Design Specifications for Azure Data Explorer / Azure Data Factory / Event Hub



Long Term Retention: Enablement and Configuration

Prepared for

JFHQ-DODIN

8/11/2025

Version 1.0 Final

Prepared by

**MS Federal CyberEstate Collective**

**fedcyberestate@microsoft.com**

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Descriptions of other companies’ products in this document, if there are any, are provided only as a convenience to you. Any such references should not be considered endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2014 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision and Signoff Sheet  
Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 1/24/2025 | Nick OConnor | 0.1 | Initial Draft |
| 5/13/2025 | Nick OConnor | 1.0 | Final |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
| Evan Carrillo | 1.0 | Security Architect | 5/13/2025 |
|  |  |  |  |
|  |  |  |  |

[1 Executive Summary 4](#_Toc198119519)

[1.1 Solution Background 4](#_Toc198119520)

[2 Capacity Planning 5](#_Toc198119521)

[3 Automation to Configure ADX LTR 6](#_Toc198119522)

[3.1 File Overview 6](#_Toc198119523)

[3.2 Deploying the Infrastructure ARM Template 6](#_Toc198119524)

[3.3 Deploying the Data Export ARM Template 7](#_Toc198119525)

[4 Manual Creation of ADX LTR 8](#_Toc198119526)

[4.1 Event Hub 8](#_Toc198119527)

[4.1.1 Create Event Hub Namespace 8](#_Toc198119528)

[4.2 Create Event Hubs 9](#_Toc198119529)

[4.3 Azure Data Explorer 10](#_Toc198119530)

[4.3.1 Create ADX Cluster 10](#_Toc198119531)

[4.3.2 Create ADX Database 14](#_Toc198119532)

[4.3.3 Configure ADX database tables 15](#_Toc198119533)

[4.3.4 Configure ADX database data connections 16](#_Toc198119534)

[4.3.5 Ingest Data into ADX from Sentinel 18](#_Toc198119535)

[5 Configure Permissions for JFHQ-DODIN 21](#_Toc198119536)

[5.1 Grant Cross-Tenant permissions 21](#_Toc198119537)

[5.2 Grant Read-Only Permissions to the Database 21](#_Toc198119538)

[6 Azure Data Factory 23](#_Toc198119539)

[6.1 Create ADF 23](#_Toc198119540)

[6.2 Configure ADF 24](#_Toc198119541)

[6.3 Ingest Data into ADX from ADF 26](#_Toc198119542)

[Tables 32](#_Toc198119543)

[Table Naming for Event Hubs/ADX database data connections 32](#_Toc198119544)

[Appendix A. DAO Consolidated Check List 34](#_Toc198119545)

1. Executive Summary

This document’s purpose is to aid DODIN Areas of Operations (DAOs) in the configuration and enablement of a long-term data retention solution through Microsoft Sentinel, Event Hubs, Azure Data Explorer (ADX), and Azure Data Factory (ADF). This effort will rapidly improve the visibility and capabilities of JFHQ-DODIN and USCYBERCOM to make informed decisions of Department of Defense (DoD) risk, exposure, threats and more.

* 1. Solution Background

Azure Data Explorer (ADX) delivers intelligent data analytics and insights across the enterprise. ADX provides a bird's-eye view across the enterprise, alleviating the stress of managing large volumes of data and enabling quick decision-making.

Azure Data Factory (ADF) enables multi-tenant data integration with scalability, higher automation, and enhanced governance across resources. Customers maintain control over who has access to their data, which resources they can access, and what actions can be taken.

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response

Through the Azure capabilities of Multi-Tenant Organization (MTO), ADX, ADF, Lighthouse, and Microsoft Sentinel, JFHQ-DODIN can create a unified data and security approach, enabling a Common Operating Picture (COP) across multiple departments and agencies. This integration maximizes the effectiveness of ADX's data analytics capabilities and Sentinel's security features, ensuring a robust and unified visibility into evolving data and cyber threats across a distributed and diverse environment.

1. Capacity Planning

Collect the following information to use throughout the creation

**Determining data ingest size per day**

Use the following KQL from within your Log Analytics Workspace to determine an appropriate number for the *Ingest TB Per Day*

union \*

| where TimeGenerated > ago(14d)

| summarize TotalIngestedTB = sum(\_BilledSize) / 1e12 by bin(TimeGenerated, 1d)

| summarize max(TotalIngestedTB)

**Event Hubs Namespace Processing Units**

Processing Units: 2 (recommended)

Reference link to optimize for your environment [Scalability - Azure Event Hubs - Azure Event Hubs | Microsoft Learn](https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-scalability#processing-units)

**Azure Data Explorer Cluster Optimized autoscale**

Minimum instance count: 2 (recommended)

Maximum instance count: 10 (recommended)

Reference link to optimize for your environment - [**Manage cluster horizontal scaling (scale out) to match demand in Azure Data Explorer - Azure Data Explorer | Microsoft Learn**](https://learn.microsoft.com/en-us/azure/data-explorer/manage-cluster-horizontal-scaling?WT.mc_id=Portal-Microsoft_Azure_Kusto#optimized-autoscale-preview)

Example table of planning results

|  |  |
| --- | --- |
| **Resource** | **Example Value** |
| ADX Minimum instance count | 2 |
| ADX Maximum instance count | 10 |
| Event Hubs Namespace Processing Units | 2 |

1. Automation to Configure ADX LTR

This solution is a setup guide to deploy and configure an Azure Data Explorer (ADX) cluster and database for the purpose of low-cost, interactive retention of Azure log data.

The end-state of this deployment will configure the following:

* Azure Event Hub Namespace (Premium)
* An Azure Event Hub per ingest table
* Azure Data Explorer (ADX) Cluster (Storage Optimized, Medium)
* ADX Database
* An ADX table, ingestion mapping, and parsing function for every source type
* An ADX data connection for every source type
  1. File Overview
* **kusto.kql**: A reference file of the Kusto script being run inline via ARM. This is here as the source of truth to have an easier editing view than directly in ARM (which doesn’t support multiline strings via Azure Portal)
* **minify-kusto.py**: Python script to take the human-readable **kusto.kql** and output it to **kusto.min.kql** for use in ARM.

Note: you must manually take the content and put it in the ARM.

* **script-test-arm.json**: A testbed to test out the minified Kusto script without redeploying the entire solution every time. NOT INTENDED FOR PRODUCTION USE.
* **script-export-arm.json**: An ARM template to run after infrastructure deployment to configure your Log Analytics Workspace Data Export for the applicable tables
* **setup-infrastructure-arm.json**: The primary ARM template to deploy the Cluster, Event Hub Namespace, and associated resources/configurations.
  1. Deploying the Infrastructure ARM Template

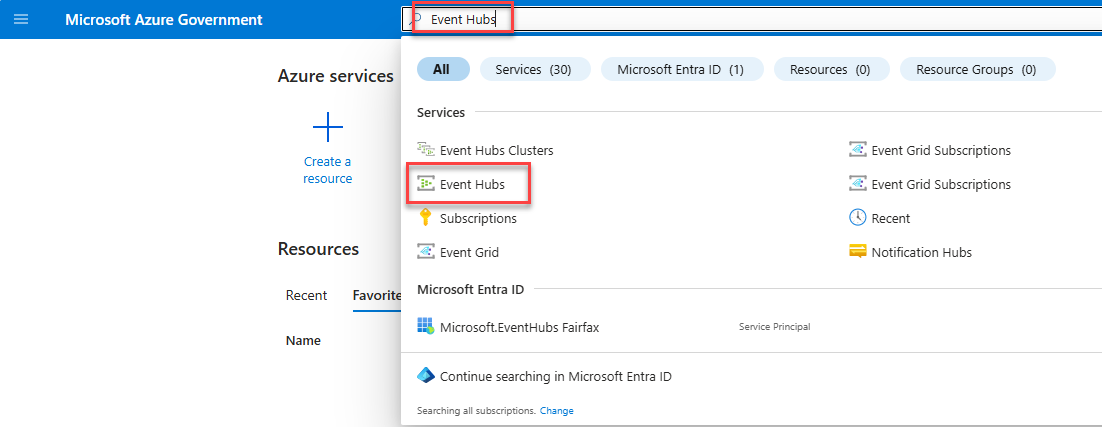
Infrastructure is deployed as code with the included ARM template. Minor manual steps may be required after deployment

To deploy the ARM template via the Azure Portal:

1. Log into the Azure Portal
2. Ensure your user has at least *Contributor* and *User Access Administrator* roles on the subscription where this solution is to be deployed
3. Search for and open the *Deploy a custom template* service
4. From the *Select a template* tab, select the *Build your own template in the editor* option
5. Click the *Load File* button, navigate to the setup-infrastructure-arm.json file, and click *Open*
6. From the *Edit template* tab, click *Save*
7. From the *Basics* tab, configure the following parameters, then click *Review + create*
   1. **Resource group**: Select an existing or create a new resource group for the cluster and event hub. This does not have to be the same resource group as your Sentinel/Log Analytics Workspace instance. Must be one of USGov Virginia, USGov Arizona, or USGov Texas. It is highly recommended to deploy this to the same region as your Log Analytics Workspace
   2. **Ingest TB Per Day**: Enter how many TBs of data your Log Analytics workspace currently ingests per day. This is used to size Event Hub appropriately. Minimum allowed value is 1.
   3. **Cluster Name**: Enter a desired cluster name
   4. **Database Name**: Enter a desired database name
   5. **Event Hub Namespace Name**: Enter a desired Event Hub namespace name
8. Wait for the infrastructure to be deployed successfully. This may take up to 30 minutes
   1. Deploying the Data Export ARM Template
9. Log into the Azure Portal
10. Ensure your user has at least *Contributor* role on the Log Analytics Workspace to deploy the data export rule to
11. Search for and open the *Deploy a custom template* service
12. From the *Select a template* tab, select the *Build your own template in the editor* option
13. Click the *Load File* button, navigate to the setup-export-arm.json file, and click *Open*
14. From the *Edit template* tab, click *Save*
15. From the *Basics* tab, configure the following parameters, then click *Review + create*
    1. **Resource group**: IMPORTANT: Select the resource group corresponding to your Sentinel/Log Analytics Workspace instance
    2. **Log Analytics Workspace Name**: Enter the name of your Log Analytics Workspace
    3. **Event Hub Resource ID**: Enter the resource ID of the Event Hub Namespace created in the previous step. This can be found in the **Properties** section of the Event Hub Namespace
    4. **Export Rule Name**: If desired, change the default value
    5. **Enable Data Export**: If you would like to configure the export rule without turning the rule on yet, set this to false
16. Manual Creation of ADX LTR
    1. Event Hub
       1. Create Event Hub Namespace

Within Azure Portal search bar, search “Event Hubs” and select the Service link to

Event Hubs



Click ‘Create’

Under Basics section populate required fields.

**Subscription:** Select the subscription where your Log Analytics Workspace exists

**Resource group:** <DAO>-M2131LTR-RG

**NOTE:** Select an existing or create a new resource group. This does not have to be the same resource group as your Sentinel/Log Analytics Workspace instance.

**Namespace name:** <DAO>-M2131LTR-EVNS

**Location:** It is recommended to deploy this to the same region as your Log Analytics Workspace.

**Pricing Tier:** Premium

**Processing Units:** 2 (refer to capacity planning section)

Accept defaults for the other sections

When finished click on Review + create button and then Create button to complete.

A screenshot of a computer

AI-generated content may be incorrect.

* 1. Create Event Hubs

Navigate to the newly created Event Hub Namespace

On the left navigation expand Entities and Click on Event Hubs

Click + Event Hub to start creating

In the Basics section populate the following

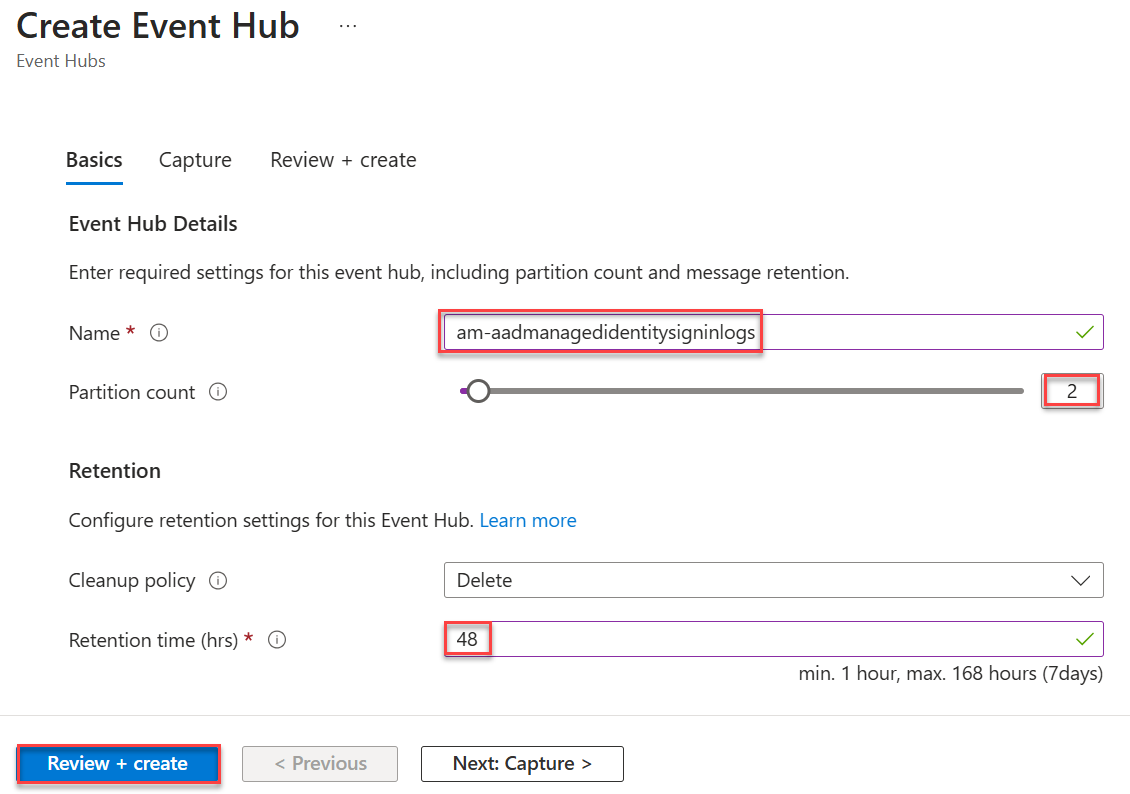
**Name (reference** [**Table 1**](#_Table_1_–)**):** am-aadmanagedidentitysignlogs

**Partition count:** 2

**Cleanup policy:** Delete

**Retention time (hrs):** 48

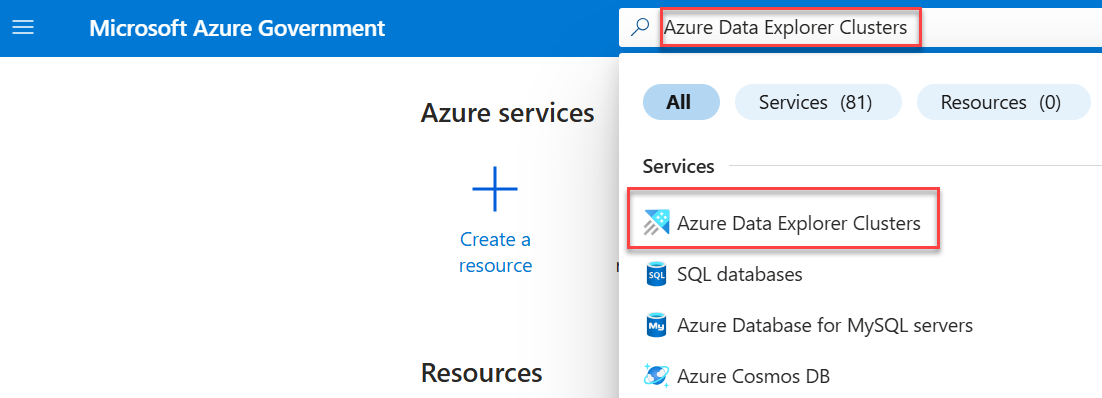
click Review + create button when finished and click on Create button to complete.



**Repeat previous steps:** Pull the name from [Table 1](#_Table_1_–) and repeat previous steps for each name

* 1. Azure Data Explorer
     1. Create ADX Cluster

Within Azure Portal search bar, search “Azure Data Explorer Clusters” and select the Service link to Azure Data Explorer Clusters



Select ‘Create’

Under Basics section populate required fields.

1. **Subscription:** Select the subscription where the previous resources were created
2. **Resource Group:** Select the resource group where the previous resources were created
3. **Cluster name:** <dao>-m2131ltr-dec

**Note:** Cluster name must be 22 characters or less.

[Naming rules and restrictions for Azure resources - Azure Resource Manager | Microsoft Learn](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftkusto)

1. **Region:** Select the region where your other resources exist
2. **Workload:** Storage Optimize
3. **Size:** Medium (8 cores)
4. **Compute specifications:** Click *Select other* and select Standard\_E8as\_v4+1TB\_PS and apply

A screenshot of a computer

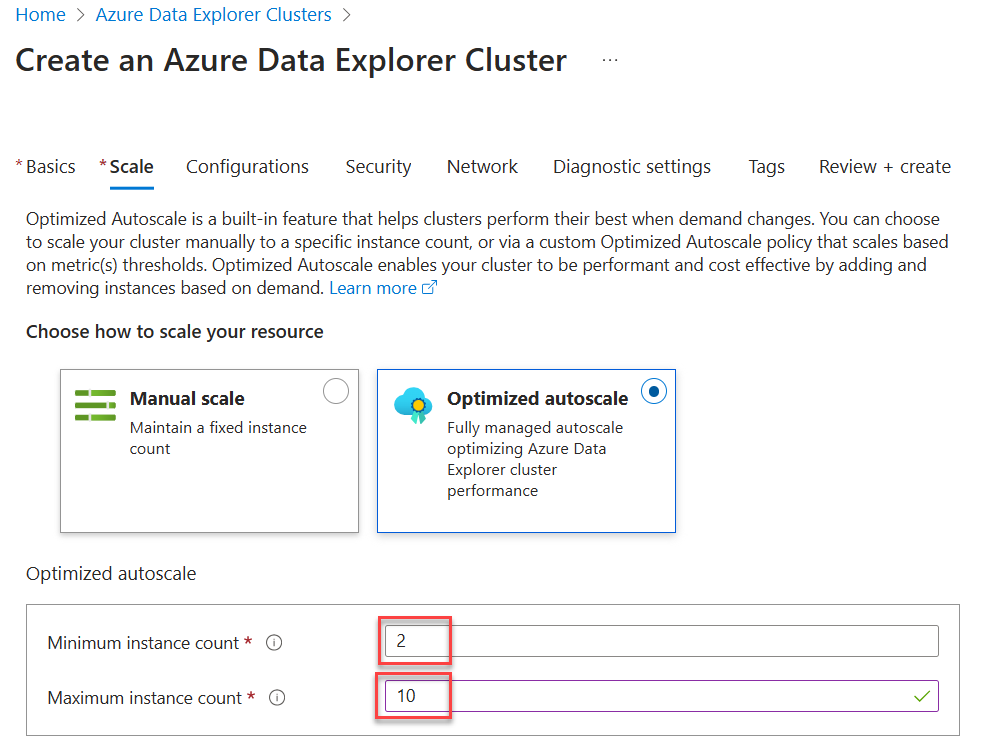
AI-generated content may be incorrect.

Click Next: Scale >

**Choose how to scale your resource:** Optimized autoscale

**Minimum instance count:** 2 (refer to capacity planning section)

**Maximum instance count:** 10 (refer to capacity planning section)



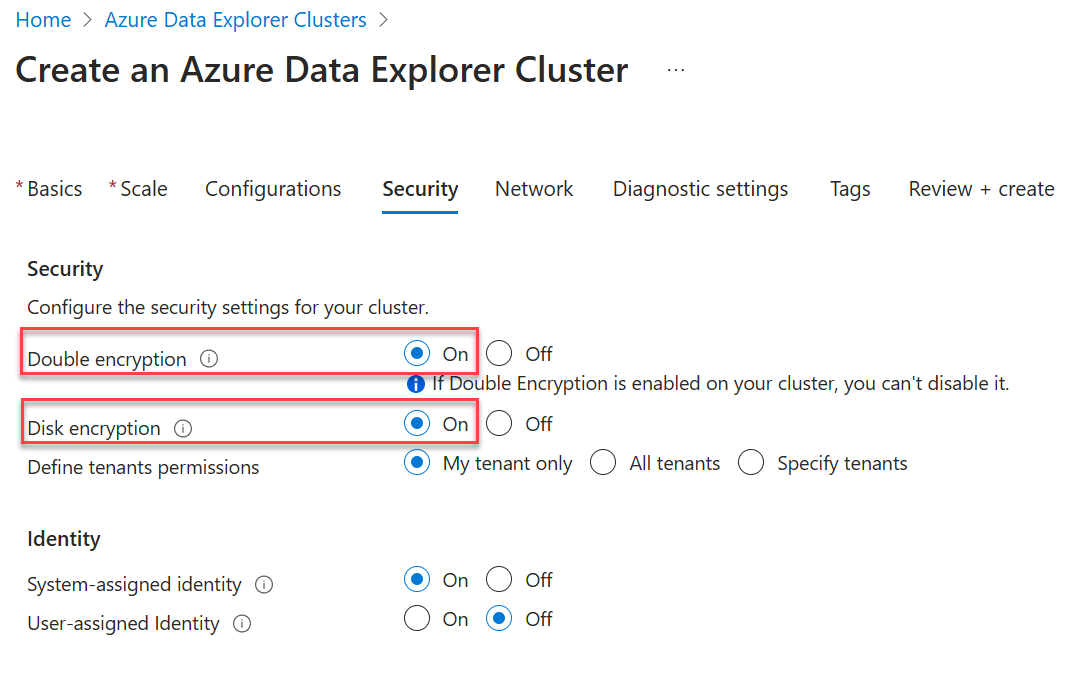
Click Next: Configurations >

Keep Defaults on Configurations section

Click Next: Security >

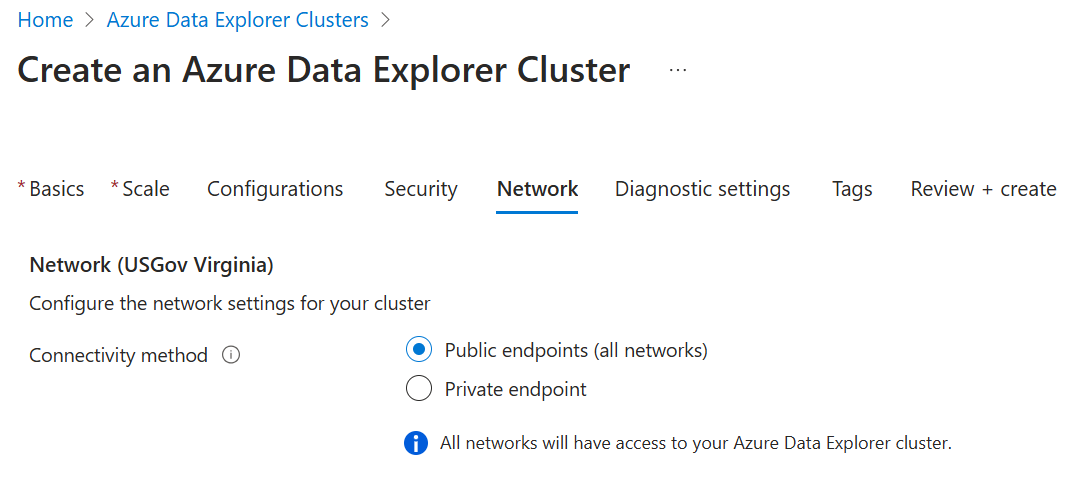
**Double encryption:** On

**Disk encryption:** On



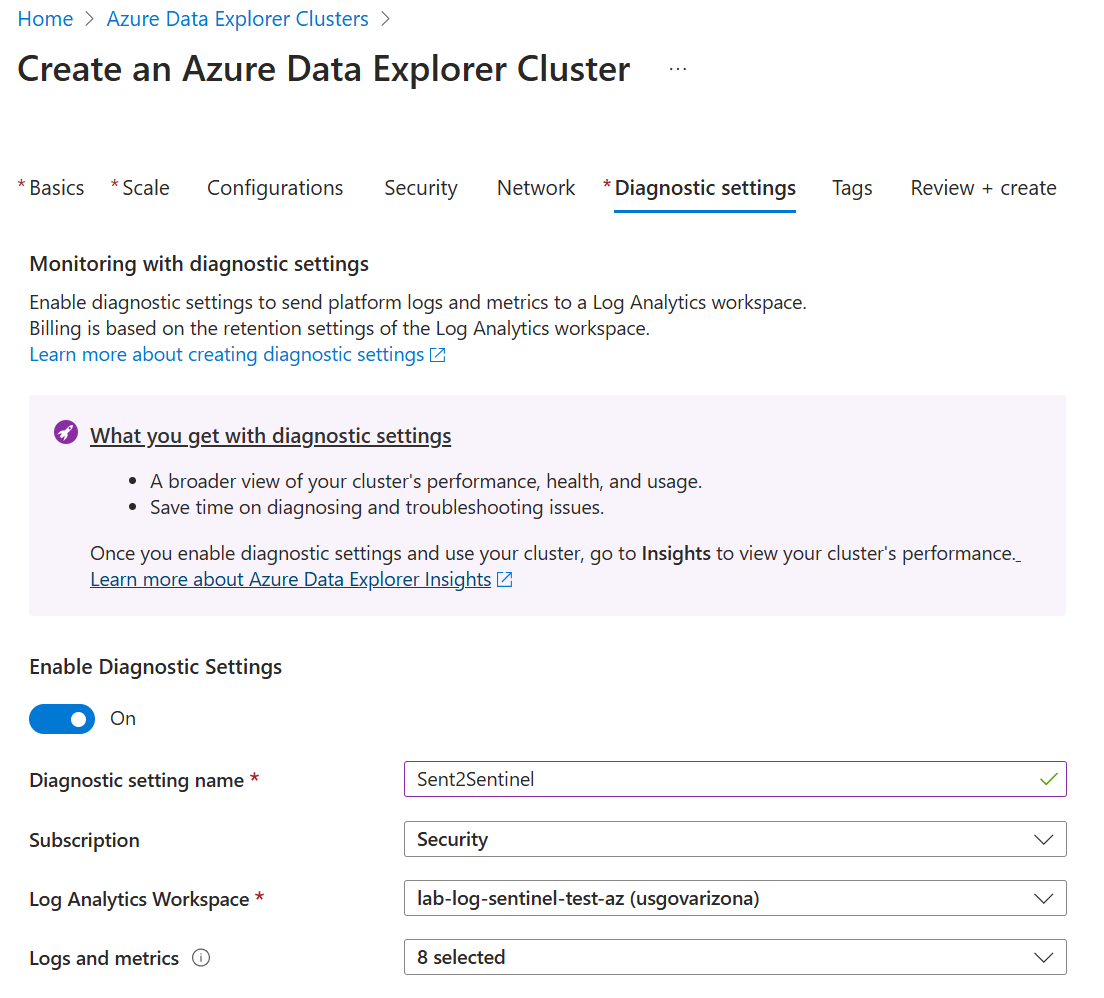
Click Next: Network >

**Connectivity method:** Public endpoints



Click Next: Diagnostics settings >

Optionally you can Enable Diagnostics Settings and send logs and metrics to your Sentinel Log Analytics Workspace



Click Review + Create

* + 1. Create ADX Database

Browse the newly created Azure Data Explorer Cluster and click on the Databases blade and Click Add Database

A screenshot of a computer

AI-generated content may be incorrect.

Database name: <DAO>-M2131LTR-DEDB

Retention period: 365 (Reference [M-21-31](https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) for retention period)

Cache period: 0

click Create

A screenshot of a computer

AI-generated content may be incorrect.

* + 1. Configure ADX database tables

This section includes table creation, schema, and mapping

Browse to the newly created Azure Data Explorer database

1. Click on Query
2. Expand the cluster name and select the database
3. Open the **kusto.kql** file and copy all and paste into the right side
4. Then select each line and click run

A screenshot of a computer

AI-generated content may be incorrect.

Click refresh to see all the new tables

A screenshot of a computer

AI-generated content may be incorrect.

* + 1. Configure ADX database data connections

Click on the Data Connections blade

1. Click on Add data connection and click Event Hub
2. **Data Connection name (reference** [**Table** **1**](#_Table_1_–)**):** am-aadmanagedidentitysigninlogs
3. **Subscription:** Select the subscription where the previous resources were created
4. **Event Hub namespace:** Select the Event Hub namespace previously created
5. **Event Hub:** am-aadmanagedidentitysigninlogs
6. **Consumer group:** $Default
7. **Table name (reference** [**Table 1**](#_Table_1_–)**):** xAADManagedIdentitySignInLogsRaw
8. **Data format:** JSON
9. **Mapping name (reference** [**Table 1**](#_Table_1_–)**):** xAADManagedIdentitySignInLogsRawMapping
10. Click create

A screenshot of a computer

AI-generated content may be incorrect.

**Repeat previous steps:** Repeat previous steps for everything referenced in [Table 1](#_Table_1_–).

* + 1. Ingest Data into ADX from Sentinel

Within Azure Portal search bar, search “Log Analytics workspaces” and select the Service link to Log Analytics workspace

A screenshot of a computer

Description automatically generated

Click on your workspace

Click on the Data export blade

Click on New export rule

A screenshot of a computer

Description automatically generated

Enter the rule name: ExportToCyberLogADX

Click Next to Source section

A screenshot of a computer

Description automatically generated

On the Source section select all the tables to export Reference [Table 1](#_Table_1_–)

A screenshot of a computer

Description automatically generated

Click Next to Destination section

**Destination type:** Event Hub

**Subscription:** Select the subscription where the previous resources were created

**Event Hub Namespace:** select namespace created

**Event Hub Name:** (Create in selected namespace)

A screenshot of a computer

AI-generated content may be incorrect.

Click Create

1. Configure Permissions for JFHQ-DODIN
   1. Grant Cross-Tenant permissions

Select the Azure Data Explorer Cluster

1. Click Security blade
2. Select specify tenants
3. Click Add tenant
4. Select Manually via tenant ID
5. Enter Tenant ID: *3a434b90-d645-4a69-8d90-502e15705e32*
6. Click Add

Click Save

A screenshot of a computer

AI-generated content may be incorrect.

* 1. Grant Read-Only Permissions to the Database

The following KQL grants viewer access to your database from JFHQ-DODIN. Run this query on your ADX cluster, replacing <your-database> with the appropriate database name you defined in the initial deployment

Command:

.add database <[your-database]> viewers ('aadGroup=30ca755b-04ec-44eb-b856-97f83ffe686d;3a434b90-d645-4a69-8d90-502e15705e32') 'Viewer permission for DODIN Logs1 tenant'

Example:

.add database [DAO-M2131LTR-DEDB] viewers ('aadGroup=30ca755b-04ec-44eb-b856-97f83ffe686d;3a434b90-d645-4a69-8d90-502e15705e32') 'Viewer permission for DODIN Logs1 tenant'

Verify by clicking on the Permissions blade for the database and see the GFUD XDR MTO Reader added-

A screenshot of a computer

AI-generated content may be incorrect.

1. Azure Data Factory
   1. Create ADF

Within Azure Portal search bar, search “Data factories” and select the Service link to Data factories

A screenshot of a computer

AI-generated content may be incorrect.

Click Create data factory

Populate the required fields under the Basics section and click on *Review + Create* and click *Create*

**Subscription:** Select the subscription where the previous resources were created

**Resource Group:** <DAO>-M2131LTR-ADF-RG

Region: Select the region where the previous resources were created

Name: <DAO>-M2131LTR-ADF

A screenshot of a computer

AI-generated content may be incorrect.

* 1. Configure ADF

Grant permission of the data factory system assigned managed identity to your ADX database.

1. Browse to the Azure Data Explorer Cluster created earlier and click on it.
2. Next expand Data > Databases and click on the database
3. Click on the Permissions blade and click Add and then click Admin

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on Enterprise applications to limit your search
2. Type the name of your ADF
3. Select your ADF
4. Click on Select

A screenshot of a computer

AI-generated content may be incorrect.

You will see the newly assigned permissions

A screenshot of a computer

AI-generated content may be incorrect.

Run this script to assign read permissions of the WindowsDefenderATP tables to the data factory system assigned managed identity

Update $ADF variable before running

$ADF = "<DAO>-M2131LTR-ADF" # Change this before running script to your DAO specific name

Connect-MgGraph -Scopes "Directory.Read.All", "Application.ReadWrite.All" -Environment USGov

$managedIdentity = $null

Write-Host "Looking for Managed Identity with default prefix names of the Data Factory..."

$managedIdentity = Get-MgServicePrincipal -Filter "displayName eq '$ADF'"

if ($null -eq $managedIdentity) {

   $managedIdentity = Read-Host -Prompt "Enter ObjectId of Managed Identity (from Data Factory):"

}

# The app ID of the Microsoft Graph API where we want to assign the permissions

$appId = "fc780465-2017-40d4-a0c5-307022471b92" # AppId for WindowsDefenderATP

$permissionsToAdd = @("Vulnerability.Read.All","Software.Read.All")

$app = Get-MgServicePrincipal -Filter "appId eq '$appId'"

    foreach ($permission in $permissionsToAdd) {

        Write-Host $permission

        $role = $app.AppRoles | Where-Object Value -Like $permission | Select-Object -First 1

        $params = @{

            principalId = $managedIdentity.Id

            resourceId = $app.Id

            appRoleId = $role.Id

        }

        New-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $managedIdentity.Id -BodyParameter $params

    }

* Verify Permissions were granted
* Browse to Microsoft Entra ID > Enterprise Applications > All Applications
* Clear any filters and search for your managed identity, captured it last step as $ADF
* Click on the managed identity

A screenshot of a computer

AI-generated content may be incorrect.

* Click on the Permissions blade and review the two permissions granted

A screenshot of a computer

AI-generated content may be incorrect.

* 1. Ingest Data into ADX from ADF

Run script to configure build out the Data Factory

* Extract zip to a working directory. This will be referenced later
* Run final.ps1
* Type the Azure environment you want to connect to
* [Login to Azure] – follow steps for device login in your web browser

A close-up of a computer code

AI-generated content may be incorrect.

* When complete, the browser will return A screenshot of a computer

  AI-generated content may be incorrect.
* Select a tenant and subscription (type a number or Enter to accept default) – This is the subscription that your Data factory was created in earlier

A screenshot of a computer screen

AI-generated content may be incorrect.

* Enter the path to the LinkedServices folder:
  + Example: C:\Repos\Working\tvm\linked
* Enter the path to the DataSets folder:
  + Example: C:\Repos\Working\tvm\dataset
* Enter the path to the Pipelines folder:
  + Example: C:\Repos\Working\tvm\pipeline
* Enter the path to the Triggers folder:
  + Example: C:\Repos\Working\tvm\trigger
* Enter the Resource Group Name:
  + Example: <DAO>-M2131LTR-ADF-RG
  + Use the name of the Resource group that was created earlier
* Enter the Data Factory Name:
  + Example: <DAO>-M2131LTR-ADF
  + Use the name of the Data Factory that was created earlier
* Once everything is entered you will see it start the deployment

A screenshot of a computer

AI-generated content may be incorrect.

Updating connections from deployment

* Browse to your ADX cluster and capture the URI. At the end of the URI, you can click on copy to clipboard and keep this for a later step.

A screenshot of a computer

AI-generated content may be incorrect.

* Click on the Databases blade and capture your database name

A screenshot of a computer

AI-generated content may be incorrect.

* Browse to your Data Factory and click on Launch Studio

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on Manage
2. Click on Linked services
3. Click on ADX\_LinkedService
4. Enter your ADX URI
   * Example: https://<DAO>-M2131LTR-dec.usgovarizona.kusto.usgovcloudapi.net
5. Enter your ADX Database name
   * Example: <DAO>-M2131LTR-DEDB

A screenshot of a computer

AI-generated content may be incorrect.

Click Save when finished

Click on Publish all to save configuration

A screenshot of a computer

AI-generated content may be incorrect.

Manually verify the pipeline for validation that the solution works

1. Click on Author
2. Expand out Pipelines and click on ETL\_TVM\_ADX
3. Click on Debug
4. Review status to ensure it Succeeded

A screenshot of a computer

AI-generated content may be incorrect.

Verify ADX table results by accessing the ADX database and running KQL on a table.

A screenshot of a computer

AI-generated content may be incorrect.

Tables

## Table Naming for Event Hubs/ADX database data connections

|  |  |  |
| --- | --- | --- |
| **Event Hub/Data Connection Name** | **Table name** | **Mapping name** |
| am-aadmanagedidentitysigninlogs | xAADManagedIdentitySignInLogsRaw | xAADManagedIdentitySignInLogsRawMapping |
| am-aadnoninteractiveusersigninlogs | xAADNonInteractiveUserSignInLogsRaw | xAADNonInteractiveUserSignInLogsRawMapping |
| am-aadprovisioninglogs | xAADProvisioningLogsRaw | xAADProvisioningLogsRawMapping |
| am-aadriskyserviceprincipals | xAADRiskyServicePrincipalsRaw | xAADRiskyServicePrincipalsRawMapping |
| am-aadriskyusers | xAADRiskyUsersRaw | xAADRiskyUsersRawMapping |
| am-aadserviceprincipalriskevents | xAADServicePrincipalRiskEventsRaw | xAADServicePrincipalRiskEventsRawMapping |
| am-aadserviceprincipalsigninlogs | xAADServicePrincipalSignInLogsRaw | xAADServicePrincipalSignInLogsRawMapping |
| am-aaduserriskevents | xAADUserRiskEventsRaw | xAADUserRiskEventsRawMapping |
| am-adfssigninlogs | xADFSSignInLogsRaw | xADFSSignInLogsRawMapping |
| am-alertevidence | xAlertEvidenceRaw | xAlertEvidenceRawMapping |
| am-alertinfo | xAlertInfoRaw | xAlertInfoRawMapping |
| am-auditlogs | xAuditLogsRaw | xAuditLogsRawMapping |
| Am-azureactivity | xAzureActivityRaw | xAzureActivityRawMapping |
| am-cloudappevents | xCloudAppEventsRaw | xCloudAppEventsRawMapping |
| am-behavioranalytics | xBehaviorAnalyticsRaw | xBehaviorAnalyticsRawMapping |
| am-deviceevents | xDeviceEventsRaw | xDeviceEventsRawMapping |
| am-devicefilecertificateinfo | xDeviceFileCertificateInfoRaw | xDeviceFileCertificateInfoRawMapping |
| am-devicefileevents | xDeviceFileEventsRaw | xDeviceFileEventsRawMapping |
| am-deviceimageloadevents | xDeviceImageLoadEventsRaw | xDeviceImageLoadEventsRawMapping |
| am-deviceinfo | xDeviceInfoRaw | xDeviceInfoRawMapping |
| am-devicelogonevents | xDeviceLogonEventsRaw | xDeviceLogonEventsRawMapping |
| am-devicenetworkevents | xDeviceNetworkEventsRaw | xDeviceNetworkEventsRawMapping |
| am-devicenetworkinfo | xDeviceNetworkInfoRaw | xDeviceNetworkInfoRawMapping |
| am-deviceprocessevents | xDeviceProcessEventsRaw | xDeviceProcessEventsRawMapping |
| am-deviceregistryevents | xDeviceRegistryEventsRaw | xDeviceRegistryEventsRawMapping |
| am-emailattachmentinfo | xEmailAttachmentInfoRaw | xEmailAttachmentInfoRawMapping |
| am-emailevents | xEmailEventsRaw | xEmailEventsRawMapping |
| am-emailpostdeliveryevents | xEmailPostDeliveryEventsRaw | xEmailPostDeliveryEventsRawMapping |
| am-emailurlinfo | xEmailUrlInfoRaw | xEmailUrlInfoRawMapping |
| am-identitydirectoryevents | xIdentityDirectoryEventsRaw | xIdentityDirectoryEventsRawMapping |
| am-identitylogonevents | xIdentityLogonEventsRaw | xIdentityLogonEventsRawMapping |
| am-identityqueryevents | xIdentityQueryEventsRaw | xIdentityQueryEventsRawMapping |
| am-intunedevices | xIntuneAuditLogsRaw | xIntuneAuditLogsRawMapping |
| am-intuneauditlogs | xIntuneDeviceComplianceOrgRaw | xIntuneDeviceComplianceOrgRawMapping |
| am-intunedevicecomplianceorg | xIntuneDevicesRaw | xIntuneDevicesRawMapping |
| am-intuneoperationallogs | xIntuneOperationalLogsRaw | xIntuneOperationalLogsRawMapping |
| am-microsoftgraphactivitylogs | xMicrosoftGraphActivityLogsRaw | xMicrosoftGraphActivityLogsRawMapping |
| am-officeactivity | xOfficeActivityRaw | xOfficeActivityRawMapping |
| am-securityalert | xSecurityAlertRaw | xSecurityAlertRawMapping |
| **Event Hub/Data Connection Name** | **Table name** | **Mapping name** |
| am-securityincident | xSecurityIncidentRaw | xSecurityIncidentRawMapping |
| am-sentinelhealth | xSentinelHealthRaw | xSentinelHealthRawMapping |
| am-signinlogs | xSigninLogsRaw | xSigninLogsRawMapping |
| am-urlclickevents | xUrlClickEventsRaw | xUrlClickEventsRawMapping |

Appendix A. DAO Consolidated Check List

|  |  |
| --- | --- |
| Action Item | Descriptions |
| Configure ADX | Configure Azure Data Explorer and accompanying pieces |
| Configure ADF | Configure Azure Data Factory to Ingest TVM Tables to ADX |
| Ingest Data into ADX | Ingest tables into ADX for Long Term Retention / M-21-31 Compliance |
| Configure DoDIN Permission | Grant DoDIN Tenant/Lighthouse Read-Only Permissions |