FPA

API Raiden FPA: Guía de actualización

Consideraciones entrega 1

Teniendo en cuenta que la actualización se realiza sobre la primera instalación (Prueba de concepto). Es necesario revisar el archivo **Web.config**

Para esta entrega en particular, es necesario modificar el config de la siguiente manera:

- Agregar tag en **appSettings**: Directorio de logs. El usuario que corre el servicio debe tener permisos de escritura sobre este directorio. (log_path)
- Agregar Tag **httpErrors** dentro de **system.webServer**. Tal cual se indica a continuación:

<httpErrors errorMode="DetailedLocalOnly" existingResponse="PassThrough"/>

```
<configuration>
  <appSettings>
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="dbo" value="dbo" />
    <add key="log_path" value="C:\raiden logs" />
  </appSettings>
  <connectionStrings>
    <add name="main" connectionString="server=HOST\INSTANCE;Database=DB;trusted_connection=TRUE"/>
  </connectionStrings>


  <system.webServer>
    <httpErrors errorMode="DetailedLocalOnly" existingResponse="PassThrough"/>
    <validation validateIntegratedModeConfiguration="false" />
    <modules runAllManagedModulesForAllRequests="true">
      <remove name="ApplicationInsightsWebTracking" />
      <add name="ApplicationInsightsWebTracking" type=
      "Microsoft.ApplicationInsights.Web.ApplicationInsightsHttpModule, Microsoft.AI.Web"
      preCondition="managedHandler" />
    </modules>
  </system.webServer>
```

Luego de hacer esta modificación es necesario realizar el paso 2 en delante de la guía de actualización.

FPA

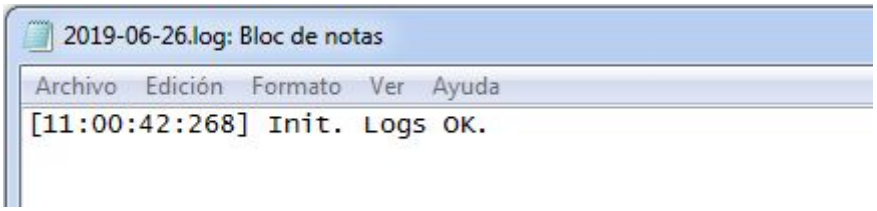
Actualización paso a paso:

A continuación, se detallan los pasos necesarios para actualizar el servicio de integración FPA-Raiden de forma manual, considerando que ya se encuentra instalado anteriormente siguiendo los pasos del documento: **FPA Raiden – Instalación.pdf**

1. Extraer el contenido del archivo **fpa_raiden.zip** en la ruta donde se almacenan los archivos del sitio web. (El directorio definido en el paso 3 del documento de instalación).

2. Reiniciar el application pool en IIS.

3. Verificar en el directorio de logs que se genere correctamente los archivos **.log**:



4. Verificar que el servicio este funcionando correctamente accediendo a: http://[host]:[port]/operaciones/status

5. Verificar que el sitio tenga acceso a la base de datos accediendo http://[host]:[port]/operaciones/var?cod=ABIERTO

6. Probar el webhook emitiendo un POST request contra el método **informar.** Este es el método de la API que se debe usar desde Raiden para informarle sus operaciones a FPA.

A continuación, se pude ver un ejemplo sobre como emitir el POST request utilizando CURL:

curl --ntlm -u : -X POST -d '{ "idRaiden" : "RDN00001" }' http://[host]:[port]/operaciones/informar

Si el StatusCode de la respuesta es 200 o 400, el webhook está funcionando correctamente.

También se puede utilizar otras herramientas como Fiddler o Postman.

Otra opción es acceder a http://[host]:[port]/operaciones/formulario desde el navegador.

FPA

En esta página se muestra un formulario HTML que realiza la llamada al webhook a través de javascript.

(Se solicitan credenciales windows)

En caso de que el servicio del app pool se detenga inesperadamente:

- Revisar si los logs de raiden se estén grabando correctamente y verificar si hay algún mensaje de error.
- Revisar los logs de IIS en el Event viewer.
- Verificar el estado del usuario que corre el app pool. Puede estar deshabilitado o con contraseña expirada. Se recomienda que usuario no tenga políticas de contraseña.

En tal caso, el mensaje de error es similar al siguiente:

> *La identidad del grupo de aplicaciones fpa_ws no es válida. Puede que el nombre de usuario o la contraseña especificados no sean correctos o que el usuario no tenga derechos de inicio de sesión por lotes Si no se corrige la identidad, el grupo de aplicaciones se deshabilitará cuando reciba su primera solicitud. Si el problema se produce por los derechos de inicio de sesión por lotes, se deberá cambiar la identidad en el almacén de configuración de IIS una vez que se hayan concedido los derechos para que el servicio WAS (Windows Process Activation Service) intente de nuevo el inicio de sesión. El grupo de aplicaciones será deshabilitado si la identidad sigue siendo no válida tras procesar la primera solicitud para dicho grupo.*