Integrate Citrix NetScaler
Abstract

This guide helps you in configuring Citrix NetScaler and EventTracker to receive Citrix NetScaler events. You will find the detailed procedures required for monitoring Citrix NetScaler Appliance.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and Citrix NetScaler 10 and 11.

Audience

Administrators, who are responsible for monitoring Citrix NetScaler using EventTracker Enterprise.
# Table of Contents

Abstract .................................................................................................................................................. 1

Introduction .......................................................................................................................................... 3

Prerequisites ......................................................................................................................................... 3

Configure Citrix NetScaler to forward all the logs to EventTracker ......................................................... 3
  Configure Syslog logging ...................................................................................................................... 3

EventTracker Knowledge Pack ............................................................................................................. 7
  Categories ............................................................................................................................................ 7
  Alerts .................................................................................................................................................. 10
  Flex Reports ...................................................................................................................................... 11

Import Citrix NetScaler knowledge pack into EventTracker ..................................................................... 18
  Category ............................................................................................................................................. 18
  Alerts ................................................................................................................................................ 19
  Templates .......................................................................................................................................... 21
  Flex Reports .................................................................................................................................... 23

Verify Citrix NetScaler knowledge pack in EventTracker ......................................................................... 24
  Category ............................................................................................................................................. 24
  Alerts ................................................................................................................................................ 24
  Template .......................................................................................................................................... 25
  Flex Reports .................................................................................................................................... 26

Create Flex Dashboards in EventTracker ............................................................................................... 28
  Schedule Reports .............................................................................................................................. 28
  Create Dashlets ............................................................................................................................... 30
  Sample Flex Dashboards ................................................................................................................ 33
Introduction

The Citrix NetScaler makes applications run five times better, reduces web application ownership costs, optimizes the user experience, and makes sure that applications are always available. Citrix NetScaler can significantly improve the user experience for XenApp and XenDesktop deployments while improving security.

To monitor Citrix NetScaler Appliance in EventTracker, configure Citrix NetScaler Appliance to send all events as Syslog to the EventTracker system.

Prerequisites

- EventTracker v7.x should be installed.
- Citrix NetScaler Appliance should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514

Configure Citrix NetScaler to forward all the logs to EventTracker

Configure Syslog logging

To configure the syslog from the Graphical User Interface (GUI) of the NetScaler appliance, complete the following steps:

1. Expand the System node in the Configuration utility of the GUI.
2. Expand the Auditing node from the System node.
3. Click Syslog as shown in the following screen shot.
4. On the Auditing Policies and Servers, select the **Servers** tab.
5. Click **Add** as shown in the following screen shot.

6. In the **Name** filed, type the name of the auditing server.
7. In the **Auditing Type** list, select **SYSLOG**.
8. In the **IP Address** field, type the IP address of the **EventTracker Manager Machine**.
9. In the **Port** field, type the remote port number. The port 514 is the standard syslog port.
10. From the **Log Levels** group, select the appropriate options to set the log level to receive the logs from the remote server.
11. If required, select the following optional components:
   - Select an appropriate log facility from the Log Facility list.
   - Select the **TCP Logging** or **ACL Logging** options.
   - Select the date format and time zone.

The following screen shot displays the sample values described in Step 6 through Step 11.

![Figure 3](image_url)

12. Click **Create**.
13. Click **Close**.
14. Select the **Policies** tab.
15. Click **Add**.
16. In the **Name** field, type the name of the auditing policy.
17. In the **Auditing Type** list, select **SYSLOG**.
18. From the Server list, select the created server in this procedure.
The following screen shot displays the sample values described in Step 14 through Step 18.

19. Click Create.
20. Click Close.
21. Click Global Bindings.
22. Click Insert Policy and select the best_syslog_policy_ever policy as shown in the following screen shot.

Figure 4

Figure 5
23. Click **OK**.

**NOTE:** In order to get reports regarding TCP, ACL or AppFlow the following should be enabled which is marked inside red box 11. But these logs are voluminous when generated.

![Figure 6](image)

**EventTracker Knowledge Pack**

Once Citrix NetScaler events are enabled and Citrix NetScaler events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Citrix NetScaler monitoring.

**Categories**

- **Citrix NetScaler: All events**
  This category provides information related to all events from Citrix NetScaler.

- **Citrix NetScaler: Buffer overflow violation**
  This category provides information related to buffer overflow violation.

- **Citrix NetScaler: Command execution**
  This category provides information related to command execution.

- **Citrix NetScaler: Confidential field added/removed**
  This category provides information related to confidential field added/removed.
• **Citrix NetScaler: Connection delinked**
  This category provides information related to connection delinked.

• **Citrix NetScaler: Connection terminated**
  This category provides information related to connection terminated.

• **Citrix NetScaler: Cookie violation**
  This category provides information related to cookie violation.

• **Citrix NetScaler: CPU started**
  This category provides information related to CPU started.

• **Citrix NetScaler: Deny URL violation**
  This category provides information related to deny URL violation.

• **Citrix NetScaler: Device down**
  This category provides information related to device down.

• **Citrix NetScaler: Device out of service**
  This category provides information related to device out of service.

• **Citrix NetScaler: Device up**
  This category provides information related to device up.

• **Citrix NetScaler: Field consistency violation**
  This category provides information related to field consistency violation.

• **Citrix NetScaler: Field format violation**
  This category provides information related to field format violation.

• **Citrix NetScaler: Field type added/removed**
  This category provides information related to field type added/removed.

• **Citrix NetScaler: HTTP request error**
  This category provides information related to HTTP request error.

• **Citrix NetScaler: Login failed**
  This category provides information related to authorization denied.

• **Citrix NetScaler: Memory allocation failed**
  This category provides information related to memory allocation failed.

• **Citrix NetScaler: Memory freed**
  This category provides information related to memory freed.

• **Citrix NetScaler: NetScaler system start/stop**
  This category provides information related to NetScaler system start/stop.

• **Citrix NetScaler: Network interface hanged**
  This category provides information related to network interface hanged.

• **Citrix NetScaler: Network interface start/stop**
  This category provides information related to network interface start/stop.
• **Citrix NetScaler: NIC migration**
  This category provides information related to NIC migration.

• **Citrix NetScaler: Pitboss process added**
  This category provides information related to pitboss process added.

• **Citrix NetScaler: Pitboss process restarted**
  This category provides information related to pitboss process restarted.

• **Citrix NetScaler: Pitboss system restarted**
  This category provides information related to pitboss system restarted.

• **Citrix NetScaler: Safe commerce violation**
  This category provides information related to safe commerce violation.

• **Citrix NetScaler: Safe object violation**
  This category provides information related to safe object violation.

• **Citrix NetScaler: Security profile added/removed**
  This category provides information related to security profile added/removed.

• **Citrix NetScaler: Security profile binded**
  This category provides information related to security profile binded.

• **Citrix NetScaler: SQL injection violation**
  This category provides information related to SQL injection violation.

• **Citrix NetScaler: SSL certificate expiry alert**
  This category provides information related to SSL certificate expiry alert.

• **Citrix NetScaler: SSL handshake failed**
  This category provides information related to SSL handshake failed.

• **Citrix NetScaler: SSL handshake success**
  This category provides information related to SSL handshake success.

• **Citrix NetScaler: SSLVPN client security check**
  This category provides information related to SSLVPN client security check.

• **Citrix NetScaler: SSLVPN connection time out**
  This category provides information related to SSLVPN connection time out.

• **Citrix NetScaler: SSLVPN HTTP request received**
  This category provides information related to SSLVPN HTTP request received.

• **Citrix NetScaler: SSLVPN license limit reached**
  This category provides information related to SSLVPN license limit reached.

• **Citrix NetScaler: SSLVPN login**
  This category provides information related to SSLVPN login.

• **Citrix NetScaler: SSLVPN logout**
  This category provides information related to SSLVPN logout.
• **Citrix NetScaler: SSLVPN resource access denied**
  This category provides information related to SSLVPN resource access denied.

• **Citrix NetScaler: SSLVPN TCP connection status**
  This category provides information related to SSLVPN TCP connection status.

• **Citrix NetScaler: Start URL violation**
  This category provides information related to Start URL violation.

• **Citrix NetScaler: XSS violation**
  This category provides information related to XSS violation.

### Alerts

• **Citrix NetScaler: Device down**
  This alert is generated when NetScaler device is down.

• **Citrix NetScaler: Device out of service**
  This alert is generated when NetScaler device is out of service.

• **Citrix NetScaler: HA propagation failed**
  This alert is generated when HA propagation failed.

• **Citrix NetScaler: HTTP resource access denied**
  This alert is generated when HTTP resource access is denied.

• **Citrix NetScaler: Interface bound or unbound from a channel**
  This alert is generated when Interface bound or unbound from a channel.

• **Citrix NetScaler: Login failed**
  This alert is generated when a module failed to login the user.

• **Citrix NetScaler: NetScaler system stopped**
  This alert is generated when NetScaler system has stopped.

• **Citrix NetScaler: Network interface hung**
  This alert is generated when network interface is in ‘hung’ state.

• **Citrix NetScaler: Network interface reset**
  This alert is generated when network interface is reset.

• **Citrix NetScaler: Network interface stopped**
  This alert is generated when network interface is stopped.

• **Citrix NetScaler: Non HTTP resource access denied**
  This alert is generated when non HTTP resource access is denied.

• **Citrix NetScaler: Pitboss process restarted**
  This alert is generated when pitboss process restarted.

• **Citrix NetScaler: Pitboss system restarted**
  This alert is generated when pitboss system restarted.
• **Citrix NetScaler: SNMP module started an alarm**
  This alert is generated when SNMP module started an alarm.

• **Citrix NetScaler: SNMP module stopped an alarm**
  This alert is generated when SNMP module stopped an alarm.

• **Citrix NetScaler: SSL certificate will expire soon**
  This alert is generated when SSL certificate will expire soon.

• **Citrix NetScaler: SSLVPN license limit reached**
  This alert is generated when SSLVPN license limit reached.

• **Citrix NetScaler: Start URL violation**
  This alert is generated when URL violation has occurred.

• **Citrix NetScaler: AAA session login failed**
  This alert is generated when AAA session login has been failed in the Citrix NetScaler.

• **Citrix NetScaler: AppFW DOS attack detected**
  This alert is generated when AppFW DOS attack has occurred in the Citrix NetScaler.

• **Citrix NetScaler: AppFW security violation detected**
  This alert is generated when AppFW security violation has been detected in the Citrix NetScaler.

• **Citrix NetScaler: Console logon failure**
  This alert is generated when Console logon failure has occurred in the Citrix NetScaler.

### Flex Reports

• **Citrix NetScaler-TCP session details**
  This report provides the information related to TCP session details like source address, destination address, byte sent and received etc in Citrix NetScaler.

**NOTE:** This report is generated only when TCP logging has been enabled

**Sample Report:**

![Sample Report](image)
Integrate Citrix NetScaler Logs Considered:

- **Citrix NetScaler-SSLVPN ICA application started or terminated**
  This report provides the information related to SSL VPN ICA whether the application has started or terminated in Citrix NetScaler.

  **Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>EVENT ID</th>
<th>Computer</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>User Name</th>
<th>User Domain</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
<th>Start Time</th>
<th>End Time</th>
<th>Duration</th>
</tr>
</thead>
</table>

- **Citrix NetScaler-SSLVPN session details**
  This report provides the information related to SSLVPN session details like user name, source address, and destination address, byte sent and received in Citrix NetScaler.

  **Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>EVENT ID</th>
<th>Computer</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>User Name</th>
<th>User Domain</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
<th>Start Time</th>
<th>End Time</th>
<th>Duration</th>
</tr>
</thead>
</table>
Logs Considered:

- **Citrix NetScaler-HTTP or Non-HTTP resource access denied**
  This report provides the information related to HTTP or non-HTTP resource access that has been denied.

  **Sample Report:**

```
<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site/Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
</table>
```

- **Citrix NetScaler-AAA session logon or logout**
  This report provides the information related to session login or logout using AAA in Citrix NetScaler.

  **Sample Report:**

```
<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site/Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/9/2016 00:12:58 PM</td>
<td>29</td>
<td>PNPL-15-KP / PNPL-15</td>
<td>BUILTIN</td>
<td>Syslog</td>
<td></td>
</tr>
</tbody>
</table>
```
Logs Considered:

- **Citrix NetScaler-AAA session logon failed**
  This report provides the information related to login failed using AAA in Citrix NetScaler.
  
  **Sample Report:**
  
<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client Name</th>
<th>Client Address</th>
<th>Reason</th>
</tr>
</thead>
</table>
  
  Figure 17

- **Citrix NetScaler-ACL rule hit details**
  This report provides the information related to rule hit details of ACL in Citrix NetScaler.
  
  **Sample Report:**
  
<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Protocol Type</th>
<th>Hit Rule</th>
<th>Hit Count</th>
</tr>
</thead>
</table>
  
  Figure 19
• **Citrix NetScaler-Console logon success**
  This report provides the information related to logon success for console in Citrix NetScaler.

  **Sample Report:**

  ![Figure 21](image1)

  **Logs Considered:**

  ![Figure 22](image2)

• **Citrix NetScaler-Command execution details**
  This report provides the information related to execution of commands along with their details like user name, user address command executed and their status in Citrix NetScaler.

  **Sample Report:**

  ![Figure 23](image3)

  **Logs Considered:**

  ![Figure 24](image4)

• **Citrix NetScaler-AppFW security violation details**
  This report provides the information related to security violation details for AppFW in Citrix NetScaler.
## Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Client Address</th>
<th>Action Taken</th>
<th>Threat Details</th>
<th>Requested URL</th>
</tr>
</thead>
</table>

### Logs Considered:

- **Citrix NetScaler-SSLVPN session login or logout**

This report provides the information related to session login or logout of SSLVPN in Citrix NetScaler.

## Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Client Address</th>
<th>Action Taken</th>
<th>Threat Details</th>
<th>Requested URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Logs Considered:

- **Citrix NetScaler-SSLVPN session login or logout**

This report provides the information related to session login or logout of SSLVPN in Citrix NetScaler.
- **Citrix NetScaler-Console logon failure**
  This report provides the information related to logon failure of console in Citrix NetScaler.

**Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Console Type</th>
<th>User Name</th>
<th>User Address</th>
<th>Command Executed</th>
<th>Execution Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/09/2016 12:35:36 PM</td>
<td>CIPL-15,KP/CIPL-15,KP</td>
<td>UI</td>
<td>nroot</td>
<td>1.2.25.335</td>
<td>login</td>
<td>ERROR: invalid username or password</td>
</tr>
</tbody>
</table>

**Figure 29**

**Logs Considered:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/9/2016 7:01:14 PM</td>
<td>24</td>
<td>CIPL-15 KP / CIPL-15</td>
<td>CMD_EXECUTED 123456789:0: User nroot - Remote_ip 10.10.10.10 - Command &quot;login nroot ***&quot; **** Status &quot;ERROR: invalid username or password&quot;</td>
</tr>
</tbody>
</table>

**Figure 30**
Import Citrix NetScaler knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Templates
- Knowledge Objects
- Flex Reports

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility.

![EventTracker Control Panel](image)

Figure 31

3. Click the **Import** tab.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate the **All Citrix NetScaler group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Figure 32](image)

4. Click the **OK** button, and then click the **Close** button.

![Figure 33](image)

### Alerts

1. Click **Alerts** option, and then click the browse button.
2. Locate the **All Citrix NetScaler group of alerts.isalt** file, and then click the **Open** button.
2. To import alerts, click the **Import** button. EventTracker displays success message.

3. Click **OK**, and then click the **Close** button.
**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on **Import** option.

![Figure 36](image)

3. Click on **Browse** button.

![Figure 37](image)
4. Locate All Citrix NetScaler group of Template.ett file, and then click the Open button

![Figure 38](image)

5. Now select the check box and then click on Import option. EventTracker displays success message.

![Figure 39](image)

6. Click on OK button.
Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **All Citrix NetScaler group of flex reports.issch** file, and then click the **Open** button.

![Figure 40](Image)

1. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

![Figure 41](Image)
Verify Citrix NetScaler knowledge pack in EventTracker

Category

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Categories**.
2. In the **Category Tree**, expand **Citrix NetScaler** group folder to see the imported categories.

![Category Management](image)

**Figure 42**

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type ‘**Citrix NetScaler**', and then click **Go** button.

Alert Management page will display the imported **Citrix NetScaler** alert.
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message Box](image)

**Figure 43**

4. Click the **OK** button, and then click the **Activate now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Template**

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter ‘Citrix NetScaler’, and then click the Search button.

EventTracker displays Flex reports of Citrix NetScaler.
Figure 46
Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.

![Figure 47](image)

2. Navigate to Reports>Configuration.

![Figure 48](image)

4. Click on ‘schedule’ to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

![Figure 49](image)

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

![Figure 50](image)
8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

### Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

   ![Figure 51](image)

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

   ![Figure 52](image)
3. Fill suitable title and description and click **Save** button.
4. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

![Widget Configuration](image)

**Figure 53**

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ 🔄 to locate and choose created dashlet.
16. Click 📦 to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard **DATA SOURCE: Citrix NetScaler - SSLVPN session login or logout**

1. **Citrix NetScaler - SSLVPN session login or logout**
   - **WIDGET TITLE:** Citrix NetScaler - SSLVPN session login or logout
   - **CHART TYPE:** Donut
   - **AXIS LABELS [X-AXIS]:** Client Address
   - **FILTER:** End Time
   - **LEGEND [SERIES]:** Status

![Client Address: 10.252.66.09](image)

Figure 57
For below dashboard **DATA SOURCE: Citrix NetScaler-AAA session login or logout**

2. **Citrix NetScaler-AAA session login or logout**
   - **WIDGET TITLE:** Citrix NetScaler - AAA session login or logout
   - **CHART TYPE:** Donut
   - **AXIS LABELS [X-AXIS]:** Reason
   - **FILTER:** End Time
   - **LEGEND [SERIES]:** Status

![Figure 58](image-url)