

# How to - Configure Infoblox DDI to forward logs to EventTracker EventTracker v9.0 and above

Publication Date: February 24, 2020

### Abstract

This guide provides instructions how to configure Infoblox DDI to forward relevant logs to EventTracker.

#### Scope

The configurations detailed in this guide are consistent with **EventTracker** version 9.x and later, **Infoblox DDI NIOS** version 7.x and later.

### Audience

Administrators who want to monitor the Infobiox DDI using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## Table of Contents

1.	0	verview	3
	1.1	Prerequisites	3
2.	Сс	onfiguring Infoblox to send syslog to EventTracker	3



### 1. Overview

Infoblox DDI is a critical technology with DNS, DHCP, IPAM functionalities which provides maximum protection and offers minimum attack surface.

Infoblox DDI is a critical technology with DNS, DHCP, IPAM functionalities which provides maximum protection and offers minimum attack surface.

Infoblox DDI forward logs to EventTracker via syslog. EventTracker receives DNS, DHCP, and IPAM logs from Infoblox DDI. EventTracker Infoblox DDI report provides information about DHCP IP assignment and DHCP IP lease expires for systems. By using these reports, for e.g. we can track events of clients receiving suspicious responses by using the DNS response policy zone. With the help of these reports, object related activities such as, a new object creation, old objects modified or deleted.

Dashboards display a graphical representation about object management, user logon activities, DHCP activities. For e.g. Object management events include, new object (DHCP range, A record, MX record, etc.) creation, existing object modified or deleted.

Alerts are triggered when a user performs any of the following activities: new object creation, old objects modified or deleted, user login failed, etc.

### 1.1 Prerequisites

- EventTracker v9.x or later should be installed.
- Infoblox Grid Manager with NIOS version 7.0.X and later.

### 2. Configuring Infoblox to send syslog to EventTracker

All Infoblox devices are managed using Infoblox Grid Manager.

1. Logon to Infoblox Grid Manager using valid credentials.

<b>Grid Manager</b> Disconnect NOW if you have not been expressly authorized to use this system.
Username Password Login



2. Navigate to Grid>Grid Manager>Members to access active grid member settings.

Infoblox 📚	Dashboards	Data Management	Smart Folders	Grid Administration
	Grid Manager	Upgrade Lice	nses HSM Group	
🚡 Infoblox 💶 🖍 📮				
DHCP DNS TFTP	HTTP (File Dist)	FTP NTP b	loxTools Captive Portal	Subscriber Collection
Members Services				
Quick Filter None	✓ Off Filter	On Show Filte	r Off <u>Replication Statu</u>	is View
Group Results Gr	roup By Choose on	e	× +	
+ ♂ ڨ ≡ ∞	🖽   🕹 •   🖶			



3. Click on the icon to show available options for selected grid members.



### Configure Infoblox DDI to forward logs to EventTracker

Infoblox 📚	Dashboards	Data Management	Smart Folders	Grid Adminis	stration		
	Grid Manager	Upgrade Licenses	HSM Group				
> Infobiox • • •	HTTP (File Dist)	FTP NTP bloxTool	ls Captive Portal	Subscriber Col	ection		
Members Services							
Quick Filter None	• Off Filter (	On Show Filter	Off <u>Replication Stat</u>	tus View			
Group Results Gr	roup By Choose one	•	+				
+   🗹   🚺 🛛 🔤	🖽 i 🌲 🚽 🖶						
Delete	HÅ -	STATU S	IPV4 ADDRESS	IPV6 ADDRESS	IDENTIFY	DHCP	DNS
Extensible A	Attributes Llocalde No S	Running	192.168.100.10		Unsupported	•	•
Generate To View Toker	oken 1						



4. Click on Edit to change options for selected Grid Member.

Grid Member Properties Editor pane is shown.

infoblox.localdomain (Grid I	Member Properties	Editor)								×
C Toggle Basic Mode	Basic Advan	ced								0
General Licenses	SYSLOG									^
Network Anycast	*Syslog Size (MB)	300			Once the syslog file server rotates the fil	reaches this size, e and opens a nev	the syslog v one.		Inherit	
Security DNS Resolver Monitoring	Log to External Syslog Servers	, 🗹								
Syslog Backup	EXTERNAL SYSLOG SE	RVERS					+   🖻	Î		
SNMP	ADDRESS	TRANSPORT	INTERFACE	SOUR	CE NODE ID	PORT	SEVERITY	CATE		
SNMP Threshold		тср	Any	Any	LAN	514	Debug	AI		
Notifications     Email		ТСР	Any	Any	LAN	514	Debug	AI		
Extensible Attributes		тср	Any	Any	LAN	514	Debug	Al 🗸		
Permissions	<							>		
										¥
Cancel									Save & Clos	e •

#### Figure 4

5. Select **Monitoring** and then click **Override** to enable customization of syslog settings.



#### Configure Infoblox DDI to forward logs to EventTracker

V Toggie Basic mode	Basic Ad	lvanced							
General Licenses	SYSLOG								
Network Anycast	*Syslog Size (MB)	300		Onc	e the syslog file rover rotates the file	eaches this size and opens a ne	, the syslog w one.		Inherit
Security DNS Resolver	Log to External Sy	rslog 🗹							
Monitoring	Servers	C SEDVEDS							
SNMP	ADDRESS	TRANSPORT	INTERFACE	SOURCE	NODE ID	PORT	SEVERITY	CATE	
NMP Threshold		тср	Any	Any	LAN	514	Debug		
otifications mail		тср	Any	Any	LAN	514	Debug	AI	
stannikla Attributan		тср	Any	Any	LAN	514	Debug		
Attributes									

#### Figure 5

- 6. Select the checkbox beside Log to External Syslog Servers to enable syslog logging.
- 7. Click the icon 📥 beside **External Log Servers** section to add new remote syslog server.
- 8. Fill the required details in Add External Syslog Server pane. As suggested below:
  - Address Fill in the IP address of syslog server
  - Transport Select UDP
  - Interface Select Any from the dropdown
  - Node ID Select LAN from drop-down
  - Source Select Any from drop down menu
  - Severity Select Info from the drop-down menu
  - Port Type 514
  - Logging Category Select Send All

# Netsurion... EventTracker\*

### Configure Infoblox DDI to forward logs to EventTracker

Toggle Basic Mode	Basic Ad	ivanced						
General		Availabl	e		Selected			
licenses		Threa	t Protection	^			~	
Network		Active	Directory Aut	henti				
Anycast		Comm	on Authenticat	ion	>			
Security		LDAP	Authentication					
ONS Resolver		Non-s	ystem Authent	icatic	<			
Ionitoring		TACA	CS Authentical	tion				
yslog Backup		ULAPI	Authentication	*			$\sim$	
NMP								_
MP Threshold						Cano	el Test	Add
tifications	ADDRESS	TRANSPORT	INTERFACE	SOURCE	NODE ID	PORT	SEVERITY	CATE
nail		TCP	Anv	Any	LAN	514	Debug	
xtensible Attributes			-	-			-	
ermissions		TCP	Any	Any	LAN	514	Debug	All
		TCP	Any	Any	LAN	514	Debug	AI 🗸
	1							

Figure 6

9. Click Add to confirm the configuration.
10. Click Save & Close To save the syslog configuration.

