Azure Logs Integration

Introduction

This document shows information related to Azure Active Directory Integration.
The Azure Logs integration retrieves different types of log data from Azure.

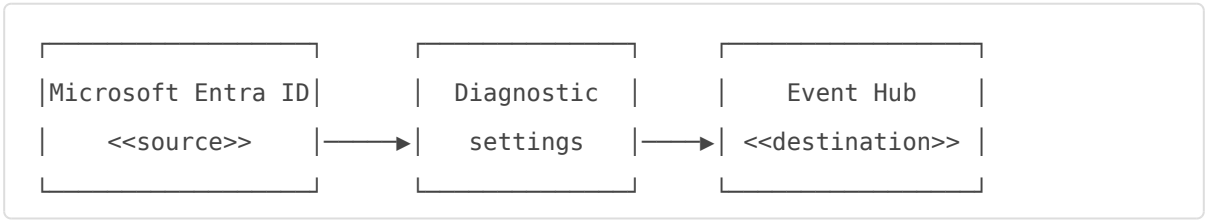
Assumptions

The procedures described in the **Requirements** section assumes that a Log Collector has already been setup.

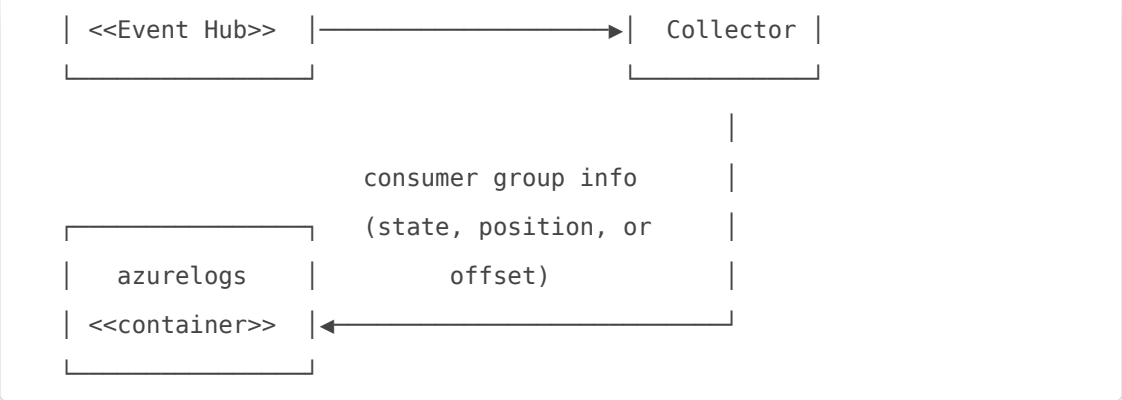
Requirements

Main Setup

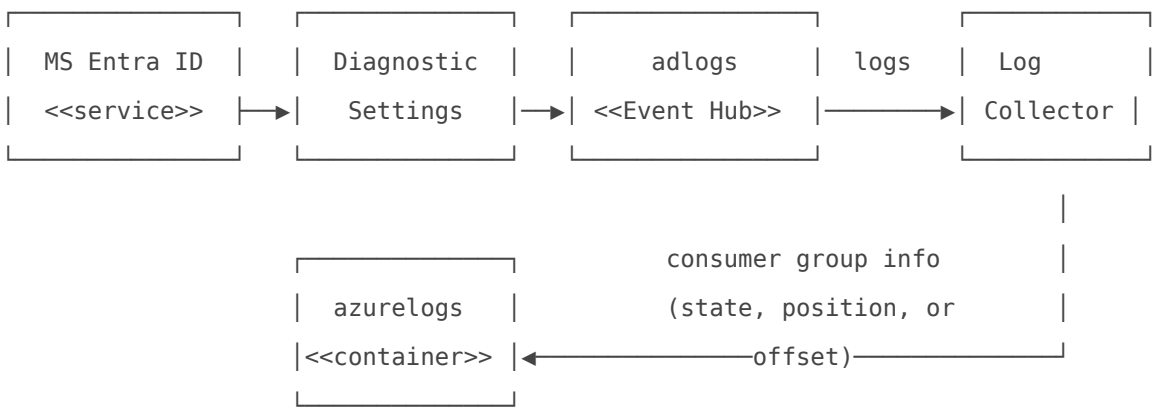
- One or more **event hub** to store in-flight logs exported by Azure services and make them available to the Log Collector
  - Example:
  - 

- One or more **diagnostic setting** to export logs from Azure services to Event Hubs
  - Example:
  - 

- One **Storage Account Container** to store information about logs consumed by the Log Collector
  - Example:
  - 



This is the final diagram of the a setup for collecting Activity logs from the Azure Monitor service.



If the integration is running behind a firewall, please proceed here.

Here are several requirements before using the integration since the logs will be read from azure event hubs.

1. **The logs have to be exported first to the event hub.**
   • Create an event hub using Azure portal.
   • More information can be found on: https://learn.microsoft.com/en-us/azure/event-hubs/event-hubscreate.
2. **To export activity logs to event hubs users can follow the steps here.**
   • Legacy collection methods
   • More information can be found on: https://learn.microsoft.com/en-us/azure/azuremonitor/essentials/activity-log?tabs=powershell#legacy-collectionmethods
3. **To export audit and sign-in logs to event hubs users can follow the steps here.**
   • Stream Azure Active Directory logs
   • More information can be found on: https://learn.microsoft.com/en-us/azure/active-directory/reportsmonitoring/tutorial-azure-monitor-stream-logs-to-event-hub

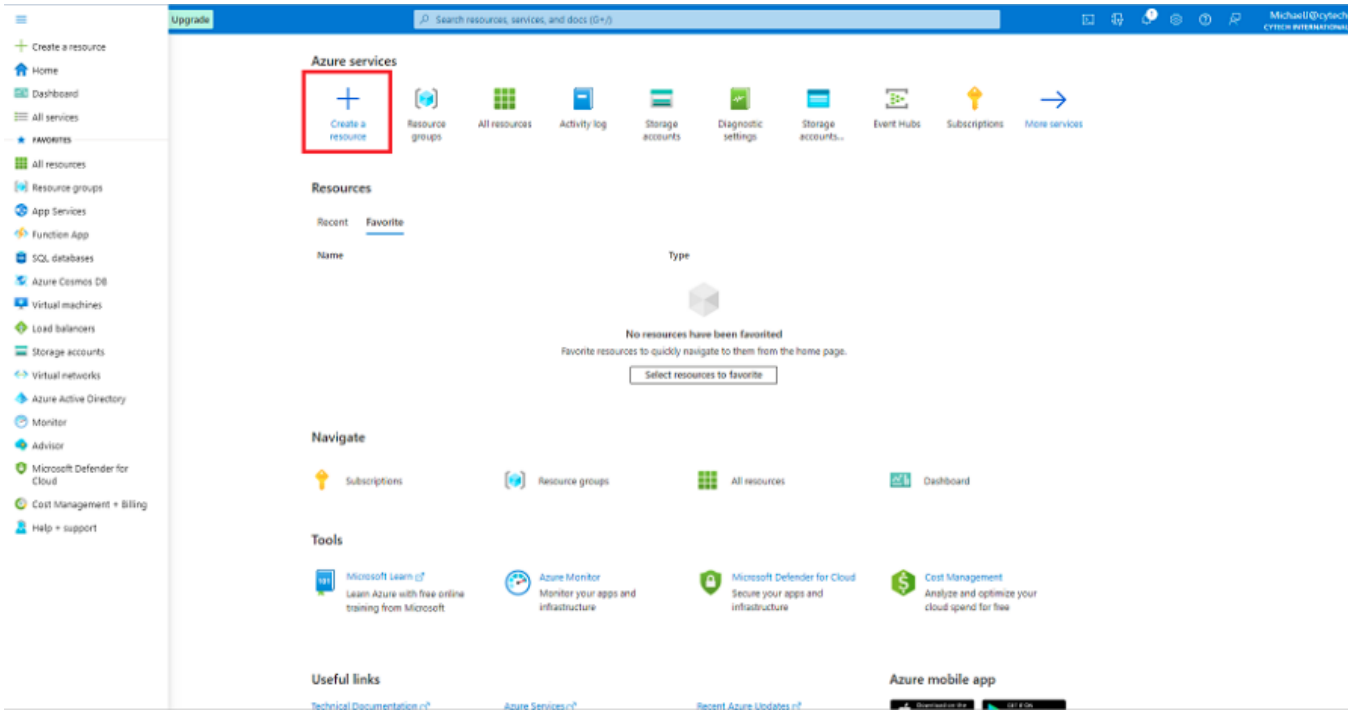
---

Azure Active Directory Integration Procedures

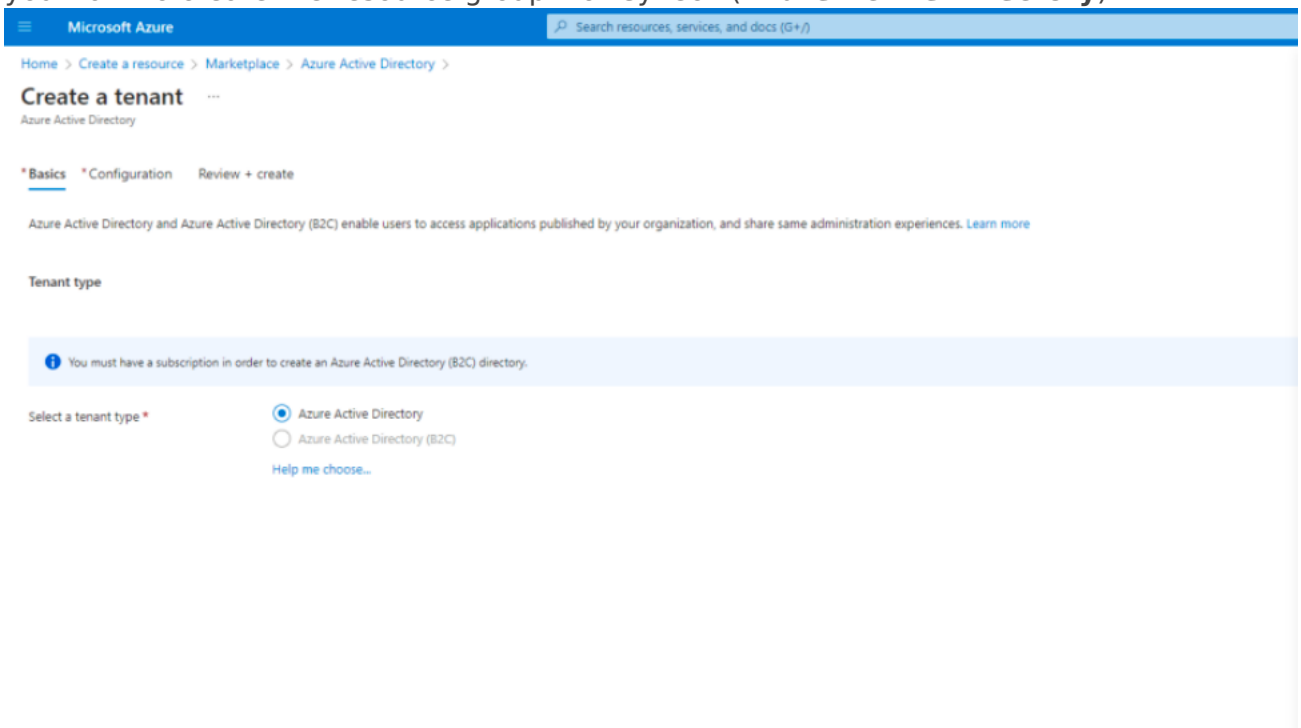
Create a Resource Group

A resource group is a logical collection of Azure resources. All resources are deployed and managed in a resource group. To create a resource group:

1. Sign in to the Azure portal.
2. In the left navigation, select R**esource groups**, and then select **Create a resource**.

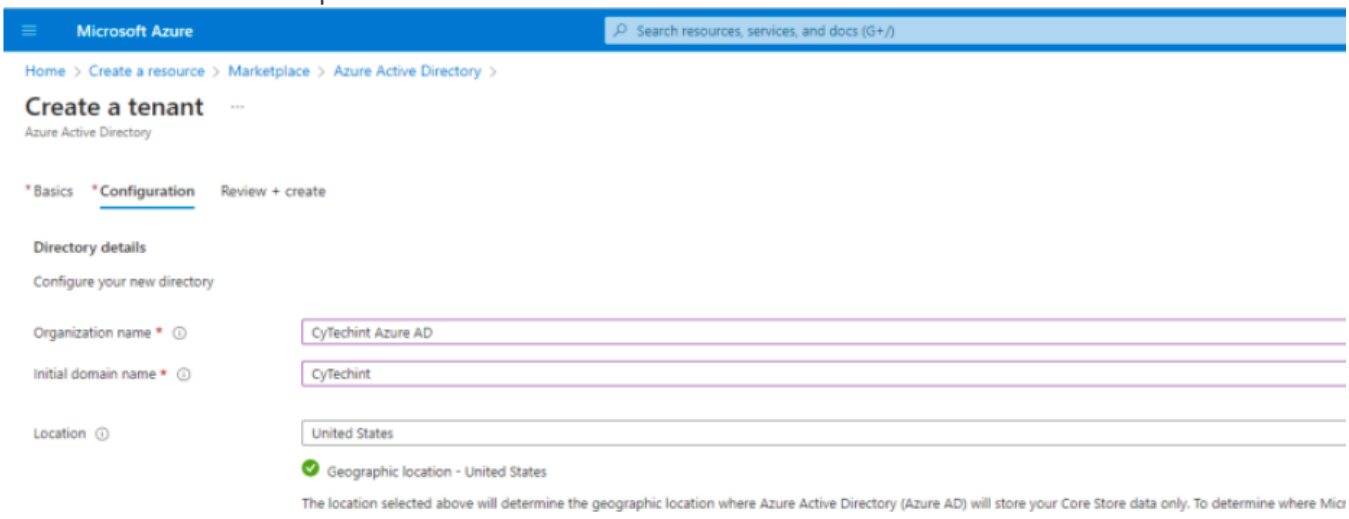


3. For **Subscription**, select the name of the Azure subscription in which you want to create the resource group. For CyTech (**Azure Active Directory**)

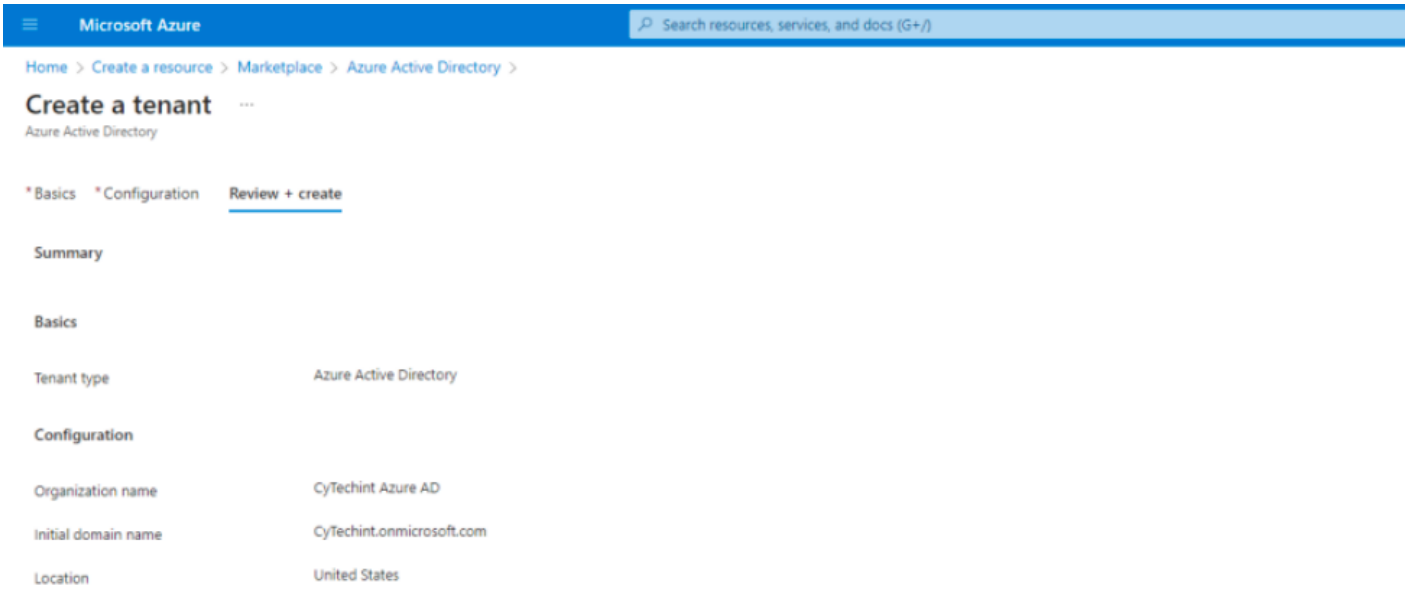


4. Type a unique **name for the resource group**. The system immediately checks to see if the name is available in the currently

selected Azure subscription.



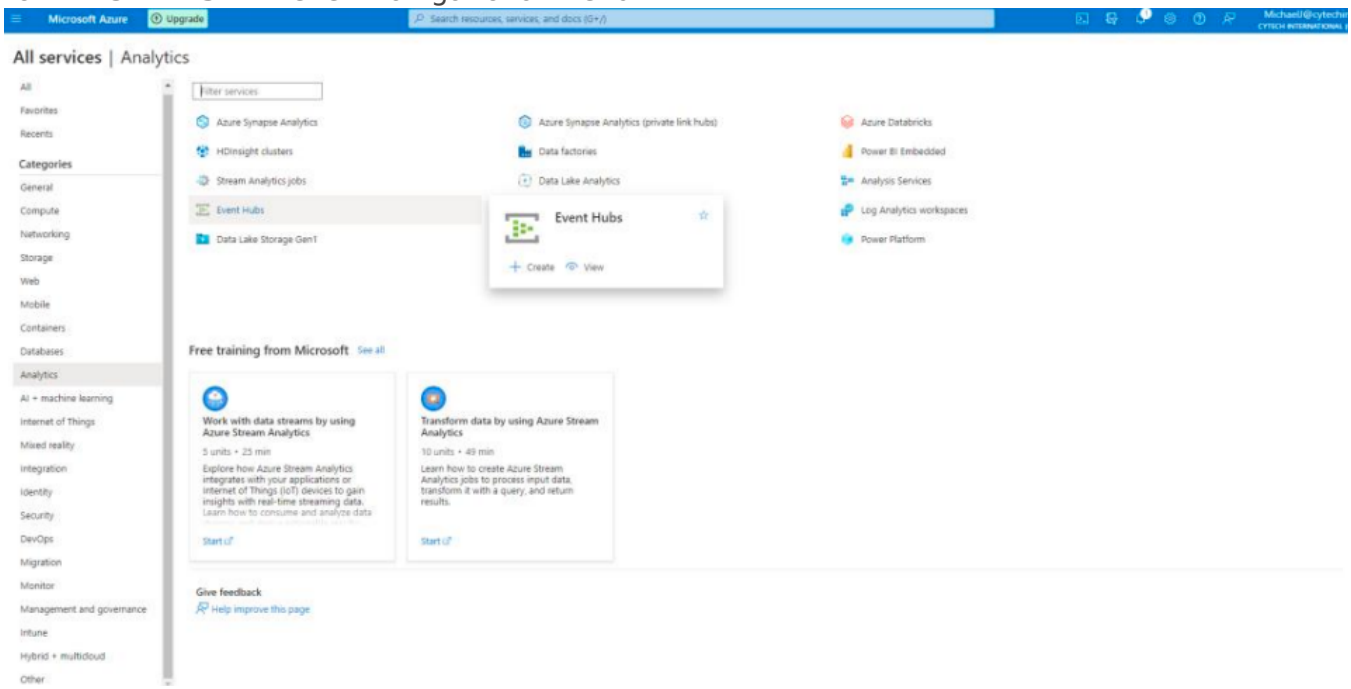
5. Select a **region** for the resource group.
6. Select **Review + Create**.
7. Takes a few minutes to complete.



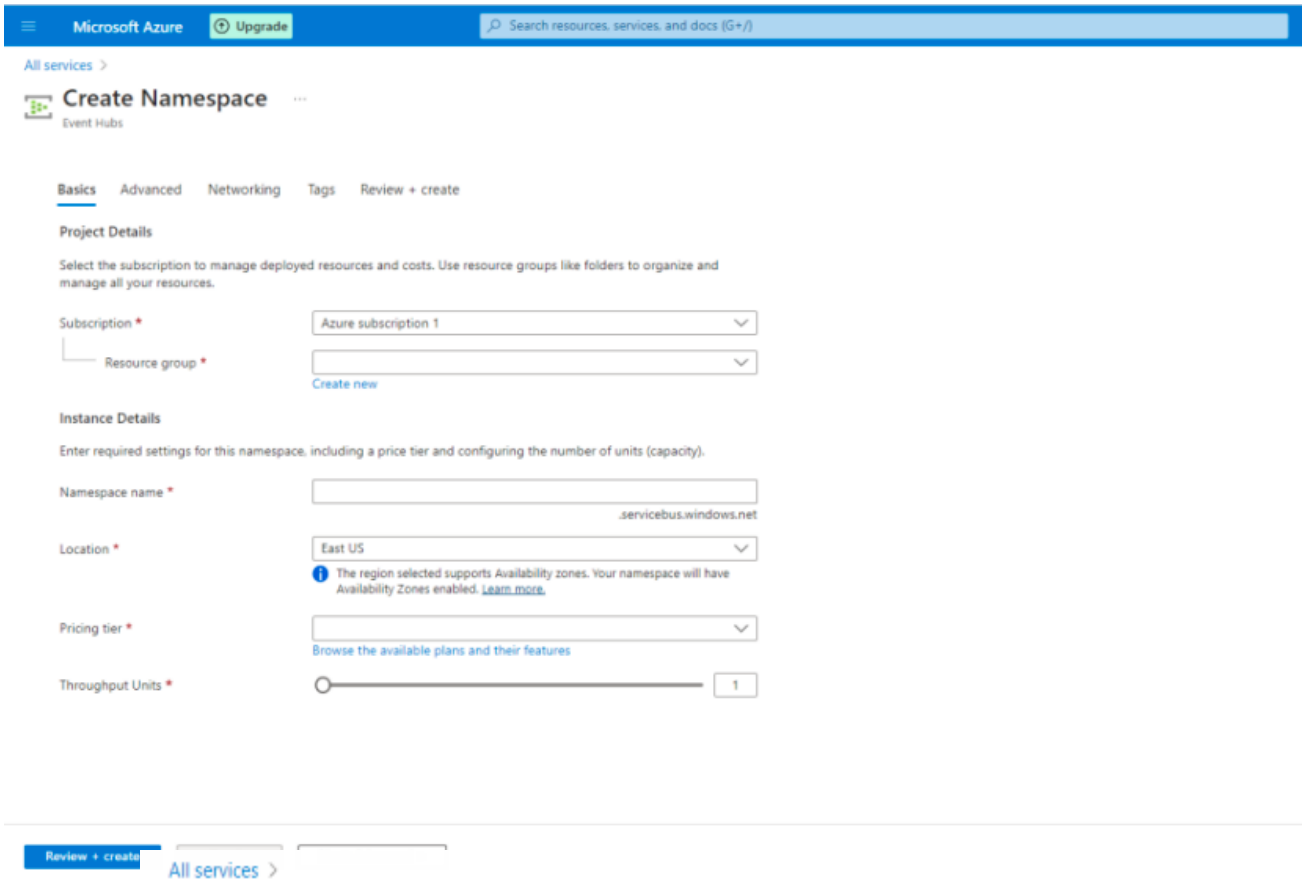
Create an Event Hubs Namespace

An Event Hubs namespace provides a unique scoping container, in which you create one or more event hubs. To create a namespace in your resource group using the portal, do the following actions:

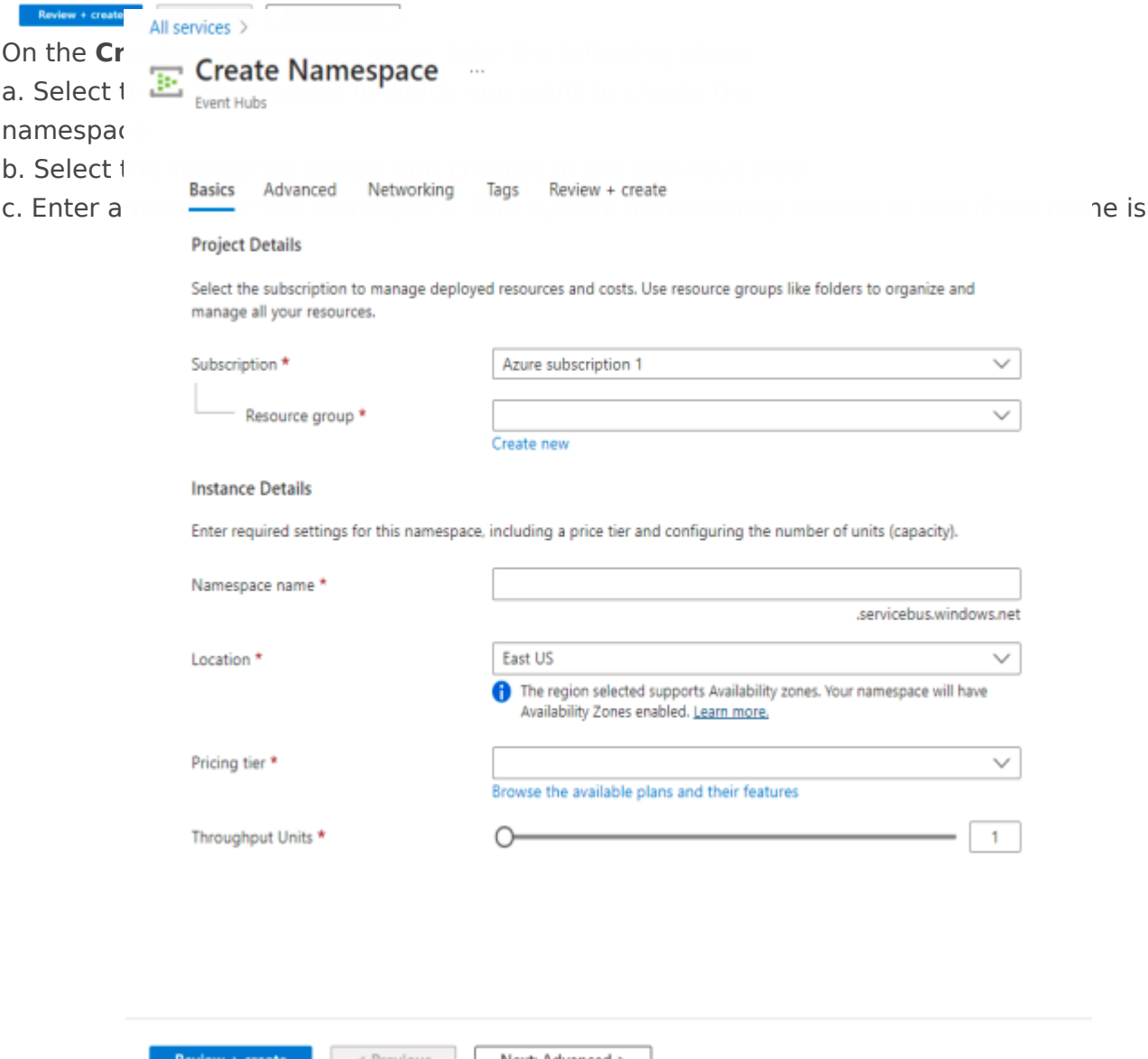
1. In the Azure portal, and select **Create a resource** at the top left of the screen.
2. Select **All services** in the left menu, and select **star (*)** next to **Event Hubs** in the **Analytics** category. Confirm that **Event Hubs** is added to **FAVORITES** in the left navigational menu.



3. Select **Event Hubs** under **FAVORITES** in the left navigational menu, and select **Create** on the toolbar.

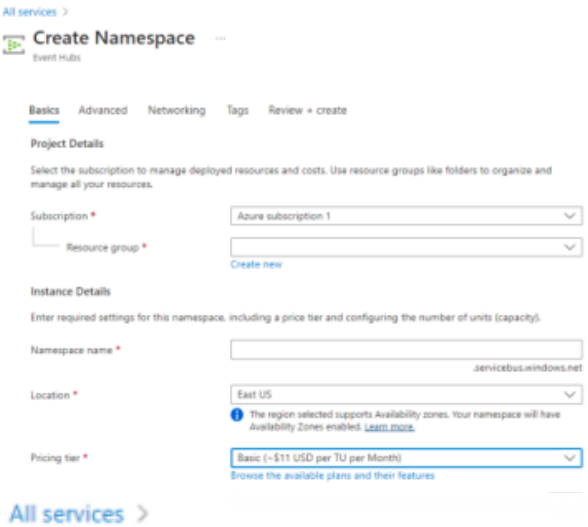


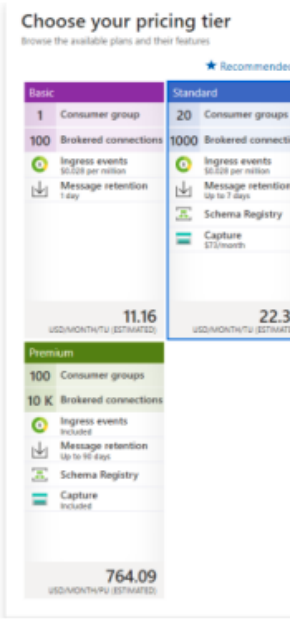
4. On the **Cr**
   a. Select t
   namespac
   b. Select t
   c. Enter a ne is available.

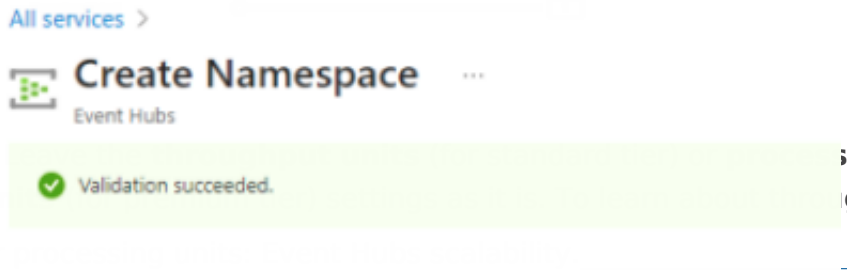


d. Select a **location** for the namespace.

e. Choose **Basic** for the **pricing tier**. To learn about differences between tiers, see Quotas and limits, Event Hubs Premium, and Event Hubs Dedicated articles.





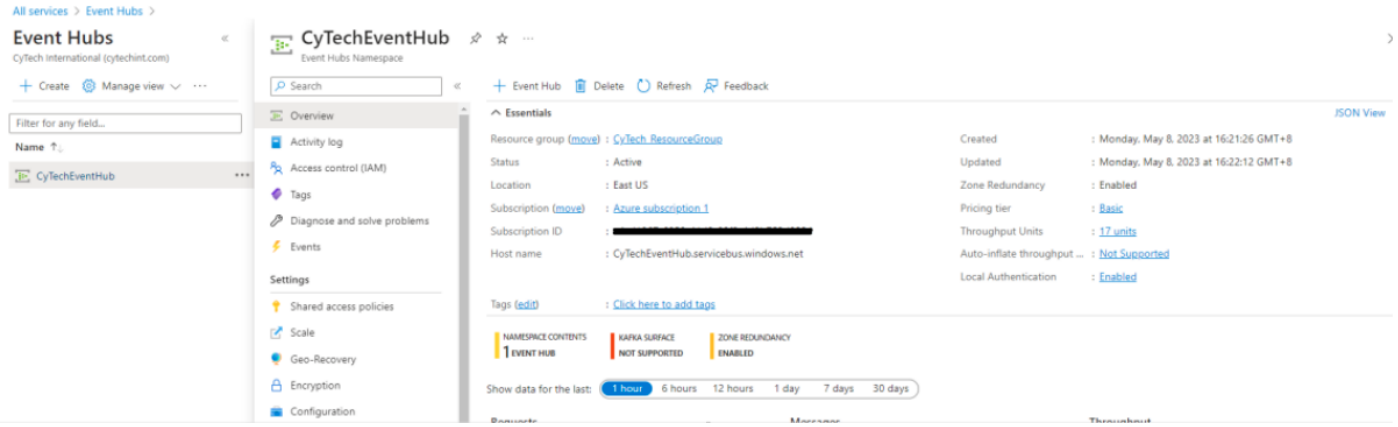


sing

ghput units

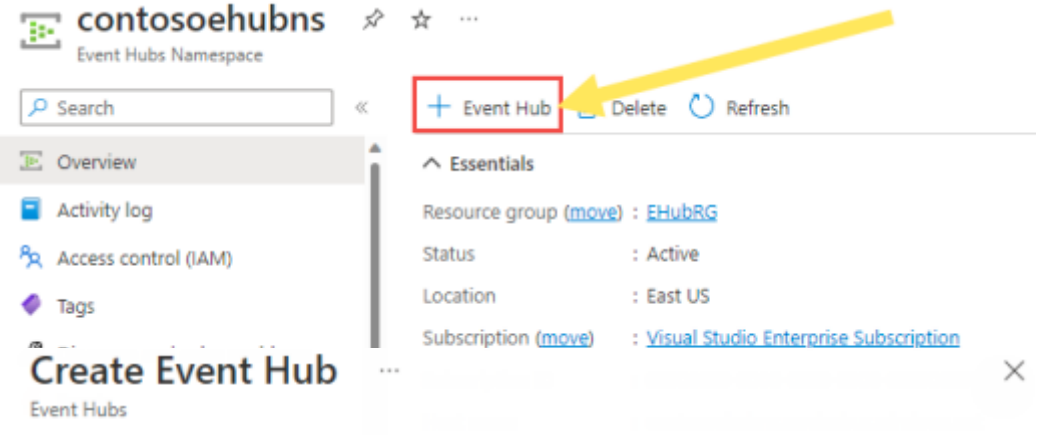
g. Select **Review + Create** at the bottom of the page.
h. On the **Review + Create** page, review the settings, and select **Create**. Wait for the deployment to complete.

5. On the **Deployment** page, select **Go to resource** to navigate to the page for your namespace.

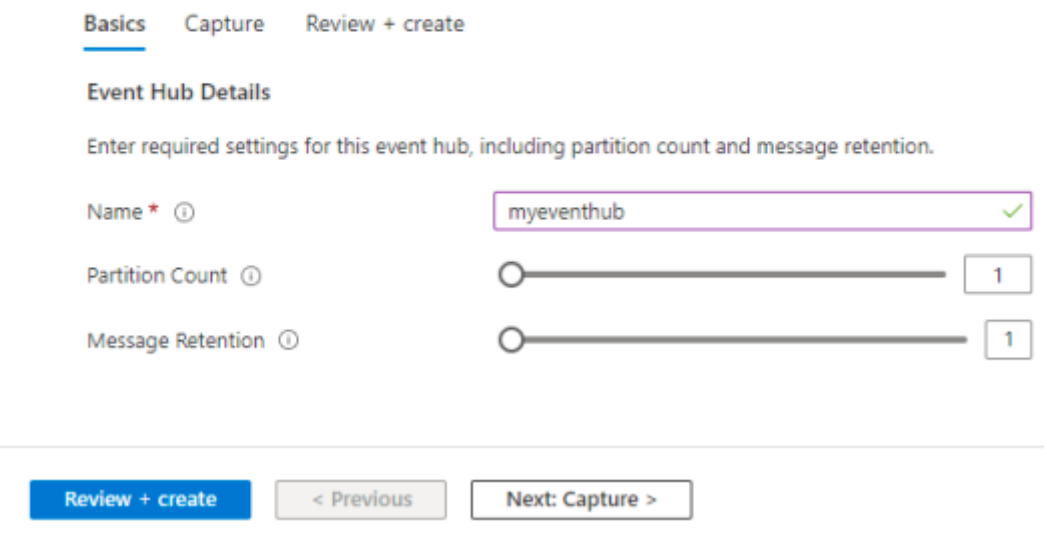


Create an Event Hub

1. To create an event hub within the namespace, do the following actions:
2. On the **Overview** page, select + **Event hub** on the command bar.

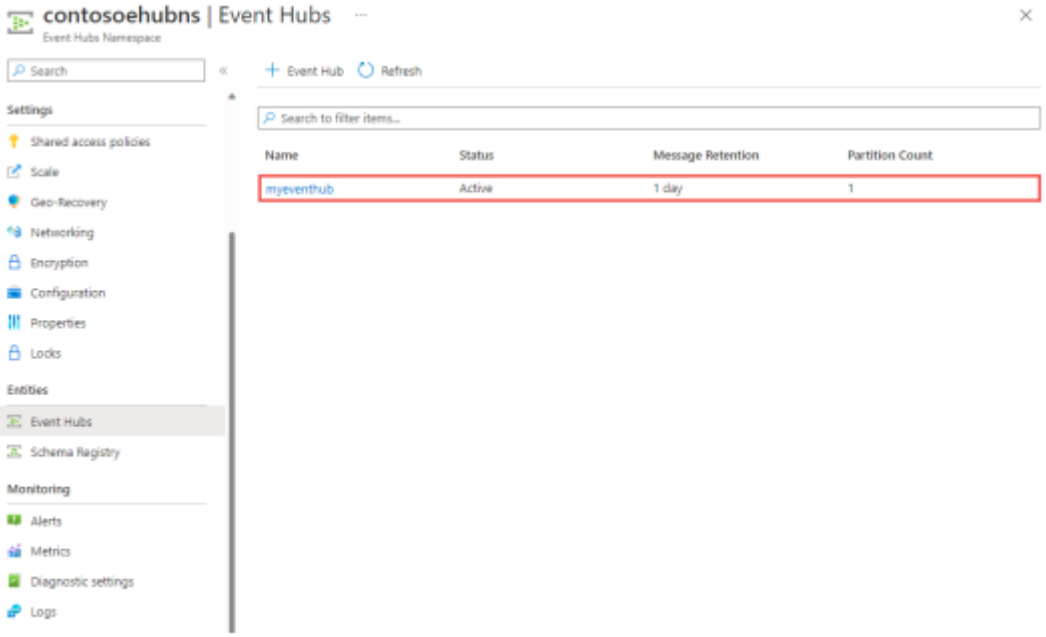


3.



The **partition count** setting allows you to parallelize consumption across
many consumers. For more information, see Partitions.
The **message retention** setting specifies how long the Event Hubs service keeps data. For more information, see Event retention.

4. On the **Review + create** page, select Create.
5. You can check the status of the event hub creation in alerts. After the event hub is created, you see it in the list of event hubs.



Create a Diagnostic Setting

The diagnostic settings export the logs from Azure services to a destination and in order to use Azure Logs integration, it must be an event hub.

To create a diagnostic settings to export logs:

1. Locate the diagnostic settings for the service (for example, Microsoft Entra ID).
2. Select diagnostic settings in the **Monitoring** section of the service. Note that different services may place the diagnostic settings in different positions.
3. Select **Add diagnostic settings**.

In the diagnostic settings page you have to select the source **log categories** you want to export and then select their **destination**.

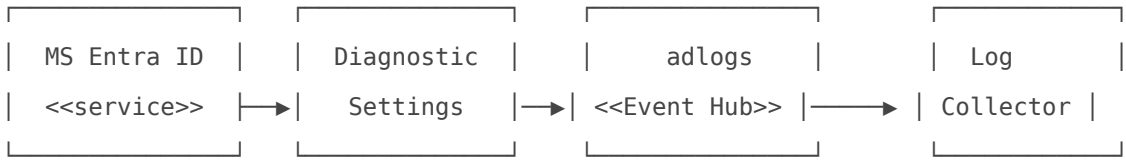
Select log categories

Each Azure services exports a well-defined list of log categories. Check the individual integration doc to learn which log categories are supported by the integration.

Select the destination

Select the **subscription** and the **Event Hubs namespace** you previously created. Select the event hub dedicated to this integration.

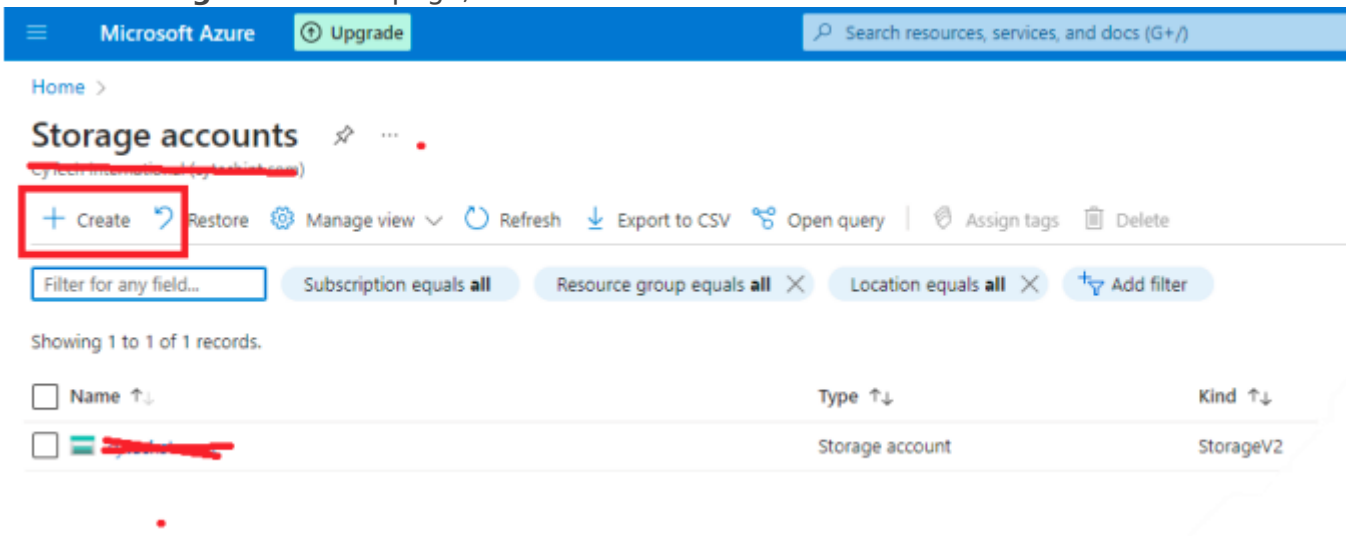
Example:



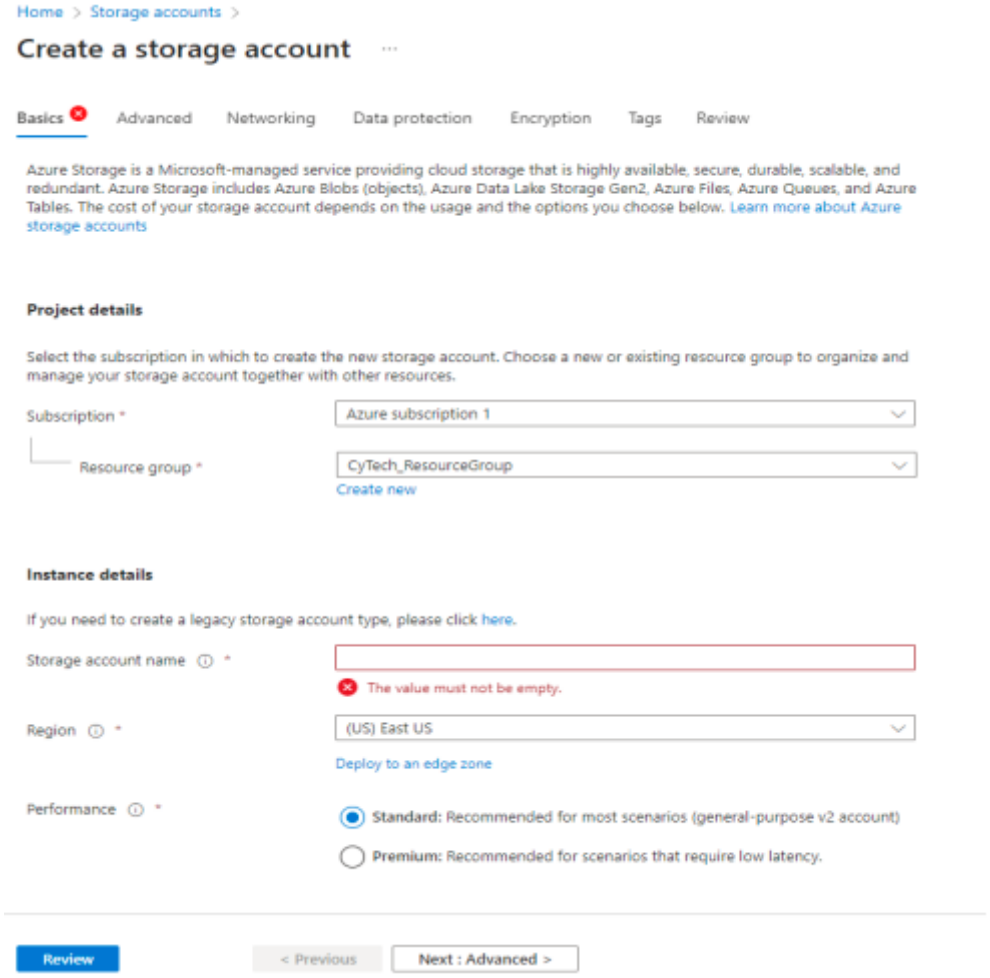
Create a Storage Account

To create an Azure storage account with the Azure portal, follow these steps:

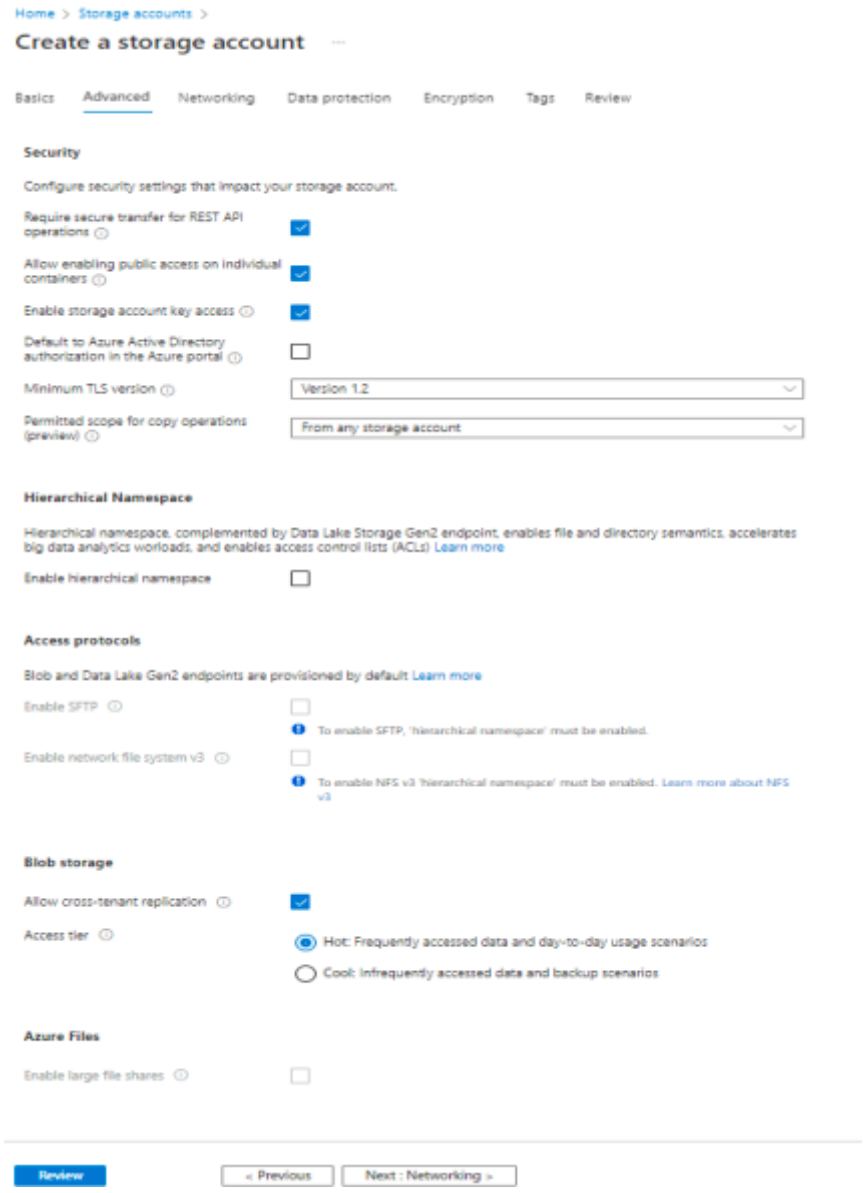
1. From the left portal menu, select **Storage accounts** to display a list of your storage accounts. If the portal menu isn't visible, click the menu button to toggle it on.
2. On the **Storage accounts** page, select **Create**.



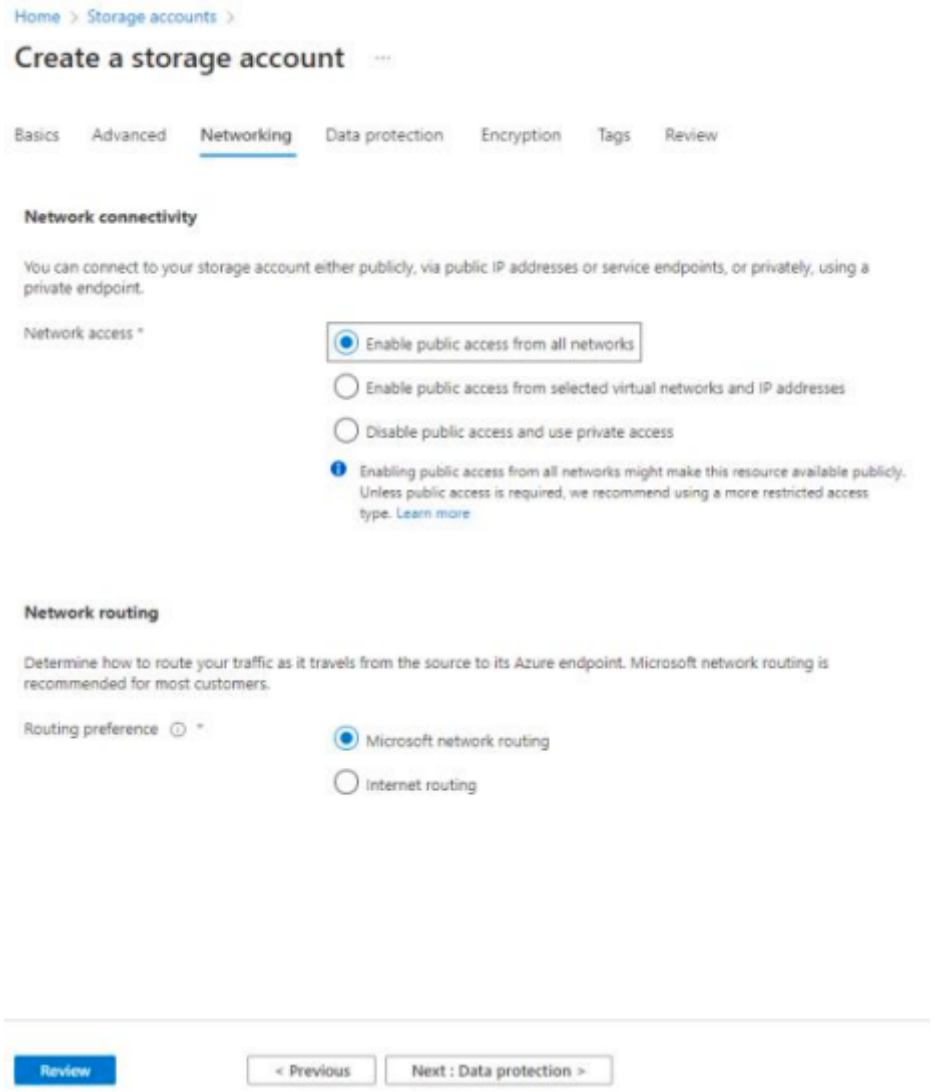
3. The following image shows a standard configuration of the basic properties



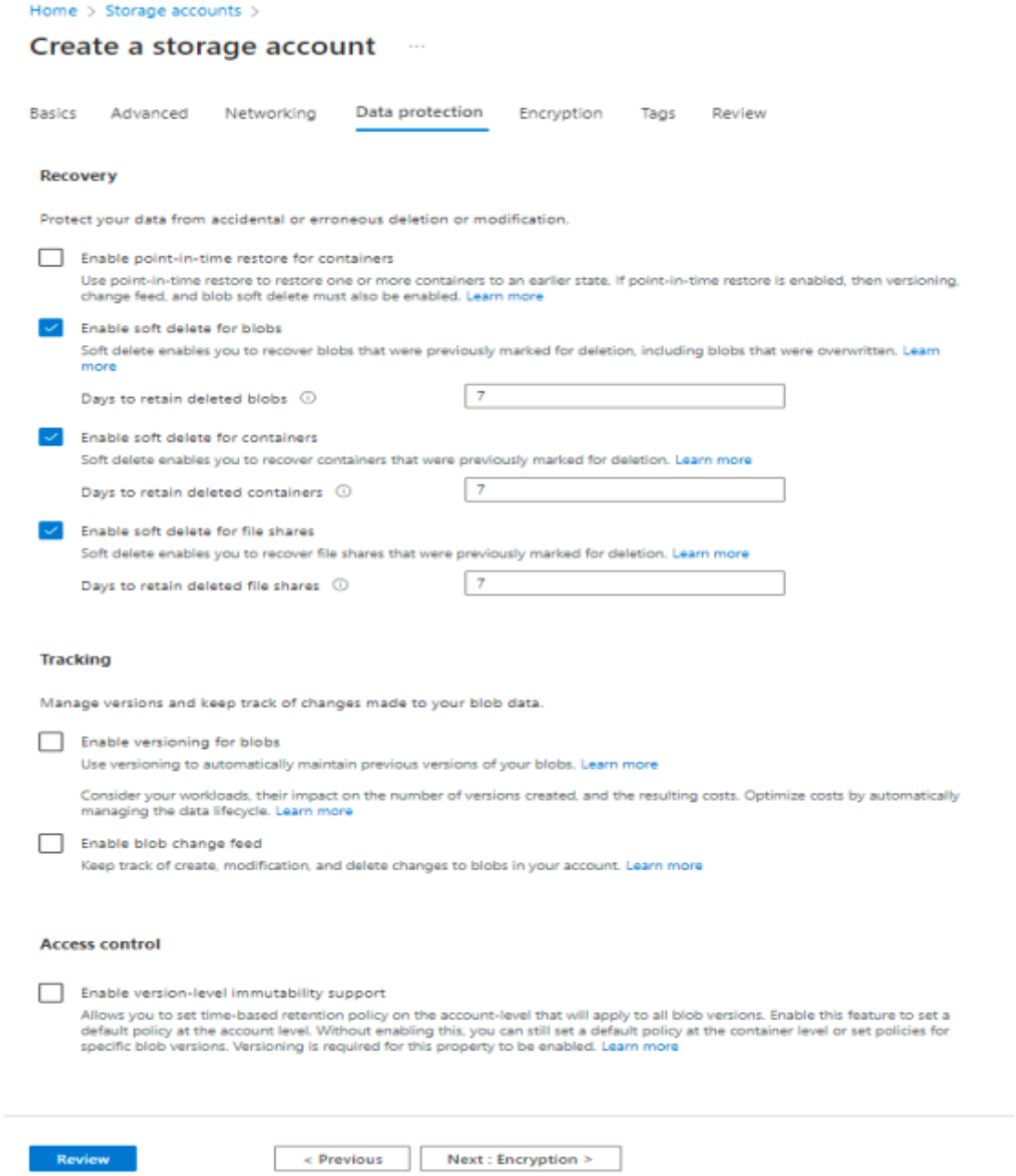
4. The following image shows a standard configuration of the advanced properties for a new storage account.



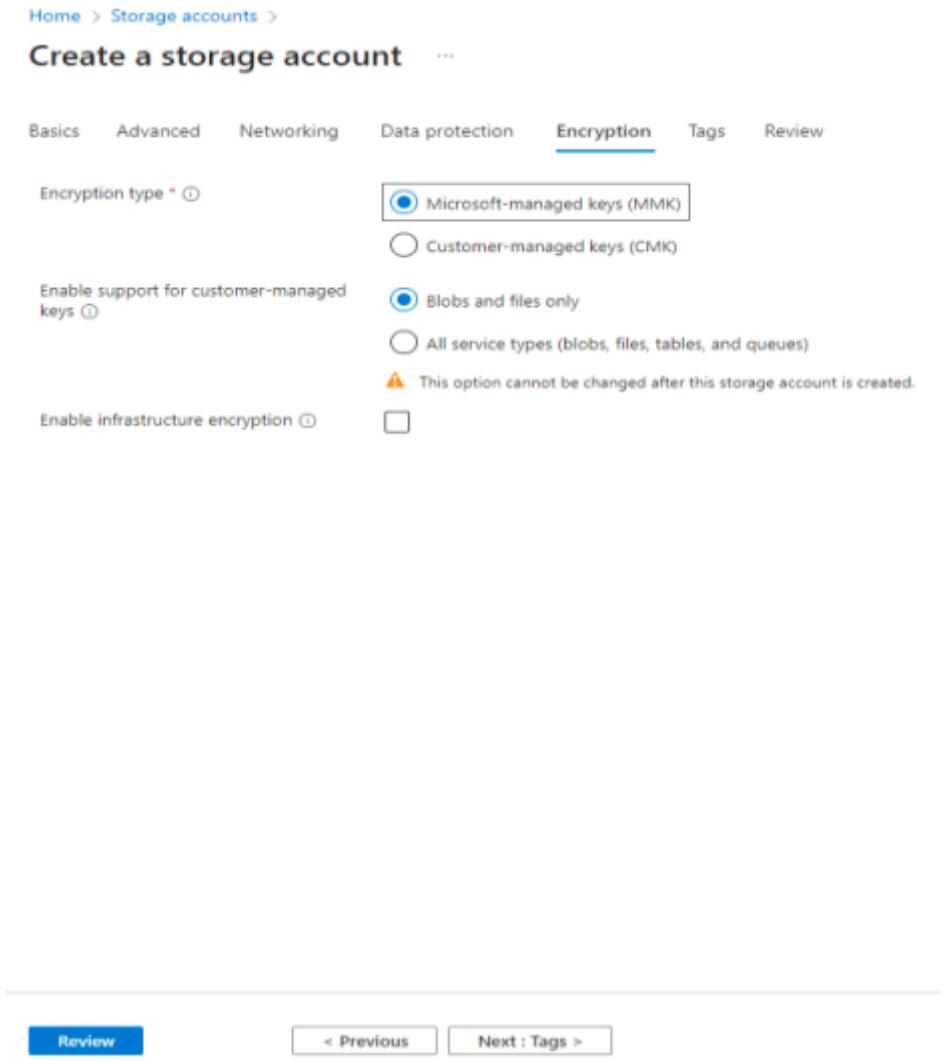
5. The following image shows a standard configuration of the networking properties for a new storage account.



6. The following image shows a standard configuration of the data protection properties for a new storage account.

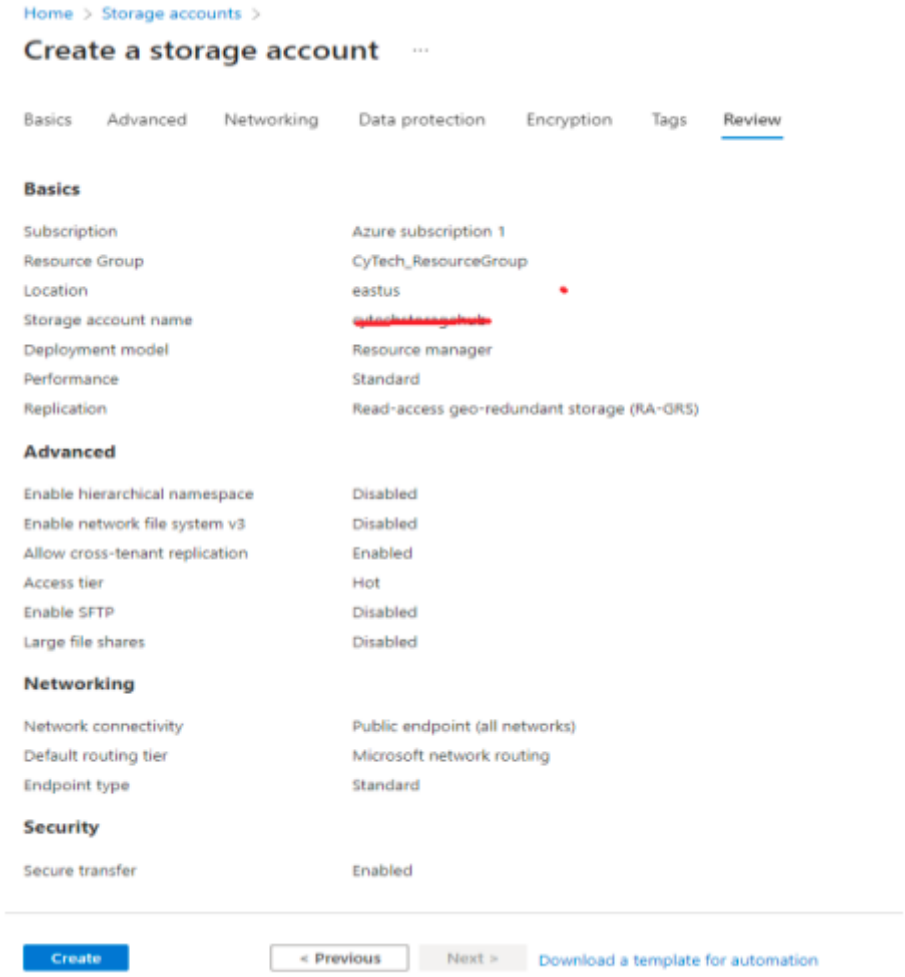


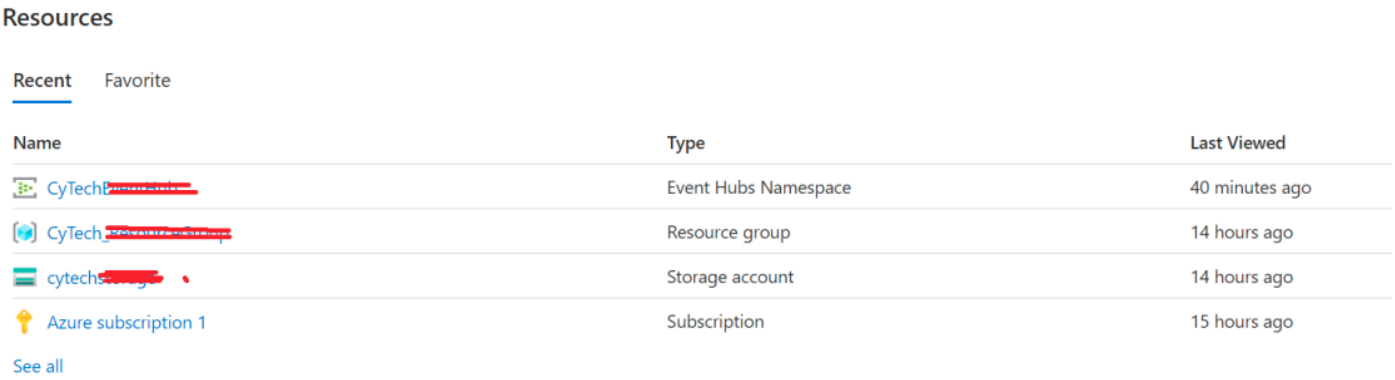
7. The following image shows a standard configuration of the encryption properties for a new storage account.



8. **Review + Create Tab**
   When you navigate to the **Review + create** tab, Azure runs validation on the storage account settings that you have chosen. If validation passes, you can proceed to create the storage account. If validation fails, then the portal indicates which settings need to be modified.

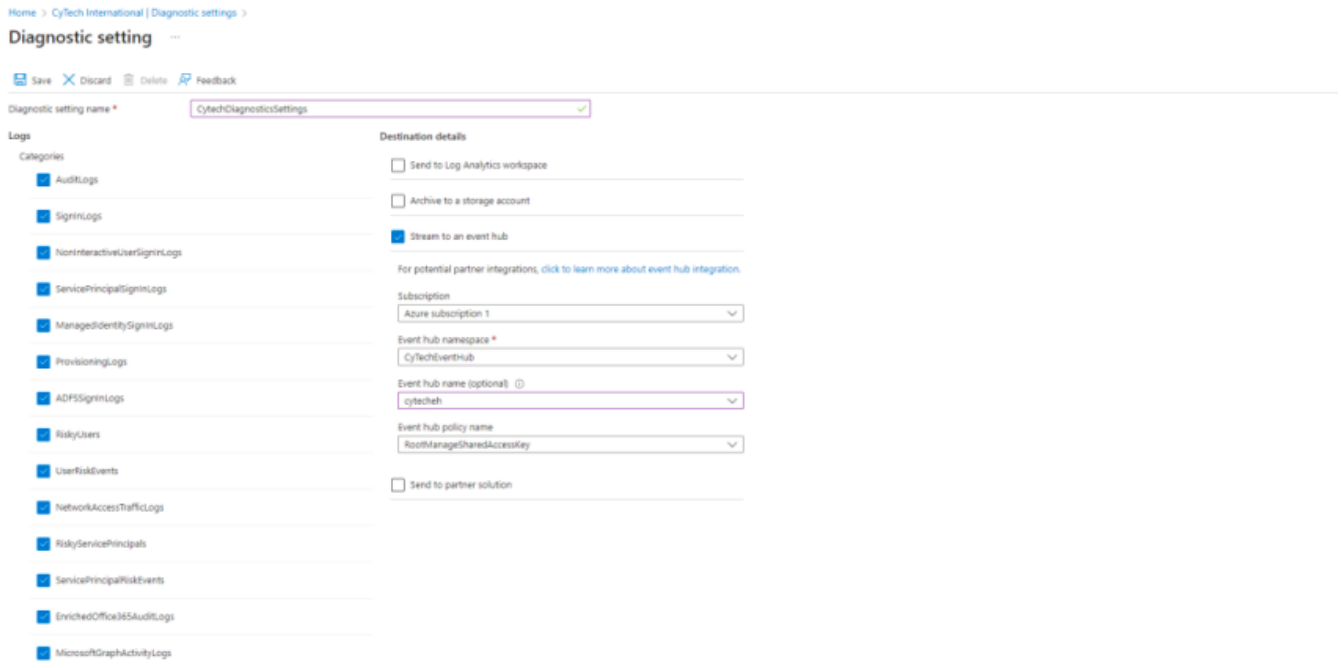
The following image shows the **Review** tab data prior to the creation of a new storage account.



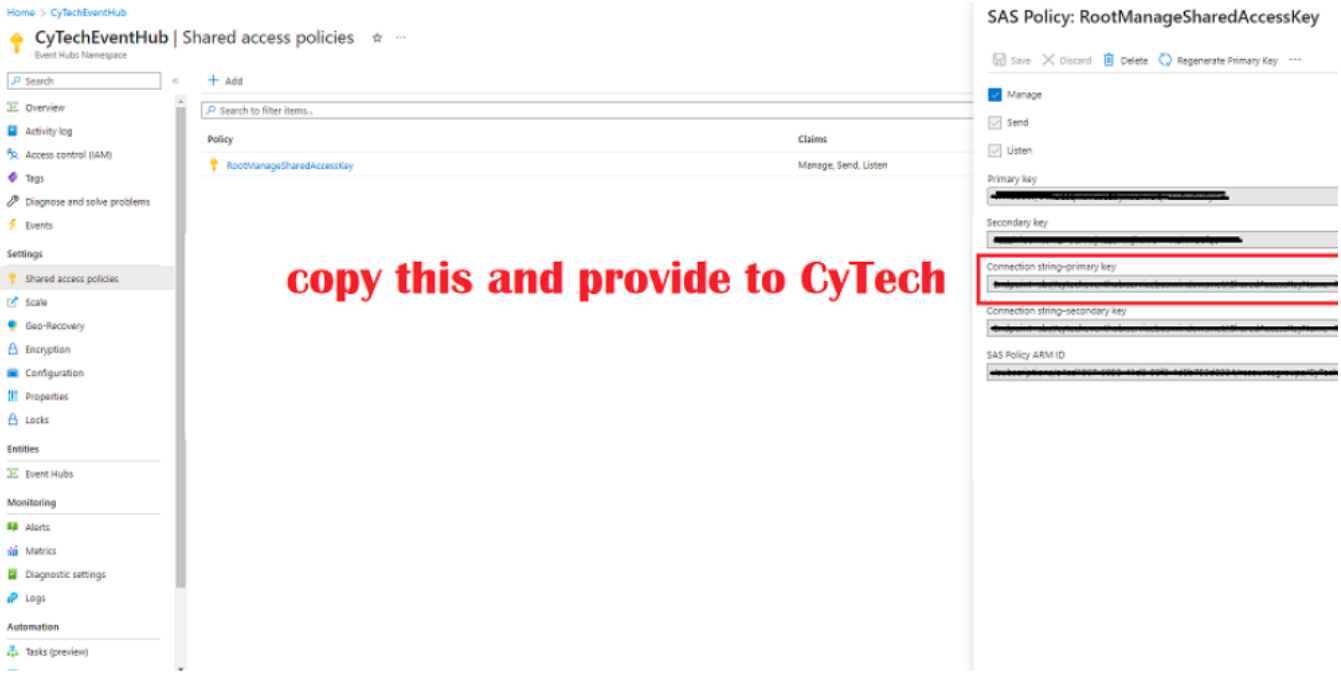


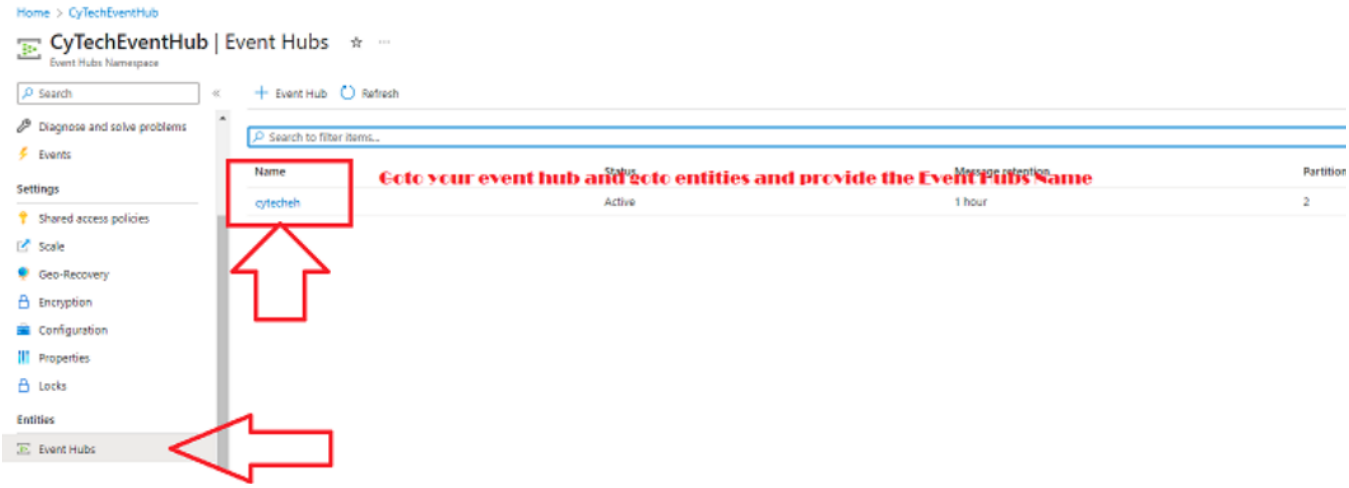
Resources needed for the integration of Azure Active Directory:

1. **Azure Diagnostics Settings**
   Create a Diagnostics Configuration and select which log from
   Azure will send to the event hub.
   Navigate to **Microsoft Entra ID > Monitoring > Diagnostic settings**

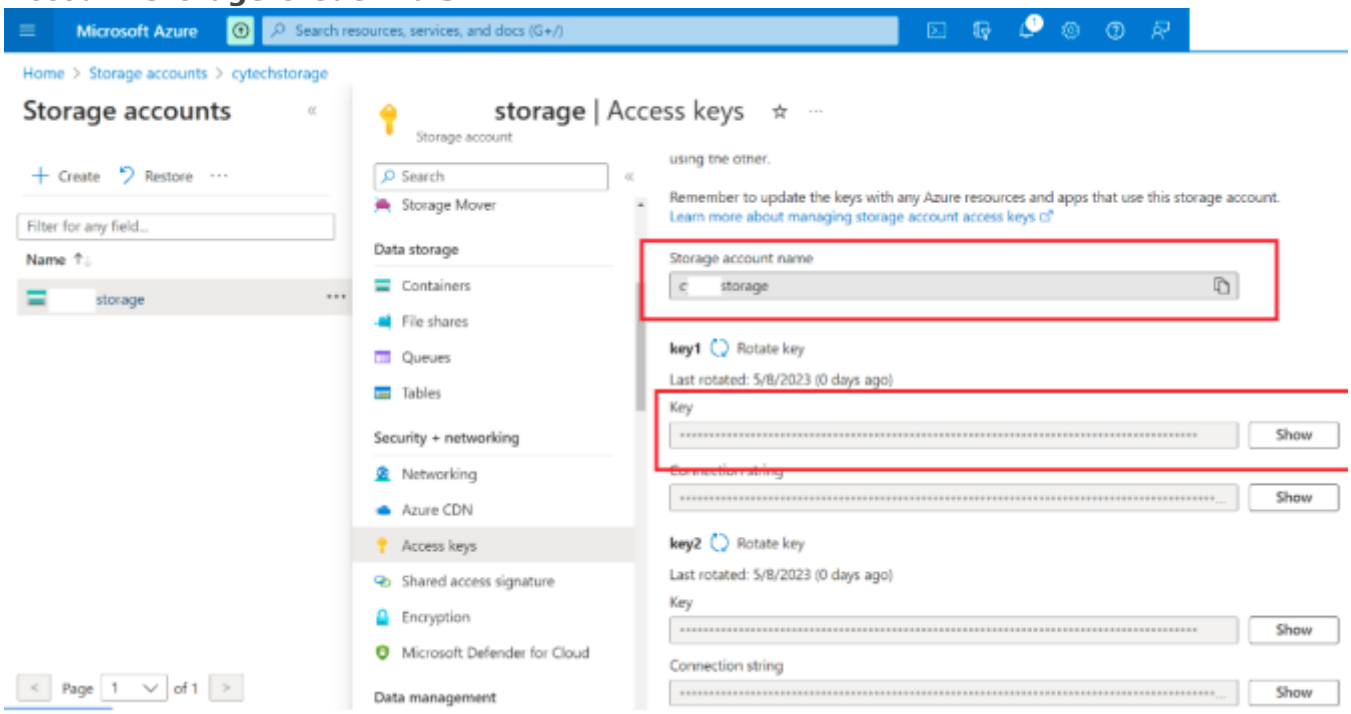


2. **Event Hub Credentials**
3. **Go to > EventHub Resources > Select Shared Access Policies**





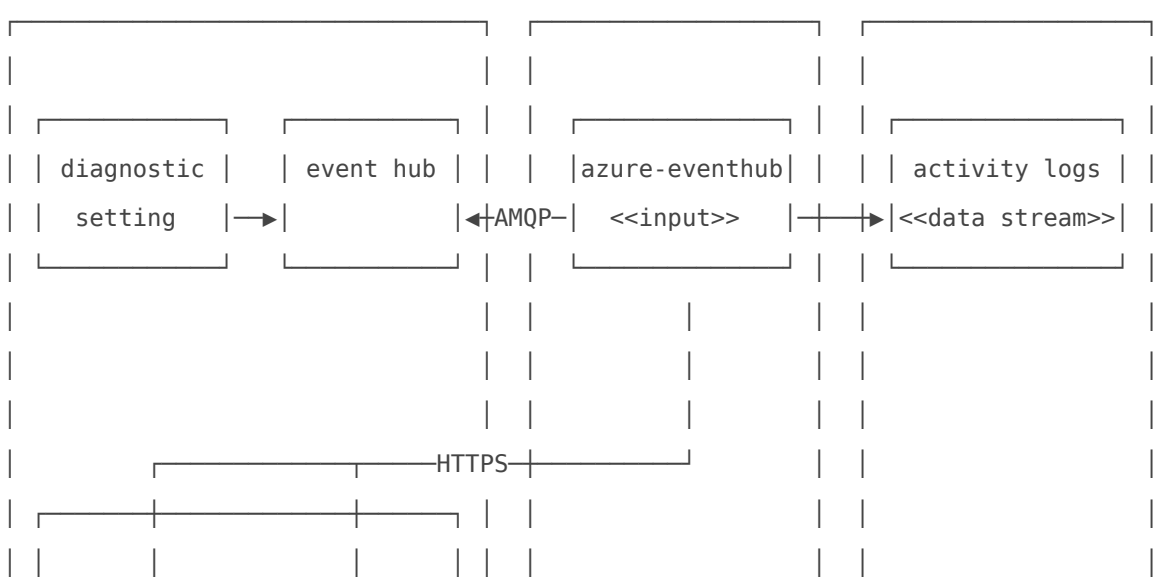
4. **Please provide CyTech the:**
   a. Event Hubs Name Not the Name Space:
   b. Connection string-primary key:
5. **Account Storage Credentials**

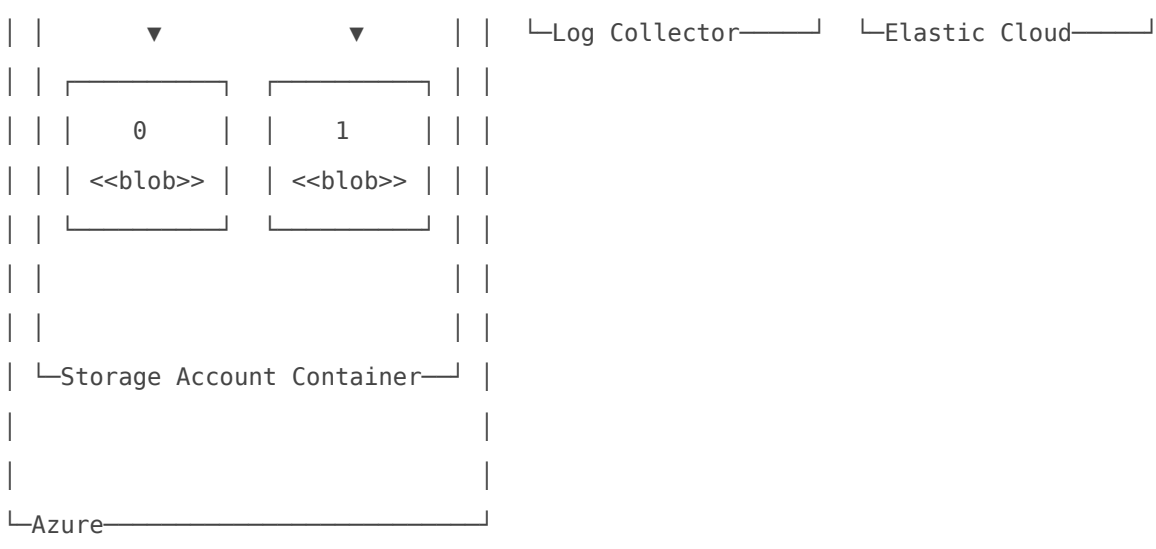


6. **Please provide CyTech the:**
   a. Storage Account Name:
   b. Key 1 Key

Running the integration behind a firewall:

When you run the Elastic Agent behind a firewall, to ensure proper communication with the necessary components, you need to allow traffic on port `5671` and `5672` for the event hub, and port `443` for the Storage Account container.





Event Hub

Port `5671` and `5672` are commonly used for secure communication with the event hub. These ports are used to receive events. By allowing traffic on these ports, the Elastic Agent can establish a secure connection with the event hub.

Storage Account Container

Port `443` is used for secure communication with the Storage Account container. This port is commonly used for HTTPS traffic. By allowing traffic on port 443, the Elastic Agent can securely access and interact with the Storage Account container, which is essential for storing and retrieving checkpoint data for each event hub partition.

DNS

Optionally, you can restrict the traffic to the following domain names:

*.servicebus.windows.net
*.blob.core.windows.net
*.cloudapp.net

Additional Information:

Azure Active Directory Logs contain

Sign-in logs – Information about sign-ins and how your users use your resources.

- Retrieves Azure Active Directory sign-in logs. The sign-ins report provides information about the usage of managed applications and user sign-in activities.

Identity Protection logs - Information about user risk status and the events that change it.

- Retrieves Azure AD Identity Protection logs. The Azure AD Identity Protection service analyzes events from AD users' behavior, detects risk situations, and can respond by reporting only or even blocking users at risk, according to policy configurations.

Provisioning logs - Information about users and group synchronization to and from external enterprise applications.

- Retrieves Azure Active Directory Provisioning logs. The Azure AD Provisioning service syncs AD users and groups to and from external enterprise applications. For example, you can configure the provisioning service to replicate all existing AD users and groups to an external Dropbox Business account or vice-versa.

The Provisioning Logs contain a lot of details about a inbound/outbound sync activity, like:

- User or group details.
- Source and target systems (e.g., from Azure AD to Dropbox).
- Provisioning status.
- Provisioning steps (with details for each step).

Audit logs – Information about changes to your tenant, such as users and group management, or updates to your tenant's resources.

- Retrieves Azure Active Directory audit logs. The audit logs provide traceability through logs for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD like adding or removing users, apps, groups, roles and policies.

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #9
Created 14 November 2024 09:37:05
Updated 17 December 2024 06:57:26 by Aldion Pueblos