Database Management Console

May 7, 2015
Announcing TLS (Transport Layer Security) feature

BMC is announcing support for TLS (Transport Layer Security) version 1.0 in the Database Management Console. The use of TLS is optional and no changes are required if you do not intend to use TLS. The following products are affected:

- BMC Log Analyzer for IMS
- BMC System Administration for IMS
- BMC System Communication for IMS
- BMC Workbench for DB2
- DELTA IMS DB/DC
- DELTA IMS DC
- DELTA IMS for DBCTL
- DELTA IMS VIRTUAL TERMINAL
- DELTA PLUS
- DELTA PLUS for DBCTL
- DELTA PLUS VIRTUAL TERMINAL
- Energizer for IMS Connect
- EXTENDED TERMINAL ASSIST PLUS
- LOCAL COPY PLUS
- MAXM Database Advisor for IMS
- Message Advisor for IMS

**Note**
If you have questions, contact Customer Support at 1 800 537 1813 (United States or Canada) or call your local support center.

To view the latest BMC documents, see the Support Central website at http://www.bmc.com/support. Notices such as flashes, technical bulletins, and release notes are available on the website. You can subscribe to proactive alerts to receive e-mail messages when notices are issued or updated. For more information about proactive alerts, see the Support Central website.
Implementing TLS

To implement TLS, you need to indicate the level of encryption you want and specify the location of the server certificate and ICSF label of the private key that matches the certificate’s public key.

**Before you begin**

Have the following items in place:

- In IBM Resource Access Control Facility (RACF):
  - A TLS certificate
  - A certificate authorization chain
  - A key ring with the TLS certificate connected first followed by any intermediate certificates used to sign the key

- Have Integrated Cryptographic Service Facility (ICSF)

  The ICSF Private Key Data Set (PKDS) should contain the private key that matches the TLS certificate.

**To implement TLS**

1. Obtain and accept PUT1501B and the following PTFs:
   - BPJ1004
   - BPJ1006
   - BPJ1029
   - BPJ1030

   BMC recommends using BMC Internet Service Retrieval (ISR) to obtain PTFs. For information about ISR, see the maintenance information in the *Installation System Reference Manual*.

   You can also obtain PTFs from eFix PTF Distribution Services (eFix). You can access eFix directly at [http://apps.bmc.com/support/efix.cgi](http://apps.bmc.com/support/efix.cgi) or from the support site. For information about eFix, see the online Help.

2. Open for edit your User Interface Middleware (UIM) startup member.

   The UIM startup member is an XML document that defines global operation parameters for the UIM Server.

   The UIM startup member is specified as the -M member name on the EXEC statement in the UIM Server PROC. This member is in the HTTPPARM DD concatenation, usually found in the UBMCCNFG data set.
3 In the startup member, add or edit the following parameter to define the encryption level required:

```xml
<BMC_PARM ID="ENCRYPTION_LEVEL" VALUE="encryptValue" />
```

An example of the UIM startup member is provided in “Example UIM startup member” on page 4. Use one of the following values for `encryptValue`:

- **SSL-IF**
  Uses SSL/TLS if the client supports it. This is the recommended value for an initial implementation to allow existing clients to connect.

- **SSL-REQUIRED**
  Does not accept a connection unless it is a TLS handshake. This option should be used with caution because any existing client connections will not work until the client code level has been reinstalled to the updated client with the TLS support. This will require a reinstall of the client and not an update.

---

**Note**

SSL-REQUIRED causes any legacy client and Database Performance for DB2 connections to not work. It is strongly recommended that SSL-IF be implemented and once all clients are updated, then switch to SSL-REQUIRED. If Database Performance for DB2 is being used, SSL-REQUIRED should not be implemented until support for SSL is available in Database Performance for DB2.

4 In the startup member, add the following section to define the location for the UIM Server certificate and associated private key:

```xml
<BMC_PARM ID="SSL_STORE" VALUE="certStorage">
  <BMC_PARM ID="SSL_CERTIFICATE" VALUE="owner/KeyRingName" />
</BMC_PARM>

<BMC_PARM ID="SSL_STORE" VALUE="ICSF">
  <BMC_PARM ID="SSL_PRIVATE_KEY" VALUE="icsf.private.key.label" />
</BMC_PARM>
```

An example of the UIM startup member is provided in “Example UIM startup member” on page 4. The keywords and valid values are:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Valid entries for associated VALUE keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_STORE (first occurrence)</td>
<td>Names the storage medium for the certificate.</td>
<td>Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DSN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage is a sequential data set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ R_DATA LIB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage is a RACF key ring and optionally the key ring owner</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
<td>Valid entries for associated VALUE keyword</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSL_CERTIFICATE</td>
<td>Name of the certificate to be used by UIM.</td>
<td>Specify one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ A data set name if DSN was indicated for the associated SSL_STORE keyword</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ A RACF key ring name if R_DATALIB was indicated for the associated SSL_STORE keyword</td>
</tr>
<tr>
<td>SSL_STORE (second occurrence)</td>
<td>Names the storage medium for the private key.</td>
<td>ICSF indicates that the storage is an ICSF label.</td>
</tr>
<tr>
<td>SSL_PRIVATE_KEY</td>
<td>Name of the private key to be used by UIM.</td>
<td>Specify the name of the ICSF label.</td>
</tr>
</tbody>
</table>

5  Save and close your User Interface Middleware (UIM) startup member.

6  Repeat steps Step 2 on page 2 through Step 5 on page 4 for every instance of the UIM Server that you have.

Example UIM startup member

The following example of the UIM startup member indicates where to change or insert the required statements:
Example UIM startup member

```
<BMCHTTP>

<!-- This is an example of an XML comment -->
<!--
This is the UIM Server configuration file. For co-existence
with MVS tape building utilities it is kept to a maximum of
.
.
.
-->  

<BMC_PARM ID="PORT"
   VALUE="3683" />
<BMC_PARM ID="AUTH_TIMEOUT_SECS"
   VALUE="1800" />
<BMC_PARM ID="AFF_TIMEOUT_SECS"
   VALUE="1800" />
<BMC_PARM ID="HFS_DATASET"
   VALUE="hlq.HFS" />
<!-- Command support - YES/NO/AUTHCRIZE(UIMLogon req'ed) -->
<BMC_PARM ID="ALLOW_NETCMD"
   VALUE="YES" />

<!-- ENCRYPTION_LEVEL = NO/CREDENTIALS-IF/CREDENTIALS-REQUIRED/SSL-IF/SSL-REQUIRED -->
<BMC_PARM ID="ENCRYPTION_LEVEL"
   VALUE="SSL-IF" />

<!-- Root path for USS HFS files - The UIM server started task user must
   have read/write access to this path. -->
<BMC_PARM ID="USG_HFS_ROOT" VALUE="/tmp/bmcuiim" />

<!-- Definition for SSL Server Certificate and Private Key.

   SSL_STORE        Names the storage medium for the certificate and
                   private key.
   .
   .
   
   SSL_PRIVATE_KEY  Name of the private key matching the certificate
   -->

<!-- RACF Exported Certificate 'UIM.TLS.TESTING'
   This certificates private key type is ICSF. -->
<BMC_PARM ID="SSL_STORE" VALUE="DSN">
   <BMC_PARM ID="SSL_CERTIFICATE"
      VALUE="RGS.UIM.PUBLIC.CERT" />
  <!-- VALUE="UIM.TLS.TESTING" / -->
</BMC_PARM>

<!-- private key for exported certificate UIM.TLS.TESTING -->
<BMC_PARM ID="SSL_STORE" VALUE="ICSF">
   <BMC_PARM ID="SSL_PRIVATE_KEY"
      VALUE="UIM.TLS.TESTING" />
</BMC_PARM>

</BMCHTTP>
```
Reinstalling the Database Management Console

After implementing TLS, you will have to reinstall the Database Management Console.

To reinstall the Database Management Console

1. Open the Database Management Console as you normally would.
   
   A pop-up might be displayed indicating that the certificate is not trusted. This can occur if the certificate is self-signed, the intermediate certificate authority certificates are not in the RACF key ring, or the root certificate authority certificate is not in the trust store.

2. (optional) Accept the certificate.

3. Cut and paste the provided Uniform Resource Locator (URL) into your browser's address bar and press Enter.
   
   A pop-up is displayed that provides the URL.

   The Database Management Console is reinstalled and opened.

After implementing and reinstalling the Database Management Console, the connection icon will include an SSL indicator as shown in the following figure:
End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

BMC SOFTWARE INC
2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA
Telephone 1 713 918 8800 (or 1 800 841 2031 United States and Canada)
Customer Support: 1 800 537 1813 (United States and Canada) or contact your local support center