more protocol services, such as DNS, and/or DHCP, locally. It can also be leveraged to discover assets via the discovery service or to push data to a SIEM or another database via the Data Connector service. NIOS-X has a few unique features that, depending on the use case, is the preferred method to serve DDI services:

- NIOS-X offers a variety of deployment options, such as private clouds, common hypervisors, physical devices and much more.
- NIOS-X leverages containerized computing which serves protocols and runs services via Kubernetes. Containerization provides reduced downtime during upgrades and introduces efficiency, allowing for multiple services to be provided by the same NIOS-X device.
- NIOS-X is useful in applications where lightweight or virtual servers can be leveraged.
- NIOS-X has HA capabilities depending on the services being leveraged.
- Server and service updates are provisioned automatically via the Infoblox Platform. Blackout periods can be defined if certain times during the week or day require full-service uptime as updates usually incur a short period of downtime.
- NIOS-X provides local survivability, capable of providing protocol services during periods of time where the Infoblox Portal cannot be reached.

When considering deployment options for DDI services, NIOS-X is best used for environments that need highly available, locally survivable protocol servers. It should not be used for external DNS but is fantastic for deployments in the cloud or on-premises. In situations where large quantities of QPS and LPS are required, more NIOS-X servers can easily be deployed, providing horizontal scalability for increased service bandwidth.

NIOS-X AS A SERVICE

NIOS-X as a Service is the industry's first serverless, managed DDI product. Connecting to NIOS-X as a Service requires IP Security (IPsec)-capable networking hardware such as a firewall or router. NIOS-X as a Service is also able to connect to cloud-based VPCs and VNets via cloud-native virtual private networks (VPNs). When configuring NIOS-X as a Service, the services DNS, DHCP, NTP and DNS security can be enabled. Specifically, DNS security allows for the blocking of DNS queries based on user-defined policies. Another benefit of NIOS-X as a Service is the ability to rapidly deploy managed DDI without needing to spin up an additional virtual machine (VM) or send IT professionals out to a physical location.

To create high availability, each NIOS-X as a Service deployment has two tunnels which exist in two separate availability zones. These tunnels connect to two separate virtual machines that the user does not need to manage or update, making this a true "as a service" DDI delivery model.

NIOS-X as a Service is best for locations that do not need local survivability, cloud deployments and small physical locations that do not have a lot of network traffic but still need managed DDI. Note, not all services are available to NIOS-X as a Service, but in situations where additional services are needed, NIOS-X or NIOS can be used.

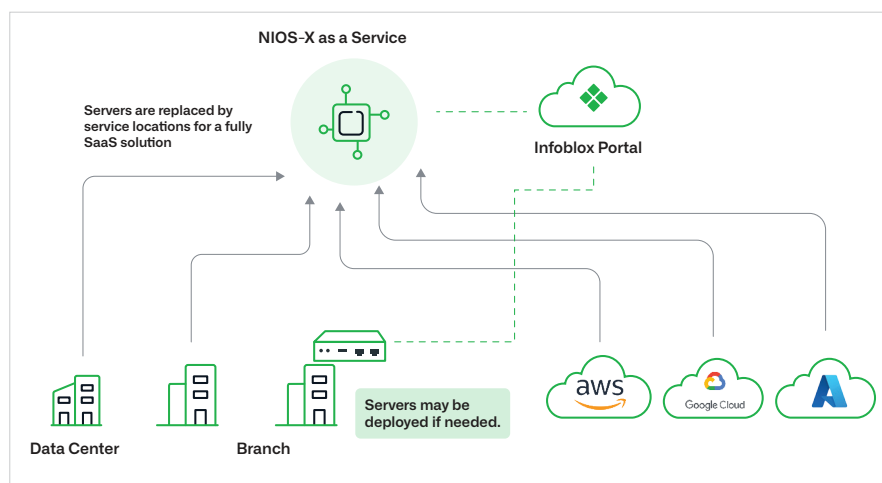


Figure 6. NIOS-X as a Service is a serverless solution that provides reliable DNS, DHCP and IPAM as managed services, regardless of where clients are; in the cloud or on-premises

ACME-Mart utilizes NIOS-X as a Service for all of their small locations, such as storefronts and offices with only a handful of employees, and cloud deployments where managed DNS is required.

THIRD-PARTY INTEGRATIONS

Various platforms are integrated with Universal DDI for a variety of use cases:

- SIEMs such as Microsoft Sentinel and Splunk. Infoblox can push DDI log data to SIEM platforms via these integrations. This allows organizations to create a single repository for all of their logs, regardless of which platforms they use.
- Configuration management databases (CMDBs) such as ServiceNow. Infoblox can ingest data from CMDBs such as ServiceNow, allowing for the aggregation of organization-wide asset data with Asset Insights.
- DNS-, DHCP- or IPAM-related platforms such as BIND and Microsoft DNS/DHCP servers. As mentioned in earlier sections, Universal DDI allows administrators to manage other DDI platforms. This enables the Infoblox Platform to be the one-stop-shop for managing organizations' DDI objects and platforms.
- Cloud platforms such as AWS, Azure and Google Cloud. Infoblox ingests data from these cloud platforms to create a database on cloud assets and allows for the read-write management of DDI objects.

Note that this list is not all inclusive and more products are being integrated with Universal DDI in each release. When designing network architectures, considering automation workflows and creating a single database for assets and logs viewing, the [Ecosystem Portal](#) is a great way to find resources and information on what platforms integrate with Universal DDI and how to integrate them.

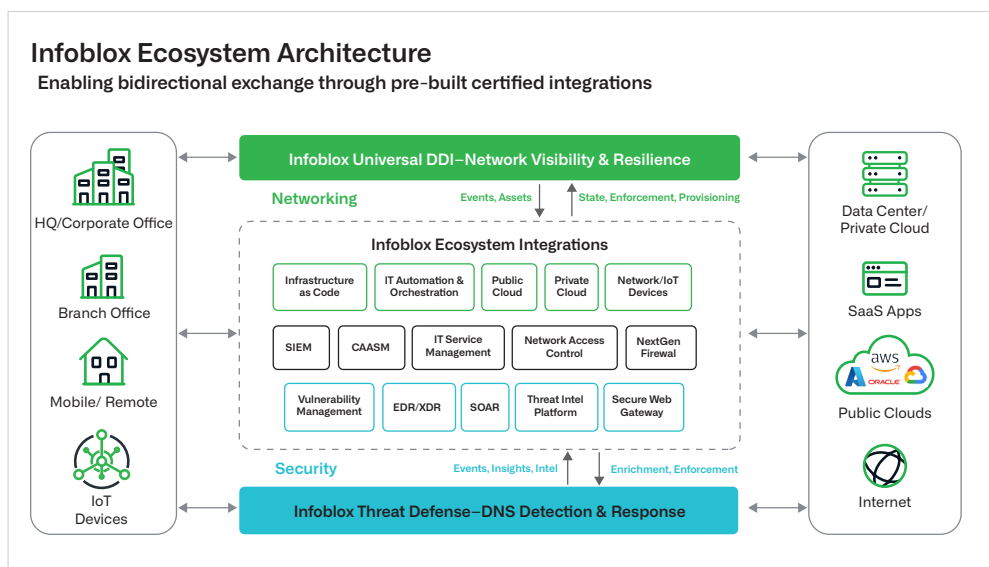


Figure 7. The Infoblox Ecosystem architecture provides a wide array of product integrations across security, network automation and the cloud

The company ACME-Mart pushes Universal DDI, DHCP and DNS data to SIEM tool, Splunk. By forwarding their logs to Splunk, they create a single location to view all of their companywide.

They sync their CMDB, ServiceNow, with Universal DDI to create a single location to view all of their network-connected assets. The integration also supports CMDB reconciliation, allowing them to identify missing, outdated or mismatched records, ensuring their CMDB remains updated, accurate and aligned with the actual state of network.

They connect and manage their disparate DNS/DHCP systems, such as BIND and Microsoft DNS and DHCP servers, through the Infoblox Portal.

They integrate their multi-cloud infrastructure to manage DNS zones hosted by the cloud providers they use, view their cloud-based assets discovered by Asset Insights and serve DNS to these platforms via NIOS-X as a Service and NIOS-X.

AUTOMATION

Universal DDI offers the ability to easily work with multiple APIs as a single touchpoint, reducing a large amount of operational overhead. When working with automation workflows, individuals can work with a single API instead of learning multiple different APIs, managing a variety of code bases and juggling multiple sets of credentials or API tokens. This benefit is exponential for each additional platform integrated with Universal DDI. Furthermore, Infoblox has plug-and-play Terraform providers and Ansible modules which allow for tedious, repetitious tasks to be scripted and easily repeated on demand.

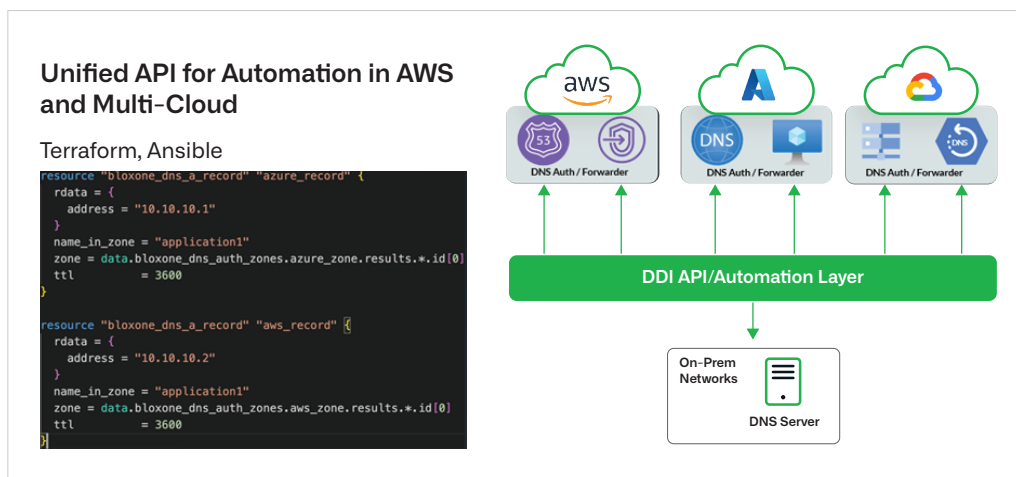


Figure 8. Infoblox Universal DDI allows for administrators to easily work with multiple DDI platforms via a single API

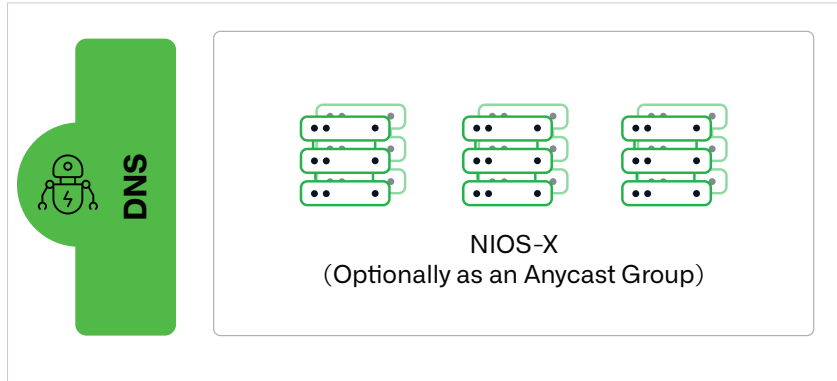
ARCHITECTURE

For all locations in the company ACME-Mart, on-premises or in the cloud, management of the entire DDI portfolio is accomplished via the Infoblox Portal. All DDI logs are pushed directly to the cloud and are visible in the Infoblox Portal.

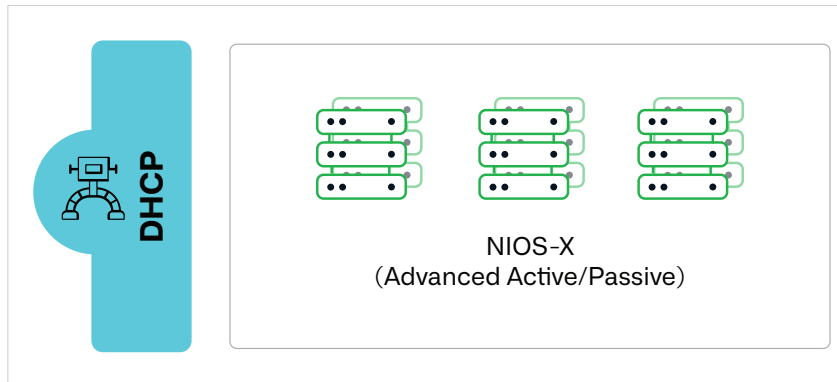
HEADQUARTERS

ACME-Mart's headquarters is located in Nashville, Tennessee. The headquarters site consists of two large office buildings, a fulfillment center, a manufacturing building and multiple additional small buildings, such as maintenance buildings and other auxiliary buildings. Highly available, resilient DDI architecture has been employed to support these buildings.

- **Internal DNS:** DNS is provided by a DNS server group containing three NIOS-X servers. Anycast is also utilized to allow all three servers to leverage the same IP in separate network segments.



- **DNS Forwarders and Recursion:** For all recursive DNS queries, DNS traffic is forwarded to the Infoblox Cloud for deeper inspection from Infoblox Threat Defense before being sent to the internet's root servers. For devices querying DNS zones that relate to ACME-Mart's AWS, Azure or Google Cloud applications, NIOS-X as a Service and NIOS-X DNS servers host copies of those DNS zones and serve them locally.
- **DHCP:** DHCP is served to the site by six NIOS-X servers running DHCP, each in a DHCP HA group: one DHCP HA group for each network segment. The type of DHCP HA they leverage is Advanced Active/Passive, which is asynchronous, meaning that servers in the DHCP HA group do not need to verify which IPs have been leased with the other server in the pair. This is also true in situations where one of the servers has an outage.



- **Network Discovery:** Network discovery is accomplished via a NIOS-X VM running the discovery service. This device has access to all network segments in the headquarters and has SNMP credentials to access switches and routers.



CLOUD

ACME-Mart hosts a variety of infrastructure on the cloud. They also have private and public DNS zones hosted in AWS, Azure and Google Cloud. They leverage Universal DDI to improve their visibility and control over their cloud-based infrastructure. Discovery and management are accomplished via discovery jobs.

- **Internal DNS:** For DNS internal to cloud platforms, ACME-Mart leverages NIOS-X as a Service which connects directly to the VPC with no additional VMs. This NIOS-X as a Service instance provides managed DNS, DNS forwarding and DNS security to all VMs and applications in each cloud provider's VPCs and VNets. Private DNS zones hosted in the cloud are managed via the Infoblox Portal. For all recursive DNS queries, DNS traffic is forwarded to the Infoblox cloud for deeper inspection from Infoblox Threat Defense before being sent to the internet's root servers.
- **External DNS:** External DNS is hosted on each cloud provider. These DNS zones are managed via the Infoblox Portal.
- **Discovery:** Due to the nature of cloud, multi-cloud and multi-account environments, keeping tabs on assets and IP usage across these spaces can be a monumental challenge. ACME-Mart leverages Infoblox Asset Insights to discover and catalog all their assets across all clouds and all accounts, subscriptions and projects. This is accomplished via API-to-API communication and discovery jobs in the Infoblox Portal and saves ACME-Mart's cloud and networking teams valuable time, finding assets and reducing wasted spend (IP or underused assets).

BRANCH LOCATIONS

ACME-Mart has various branch locations, fulfillment centers and offices, spanning the globe. These locations serve anywhere from a handful of employees to hundreds of employees. Due to the variability of these locations, both NIOS-X and NIOS-X as a Service are employed to serve DHCP and DNS. DHCP is served by one or more pairs of NIOS-X devices running in DHCP HA groups, or by NIOS-X as a Service with support for two tunnels creating redundancy. For all NIOS-X as a Service deployments, two servers are automatically deployed in two different availability zones (AZs), with shared databases. This is a default configuration with no additional configuration required, aside from connecting to these two tunnels. Based on the location, DNS is served by NIOS-X as a Service or a NIOS-X DNS server group. Recursive DNS is sent to the cloud for further inspection via Infoblox Threat Defense. DTC is also leveraged.

SMALL-FOOTPRINT LOCATIONS (STOREFRONTS)

ACME-Mart contains many small locations globally that only have a few employees, a handful of point-of-sales devices, a couple devices connecting to corporate networks (such as laptops and personal computers) and other IoT devices. These storefronts leverage NIOS-X as a Service, which utilizes local routers to tunnel managed DDI directly to these small locations with no additional DDI hardware required. As a true SaaS offering, NIOS-X as a Service allows for consistent policy application and convenient management for DDI teams, as this product is managed via the Infoblox Portal. Recursive queries for non-internal domains are sent to the Infoblox cloud for further inspection from Infoblox Threat Defense before being sent to the DNS root servers.



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