KQL for Azure Admins

Course Duration: 16 Hours (2 Days)

Overview

The "KQL for Azure Admins" course is designed to equip learners with the skills to utilize Kusto Query Language (KQL) effectively within Azure services. As a vital tool for Azure administrators, KQL helps in analyzing and managing large datasets across various Azure resources. Starting with an introduction to KQL commands, syntax, elements, and operators, learners will gain foundational knowledge necessary to run KQL queries. The course progresses to more advanced topics such as Analyzing query results, utilizing operators to summarize, filter, and Visualize data, and building multi-table statements to extract comprehensive insights. Learners will also explore constructing KQL statements specifically for Microsoft Sentinel, including the use of various operators like search, where, extend, and project. Hands-on lessons guide participants in writing their first queries, connecting to resources, and manipulating data returns. Finally, the course covers Data exportation techniques to CSV files and Power BI, ensuring learners can share their insights effectively. Through this KQL training and Kusto training, Azure administrators will be empowered to perform complex data analysis, enhancing their operational capabilities within the Azure ecosystem.

Audience Profile

KQL for Azure Admins is a comprehensive IT training course designed for professionals looking to master KQL for efficient data management in Azure.

- Azure Administrators
- Data Engineers
- Cloud Solution Architects
- Security Analysts working with Microsoft Sentinel
- IT Professionals interested in analytics and data visualization within Azure
- Database Administrators looking to enhance their querying skills
- System Analysts and Developers responsible for monitoring and querying Azure resources
- Business Intelligence Professionals seeking to integrate Azure data with Power BI
- Technical Support Engineers involved in troubleshooting Azure environments
- DevOps Engineers who need to analyze and visualize data as part of CI/CD processes

Course Syllabus

Introduction to KQL

- Introduction to KQL commands
- Understanding KQL syntax
- Elements and operators

- Running KQL queries

Analyzing Query Results Using KQL

- Using the Summarize operator
- Filtering results with the Summarize operator
- Preparing data with the Summarize operator
- Creating visualizations with the Render operator

Building Multi-Table Statements Using KQL

- Using the Union operator
- Using the Join operator

Constructing KQL Statements for Microsoft Sentinel

- Understanding KQL language statement structure
- Using the Let statement
- Using the Search operator
- Using the Where operator
- Using the Extend operator
- Using the Order operator
- Using the Project operator

Writing Your First Query with KQL

- Understanding the basic structure of a KQL query
- Connecting to resources
- Returning a specific number of rows using the Take operator
- Selecting columns to return using the Project operator
- Filtering data using the Where operator
- Reordering returned data using the Sort operator

Exporting Data Using KQL

- Exporting to CSV files
- Exporting to Power BI