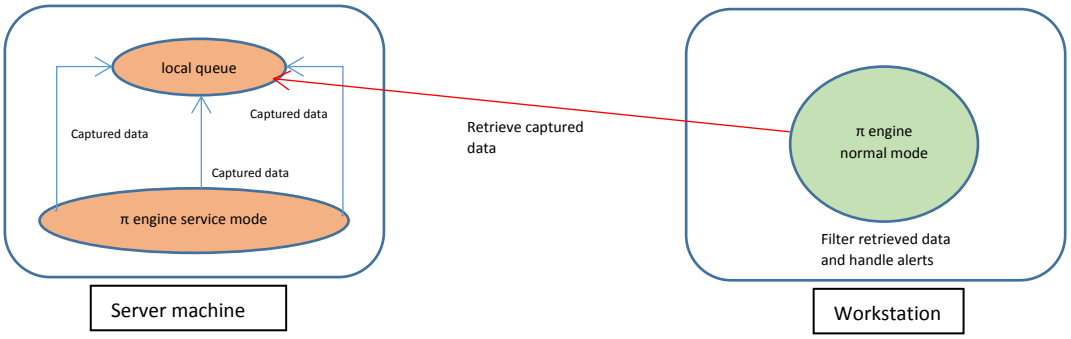
Service mode usage

Contents

Introduction

This tutorial shows how to configure and setup the Service mode. The Service mode is used on resource critical servers or machines. The engine is setup as a minimal service. All the filterting and alerting mecanism are not handled directly on the same machine but rather on a separate host. This is to minimize the impact on local resources. The following diagram describes the Service mode usage:



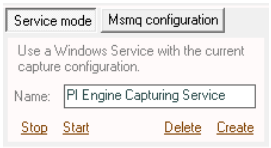
The idea behind the Service mode is to separate the capturing process from the filtering & alerting process. In this tutorial, the Service process refers to the left diagram and the Client process refers to the right diagram.

Setup the Service process

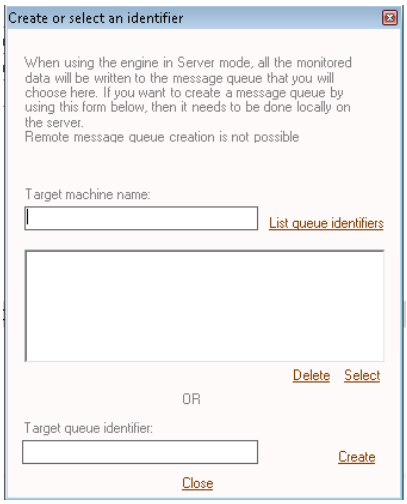
In order to run, the service process needs first to installed on the server host machine. Then you have to create the local message queue. You can achieve those two steps by using the configuration dashboard:

Install the Service process:

1. Launch PI Engine locally on the Server host machine
2. Click on the configuration dashboard icon
3. Select the desired of your Service process. This is the name that will appear in the Windows Services list



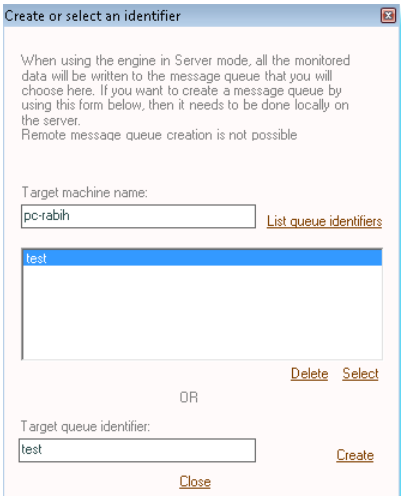
4. Click on the "*Create*" link button. This will create the Windows Service with the specified name.
5. Click on the "*Msmq configuratin*" tab
6. Click on the *"Configure"* link button. This will open the following popup:



7. Specify the desired name n the "*Target queue identifier" textbox*
8. *Click on the* "*Create"* link button.

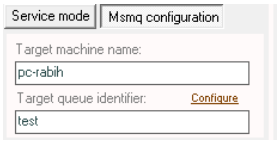
9. Specify the name of your local Server machine in the *"Target machine name" text box*

10. *Click on* "*List queue identifier"*

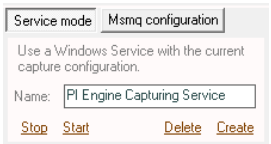


11. Select the queue identifier that you just create and click on *"Select"*

12. This will setup the following configuration:



13. Click on the *"Service mode"* tab and start the service by clicking on *"Start"*

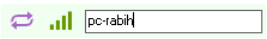


Once you have finished those steps, the Service process is started. It will capture HTTP, SQL Server, Oracle and MySQL traffic according to your current configuration. Raw traffic is captured by the Service process only if you have specified some tcp ports. Otherwise general raw traffic is not captured. All captured data are sent to the local message queue.

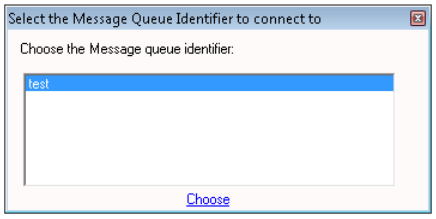
Setup the Client process

The Client process is simply the PI Engine connected to the remote queue. Any instance of the PI Engine can become a Client process as soon as it connects to a remote queue. To connect to a remote queue, please follow those steps:

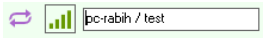
1. Launch PI Engine
2. Specify the name of the target machine that hosts the Service process



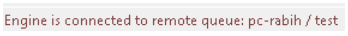
3. Click on the green button. This will open a popup where you can select the desired queue to connect to:



4. Click on *"Choose"*
5. This will setup the following configuration:



At the bottom of the engine, you also the following status message:



6. Now if you click on any of the following icons:

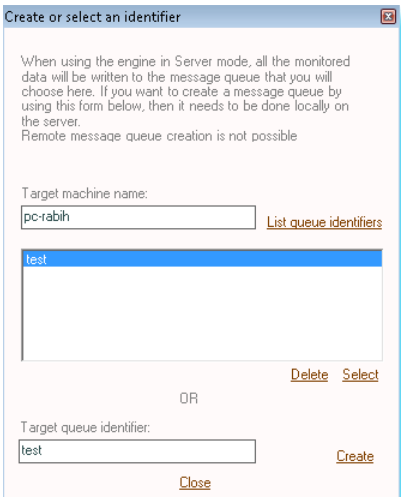
It will start a remote capture. Precisely, it will connect to the remote queue and retrieve the data captured by the Service process.

7. You can define filters and alerts as if you were using the engine in simple mode.

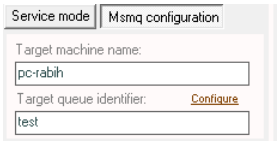
Run the Client process at computer startup

If you want to automatically start the Client process at startup, you have to configure the remote machine name and queue identifier with the configuration dashboard:

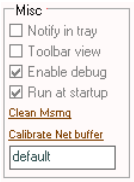
1. Open the configuration dashboard
2. Click on the *"Msmq configuration"* tab
3. Click on the *"Configure"* link button. This will open the following popup



4. Specify the name of the target machine that hosts the Service process
5. Click on the *"List queue identifiers"* link button
6. Select the queue that you wish to connect to
7. Click on the "*Select"* link button
8. This will setup the following configuration:



9. Check the *"Run at startup"* checkbox in the miscellaneous part of the configuration dashboard



10. Save the configuration dashboard.