HP RUM Server Collector

Server Collector was introduced in RUM 9.21 as an alternative way to route network traffic to RUM, without the need for network configuration. This document describes the advantages and limitations of Server Collector.

Speed-up RUM POC
One of the main use cases for Server Collector is the POC scenario, where you want to show value to the customer in the shortest time, without any need for network configuration.

Extend RUM monitoring coverage
Even existing RUM customers do not always benefit from all available functionality because of network configuration limitations – for example, monitoring application back-end tiers. Server Collector may be a possible solution.

Motivation: When should you use Server Collector?

Quick Demo

It is always preferable to use the standard methods of traffic forwarding to the Probe (switch/TAP), when possible. These standard methods put no overhead at all on the server and you do not have to maintain multiple instances of Server Collector software.

However, when you need to show RUM capabilities quickly, and you have access to the server to install software, Server Collector may be of great help. This includes a POC for a new application, or monitoring application back-end tiers. Refer to capacity and performance metrics below to ensure that Server Collector can be safely installed in your particular scenario. At a later stage, you can replace Server Collector with a network tapping configuration.

No network access

In some cases the network infrastructure may be owned by a 3rd-party provider, making it impossible to TAP the network traffic in particular places using standard methods. In such cases, Server Collector can be used as a permanent solution, provided that capacity requirements are met.

Virtual environments

Traffic between Virtual Machines may not pass through a physical network, again making it impossible to TAP the network on a switch level. In such a case, there are a number of alternatives for configuring RUM. See below for details.

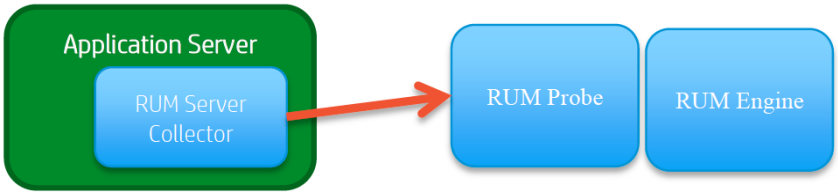
Introduction

Getting traffic to RUM

The standard way to route network traffic to RUM is by configuring a Span Port on a network switch, or by inserting a TAP device to the network topology, so that relevant traffic is duplicated and sent to the RUM Probe for processing.

In some cases, such configurations may take a long time for a customer because of various IT processes required for making such changes in the network. Server Collector offers an alternative solution, by installing a light-weight component directly on the server machine which captures all traffic from the local network card,

and sends it to a RUM Probe, as shown in the following diagram:



Capacity and Sizing

Throughput Limitations

Server Collector sends network packets to the RUM Probe. The maximum traffic throughput that can be duplicated without any data loss by a single Server Collector is 140 Mbps on Windows machines and 250 Mbps on Linux. If a server is handling higher volumes of traffic, some data may be lost and you should consider alternative solutions (such as regular tapping in the network).

Resource utilization

- By default, Server Collector transfers data to the RUM Probe over a secured channel (see the Hardening section below). In secured networks (if there is no risk of eavesdropping) SSL can be disabled to decrease both the amount of traffic and CPU usage. The SSL layer adds 10% overhead to the traffic volume. For example, assuming the server consumes 100Mbps of network bandwidth, adding Server Collector monitoring increases the consumption to 210Mbps (an additional 100Mbps of duplicated traffic to the RUM Probe + 10Mbps of SSL overhead).
  Note that depending on network topology and server configuration, the connection to the RUM Probe could use a different network card and/or route so that the network path between the server and its clients will not be affected.

- For each 100Mbps of mirrored traffic, the Server Collector utilizes up to 70% of a single CPU core on a Windows server, and up to 40% of a single CPU core on a Linux server. (The test was carried out on a 2.67GHz processor.) For example, on a Windows server with 16 cores of 2.67GHz, the Server Collector will consume up to 4% CPU for 100 Mbps or mirrored traffic (or 2.5% CPU for a Linux server).

RUM Probe Sizing

Multiple Server Collectors can be connected to a single RUM Probe. All regular sizing rules for the RUM Probe are applicable, but you should take into consideration the sum of the traffic reaching the Probe, both from network tapping and from Server Collectors.

Hardening

Ports on the server

The connection is always opened from the RUM Probe to Server Collector; a single TCP port is required to be open (including the whole path between the Probe and Collector). By default, port 2002 is used, but this can be changed in Server Collector's configuration (see Configuration section below).

Secured connections

The communication channel between the RUM Probe and Server Collector uses an SSL connection over TCP. The SSL handshake is further secured with Client Certificate, which ensures that only a valid RUM Probe can pull data from the server and no other unauthorized party can pretend to be the RUM Probe and get access to sensitive data. Both products are shipped with predefined keys:

- For an SSL connection initiated by RUM Probe:
  - Private Key and Certificate on Server Collector
  - CA Certificate on RUM Probe (that is used to verify the certificate above)
- For client validation (Client Certificate):
  - Private Key and Certificate on RUM Probe
  - CA Certificate on Server Collector (that was used to verify the certificate above)

Installation

The Server Collector can be downloaded from the SSO site.

For Windows Server

Windows Server 2008 R2, 64bit is supported.
Run the installer program and follow on-screen instructions. The default installation path is `<Program Files>\HP\RUMSC` which you can change during the installation.

You can start/stop the service from the Services management console. By default, the service is started after the installation and it also starts automatically after a system restart.

For Linux Server

Linux Red Hat 5.X and 6.x, 64bit are supported.

Run the installer script from command-line shell when logged in as root user. Server Collector will be installed under `/opt/HP` folder.

Configuration

RUM Applications in BSM

You should define the application in BSM Administration in same way regardless the method of network packets' delivery to RUM Probe. All RUM functionality is supported with Server Collector.

Instructing RUM Probe to connect to Server Collector

This configuration must be done on the RUM Engine:

- On the RUM Engine, open the `HPRUM\conf\configurationmanager` folder
- Locate the `Beatbox_<probe-name>_Const_Configuration.xml` file (or add a new one if it does not exist). The `<probe-name>` should be the host name you configured in Probe management when you added the Probe to the RUM Engine
- In case this file does not exist, the following is the content you should add to the new file:

```
<?xml version="1.0" encoding="UTF-8"?>
<consts>
    <collector><![CDATA[

[collector]
device all

]]></collector>
</consts>
```

- Add the following line to the [collector] section for each Server Collector you want to use with this Probe:
  `device rpcap://[16.60.10.10]:2002/`
  (Substitute the correct server IP instead of 16.60.10.10 in the above example. Also, substitute the correct port number if you configured the Server Collector to use non-default port).
  The above line instructs the RUM Probe to collect data from all network devices of a given server. If you want to use a specific device instead, append its name to the end of the line, as shown in the following examples:
  `device rpcap://[ 16.60.10.10]:2002/eth0`
  `device rpcap://[ 16.60.10.10]:2002/\Device\NPF_{2A488F9E-57E5-42C5-9231-551D0193A957}`
- Sync the configuration in RUM Engine web console.

Connection Properties on RUM Probe

In the RUM Probe, the following configuration is available in the `[servercollector]` section of the `rp_security.conf` configuration file:

- `collector_enable_ssl`: when true (default), connects to Server Collector over SSL.
- The private key and certificates mentioned in the Hardening section can be changed using `collector_ca_cert`, `collector_ssl_client_key` and `collector_ssl_client_cert` parameters accordingly.

Server Collector Configuration

The `collector.conf` configuration file is located in the `etc/rum_collector` folder under Server Collector's installation path.

- Use the `port` field in the `[general]` section to change the listening port of Server Collector (default is 2002).
- You can also configure the address parameter to make the server bind to a specific IP address (if multiple addresses are available on the server).
- The `use_ssl` flag determines the type of connection between the RUM Probe and Collector (true – SSL by default);
- The private key and certificates mentioned in the Hardening section can be changed using `ssl_ca_file`, `ssl_key` and `ssl_cert` parameters accordingly.