Tokyo

AWS re:Invent Recap – Database
re:Invent 期間中に発表された Amazon RDS/Amazon Aurora 新機能まとめ Part 2

小林 隆浩 (こばやし たかひろ)
データベース スペシャリスト ソリューション アーキテクト
アマゾン ウェブ サービス ジャパン 合同会社

アジェンダ

- **Preview** Amazon GuardDuty RDS Protection
- **New!** Trusted Language Extensions (TLE) for PostgreSQL
- **New!** AWS DMS Schema Conversion

自己紹介

- **小林 隆浩** (こばやし たかひろ)
  - データベース スペシャリスト ソリューション アーキテクト

- 好きなサービス
  - Amazon Aurora/RDS
  - AWS DataSync

- 趣味
  - DBソムリエ（＝いろいろなDBMSの調査、味見）

プレビュー

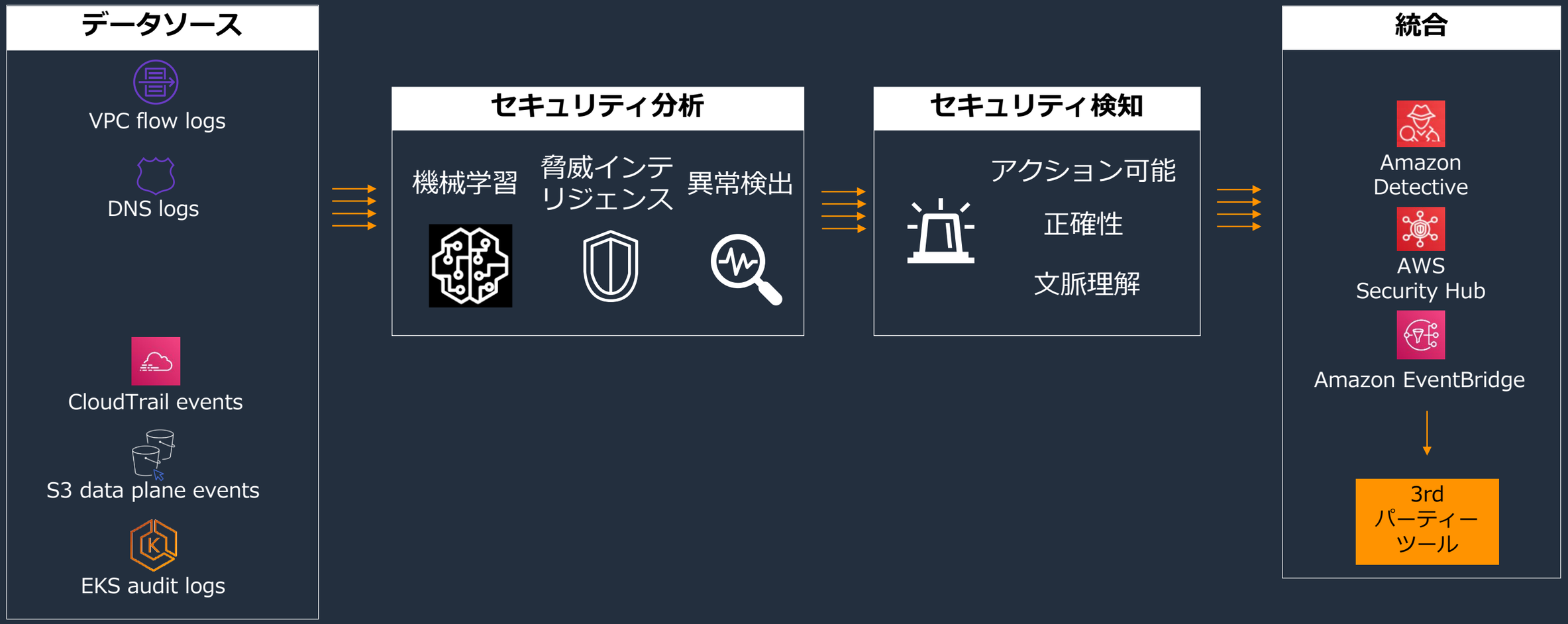
Amazon GuardDuty RDS Protection (Preview)

AWS RE:INVENT RE:CAP

Amazon GuardDutyとは

プレビュー

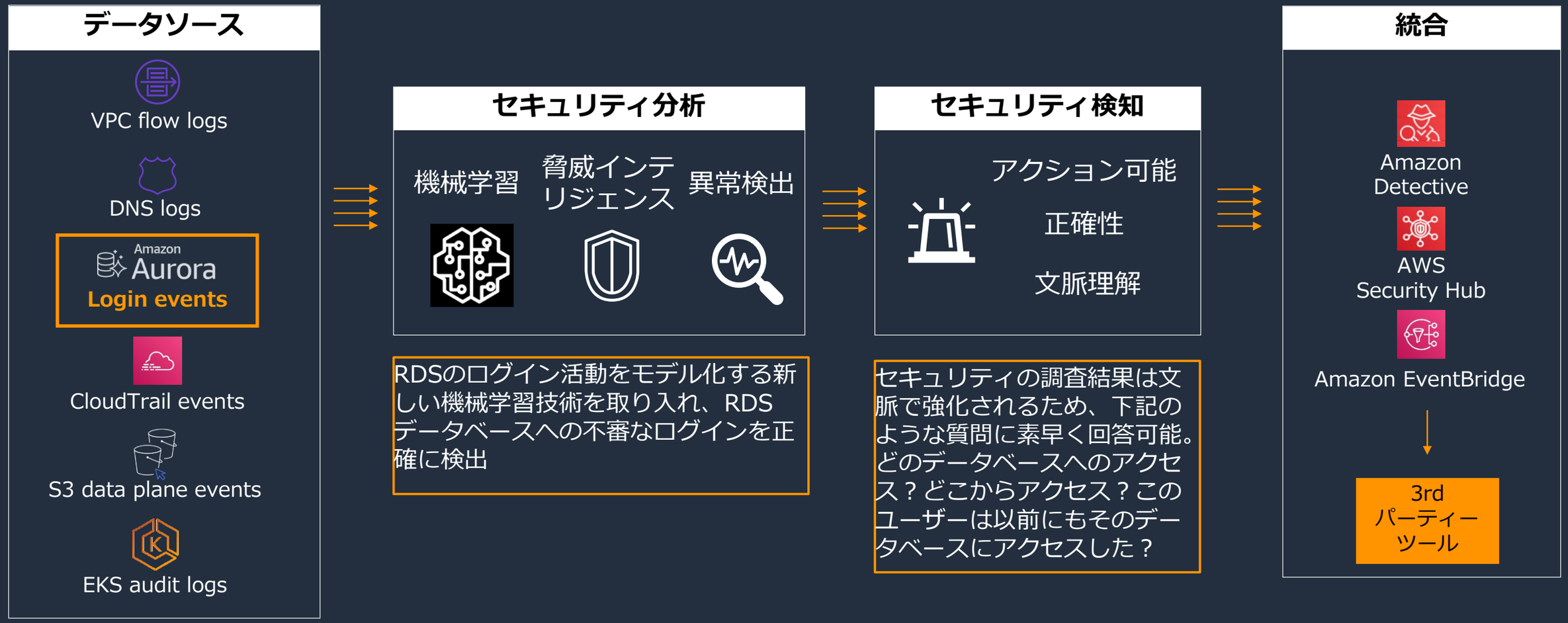
インテリジェントな脅威検出でAWSアカウントを保護



Amazon GuardDuty RDS Protectionの概要

プレビュー

GuardDutyの対象をAmazon RDSに拡張



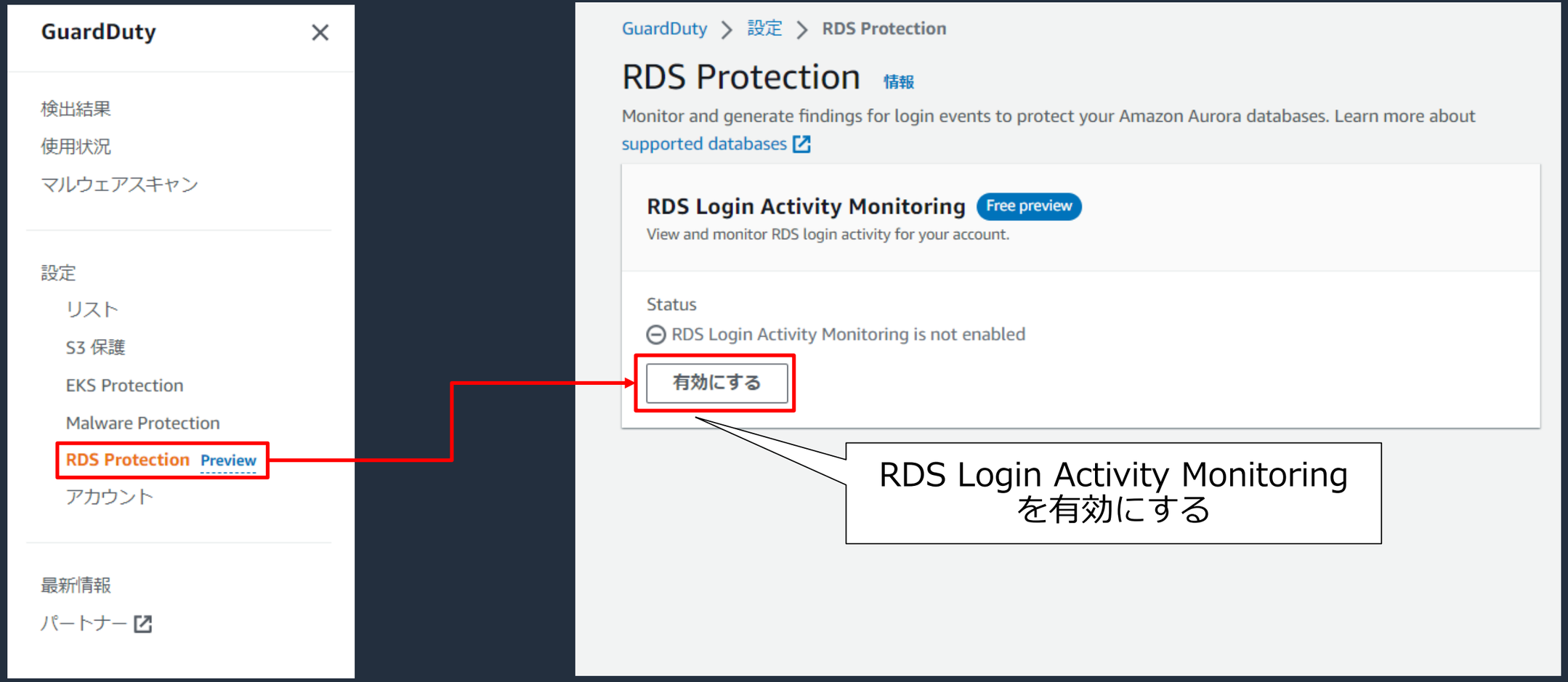
Amazon GuardDuty RDS Protectionの特徴

プレビュー

- RDS Protection機能を有効にすると、データベースに対するログインアクティビティの監視を開始
- 何百万ものデータベースに関するAWSの長年の運用経験と、Amazon GuardDutyの脅威を検出する機械学習機能で、疑わしいログインアクティビティを検出
- 疑わしいログインが検出されると、詳細なセキュリティ所見と推奨アクションを提示（Amazon GuardDutyコンソールやEventBridgeなどに通知）
- データベースパフォーマンスへの影響や修正の必要がないように設計
- Amazon EventBridge、Amazon Detective、AWS Security Hubとの連携が可能（プレビュー期間中はEventBridgeのみ）
- PCI DSS（Payment Card Industry Data Security Standard）などのセキュリティガバナンス確立の迅速化に貢献

Amazon GuardDuty RDS Protectionの使用方法

プレビュー



検出される脅威と推奨されるアクション①

プレビュー

- 異常な方法でのログイン成功
  - 悪意あるユーザがロールを不正利用してログインしている疑いがあるケース

脅威タイプ

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Resource Type : RDSDBInstance

Default severity: Medium

Data source: RDS login activity monitoring

推奨アクション

関連するデータベースロールのパスワードを変更し、ロールを悪用しているユーザーによって実行されたアクティビティについて利用可能な監査ログを確認する

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-remediate-compromised-database-rds.html

検出される脅威と推奨されるアクション②

プレビュー

- 大量のログイン失敗
  - ブルートフォース攻撃の疑いがあるケース

脅威タイプ

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Resource Type : RDSDBInstance

Default severity: Low

Data source: RDS login activity monitoring

推奨アクション

このアクティビティが関連するデータベースにとって予期しないものである場合、データベースがパブリックで公開されている、あるいは、データベースに対して過度に寛容なアクセスポリシーが設定されている可能性がある。必要なリソースからのアクセスのみ許可するようにデータベースのセキュリティグループなどのアクセス設定を確認する

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-remediate-compromised-database-rds.html

Amazon GuardDuty RDS Protectionの要件

プレビュー

- Amazon GuardDuty が有効であることが利用前提
- 以下のAuroraサービスに対応
  - Aurora MySQL バージョン 2.10.2，3.2.1 以降
  - Aurora PostgreSQL バージョン 10.17, 11.12, 12.7, 13.3, 14.3 以降
- 以下の5つのAWSリージョンで利用可能
  - US East (N. Virginia)
  - US East (Ohio)
  - US West (Oregon)
  - Asia Pacific (Tokyo)
  - Europe (Ireland)

Amazon GuardDuty RDS Protectionの料金

プレビュー

- プレビュー期間中
  - 追加費用なしで利用可能
    - ただし、この機能と組み合わせて他のAWSサービス（例えばEventBridgeなど）を使用した場合、そのサービスの費用は発生するので注意
- GA後
  - 料金は現時点で非公表

Amazon GuardDuty RDS Protectionの情報源

プレビュー

- What’s new
  - https://aws.amazon.com/jp/about-aws/whats-new/2022/11/amazon-guardduty-rds-protection-preview/
- User Guide (GuardDuty)
  - https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/rds-protection.html
- Users Guide (Aurora)
  - https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/guard-duty-rds-protection.html

Trusted Language Extensions (TLE) for PostgreSQL

RDSのPostgreSQL Extensionに関する課題

- PostgreSQLの拡張性を支えるExtension
- RDS/Auroraでサポートされているのは85個以上
  - しかし、PostgreSQLのExtensionはPGXNに登録されてるだけでも348個
- 現在、RDS/Auroraでは一部のExtensionをサポートしている

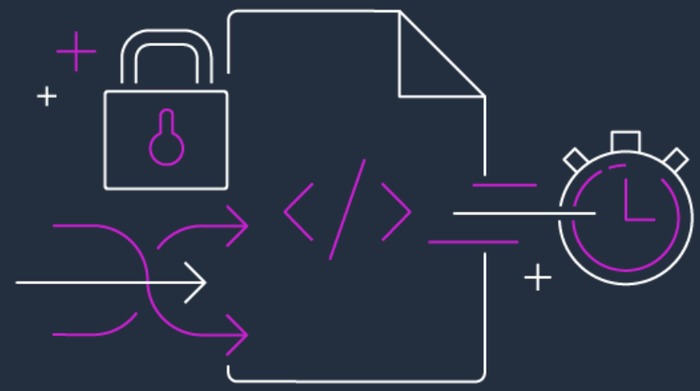
- 利用者は、もっと自由にRDS/AuroraでExtensionを使いたい
- 開発ベンダーは、素早くRDS/Auroraで使えるようになって欲しい

（現状は開発したExtensionがRDS/Auroraに取り込まれるのを待つ必要があり、AWSが対応できないケースもある）

Trusted Language Extensions for PostgreSQLの特徴

信頼できる言語を用いて、RDS/Auroraに導入可能なExtensionを開発するためのキット

- Trusted Language Extensions (TLE) for PostgreSQLはこの開発キットの正式名称で、pg_tleとしてパッケージングされ、AWSがGithubで公開
- TLE for PostgreSQLを使うことで効率的にExtensionを開発でき、それらをRDS/Auroraで安全に実行できる
- 利用者にとっては、適切な権限制御の元、RDS/Auroraに柔軟にPostgreSQL Extensionを追加できる
- 開発ベンダーにとっては、自社のExtensionがAWSによる認証を待たずにRDS/Auroraで利用可能となり、市場への投入までの時間が改善される

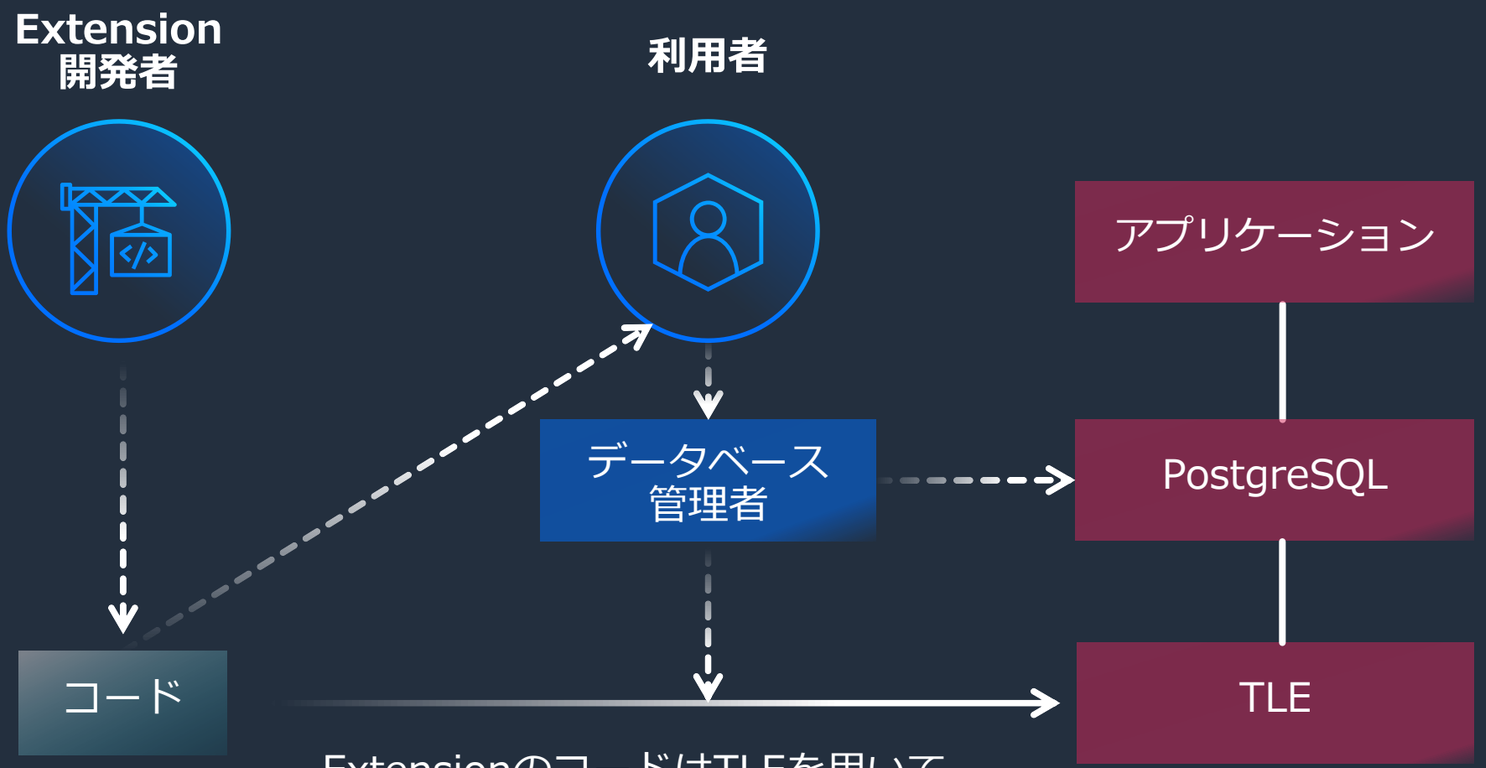


TLE for PostgreSQLの利用イメージ

Extensionの開発者はTLEのフレームワークを用いて、新しいExtensionを開発

利用者はアプリケーションで使いたいTLE Extensionを選択

データベース管理者はTLE Extensionをインストール・管理が可能



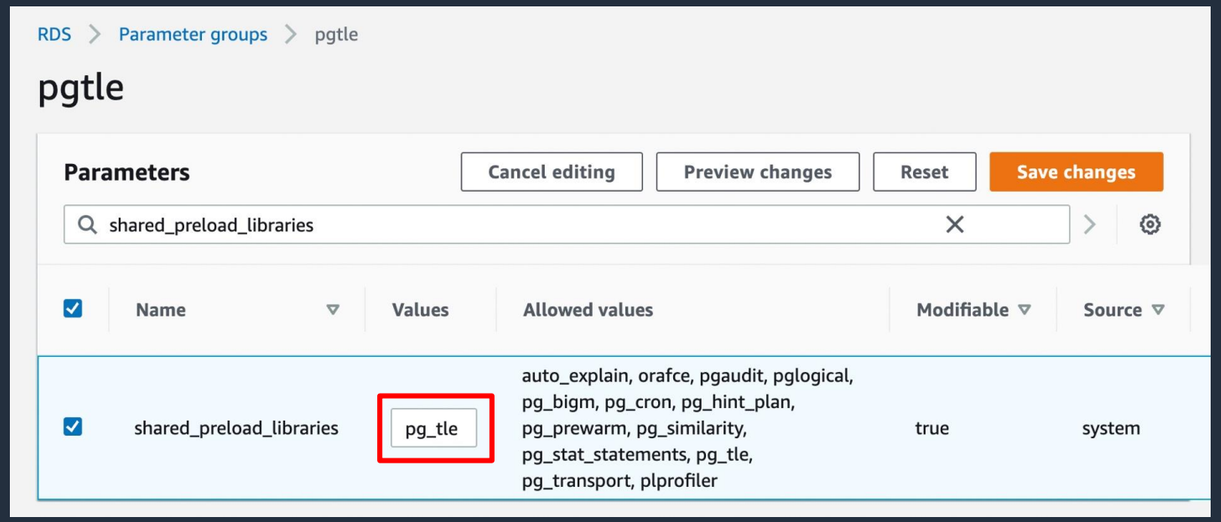
ExtensionのコードはTLEを用いてインストールされる

例） SELECT pgtle.install_extension();

TLE for PostgreSQLの使用方法

設定時の注意点

- pg_tleの利用には事前にRDS/Auroraの設定が必要
- カスタムDBパラメータグループを作成し、shared_preload_librariesにpg_tleを指定します（rds_superuserの権限が必要）
- 以下はpgtleというパラメータグループに設定を追加した例



- その他のPostgreSQL側のCreate Extensionなどの設定方法はUser Guideを参照

Trusted Language Extensions for PostgreSQLの要件

- TLE for PostgreSQLを利用可能なRDS/Auroraのバージョン
  - RDS for PostgreSQL
    - バージョン14.5以上
  - Aurora PostgreSQL Compatible Edition
    - バージョン14.5以上
- pg_tle version 1.0.1の制限事項
  - 利用可能な言語：JavaScript, Perl, PL/pgSQL, SQL
    Rust (coming soon)
  - 対応済みのhook：Password-check hookのみ

※現在は、従来のExtensionが全て移植できる開発キットではありません。

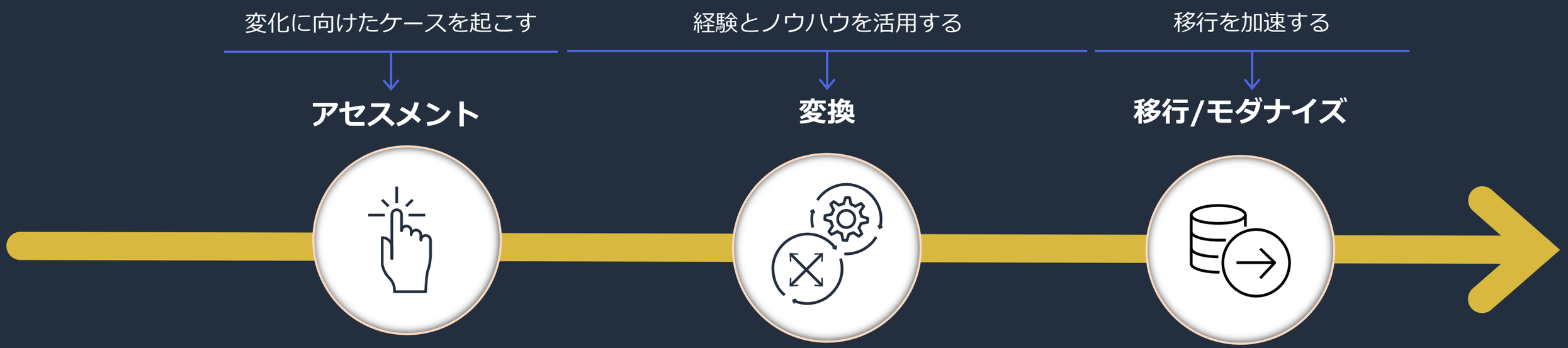
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/PostgreSQL_trusted_language_extension.html

Trusted Language Extensions for PostgreSQLの情報源

- What’s new
  - https://aws.amazon.com/about-aws/whats-new/2022/11/trusted-language-extensions-postgresql-amazon-aurora-rds/
- Blog “New – Trusted Language Extensions for PostgreSQL on Amazon Aurora and Amazon RDS”
  - https://aws.amazon.com/jp/blogs/aws/new-trusted-language-extensions-for-postgresql-on-amazon-aurora-and-amazon-rds/
- User Guide “Working with Trusted Language Extensions for PostgreSQL”
  - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL_trusted_language_extension.html
- Github (pg_tle)
  - https://github.com/aws/pg_tle

AWS DMS Schema Conversion

AWSが提供する移行ツールとサービス



ツール	AWS DMS Fleet Advisor	AWS Schema Conversion Tool (AWS SCT)	AWS Database Migration Service (AWS DMS)
担当者	AWS Solutions Architects	AWS Partners and Professional Services	Amazon Database Migration Accelerator advisors
プログラム	AWS Migration Acceleration Program(MAP) AWS Optimization and Licensing Assessment(OLA)	Database Freedom Database migration best practices, playbooks, and guides	Data Lab Amazon Database Migration Accelerator (DMA)

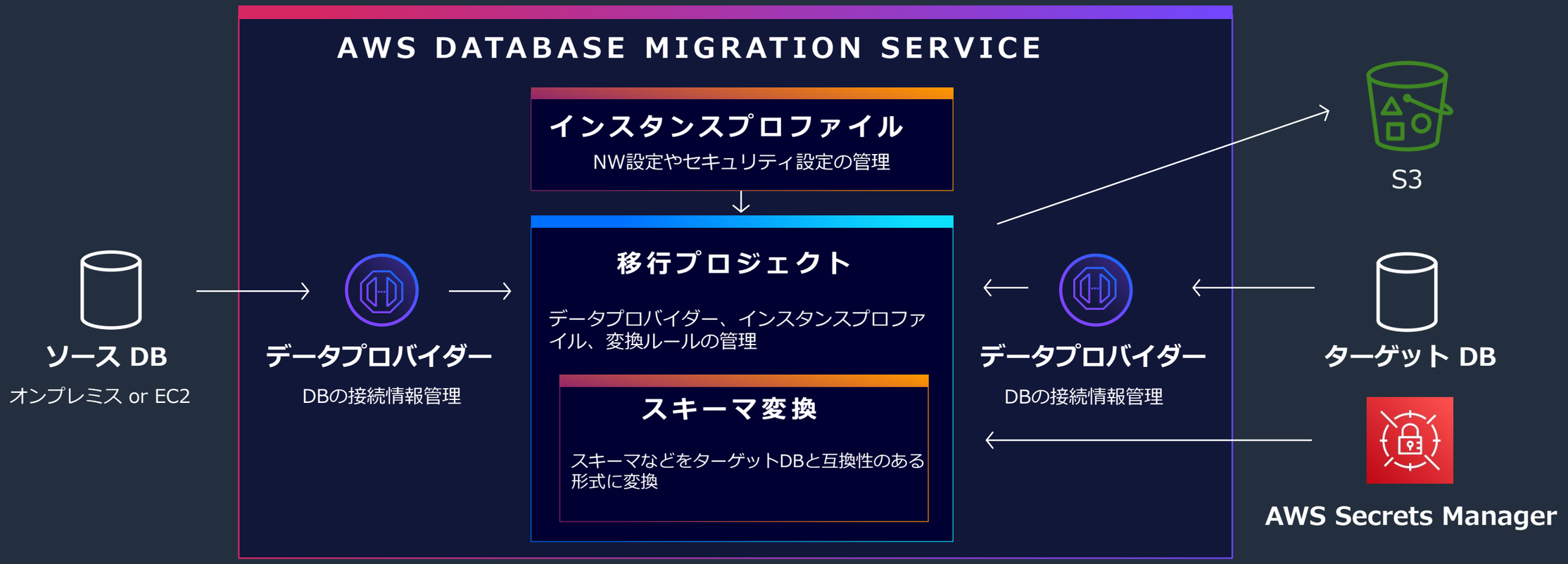
AWS Schema Conversion Tool（SCT）の課題

- SCTはスキーマを異種DB間で変換可能なツールだが、利用には制約があった

  - 動作環境の制限
    - 対象OS: Windows / Ubuntu / Fedora
  - ネットワーク要件
    - SCTを動かす端末は、ソースおよびターゲットデータベースに接続が必要な場合がある
  - セキュリティ要件
    - 端末にSCTをインストールする必要がある
    - SCTにDBのID/Password を入力する場合がある ※AWS Secrets Managerを使ってセキュリティ向上も可能

AWS DMS Schema Conversion の概要

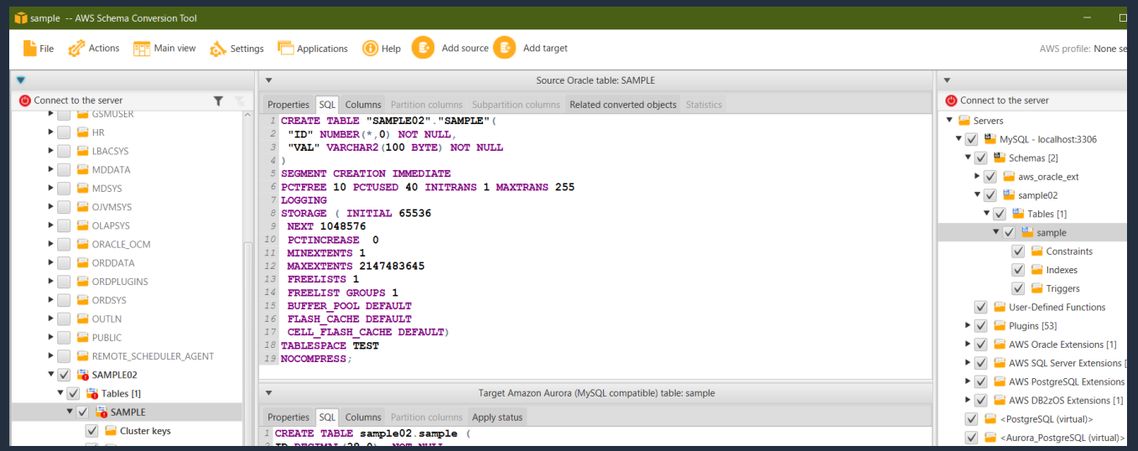
- 無料で利用できるWeb版のSCT
- DB接続用のID/Passwordは、AWS Secrets Managerに保存
- 移行評価レポートは、S3に保存



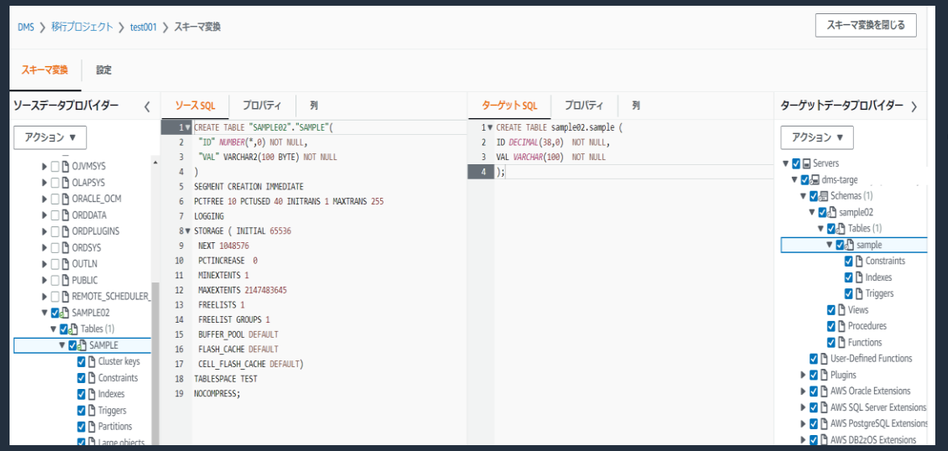
DMS Schema Conversion の機能①

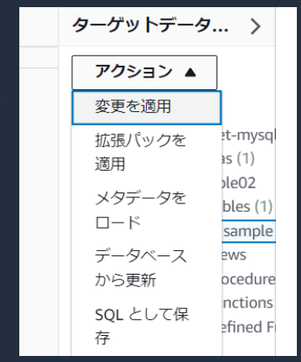
- スキーマ変換処理
  - SCTと同等の画面で変換前と変換後のSQLを確認し、ターゲットへの適用が可能

(従来のSCT)

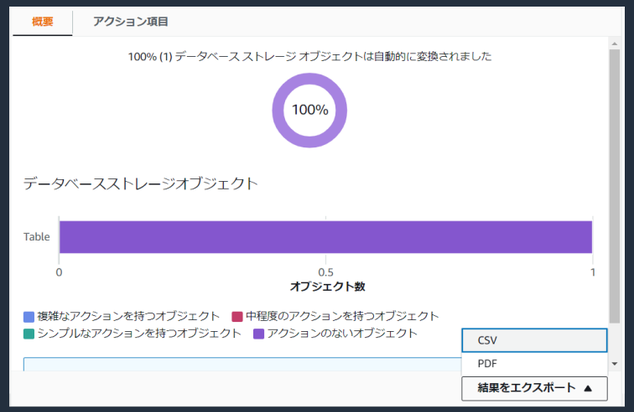


(DMS Schema Conversion)



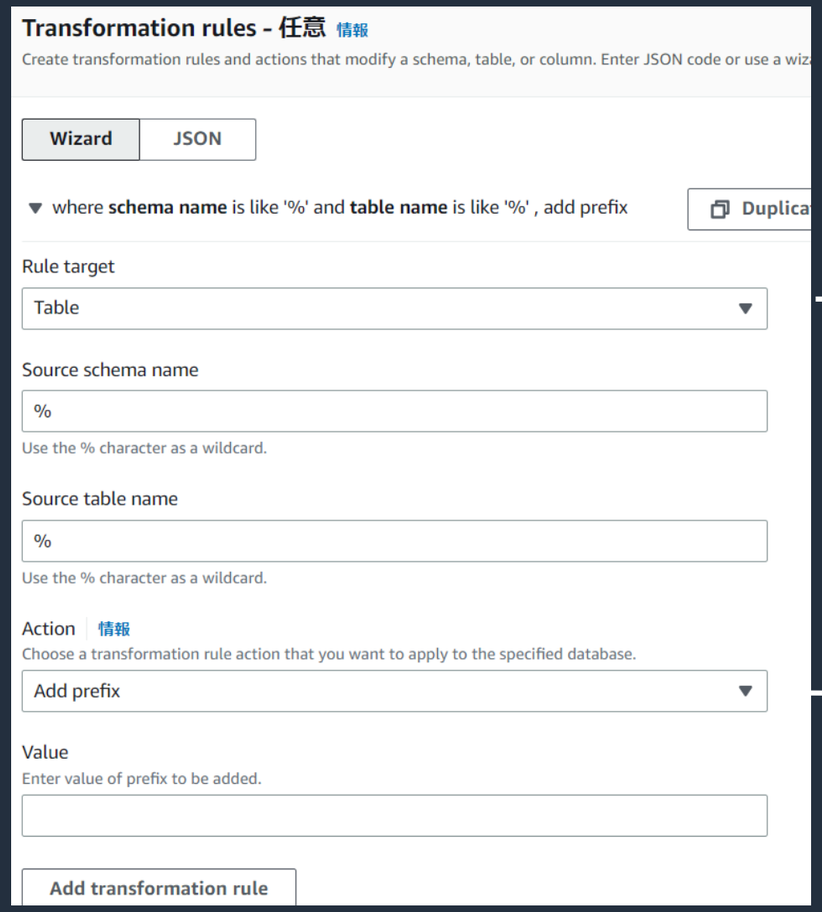


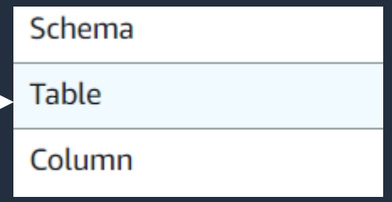
  - 変換後のSQLをS3にエクスポート可能
- 移行評価レポートの作成
  - 結果はS3に保存

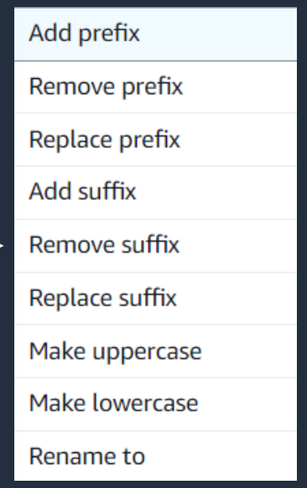


DMS Schema Conversion の機能②

- 変換ルールの作成
  - Schema，Table，Columnについて、prefix/suffixの付与や名前変更のルールを設定可能







DMS Schema Conversion の要件

- リージョン
  - US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), Europe (Frankfurt), Europe (Stockholm), Asia Pacific (Sydney), Asia Pacific (Tokyo), Asia Pacific (Singapore).
- ソースDB
  - オンプレミス or EC2で稼働している以下のDB
    - Microsoft SQL Server version 2008 R2 and higher
    - Oracle version 10.2 and later, 11g and up to 12.2, 18c, and 19c
- ターゲットDB
  - EC2 or RDSで稼働する以下のDB
    - MySQL version 8.x
    - PostgreSQL version 14.x

DMS Schema ConversionのFAQ

- Q) AWS SCTとDMS Schema Conversionの違いは何か？

  A) AWS SCTはダウンロードして使えるクライアントソフトウェアです。DMS Schema ConversionはSCTの機能をフルマネージドなDMSサービスに組み込み、お客様にシンプルなワークフローを提供します。
  2023年1月現在、AWS SCTとDMS Schema Conversionでは対応するDBMSなどに機能の違いがあります。

- Q) AWS SCTとDMS Schema Conversionの使い分けは？

  A) ソースDBとターゲットDBがサポートされている場合、 DMS Schema Conversionを使用できます。それ以外の場合はAWS SCTをお使い頂くことになります。

DMS Schema Conversion の情報源

- What’s new
  - https://aws.amazon.com/jp/about-aws/whats-new/2022/11/aws-dms-schema-conversion-feature/
- Blog “New – A Fully Managed Schema Conversion in AWS Database Migration Service”
  - https://aws.amazon.com/jp/blogs/aws/new-a-fully-managed-schema-conversion-in-aws-database-migration-service/
- User Guide
  - https://docs.aws.amazon.com/dms/latest/userguide/CHAP_SchemaConversion.html

Thank you!