Table of Contents

Release Notes

Release Notes

RELEASES:

Baffle Release 2.5.0.4

Release Date	Version Number
Oct 6, 2023	2.5.0.4

Baffle Release 2.5.0.4 has a number of enhancements and bug fixes from the previous Baffle release, version 2.4.0.7.

What's new

The current Baffle release has added the following new enhancements, version updates, and improved user experience.

- Detailed **audit logs** have been added for Baffle Manager in order to create a chronological record of Manager users' activities.
- Expanded Data Protection Policy configuration for **JSON** and **JSONB** data types has been added in Baffle Manager. Policies can encrypt a JSON column in its entirety or point to specific key-value pairs in a JSON object.
- Baffle Manager's **Data Protection Policy workflow** has been enhanced to improve ease of use and support more flexible, reusable policy assets. Now, the same **data source** configurations can be reused and referenced in multiple different protection policies.
- The Baffle HTTP data proxy has added support for complex **Access Control** policies.

Fixes and stabilization

As part of this release, multiple defects have been addressed, and several smaller-scope enhancements have been added.

- We addressed issues in Baffle Advanced Encryption version 2 related to Hibernate compatibility.
- If many Data Protection Policies were saved in Baffle Manager, an erroneous error message would state, 'Communication with server failed'. This has been removed, and performance optimizations have been made to support large numbers of Data Protection Policies.
- If Baffle Manager was running in multiple tabs for longer than ten minutes, the session would

be logged out spontaneously.

- When configuring a multi-region AWS KMS keystore, the replica regions would be inaccurately displayed.
- On the Instances pane in the Database Proxy service, an inaccurate Hostname/IP was displayed.
- FPE-DECIMAL Encryption Mode is not supported for JSON data types. This option is blocked during policy creation.
- We fixed an issue during upgrades from version 2.2 and earlier, if AWS Secrets Manager was configured with Baffle Manager.
- When enrolling a new database instance, naming your database with an email address was rejected.
- Added support for the parsing of a key and certificate file generated by a Windows/DOS system.
- Added a new Format-Preserving Encryption (FPE) format for UTF-8 data types.
- Importing Views via a .csv file is now supported via the Data Sources interface.

Known Issues

The following known issues are present on Baffle Manager Release 2.5.0.4.

1. **CA certificate upgrades are not supported** from version 2.1 or earlier to the current version 2.5.0.4. Connections from Manager to Shield proxy instances will fail after this upgrade path.
2. When configuring a **large number of database columns** for use in your policies (>1000), Baffle Manager will experience some performance degradation. This is currently under investigation and will be optimized.
3. The following Data Protection Policy permutation will cause a display issue if you view the **Tenants and Tenant Columns** listing: at least one Data Source, disabled Encryption, enabled Access Control.
4. When configuring a data source for **JSON columns via Direct Input**, and you add a JSON subset, it cannot be deselected for the next column(s) you plan to add via Direct Input. **Workaround:** choose a different method of column selection and then return to the Direct Input pane to clear selections.
5. During encryption configuration in data protection policies, if you change your **FPE format** more than once, the Next button may be disabled. **Workaround**: refresh the page or return to the previous step to re-select your FPE formats.
6. Baffle Manager's JSON parser for data sources does not support parsing an array of JSON objects.
7. When creating a new Data Protection Policy, there may be some issues with using the **Back button** to revise previous policy configurations.
8. AWS Database Migration Service (**DMS**) Change Data Capture (**CDC**) does not work while running Baffle decryption.
9. If an **API services Role** is renamed, it must be re-deployed at the services pane for the change to take effect.
10. When re-deploying an **API service policy**, the Sync ID changes between deployments.
11. Database-Level Encryption (DLE) and Record-Level Encryption (RLE) **cannot both be configured** on the same DB Proxy service.
12. **BOOLEAN and BINARY data types** are not supported in Data Protection Policies that use a combination of Multi-tenant Encryption, Access Control, and Masking.
13. Newly-created Key Encryption Keys (KEKs), or KEKs which do not wrap any Data Encryption

Keys (DEKs), **cannot be rotated**.

14. Data Encryption Keys (DEKs) must have **unique names** across Baffle Manager, even if they are wrapped with different Key Encryption Keys (KEKs).
15. For some certificates on the CA Certificates page, the **Subject Name** field is displayed incorrectly as the issuer.
16. If a deployment is created where some encrypted columns are removed from the policy, and others are added to the policy, then the **Shield must be restarted**.
17. Intermittently, when **handling over ten users** simultaneously, Baffle Manager will throw a 500 error.
18. After enabling an Access Control & Masking Policy using `DB_Roles` user determination, there is no **inject query** in the shield log that shows user roles fetched in the database.

> **Note**
> RBAC Mode must be set to **required** to work with `DB_Roles`.

19. When applying **Tenant Encryption, only one session variable can be used** to access a given table.Therefore, all columns will be encrypted with one Tenant according to the configured session.
20. Ensure that when you enroll in an **AWS KMS or Azure Key Vault keystore**, precise connection parameters are used.
21. The **Azure Key Vault storage account key** is not currently saved in the Baffle Manager Secret Store.
22. Incorrect database credentials or database network access permissions will result in a generic **"Failed To Fetch"** error message.
23. **Tenant Identifier** values must be unique across your Baffle Manager. If a previous Tenant Identifier was deleted, it cannot be used to identify a new Tenant.
24. **Custom Mask formats for MySQL** databases are not supported.

Baffle Release 2.4.0.7

Release Date	Version Number
September 5, 2023	2.4.0.7

Baffle Release 2.4.0.7 provides a number of enhancements and bug fixes from the previous Baffle release, version 2.3.0.4. Major new features include:

What's new

The current release has added the following new enhancements and cloud infrastructure support.

- Enhanced Baffle Manager user experience to **improve ease of use** when enrolling Keystores, Databases, Key Encryption Keys (KEKs) and Tenants.
- When configuring a Database Proxy Service, **encryption is optional**. If encryption is not being performed, then you no longer need to enroll a Keystore.
- **Azure Key Vault** can be configured as a Baffle **Secret Store**.
- Baffle **Advanced Encryption version 1** support has been added to Baffle Manager's Database Proxy Service configuration.
    - Baffle **Advanced Encryption version 2** is available in Beta release. For more

information, contact your Baffle support representative.

- When Baffle is configured to store Data Encryption Keys (DEKs) in an AWS S3 bucket, Baffle can optionally detect your **server-side encryption** policies. By default, Baffle uses the (SSE-S3) policy.

Fixes and stabilization

As part of this release, support for different database versions has been expanded. In addition, multiple bugs have been addressed, and a number of smaller-scoping enhancements have been made.

- **PostgreSQL versions 14 and 15** are now supported in Baffle Manager. Baffle Advanced Encryption now supports PostgreSQL 14.
- **MySQL version 8** is now supported.
- When Baffle is configured to store Data Encryption Keys (DEKs) in an AWS S3 bucket, permissions for **s3:PutBucketVersioning** are no longer required.
- Fixed an issue where it was possible to enroll two Key Encryption Keys (KEKs) with the **same name**.
- Some service **configuration files** were incorrectly listed and would not be downloaded properly.
- The **Rename function** for Data Protection Policies was not working correctly.
- Fixed **inline error messages** throughout the Baffle Manager UI.
- Addressed 45 various **SQL operation issues** in Baffle Advanced Encryption version 2.

Known Issues

The following known issues are present on Baffle Manager Release 2.3.0.4.

1. If there are **many Data Protection Policies** saved in Baffle Manager, there may be an error message thrown in error, stating 'Communication with server failed'. This is an inaccurate error message and can be dismissed.
2. Database-Level Encryption (DLE) and Record-Level Encryption (RLE) **cannot both be configured** on the same DB Proxy service.
3. If Baffle Manager is running in multiple tabs for longer than ten minutes, the session may be logged out spontaneously.
4. **BOOLEAN and BINARY data types** are not supported in Data Protection Policies that use a combination of Tenant Determination, Access Control and Masking.
5. Newly-created Key Encryption Keys (KEKs), or KEKs which do not wrap any Data Encryption Keys (DEKs), **cannot be rotated**.
6. Data Encryption Keys (DEKs) must have **unique names** across Baffle Manager, even if they are wrapped with different Key Encryption Keys (KEKs).
7. For some certificates on the CA Certificates page, the **Subject Name** field is displayed incorrectly as the issuer.
8. **FPE-DECIMAL** Encryption Mode is not supported for JSON data types.
9. There are some issues with the **Direct Input pane for columns** during Data Protection Policy creation.
    1. When inputting columns that are not present (verified) on your **Database Reference**, if the column path is shared with an existing column on your DB Reference, then the BM will treat it as the existing column and it must have a compatible data type.
    2. For a **Redshift Policy**, it is possible to input a column with an invalid data type.

Ensure that you submit the correctly-formatted data type for your columns.

10. Importing **Views via a .csv** file is unsupported.
11. In some scenarios, on the Instances pane in your Database Proxy service, an **inaccurate Hostname/IP** is displayed.
12. If a deployment is created where some encrypted columns are removed from the policy, and others are added to the policy, then the **Shield must be restarted**.
13. Intermittently, when **handling over 10 users** simultaneously, Baffle Manager will throw a 500 error.
14. After enabling an Access Control & Masking Policy using `DB_Roles` user determination, there is no **inject query** in the shield log that shows user roles fetched in the database.

Note:
RBAC Mode must be set to **required** to work with `DB_Roles`.

15. When applying **Tenant Encryption, only one session variable can be used** to access a given table. Therefore, all columns will be encrypted with one Tenant according to the configured session.
16. Ensure that when you enroll an **AWS KMS or Azure Key Vault keystore**, precise connection parameters are used.
17. The **Azure Key Vault storage account key** is not currently saved in the Baffle Manager Secret Store.
18. Incorrect database credentials or database network access permissions will result in a generic **"Failed To Fetch"** error message.
19. `FPE_DECIMAL` is currently not supported for Encryption Policy.
20. Format-Preserving Encryption (FPE) is **not supported for JSON** columns.
21. **Tenant Identifier** values must be unique across your Baffle Manager. If a previous Tenant Identifier was deleted, it cannot be used to identify a new Tenant.
22. **Custom Mask Policies for MySQL** databases are not supported.

Baffle Release 2.3.0.4

Release Date	Version Number
July 31, 2023	2.3.0.4

Baffle Release 2.3.0.4 provides a number of enhancements and bug fixes from the previous release, 2.2.0.2. Major new features include enhanced HA/DR capability, Database-Level Encryption, and support for additional SSO providers.

What's new

The current release has added the following new features and cloud infrastructure support.

- Added support for **multi-region AWS endpoints** for the essential cloud services that integrate with Baffle. These include AWS Key Management Service (KMS), Secrets Manager, Relational Database Service (RDS), and AWS S3. Deploying with multi-region endpoints improves your **high availability and disaster recovery (HA/DR)** posture.

- Added additional flexibility for keystore configuration. Now, an individual keystore can be assigned to encrypt an individual SQL database. This feature is called **Database-Level Encryption (DLE).**
- Baffle Manager's supported SSO platforms include **JumpCloud** and **Azure Active Directory**.

Fixes and stabilization

Multiple bugs have been addressed as part of the release. In addition, a number of smaller-scale enhancements have been added.

- AWS **Secrets Manager** can now enroll with Baffle Manager without needing access keys, instead using an AWS IAM role.
- Baffle **Advanced Encryption** now supports some PostgreSQL User-defined functions (UDFs).
- Fixed an issue where duplicate **Encryption Policies** could be available for selection while creating your Data Protection Policy.
- Fixed an error message that would occur for an **invalid date** sent by the Manager. This message occurred when a poll coincided with a whole second (with no millisecond value).
- Fixed an issue where a newly-created Baffle Manager user, who was assigned the role of **System Administrator,** could not log in.
- Occasionally, the user **email address** for system administrators would not be displayed properly.
- Fixed an issue where **new user creation** would be successful, even if their member group ID was incorrect.
- When creating a **custom Mask Policy,** properly-formatted values for some TIMESTAMP and DATETIME policies would not be accepted.

Known Issues

The following known issues are present in Baffle Manager Release 2.3.0.4.

1. **BOOLEAN and BINARY data types** are not supported in Data Protection Policies that combine Tenant Determination, Access Control, and Masking.
2. Newly-created Key Encryption Keys (KEKs) or KEKs that do not wrap any Data Encryption Keys (DEKs) **cannot be rotated**.
3. Data Encryption Keys (DEKs) must have **unique names** across Baffle Manager, even if they are wrapped with different Key Encryption Keys (KEKs).
4. For some certificates on the CA Certificates page, the **Subject Name** field is displayed incorrectly as the issuer.
5. **FPE-DECIMAL** Encryption Mode is not supported for JSON data types.
6. There are issues with the **Direct Input pane for columns** during Data Protection Policy creation.

1. When inputting columns that are not present (verified) on your **Database Reference**, if the column path is shared with an existing column on your Database Reference, then the BM will treat it as the existing column and must have a compatible data type.
2. For a **Redshift Policy**, it is possible to input a column with an invalid data type. Ensure that you submit the correctly-formatted data type for your columns.

7. Importing **Views via a .csv** file is unsupported.
8. In some scenarios, on the Instances pane in your Database Proxy service, an **inaccurate Hostname/IP** is displayed.
9. If a deployment is created where some encrypted columns are removed from the policy, and others are added, then the **Shield must be restarted**.
10. Intermittently, when **handling over 10 users** simultaneously, Baffle Manager will throw a 500 error.
11. After enabling an Access Control and Masking Policy using `DB_Roles` user determination, there is no **inject query** in the shield log that shows user roles fetched in the database.

> **Note:**
> RBAC Mode must be set to **required** to work with `DB_Roles`.

11. When applying **Tenant Encryption, only one session variable can** access a given table. Therefore, all columns will be encrypted with one Tenant according to the configured session.
12. Ensure that when you enroll an **AWS KMS or Azure Key Vault keystore**, precise connection parameters are used.
13. The **Azure Key Vault storage account key** is not currently saved in the Baffle Manager Secret Store.
14. Incorrect database credentials or network access permissions will generate a generic **"Failed To Fetch"** error message.
15. `FPE_DECIMAL` is currently not supported by Encryption Policy.
16. Format-Preserving Encryption (FPE) is **not supported for JSON** columns.
17. **Tenant Identifier** values must be unique across your Baffle Manager. If a previous Tenant Identifier was deleted, it cannot be used to identify a new Tenant.
18. **Custom Mask Policies for MySQL** databases are not supported.

Baffle Release 2.2.0.2

Release Date	Version Number
June 22, 2023	2.2.0.2

Baffle Release 2.2.0.2 provides a number of enhancements and bug fixes from the previous release, 2.1.0.4. There are also two new features added to Baffle Manager.

What's new

The following new features and supported platforms have been added in the current release.

- Baffle Manager **Member Management** with new roles, privileges and member groups

functionality, that enables complex configuration of the Baffle Manager user's access and capabilities.
- Support for connecting to and using an externally-located **MongoDB** or Amazon **DocumentDB,** instead of the default, pre-packed MongoDB that is included with Baffle Manager deployments.
- HTTP Proxy support for **Azure Blob Storage** (ABS)

Fixes and stabilization

Multiple bugs have been addressed as part of the release. In addition, a number of smaller-scoping enhancements have been added.

- **Performance improvements** for the MySQL database proxy
- Support for standard encryption on **PostgreSQL version 15**
- Improvements to the Database Proxy's **transactional logging** feature
- Fixed an issue in Baffle Advanced Encryption, where **long KeyIDs** would be truncated
- Fixed an issue in Data Protection Policy creation, where the **Object Type field** (TABLE or VIEW) would not be displayed correctly.
- Fixed an issue in Data Protection Policy creation, where the column Direct Input interface would not be compatible with **Tenant Encryption** policies.
- In some Baffle Manager deployments using **Single Sign-On (SSO)**, Database Proxy instances could not connect to the Baffle Manager.
- Occasionally, **member-group associations** with local Baffle Manager users would not be updated across the Manager.
- When applying a second **Mask Policy** to a Database Proxy deployment, the instances enrolled with that deployment would need to be restarted. This requirement has been removed.
- Fixed issues relating to **error message notifications** and pop-up messages.
- Addressed an issue where a Baffle Manager Members using the **OKTA SSO** integration would not be displayed correctly.
- Implemented support for **Record-Level Encryption (RLE) for database views**.

Known Issues

The following known issues are present on Baffle Manager Release 2.2.0.2.

1. **BOOLEAN and BINARY data types** are not supported in Data Protection Policies which use a combination of Tenant Determination, Access Control and Masking.
2. For some certificates on the CA Certificates page, the **Subject Name** field is displayed incorrectly as the issuer.
3. **FPE-DECIMAL** Encryption Mode is not supported for JSON data types.
4. There are some issues with the **Direct Input pane for columns**, during Data Protection Policy creation.
    1. When inputting columns which are not present (verified) on your **Database Reference**, if the column path is shared with an existing column on your DB Reference, then the BM will treat it as the existing column and it must have a compatible data type.
    2. For a **Redshift Policy**, it is possible to input a column with an invalid data type. Ensure that you submit the correctly-formatted data type for your columns.
5. Importing **Views via a .csv** file is unsupported.

6. In some scenarios, on the Instances pane in your Database Proxy service, an **inaccurate Hostname/IP** is displayed.
7. If a deployment is created where some encrypted columns are removed from the policy, and some other columns are added to the policy, then the **Shield must be restarted**.
8. Intermittently, when **handling over 10 users** simultaneously, Baffle Manager will throw a 500 error.
9. After enabling an Access Control & Masking Policy using `DB_Roles` user determination, there is no **inject query** in the shield log that shows user roles fetched in the database.

> **Note:**
> RBAC Mode must be set to required to work with `DB_Roles`.

10. Occasionally, an error message is thrown for an **invalid date** sent by the Manager. This message occurs when a poll coincides with a whole second (with no millisecond value). It is innocuous.
11. When applying **Tenant Encryption, only one session variable can be used** to access a given table.Therefore, all columns will be encrypted with one Tenant according to the configured session.
12. Ensure that when you enroll an **AWS KMS or Azure Key Vault keystore**, precise connection parameters are used.
13. The **Azure Key Vault storage account key** is not currently saved in the Baffle Manager Secret Store.
14. Incorrect database credentials or database network access permissions will result in a generic **"Failed To Fetch"** error message.
15. `FPE_DECIMAL` is currently not supported for Encryption Policy.
16. Format-Preserving Encryption (FPE) is **not supported for JSON** columns.
17. **Tenant Identifier** values must be unique across your Baffle Manager. If a previous Tenant Identifier was deleted, it still cannot be used to identify a new Tenant.
18. **Custom Mask Policies for MySQL** databases are not supported.

Baffle Release 2.1.0.4

Release Date	Version Number
23-May-2023	2.1.0.4

Baffle Release 2.1.0.4 is a significant upgrade from previous releases.

What's new

- A complete **user interface overhaul** to include more reusable components for easier enterprise deployments
- **REST API support** that is capable of anything that the UI can do for automation
- Comprehensive **key management**, including:
    - Key Encryption Key (KEK) rotation
    - Data Encryption Key (DEK) naming and management
    - Multi-tenant management
- **Keystores** (Key Encryption Key/Data Encryption Key)

    - `AWS_KMS` /AWS S3
    - Azure KeyVault/Azure Blob Storage
    - Hashicorp Vault/Hashicorp Vault
- **Secrets Manager**
    - AWS Secrets
    - Hashicorp Vault
- Improvements to BM **user management** and roles
- Enhanced **CA Certificate** management

PostgreSQL Database Proxy

Configuration and monitoring of the PostgreSQL database proxy.

- New **database navigation** that enables faster entry for bulk imports, enabling policies for columns that don't yet exist, and column search.
    - Manual Entry
    - CSV import
    - Search
    - Existing database browsing
- **Global Encryption** (column-level)
    - `AES-CTR-DET` Traditional AES encryption where plaintext values always create the same ciphertext for each operation (assuming the same key)
    - `AES_CTR-RND` Traditional AES encryption where plaintext values create randomized ciphertext for each operation (even with the same key)
    - Format-Preserving Encryption (FPE) where the ciphertext has the same format and length of the plaintext.
- **Access Control Policies with Data Masking**. Full or partial masking with predefined and user-definable mask formats.
    - Session mode — access is defined by the user logging into the database
    - SQL-comment mode — access is defined by a specially crafted comment included in the SQL commands
- Global Encryption and RBAC Access Control may be combined for best practice.
- **Tenant Encryption** (record-level) where each entry of the configured columns is encrypted with a separate key. This is ideal for multi-tenant applications that need to keep each tenant's data logically isolated.
    - Session mode — encryption/decryption is defined by the user logging into the database
    - SQL-comment mode — encryption/decryption is defined by a specially crafted comment included in the SQL commands
    - Tenant Column mode — encryption/decryption is defined by matching a field in a given column

API Services

Baffle Manager can now be used to configure and monitor Baffle API services.

- Any data sent to the API can be **encrypted or decrypted** using AES or FPE.
- **Multiple roles** can be used to support multi-tenant encryption, decryption, and masking.

- **Baffle Controller** has been added to assist Kubernetes scaling

New features from Release 2.0.0.0

From the initial Baffle Manager 4 release in 2.0.0.0, the following new features have been added.

- Enhanced Baffle **Advanced Encryption** support for CITEXT data type and Long KeyID
- **Redshift** Datastore support for use with Database Proxy services
- **MySQL** Database support for use with Database Proxy services
- Support for Database **Views**
- **OIDC** integration for use with OKTA and PingID
- Support for **User Determination by Database Roles** in Data Protection Policies with Access Control and Masking

Known Issues

The following known issues are present on Baffle Manager Release 2.1.0.4.

1. **Boolean datatype** is not supported in Data Protection Policies which use a combination of Tenant Determination, Access Control and Masking.
2. There are some issues with the **Direct Input pane for columns**, during Data Protection Policy creation.
    1. Direct Input cannot be used in a policy with **Tenant Encryption**.
    2. When inputting columns which are not present (verified) on your **Database Reference**, if the column path is shared with an existing column on your DB Reference, then the BM will treat it as the existing column and it must have a compatible data type.
    3. For a **Redshift Policy**, it is possible to input a column with an invalid data type. Ensure that you submit the correctly-formatted data type for your columns.
3. When selecting an **Encryption Policy** during Data Protection Policy creation, duplicate options may be displayed for the same policy. Either option may be selected.
4. During DPP creation, when selecting all columns in a search result, the **Object Type field** (TABLE or VIEW) is not displayed correctly.
5. Importing **Views via a .csv** file is unsupported.
6. After upgrading the Baffle Manager, your **Secret Store** must be defined again in the YAML configuration files.
7. In some scenarios, on the Instances pane in your Database Proxy service, an **inaccurate Hostname/IP** is displayed.
8. If a deployment is created where some encrypted columns are removed from the policy, and some other columns are added to the policy, then the **Shield must be restarted**.
9. In order to **encrypt a Database View**, the underlying table must also be encrypted using the same Encryption Policy.
10. Intermittently, when **handling over 10 users** simultaneously, Baffle Manager will throw a 500 error.
11. **Record-Level Encryption (RLE) for database views** is currently unsupported.
12. After enabling an Access Control & Masking Policy using `DB_Roles` user determination, there is no **inject query** in the shield log that shows user roles fetched in the database.
    4. Note: RBAC Mode must be set to **required** to work with `DB_Roles` .
13. Occasionally, an error message is thrown for an **invalid date** sent by the Manager. This message occurs when a poll coincides with a whole second (with no millisecond value). It is

innocuous.

14. Access Control Policies presently do not support User Determination via **SQL Comment JWT** authentication.
15. When applying **Tenant Encryption, only one session variable can be used** to access a given table. Therefore, all columns will be encrypted with one Tenant according to the configured session.
16. `PG_Dump` will not work when SQL comments are used for Tenant Determination. Use –column-inserts –attribute-inserts flags when using PGDump insert. For more information, please refer to the separate documentation on PG_Dump.
17. Ensure that when you enroll an **AWS KMS or Azure Key Vault keystore**, precise connection parameters are used.
18. The **Azure Key Vault storage account key** is not currently saved in the Baffle Manager Secret Store.
19. Incorrect database credentials or database network access permissions will result in a generic **"Failed To Fetch"** error message.
20. `FPE_DECIMAL` is currently not supported for Encryption Policy
21. Format-Preserving Encryption (FPE) is **not supported for JSON** columns.
22. **Tenant Identifier** values must be unique across your Baffle Manager. If a previous Tenant Identifier was deleted, it still cannot be used to identify a new Tenant.

Baffle Release 2.0

Release Date	Version Number
18-Apr-2023	2.0

Release 2.0

Baffle Manager 2.0 is a significant upgrade from previous releases.

What's new

- A complete user interface overhaul to include more reusable components for easier enterprise deployments
- REST API support that is capable of anything that the UI can do for automation
- Comprehensive key management, including:
    - Key Encryption Key (KEK) rotation
    - Data Encryption Key (DEK) naming and management
    - Multi-tenant management
- Keystores (Key Encryption Key/Data Encryption Key)
    - `AWS_KMS` /AWS S3
    - Azure KeyVault/Azure Blob Storage
    - Hashicorp Vault/Hashicorp Vault
- Secrets Manager
    - AWS Secrets
    - Hashicorp Vault
- Improvements to BM user management and roles

- Enhanced CA Certificate management

PostgreSQL Database Proxy

Configuration and monitoring of the PostgreSQL database proxy.

- New database column navigation that enables faster entry for bulk imports, enabling policies for columns that don't yet exist, and column search.
    - Manual Entry
    - CSV import
    - Search
    - Exisitng databse navigation
- Global Encryption (column-level)
    - `AES-CTR-DET` Traditional AES encryption where plaintext values always create the same ciphertext for each operation (assuming the same key)
    - `AES_CTR-RND` Traditional AES encryption where plaintext values create randomized ciphertext for each operation (even with the same key)
    - Format-Preserving Encryption (FPE) where the ciphertext has the same format and length of the plaintext.
- Role-based access control using masking. Full or partial masking with pre-defined and user-definable mask formats.
    - Session - access is defined by the user logging into the database
    - SQL-comment - access is defined by a specially crafted comment included in the SQL commands
- Global Encryption and RBAC access control may be combined for best practices.
- Tenant Encryption (record-level) where each entry of the configured columns is encrypted with a separate key. This is ideal for multi-tenant applications that need to keep each tenant's data logically isolated.
    - Session- encryption/decryption is defined by the user logging into the database
    - Tenant Column - encryption/decryption is defined by matching a field in a given column
    - SQL-comment - encryption/decryption is defined by a a specially crafted comment included in the SQL commands