



**DEPLOYMENT GUIDE** 

# **INFOBLOX NIOS & VENDORN VISION DEPLOYMENT GUIDE**

# **TABLE OF CONTENT**

OVERVIEW	3
HOW IT WORKS	3
CONFIGURATION	4
SYSLOG	.4
INFOBLOX DATA CONNECTOR	.6
DNSTAP	.7

### **OVERVIEW**

Infoblox NIOS and VendorN Vision work together in providing organizations with long-term access to enterprise DNS log history, providing a current unparalleled view into your DNS data and context. Once aggregated, your DNS data can then be fed into your SIEM or SOAR platforms to enhance security operations and improve effectiveness. The VendorN Vision platform drives value from DNS data in a host of ways:

#### **Discover New Connections**

Vision has been designed with a "what has changed" philosophy, so new data can be easily identified using simple filtering and sorting.

### **Prioritize Data**

Groups can be created for critical networks and devices so that DNS data and events can be quickly identified and prioritized.

### **Navigate History**

Instantly and easily understand which devices have performed which queries and which records these queries have resolved to.

## **HOW IT WORKS**

Vision receives DNS query and response logs from Infoblox NIOS Grid DNS servers. It aggregates and stores this data while also optionally sending events and aggregated DNS data to an organization's SIEM. An organization can also use its SOAR and other systems to query the Vision API to access DNS activity history data. When sending data to Vision, NIOS has a comprehensive suite of features which can be used, these are Syslog, the Infoblox data connector and DNSTAP:



The CONFIGURATION section contains a sub-section documenting how each of these methods are configured in the Infoblox NIOS platform.

### CONFIGURATION

#### **SYSLOG**

With the Syslog method, NIOS Grid DNS servers are configured to forward their Syslogs to a Vision Sensor. Note: Query and response logging must be enabled on the DNS servers.

To configure the Syslog method in Infoblox NIOS use the following steps:

1. Once the Infoblox NIOS user interface has been accessed, navigate to the Grid / Grid Manager / Members page:

Infoblox 📚		Dashboards Data Management Smart Folders Grid Administration
		Grid Manager Upgrade Licenses HSM Group
Finder	~	Infoblox 🔳 🖉 📮
Smart Folders	+	DHCP DNS TFTP HTTP (File Dist) FTP DFP NTP bloxTools Captive Portal Subscriber Collection
Bookmarks	+	Visualization Members Services
Recycle Bin	+	Orlick Filter On Show Filter Of Replication Status View
URL Links	+	
		Group Results Group By Choose one
		+   ∅'   ē   ≔   ≖   <b>Ξ</b>   <b>Ξ</b>   <b>Ξ</b> -   ⊖
		🖹 🗏 Name HA Status
		🗹 🗏 🔶 Infoblox.localdomain No Running

2. Select a member and click the "edit" button displayed in the table toolbar to edit the member properties:

gle Basic Mode	Basic	c Advanx	bed							
General CSP Config	SYSLO	G								
es K	*Syslog	) Size (MB)	300		0	nce the syslog file new one. For Low	reaches this size Disk(60G)Image	t, the syslog ser s rotation size in	ver rotates the file and opens s syslog size(MB)/3.	Inheri
w ly tesolver	Log to I Servers	External Syslog								
oring	EXTERN	NAL SYSLOG S	ERVERS						+1211	
Backup	🗖 Ad	Idress	Transport	Interface	Source	Node ID	Port	Severity	Category	
Thrashold	E 19	92.168.0.111	TCP	Any	Internal	LAN	8514	Debug	DNS Queries, DNS Responses	
ations										
isions										

- 3. Under the Monitoring / Basic tab make the following changes and save and close the dialog:
  - a. Check the "Log to External Syslog Servers" checkbox.
  - b. Add a Vision Sensor under the "EXTERNAL SYSLOG SERVERS" table, ensuring TCP port 8514 is specified and ensure "Category" is set to "DNS Queries" and "DNS Responses".

4. Next, navigate to the Data Management / DNS / Members page:



5. Select a member and click the "edit" button displayed in the table toolbar to edit the member DNS properties:

infoblox.localdomain (	Member DNS Propertie	s)		
C Toggle Basic Mode	Basic Advance	bed		
General				
DNS Views	Logging Facility	DAEMON Y		Override
Forwarders	Inherited from Grid Infob	lox		
Updates				
Queries	Logging Category	Log these categories of r	nessages	Tehnuit
Zone Transfers	general	client	resolver	and the second
Root Name Servers				
Sort List		Connig	responses	
Blackhole		🗹 database	🗌 rpz	
Logging				
Host Naming		dnssec	security	
GSS-TSIG			T transfor in	
DNSSEC		<ul> <li>Idme servers</li> </ul>	Vansier-in	
Blacklist		network	✓ transfer-out	
DNS64				
RRset Order		notify	🗹 update	
Security		austice.	🗾 undala socuritu	
Permissions		duenes	Update-security	
		query rewrite	DTC health monitors	
		🛃 rate-limit	DTC load balancing	
	4		_	
	Concerning and the second			
Cancel				Save & Close •

- 6. Under the Logging / Basic tab make the following changes and then save and close the dialog:
  - a. Check the "queries" checkbox.
  - b. Check the "responses" checkbox.
- 7. Once saved, a service restart of the DNS server will be required for the changes to take effect.

Following this, NIOS Grid DNS servers will log query and response messages to their local Syslog which is then forwarded to the Vision Sensor in real-time.

•

#### **INFOBLOX DATA CONNECTOR**

With the Infoblox Data Connector method, NIOS Grid DNS servers are configured to periodically send files to a Vision Sensor which contain similar query and response messages to the Syslog method but using SCP.

To configure the Infoblox Data Connector method in Infoblox NIOS use the following steps:

1. Once the Infoblox NIOS user interface has been accessed, navigate to the Data Management / DNS / Members page:

Infoblox 📚		Dashboards Data Management Smart Folders Grid Administration
default	~	PAM VLANs Super Host DHCP DNS File Distribution
Finder	«	Zones Members Name Server Groups Shared Record Groups Subscriber Services Deployment
Smart Folders	+	Quick Filter None V Orr Filter On Show Filter
Bookmarks	+	
🚡 Recycle Bin	+	Group Results Group By Choose one
🔚 URL Links	+	$\rightarrow   \mathcal{C}   \perp \cdot   \ominus$
		Ten Status
		🗹 🚍 

2. Select a member and click the "edit" button displayed in the table toolbar to edit the member DNS properties:

Basic Mode	Basic Advanced			
	DNSTAP settings for DNS Qu	eries/Responses		
ws MS	DNSTAP Queries/Responses	s supports when ADP/DCA is	i Enabled.	
	Queries Responses			
	*DNSTAP Receiver Address	109.155.124.193		
nsfors no Sorvers	*DNSTAP Receiver Port	6000		
	Inherited from Grid Infohiov			
	Data connector for all DNS Q	ueries/Responses to a Dor	nain	
	Capture DNS Queries	Capture DNS Responses	1	
	Capture queries/n	esponses for all domains		
	O LIMIT CAPTURE 1	O THESE DOMAINS		+-18
rder	Domain			
	No data			
ons				
	EXCLUDE THE FOL	LOWING DOMAINS		+- 8
	Domain			
	No data			
	C Pathle contrast and	and an all share the local d		
	Event to	enesireplies on the local o	154	
	Export to	SCP.		
	TCP port	8022		
	"Directory Path	1		
	*Server Address	192.168.0.111		
	"Username	Ignored		
	Password			

- 3. Under the Logging / Advanced tab, make the following changes and then save and close the dialog:
  - a. Check the "Capture DNS Queries" checkbox.
  - b. Check the "Capture DNS Responses" checkbox.
  - c. Check the "Capture queries/responses for all domains" radio button.
  - d. Uncheck the "Retain captured queries/replies to the local disk" checkbox.
  - e. Set "Export to" to "SCP".
  - f. Set "TCP port" to "8022".
  - g. Set "Directory Path" to "/".
  - h. Set "Server Address" to be the Vision Sensors IP address.
  - i. Set "Username" and "Password" to "ignored" the Vision Sensor will refuse connections from devices it has not been configured with, the username and password specified is ignored by the sensor.
- 4. Once saved, a service restart of the DNS server will be required for the changes to take effect.

Following this, NIOS Grid DNS servers will log query and response messages to a local file which is then forwarded to a Vision Sensor periodically.

### **DNSTAP**

With the dnstap method, NIOS Grid DNS Servers are configured to forward DNS queries and responses to a Vision Sensor using the dnstap protocol.

To configure the dnstap method in Infoblox NIOS, take the following steps:

1. Once the Infoblox NIOS user interface has been accessed navigate to the Data Management / DNS / Members page:



2. Select a member and click the "edit" button displayed in the table toolbar to edit the member DNS properties:

infoblox.localdomain	(Member DNS Properties)	
C Toggle Basic Mode	Basic Advanced	
General DNS Views Forwarders	DNSTAP settings for DNS Queries/Responses DNSTAP Queries/Responses supports when ADP/DCA is Enabled.	
Updates Queries Zone Transfers Root Name Servers Sort List Blackhole	Queries         Responses           *DNSTAP Receiver Address         192.168.0.111           *DNSTAP Receiver Port         6000	
<ul> <li>Logging</li> <li>Host Naming</li> <li>GSS-TSIG</li> </ul>	Data connector for all DNS Queries/Responses to a Domain Capture DNS Queries Capture DNS Responses	Inherit
DNSSEC Blacklist DNS64 Reset Order	Capture queries/responses for all domains LIMIT CAPTURE TO THESE DOMAINS	
Permissions	No data	•
Cancel		Save & Close

- 3. Under the Logging / Advanced tab make the following changes and then save and close the dialog:
  - a. Check the "Queries" checkbox.
  - b. Check the "Responses" checkbox.
  - c. Set "DNSTAP Receiver Address" to the Vision Sensors IP address.
  - d. Set "DNSTAP Receiver Port" to "6000".
- 4. Once saved, a service restart of the DNS server will be required for the changes to take effect.

Following this, NIOS Grid DNS servers will send DNS query and response messages to a Vision Sensor in real-time.

# 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

G 💥 in

0)

@ 2024 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

Version: 20240322v1