Microsoft Community Workshop

Azure Data Explorer (ADX) Onboarding

Duration: 1-4 days [Onsite/Remote] | **Focus Area:** Performance and Scalability | **Difficulty:** 300 - Advanced

Intended Audience

Developers, Architects, Data Scientists Interested in Azure Data Explorer Workloads

Overview

ADX Onboarding caters towards mix scopes/workloads as described below as a one-day workshop or up to four days.

ADX with Azure-Sentinel

- (1-day) Azure Data Explorer (ADX) is a big data analytics platform that is highly optimized for log and data analytics. Security logs are useful for identifying threats and tracing unauthorized attempts to access data. Security attacks can begin well before they're discovered. As a result, having access to long-term security logs is important. Querying long-term logs is critical for identifying the impact of threats and investigating the spread of illicit access attempts. This workshop will guide you how to implement ADX as long-term retention storage for Microsoft Sentinel security logs, which enables you to run cross-platform queries and visualize data across both ADX and Microsoft Sentinel.

ADX with IOT Analytics

- (1-day) Azure Data Explorer is a fast, fully managed data analytics service for real-time analysis on large volumes of data streaming from applications, websites, IoT devices, and more. Ask questions and iteratively explore data on the fly to improve products, enhance customer experiences, monitor devices, and boost operations. Quickly identify patterns, anomalies, and trends in your data. Explore new questions and get answers in minutes. Run as many queries as you need, thanks to the optimized cost structure. This workshop will bring you up to speed on creating world class I(I)oT solutions based on Azure Data Explorer. We'll cover topics around data representation in ADX, connections and visualization of data.

KQL in a Day

- (1-day) This is a 1-day workshop for Kusto right from basics of Kusto to Advanced (Level 300). Encompassing functions and datasets.

TSI migration to ADX

- (1/2-day) The Time Series Insights (TSI) service will no longer be supported after March 2025. Consider migrating existing TSI environments to alternative solutions as soon as possible. We look at the feature comparison with ADX and help execute migration steps.

Microsoft

Delivery Outline – Scope: ADX with Azure-Sentinel (1 day)

Module 1: Azure Data Explorer E2E Overview

- Introducing ADX
- How to choose a database
- Customer Case study

Module 2: ADX Architecture Overview

- What is ADX and how it works
- Major Components of ADX

Module 3: ADX Integration/Ingestion Patterns

- Streaming ingestion
- Batch Ingestion
- ADX Web UI One-Click (wizard)
- KQL, Cross Queries, Data Sharing

Module 4: Microsoft Sentinel overview

- What is Sentinel and how it works
- Sentinel log storage

Module 5: Microsoft Sentinel Data Ingestion

- Native data connectors
- Data Ingestion methods

Module 6: KQL basics for Sentinel

- Filter, Prepare and Analyze
- Visualize
- Advanced Topics
- Working with JSON and arrays
- Demos

Module 7: Sentinel Log Retention/Archival Options

- Parallel Data Ingestion
- Data Export to ADX (Automation)
- Managed Log Archive
- Demos

Module 8: Key Takeaways & Resources

- Key takeaways, related workshops
- Product Links and additional resources

Pre-requisites

Before attending this course, it is recommended that you meet the following criteria

- Lab Azure subscription will not be provided for the course
- Hands-on is optional, if attendee(s) would like to try demos with the instructor together, attendee(s) must have:
    - Powershell 7+ and Kusto CLI installed
    - Their own Azure subscription with sufficient permissions to provision resources, such as:
        - Resource Group
        - ADX Cluster and databases
        - Log Analytics workspace or Sentinel
        - Storage Account
        - EventHubs Namespace and EventHub
- Powershell basic knowledge
- KQL, JSON basic knowledge
- Basic concept of Azure Log Analytics, Sentinel, Azure Monitor

For more information

Contact your Microsoft Account Representative for further details.

Delivery Outline – scope: ADX with IOT Analytics (1 day)

Module 1: ADX Introduction & Overview

- Overview of the service
- ADX Architecture the Why/What/How
- Proven Technology & Customer Use-Cases
- Demos
- Knowledge check & Agenda

Module 2: ADX for IoT Analytics

- IoT essential + Feedback loop
- Reference Architecture
- More demos using Thermostat data and more.

Module 3: Hands-On Lab

- Full walkthrough of Hands-On Lab materials
- Execution of Lab steps throughout
- Help & encourage participants

Module 4: Azure Digital Twins (ADT)

- Introduction of ADT
- Next generation IoT solutions
- Integration with ADX

Module 5: KQL for IoT

- KQL in ADX for IoT Analytics
- Overview of KQL & Common usage for IoT
- Reinforce knowledge of queries from Hands-On Lab
- Incl. Materialized Views, External Tables, ADT Query, Python Unsupervised & Supervised ML.
- KQL Best Practices & Knowledge check

Module 6: ML & Time series for IoT

- Time series analysis
- Anomaly detection and forecasting
- Machine learning
- Language plugins (Python & R)

Module 7: Visuals

- Built-in Dashboards & Power BI

Module 8: Ops & Management

- Management (Cluster, Database & Data), BCDR
- Monitor & Troubleshoot

Module 9: Advanced

- Cmds, Policies, Cache
- API common usage (SDKs & Python)
- Optimize

Pre-requisites

Before attending this course, it is recommended that you meet the following criteria

- In order to execute the Hands-On Lab attendees **must have their own subscription** with access to create scripted resources. Lab Azure subscriptions will not be provided for the course.
- If attendee(s) has a Microsoft Account (**hotmail.com**, **live.com**, **outlook.com**), temporary access may be granted to workshop cluster to run queries.
- **Essentials:**
    - KQL from Scratch
    - Azure data exploring
    - How to start with Azure Data Explorer , (blog)
    - Advanced KQL , (blog)

Timeline

- Modules 1-3: ~3hrs (with lunch break)
- Module 4: 15 mins
- Modules 5-9: ~2 hr

For more information

Contact your Microsoft Account Representative for further details.

Delivery Outline – scope: KQL in a Day (1 day)

Module 1: Introduction to Kusto Query Language

- Entities and Data Types
- Essential Elements - basic aggregate functions
- Graph output using Visualization/ render commands
- KQL Tools
- Kusto Explorer
- CLI
- Demos

Module 2: Functions

- String Functions
- Parsing Functions
- Datetime Functions
- Mathematical functions
- Conversion Functions
- Window functions
- Demos

Module 3: Datasets

- Datatable
- Joins
- Union
- Let Statement
- Set Statement
- Batches
- Demos

Module 4: Advance Functions

- Pivot
- Basket
- Auto cluster
- Time Series Insights

Pre-requisites

Before attending this course, it is recommended that you meet the following criteria

- You understand that you are aware of Log Analytics
- Basic knowledge of the Microsoft Azure platform.
- Be familiar with maneuvering around Azure portal.
- In order to execute the Hands-On Lab, attendees **must have their own subscription**. Lab Azure subscriptions will not be provided for the course.

If you are new to these, here are a few references you can complete prior to class:

•Log Analytics
•Microsoft Azure

For more information

Contact your Microsoft Account Representative for further details.

Delivery Outline – scope: TSI to ADX migration (1/2 day)

Module 1: Why TSI to ADX migration?

- Explain the migration path, options, timelines. What is possible and what is not

Module 2: Understanding Azure Data Explorer

- Explain the differences between TSI and ADX. Highlight the "breaking" differences and how these will be handled

Module 3: Migrating from TSI to ADX

- Explain what actions customers need to take to complete the migration. Explain the key attention items. Explain the automation options available at each step

Module 4: Finalizing the migration

- Explain how long TSI and ADX need to run in parallel, how to plant the cutover, actions needed to cut over, user migration, updating DNS entries, etc.

Pre-requisites

Before attending this course, it is recommended that you meet the following criteria

- In order to execute the migration process attendees:
    - **must have their own subscription** with access to read TSI resources.
    - Access to create ADX resources
- Azure subscriptions will not be provided for the course.
- Basic knowledge of:
    - PowerShell, and Azure CLI

      or
    - Azure Data Factory
- **Essentials:**
    - Free online courses: Azure Data Explorer

For more information

Contact your Microsoft Account Representative for further details.