PLATINA v3 - Plataforma Corporativa de Interoperabilidad

Desactivar SSLv3 en productos

Versión: 0101

Fecha:16/12/2013

[3.2.0.0]

HOJA DE CONTROL

Organismo	**Consejería de Hacienda y Administración Pública**		
Proyecto	PLATINA v3 - Plataforma Corporativa de Interoperabilidad		
Entregable	Desactivar SSLv3 en productos		
Autor	Servicio de Coordinación y Desarrollo de Sistemas Horizontales		
Aprobado por		**Fecha Aprobación**	
		Nº Total de Páginas	15

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Versión inicial	Srv. de Coord. y Desarrollo de Sistemas Horizontales	30/10/2014

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Juan Sebastián Ojeda Pérez (SCDSH)
Antonio Blanco Morales (SCDSH)
Francisco Rodríguez Corredor (SCDSH)
Juan Antonio Campano Berlanga (SCDSH)

1 INTRODUCCIÓN

El objetivo de este documento es indicar las configuraciones necesarias que se deben aplicar a los diferentes productos con base Carbon 4.1.X y 4.0.X, para desactivar el protocolo SSLv3 debido al reciente problema de seguridad publicado acerca del mismo, conocido como POODLE (Padding Oracle On Downgrade Legacy Encription)

2 Desactivar SSLv3 en productos Carbon

Toda la configuración descrita, se realizará siempre con las instancias paradas.

Para desactivar el soporte SSL 3.0 en los servidores con base Carbon 4.1.X y 4.0.X, se deben seguir las siguientes instrucciones:

- Abrir $HOME_PRODUCTO/repository/conf/tomcat/catalina-server.xml

- Buscar la configuración del conector correspondiente a TLS (normalmente configuración con puerto 9443 y parámetro **sslProtocol** como **TLS**):

```
<Connector  protocol="org.apache.coyote.http11.Http11NioProtocol"
        port="9443"
        bindOnInit="false"
        sslProtocol="TLS"
        maxHttpHeaderSize="8192"
        acceptorThreadCount="2"
        maxThreads="250"
        minSpareThreads="50"
        disableUploadTimeout="false"
        enableLookups="false"
        connectionUploadTimeout="120000"
        maxKeepAliveRequests="200"
        acceptCount="200"
        server="WSO2 Carbon Server"
        clientAuth="false"
        compression="on"
```

```
        scheme="https"

        secure="true"

        SSLEnabled="true"

        compressionMinSize="2048"

        noCompressionUserAgents="gozilla, traviata"

                                compressableMimeType="text/html,text/javascript,application/x-
javascript,application/javascript,application/xml,text/css,application/xslt+xml,text/xsl,image/gif,image/jpg,ima
ge/jpeg"

        keystoreFile="${carbon.home}/repository/resources/security/wso2carbon.jks"

        keystorePass="wso2carbon"

        URIEncoding="UTF-8"/>
```

- Si se está utilizando JDK 1.6, quitar el atributo **sslProtocol=”TLS”** y establecer en su lugar **sslEnabledProtocols=”TLSv1”,** quedando la configuración de la siguiente forma:

```
<Connector  protocol="org.apache.coyote.http11.Http11NioProtocol"

        port="9443"

        bindOnInit="false"

        sslEnabledProtocols="TLSv1"

        maxHttpHeaderSize="8192"

        acceptorThreadCount="2"

        maxThreads="250"

        minSpareThreads="50"

        disableUploadTimeout="false"

        enableLookups="false"

        connectionUploadTimeout="120000"

        maxKeepAliveRequests="200"

        acceptCount="200"

        server="WSO2 Carbon Server"
```

```
        clientAuth="false"

        compression="on"

        scheme="https"

        secure="true"

        SSLEnabled="true"

        compressionMinSize="2048"

        noCompressionUserAgents="gozilla, traviata"

                                compressableMimeType="text/html,text/javascript,application/x-
javascript,application/javascript,application/xml,text/css,application/xslt+xml,text/xsl,image/gif,image/jpg,ima
ge/jpeg"

        keystoreFile="${carbon.home}/repository/resources/security/wso2carbon.jks"

        keystorePass="wso2carbon"

        URIEncoding="UTF-8"/>
```

- Si se está utilizando JDK 1.7, quitar el atributo **sslProtocol=”TLS”** y establecer en su lugar **sslEnabledProtocols=”TLSv1,TLSv1.1,TLSv1.2”,** quedando la configuración de la siguiente forma:

```
<Connector  protocol="org.apache.coyote.http11.Http11NioProtocol"

        port="9443"

        bindOnInit="false"

        sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

        maxHttpHeaderSize="8192"

        acceptorThreadCount="2"

        maxThreads="250"

        minSpareThreads="50"

        disableUploadTimeout="false"

        enableLookups="false"

        connectionUploadTimeout="120000"
```

```
maxKeepAliveRequests="200"

acceptCount="200"

server="WSO2 Carbon Server"

clientAuth="false"

compression="on"

scheme="https"

secure="true"

SSLEnabled="true"

compressionMinSize="2048"

noCompressionUserAgents="gozilla, traviata"

                                        compressableMimeType="text/html,text/javascript,application/x-
javascript,application/javascript,application/xml,text/css,application/xslt+xml,text/xsl,image/gif,image/jpg,ima
ge/jpeg"

keystoreFile="${carbon.home}/repository/resources/security/wso2carbon.jks"

keystorePass="wso2carbon"

URIEncoding="UTF-8"/>
```

2 Configuración de los productos que tengan activado Pass-Thru transport

Para cambiar la configuración de los productos que tengan activado el transporte PTT (WSO2 ESB, WSO2 API Manager), habrá que realizar la siguiente configuración:

- Abrir $HOME_PRODUCTO/repository/conf/axis2/axis2.xml

- Localizar la configuración de **transportReceiver** para **org.apache.synapse.transport.passthru.PassThroughHttpSSLListener**

- Si se esta utilizando JDK 1.6, añadir el parámetro:

  <parameter name="HttpsProtocols">TLSv1</parameter>

  a la configuración de dicho transporte, quedando de la siguiente forma:

```
 <transportReceiver name="https"
class="org.apache.synapse.transport.passthru.PassThroughHttpSSLListener">

        <parameter name="port" locked="false">8243</parameter>

        <parameter name="non-blocking" locked="false">true</parameter>

        <parameter name="bind-address" locked="false">esb.worker.pci.int.i-administracion.junta-
andalucia.es</parameter>

        <parameter name="WSDLEPRPrefix" locked="false">https://esb.worker.pci.int.i-administracion.junta-
andalucia.es</parameter>

        <parameter name="httpGetProcessor"
locked="false">org.wso2.carbon.transport.nhttp.api.PassThroughNHttpGetProcessor</parameter>

        <parameter name="keystore" locked="false">

           <KeyStore>

              <Location>repository/resources/security/wso2carbon.jks</Location>
```

```
            <Type>JKS</Type>
            <Password>wso2carbon</Password>
            <KeyPassword>wso2carbon</KeyPassword>
         </KeyStore>
      </parameter>
      <parameter name="truststore" locked="false">
         <TrustStore>
            <Location>repository/resources/security/client-truststore.jks</Location>
            <Type>JKS</Type>
            <Password>wso2carbon</Password>
         </TrustStore>
      </parameter>
      <parameter name="HttpsProtocols">TLSv1</parameter>
   </transportReceiver>
```

- Si se esta utilizando JDK 1.7, añadir el parámetro:

  <parameter name="HttpsProtocols">TLSv1,TLSv1.1,TLSv1.2</parameter>

  a la configuración de dicho transporte, quedando de la siguiente forma:

```
 <transportReceiver name="https"
class="org.apache.synapse.transport.passthru.PassThroughHttpSSLListener">
      <parameter name="port" locked="false">8243</parameter>
      <parameter name="non-blocking" locked="false">true</parameter>
      <parameter name="bind-address" locked="false">esb.worker.pci.int.i-administracion.junta-
andalucia.es</parameter>
      <parameter name="WSDLEPRPrefix" locked="false">https://esb.worker.pci.int.i-administracion.junta-
```

```
andalucia.es</parameter>

        <parameter name="httpGetProcessor"
locked="false">org.wso2.carbon.transport.nhttp.api.PassThroughNHttpGetProcessor</parameter>

        <parameter name="keystore" locked="false">

            <KeyStore>

                <Location>repository/resources/security/wso2carbon.jks</Location>

                <Type>JKS</Type>

                <Password>wso2carbon</Password>

                <KeyPassword>wso2carbon</KeyPassword>

            </KeyStore>

        </parameter>

        <parameter name="truststore" locked="false">

            <TrustStore>

                <Location>repository/resources/security/client-truststore.jks</Location>

                <Type>JKS</Type>

                <Password>wso2carbon</Password>

            </TrustStore>

        </parameter>

        <parameter name="HttpsProtocols">TLSv1,TLSv1.1,TLSv1.2</parameter>

    </transportReceiver>
```

3 Validación de la configuración aplicada

Para asegurar la correcta configuración de la solución, se suministra utilidad java (TestSSLServer.jar) que indica las versiones de protocolo soportadas. Ejecutar el siguiente comando:

$ java -jar TestSSLServer.jar host_servidor 9443 (habrá que tener en cuenta el Offset para cada uno de los servidores)

o bien

$ java -jar TestSSLServer.jar host_esb 8243 (para verificar el puerto utilizado por el transporte PTT y teniendo en cuenta el Offset)

La salida que produciría antes de aplicar la solución descrita en este documento sería similar a:

```
Supported versions: SSLv3 TLSv1.0

Deflate compression: no

Supported cipher suites (ORDER IS NOT SIGNIFICANT):

  SSLv3

    RSA_EXPORT_WITH_RC4_40_MD5

    RSA_WITH_RC4_128_MD5

    RSA_WITH_RC4_128_SHA

    RSA_EXPORT_WITH_DES40_CBC_SHA

    RSA_WITH_DES_CBC_SHA

    RSA_WITH_3DES_EDE_CBC_SHA

    DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

    DHE_RSA_WITH_DES_CBC_SHA
```

DHE_RSA_WITH_3DES_EDE_CBC_SHA

RSA_WITH_AES_128_CBC_SHA

DHE_RSA_WITH_AES_128_CBC_SHA

RSA_WITH_AES_256_CBC_SHA

DHE_RSA_WITH_AES_256_CBC_SHA

(TLSv1.0: idem)

Después de aplicar los cambios sería:

Supported versions: TLSv1.0

Deflate compression: no

Supported cipher suites (ORDER IS NOT SIGNIFICANT):

TLSv1.0

RSA_EXPORT_WITH_RC4_40_MD5

RSA_WITH_RC4_128_MD5

RSA_WITH_RC4_128_SHA

RSA_EXPORT_WITH_DES40_CBC_SHA

RSA_WITH_DES_CBC_SHA

RSA_WITH_3DES_EDE_CBC_SHA

DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

DHE_RSA_WITH_DES_CBC_SHA

DHE_RSA_WITH_3DES_EDE_CBC_SHA

RSA_WITH_AES_128_CBC_SHA

DHE_RSA_WITH_AES_128_CBC_SHA

RSA_WITH_AES_256_CBC_SHA

DHE_RSA_WITH_AES_256_CBC_SHA

Productos y versiones afectadas en la Plataforma PLATINA

A continuación de detallan los productos afectados dentro de la Plataforma Platina:

Nombre Producto	Versión Producto	Versión Carbon
WSO2 ESB	4.7.0	4.1.4
WSO2 DSS	3.0.1	4.0.5
WSO2 Gobernance Registry	4.5.3	4.0.5
WSO2 BAM	2.2.0	4.0.7
WSO2 Message Broker	2.1.1	4.1.7
WSO2 Identity Server	4.1.0	4.0.7

4 Bibliografía y referencias

Exploiting the SSL 3.0 Fallback:

https://www.openssl.org/~bodo/ssl-poodle.pdf