Log Analytics とは?

Log Analytics

Log Analytics は、クラウド環境とオンプレミス環境のリソースによって生成されたデータを収集および分析するのに役立つサービスです。

ログ クエリを使用すると、Azure Monitor Logs で収集されたデータの値を 完全に活用できます。<mark>強力なクエリ言語</mark>を使用すると、複数のテーブルのデータを結合し、大量のデータを集計し、最小限のコードで複雑な操作を実行できます。サポートデータが収集され、適切なクエリの作成方法を理解していれば、ほとんどすべての質問に答え、分析を実行できます。

洞察やソリューションなどの Azure Monitor の一部の機能は、基になるクエリに公開することなくログ データを処理します。Azure Monitor の他の機能を完全に活用するには、クエリの構築方法と、クエリを使用して Azure Monitor Logs でデータを対話的に分析する方法を理解する必要があります。

Kusto クエリ言語 (KQL)

Log Analytics の起動方法

Log Analytics は、Azure portal 内の複数の場所から起動できます。 Log Analytics で使用できるデータのスコープは、起動方法によって決まります。 詳しくは、「クエリ スコープ」を参照してください。

- [Azure Monitor] メニューまたは [Log Analytics ワークスペース] メニューの [ログ] を選択します。
- Application Insights アプリケーションの [概要] ページから [ログ] を選択します。
- Azure リソースのメニューから [**ログ**] を選択します。

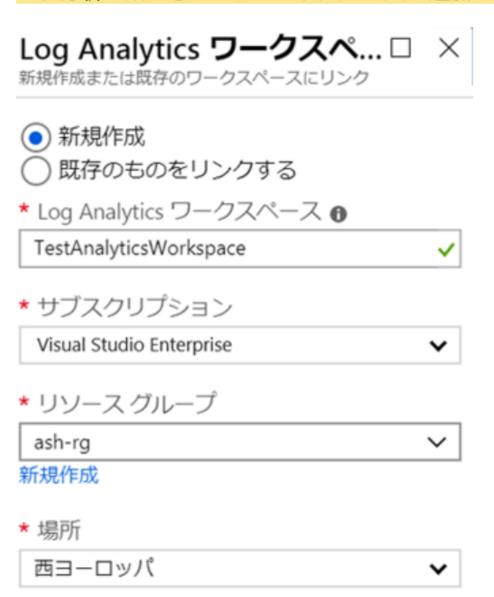
Azure Monitor ログのデプロイの設計

2019/09/20 • 🗐 😷 🛎 🤿

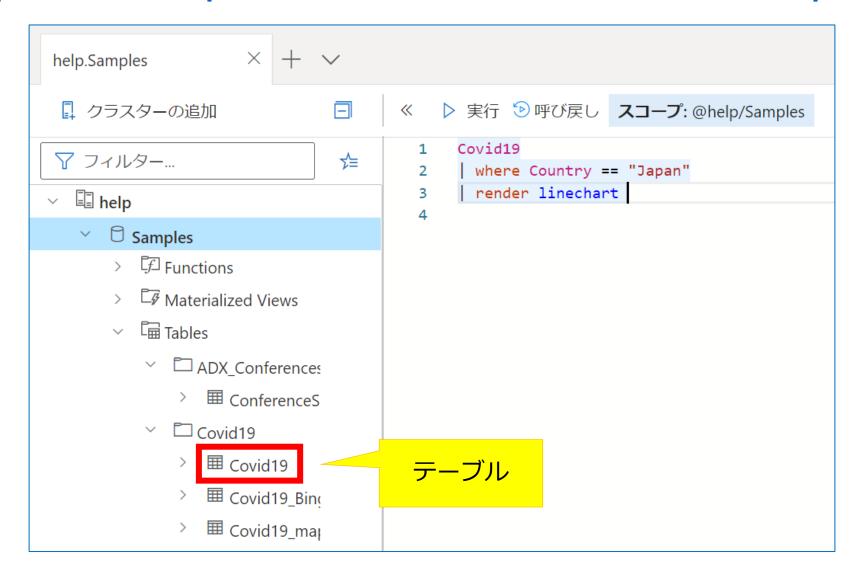
Azure Monitor では、ログデータが Log Analytics ワークスペースに格納されます。Log Analytics ワークスペースは Azure リソースであり、データが収集、集計され、管理境界として機能するコンテナーです。 1 つまたは複数のワークスペースを Azure サブスクリプションにデプロイできますが、組織のニーズを満たす、コスト効率に優れ、管理可能で、スケーラブルなデプロイを実現するためのガイドラインに初期のデプロイが従っていることを確認するために、理解しておく必要がある考慮事項がいくつかあります。

ワークスペースの作成

ログ分析を始めるには、ワークスペースを追加する必要があります。



https://help.kusto.windows.net/Samples



https://help.kusto.windows.net/Samples

	構造化問い合わせ言語 (SQL)	Kusto クエリ言語 (KQL)
StormEvents テーブルの データを10件表示	select top 10 * from StormEvents order by StartTime desc	StormEvents <mark>top</mark> 10 by StartTime desc
StormEvents テーブルの データ件数を表示	select count(*) from StormEvents	StormEvents count

https://help.kusto.windows.net/Samples

	Kusto クエリ言語 (KQL)
Covid19テーブルの 全データを表示	Covid19
Covid19テーブルの、 Country列の値がJapanである データを表示	Covid19 where Country == "Japan"
Covid19テーブルの、 Country列の値がJapanである データを 線グラフ(linechart) で表示	Covid19 where Country == "Japan" render linechart