A Deep Dive into Encryption at Rest

Dinç Çiftçi
he/him
Sr. Software Engineer
Tableau

Jakob Mund
he/him
Product Manager
Tableau

#data19
Benefits of Encryption at Rest

1. Increased security for already published extracts
2. Publish sensitive data to Tableau Server that may not be previously allowed
3. Helps achieve compliance
What does this session cover?

- Introduction to Encryption at Rest for Extracts
- Demo: Configuring and Managing Encryption at Rest
- Security Internals
- Backup and Site Import/Export
- Key Rotation
- Performance
- Q&A
Introduction to Encryption at Rest for Extracts
What is an extract?

Excerpts

Encryption
A compressed snapshot of data stored on disk and loaded into memory as required to render a Tableau viz.”

Gordon Rose

Understanding Tableau Data Extracts
### Sales Target Extract

Extract will include all data.

<table>
<thead>
<tr>
<th>Office Supplies</th>
<th>03.01.2014</th>
<th>15</th>
<th>Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Supplies</td>
<td>04.01.2014</td>
<td>300</td>
<td>Home Office</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>05.01.2014</td>
<td>21</td>
<td>Consumer</td>
</tr>
<tr>
<td>Furniture</td>
<td>06.01.2014</td>
<td>2,316</td>
<td>Home Office</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>17</td>
<td>Consumer</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>14</td>
<td>Corporate</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>699</td>
<td>Home Office</td>
</tr>
</tbody>
</table>
### Sales Target Extract

**Extract will include all data.**

<table>
<thead>
<tr>
<th>Category</th>
<th>Order Date</th>
<th>Sales Target</th>
<th>Segment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office Supplies</td>
<td>03.01.2014</td>
<td>15</td>
<td>Consumer</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>04.01.2014</td>
<td>300</td>
<td>Home Office</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>05.01.2014</td>
<td>21</td>
<td>Consumer</td>
</tr>
<tr>
<td>Furniture</td>
<td>06.01.2014</td>
<td>2,316</td>
<td>Home Office</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>17</td>
<td>Consumer</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>14</td>
<td>Corporate</td>
</tr>
<tr>
<td>Office Supplies</td>
<td>06.01.2014</td>
<td>699</td>
<td>Home Office</td>
</tr>
</tbody>
</table>
What is an extract?

• Benefits:
  • Faster query performance
  • Reduced load on production databases
  • Offline analysis
  • Consistent point-in-time data

• Can be bundled with a workbook, data source, flow

• Stored on the file system on Tableau Server
What is encryption?
What is encryption?

- Translating data such that it can only be read by those who hold the encryption key
What is encryption?

- Translating data such that it can only be read by those who hold the encryption key
- Plaintext: Un-encrypted data
- Ciphertext: Encrypted data
What is encryption?

- Translating data such that it can only be read by those who hold the encryption key
- Plaintext: Un-encrypted data
- Ciphertext: Encrypted data
- Encryption key: A random string of data that is used to encrypt the plaintext. The key is needed to convert ciphertext back into plaintext
What is encryption?

- Translating data such that it can only be read by those who hold the encryption key
- Plaintext: Un-encrypted data
- Ciphertext: Encrypted data
- Encryption key: A random string of data that is used to encrypt the plaintext. The key is needed to convert ciphertext back into plaintext
- Cipher: The computational method (or algorithm) used to convert the plaintext into ciphertext
What is Encryption at Rest for Extracts?
What is Encryption at Rest for Extracts?

- Available starting with Tableau Server 2019.3
- Data in extracts is encrypted when stored on disk in Tableau Server
What is Encryption at Rest for Extracts?

• Temporary files, caches, logs, workbooks, external files (e.g., .csv) are not encrypted
What is Encryption at Rest for Extracts?

- Temporary files, caches, logs, workbooks, external files (e.g., .csv) are not encrypted
- *Extracts only!*
What is Encryption at Rest for Extracts?

- Encryption happens through a background job after an extract is published
What is Encryption at Rest for Extracts?

- Encryption happens through a background job after an extract is published
- Decryption happens in-memory when needed
What is Encryption at Rest for Extracts?

• Works with Tableau Desktop, Server APIs, and various third party tools seamlessly
What is Encryption at Rest for Extracts?

- Works with Tableau Desktop, Server APIs, and various third party tools seamlessly
- Refreshing an extract keeps it encrypted
What is Encryption at Rest for Extracts?

- Works with Tableau Desktop, Server APIs, and various third party tools seamlessly
- Refreshing an extract keeps it encrypted
- No performance impact for end-users, but increased server load
Demo: Setting up and Managing Encryption at Rest
Extract Encryption at Rest

You can specify whether extracts stored on this site are encrypted.

- Disable: Do not allow encrypted extracts on this site.
- Enable: Allow users to optionally encrypt extracts on this site.
- Enforce: All extracts published and stored on this site are encrypted.

Encryption not running.
0/2 Encrypted
2/2 Unencrypted
Security
## Security Highlights

<table>
<thead>
<tr>
<th>Security Property</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher used for encryption: AES GCM with a 256-bit key</td>
<td>FIPS-approved cryptographic algorithm used across the board. Prevents data tampering.</td>
</tr>
<tr>
<td>Multiple layers (or a hierarchy) of encryption keys</td>
<td>Allows components to do encryption without needing access to more privileged keys</td>
</tr>
<tr>
<td>Scoped encryption keys</td>
<td>Limits the impact of a compromised key</td>
</tr>
</tbody>
</table>
Envelope Encryption
Envelope Encryption
Envelope Encryption
Envelop Encryption

- Keys need to be scoped
Envelope Encryption
Envelope Encryption
Enveloped Encryption
Envelope Encryption

- Keys need to be scoped
- Keys need to be protected
Envelope Encryption
Envelope Encryption
Envelope Encryption
Envelope Encryption
Envelope Encryption

Data Encryption Key

Master Key
Envelope Encryption
Envelop Encryption

Encrypted Extract

Encrypted Data Encryption Key
Envelope Encryption

- Encrypted Data Encryption Key
- Encrypted Extract
Envelope Encryption
Envelope Encryption
Envelope Encryption
Envelope Encryption
Envelope Encryption

Master Key

Data Encryption Key
Envelope Encryption

- Keys need to be scoped
- Keys need to be protected ☑
Envelope Encryption

Master Key

Data Encryption Key
Envelope Encryption

- Master Key
- Data Encryption Keys
Envelope Encryption

Master Key

Data Encryption Keys
Envelope Encryption

No knowledge of the master key
Envelope Encryption

Authorization + audit trail
Envelope Encryption

• Keys need to be scoped ✓
• Keys need to be protected ✓
Envelope Encryption

Master Key

Data Encryption Keys
Key Hierarchy

Master Key ➔ Data Encryption Keys
Key Hierarchy

Master Key

Intermediary Keys

Data Encryption Keys
Key Hierarchy

Master key store encrypts Configuration encryption key encrypts Master extract key

Key encryption key encrypts Data encryption key encrypts Encrypted extract

Key Hierarchy

Master key store encrypts Configuration encryption key encrypts Master extract key

One per extract

Key encryption key encrypts Data encryption key encrypts Encrypted extract
Encryption at Rest for Extracts in Tableau Server 2019.3

https://www.tableau.com/learn/whitepapers/encryption-at-rest
Backup and Site Imports/Exports
How do Backups and Site Import/Export work?

Backup/Restore:
• Extracts stay encrypted
• Keys stored unencrypted in the backup file
• Restore will restore encryption keys from backup

Site Import/Export:
• Extracts are decrypted for site export
• The extracts’ encryption status will be remembered
• Site import will respect the destination’s encryption mode
Checklist for Backup and Import/Export

1. Using custom/third-party backup solutions?
   • Extracts might not be restorable due to key rotation
   • Use site export instead

2. Are size of backups a problem?
   • Size of backups will increase by roughly 2X
   • Create a site for sensitive data only, or selectively encrypt in ‘enabled’ mode
   • Use —no—compression if using encryption to save time

3. Is cluster/backgrounder load a problem?
   • Site import and export will generate additional load spikes
   • Consider scheduling during off-business hours or add capacity (temporarily)

4. Who has access to backup files?
   • Backups contain encryption keys, and extracts in site export are unencrypted
   • Ensure means are in place to limit exposure of backup and site export files
Key Rotation
Key Rotation - When?

- Periodically – e.g. every 6 months
- When privileged staff leave – e.g. Server Admin
- After data migration – Backup/restore
Key Rotation
Key Rotation
Key Rotation
Key Rotation
Key Rotation

Master key store encrypts Configuration encryption key encrypts Master extract key

Key encryption key encrypts Data encryption key encrypts Encrypted extract
Key Rotation

- tsm security regenerate-internal-tokens
Key Rotation

- `tsm security regenerate-internal-tokens`
- `tabcmd reencryptextracts <site-name>`
Key Rotation

- `tsm security regenerate-internal-tokens`
- `tabcmd reencryptextracts <site-name>`

[Diagram showing key rotation process]

Performance
What happens behind the scenes?

Extract (.hyper)
What happens behind the scenes?

Extract
(.hyper)

Column
What happens behind the scenes?

Extract (.hyper)

Data Block
What happens behind the scenes?

Extract (.hyper)

Objects in file
What happens behind the scenes?

Extract (.hyper)

Objects in file
What happens behind the scenes?

Extract (.hyper)

Objects in file
What happens behind the scenes?

Extract (.hyper)

Objects in file
What happens behind the scenes?

Extract (.hyper)

Objects in file

Data Block
What happens behind the scenes?

Extract (.hyper)

Objects in file

Data Block

TABLEAU CONFERENCE
What happens behind the scenes?

Extract (.hyper)

Objects in file

Data Block
What happens behind the scenes?

Extract (.hyper)

Objects in file → Data Block

Tableau Conference
What happens behind the scenes?

Extract (.hyper)

Objects in file

Data Block
What happens behind the scenes?

Extract (.hyper)

Objects in file

Data Block

Extract

$\rightarrow$
Performance Impact

For end-users:
• Loading and interacting has no significant impact
• Vizzes are available right away after publishing

For the Tableau Server cluster:
• Increased backgrounder load and temporary disk space
  • when toggling encryption mode
  • refreshes using API, third-party tools (Alteryx, Informatica, ..) or Tableau Bridge
• Size of backups increase by roughly 2X
Integration with AWS KMS
Integration with AWS KMS

- Moves the highest key in the hierarchy to the cloud
- Allows BYOK
- For deployments in AWS EC2
- Requires the Server Management Add-on
Integration with AWS KMS
Integration with AWS KMS

Master key store
encrypts
Configuration encryption key
encrypts
Master extract key

Key encryption key
encrypts
Data encryption key
encrypts
Encrypted extract
Integration with AWS KMS

AWS customer master key encrypts Root master key encrypts Master extract key

Key encryption key encrypts Data encryption key encrypts Encrypted extract
Integration with AWS KMS

What did we cover?

- Introduction to Encryption at Rest for Extracts
- Demo: Configuring and Managing Encryption at Rest
- Security Internals
- Backup and Site Import/Export
- Key Rotation
- Performance
- Integration with AWS KMS
Meetup: Security
Friday | 12:15pm - 1:15pm

Enhance Your Enterprise Capabilities with the Tableau Server Management Add-on
Friday | 10:30am - 11:30am
Please complete the session survey in the mobile app.

View ‘My Evaluations’ in the menu or find your session under ‘Schedule’.
Q&A
Resources
Resources

Understanding extracts:
https://www.tableau.com/about/blog/2014/7/understanding-tableau-data-extracts-part1

Jakob’s blog post about Encryption at Rest:

Help article on Encryption at Rest:

Help article on KMS, covering key rotation and AWS KMS integration:

Security Whitepaper on Encryption at Rest:
https://www.tableau.com/learn/whitepapers/encryption-at-rest
Thank You
TABLEAU CONFERENCE