

# 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.

---

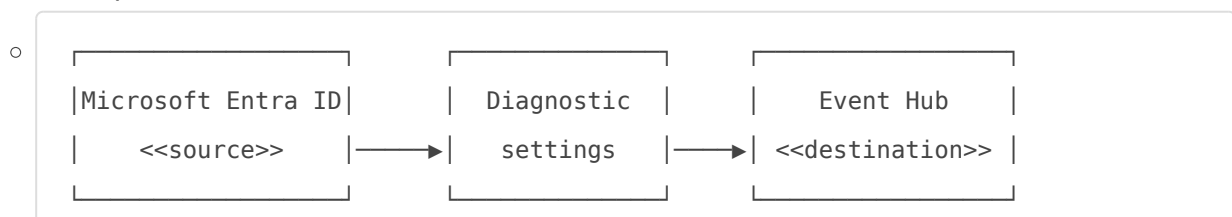
## Requirements

### 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:

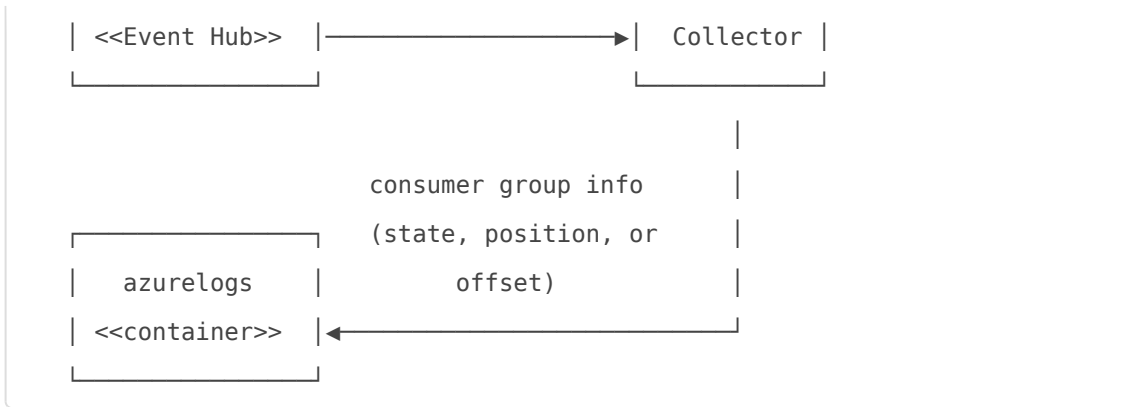


- One or more **diagnostic setting** to export logs from Azure services to Event Hubs
  - Example:

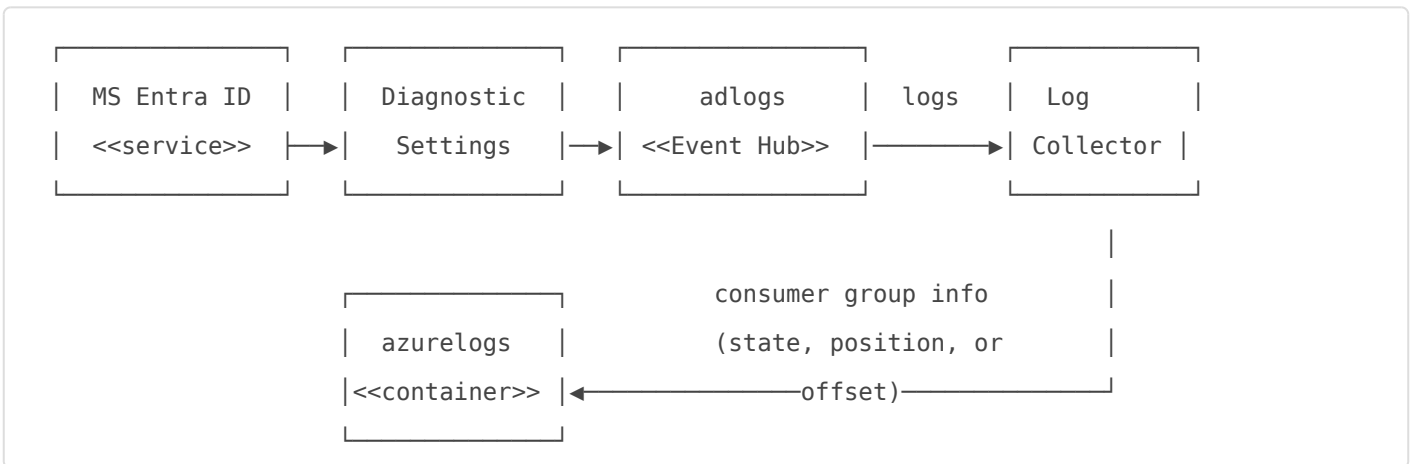


- One **Storage Account Container** to store information about logs consumed by the Log Collector
  - Example:





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.

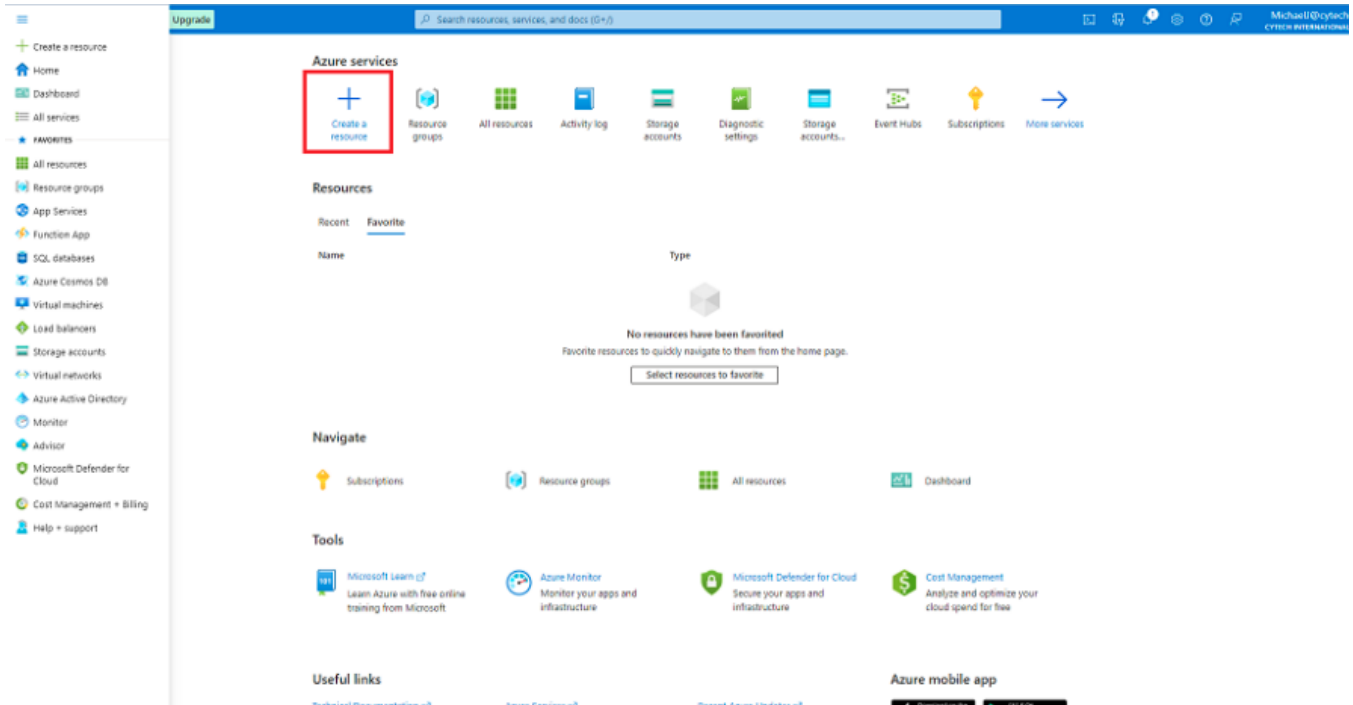
1. **The logs have to be exported first to the event hub.**
  - Create an event hub using Azure portal.
  - More information can be found on: <https://learn.microsoft.com/en-us/azure/event-hubs/event-hubscreate>.
2. **To export activity logs to event hubs users can follow the steps here.**
  - Legacy 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

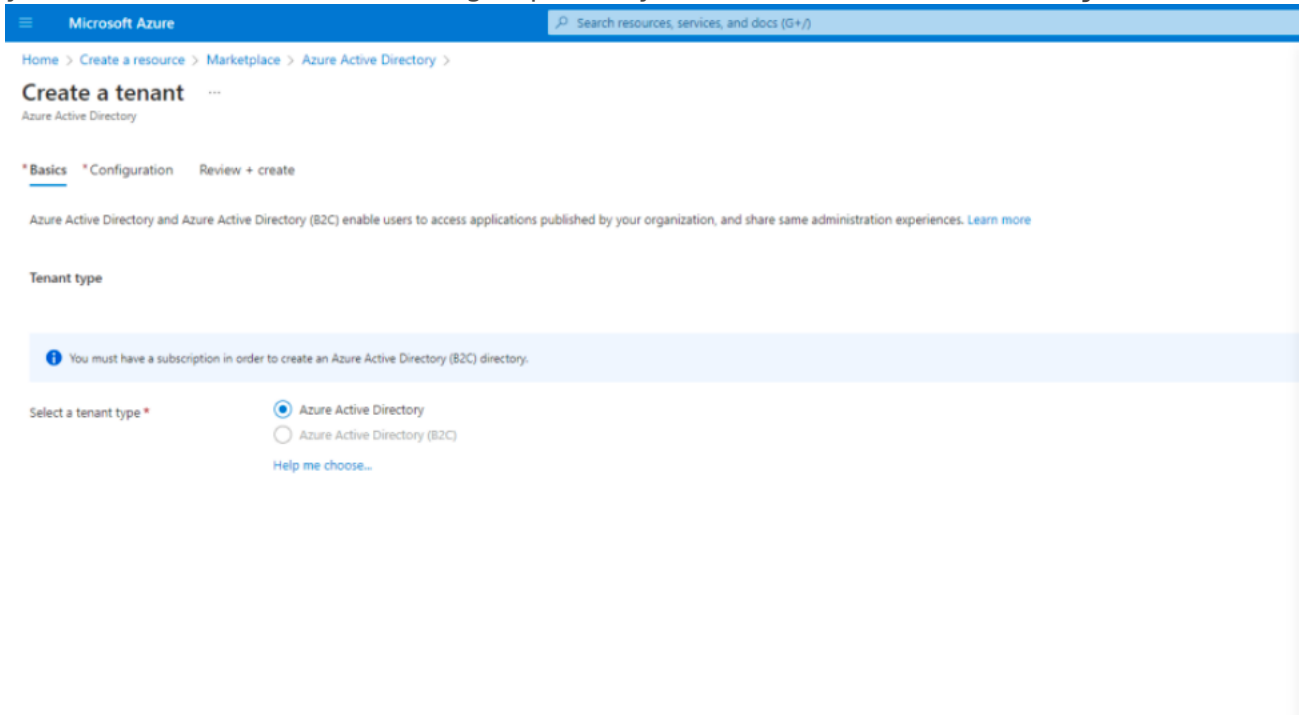
## Create a Resource Group

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 **Resource 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.

The screenshot shows the 'Create a tenant' page in the Microsoft Azure portal, specifically the 'Configuration' tab. The page title is 'Create a tenant' with a three-dot menu icon. Below the title is the breadcrumb 'Home > Create a resource > Marketplace > Azure Active Directory > Create a tenant' and the subtitle 'Azure Active Directory'. There are three tabs: '\* Basics', '\* Configuration' (which is selected and underlined), and 'Review + create'. Under the 'Configuration' tab, there is a section titled 'Directory details' with the instruction 'Configure your new directory'. It contains three input fields: 'Organization name' with the value 'CyTechint Azure AD', 'Initial domain name' with the value 'CyTechint', and 'Location' with the value 'United States'. Below these fields, there is a green checkmark icon followed by the text 'Geographic location - United States'. At the bottom of this section, there is a note: 'The location selected above will determine the geographic location where Azure Active Directory (Azure AD) will store your Core Store data only. To determine where Micr'.

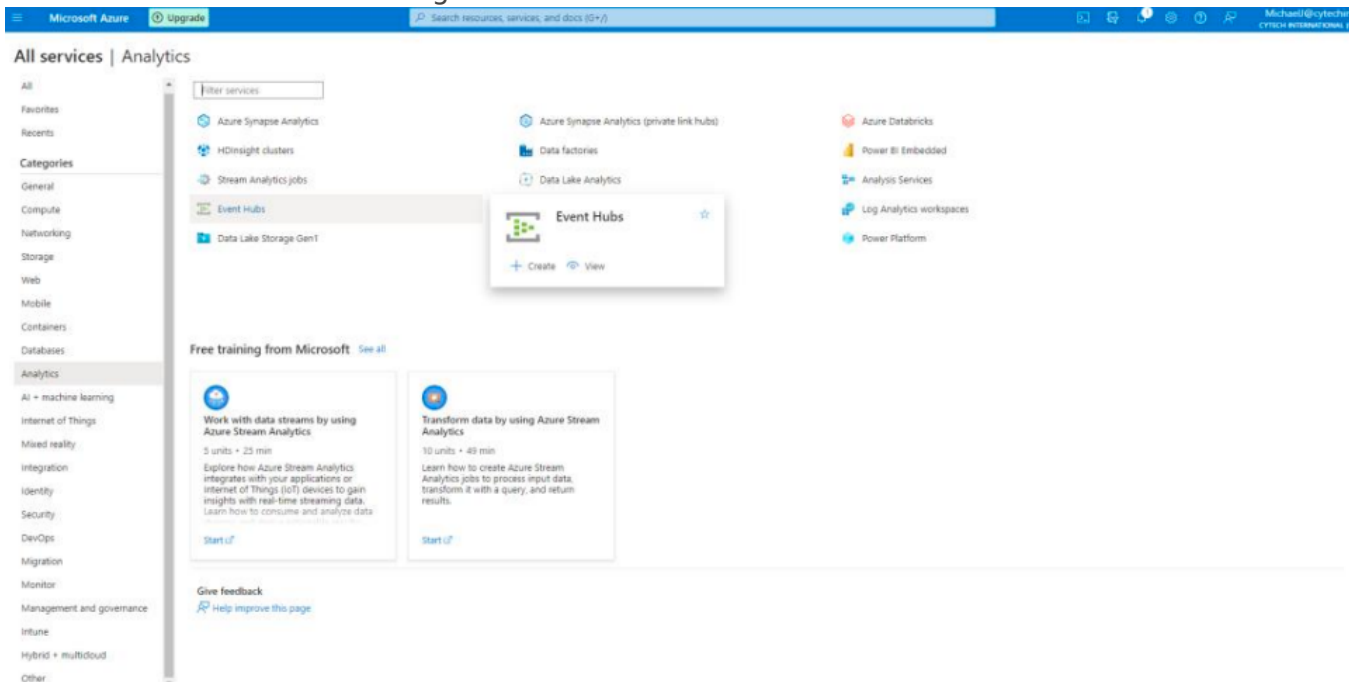
5. Select a **region** for the resource group.
6. Select **Review + Create**.
7. Takes a few minutes to complete.

The screenshot shows the 'Create a tenant' page in the Microsoft Azure portal, specifically the 'Review + create' tab. The page title is 'Create a tenant' with a three-dot menu icon. Below the title is the breadcrumb 'Home > Create a resource > Marketplace > Azure Active Directory > Create a tenant' and the subtitle 'Azure Active Directory'. There are three tabs: '\* Basics', '\* Configuration', and 'Review + create' (which is selected and underlined). Under the 'Review + create' tab, there is a section titled 'Summary'. Below the summary, there is a section titled 'Basics' with the following information: 'Tenant type' is 'Azure Active Directory'. Below that, there is a section titled 'Configuration' with the following information: 'Organization name' is 'CyTechint Azure AD', 'Initial domain name' is 'CyTechint.onmicrosoft.com', and 'Location' is 'United States'.

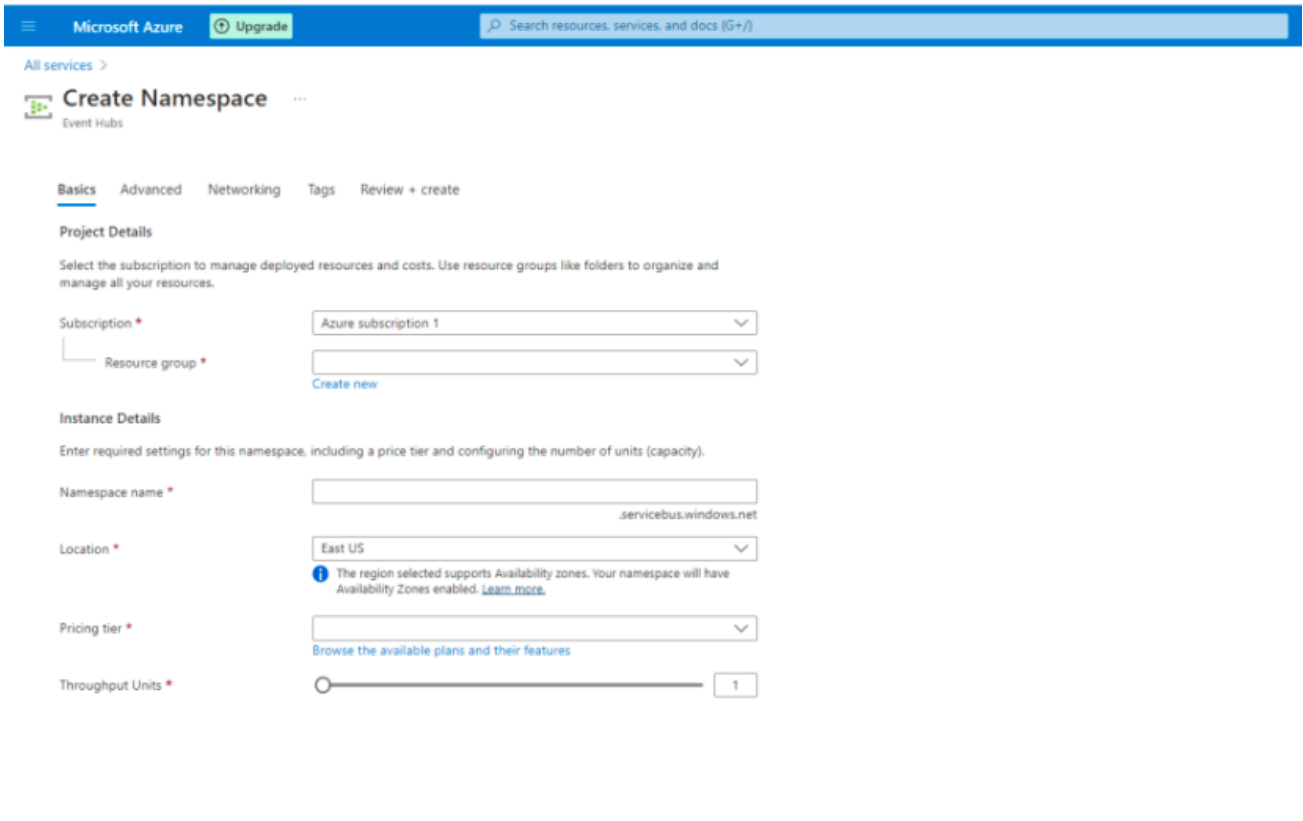
## Create an Event Hubs Namespace

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:

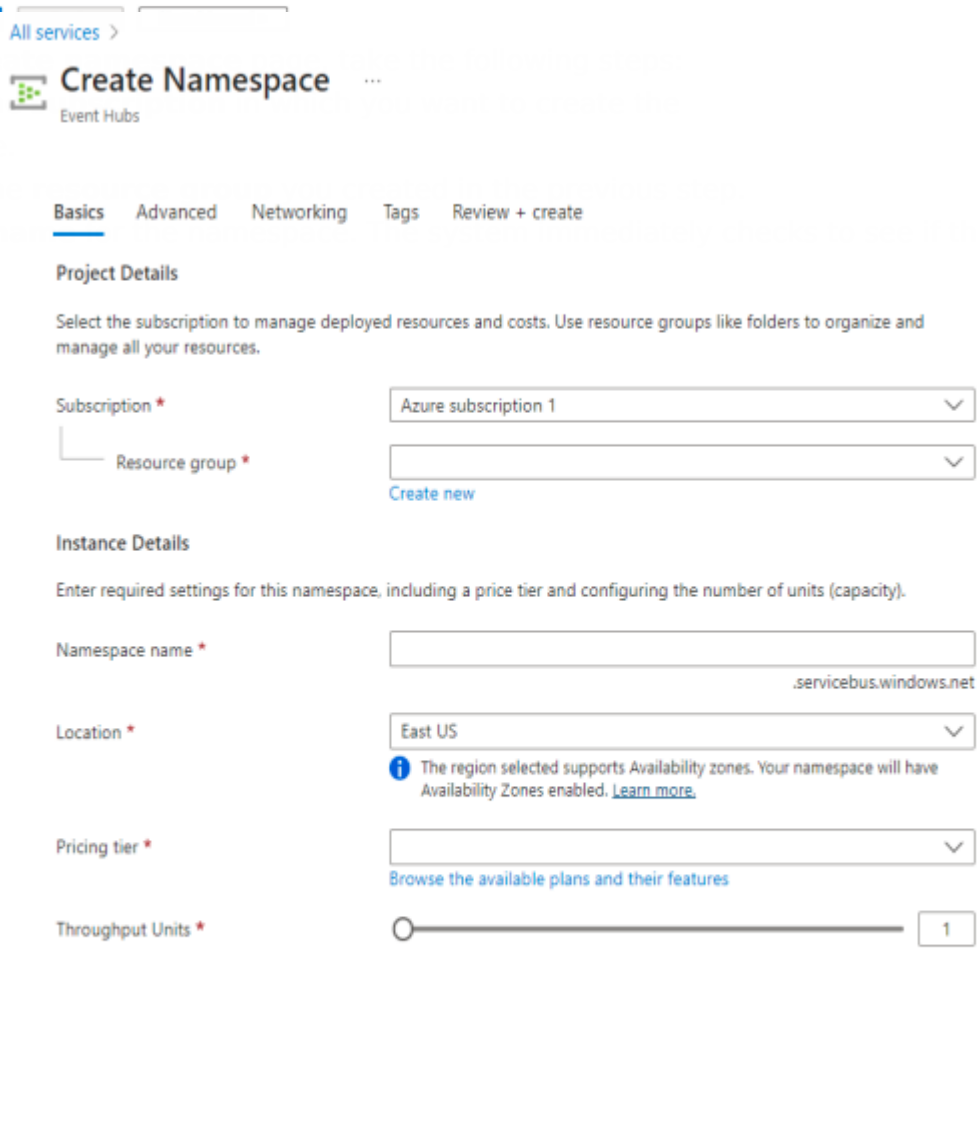
1. In the Azure portal, and select **Create a resource** at the top left of the screen.
2. Select **All services** in the left menu, and select **star (\*)** next to **Event Hubs** in the **Analytics** category. Confirm that **Event Hubs** is added to **FAVORITES** in the left navigational menu.



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



4. On the **Create Namespace** page:
  - a. Select the subscription to manage deployed resources and costs.
  - b. Select the resource group to manage all your resources.
  - c. Enter a namespace name.



ne is

available.

[Review + create](#)

[< Previous](#)

[Next: Advanced >](#)

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.

All services >

### Create Namespace

Event Hubs

Basics | Advanced | Networking | Tags | Review + create

**Project Details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*

[Create new](#)

**Instance Details**

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name \*

Location \*

Pricing tier \*

### Choose your pricing tier

Browse the available plans and their features

Basic		Standard	
1	Consumer group	20	Consumer groups
100	Brokered connections	1000	Brokered connections
Ingress events	50,000 per million	Ingress events	50,000 per million
Message retention	1 day	Message retention	Up to 7 days
		Schema Registry	
		Capture	\$75/month
11.16		22.3	
USD/MONTH/TU (ESTIMATED)		USD/MONTH/TU (ESTIMATED)	
Premium			
100	Consumer groups		
10 K	Brokered connections		
Ingress events	Included		
Message retention	Up to 16 days		
Schema Registry			
Capture	Included		
764.09			
USD/MONTH/TU (ESTIMATED)			

All services >

### Create Namespace

Event Hubs

Validation succeeded.

ing  
ghput units

Basics | Advanced | Networking | Tags | Review + create

Event Hubs Namespace  
by Microsoft

#### Basics

Namespace name: CytechTesting  
Subscription: Azure subscription 1  
Resource group: CyTech\_ResourceGroup  
Location: East US  
Pricing tier: Basic  
Throughput Units: 1  
Availability Zones (Zone Redundancy): Enabled

#### Networking

Connectivity method: Public access

#### Security

Minimum TLS version: 1.2  
Local Authentication: Enabled

Create

< Previous

Next >

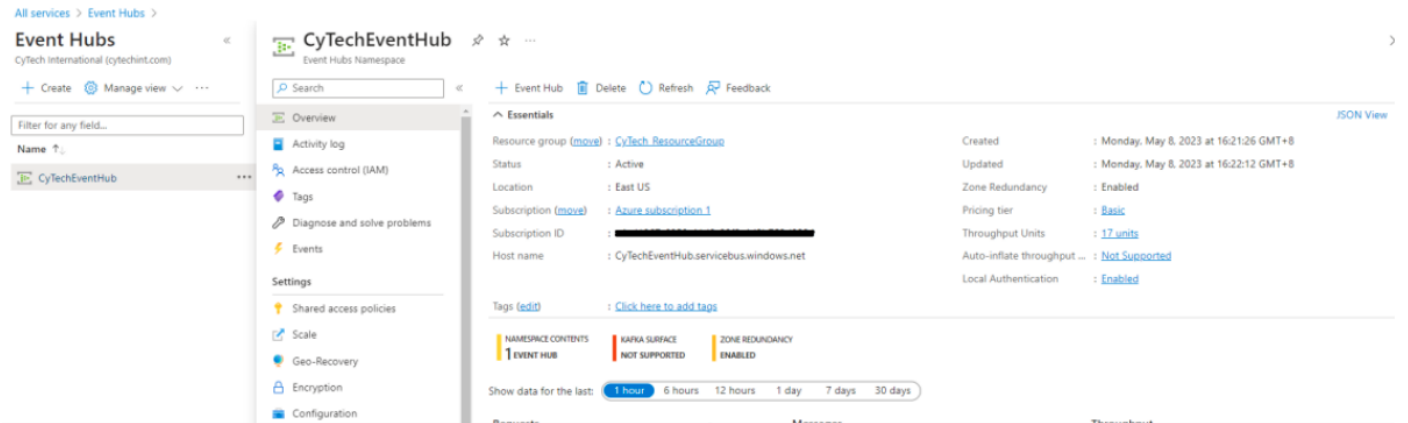
g. Select **Review + Create** at the bottom of the

page.

h. On the **Review + Create** page, review the settings, and select **Create**.

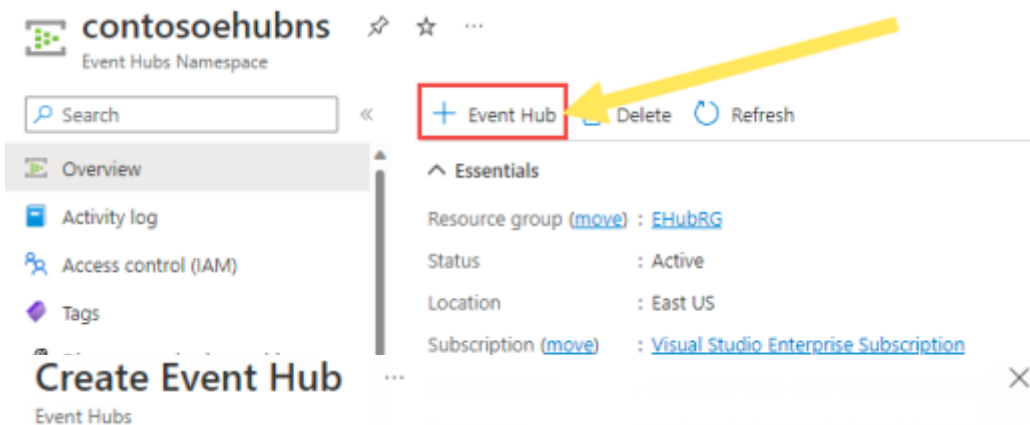
Wait for the deployment to complete.

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

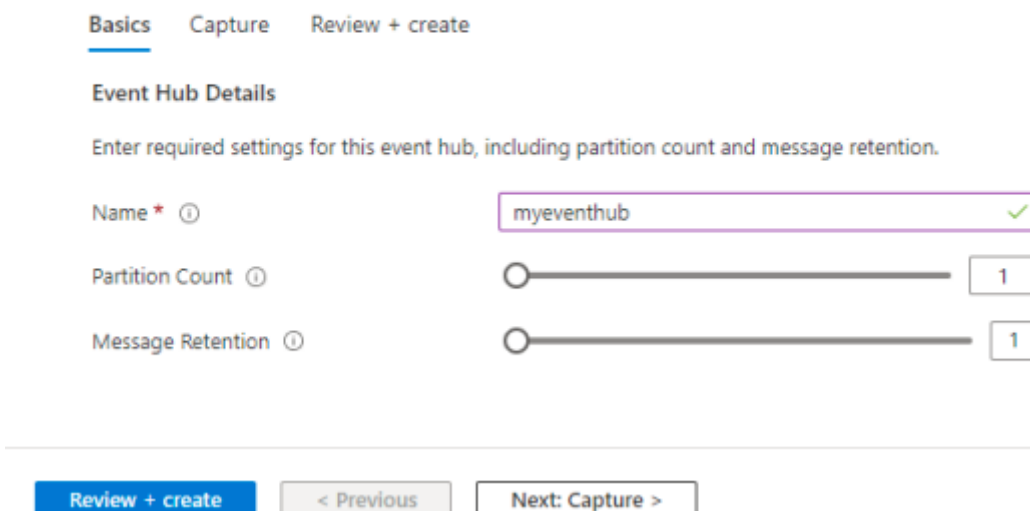


## Create an Event Hub

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.

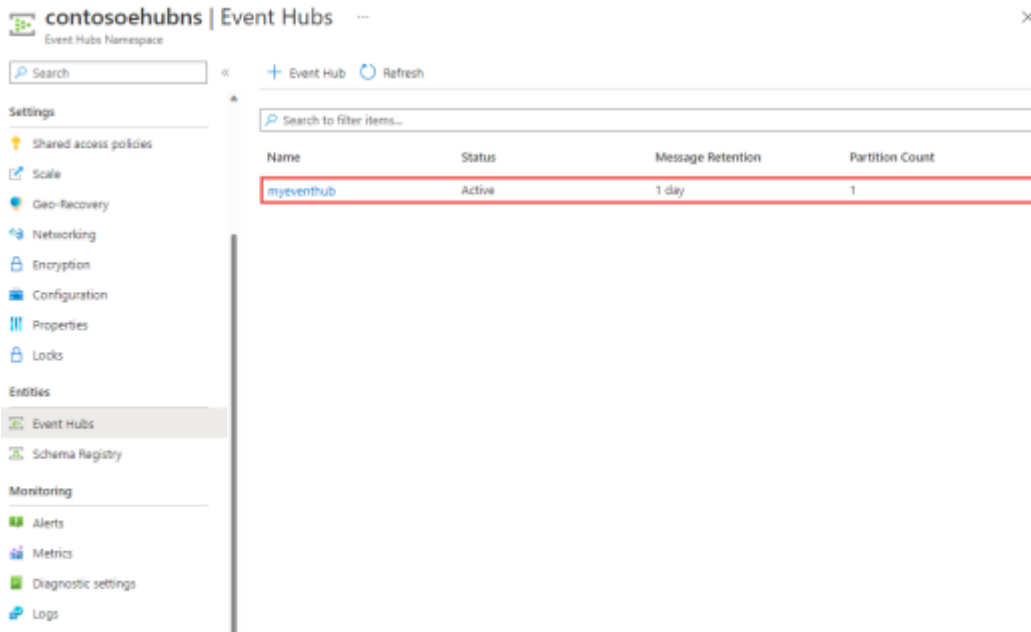


The **partition count** setting allows you to parallelize consumption across

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.

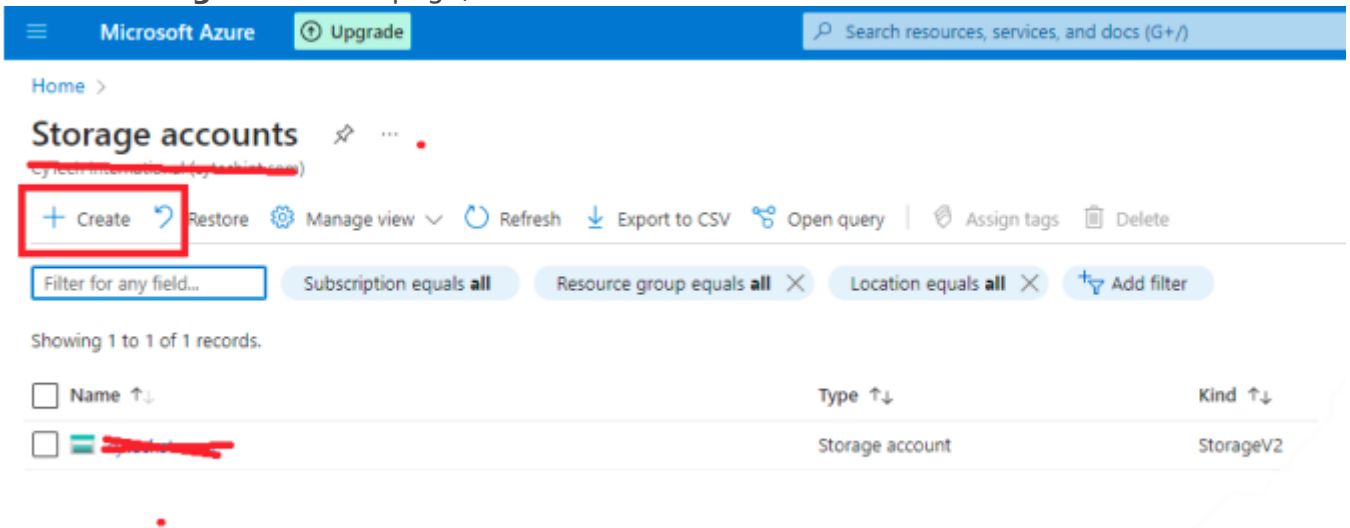
Example:



## 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

[Home](#) > [Storage accounts](#) >

## Create a storage account ...

**Basics** ⓧ [Advanced](#) [Networking](#) [Data protection](#) [Encryption](#) [Tags](#) [Review](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

#### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \*

Resource group \*  [Create new](#)

#### Instance details

If you need to create a legacy storage account type, please [click here](#).

Storage account name  ⓧ \*  
ⓧ The value must not be empty.

Region  ⓧ \*  
[Deploy to an edge zone](#)

Performance  ⓧ \*  
 Standard: Recommended for most scenarios (general-purpose v2 account)  
 Premium: Recommended for scenarios that require low latency.

[Review](#) [< Previous](#) [Next : Advanced >](#)

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

Home > Storage accounts >

## Create a storage account

Basics **Advanced** Networking Data protection Encryption Tags Review

### Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations

Allow enabling public access on individual containers

Enable storage account key access

Default to Azure Active Directory authorization in the Azure portal

Minimum TLS version

Permitted scope for copy operations (preview)

### Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) [Learn more](#)

Enable Hierarchical namespace

### Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default [Learn more](#)

Enable SFTP   
**i** To enable SFTP, 'Hierarchical namespace' must be enabled.

Enable network file system v3   
**i** To enable NFS v3 'Hierarchical namespace' must be enabled. [Learn more about NFS v3](#)

### Blob storage

Allow cross-tenant replication

Access tier  Hot: Frequently accessed data and day-to-day usage scenarios  
 Cool: Infrequently accessed data and backup scenarios

### Azure Files

Enable large file shares

---

[Review](#) [< Previous](#) [Next : Networking >](#)

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

Home > Storage accounts >

## Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review

### Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access \*

- Enable public access from all networks
- Enable public access from selected virtual networks and IP addresses
- Disable public access and use private access
- i** Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. [Learn more](#)

### Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference ⓘ \*

- Microsoft network routing
- Internet routing

---

[Review](#) [< Previous](#) [Next: Data protection >](#)

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

[Home](#) > [Storage accounts](#) >

## Create a storage account

Basics   Advanced   Networking   **Data protection**   Encryption   Tags   Review

### Recovery

Protect your data from accidental or erroneous deletion or modification.

- Enable point-in-time restore for containers  
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)
- Enable soft delete for blobs  
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)  
Days to retain deleted blobs ⓘ
- Enable soft delete for containers  
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)  
Days to retain deleted containers ⓘ
- Enable soft delete for file shares  
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)  
Days to retain deleted file shares ⓘ

### Tracking

Manage versions and keep track of changes made to your blob data.

- Enable versioning for blobs  
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)  
Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#)
- Enable blob change feed  
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)

### Access control

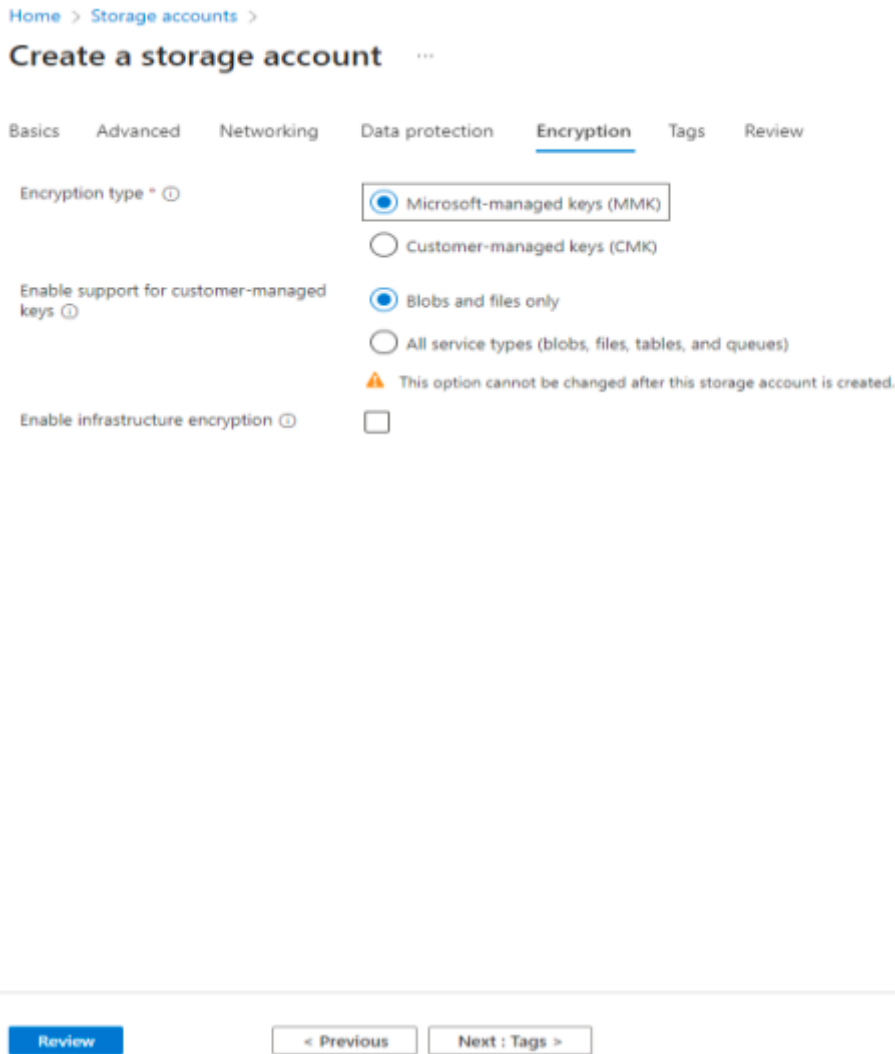
- Enable version-level immutability support  
Allows you to set time-based retention policy on the account-level that will apply to all blob versions. Enable this feature to set a default policy at the account level. Without enabling this, you can still set a default policy at the container level or set policies for specific blob versions. Versioning is required for this property to be enabled. [Learn more](#)

[Review](#)

[< Previous](#)

[Next : Encryption >](#)

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.

## Create a storage account ...

Basics   Advanced   Networking   Data protection   Encryption   Tags   Review

### Basics

Subscription	Azure subscription 1
Resource Group	CyTech_ResourceGroup
Location	eastus
Storage account name	<del>cytechstorage001</del>
Deployment model	Resource manager
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

### Advanced

Enable hierarchical namespace	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Enabled
Access tier	Hot
Enable SFTP	Disabled
Large file shares	Disabled

### Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing
Endpoint type	Standard





### Security

Secure transfer	Enabled
-----------------	---------

[Create](#)   [< Previous](#)   [Next >](#)   [Download a template for automation](#)

## Resources

Recent   Favorite

Name	Type	Last Viewed
 CyTech <del>storage001</del>	Event Hubs Namespace	40 minutes ago
 CyTech <del>storage001</del>	Resource group	14 hours ago
 cytech <del>storage001</del>	Storage account	14 hours ago
 Azure subscription 1	Subscription	15 hours ago

[See all](#)

## 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**

## Diagnostic setting

Save Discard Delete Feedback

Diagnostic setting name \*

Logs	Destination details
<b>Categories</b>	<input type="checkbox"/> Send to Log Analytics workspace
<input checked="" type="checkbox"/> AuditLogs	<input type="checkbox"/> Archive to a storage account
<input checked="" type="checkbox"/> SignInLogs	<input checked="" type="checkbox"/> Stream to an event hub
<input checked="" type="checkbox"/> NonInteractiveUserSignInLogs	
<input checked="" type="checkbox"/> ServicePrincipalSignInLogs	For potential partner integrations, click to learn more about event hub integration.
<input checked="" type="checkbox"/> ManagedIdentitySignInLogs	Subscription: Azure subscription 1
<input checked="" type="checkbox"/> ProvisioningLogs	Event hub namespace *: CyTechEventHub
<input checked="" type="checkbox"/> ADPSSignInLogs	Event hub name (optional): cytech
<input checked="" type="checkbox"/> RiskyUsers	Event hub policy name: RootManageSharedAccessKey
<input checked="" type="checkbox"/> UserRiskEvents	<input type="checkbox"/> Send to partner solution
<input checked="" type="checkbox"/> NetworkAccessTrafficLogs	
<input checked="" type="checkbox"/> RiskyServicePrincipals	
<input checked="" type="checkbox"/> ServicePrincipalRiskEvents	
<input checked="" type="checkbox"/> EnrichedOffice365AuditLogs	
<input checked="" type="checkbox"/> MicrosoftGraphActivityLogs	

## 2. Event Hub Credentials

### 3. Go to > EventHub Resources > Select Shared Access Policies

## CyTechEventHub | Shared access policies

- Search
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Events
- Settings
  - Shared access policies
  - Scale
  - Geo-Recovery
  - Encryption
  - Configuration
  - Properties
  - Locks
- Entities
  - Event Hubs
- Monitoring
  - Alerts
  - Metrics
  - Diagnostic settings
  - Logs
- Automation
  - Tasks (preview)

Policy	Claims
RootManageSharedAccessKey	Manage, Send, Listen

**copy this and provide to CyTech**

## SAS Policy: RootManageSharedAccessKey

Save Discard Delete Regenerate Primary Key

Manage

Send

Listen

Primary key: [Redacted]

Secondary key: [Redacted]

Connection string-primary key: [Redacted]

Connection string-secondary key: [Redacted]

SAS Policy ARM ID: [Redacted]

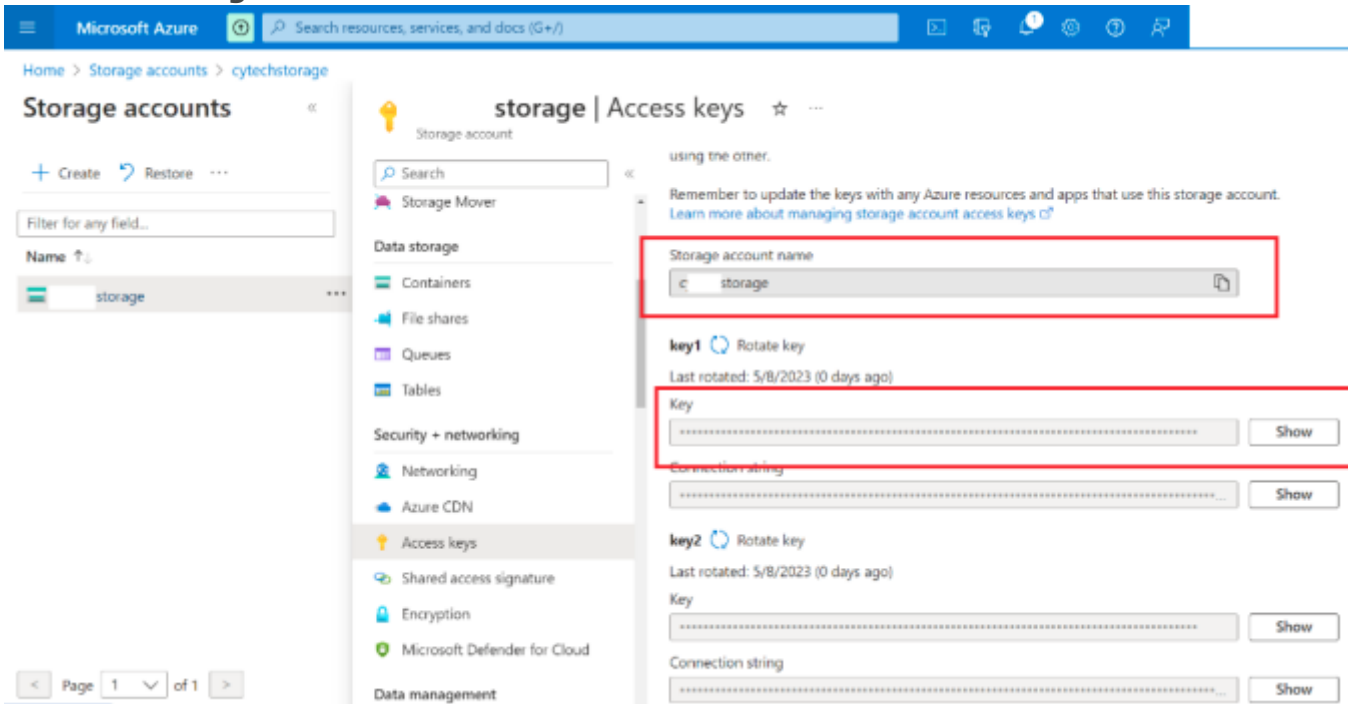
## CyTechEventHub | Event Hubs

- Search
- Diagnose and solve problems
- Events
- Settings
  - Shared access policies
  - Scale
  - Geo-Recovery
  - Encryption
  - Configuration
  - Properties
  - Locks
- Entities
  - Event Hubs

Name	Status	Manage-operations	Partition
cytech	Active	1 hour	2

**Go to your event hub and go to entities and provide the Event Hubs Name**

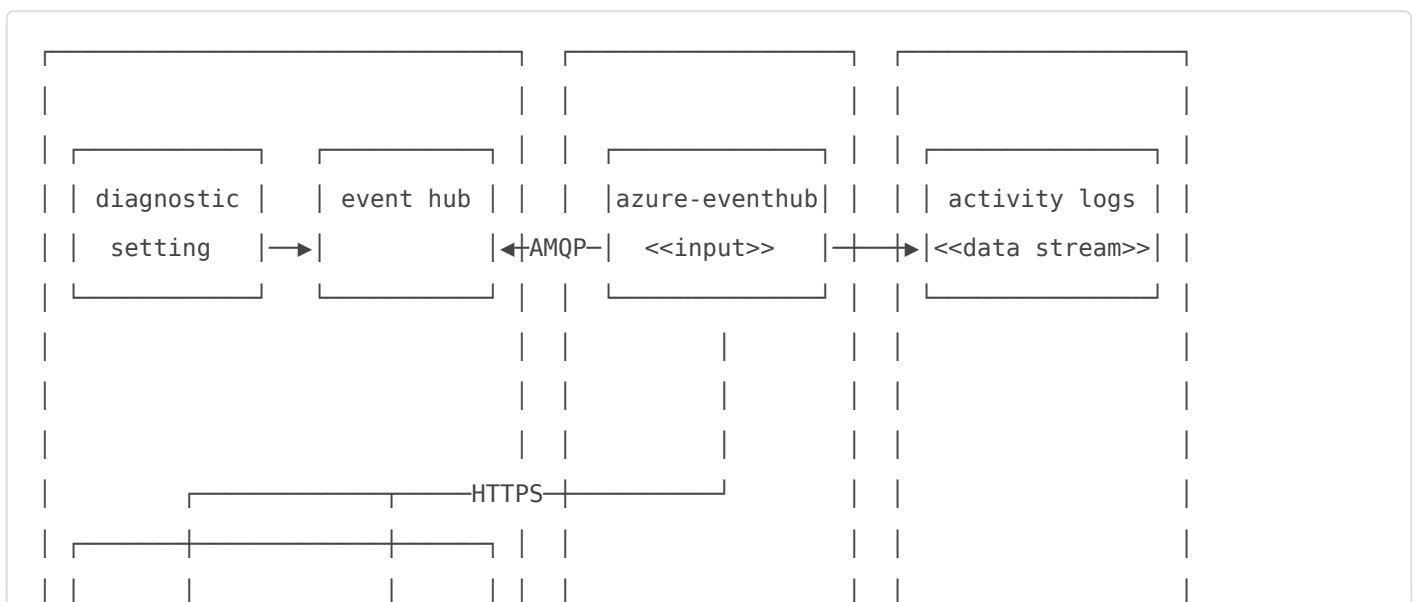
4. **Please provide CyTech the:**
  - a. Event Hubs Name Not the Name Space:
  - b. Connection string-primary key:
5. **Account Storage Credentials**



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](mailto: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