Integrate Routing and Remote Access Service (RRAS)

EventTracker v8.x and above

Publication Date: June 27, 2018
Abstract

This guide provides instructions to configure Routing and Remote Access Service (RRAS) to send the windows based events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Microsoft Windows Server 2008 and later.

Audience

Routing and Remote Access Service (RRAS) users, who wish to forward windows based messages to EventTracker manager.
# Table of Contents

Abstract ............................................................................................................................................................. 1  
Scope ............................................................................................................................................................... 1  
Audience........................................................................................................................................................... 1  
Introduction....................................................................................................................................................... 3  
Prerequisites..................................................................................................................................................... 3  
Configuration.................................................................................................................................................... 3  
  Forward RRAS Logs to EventTracker by deploying the Agent............................................................... 5  
Import RRAS VPN logs into EventTracker via LFM .................................................................................. 6  
EventTracker Knowledge Pack (KP) ............................................................................................................ 13  
  Flex Reports................................................................................................................................................ 13  
  Categories and Saved Searches.................................................................................................................. 16  
Import RRAS knowledge pack into EventTracker ....................................................................................... 16  
  Token Templates: ....................................................................................................................................... 16  
  Flex Reports: ............................................................................................................................................ 17  
Verify RRAS Knowledge Pack in EventTracker ....................................................................................... 19  
  Verify RRAS Token Templates................................................................................................................ 19  
  Verify RRAS Flex Reports ....................................................................................................................... 19
Introduction

RRAS stands for Routing and Remote Access Service. It is a Microsoft API and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router.

An RRAS server provides two different types of remote access connectivity:

- **Virtual private networking** - A virtual private network (VPN) is a secured, point-to-point connection across a public network, such as the Internet. A VPN client uses TCP/IP-based tunneling protocols to make a connection to a port on a remote VPN server.

- **Dial-up networking** - In dial-up networking, a remote access client makes a dial-up telephone connection to a physical port on a remote access server by using the service of a telecommunication provider, such as analog telephone or ISDN.

Prerequisites

Prior to configuring Routing and Remote Access Service (RRAS) and EventTracker, ensure that you meet the following prerequisites:

- Microsoft Windows Server 2008 or above version should be installed.
- Proper access permissions to make configuration changes.
- EventTracker agent should be installed in Windows Server.
- Administrative access on EventTracker.

Configuration

You must enable and configure logging on Routing and Remote Access Service (RRAS) prior to configuring EventTracker.

**To configure logging in RRAS,**

1. In the **Routing and Remote Access MMC snap-in**, in the navigation pane, right-click the server used, and then click **Properties**. If you are using Server Manager, right-click **Routing and Remote Access**, and then click **Properties**.
2. On the **Logging** tab, choose **Log errors and warnings** option
3. Click **Apply**, and then click the **OK** button to save changes.

It will forward the logs to Event Viewer.

Forward RRAS Logs to EventTracker by deploying the Agent

VPN log is stored in a separate file path (i.e. `C:\Windows\System32\LogFiles\IN1408.log`) and RRAS operation is displayed in EventViewer.

1. Open **Routing and Remote Access**.
2. Double-click **Routing and Remote Access**, and then double-click the server name on which you want to configure logging.
3. In the console tree, right-click **Remote Access Logging & Policies** and then select **Launch NPS**.
4. In left pane, click **Accounting**, click **Change Log File properties** and then select **Log File** tab.
5. Change the log file **Directory**: and log **Format**: (ODBC recommended) as per requirement.

6. Click **Apply** and then click **OK** button to save the changes.

**Import RRAS VPN logs into EventTracker via LFM**

1. Go to the EventTracker installation file path and search for **etaconfig** application.
2. Then right click on the application icon and **Run as Administrator**.
3. Select **Logfile Monitor** tab.
EventTracker opens the ‘Logfile Monitor’ tab.

4. Click the Add File Name button. EventTracker displays the ‘Enter File Name’ window.
5. Click the **Get All Existing Log Files** checkbox, if you want all the existing files prior to this configuration and the files that are logged after this configuration.

6. Select the logfile type as **TEXTLINE** from the **Select Logfile Type** drop-down list.

7. Click the **Enter File Name** path option.
   EventTracker displays the ‘Select Folder/File Name’ window.

8. In **Select Folder name**: Select appropriate folder associated with selected Log File Type.

9. Click **OK**.
   EventTracker displays the ‘**Select file extension**’ window.
10. Type *.log and click OK.

EventTracker displays the ‘Enter File name’ window.

11. Click OK.

EventTracker displays the ‘EventTracker Agent Configuration’ message box.

12. Click Yes.

EventTracker displays the Search String dialog box.
13. Click the **Add String** button.

   EventTracker displays the ‘Enter Search String’ dialog box.

![Search String Dialog](image)

Figure 10

14. Select the file name as **TEXT** from the **Select Field Name** drop-down list.
15. Type **“*”** in the **Enter Search String** field.
16. Click the **Current DateTime**
17. Click **OK**.
EventTracker displays the Search String dialog box.

![Search String dialog box](image)

**Figure 12**

18. Click **OK**.

EventTracker displays the ‘Agent Configuration’ window with the newly added Logfile entry.
19. Click the **Save** button.
EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v8.x to support Microsoft Windows Routing and Remote Access Service (RRAS) monitoring.

**Flex Reports**

- **MS RRAS-Access request** - This report provides information related to all access request send for VPN connection.

![Figure 14](image1)

**Sample logs:**

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>
```

![Figure 15](image2)
- **MS RRAS-Access failure** - This report provides information related to failure client access request.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Client Computer Name</th>
<th>Packet Type</th>
<th>Username</th>
<th>Source IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/21/2018 01:23:10 PM</td>
<td>RRAS</td>
<td>A00250</td>
<td>3</td>
<td>SCIENCEgxf555</td>
<td>10.25.99.13</td>
</tr>
<tr>
<td>06/21/2018 01:23:10 PM</td>
<td>RRAS</td>
<td>A00250</td>
<td>3</td>
<td>SCIENCEgxf542</td>
<td>10.25.9.23</td>
</tr>
<tr>
<td>06/21/2018 01:23:10 PM</td>
<td>RRAS</td>
<td>A00250</td>
<td>3</td>
<td>SCIENCEgxf589</td>
<td>10.25.96.30</td>
</tr>
</tbody>
</table>

Figure 16

**Sample logs:**

```
Jun 21 01:23:11 PM  ENTRY:"A00250", "RRAS", 06/13/2018, 23:05:01.3, "SCIENCE\00250" 1714, 3, 12.223.22.55 05/17/2018 04:05:52.4583, "Microsoft Routing and Remote Access Service Policy", 1...
```

Figure 17

- **MS RRAS-Access success** - This report provides information related to successful client access request.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Client Computer Name</th>
<th>Username</th>
<th>Packet Type</th>
<th>Source IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>A00250</td>
<td>science.domain/KU</td>
<td>1</td>
<td>10.25.9.13</td>
</tr>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>A00257</td>
<td>science.domain/KU Users/Active/lK4</td>
<td>1</td>
<td>10.5.9.22</td>
</tr>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>A00253</td>
<td>science.domain/KU Users/Active/pg22</td>
<td>4</td>
<td>13.5.99.11</td>
</tr>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>A00250</td>
<td>science.domain/KU Users/Active/kp225</td>
<td>2</td>
<td>13.5.99.23</td>
</tr>
</tbody>
</table>

Figure 18
**Sample logs:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

- **MS RRAS- Accounting request** - This report provides information related to client status for the accounting request.

![Figure 19](image)

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Username</th>
<th>Client IP Address</th>
<th>Client Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>vjc26</td>
<td>76.7.15.12</td>
<td>MSRAS-0-PB13132</td>
</tr>
<tr>
<td>06/21/2018 01:23:08 PM</td>
<td>RRAS</td>
<td>vjc26</td>
<td>76.7.15.10</td>
<td>MSRAS-0-PB13132</td>
</tr>
<tr>
<td>06/21/2018 01:23:09 PM</td>
<td>RRAS</td>
<td>mktrlg430</td>
<td>19.61.37.80</td>
<td>MSRAS-0-PB09261</td>
</tr>
</tbody>
</table>

![Figure 20](image)

**Sample logs:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

![Figure 21](image)
Integrate Routing and Remote Access Service

Categories and Saved Searches

- **MS RRAS: Accept Request** - This category provides information related to client access request for VPN.
- **MS RRAS: Access Accept** - This category provides information related to client access accept.
- **MS RRAS: Access Reject** - This category provides information related to client access reject.
- **MS RRAS: Accounting Type** - This category provides information related to accounting type.
- **MS RRAS: Authentication Failure** - This category provides information related to authentication failure.
- **MS RRAS: Request Discard** - This category provides information related to client request discard.

**Import RRAS knowledge pack into EventTracker**

Import knowledge pack items in the following sequence:

- Token Templates
- Flex Reports

**Token Templates:**

1. Logon to *EventTracker Enterprise*.
2. Click the **Admin** dropdown, and then click **Parsing rule**.
3. Select the **Template** tab option and click the **""** button.
4. Locate the **All RRAS Token Template .ettd files** and click the **Open** button.

![Figure 22](image-url)
5. To import token templates, click the **Import** button. EventTracker displays success message.

![Template(s) imported successfully](image)

**Figure 23**

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

**Flex Reports:**

1. Go to the EventTracker installation path and search for `ETControlPanel` application.

2. Then right click on the application icon and **Run as Administrator**.

3. Double click **Export Import Utility** and click **Import** tab.

![Export Import Utility](image)

**Figure 24**
4. Click **Report** option, select the **New (.etcrx)** and then click the **...** button.

![Figure 25](image1.png)

5. Locate the **All RRAS group of Report.etcrx** file, and then click the **Open** button.

6. Click **...** button to import the scheduled reports.

   EventTracker displays success message.

![Figure 26](image2.png)

7. Click **OK**, and then click the **Close** button.
Verify RRAS Knowledge Pack in EventTracker

Verify RRAS Token Templates

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Parsing Rules.
3. Imported RRAS tokens added in Microsoft RRAS Groups list at left side of Template tab of EventTracker Enterprise (as shown in below figure).

![Parsing Rules](image)

### Figure 27

Verify RRAS Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu. Select Configuration.
3. In the Reports Configuration, select Defined from radio button. EventTracker displays Defined page.
4. Select the ‘Microsoft RRAS’ Groups.
EventTracker displays Flex reports of RRAS.

![Figure 28](image-url)