Customer Coffee Corner for SAP IQ – Encryption – Part 2

SAP Product Support
January, 2018
Agenda

- Objectives
- Advanced security in SAP IQ
- Encryption - Columns
- Encryption - Database
- FAQs
- Closing remarks
- Open discussion
Objectives

- Proactive outreach based on feedbacks
- Target audience – IQ DBAs Novice/Beginner
- Awareness about advanced security in SAP IQ avoiding “how to” IQ incidents. Part 2 scope and discussion is limited to encryption of columns and database.
Advanced security in SAP IQ (Birds eye view)

**Encryption**

**Part 1 - Over the wire, “in motion”**

Password, Data packets
data is unreadable to anyone who is sniffing network traffic

**Part 2 – In memory, “In use”**

On disk, “At rest”

User data in column
Unreadable to anyone with SQL access but without key

User data in entire database
Dbfile data unreadable to anyone by looking at disk.
Encryption – Encryption term definitions

- **Plaintext**
  data in its original, intelligible form.
  Plaintext is not limited to string data, but is used to describe any data in its original representation.

- **Ciphertext**
  data in an unintelligible form that preserves the information content of the plaintext form.

- **Encryption**
  a reversible transformation of data from plaintext to ciphertext. Also known as enciphering.

- **Decryption**
  the reverse transformation of ciphertext back to plaintext. Also known as deciphering.

- **Key**
  a number used to encrypt or decrypt data.
  Symmetric-key encryption systems use the same key for both encryption and decryption.
  Asymmetric-key systems use one key for encryption and a different (but mathematically related) key for decryption.
  **The SAP IQ interfaces accept character strings as key.**

- **AES**
  Advanced Encryption Standard, a FIPS-approved cryptographic algorithm for the protection of sensitive (but unclassified) electronic data.
  **SAP IQ supports AES algorithm.**
Encryption - Columns

- Default behavior – Column is not encrypted.
  SAP IQ compresses column data on disk regardless of whether the column itself is encrypted.
  There is no customer-visible way of decompressing column on disk.
  There is no way to change what compression algorithm is used or disable compression. It is done internally in the product.

- Separate licensing options – 2
  IQ_SECURITY, IQ_UDA (only if encrypted values are LONG BINARY)

- Supported datatypes for encryption

- Encryption methods – 2
  aes_encrypt() AES_ENCRYPT(<case-sensitive-string-expression>|<binary value>|<supported datatype value>, <key>)
  Load Table Encrypted Clause ENCRYPTED(<data-type>‘<key>’[, ‘<algorithm-string>’] )

- Decryption methods - 1
  aes_decrypt() AES_DECRYPT(<ciphertext in varbinary>, <key> [, <data-type> ] )

- Database options – 4 with recommendations
  string_rtruncation – ON
  conversion_error – 1
  ase_binary_display – OFF
  aes_encrypt_header_format – depends on source database version before upgrading
Encryption - Columns

- **Key** – Required every time while encrypting and decrypting the data.
  At least 16 characters long, a mix of uppercase and lowercase letters, includes numbers and special characters.
  Protect the encryption key by using user-defined functions (UDFs), other views, or both.

- **After encryption Datatype is VARBINARY**, length after encryption is multiples of 16 bytes with minimum of 32 bytes
  
  \[
  \text{DATALENGTH}(\text{ciphertext}) = (((\text{DATALENGTH}(\text{plaintext}) + 15) / 16) + 1) \times 16
  \]

- **Considerations –**
  Decrypting into original data value requires knowledge of original datatype of the input data, not the datatype of the storage field.
  CAST() original input values to the destination column datatype.
  When declaring encrypted column, use minimum varbinary(32).

- **Implementation – Example**
  Understand storage impact.
  - Identify target tables/columns for encryption.
  - Decide whether to keep both unencrypted and encrypted data.

  Understand application impact.
  - Identify key and Decide how to protect the key. This will involve creating UDFs or views or both.
  - If encrypted columns are used in joins, note that only 4 predicates can be used ( = , <> , IS NULL , IS NOT NULL )
  - Understand how non-previleged users can use encrypted predicates in joins without knowing encryption key.
--- Decrypting into original data value requires knowledge of original datatype of the input data, not the datatype of the storage field

--- This example requires multiple aes_decrypt() to get original values.
create table test( c1 int , ec1 varbinary(32) ) ;
insert test select 1 , aes_encrypt( 1 , 'Secret' ) ;
insert test select 1234567 , aes_encrypt( 1234567 , 'Secret' ) ;
select c1 , aes_decrypt( ec1 , 'Secret' ) from test ;

select c1 , aes_decrypt( ec1 , 'Secret' , integer ) from test ;  -- Decryption error: Incorrect CAST type integer for decrypt data of type smallint.
select c1 , aes_decrypt( ec1 , 'Secret' , smallint ) from test where c1 = 1 ;
select c1 , aes_decrypt( ec1 , 'Secret' , integer ) from test where c1 = 1234567 ;

--- CAST() original input values to the destination column datatype

--- This example requires multiple aes_decrypt() to get original values.
create table test( c1 int , ec1 varbinary(32) ) ;
insert test select 1 , aes_encrypt( cast( 1 as integer ) , 'Secret' ) ;
insert test select 1234567 , aes_encrypt( cast ( 1234567 as integer ) , 'Secret' ) ;
select c1 , aes_decrypt( ec1 , 'Secret' , integer ) from test ;  -- No Decryption error

--- When declaring encrypted column, use minimum varbinary(32).
create table test( c1 varbinary ) ;
insert into test values( aes_encrypt(100,'seCr3t') ) ;  -- Data exception - string data, right truncation
alter table test add c2 varbinary(32) ;
insert test values( 100 , aes_encrypt(100,'seCr3t') ) ;
select datalength( c1 ) , datalength( c2 ) from test ;
Encryption - Database

- Default behavior – Database is not encrypted.
  SAP IQ compresses data on while saving to the disk.
  There is no customer-visible way of decompressing data on disk.
  There is no way to change what compression algorithm is used or disable compression. It is done internally in the product.

- Separate licensing options – 1
  IQ_SECURITY

- Encryption methods – 2
  iqinit
  create database

- Decryption methods - None

- Startup flags –
  -ek key, provide key after flag
  -ep, prompts user to enter key
FAQs -

- **What if the encryption key is lost?**
  If you lose the encryption key, there is no way to access the data, even with the assistance of Technical Support. The database must be discarded and you must create a new database. The column must be recreated from other data sources.

- **Can column encryption be tested without IQ_SECURITY license?**
  Yes. When any feature is used for only testing, license related to such feature will be checked out in 1 month grace mode. After grace period ends, IQ does not automatically forbids user from use of unlicensed option. It will shutdown. To prevent IQ auto shutdown at the end of the grace period, perform the following, before the end of the grace period:

  Plan a down time, stop and restart IQ
  Run: `sp_iqlmconfig() 'disallow', '<license_type_name>'`
  Stop and restart IQ again.
  Run: `sp_iqlmconfig` and check the feature option is "Disallowed"

- **Is there any storage overhead of using column encryption?**
  Yes. Refer ciphertext datalength chart. Apply it to columns encrypted, column datatype, number of data values.
FAQs -

Is there an easy to refer ciphertext data length conversion chart?

<table>
<thead>
<tr>
<th>CipherText</th>
<th>PlainText</th>
<th>Other datatypes</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>0</td>
<td>numeric(1,0) – numeric(20,0), tinyint, smallint, int, bigint</td>
</tr>
<tr>
<td>32</td>
<td>1-16</td>
<td>numeric(21,0) – numeric(52,0)</td>
</tr>
<tr>
<td>48</td>
<td>16-32</td>
<td>numeric(53,0) – numeric(84,0)</td>
</tr>
<tr>
<td>64</td>
<td>33-48</td>
<td>numeric(85,0) – numeric(116,0)</td>
</tr>
<tr>
<td>80</td>
<td>49-64</td>
<td>numeric(117,0) – numeric(128,0)</td>
</tr>
<tr>
<td>96</td>
<td>65-80</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>81-96</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>97-112</td>
<td></td>
</tr>
<tr>
<td>144</td>
<td>113-128</td>
<td></td>
</tr>
<tr>
<td>160</td>
<td>129-144</td>
<td></td>
</tr>
<tr>
<td>176</td>
<td>145-160</td>
<td></td>
</tr>
<tr>
<td>192</td>
<td>161-176</td>
<td></td>
</tr>
<tr>
<td>208</td>
<td>177-192</td>
<td></td>
</tr>
<tr>
<td>224</td>
<td>193-208</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td>208-224</td>
<td></td>
</tr>
</tbody>
</table>
FAQs -

• How to hide functions and views with column encryption key?
  Use “set hidden” clause. Eg. Alter view xyz set hidden

• How to automate scripts involving start_iq and yet hide database encryption?
  In scripts using start_iq, use environmental variables. Populate them before calling script.
  $ setenv DBKEY foobar
  $ start_iq @params.cfg DEVIQ.db ${DBKEY:+-ek $DBKEY}

• Is –ek hidden in ps output?
  Yes. Key is hidden in ps output.

• Will object text be accessible even though it is hidden?
  Yes. It is accessible but obfuscated.
  > create view tv as select 1
  > sp_helptext tv  returns ( create view "DBA"."tv" as select 1 )
  > alter view tv set hidden
  > sp_helptext tv  returns ( create view "DBA"."tv" hidden
  ')((!!)$($$$)$&&&$$)((!!)$())[b5!x$%!#@5$5x5(5$05@xb@b!m!b$%$@x' )
FAQs -

- Is there any feature for encrypting entire table?
  No. User has to encrypt each column in table.

- Is there any change in database connection parameters if database is encrypted?
  No.

- How to check whether database is encrypted or not?
  `select property( 'commandline' )`, returns `commandline` with which server started. Existence of `-ek` with `*` indicates that it is encrypted database with a key.

- How to backup and restore encrypted database?
  Backup – regular "backup database" sql command
  Restore – regular "restore database" sql command but add key clause.

- How to extract everything from database so that unencrypted<->encrypted database migration can be done?
  Use `iqunload` with `-n` option
FAQs -

• Is there any performance overhead of using database encryption?
   Yes. Performance is slower when the database is encrypted. The performance impact depends on how often pages are read from or written to disk, and can be minimized by ensuring that the server is using an adequate cache size. Increase the starting size of the cache with the -c option.

• Can encrypted and unencrypted data get mixed in column?
   Yes. From SAP IQ perspective all data is all varbinary. End-user should prevent such activity.

• Can encrypted column joined with non-encrypted column in a query?
   Yes, nothing prevents it. It is a meaningless operation. SAP IQ will simply make sure both sides of predicate are varbinary.
KBA’s - specific to today’s topic

2077639 - New database option AES_Encrypt_Header_Format has been added
1957044 - Data extraction facility cannot be converted the decrypted numeric type - SAP IQ

2480880 - Decryption error Input must be a multiple of 16 bytes - SAP IQ
2480936 - Decryption error "Input passed to decrypt has length ..." - SAP IQ
2239576 - LOAD TABLE with ENCRYPTED() shows decryption key in sqllog - SAP IQ
2237776 - aes_decrypt() causes crash - SAP IQ

2228977 - How to use a database encryption key - SAP IQ
KBA’s - product specific

2309381 – Customer Virtual Coffee corner for ASE, IQ, Replication Server, Software Developers Kit …
2137179 – Customer Coffee Corner for SAP IQ – Americas

2580620 - How to set up network keepalive - SAP IQ
2583231 - SAP IQ server crashes with the phrases hos_RWLock::UnLock() and s_bufpool::Sweep() - SAP IQ
2583897 - After upgrade from SAP IQ 15.4, update fails with s_mergeRHSReader::WriteCurrentBlock - SAP IQ
2584345 - Coordinator denies new connections for few minutes intermittently - SAP IQ
2589639 - How does Load work in IQ ? -- SAP IQ
2590223 - @@trancount increase after exiting from stored procedure - SAP IQ

2583132 - After upgrade IQ Cockpit RSL error 1 of 2 in Monitor tab while Explore and Alert tabs are working fine - SAP IQ Cockpit

2593658 - When connect to NLS (IQ) , raised error " Unable to load libdbodbc16.so' " , under SAP HANA/BW + NearLine-Solution with IQ
Closing Remarks

• What’s next?

• Please provide your feedback to IQ VCC coordinators on
  – Did you learn something new/useful?
  – Did this outreach help understanding column and database encryption better?
Any Questions ?
Thank you