ログの取得・保管について

ログの取得・保管が必要な理由

- クラウドサービスにおいてログの取得や保管等の管理はクラウドサービスの利用者が行います。
- 問題が発生したときの原因調査に備えて、事前にログの取得・保管設定を行っておくことが必要です。
  （例えば、Webサービスの一時的な中断の原因を調べたい、誰かがリソースの設定変更を行っていないか確認したい、通信履歴を確認したい 等）

取得対象

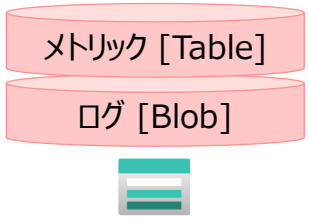
- 仮想マシンの診断ログ（起動時のログやパフォーマンスログ 等）
- 仮想マシン以外のAzureリソースのリソースログ（旧称:診断ログ、Network Security Group や VPN Gateway のログ 等）
- アクティビティログ（Azure上の操作ログ）

取得イメージ

アプリケーション
ゲストOS
リソース
操作

※VMにはエージェント(Azure Diagnostics, AMA 等)のインストールが必要です
※アプリケーションにはインストルメンテーションのインストールが必要です

収集



※リージョン毎にストレージアカウントが必要です

設定方法

- Azure Monitor全般 — Azure Monitor のドキュメント
- 仮想マシンの診断ログ(Windows) — インストールと構成
- 仮想マシンの診断ログ(Linux) — メトリックとログを監視する
- 仮想マシン以外のリソースログ — 診断設定を作成する
- アクティビティログ — Azure Storage への送信
- Log Analytics — ワークスペースを作成する
- Application Insights — 概要