Advanced installation of Web tier collectors

This section includes the following topics:

- Defining the server upon which the FocalPoint is to be installed
- Sampling Alerts custom metrics from the monitored instance
- Associating collected server-side performance information with network performance information
- Instrumenting Web pages to collect client-side response time information
- Monitoring Web applications using SSL
- Monitoring a Web application that is not the root application
- Monitoring a Web application that uses client-side certification
- Monitoring a Web application that uses an authentication mechanism
- Using cluster shared configuration in Precise for Web

Defining the server upon which the FocalPoint is to be installed

The default location for the FocalPoint installation is on the same server as the Precise Framework. The General tab allows you to define a different server as the location for the FocalPoint installation.

To enter FocalPoint inputs

1. After adding all Tier installation instance properties inputs, click **Advanced**.
2. Click the General tab.
3. Click the drop-down menu and select the server which the FocalPoint should be installed upon.
4. Click **OK**.

Sampling Alerts custom metrics from the monitored instance

To enable sampling of Alerts custom metrics for this instance

1. After adding all Tier installation instance properties inputs, click **Advanced**.
2. Click the General tab.
3. Mark the box “Enable sampling of custom metrics for this instance."
4. Click **OK**.

Associating collected server-side performance information with network performance information

By default, this option is already marked. This option allows you to correlate the data collected by the Web server-side collection with the data collected by the Insight Savvy for Network.

This option is not available for IIS 7.x monitoring.

To associate collected server-side performance information with network performance information

1. After adding all Tier installation instance properties inputs, click **Advanced**.
2. Click the Monitoring Options tab.
3. Mark the “Collect network response time” check box.
4. Click **OK**.

Instrumenting Web pages to collect client-side response time information

To collect client-side data, your Web application page needs to be instrumented to insert Web performance monitoring code. It uses a Web server filter to instrument the page in real-time, without changing the pages stored on the disk.

Dynamic instrumentation is not supported for Apache 1.3 and iPlanet Web servers. This means that client-side monitoring is not available for these Web servers.

To instrument Web pages to collect client-side response time information

1. After adding all Tier installation instance properties inputs, click **Advanced**.
2. Click the Monitoring Options tab.
3. Mark the “Collect client-side performance metrics” check box.

By default, this option is marked, except on Apache 1.3 and iPlanet servers.

4. Click **OK**.

Monitoring Web applications using SSL

If the only way available to connect to the Web server is via a SSL connection, enable this option.

To enable this option

1. After specifying the web domains to be monitored on the Domain Information screen, click **Advanced**.
2. Click the SSL tab.
3. Mark the “Web server uses special SSL configuration” box.
4. Enter the special ciphers to be used when connecting the Web server via SSL.

> This field should contain ciphers that are not default ciphers for the SSL version (such as: SSLv2 or SSLv3) used by the Web server. For example: RC4, RC2. For more information see http://www.openssi.org/docs/apps/ciphers.html#CIPHER_LIST_FORMAT. For a complete list of cipher names, see: http://www.openssl.org/docs/apps/ciphers html#CIPHER_SUITE_NAMES.

5. Click **OK**.

Monitoring a Web application that is not the root application

Precise for Web uses HTTP requests to the monitored application to manage the Precise for Web agents. Therefore, it needs to be updated with the application context path.

If you did not install the filter on the root Web application, update the correct site name (application context path).

To update the site name

1. After specifying the web domains to be monitored on the Domain Information screen, click **Advanced**.
2. Click the Site Name tab.
3. Enter the updated site name (application context path).
4. Click **OK**.

Monitoring a Web application that uses client-side certification

This specifies whether the Web server needs a client certificate to establish a connection.
To specify whether the Web server needs a client certificate to establish a connection
1. After specifying the web domains to be monitored on the Domain Information screen, click Advanced.
2. Click the SSL tab.
3. Mark the “Web server uses client-side certification” box.
4. Enter the full path to the client certificate file or click the browse (...) button to locate and select the appropriate path.
5. Enter the full path to the client certificate private key file (if not included in the certificate file) or click the browse (...) button to locate and select the appropriate key path.
6. Enter the encrypted password for the client certificate, if required. The password should be encrypted using the Precise CLI utility.
7. Click OK.

Monitoring a Web application that uses an authentication mechanism

If the monitored Web server uses an authentication mechanism to allow incoming requests, you need to enter additional inputs.

To enter additional inputs

1. After specifying the web domains to be monitored on the Domain Information screen, click **Advanced**.
2. Click the Authentication tab.
3. Mark the “Web server uses authentication” box.
4. Enter the user name.
5. Enter the password (encrypted using the Precise CLI utility).
6. Enter the domain.
7. Select the method from the drop-down menu. You can choose from:
    - **Basic**
    - **Digest**
    - **NTLM**
8. Click **OK**.

Using cluster shared configuration in Precise for Web

> This option is only relevant for WebSphere and WebLogic.

To use cluster shared configuration

1. After adding all Tier installation instance properties inputs, click **Advanced**.
2. Click the Monitoring Options tab.
3. Verify that the “Use cluster shared configuration” check box is marked.
4. Click **OK**.
5. Complete the installation and perform the displayed action items.

After following the previous procedure, all WebLogic/WebSphere servers running the same application will be auto-installed as part of the cluster.