Infoblox

The Business Case for Infoblox BloxOne DDI

Tolly Report #220120

August 2020

Contents

1 Executive Summary

Introduction

We've all recently witnessed how critical distributed networks have become for businesses. Many organizations have had to assess, act, and add tens, hundreds and even thousands of remote sites and locations to their networks in a matter of days. These activities were more than just important, they were essential to business continuity. Decentralization of the enterprise is the "New Normal", and this trend is showing no signs of slowing as the number of locations, devices, and users continue to increase.

This growing importance of distributed business locations is at odds with traditional, long-standing hierarchal deployments that made the headquarters the center of the universe. In that model, branch-office and satellite sites relied on the central site for services. In many cases, if the WAN access between the remote location and the central office was unavailable, the branch office could see services limited or unavailable, including core networking services such as DNS, DHCP, and IP Address Management (or DDI). This model is no longer feasible, as the need for continued business operations at distributed locations has become a top priority in nearly every environment. Infoblox BloxOne DDI provides the industry's first comprehensive core network services solution to address these challenges, while streamlining the deployment, administration, and control of distributed enterprises, through a centralized cloud-based interface.

Infoblox commissioned Tolly to analyze key challenges facing enterprise IT organizations, and to identify if and how BloxOne DDI could meet their expanding requirements. Tolly analysts assessed the BloxOne DDI solution in a lab deployment and reviewed technical documentation during the course of the project. Tolly found three key areas where BloxOne DDI enhances the management and control of today's distributed enterprise networks: 1) Centralized Administration, 2) Mobility & Cloud Optimization, and 3) Distributed Site Survivability. Additional benefits include simplified deployments, streamlined operations, reduced TCO, and flexible physical or virtual deployment options provided by the BloxOne Platform.

Centralized Administration

Combining the best of both worlds, cloud management via the BloxOne DDI Cloud Service Portal (CSP) provides single-pane of glass management access to all of your BloxOne devices without the need to install or maintain an on-prem management server. As illustrated later in this paper, CSP can be used for the full range of management tasks, from status checks, configuration and software maintenance to detailed troubleshooting, and remote packet capture. BloxOne CSP was designed to be highly-available, so users can check current and historical uptime with a single click at: https://status.infoblox.com/. The ability to manage company-wide devices from a centralized interface provides an important economic benefit as it can greatly improve operational efficiency for your system managers.

Mobility & Cloud Optimization

Core business applications are increasingly transitioning to Software-as-a-Service (SaaS) solutions. Whether the application is Salesforce, Microsoft Office 365 or an industry-specific vertical application, these cloud applications now serve as core business functions. When it comes to core business applications, performance matters, and slow network connections have an immediate and ongoing negative impact on productivity. Unfortunately, central-site, back-hauled DNS generally provides communications paths between client and cloud apps that are not optimal and degrade the user experience.

With BloxOne DDI, network services and connections are optimized for each location and provide an optimal path between location and target cloud applications. In our example detailed later in this paper, "before" the deployment of BloxOne DDI the connection test from a test client to Office 365 required 67 ms when "after" BloxOne DDI was activated, that time dropped down to a mere 3 ms. This is an ongoing performance benefit for every remote user of every cloud application in the distributed environment.

Distributed Site Survivability

With back-hauled, DNS & DHCP services, the WAN link to the central site becomes a potential exposure with respect to reliability and availability for distributed users. Should that link fail, connectivity would be compromised as users would no longer have access to critical resources. Even without failure, severe congestion on back-hauled link could impact the response time and experience.

When BloxOne DDI is deployed, and running locally at each location, these survivability worries are no more. Because network services are co-located with users, they are always available. Access to services is now "survivable" even in situations where access to the company's central site is interrupted or degraded.

Total Economic Impact

BloxOne DDI not only provides technical benefits, but also has a positive economic benefit on both the IT organizations deploying and supporting the environment, as well as the end users. These benefits accrue both to end-users and administrators. Even an improvement of one second in response time for transaction-intensive users allows them to get more work done in less time. In models developed for this project, per-user cost reductions of several dollars per hour resulted based on a user think time of 15 seconds and a 1 second response time improvement. Similarly, the efficiencies of centralized administration and automated updates showed significant savings in admin time/cost especially for companies with 30 or more sites.

See https://www.infoblox.com for information on a joint Tolly-Infoblox webinar that explores the BloxOne DDI Total Economic Impact (TEI) in more detail.

2 Centralized Administration

Benefit

Centralized anytime, anywhere management and control of core network services for all distributed locations (i.e., branches, remote, home offices).

Situation

In situations where network services are deployed at the local level they are typically part of an existing router/firewall or as a standalone appliance. In fact, many of these deployments are as basic as those found in home routers with the combination Wi-Fi and WAN router providing basic network services and DNS forwarding. However, each location requires some level of initial and ongoing management for configuration, updates and troubleshooting.

Challenge/Exposure

Distributed locations are notoriously difficult to manage. In almost every case, each must be managed individually. This certainly brings complexity from documenting the administrative credentials for each device to performing the required tasks, all the way through to the local IP address of the management function. Strategically, this approach is a nightmare as administrative and policy management must be configured for each location via a separate login and management session.

Solution

A centralized, single-pane-of-glass management and control interface for all locations with the ability to configure and deploy policies to all or a subset of locations from a single session is a major improvement.

Infoblox BloxOne DDI provides centralized, cloud-based DDI administration that provides visibility into, and allows policies to be configured and deployed across all locations. Additionally, BloxOne DDI can be used to simplify deployments to new locations. Cloud-based administration removes the need for separate, local servers to host management. It also removes the need for the customer to manage updates to the management system and it provides flexible access to any authorized user from distributed locations.

A Solid Foundation: The Infoblox BloxOne Platform

Infoblox BloxOne DDI is based on the BloxOne Platform, a Secure Access Service Edge (SASE) compliant framework that utilizes the latest innovations in software-defined networking, microservices and containerization to move the management plane from the appliance to the cloud. In doing so, it greatly simplifies management of complex network assets, is highly-scalable, and enables the rapid delivery of new capabilities and features.

The Infoblox BloxOne Platform enables the BloxOne DDI solution to:

- *Offer the elastic scalability and centralized management of cloud deployment*
- *Lower capital expense by running on low-cost commodity hardware and/or as virtual machines or containers*
- *Use a predictable, consumption-based subscription pricing model*
- *Secure devices anywhere: on-premises, roaming and in branch offices*

Source: Infoblox

Proof Points

By now, it is more than likely that you have at least one business system delivered via cloud administration and, thus, the general benefits are already evident to you. Therefore in this section we'll focus on the specific benefits of cloud management with respect to BloxOne DDI.

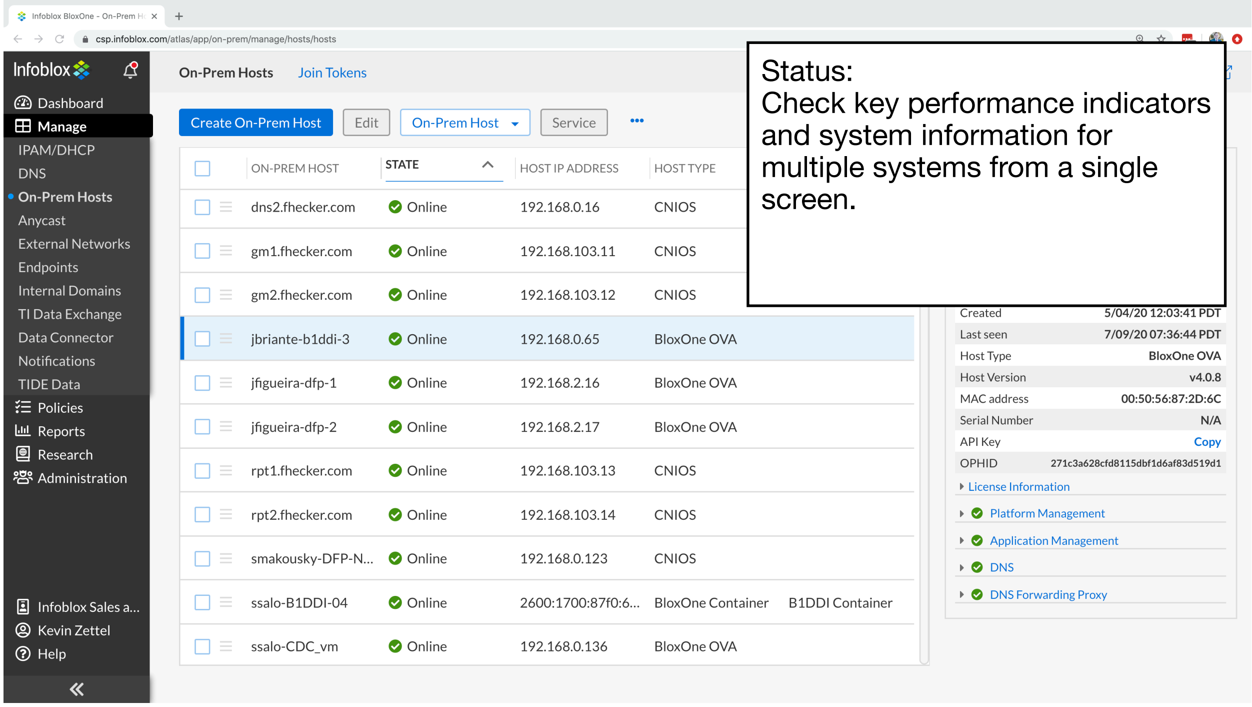
In the absence of centralized cloud management and control, the addition of a new site increases management complexity. Each site has its own management IP address, credentials and, perhaps, unique management interface (e.g. local web interface, terminal interface, etc). With cloud management and control this is not the case. Each new location is managed in the same manner as existing locations and is managed from the same "pane of glass" cloud management interface.

A quick look at the table below illustrates this very significant difference cloud and legacy device management. Each of the scenarios illustrates the benefits of unified cloud management. Key status, configuration, update and troubleshooting tasks can all be performed from a single portal within a single session using a single login. And, as also noted in the table, the Infoblox DDI can be deployed using whatever form factor best suits your needs and all can be managed via the same cloud administration interface.

On the next few pages, we'll provide a brief visual tour of these cloud management scenarios.

Cloud Management & Control: Proof Points

Scenario	Infoblox DDI	Legacy
Check Remote Device Status for Multiple Locations	Log in to one cloud platform for access to every device	Log in to each device individually
Configure DNS/DHCP Services	Log in to one cloud platform for access to every device	Log in to each device individually
Upgrade Software of a Group of Locations	Automatic with the ability to control upgrade timeline through one cloud portal	Log in to each device individually, download software, install software
Troubleshoot Multiple Locations	Run tests and traffic capture through the portal	Log in to each device individually
	Deployment Options	
Local DDI Options	**Infoblox DDI**	**Legacy**
Hardware Appliance	Available	Available
Virtual Appliance	Available	Vendor-dependent
Docker Container	Available	Vendor-dependent

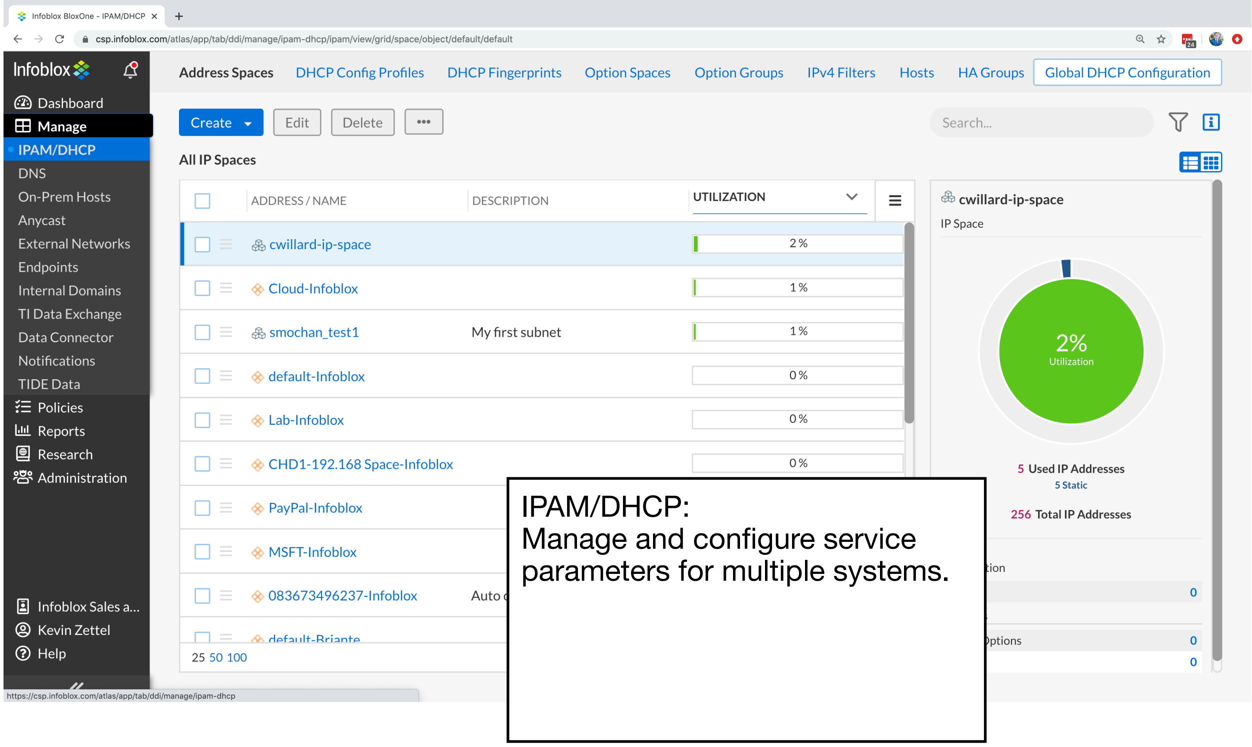


ON-PREM HOST	STATE	HOST IP ADDRESS	HOST TYPE	
dns2.fhecker.com	Online	192.168.0.16	CNIOS	
gm1.fhecker.com	Online	192.168.103.11	CNIOS	
gm2.fhecker.com	Online	192.168.103.12	CNIOS	
jbriante-b1ddi-3	Online	192.168.0.65	BloxOne OVA	
jfigueira-dfp-1	Online	192.168.2.16	BloxOne OVA	
jfigueira-dfp-2	Online	192.168.2.17	BloxOne OVA	
rpt1.fhecker.com	Online	192.168.103.13	CNIOS	
rpt2.fhecker.com	Online	192.168.103.14	CNIOS	
smakousky-DFP-N...	Online	192.168.0.123	CNIOS	
ssalo-B1DDI-04	Online	2600:1700:87f0:6...	BloxOne Container	B1DDI Container
ssalo-CDC_vm	Online	192.168.0.136	BloxOne OVA	

Created	5/04/20 12:03:41 PDT
Last seen	7/09/20 07:36:44 PDT
Host Type	BloxOne OVA
Host Version	v4.0.8
MAC address	00:50:56:87:2D:6C
Serial Number	N/A
API Key	Copy
OPHID	271c3a628cfd8115dbf1d6af83d519d1

- License Information
- ✓ Platform Management
- ✓ Application Management
- ✓ DNS
- ✓ DNS Forwarding Proxy

Status:
Check key performance indicators and system information for multiple systems from a single screen.



ADDRESS / NAME	DESCRIPTION	UTILIZATION
cwillard-ip-space		2 %
Cloud-Infoblox		1 %
smochan_test1	My first subnet	1 %
default-Infoblox		0 %
Lab-Infoblox		0 %
CHD1-192.168 Space-Infoblox		0 %
PayPal-Infoblox		
MSFT-Infoblox		
083673496237-Infoblox	Auto c	
default-Briante		

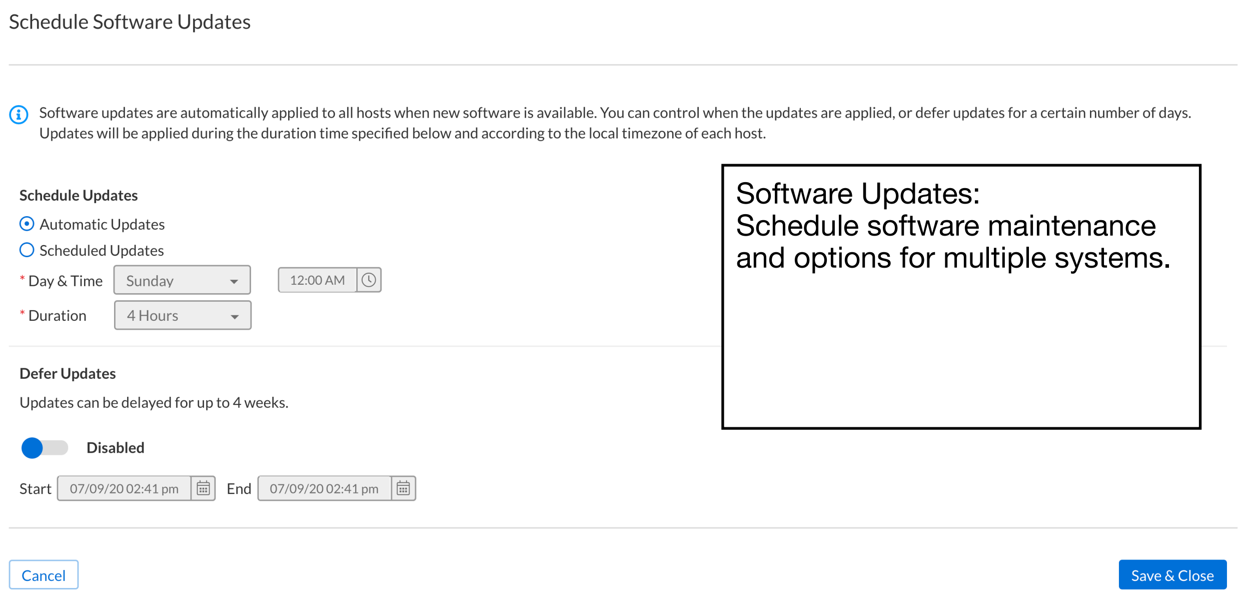
cwillard-ip-space
IP Space

5 Used IP Addresses
5 Static

256 Total IP Addresses

tion	
	0
ptions	0
	0

IPAM/DHCP:
Manage and configure service parameters for multiple systems.



Schedule Software Updates

ⓘ Software updates are automatically applied to all hosts when new software is available. You can control when the updates are applied, or defer updates for a certain number of days. Updates will be applied during the duration time specified below and according to the local timezone of each host.

Schedule Updates

● Automatic Updates

○ Scheduled Updates

* Day & Time: Sunday, 12:00 AM

* Duration: 4 Hours

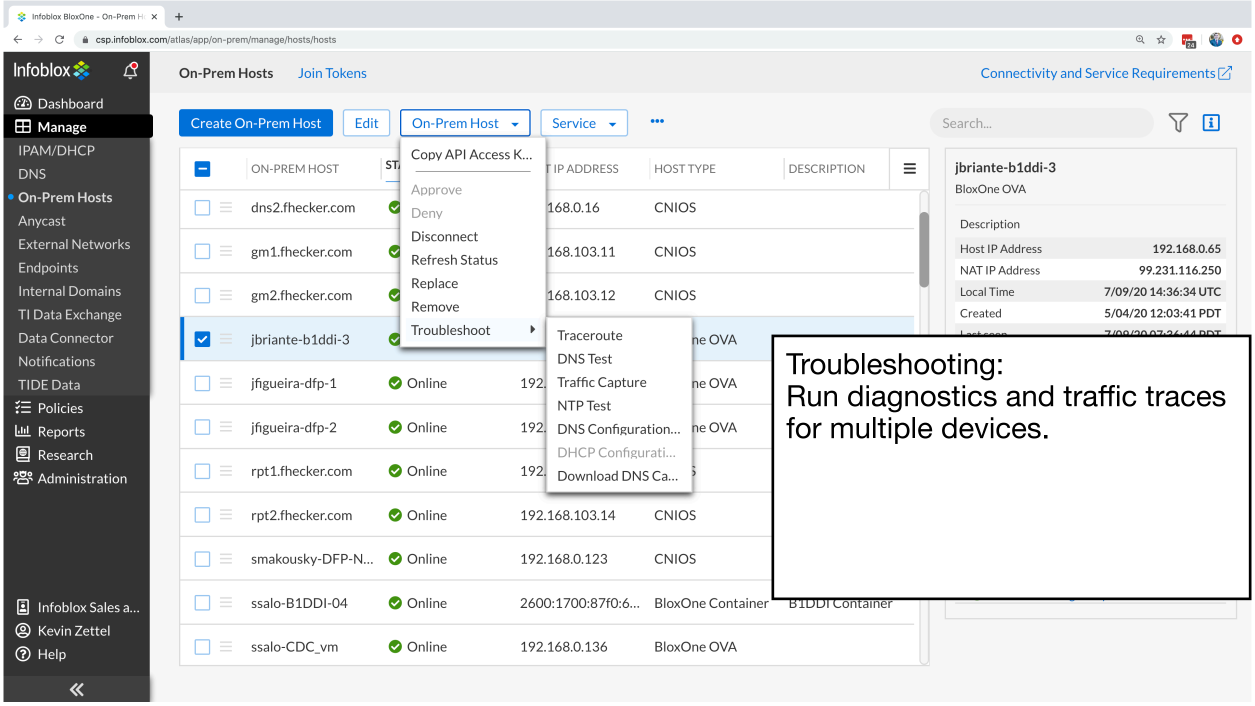
Defer Updates

Updates can be delayed for up to 4 weeks.

Disabled

Start 07/09/20 02:41 pm End 07/09/20 02:41 pm

Software Updates:
Schedule software maintenance and options for multiple systems.



Infoblox BloxOne - On-Prem H

csp.infoblox.com/atlas/app/on-prem/manage/hosts/hosts

	ON-PREM HOST	ST	IP ADDRESS	HOST TYPE	DESCRIPTION
☐	dns2.fhecker.com	✓	168.0.16	CNIOS	
☐	gm1.fhecker.com	✓	168.103.11	CNIOS	
☐	gm2.fhecker.com	✓	168.103.12	CNIOS	
☑	jbriante-b1ddi-3	✓		ne OVA	
☐	jfigueira-dfp-1	✓ Online	192.	ne OVA	
☐	jfigueira-dfp-2	✓ Online	192.	ne OVA	
☐	rpt1.fhecker.com	✓ Online	192.	S	
☐	rpt2.fhecker.com	✓ Online	192.168.103.14	CNIOS	
☐	smakousky-DFP-N...	✓ Online	192.168.0.123	CNIOS	
☐	ssalo-B1DDI-04	✓ Online	2600:1700:87f0:6...	BloxOne Container	B1DDI Container
☐	ssalo-CDC_vm	✓ Online	192.168.0.136	BloxOne OVA	

jbriante-b1ddi-3

BloxOne OVA

Description

Host IP Address	192.168.0.65
NAT IP Address	99.231.116.250
Local Time	7/09/20 14:36:34 UTC
Created	5/04/20 12:03:41 PDT

Troubleshooting:
Run diagnostics and traffic traces for multiple devices.

3 Mobility & Cloud Optimization

Benefit

Optimizing mobile, and distributed user experiences with SaaS and other business critical applications.

Situation

With back-hauled services, the target server (and, thus, the communication path) that the remote client will use to reach a cloud application, such as Microsoft Office 365, is determined by the DNS service running at the central location. This is true even when, for instance, the branch office and the back-hauled DNS server are situated on different continents.

Challenge/Exposure

Almost by definition, the centralized server handling back-hauled DNS will be less than optimally located for most of the distributed locations that it services. Thus, when it provides address resolution to the remote client, it will likely provide the address of a target server location that is closer to headquarters than it is to the distributed-office user. For example, if a user in NYC uses DNS services that are back-hauled to San Francisco for DNS resolution, it could be given an Office 365 in Washington State when Office 365 servers are available in the NY metro area. This results in additional latency (delay) throughout the entire session and a likely degradation of the user experience for the cloud application.

Solution

DNS services co-located with clients at the distributed location eliminates this problem. Because the server will be resolving the target server from the same location as the client, it will return a target server that is closest to the actual user thus optimizing the connectivity and improving the user experience of the cloud application.

Infoblox BloxOne DDI provides DNS services locally and delivers this optimization for each and every cloud application and cloud user individually.

Expand the Value of Network Services with Next-Level Security

Infoblox BloxOne Threat Defense works with your existing solutions to enhance the protection of your distributed SD-WAN, mobile, IoT, and cloud environment.

BloxOne Threat Defense powers Security Orchestration and Response (SOAR) solutions, to slash the time required to investigate and remediate cyberthreats, optimize the performance of the entire security ecosystem and reduces the total cost of enterprise security.

BloxOne Threat Defense leverages the BloxOne platform, and pairs up with BloxOne DDI to expand the value of core network services with foundational security for the distributed enterprise as well.

DDI services play a central role in all network communications. With Infoblox, they also enable your security stack to work in unison and at Internet scale to detect and anticipate threats sooner, well before your users are impacted.

Source: Infoblox

Proof Points

A simple "before" and "after" cloud application scenario provides all the proof that is needed of the performance benefits of local DDI. Our proof point example uses Microsoft Office 365 but the situation applies to any cloud application, such as Salesforce, ServiceNow and so forth. The table below sums up the situation.

Using central-site, back-hauled DNS that is geographically distant from your user's location will result in in the selection of a sub-optimal communications path. The path selected would be good for clients co-located with the DNS resource but not for the remote user. In our example, we have a client located in San Francisco with the central-site DNS located in Virginia. The result is a longer path, translating to greater latency (delay) and slower client interaction. However, when BloxOne DDI is activated at the client site, an optimal path is selected. Response time improves dramatically, not just for an initial "PING" but for the entire session. The visuals below illustrate "before" and "after."

Performance: Proof Points

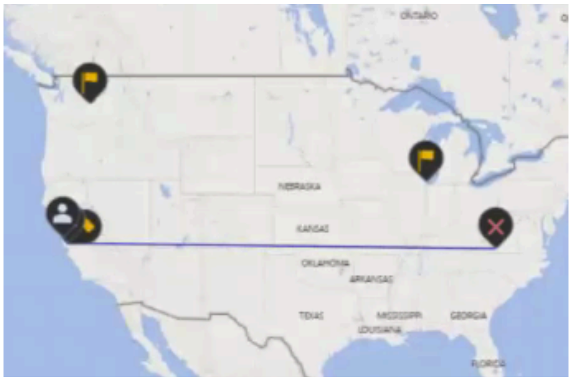
Scenario	Infoblox DDI	Legacy
Resolve Cloud Application Server	Resolves to target server closest to user	Resolves to target server near back-hauled central IT site
Application Latency/Performance	Improved. Test results showed "ping" time to Infoblox-selected server as 3 ms.	Degraded. Test results showed "ping" time to back-haul selected server much higher (worse) at 67 ms.

"Before" BloxOne DDI: Degraded Experience

Scenario:

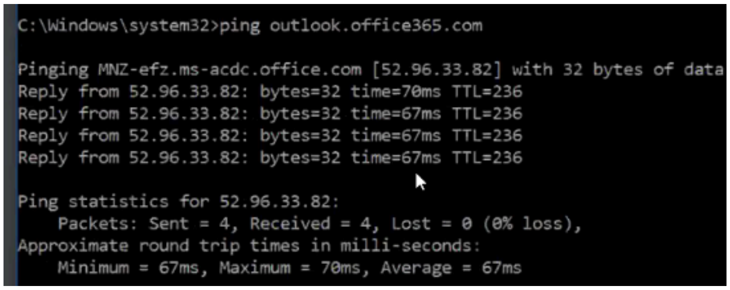
User based in San Francisco (person icon) with central-site DNS in Virginia (X).

Path from user to Office 365 is diverted "cross country."



Performance Hit:

"PING" connectivity test from SF user machine to Office 365 is slow taking an average of 67 ms.

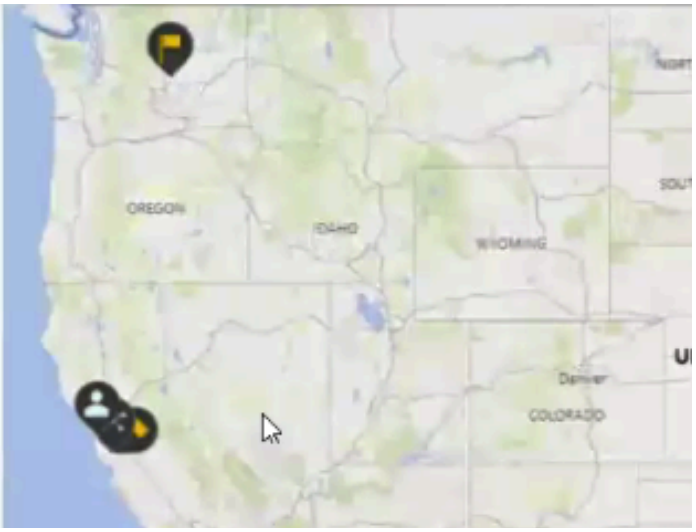

```
C:\Windows\system32>ping outlook.office365.com

Pinging MNZ-efz.ms-acdc.office.com [52.96.33.82] with 32 bytes of data
Reply from 52.96.33.82: bytes=32 time=70ms TTL=236
Reply from 52.96.33.82: bytes=32 time=67ms TTL=236
Reply from 52.96.33.82: bytes=32 time=67ms TTL=236
Reply from 52.96.33.82: bytes=32 time=67ms TTL=236

Ping statistics for 52.96.33.82:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 70ms, Average = 67ms
```

“After” BloxOne DDI is Implemented: Optimized Experience

Scenario:

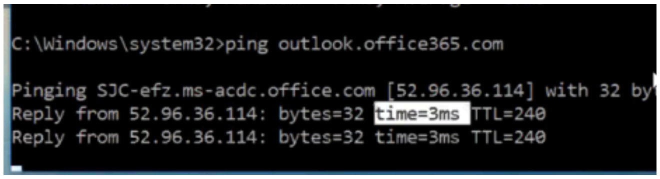
Local DNS activated (BloxOne DDI) at users local office.

Path from user to Office 365 is optimized to select nearest server.



Performance IMPROVEMENT:

“PING” connectivity test from SF user machine to Office 365 is fast - now taking an average of 3 ms.



```
C:\Windows\system32>ping outlook.office365.com

Pinging SJC-efz.ms-acdc.office.com [52.96.36.114] with 32 by
Reply from 52.96.36.114: bytes=32 time=3ms TTL=240
Reply from 52.96.36.114: bytes=32 time=3ms TTL=240
```

4 Distributed Site Survivability

Benefit

Local survivability of distributed locations when WAN links to centralized DDI services and applications are unavailable.

Situation

Oftentimes DDI services and critical business applications are centralized at the company headquarters or regional datacenter. This is a natural outgrowth of the traditional, hub-and-spoke networking architecture that has developed over decades. The distributed locations rely on the central site for all services, which are back-hauled over the central site link.

Challenge/Exposure

The WAN link (MPLS or internet link) between the central site and the distributed location must be up and operational in order for essential services to function. In the event of failure, the remote sites would lose their ability to resolve DNS names as well as for new stations to receive required IP addresses and address assignments to be managed. Thus, even if the distributed location had a separate internet connection to access non-corporate sites, it could lose its ability to function if it is unable to receive an address from the central datacenter. The location would not survive a failure of the link to the headquarters/central site location.

Solution

Having DDI services residing locally at each distributed site would eliminate dependence upon the central site and make the remotes survivable in the event of a link failure. Local network services would also reduce the traffic load on the link to the central site and improve the user experience at each distributed site. Infoblox BloxOne DDI provides these services.

Proof Points

The proof points with respect to survivability are self evident. With the link to the central site down, the centralized services are simply not available. In situations where the link to the central site is up but becomes congested, perhaps because other links are down or a backup was mistakenly started during business hours, it stands to reason that other traffic traversing that link (i.e. IP address requests) will be delayed and, thus, users will experience degradation in their session performance. See the table below for a summary of the situation with and without the Infoblox solution.

Survivability: Proof Points

Scenario	Infoblox DDI	Legacy
Link to Central Site Unavailable	All DDI services available locally. No interruption.	DDI services unavailable. User connectivity compromised.
Link to Central Site Congested	All DDI services available locally. No interruption.	DDI services available but user experience likely degraded.

5 Summary & Conclusion

The Tolly Group concludes that Infoblox BloxOne DDI greatly simplifies the management and control of today's distributed enterprise networks through:

Centralized Administration for anytime, anywhere management and control of DNS, DHCP, and IP Address Management for all distributed locations. Reducing administrative overhead, and improving efficiency.

Mobility & Cloud Optimization to ensure optimal performance of mobile, SaaS and other remote applications for all distributed sites, services and users. Here too, because "time is money," this optimization reduces wait time and improves productivity.

Distributed Site Survivability brings greater independence and service reliability to each distributed location as that location no longer is dependent upon a central datacenter for services.

The additional benefits including simplified deployments, streamlined operations, reduced TCO, and flexible physical or virtual deployment options provided by the BloxOne Platform, and Next-Level foundation security with BloxOne Threat Defense combine to enhance the overall value of this solution for IT organizations of all sizes and staffing levels.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for over 30 years.
Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
Tolly also assists medium-sized businesses and large enterprises evaluate, benchmark and select IT products for deployment.

You can reach the company by email at sales@tolly.com, or by telephone at
+1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

220120- jc-9—wt-2020-08-08—VerH