Microsoft

DA21

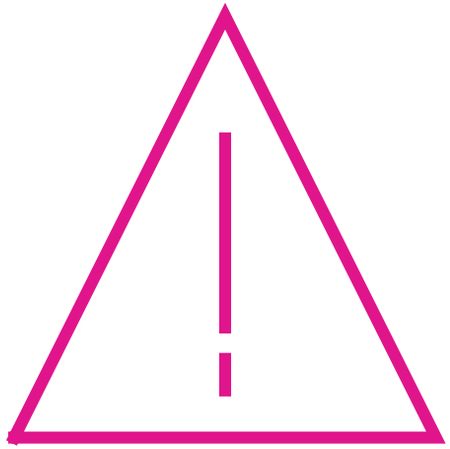
今年もまかせて！Azure SQL Database
～その進化はまだまだ止まらない！編～

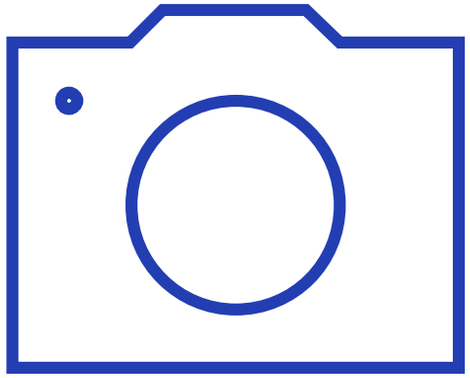
日本マイクロソフト 株式会社
パートナー技術統括本部
テクニカルエバンジェリズム本部
テクニカルエバンジェリスト
山本 美穂

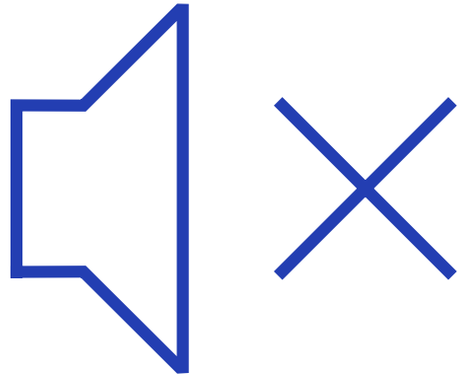
de:code 2018

注意事項

- このセッションは 2018年5月22日時点の情報を元にしています。







資料は公開しますので、
撮影しなくても大丈夫ですよ

Microsoft

セッションアンケートにご協力ください。

公式イベントアプリで、「de:code 2018 参加者アンケート（必須）」と「各セッションアンケート（４つ以上）」、合わせて 5 つ以上 のアンケートにご回答ください。もれなく de:code 2018 オリジナルグッズを贈呈いたします。

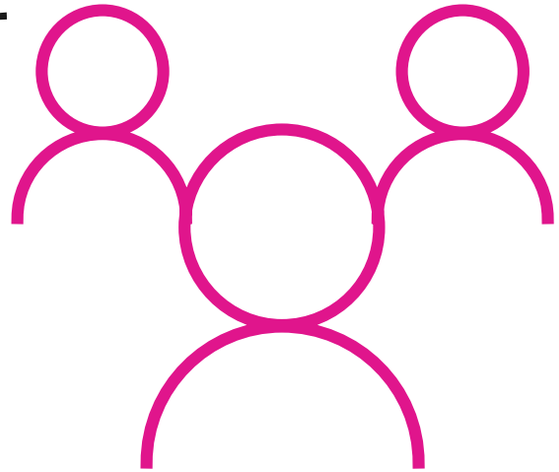
Twitter のご案内

#decode18 #DA21

本セッションに関するご質問やご感想は、#decode18 と セッション ID の ハッシュタグで、ご投稿をお願いします。

このセッションの対象

- Azure SQL Database について最新情報をキャッチアップしたい方
- Azure SQL Database について深く理解をしたい方



- Azure SQL Database ならまかせて！
  Azure Database for MySQL、Azure Database for PostgreSQL についてキャッチアップしたい！
  お客様は対象としておりません

おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

Azure のデータベースサービス

オンプレ RDBMS 連動型

- Azure Database Migration Service
- SQL Server Stretch Database

IaaS +

- SQL Server on VM

ETL

- Data Factory

PaaS RDB

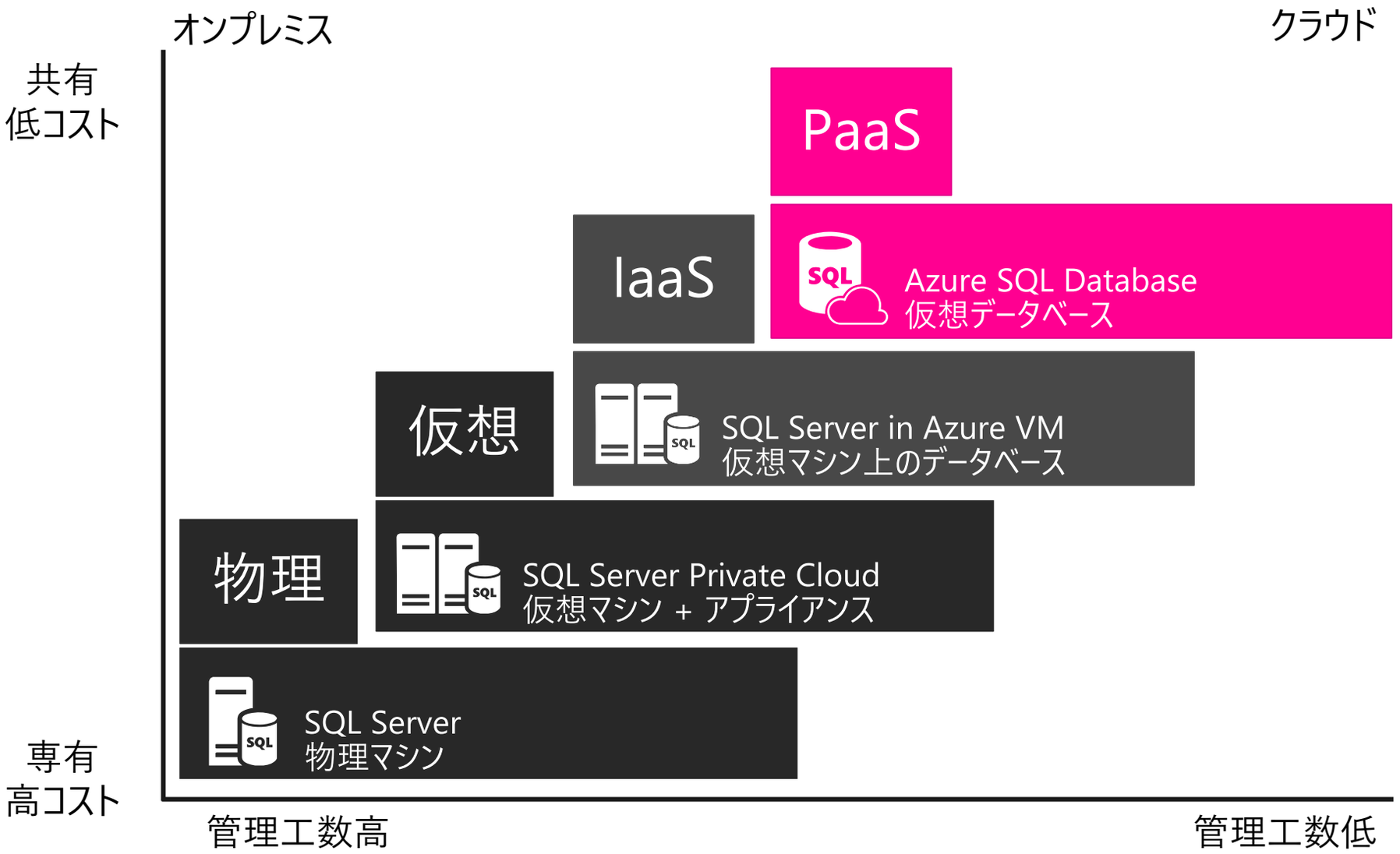
- Azure SQL Database
- Azure SQL Data Warehouse
- Azure Database for PostgreSQL
- Azure Database for MySQL

PaaS NoSQL

- Table Storage
- Redis Cache
- Azure Cosmos DB

参考：データベース
https://azure.microsoft.com/ja-jp/product-categories/databases/

SQL Server ファミリーのポートフォリオ



フルマネージドの SQL Server

VM上の SQL Server

利用者が管理

- データベース
- SQL Server
- OS

Azure が管理

- 仮想化
- ホスト OS

フルコントロール

Azure SQL Database

- データベース
- SQL Server
- OS
- 仮想化
- ホスト OS

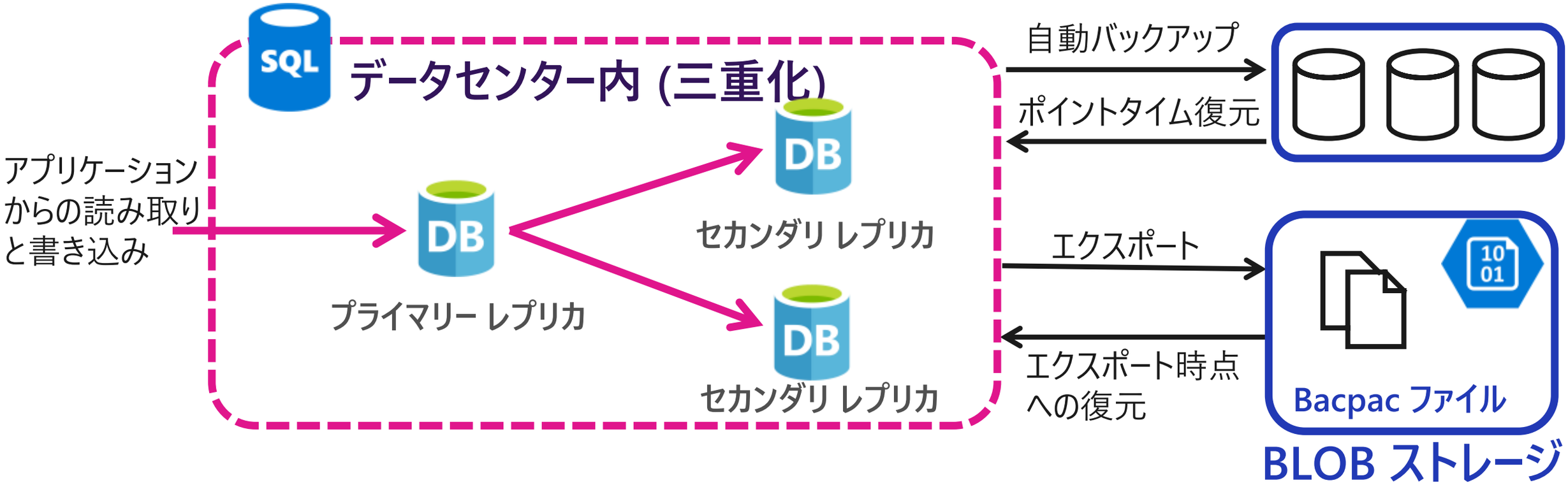
容易な管理

SQL Server と SQL Database エンジンの比較

項目	SQL Server	SQL Database
冗長構成	SQL Server の高可用性機能を使用し個別に構成	既定で DC 内の3重化構成 (SLA:99.99 %) Geo レプリケーションでリージョン間の冗長構成が可能 Premium / Business Critical では、ゾーン冗長 / 読み取りスケールを利用可能
トランザクション分離レベル	ロック方式 (Read Committed) が既定、行バージョン管理方式への変更可能	行バージョン管理方式 (RCSI または、SNAPSHOT) が既定

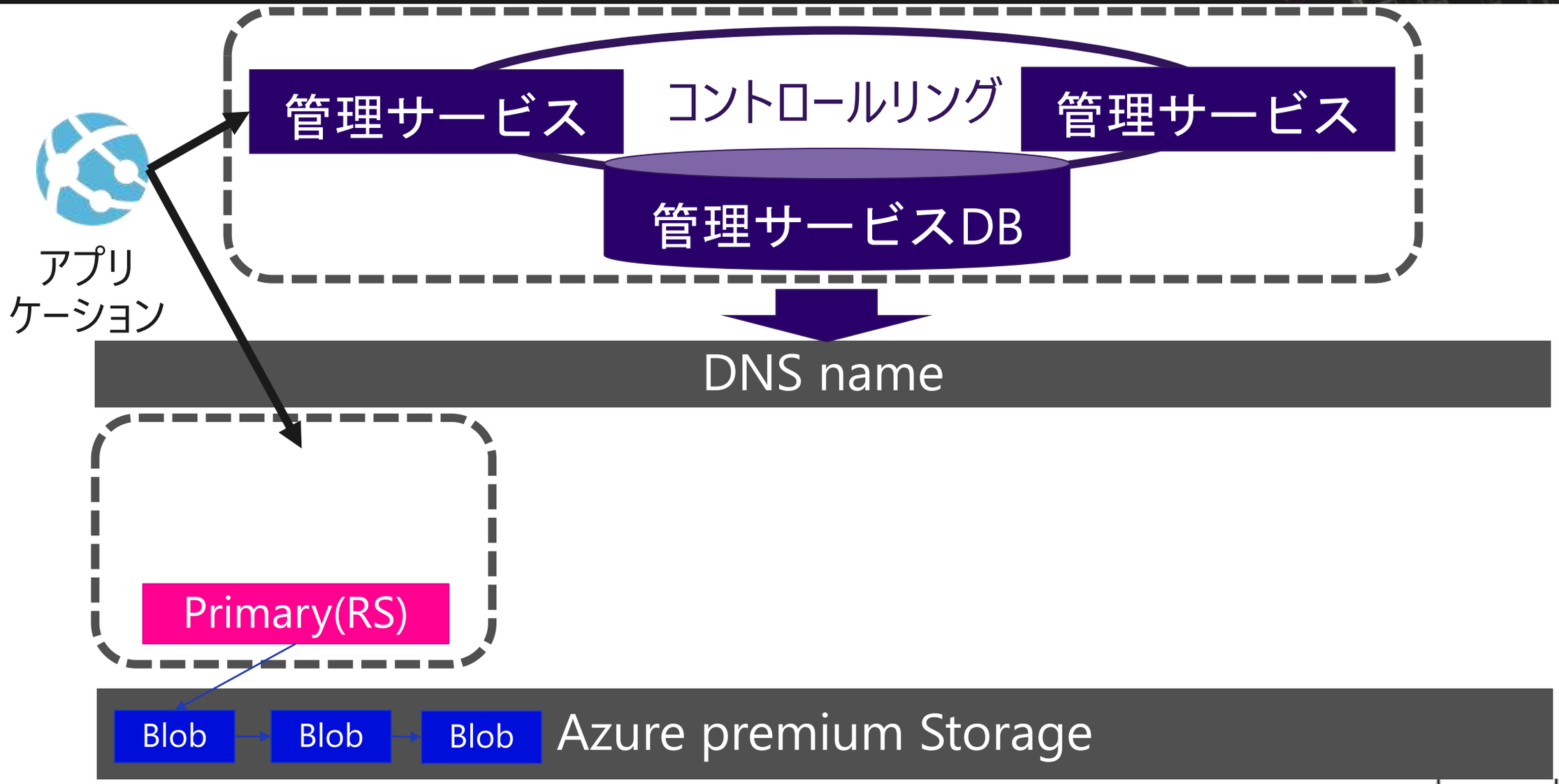
データベースの継続性

- 自動的に作成される 2 つのセカンダリ レプリカ
- ビルトインされたデータベースの自動バックアップ 機能

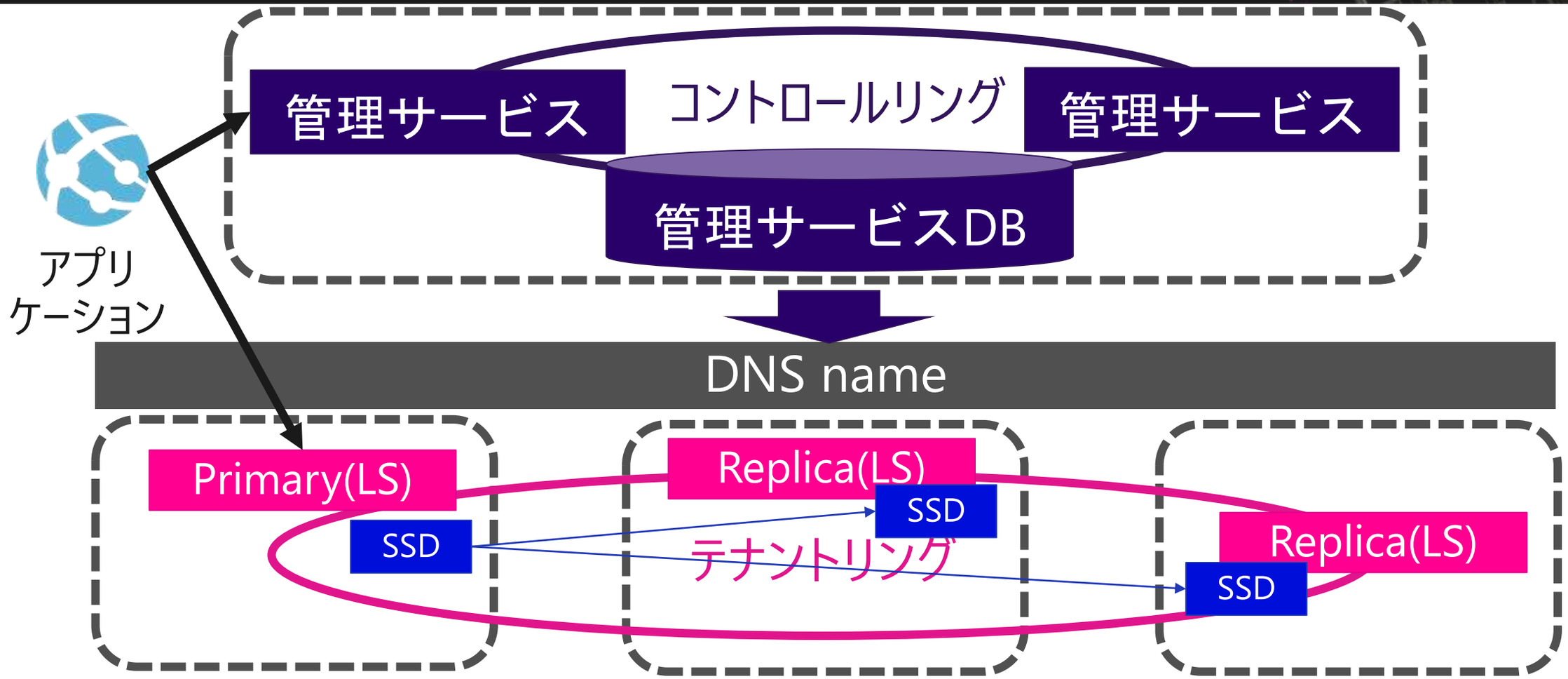


参考：読み取り専用レプリカを使用して読み取り専用クエリ ワークロードを負荷分散する (プレビュー)
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-read-scale-out

冗長構成について（Basic/Standard/汎用）



冗長構成について(Premium/Business Critical)



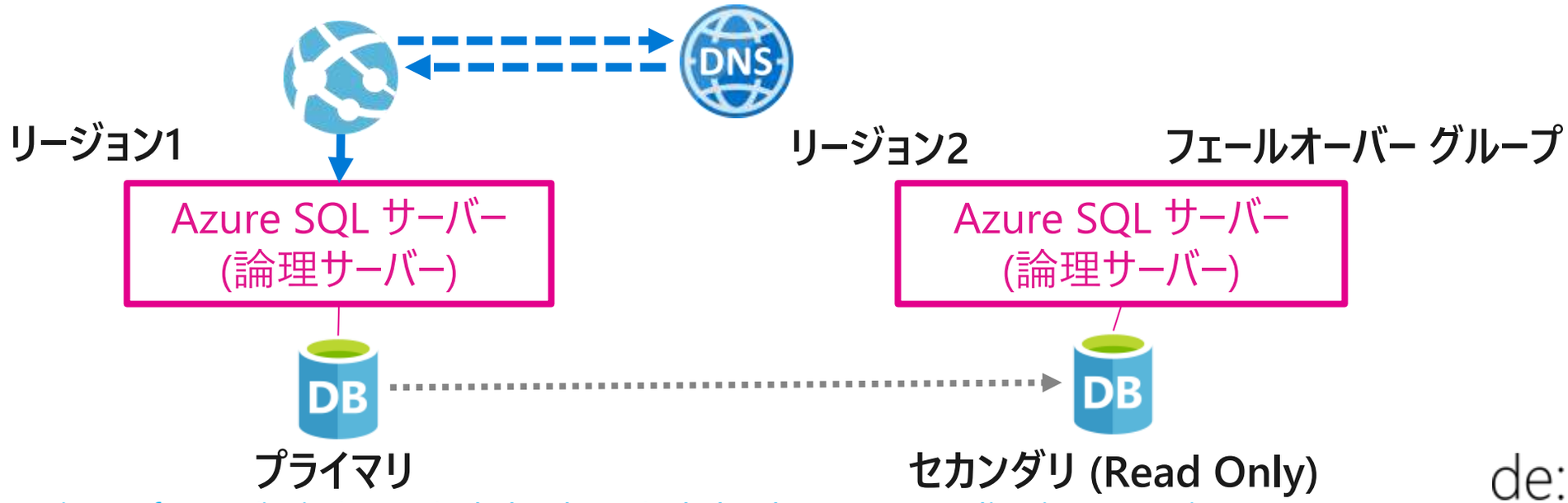
アクティブ geo レプリケーション

参考：読み取り専用レプリカを使用して読み取り専用クエリ ワークロードを負荷分散する (プレビュー)
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-read-scale-out

自動フェールオーバーグループ (プレビュー)

- Geoレプリケーション（プライマリサーバーとセカンダリサーバー）環境下で構成
  - グループレベルのレプリケーションと自動フェールオーバーの構成が可能
  - フェールオーバー時、プライマリとセカンダリの DNS サーバー CNAME レコードが切り替わる
  - フェールオーバー後接続文字列を変更しないで再接続できる

2 種類の CNAME レコード
- 読み取り/書き込みリスナー：<グループ名>.database.windows.net
- 読み取りリスナー：<グループ名>.secondary.database.windows.net



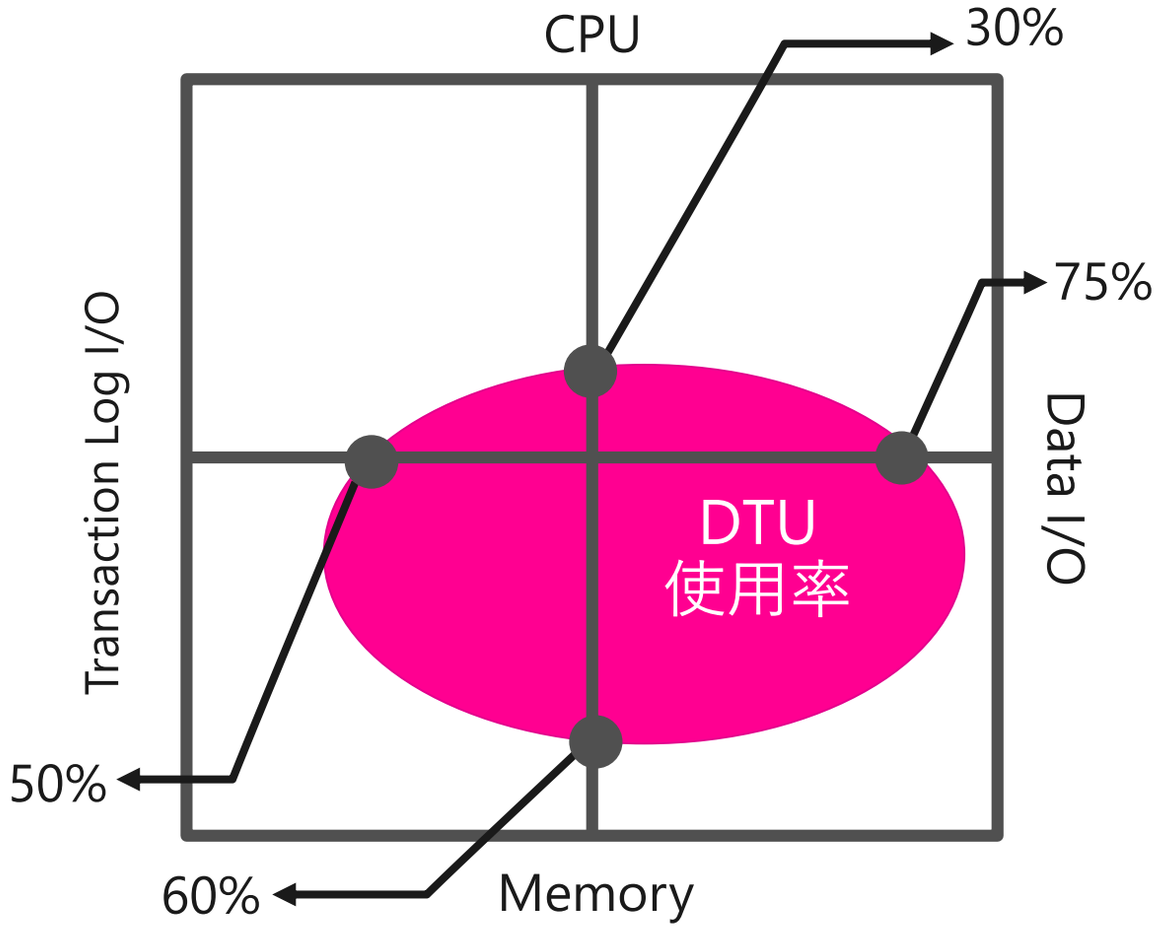
参考：
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-geo-replication-overview

おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

おさらい：Database Transaction Unit (DTU) とは

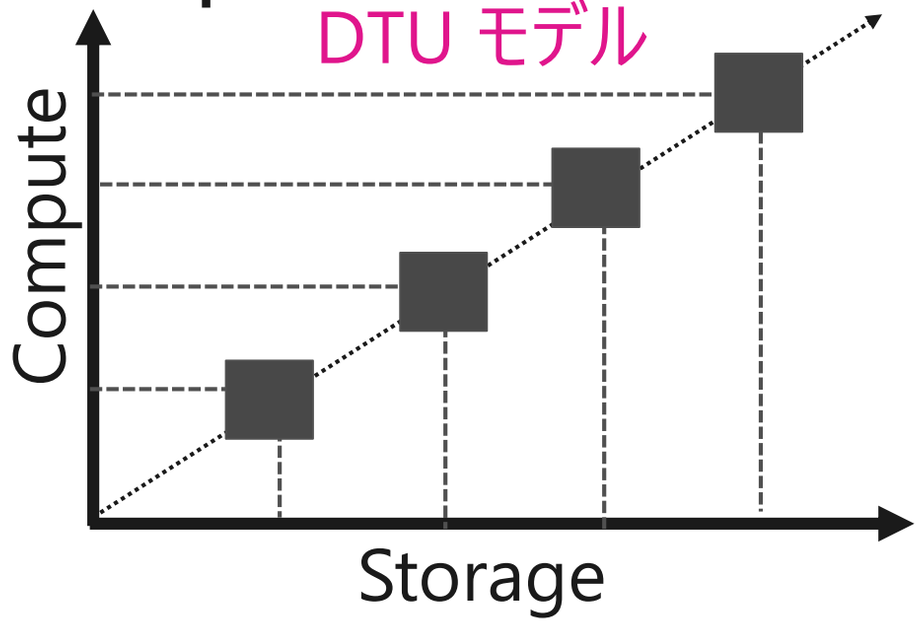
- 一定のパフォーマンスレベルで利用できることが保証されているリソースの最小単位
- リソースの上限に達すると、それ以上割り当てられなくなりワークロードが遅くなる
  - CPU
  - メモリ
  - データの I/O
  - トランザクションログの I/O

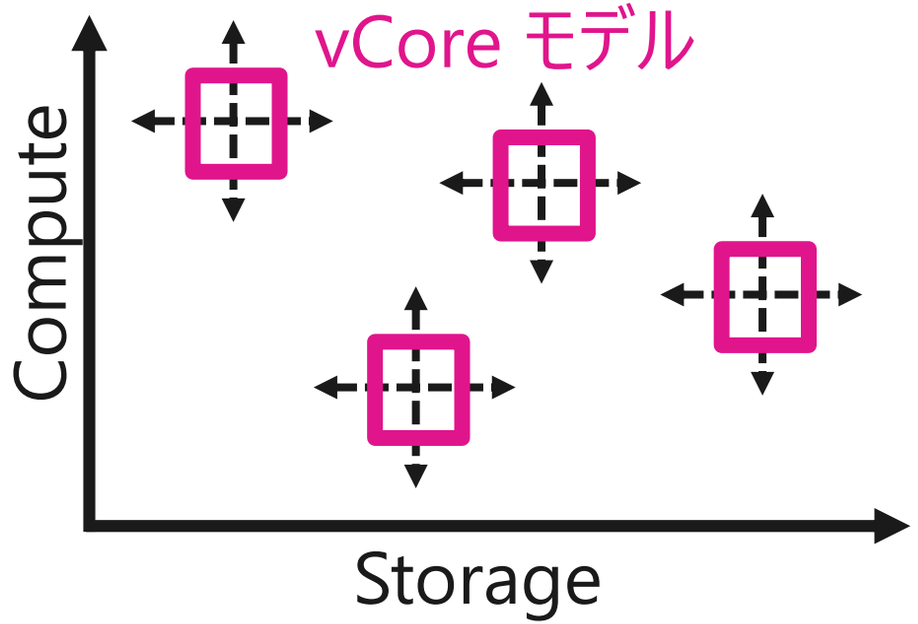


参考：データベース トランザクション ユニット (DTU) とエラスティック データベース トランザクション ユニット (eDTU) の説明
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-what-is-a-dtu

vCore モデル（プレビュー）

- Compute リソースと Storage リソースを独立してスケール





- Compute / Storage / IO リソースが事前に構成されている
- シンプルな利用モデル

- Compute / Storage / IO リソースを独立してスケール可能
- リソースの柔軟性 / 制御性 / 透明性を重視した利用モデル

参考： vCore-based purchasing model for Azure SQL Database (preview)
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-service-tiers-vcore

vCore モデル別の違い

モデル	SLA	説明
汎用	99.99 %	ほとんどのビジネスワークロードに最適でバランスのとれたオプション Azure Premium Storage ページ BLOB を使用
Business Critical		IO要件の高いビジネスアプリケーション 分離された複数のレプリカを使用した最高の耐障害性 ローカルSSDストレージを使用

Premium ≒ Business Critical

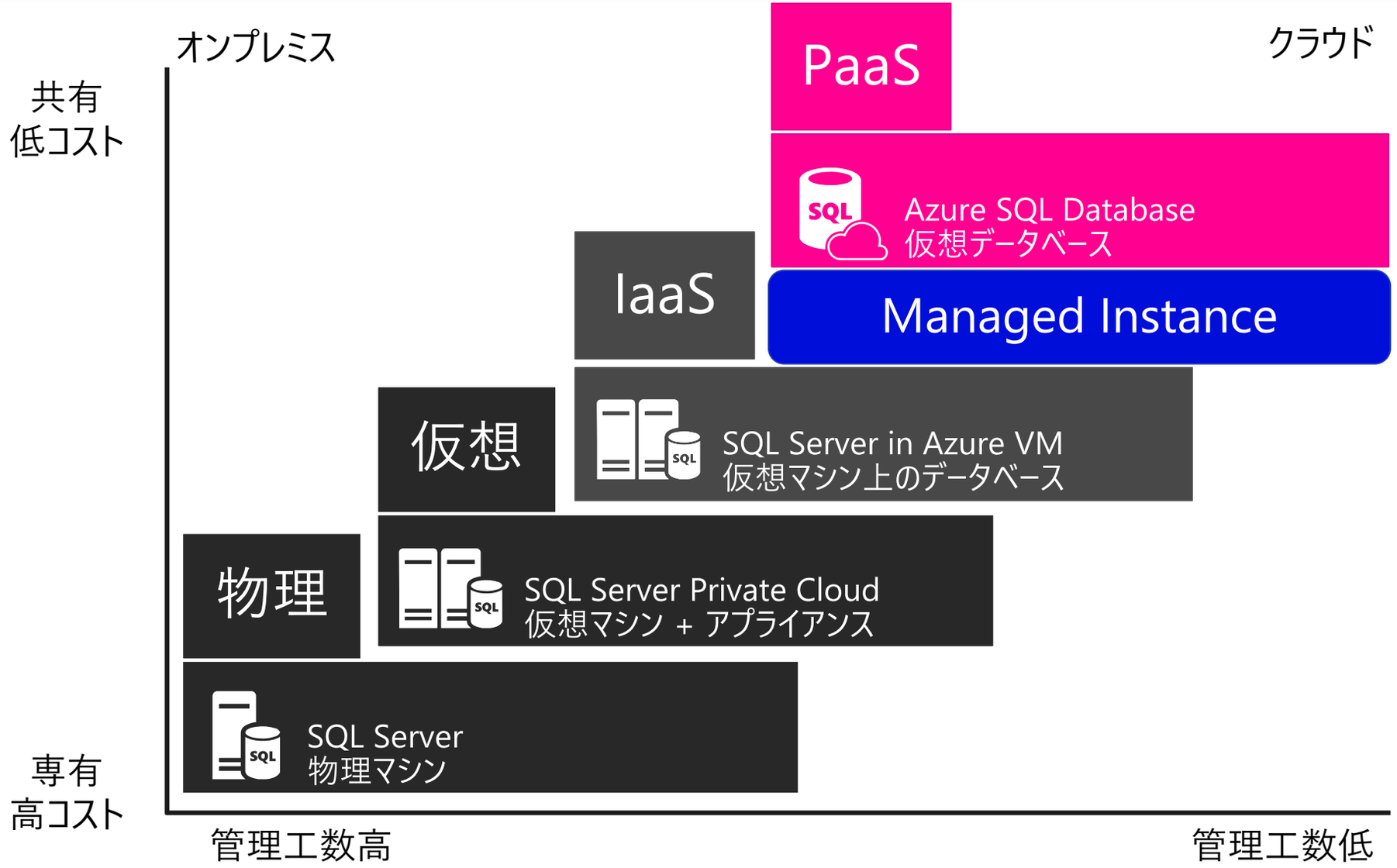
SQL Server の Azure ハイブリッド特典を使用することで
ライセンスコストを減らすことも可能

SQL Database Managed Instance (プレビュー)

- SQL Server Enterprise Edition とほぼ完全互換を目指したマネージドサービス
- PaaS のメリットを享受可能
  - 自動パッチ、バージョンアップデート、バックアップ、高可用性
- vCore ベースの購入モデル（DTUではない点に注意）
  - SA特典のライセンス持ち込み可能
- VNET サポート

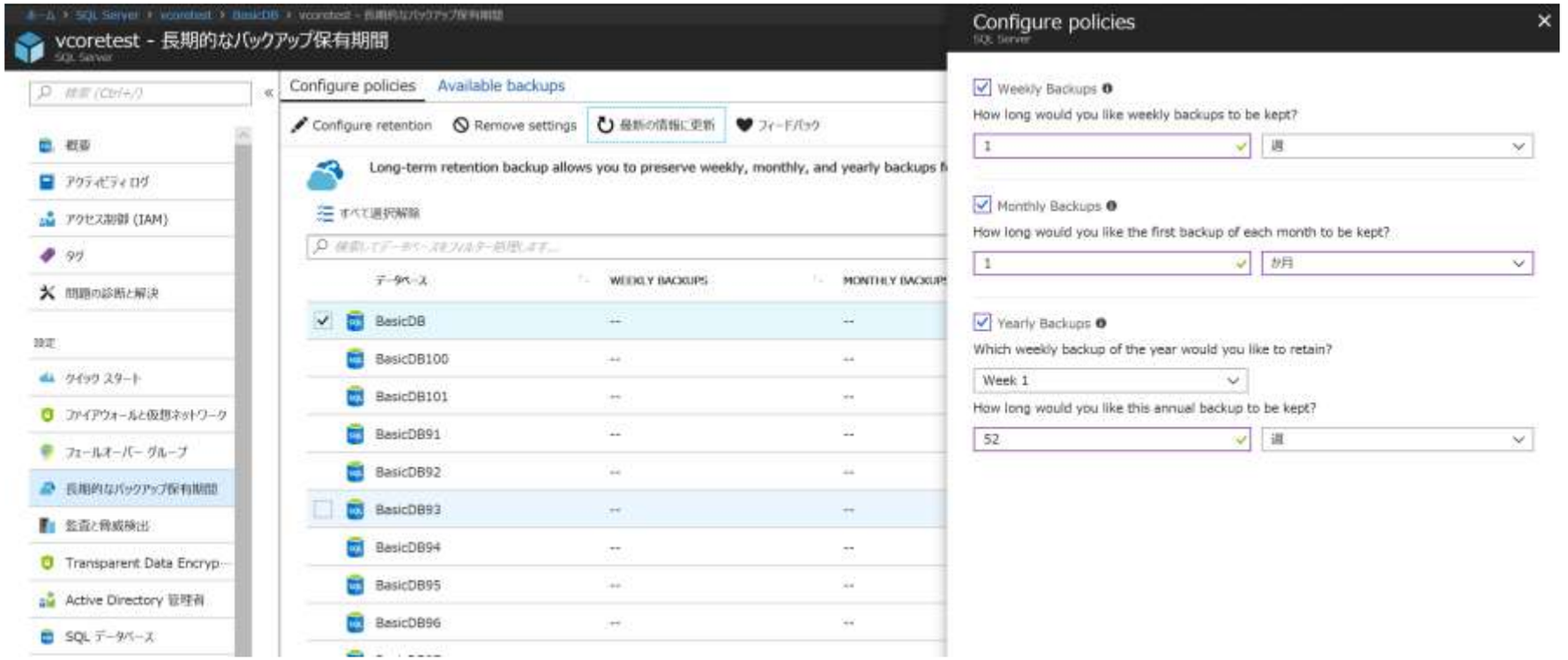
参考：マネージ インスタンス (プレビュー) とは?
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance

SQL Server ファミリーのポートフォリオ



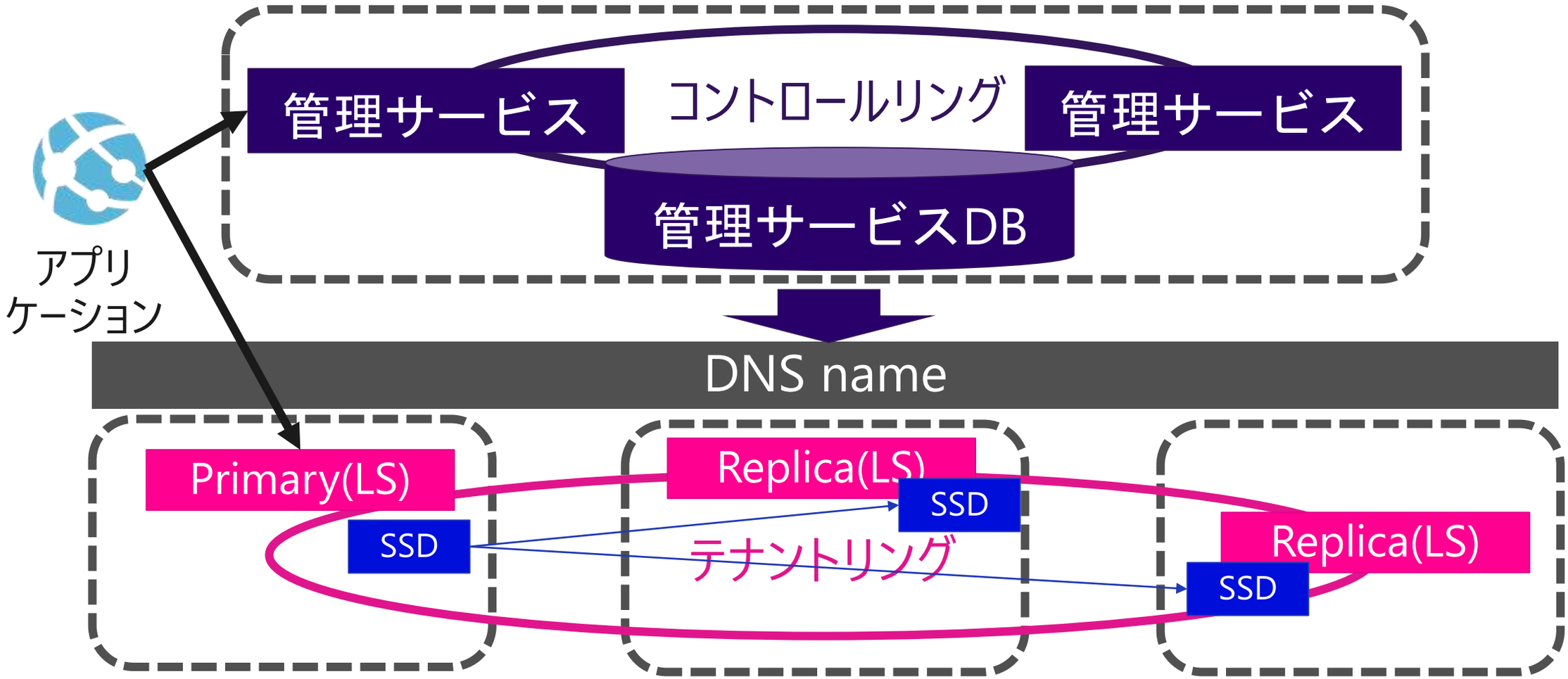
長期的なバックアップ保有期間 (プレビュー)

- 最長10 年間任意のサイクルでのバックアップを保持可能
  - 週次 / 月次 / 年次バックアップの保持期間を指定することが可能
  - 各バックアップの保持期間を 日 / 週 / 月 / 年 で指定することができる

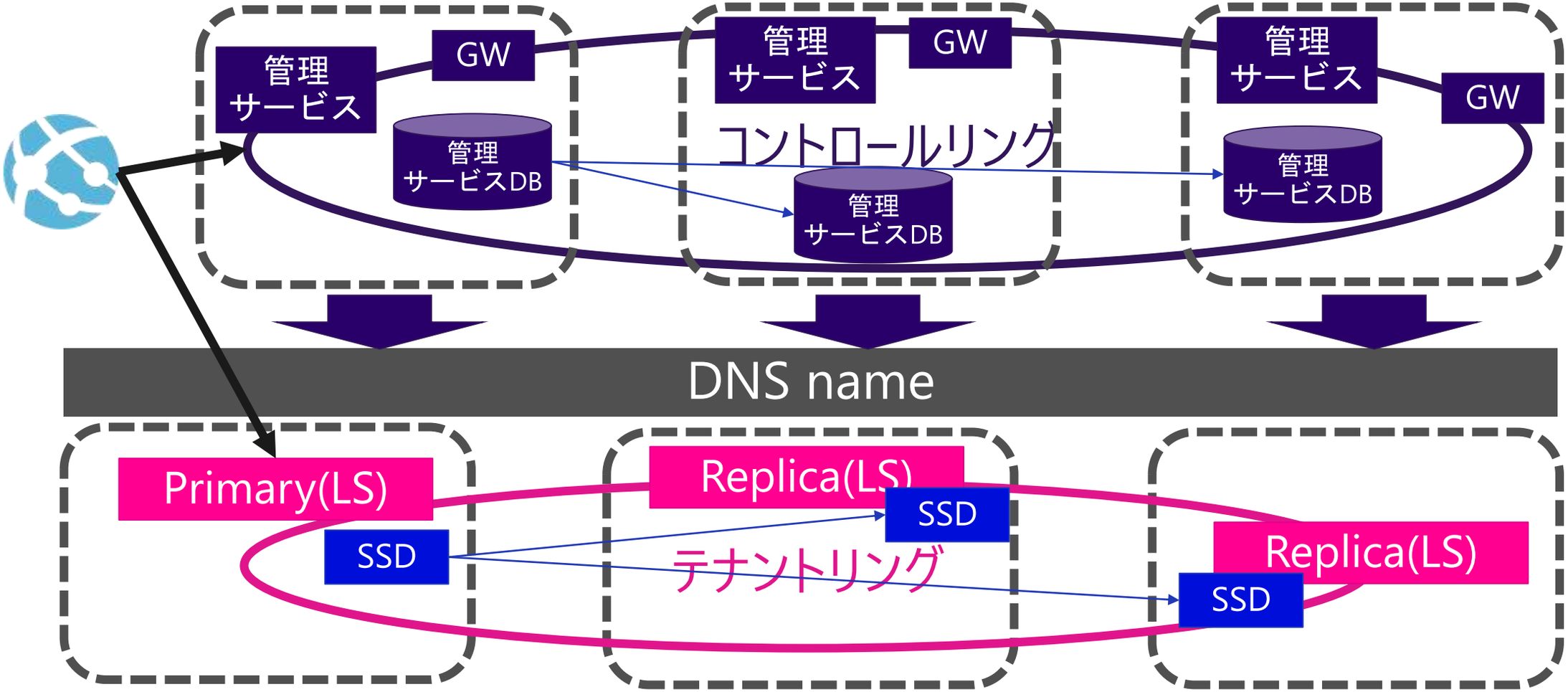


参考： 最大で 10 年間 Azure SQL Database のバックアップを格納する
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-long-term-retention

おさらい: 冗長構成について



ゾーン冗長の構成（プレビュー）



おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

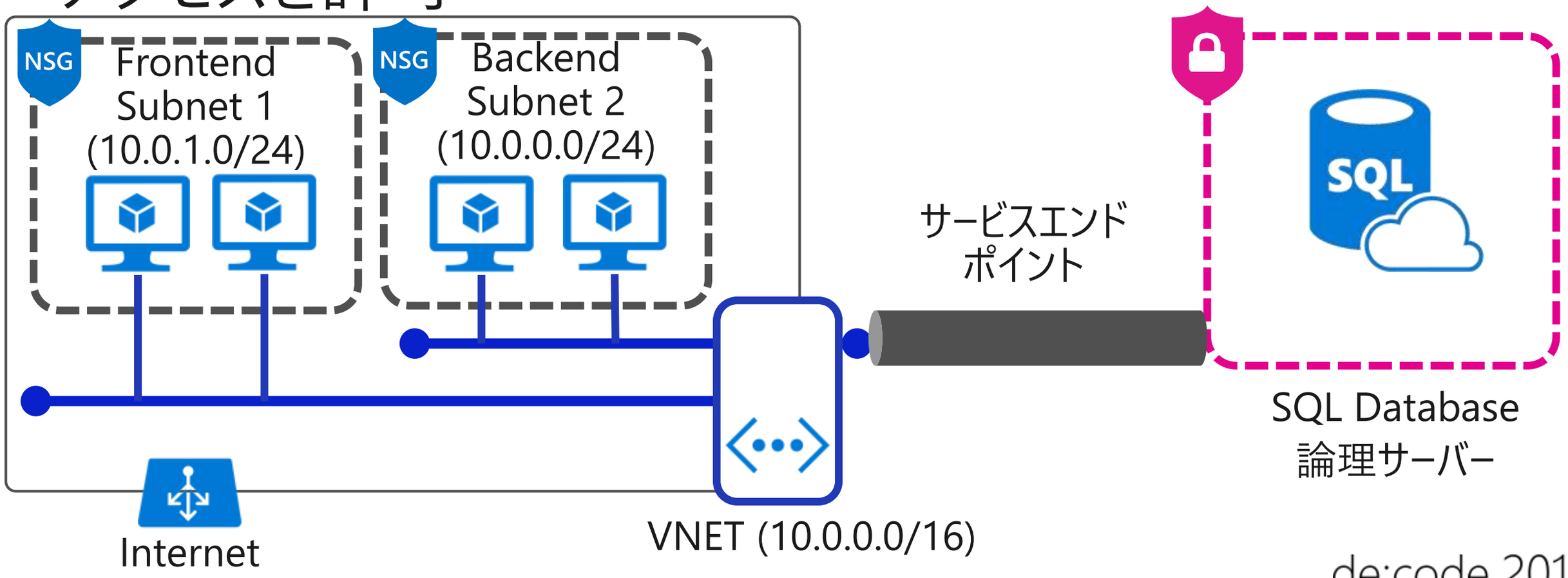
透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

Virtual Network サービス エンドポイント

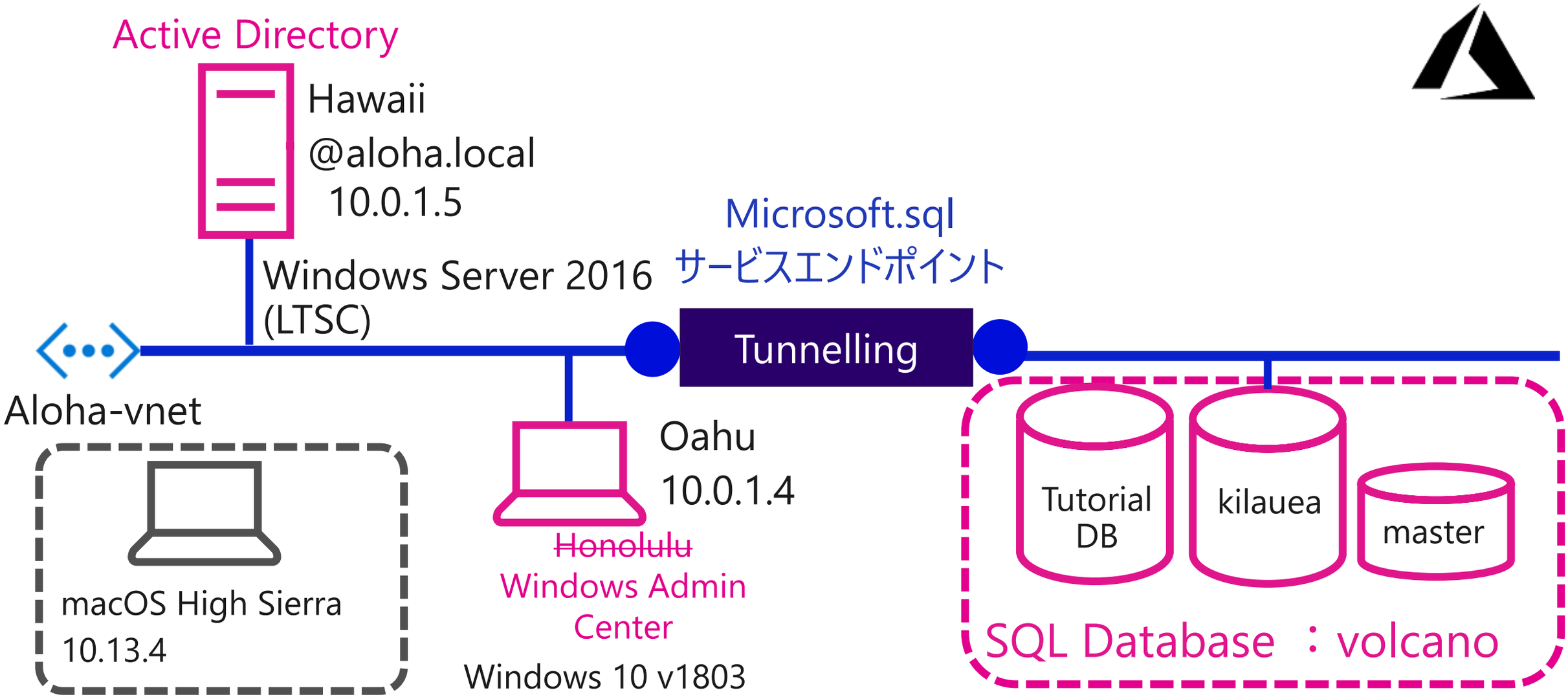
- 特定の仮想ネットワーク(VNET)のサブネットからアクセスを許可



Virtual Network サービスエンドポイント注意点

- Allow all Azure Services を削除した場合の影響
  - Import Export Service
  - SQL Database クエリ エディター
  - テーブル監査
  - データ同期への影響
- Azure Storage で VNET サービス エンドポイントを使用した場合の影響
  - Azure SQLDW PolyBase（軽減策あり）
  - Azure SQLDB の BLOB 監査

デモ環境


Active Directory
Hawaii
@aloha.local
10.0.1.5
Windows Server 2016
(LTSC)
Microsoft.sql
サービスエンドポイント
Tunnelling
Aloha-vnet
macOS High Sierra
10.13.4
Oahu
10.0.1.4
~~Honolulu~~
Windows Admin
Center
Windows 10 v1803
Tutorial
DB
kilauea
master
SQL Database ：volcano

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

データの検出と分類 (プレビュー)

- 機微なデータの**検出、分類、ラベル付け & 保護**を行う

ポータルから設定状況を確認可能

推奨事項の確認/設定と手動設定が可能

name	timestamp	application_name	client_ip	statement	data_sensitivity_information
audit_event	2018-04-03 14:51:40.9647445	Microsoft SQL S...	10.0.0.4	SELECT StateProvince FROM SalesLT.Add...	
audit_event	2018-04-03 14:51:41.0451455	Microsoft SQL S...	10.0.0.4	SELECT * FROM SalesLT.Address	Confidential - GDPR
audit_event	2018-04-03 14:51:41.0593738	Microsoft SQL S...	10.0.0.4		
audit_event	2018-04-03 14:51:41.0622653	Microsoft SQL S...	10.0.0.4	DECLARE @edition sysname; SET @editio...	
audit_event	2018-04-03 14:51:41.9990200	Microsoft SQL S...	10.0.0.4	SELECT @@SPID;	
audit_event	2018-04-03 14:51:42.0047041	Microsoft SQL S...	10.0.0.4	SELECT StateProvince FROM SalesLT.Add...	
audit_event	2018-04-03 14:51:42.0796559	Microsoft SQL S...	10.0.0.4	SELECT * FROM SalesLT.Address	Confidential - GDPR
audit_event	2018-04-03 14:51:42.3287990	Microsoft SQL S...	10.0.0.4		
audit_event	2018-04-03 14:51:42.3387285	Microsoft SQL S...	10.0.0.4	DECLARE @edition sysname; SET @editio...	

参考： Azure SQL Database のデータの検出と分類
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-data-discovery-and-classification

SQL 脆弱性評価

- データベース スキャン レポートが必要なコンプライアンス要件を満たす。
- データのプライバシー基準を満たす。
- 変更の追跡が困難である動的データベース環境を監視する。

参考：SQL 脆弱性評価
https://docs.microsoft.com/ja-jp/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント

Azure Active Directory 多要素認証

動的データマスク

行レベルセキュリティ

Security Management

データの検出と分類

脆弱性評価

Information Protection

透過的データ暗号化（TDE）

Bring Your Own Key

Always Encrypted

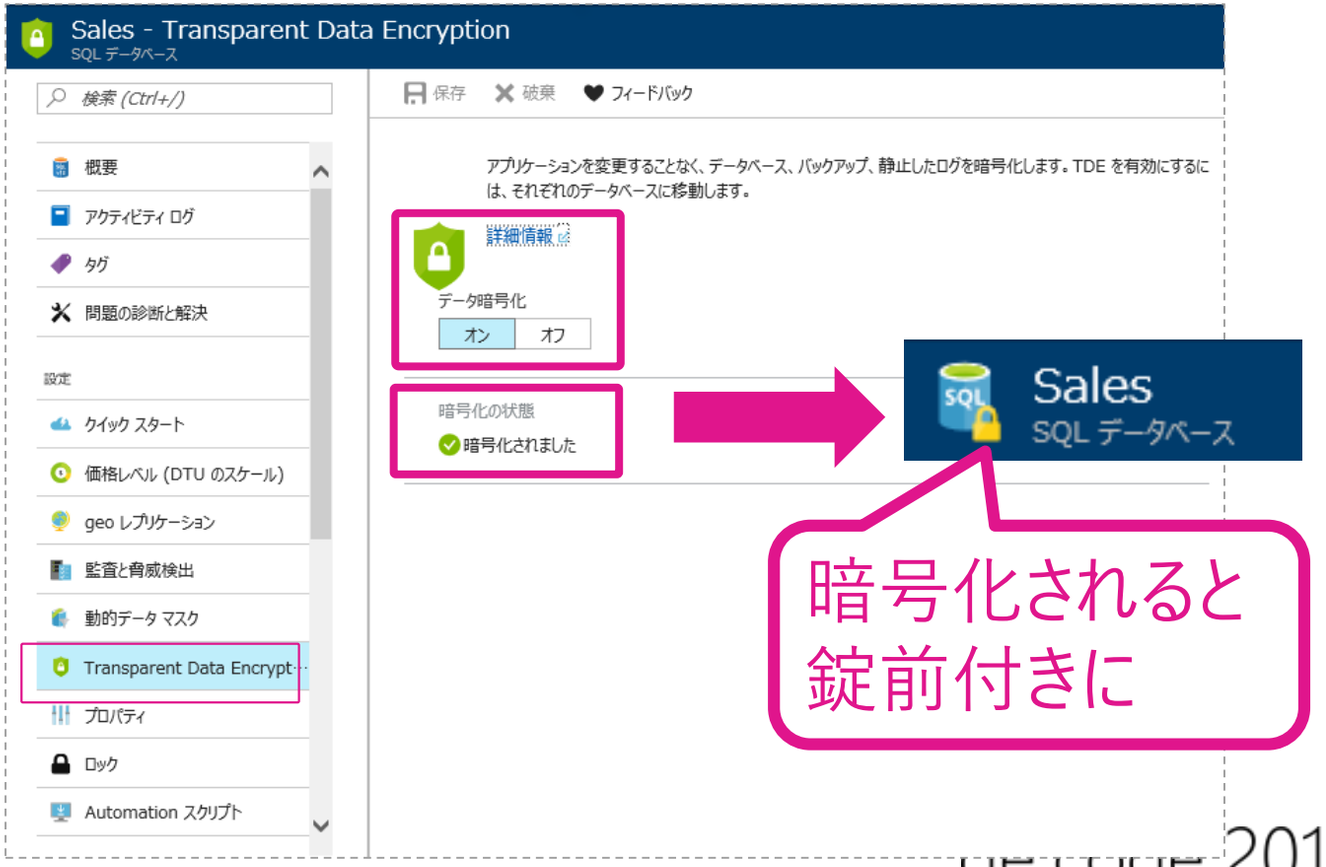
Threat Protection

脅威の検出

ファイアウォール

透過的なデータ暗号化 (TDE)

- データベース (データ / ログ / バックアップ) の暗号化
- 暗号化の状態が引き継がれる操作
  - Geo レプリケーション
  - ポイント イン タイム復元
  - 削除されたデータベースからの復元
  - データベースのコピー

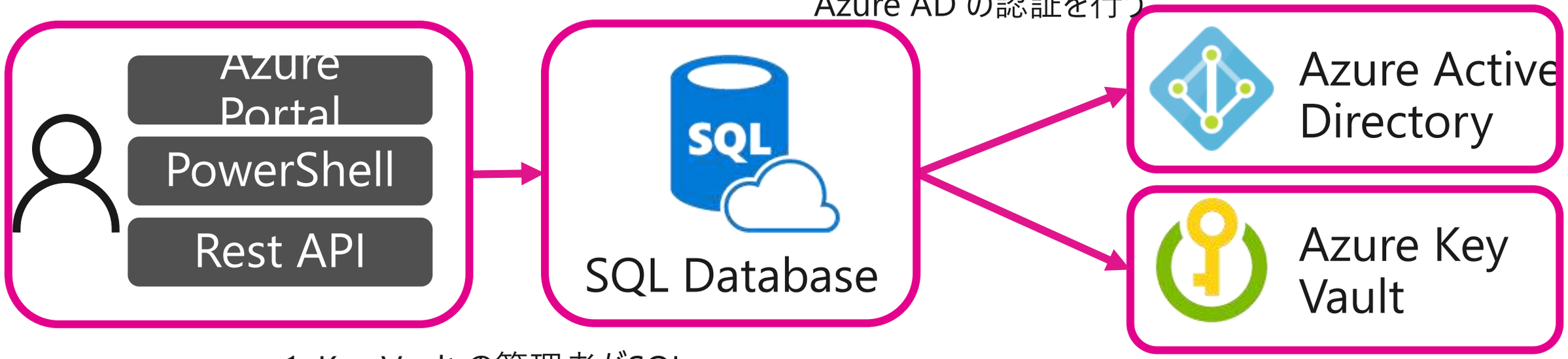


bacpac ファイル / bcp コマンドによるエクスポート時には暗号化されていないことに注意

暗号化されると錠前付きに

透過的データ暗号化(BYOK)

- TDE プロテクター(非対称キー)を使って、データベース暗号化キー (DEK) を暗号化
- TDE プロテクターは、Azure のクラウドベースの外部キー管理システムである Azure Key Vault のコントロールに格納



参考：Azure SQL Database および Data Warehouse 用の Bring Your Own Key サポートによる Transparent Data Encryption
https://docs.microsoft.com/ja-jp/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql?view=azuresqldb-current

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント

Azure Active Directory 多要素認証

動的データマスク

行レベルセキュリティ

Security Management

データの検出と分類

脆弱性評価

Information Protection

透過的データ暗号化（TDE）

Bring Your Own Key

Always Encrypted

Threat Protection

脅威の検出

ファイアウォール

セキュリティ関連機能一覧

Access Management

Virtual Network サービスエンドポイント
Azure Active Directory 多要素認証
動的データマスク
行レベルセキュリティ

Security Management

データの検出と分類
脆弱性評価

Information Protection

透過的データ暗号化（TDE）
Bring Your Own Key
Always Encrypted

Threat Protection

脅威の検出
ファイアウォール

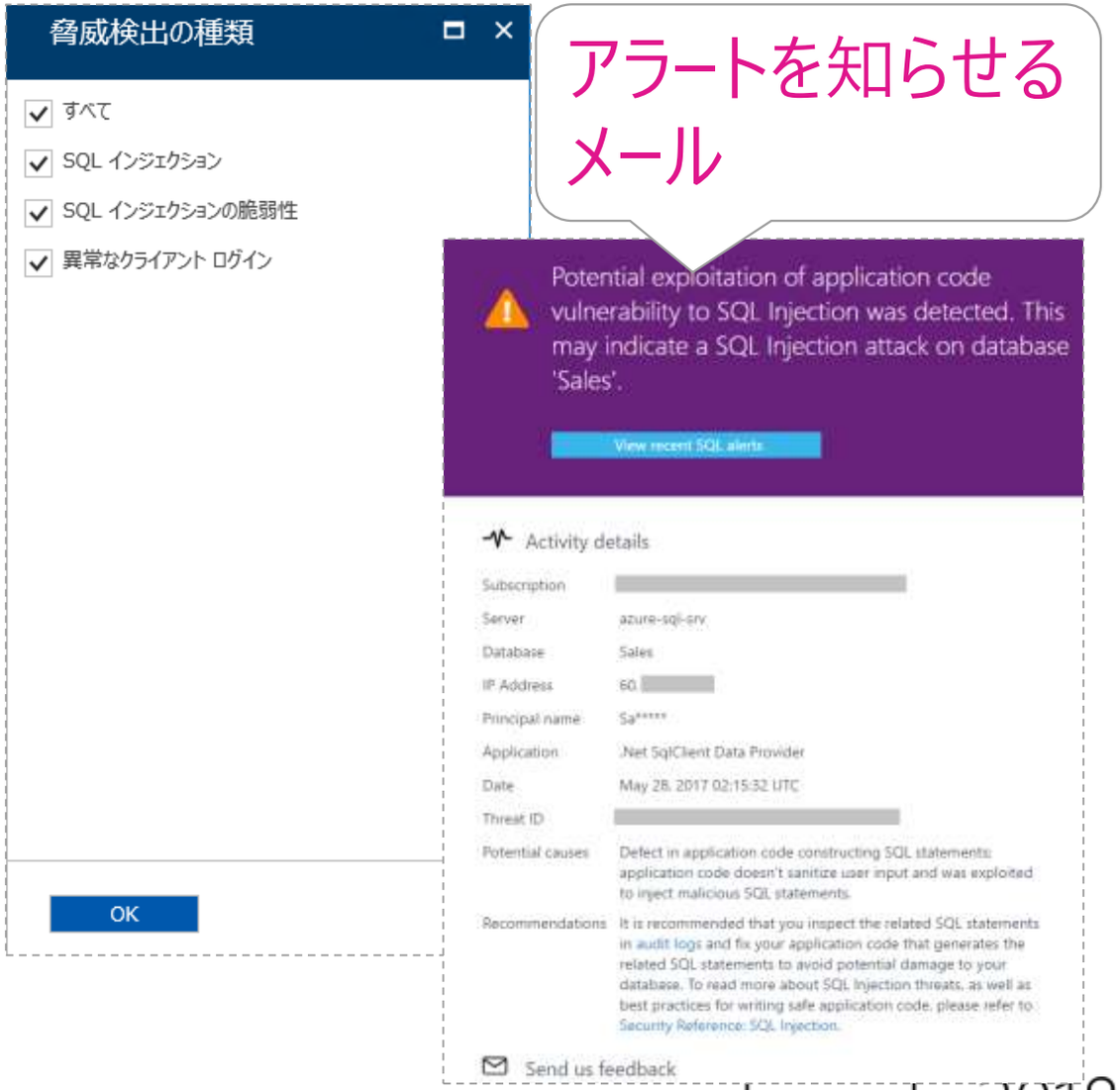
監査と脅威の検出

- Azure Security Center の機能を使用
- 潜在的なセキュリティ脅威を示す異常な アクティビティ を検出
- 指定されたメール アドレスにアラートを送信
- [監査ログ] ブレードで詳細を確認

参考： SQL Database の脅威の検出
https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-threat-detection

脅威検出の種類と方法

- 既定ではすべてを検出
  - SQL インジェクション
  - SQL インジェクションの脆弱性
  - 異常なクライアント ログイン
- 脅威検出の方法
  - 確定的な検出
  - 動作検出

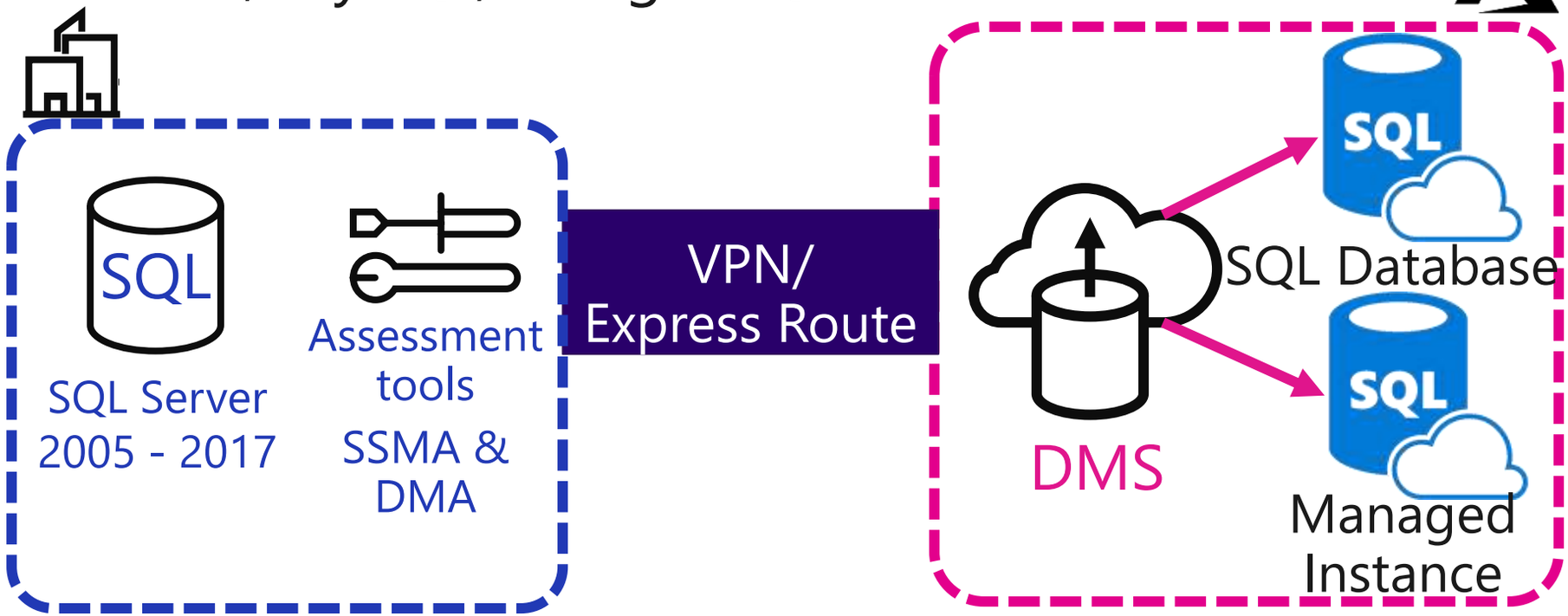


おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

Azure Database Migration Service (DMS)

- 様々なシナリオでの移行をサポートするサービス
  - 現在は SQL Server → Azure SQL Database, Managed Instance (Preview)
  - 今後は Oracle , Netezza, MySQL, PostgreSQL に対応予定



おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

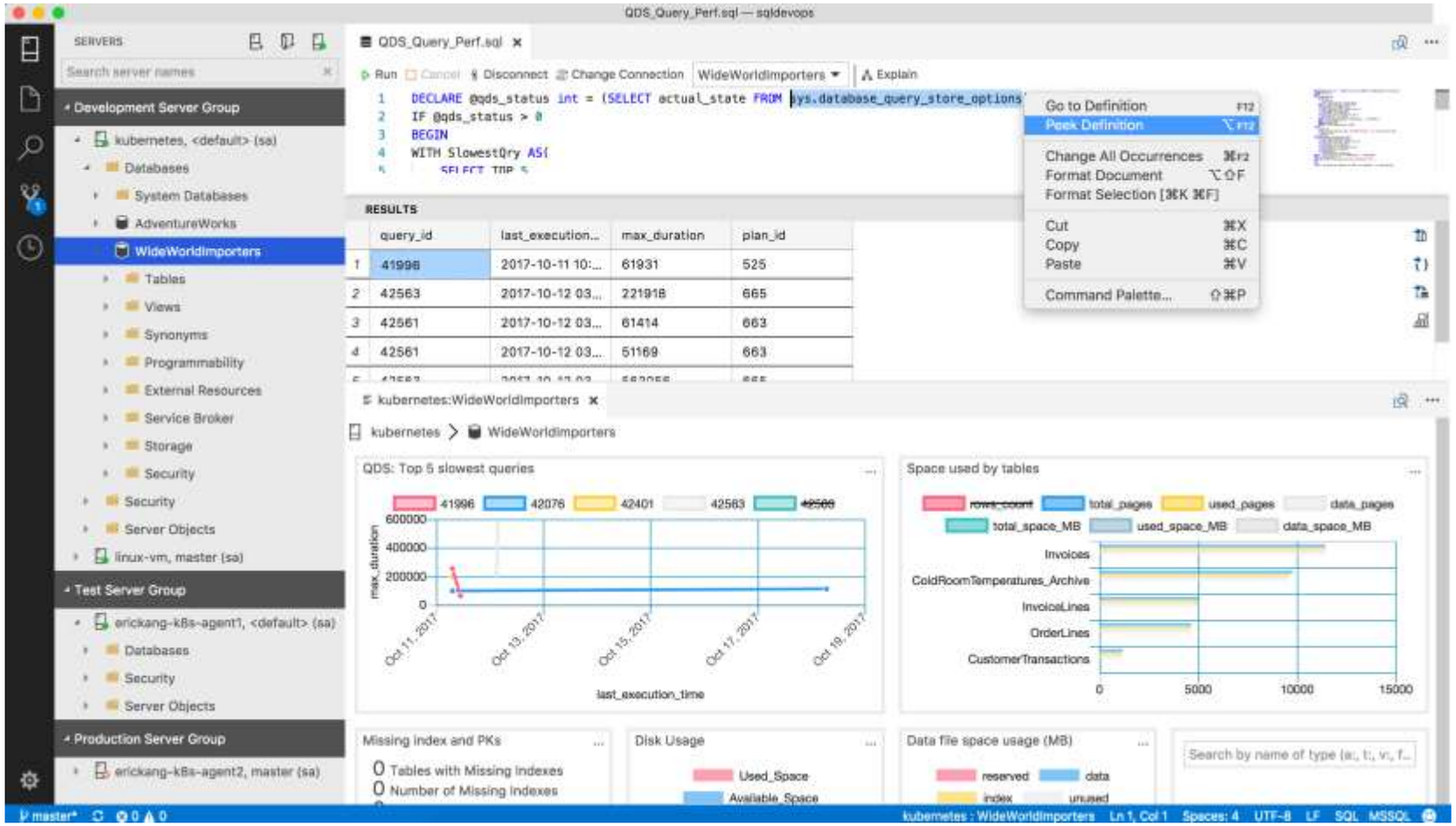
SQL Database の管理ツール

SQL Server Management Studio	Visual Studio Code プラグイン（vscode-mssql)	SQL Operations Studio（プレビュー）
	New	New
• 以前からあるツール • Windows 版のみ • 最新版は17.6 • SQL Server インストール媒体と別に配布	• マルチプラットフォーム対応 • OSS • マーケットプレイスからインストール可能	• マルチプラットフォーム対応 • OSS

- mssql
  https://marketplace.visualstudio.com/items?itemName=ms-mssql.mssql
- SQL Operations Studio
  https://docs.microsoft.com/en-us/sql/sql-operations-studio/download

SQL Operations Studio

- 2017/11 PASS Summit で発表。新しいツール



おしながき

- SQL Database のおさらい
- SQL Database What's New
  - 基本機能
  - セキュリティ関連機能
  - オンプレ連動
  - ツール
- まとめ

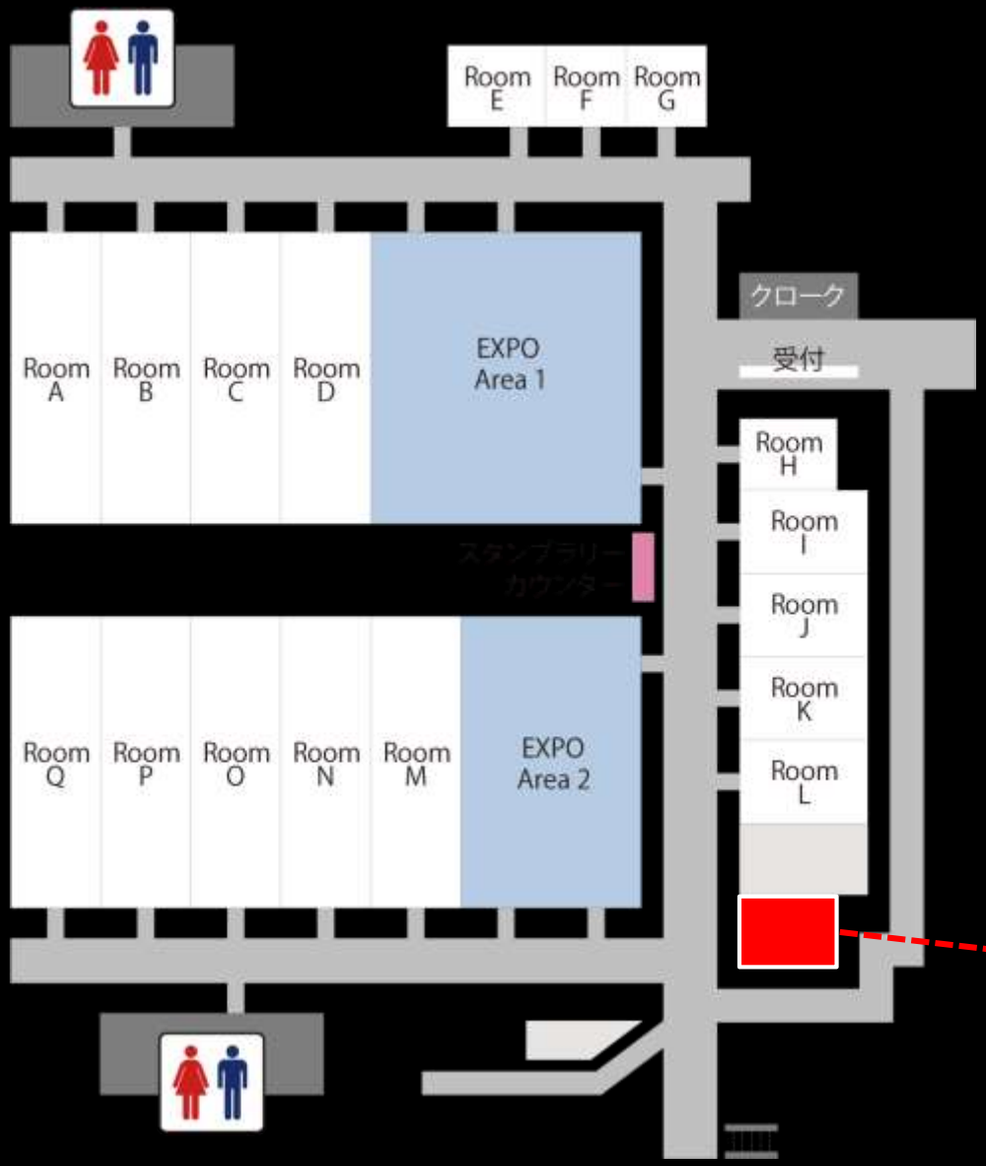
まとめ

- SQL Database は日々進化を続けています。
- セキュアで運用負荷を少なくするための選択肢として
  SQL Database をご利用ください！

このセッションの資料と参考スクリプトはこちら

https://github.com/miyamam/decode18

Microsoft



Ask the Speaker のご案内

ブレイクアウトセッション終了後の休憩時間に、登壇したスピーカーに直接ご質問いただけるコーナーを「Ask The Speakers」Room に用意しております。セッション内容のより深い理解のため、ぜひお役立てください。

■「Ask The Speakers」Room

de:code 2018

Microsoft

- 本書に記載した情報は、本書各項目に関する発行日現在の Microsoft の見解を表明するものです。Microsoftは絶えず変化する市場に対応しなければならないため、ここに記載した情報に対していかなる責務を負うものではなく、提示された情報の信憑性については保証できません。
- 本書は情報提供のみを目的としています。 Microsoft は、明示的または暗示的を問わず、本書にいかなる保証も与えるものではありません。
- すべての当該著作権法を遵守することはお客様の責務です。Microsoftの書面による明確な許可なく、本書の如何なる部分についても、転載や検索システムへの格納または挿入を行うことは、どのような形式または手段（電子的、機械的、複写、レコーディング、その他）、および目的であっても禁じられています。
  これらは著作権保護された権利を制限するものではありません。
- Microsoftは、本書の内容を保護する特許、特許出願書、商標、著作権、またはその他の知的財産権を保有する場合があります。Microsoftから書面によるライセンス契約が明確に供給される場合を除いて、本書の提供はこれらの特許、商標、著作権、またはその他の知的財産へのライセンスを与えるものではありません。

© 2018 Microsoft Corporation. All rights reserved.
Microsoft, Windows, その他本文中に登場した各製品名は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。
その他、記載されている会社名および製品名は、一般に各社の商標です。

© 2018 Microsoft Corporation. All rights reserved.

本情報の内容（添付文書、リンク先などを含む）は、作成日時点でのものであり、予告なく変更される場合があります。

- Analyzing the Azure SQL Database DTU Calculator Results https://justinhenriksen.wordpress.com/2015/11/16/analyzing-the-azure-sql-database-dtu-calculator-results/

参考資料

- Azure SQL Database 用 VNet サービス エンドポイントの一般提供を開始
  https://blogs.technet.microsoft.com/jpitpro/2018/03/01/vnet-service-endpoints-for-azure-sql-database-now-generally-available/
- VNet Service Endpoints for Azure SQL Database now generally available
  https://azure.microsoft.com/en-us/blog/vnet-service-endpoints-for-azure-sql-database-now-generally-available/
- SQL Database と SQL Data Warehouse でのユニバーサル認証 (MFA 対応の SSMS サポート)
  https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-ssms-mfa-authentication
- Azure SQL Database のデータの検出と分類
  https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-data-discovery-and-classification
- SQL 脆弱性評価
  https://docs.microsoft.com/ja-jp/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-2017
- SQL Database 監査の使用
  https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-auditing
- SQL Database の脅威の検出
  https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-threat-detection

参考資料

- Azure SQL Database および Data Warehouse 用の Bring Your Own Key サポートによる Transparent Data Encryption
  https://docs.microsoft.com/ja-jp/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql?view=azuresqldb-current
- 概要: フェールオーバー グループとアクティブ geo レプリケーション
  https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-geo-replication-overview