SOLUTION NOTE

INFOBLOX REPORTING & ANALYTICS QUERY LOGGING

SUMMARY

With DNS increasingly becoming a vital exploit path for malware and data exfiltration, security teams are often blind to the wealth of threat mitigation data available through their core networking infrastructure.

To gain access to this critical data, DNS query logging must be enabled; however, traditional query logging is extremely resource intensive and can impact critical DNS services. Infoblox Reporting and Analytics offloads and streamlines the process of collecting, archiving, reporting on, and sharing DNS query data, while ensuring minimal impact on the DNS infrastructure.

CHALLENGES OF DNS QUERY LOGGING

Many “do-it-yourself” DNS query logging solutions rely on operating system-level logging facilities such as Unix Syslog or Windows event logs. The problem with this approach is that in environments with high DNS query volumes, those logging facilities put a strain on the server resources resulting in a potential degradation to the DNS service (as well as other services being hosted on the system). This strain is generated because operating system logging facilities are not suited to handle hundreds or thousands of messages per second. The overhead of submitting the message to the logging facility, formatting the message, and associating the metadata results in unnecessary CPU and memory utilization.

Once this barrier is removed, the next challenge is around efficiently storing the data in a format that is easily searchable and provides redundancy. Only a couple of hundred queries per second can translate into multiple gigabytes of storage per day, which can add up to significant storage over months or years. Architecting a platform that ensures this unwieldy amount of data-on-disk is redundant, can be survive a disaster recovery event, and is readily searchable is also a huge undertaking.

With the appropriate infrastructure in place to collect the information, log data still needs to be parsed and searching/visualization tools need to be leveraged to be able to make use of the data. Even some enterprise-grade tools on the market can take days to return search results from these aforementioned monstrous datasets.

As you’ve likely already surmised, getting readily consumable DNS query logging data is substantially more difficult than simply turning on a logging feature on your DNS services. It is a considerable effort to architect a suitable and scalable platform, implement that platform, integrate the components, and develop the reports and visualizations. This effort has both CapEx and OpEx implications, and can take months if not years to complete.

INFOBLOX REPORTING AND ANALYTICS DNS QUERY LOGGING

Infoblox Reporting and Analytics DNS Query Logging simplifies the effort of architecting and deploying a suitable query logging infrastructure and can be implemented in as little as 20 minutes. Instead of cobbling together a complex and costly “do-it-yourself” approach, leverage Infoblox to remove the complexity of DNS query logging. Infoblox removes this complexity with a solution that:

1. Efficiently collects DNS query data
2. Provides a robust data transmission and archival infrastructure
3. Provides ready-to-use reports, all within a single unified platform!

Efficient DNS Query Data Collection:

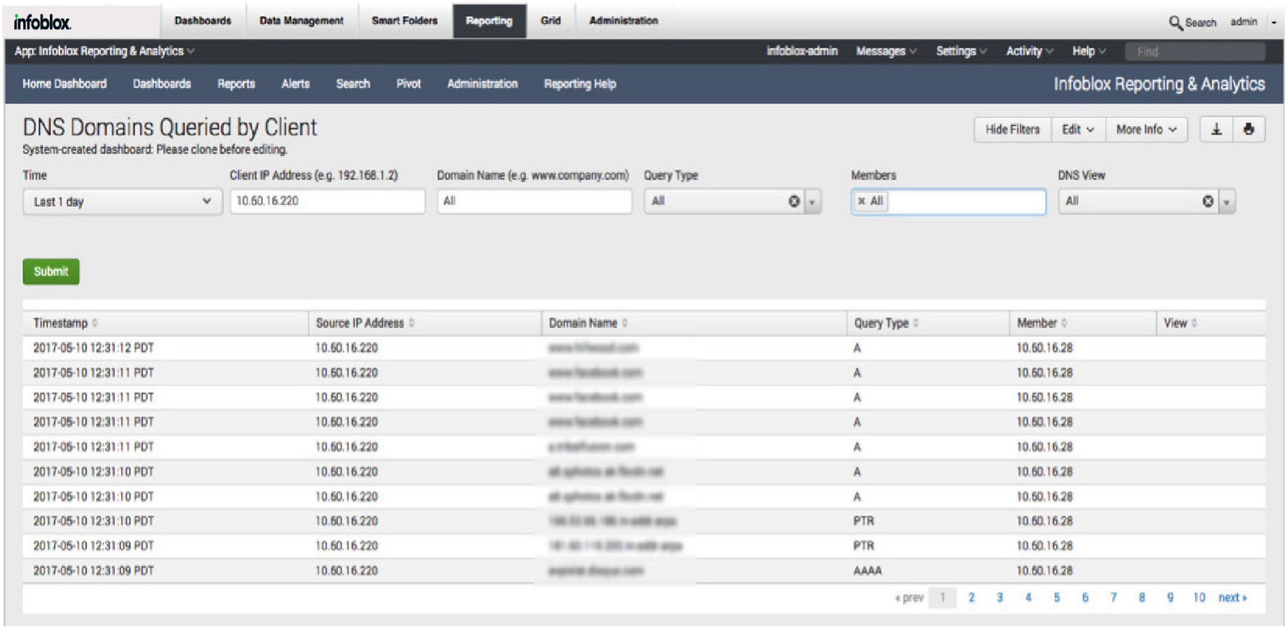
Infoblox DNS appliances utilize a customized message handling mechanism to extract DNS query data directly from the DNS daemons, bypassing the OS-based logging mechanisms. This reduces the operating system overhead by up to 80 percent, which reduces the risk of impacting critical DNS services.

Robust Data Transmission and Archival:

Infoblox Reporting and Analytics Query Logging solution leverages guaranteed delivery messaging systems, high efficiency databases, and distributed storage-based clustering technologies. This ensures your DNS log data is thoroughly captured and it’s always accessible, which is especially critical for security and forensic analysis.

Ready-to-use Reports:

Infoblox extracts the relevant data from the raw DNS query logs and provides ready to use reports that allow you to get the information you need in seconds. Infoblox’s reporting platform is highly customizable, allowing you to create new views and get new insights into your data. Furthermore, Infoblox has built a community around customized reports and visualizations, so new report templates that address real world problems are constantly being submitted to the community by DNS experts from around the world.



DNS Domains Queried by Client

System-created dashboard: Please clone before editing.

Time: Last 1 day

Client IP Address (e.g. 192.168.1.2): 10.60.16.220

Domain Name (e.g. www.company.com): All

Query Type: All

Members: All

DNS View: All

Timestamp	Source IP Address	Domain Name	Query Type	Member	View
2017-05-10 12:31:12 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:11 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:11 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:11 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:11 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:10 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:10 PDT	10.60.16.220	[redacted]	A	10.60.16.28	
2017-05-10 12:31:10 PDT	10.60.16.220	[redacted]	PTR	10.60.16.28	
2017-05-10 12:31:09 PDT	10.60.16.220	[redacted]	PTR	10.60.16.28	
2017-05-10 12:31:09 PDT	10.60.16.220	[redacted]	AAAA	10.60.16.28	

Figure 1: Infoblox’s supplied “DNS Domains Queried by Client” reports; Demonstrates searching for all DNS queries made by a specific client.

SCALABILITY AND FLEXIBILITY

With a clustering implementation, Infoblox's Reporting and Analytics Query Logging solution is capable of horizontally scaling. As DNS loads increase, or retention requirements change, adding cluster members supplies the necessary resources to meet the need.

Infoblox Reporting and Analytics Query Logging is licensed based on the volume of data being logged. To provide maximum flexibility, the solution can be licensed in a subscription model. This subscription model creates savings by allowing you to right size your licensing. If you exceed the licensed indexing capacity, you can simply upgrade to the next subscription tier. Additionally, this subscription model permits you to use as many Infoblox virtual appliances as necessary to meet your scaling needs on both the data indexing (ingestion) and data retention sides, as well as upgrade to the latest and greatest virtual models at any time.

LEARN MORE

Learn more about the solution at https://www.infoblox.com/products/reporting-analytics.

ABOUT INFOBLOX

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

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: 20230919v1