Integrate Infoblox DDI with EventTracker
EventTracker v9.0 and above

Publication Date: February 24, 2020
Abstract

This guide provides instructions 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 Infoblox DDI using EventTracker.
# Table of Contents

1. Overview .................................................................................................................................................. 3  
   1.1 Prerequisites .................................................................................................................................. 3  
2. Configuring Infoblox to send syslog to EventTracker ....................................................................... 3  
3. EventTracker Knowledge Pack (KP) ................................................................................................. 7  
   3.1 Saved Searches ............................................................................................................................... 7  
   3.2 Alerts .............................................................................................................................................. 8  
   3.3 Reports .......................................................................................................................................... 8  
   3.4 Dashboards ..................................................................................................................................... 11  
   3.5 Event Filters ................................................................................................................................... 13  
4. Importing knowledge pack into EventTracker .................................................................................. 13  
   4.1 Saved Searches ............................................................................................................................... 14  
   4.2 Alerts .............................................................................................................................................. 15  
   4.3 Token Templates .............................................................................................................................. 16  
   4.4 Flex Reports ................................................................................................................................... 18  
   4.5 Knowledge Objects ........................................................................................................................ 19  
   4.6 Dashboards ..................................................................................................................................... 21  
   4.7 Event Filters ................................................................................................................................... 22  
5. Verifying knowledge pack in EventTracker ....................................................................................... 23  
   5.1 Saved Searches ............................................................................................................................... 23  
   5.2 Alerts .............................................................................................................................................. 24  
   5.3 Token Templates .............................................................................................................................. 24  
   5.4 Flex Reports ................................................................................................................................... 25  
   5.5 Knowledge Objects ........................................................................................................................ 25  
   5.6 Dashboards ..................................................................................................................................... 26  
   5.7 Event Filters ................................................................................................................................... 26
1. Overview

Applies To: Infoblox DDI (DHCP, DNS, and IPAM) with NIOS version 7.0.x and later.

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

Infoblox DDI forwards 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 expiration of the systems.

These reports help to track, client’s events receiving suspicious responses by the DNS response policy zone.

Dashboards display a graphical representation of the 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 modification or deletion.

Alerts are triggered when a user performs any of the following activities: new object creation, old objects modification or deletion, user login fails, 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.
2. Navigate to Grid>Grid Manager>Members to access active grid member settings.

3. Click on the icon to show available options for selected grid members.
Integrate Infoblox DDI with EventTracker

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

Grid Member Properties Editor pane is shown.

5. Select **Monitoring** and then click **Override** to enable customization of syslog settings.
Integrate Infoblox DDI with EventTracker

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 drop-down
   - **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

Figure 5
9. Click **Add** to confirm the configuration.
10. Click **Save & Close** to save the syslog configuration.

3. **EventTracker Knowledge Pack (KP)**

Once logs are received into EventTracker, Alerts, and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker v9.x and later to support Infoblox monitoring.

3.1 Saved Searches

- **Infoblox DDI: Object management activities** - This saved search provides information related to the object created, deleted and modified.
- **Infoblox DDI: DHCP activities** – This saved search provides information related to the assignment and renewal of IP address to a system, release of IP address from a system, and expire of lease-duration of IP address of a system.
- **Infoblox DDI: Threat detection activities** – This saved search provides information related to the attacks are happening on DNS servers. For e.g. potentially DDoS related site detected.
- **Infoblox DDI: User logon activities** – This saved search provides information related to Infoblox DDI user login allowed, user login denied, and user logout.
• **Infoblox DDI: DNS response policy zone activities** – This saved search provides information related to Infoblox DDI you can create policies for how to handle specific queries (or responses) and choose which of a number of possible actions to take.

### 3.2 Alerts

- **Infoblox DDI: High CPU Usage Detected** – This alert is generated when CPU usage is critical.
- **Infoblox DDI: High Disk Usage Detected** – This alert is generated when disk space usage is critical.
- **Infoblox DDI: High Memory Usage Detected** – This alert is generated when memory usage is critical.
- **Infoblox DDI: Object created deleted and modified** – This alert is generated when an object (DHCP range, A record, etc.) is in, deleted or modified.
- **Infoblox DDI: User login failed** – This alert is triggered when a user tries to login but fails. For e.g. Incorrect username or password. (e.g. user tries to login from GUI).

### 3.3 Reports

- **Infoblox DDI - User login failed** – This report provides information related to user login failed which includes device address, username, group name, source address, console type, logon status, reason, and authentication type fields.

  **Sample_Report**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Login Console Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/19/2020 12:48:46 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>martz</td>
<td>10.20.1.186</td>
<td>GUI</td>
</tr>
<tr>
<td>02/19/2020 12:48:56 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>brucew</td>
<td>10.20.1.137</td>
<td>Direct</td>
</tr>
<tr>
<td>02/19/2020 12:49:07 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>maya</td>
<td>10.20.1.137</td>
<td>Direct</td>
</tr>
<tr>
<td>02/19/2020 12:49:36 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>kenneth</td>
<td>10.20.1.186</td>
<td>GUI</td>
</tr>
<tr>
<td>02/19/2020 12:49:43 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>admin</td>
<td>10.20.1.186</td>
<td>Direct</td>
</tr>
<tr>
<td>02/19/2020 02:38:10 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>martz</td>
<td>10.20.1.186</td>
<td>GUI</td>
</tr>
<tr>
<td>02/19/2020 04:26:52 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>frantz</td>
<td>10.30.1.10</td>
<td>GUI</td>
</tr>
<tr>
<td>02/19/2020 05:11:03 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>kenneth</td>
<td>10.30.1.10</td>
<td>Direct</td>
</tr>
<tr>
<td>02/19/2020 05:16:51 AM</td>
<td>10.20.1.181-SYSLOG</td>
<td>martin</td>
<td>10.30.1.10</td>
<td>GUI</td>
</tr>
</tbody>
</table>

  **Log_Sample**

Feb 19 00:48:46 10.8.9.18 Feb 19 08:48:45 12.68.10.10 httpd: 2020-02-19 08:48:45.303Z [martz]: Login_Denied - - to=AdminConnector ip=12.68.10.18 info=Local apparently_via=GUI

- **Infoblox DDI - User login and logout** - This report provides information related to user login and logout success which includes device address, username, group name, source address, console type, logon status, reason, and authentication type fields.
Integrate Infoblox DDI with EventTracker

Sample_Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Group Name</th>
<th>Source IP Address</th>
<th>Authentication Type</th>
<th>Connecting To</th>
<th>Login Console Type</th>
<th>User Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/18/2020 03:28:27 AM</td>
<td>admin</td>
<td>admin-group</td>
<td>172.26.9.166</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Session/04:06:00</td>
</tr>
<tr>
<td>02/18/2020 03:51:25 AM</td>
<td>admin</td>
<td>admin-group</td>
<td>172.26.9.166</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Session/04:06:00</td>
</tr>
<tr>
<td>02/18/2020 03:54:49 AM</td>
<td>admin</td>
<td>admin-group</td>
<td>172.26.9.166</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Session/04:06:00</td>
</tr>
<tr>
<td>02/19/2020 04:19:22 AM</td>
<td>admin</td>
<td>admin-group</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Normal/04:06:00</td>
</tr>
<tr>
<td>02/19/2020 04:20:54 AM</td>
<td>admin</td>
<td>admin-group</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Normal/04:06:00</td>
</tr>
<tr>
<td>02/15/2020 04:23:01 AM</td>
<td>kenneth</td>
<td>kenneth</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>System/04:06:00</td>
</tr>
<tr>
<td>02/15/2020 04:23:05 AM</td>
<td>kenneth</td>
<td>kenneth</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>System/04:06:00</td>
</tr>
<tr>
<td>02/18/2020 04:23:17 AM</td>
<td>kenneth</td>
<td>kenneth</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Normal/04:06:00</td>
</tr>
<tr>
<td>02/18/2020 04:26:26 AM</td>
<td>franz</td>
<td>admin-group</td>
<td>172.26.10.10</td>
<td>LOCAL</td>
<td>Admin Connector</td>
<td>GUI</td>
<td>Login_Allowed</td>
<td>Normal/04:06:00</td>
</tr>
</tbody>
</table>

Log_Sample


- **Infoblox DDI – Threat detection detail** – This report provides information related to suspicious URLs detected as DDoS activities, severity, IP address, port number, etc.
- **Infoblox DDI – DNS query and responses** – This report provides information related to client requested queries and server responses, IP address, URL address, and record type.

Sample_Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Record Type</th>
<th>Source IP Address</th>
<th>Client IP Address</th>
<th>Client Port</th>
<th>Query</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/18/2020 02:19:10 PM</td>
<td>172.26.9.168-SYSLOG</td>
<td>WA</td>
<td>192.168.100.10</td>
<td>192.168.100.47</td>
<td>12818</td>
<td>2.centos.pool.ntp.org</td>
<td>SERVFAIL</td>
</tr>
<tr>
<td>02/18/2020 02:19:10 PM</td>
<td>172.26.9.168-SYSLOG</td>
<td>WA</td>
<td>192.168.100.10</td>
<td>192.168.100.47</td>
<td>12818</td>
<td>2.centos.pool.ntp.org</td>
<td>SERVFAIL</td>
</tr>
<tr>
<td>02/18/2020 02:19:10 PM</td>
<td>172.26.9.168-SYSLOG</td>
<td>WA</td>
<td>192.168.100.10</td>
<td>192.168.100.47</td>
<td>12814</td>
<td>3.centos.pool.ntp.org</td>
<td>SERVFAIL</td>
</tr>
</tbody>
</table>

Log_Sample

Feb 20 00:40:01 12.2.9.81 Feb 20 08:40:00 12.18.10.10 named[7365]: client @0x7f02d84f9e10 12.18.10.47#55607 (2.centos.pool.ntp.org.silocal): query failed (SERVFAIL) for 2.centos.pool.ntp.org.silocal/IN/AAAA at query.c:12307

- **Infoblox DDI – DNS response policy zone threat detail** – This report provides information related to Infoblox DDI to create rules for handling specific queries, IP address, port details, Severity level, URL address, etc.
- **Infoblox DDI – DHCP IP assignment details** – This report provides information related to the assignment, release and expire of IP address to the system which includes IP address, MAC address, lease-duration and status (assign, renew, release or expired) fields.
Sample_Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>IP address</th>
<th>MAC Address</th>
<th>Status</th>
<th>Lease Duration</th>
<th>By interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/19/2020 06:50:33 AM</td>
<td>172.28.9.181-SYSLOG</td>
<td>192.168.100.46</td>
<td>00:50:56:be:05:43</td>
<td>RENEW</td>
<td>43200</td>
<td>eth1</td>
</tr>
<tr>
<td>02/19/2020 07:09:09 AM</td>
<td>172.28.9.181-SYSLOG</td>
<td>192.168.100.47</td>
<td>00:01:29:31:1a:8c</td>
<td>RENEW</td>
<td>43200</td>
<td>eth1</td>
</tr>
<tr>
<td>02/19/2020 09:39:01 AM</td>
<td>172.28.9.181-SYSLOG</td>
<td>192.168.100.50</td>
<td>4cd9:3f:04:ac:6a</td>
<td>RENEW</td>
<td>43200</td>
<td>eth1</td>
</tr>
<tr>
<td>02/19/2020 09:39:55 AM</td>
<td>172.28.9.181-SYSLOG</td>
<td>192.168.100.49</td>
<td>e8:9f:3f:50:62:26</td>
<td>RENEW</td>
<td>43200</td>
<td>eth1</td>
</tr>
<tr>
<td>02/19/2020 11:32:52 AM</td>
<td>172.28.9.181-SYSLOG</td>
<td>192.168.100.48</td>
<td>00:50:56:be:05:43</td>
<td>RENEW</td>
<td>43200</td>
<td>eth1</td>
</tr>
</tbody>
</table>

Log_Sample

Feb 19 22:29:51 12.28.9.81 Feb 20 06:29:51 12.18.100.10 dhcpd[12236]: DHCPACK on 102.18.100.46 to 00:50:56:be:05:43 via eth1 relay eth1 lease-duration 43200 (RENEW)

- **Infoblox DDI – object created deleted and modified** – This report provides information related to the creation, deletion and modification of objects (like DHCP range, A record, MX record) which includes object type, object name, action and messages (information about the changes) fields.

Sample_Report

Log_Sample
3.4 Dashboards

- **Infoblox DDI – User login failed** - This dashboard will display the information about user login failures.

  ![Infoblox DDI - User login failed](image)

  *Figure 7*

- **Infoblox DDI – user login allowed** - This dashboard will display the information about user login success and user logout success.
• **Infoblox DDI – Object management** – This dashboard will display the information about new object created, old objects are modified or deleted. For e.g. DHCP range, A record, MX record, .etc.
• **Infoblox DDI – DHCP activities** – This dashboard will display the information about system DHCP IP assignment details like DHCP ack, DHCP expires, and DHCP release.

![Infoblox DDI - DHCP management](image)

**Figure 10**

### 3.5 Event Filters

• **Infoblox DDI: Kernal and called logs** – This filter can filter out the logs generated for kernel and called logs.

### 4. Importing knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.
3. Click the **Import** tab.

4.1 **Saved Searches**

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click the **Category** option, and then click **Browse**....
2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like “**Categories_Infoblox DDI. iscat**” and then click “**Import**”. 

![Figure 11](image1.png)

![Figure 12](image2.png)
Integrate Infoblox DDI with EventTracker

EventTracker opens a success message:

Figure 13

4.2 Alerts

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Alert option, and then click Browse ...
2. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “Alerts_Infoblox DDI.isalt” and then click “Import”.

Figure 14
EventTracker displays a success message.

Figure 15

Figure 16

4.3 Token Templates

For importing “Token Template”, navigate to the EventTracker manager web interface.

1. Click Parsing Rules under the Admin option in the EventTracker manager web interface.
2. Click the “Template” tab and then click “Import Configuration”.

3. Now, click “Browse” and navigate to the knowledge packs folder (type \Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.ettd”, e.g. “Templates_Infoblox DDI.ettd” file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click “Import”. 

---

**Integrate Infoblox DDI with EventTracker**
4.4 Flex Reports

1. In the EventTracker control panel, select “Export/Import utility” and select the “Import tab”. Click Reports option, and choose “New (*.etcrx)”:

2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click “Select File” and navigate to the knowledge pack folder and select file with the extension “.etcrx”, e.g. “Reports_Infoblox DDI.etcrx”.

Figure 20

Figure 21
3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click **Import**.

EventTracker displays a success message.

### 4.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.
2. Click “import object”.

3. A pop-up box will appear, click “Browse” in that and navigate to the knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “KO_ Infoblox DDI.etko” and then click “Upload”.

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click “Import”.

Figure 25

Figure 26

Figure 27

Figure 28
4.6 Dashboards

1. Login to the EventTracker web interface.
2. Navigate to Dashboard → My Dashboard.

4. Select the Browse and navigate to the knowledge pack folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.etwd”, e.g. “Dashboard_Infoblox DDI.etwd” is saved and click “Upload”.

5. Wait while EventTracker populates all the available dashboards. Now, choose “Select All” and click “Import”.

![Figure 29](image1)

![Figure 30](image2)
4.7 Event Filters

3. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Filters option, and then click Browse ...

4. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “Filters_Infoblox DDI.isfil” and then click “Import”.

Figure 31

Figure 32
Integrate Infoblox DDI with EventTracker

Figure 33

EventTracker displays a success message.

Figure 34

5. Verifying knowledge pack in EventTracker

5.1 Saved Searches

1. Login to the EventTracker web interface.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, click “Search” and search with the “Infoblox DDI”.

You will see the below results.

![Category Tree](image)

**Figure 35**

### 5.2 Alerts

1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
2. In the search box enter “Infoblox DDI” and then click Search.

EventTracker displays an alert related to Infoblox DDI:

![Alerts](image)

**Figure 36**

### 5.3 Token Templates

1. In the EventTracker web interface, click the Admin dropdown, and then click “Parsing Rules”.
2. In the “Template” tab, click on the “Infoblox DDI” group folder to view the imported Token.
5.4 Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.

2. In Reports Configuration pane, select the Defined option.
3. Click on the “Infoblox DDI” group folder to view the imported reports.

5.5 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand the “Infoblox DDI” group folder to view the imported Knowledge objects.
5.6 Dashboards

1. In the EventTracker web interface, Click Home and select “My Dashboard”.

2. In “Infoblox DDI” dashboard you should be now able to see something like this:

5.7 Event Filters

1. In the EventTracker web interface, click the Admin dropdown, and then click Event Filters.
2. In the search box enter “Infoblox DDI” and then click Search.
EventTracker displays Event Filters related to **Infoblox DDI**:

![Event Filters Diagram](image)

**Figure 43**