SOLUTION NOTE

TRINZIC X6 SOLVES AUTOMATION, SECURITY AND UPTIME CHALLENGES IN HYBRID, MULTI-CLOUD NETWORKS

NIOS 9.0.1

The benefits of cloud networking are driving organizations from virtually every market vertical to migrate data platforms and applications from legacy and physical data centers to hybrid, multi-cloud environments.

Application uptime, resiliency, disaster recovery, workflow automation, scalability, agility and potential IT cost advantages are among the compelling, if not urgent, reasons to modernize business infrastructure. Along the hybrid, multi-cloud migration journey, however, organizations encounter myriad challenges that can delay or even stall workplace modernization efforts and attainment of cloud benefits. As the leader in unified networking and security services, Infoblox has anticipated these challenges and worked with leading global companies to understand and develop solutions to simplify and resolve key cloud migration roadblocks. With NIOS 9.0.1 and Trinzic X6, Infoblox's purpose-built physical and software appliance platform, Infoblox helps companies avoid common pitfalls, realize cloud benefits faster and deploy better, more robust solutions to achieve greater time to value.

BUSINESS CHALLENGES

With NIOS 9.0.1, Infoblox solves some of the most frequent business challenges and enables workplace modernization by including three cost-saving "sitewide" licenses (previously sold separately) as part of the Trinzic X6 platform: Cloud Platform (CP) API automation, DNS Firewall (DFW) and DNS Traffic Control (DTC) 0global server load balancing. These solutions address business problems like scaling workload automation and survivability across silos and multi-cloud environments; protecting your enterprise at the edge by using response policy zones (RPZs) to intercept and block DNS resolution from malicious network IPs or domains; and improving application uptime and user experience by removing latency and enabling disaster recovery. This Solution Note examines each of these features and capabilities individually, including key use cases, how the solution works and its potential advantages for hybrid, multi-cloud environments.

Trinzic X6 solves pressing cloud modernization challenges by including "sitewide" licenses for Cloud Platform (CP) API Automation, DNS Firewall (DFW) and DNS Traffic Control (DTC) global server load balancing.

CLOUD PLATFORM (CP) API AUTOMATION

USE CASES

- Scale API DDI automation
- Avoid backhauling API calls
- Extend DDI to multi-cloud environments
- Simplify access control for networking and cloud teams
- Reduce complexity of network operations
- Save costs and deliver strong ROI

BENEFITS

- **Distributed API processing:** CP license scales DDI performance and distributes API loads locally.
- **Delegated administration and multi-tenancy:** Administrators can delegate DDI objects for programmatic

CLOUD PLATFORM (CP) API AUTOMATION

SCALING AND AUTOMATING DDI INFRASTRUCTURE FOR CLOUD ENVIRONMENTS

As enterprises adopt cloud deployments, orchestration and automation functions become critical. The Infoblox CP API license improves the scalability and resilience of data center deployments by distributing API processing and keeping API calls and DNS/DHCP protocol services local to each data center or cloud environment. This type of localization lets enterprises scale their critical network services with an architecture that optimizes the needs of today's distributed cloud deployments and enables future deployment topologies.

WHY CHANGE: MODERNIZE DNS AND IPAM INFRASTRUCTURE

Automation and distribution of critical DDI (DNS, DHCP and IPAM) networking services are essential for modern, dynamic infrastructures. Applications can be deployed on-premises in private clouds, off-premises in public clouds or in a hybrid environment simply by changing configurations in the cloud management or orchestration platform. Similarly, applications can be moved to make better use of infrastructure-as-a-service (IaaS) resources. Therefore, it is critical that DDI be flexible, automated and distributed across these environments.

As part of the provisioning workflow, integration is necessary between the server/cloud teams to provision the compute, storage and network requirements for each virtual machine (VM):

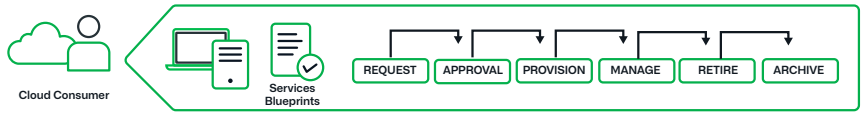

Figure 1: Creation of virtual machines (VMs) crosses server/cloud and network teams to provision, manage and retire VMs.

WHY NOW: AUTOMATE AND SCALE ENTERPRISE-GRADE DDI FOR HYBRID, MULTI-CLOUD NETWORKS

The CP API license solves the challenge of distributed DDI services by serving DNS and DHCP protocols with API management of DDI records in a single Trinzic X6 platform directly integrated into the Infoblox Grid. As VMs are provisioned, the CP license allocates IP addresses and automatically creates DNS records for each VM, eliminating bottlenecks created by manually provisioning IP addresses and individual DNS records. The CP license further enables API survivability, distributed API processing and authority delegation.

Infoblox integrates with leading cloud management platforms using RESTful APIs to improve agility by providing IP address management and automated DNS provisioning for workloads. Cloud-orchestration platforms use API calls to provision network services for DNS and IP address automation. Servicing these API calls becomes critical to provisioning VMs and requires a scalable, resilient solution with no single point of failure.

management by specific cloud or automation projects. They also can segment and manage the objects by tenant while maintaining centralized visibility.

- **Improved survivability:** Because API automation happens at the local appliance level, cloud and virtualization creation can continue to occur even if connectivity to the Grid Manager is lost.
- **Full integration with Infoblox DDI:** CP functionality works with traditional DDI appliances in an Infoblox Grid and supports Infoblox Internal DNS Security.
- **Direct integration with leading platforms:** Infoblox has pre-built integrations with VMware vRA/vRO, AWS EC2, GCP, Azure, OpenStack and other platforms that are optimized for fast deployment and time to value.

Centralized Visibility and Management for Hybrid Cloud Deployments

The data synchronization and distributed database capabilities of the Infoblox Grid make it easy to centrally manage all DDI data while distributing DNS and DHCP protocol support. The CP license takes this concept a step further by enabling API updates on the same Infoblox members that serve DNS/DHCP. The Infoblox Grid performs bi-directional synchronization of all data within the Grid in near real time, providing the unique capability of allowing updates of critical DDI records through the Grid Manager and/or through Trinzic X6 CP members. This capability gives enterprises the same benefits of distributed, highly available API processing as they would get serving DNS/DHCP protocols from their Infoblox Grid.

Improved API Handling with Cloud Management Platforms

Without the CP license, API calls are sent to the Infoblox Grid Manager as part of the Infoblox Cloud Network Automation deployment. This approach works fine if communication with the Grid Manager is available. But if network connectivity is disrupted between the cloud management platform/orchestrator and the primary data center hosting the Grid Manager, DNS and IP address management will be impacted, and the risk of a service outage increases.

The Infoblox CP license serves DNS and DHCP just as traditional Grid Members do, but it is also able to synchronize and manage IPAM records. These capabilities ensure that all of the API calls are kept within the same data center or cloud environment while DNS/DHCP changes happen in real time. As such, availability and latency issues are eliminated, even if connectivity to the Grid Manager is lost. When connection resumes, data is synchronized between the Grid Manager and cloud platform members automatically. This synchronization step ensures local survivability while still providing centralized visibility and management. In scaled-out cloud environments where VMs are spun up across multiple locations, the local API capability improves overall system reliability and avoids latency with API calls that have to be sent over a WAN.

Distributed DDI Management and Multi-Tenancy Support

The Infoblox CP license supports a delegation model enabling organizations to segment DDI to delegate management of records for zones, subzones, networks/subnets or ranges to particular organizations or projects within an organization. When used with Infoblox Cloud Network Automation, the CP license enables network admins to delegate and isolate management of DDI records specific to OpenStack or VMware vRA tenants or AWS EC2 VPCs, facilitating management of multi-tenant environments.

Additional CP licenses can be deployed on-demand to increase protocol and API capacity or to furnish critical network services for new cloud environments as they are provisioned. This capability improves overall time to service while providing additional scalability and resiliency for cloud deployments. The CP capability is essential for supplying the dynamic and scalable DDI services that hybrid, multi-cloud deployments need.

WHY INFOBLOX: SCALING RELIABLE DDI AUTOMATION, PERFORMANCE AND SURVIVABILITY FOR THE MULTI-CLOUD ENTERPRISE

Infoblox's CP license optimizes enterprise-grade DDI for reliable and scalable cloud network automation performance and survivability. It delivers complete visibility of physical and virtual resources with single control plane management. It also leverages robust API integrations with AWS, Azure, GCP, OpenStack, VMware and other platforms to scale automation across the hybrid, multi-cloud enterprise.

DNS FIREWALL (DFW)

PROTECTING DNS TO THE EDGE OF THE ENTERPRISE

Infoblox DNS Firewall is a Domain Name System (DNS) service that utilizes Response Policy Zones (RPZs) with a threat intelligence service (malware feed) to protect DNS by detecting, containing and controlling malware. This type of malware utilizes DNS to communicate with Command and Control (C&C) servers and botnets for intrusion, data exfiltration or other malicious activities. RPZs provide a way to understand the reputation of the servers and services clients are querying and set policies and actions to prevent network users and systems from connecting to known malicious Internet locations. By including the DFW license in NIOS for physical and software appliances, Infoblox helps you protect your entire enterprise across on-prem sites, data centers and through the cloud to the network edge.

WHY CHANGE: DNS INFRASTRUCTURE IS UNDER ATTACK

Attacks on DNS infrastructure continue to be a leading source of the thousands of data breaches occurring in every industry daily across the globe. DNS is attacked through a wide range of volumetric DNS, DDoS or DNS amplification/reflection attacks and exploits, such as DNS cache poisoning, spoofing and session hijacking, that bypass or even disrupt the operation of today's Next Generation Firewalls (NGFWs). Most NGFWS are unable to identify or handle these threats because they allow traffic to pass through Port 53, the protocol over which DNS queries and responses are sent.

WHY NOW: PREVENT DATA EXFILTRATION AND CONNECTION TO MALICIOUS LOCATIONS

DNS is increasingly used as a pathway for data exfiltration by tunneling IP protocol through Port 53, either unwittingly, through undetected malware-infected devices or intentionally by malicious bad actors. Making matters worse is the fact that most malware is not detected for more than 200 days after infection, leaving companies exposed to loss of sensitive customer data, financials, intellectual property and other critical information.

WHY INFOBLOX: UNIFYING NETWORKING AND SECURITY FOR PROTECTION AND PERFORMANCE

Infoblox DFW is the leading DNS-based network security solution. With DFW, Infoblox unifies networking and security by containing and controlling data exfiltration malware across on-prem deployments to the edge of the cloud network. DFW works by integrating DNS RPZs, Infoblox's optional BloxOne Threat Defense, Threat Insight or forensic third-party indicators of compromise (IoCs) feeds to detect, block and redirect malware. Infoblox combines DFW with networking IPAM data in the Grid to help isolate infected devices for remediation. By leveraging DHCP fingerprinting and Identity Mapping, administrators can capture the username tied to an infected device and reduce the impact of threats early in the cyber kill chain. In addition, DFW enables DNS redirection, allowing administrators to block or forward domains to a "walled garden" or other designated locations. DFW can further be used as a trigger for Security Ecosystem integrations for customers with the Ecosystem license. DFW also integrates with Infoblox Reporting and Analytics to provide summary reports and rich contextual data including top RPZ hits, top malicious hostnames, top malicious users and many other

DNS FIREWALL (DFW)

USE CASES

- Bring IOC detection to the network edge (on-prem or in the cloud)
- Enable DFW on the hardware or software appliance
- Allow threat protection with Infoblox and/or 3rd party feeds
- Ensure DNS malware protection
- Improve the existing security stack

BENEFITS

- **Detect, contain and control malware:** Combine networking and security tools and data to enable early detection of infected or malicious communications.
- **Reduce enterprise DNS threat impact:** Combine RPZs with optional threat intelligence feeds to protect the enterprise from on-prem to cloud deployments.
- **Improve visibility, automation and control:** Enable administrators to see rich contextual data, automate threat response, redirect and remediate security threats.
- **Trigger Security Ecosystem integrations:** Improve threat awareness, visibility, sharing and response through extensive ecosystem integrations.
- **Integrate Reporting and Analytics:** Gain on-demand summary, forensic and visualized reports of rich network data.

security metrics. Finally, DFW provides a reliable foundation for DNS malware protection and improves the impact and ROI of the customer's existing security stack.

How Does it Work?

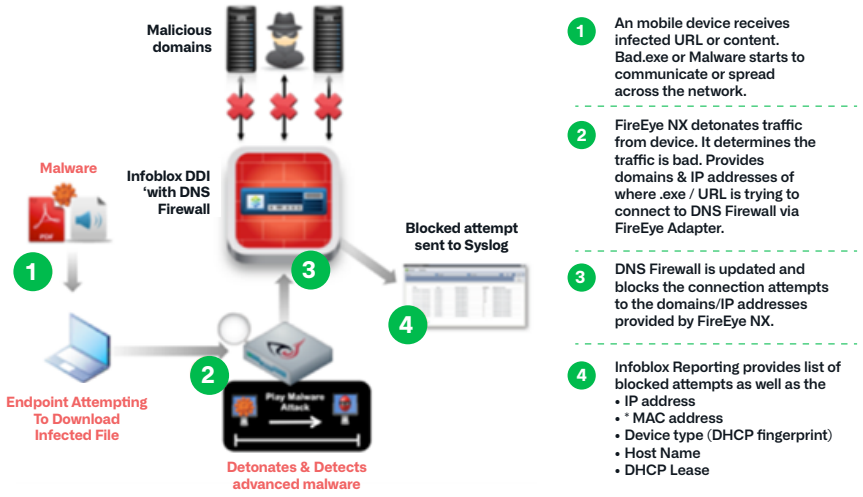

Figure 2: How DNS Firewall works to block malicious connection attempts.

DNS TRAFFIC CONTROL (DTC)

IMPROVING TRAFFIC MANAGEMENT, APPLICATION UPTIME AND USER EXPERIENCE

The Infoblox DTC license is an integrated Global Server Load Balancing (GSLB) solution that delivers network traffic management, reliable application uptime, service resiliency and disaster recovery (DR) for on-prem and hybrid, multi-cloud networks. DTC integrates authoritative IPAM data with DNS and GSLB server health metrics, geo-IP and Extensible Attributes (EAs or user metatags) to intelligently direct user traffic to optimal servers for maximum uptime and user experience.

WHY CHANGE: GLOBAL MODERNIZATION IS CHANGING THE NETWORK LANDSCAPE

Regional and global workplace modernization is changing the on-prem and hybrid, multi-cloud enterprise. Direct access to cloud applications from everywhere has raised expectations for a fast, efficient and always-available customer experience. SD-WAN is enabling direct Internet access for local branches. 5G capabilities are emerging and IoT is increasing connectivity demands on network resources. These challenges magnify as organizations adopt new platforms and technologies. Users expect real-time performance, especially from e-commerce and internal portals. Managing legacy and modern apps is becoming more complex, especially with mergers and acquisitions. Privacy regulations are intensifying with severe penalties for non-compliance. Changing trends in mobile and remote workers and branches, globalization, data center consolidation, ongoing resource limitations and expanding DNS, malware and stealth attacks are placing an even greater strain on teams tasked with managing network traffic, uptime and business continuity in a responsible and sustainable manner.

- Enhance the existing security stack: Improve the impact, value and ROI of existing security tools and integrations.

DNS TRAFFIC CONTROL (DTC)

USE CASES

- Cost-effective global traffic management on internal and external on-prem and hybrid clouds
- Uptime for on-prem and SaaS apps based on subnet, GeoIP and Extensible Attributes
- Disaster Recovery (DR) for resiliency following catastrophic disruptions
- Domain Zone consolidation and replication of servers and resources
- API-based application scaling across private, hybrid and multi-clouds
- Site-level awareness for MS AD clients
- Fully integrated reporting and analytics

BENEFITS

- **Integrated DNS/Global Server Load Balancing (GSLB):** Integrates authoritative IP address management (IPAM) with DNS and GSLB to deliver five-nines, highly available Intranet and Internet app uptime and performance without dependence on a separate DNS platform.
- **Intelligent Global Traffic Management:** Uses DNS-based GSLB to intelligently direct user traffic to the optimal server based on client and server location, server health and server availability.

WHY NOW: AFFORDABLE, RELIABLE GLOBAL UPTIME AND BUSINESS CONTINUITY

Infoblox's DTC provides an affordable solution relative to other competing Application Delivery Controllers (ADCs) to solve changing global traffic management challenges. DTC delivers strong user satisfaction through reliable application uptime, performance and seamless failover. It uses an easy user interface and robust APIs to distribute network traffic loads across geo-diverse, on-premises and hybrid, multi-cloud environments for e-commerce, customer-facing portals, the web and internal business-critical applications. It also supplies business continuity and disaster recovery in the event of a catastrophic event to restore normal operations.

WHY INFOBLOX: UNIFYING NETWORKING AND SECURITY FOR PROTECTION AND PERFORMANCE

Infoblox's DTC integrates authoritative IPAM data with DNS and GSLB to intelligently direct user traffic to optimal servers. Unlike competing ADCs, it's a fully integrated DNS solution, so it's faster and more reliable than bolting-on Layer-2 and Layer-3 protocols. It provides multiple load balancing algorithms and flexible, automated, health checks to ensure server availability. DTC is scalable to meet changing data traffic volumes and business needs. For optimal visibility, DTC uses a simple user interface and visualizer that displays Load Balanced Domain Names (LBDNs), pool and server relationships and attributes. Also, unlike other ADCs, it allows real-time, pre-production testing of LBDNs, pools and servers to ensure readiness before go-live. DTC can use GeoIP and EA data (user-defined metatags) to control traffic to region-specific zones for regulatory and privacy compliance along with application optimization. An integrated Splunk-based Reporting and Analytics tool offering pre-built and customizable DTC dashboards, reports, search, alerting and automated report distribution is available separately. Finally, DTC integrates with Infoblox discovery sources to automatically update topologies based on IP subnet, GeoIP and EA data. APIs can be used to quickly add new server instances, provision new apps, integrate with other systems and automate routine tasks. Because DTC is integrated directly into the Grid, there is no need to manage a separate platform's software deployments, configurations and updates.

- **DTC Visualizer:** Displays load-balanced domain names (LBDNs), pool and server relationships and attributes through a single GUI visualization.
- **Pre-Production Testing:** Allows testing of new and updated LBDNs, pools and servers quickly and in real time to ensure pre-production readiness before go-live.
- **Compliance:** Allows the use of GeoIP and Extensible Attribute (EA) data to restrict traffic to region-specific zones for LBDNs and pools to assist with meeting privacy compliance.
- **Integrated Reporting and Analytics:** Supplies Splunk-based pre-built and customizable dashboards, reports, search, alerting and automated report distribution for enhanced visibility and control.
- **API Automation:** Add new server instances, provision new apps quickly, integrate with other systems and automate routine GSLB management tasks, saving time and money with this easy-to-use, well documented API that mirrors the functionality of the web GUI.

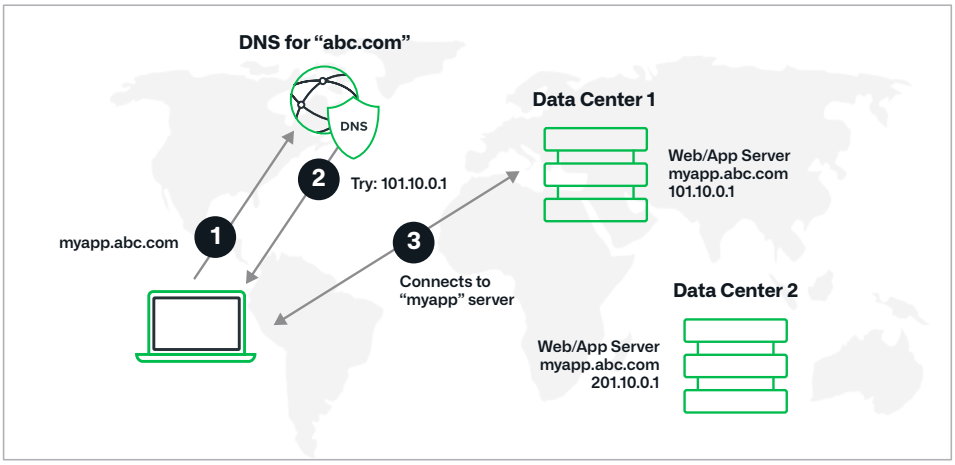

Figure 3: DTC provisioning showing 1) app deployment initiation, 2) company DNS connection, and 3) myapp server provisioning in distributed data centers.

SUMMARY AND NEXT STEPS

With NIOS 9.0.1 and the Trinzic X6 platform, Infoblox adds value by solving cloud modernization challenges by including “sitewide” licenses previously sold separately for Cloud Platform (CP) API Automation, DNS Firewall (DFW) and DNS Traffic Control (DTC) global server load balancing. These solutions address frequently encountered business problems like scaling workload automation and survivability across silos and multi-cloud environments; protecting your enterprise to the edge by using response policy zones (RPZs) to intercept and block DNS resolution from malicious network IPs or domains; and improving traffic management, application uptime and user experience. To learn more or start a trial, contact your Account Team at Infoblox.com.

CONTACT US

For additional technical information, please see the NIOS 9.0.1 Release Notes (available at GA, 8/21/2023) located in the Infoblox Support Portal at https://support.infoblox.com.

To get specific answers on Infoblox’s NIOS or Trinzic X6 platform, or the extensive lineup of hybrid, multi-cloud integrations for workplace modernization, connect with your Infoblox account team 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

Version: 20230731v1