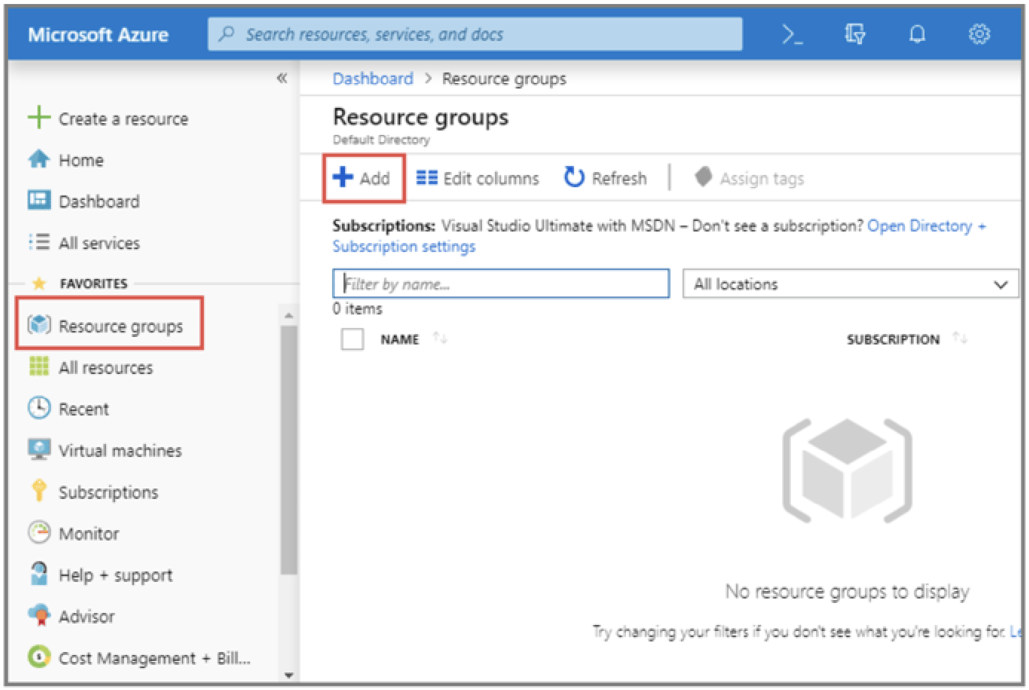
# SOC Management Azure Integration

## Event Hub Creation

1. Log into your Azure Portal.

2. Select "Resource Group" from the left-hand menu and click "Add" at the top of the page.

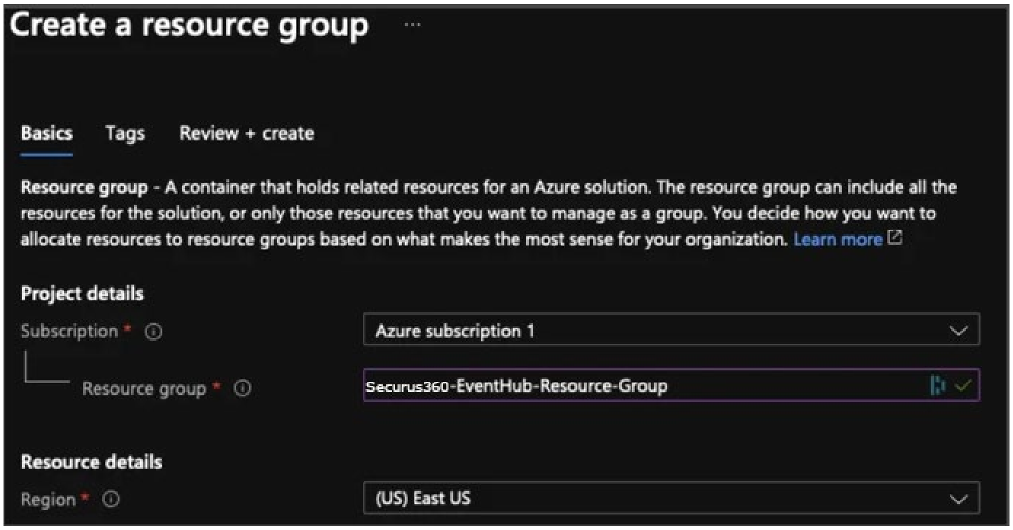


**Subscriptions:** Visual Studio Ultimate with MSDN – Don't see a subscription? Open Directory + Subscription settings

No resource groups to display

Try changing your filters if you don't see what you're looking for. L

3. Select the correct subscription and region, then give the Group a unique name.



**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

**Project details**

Subscription * : Azure subscription 1

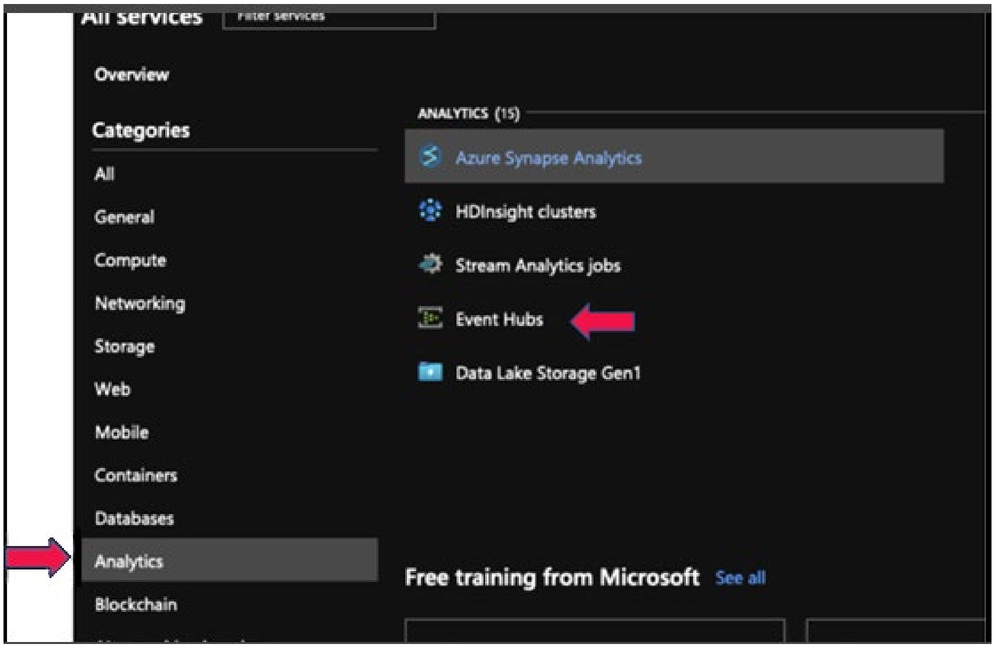
Resource group * : Securus360-EventHub-Resource-Group

**Resource details**

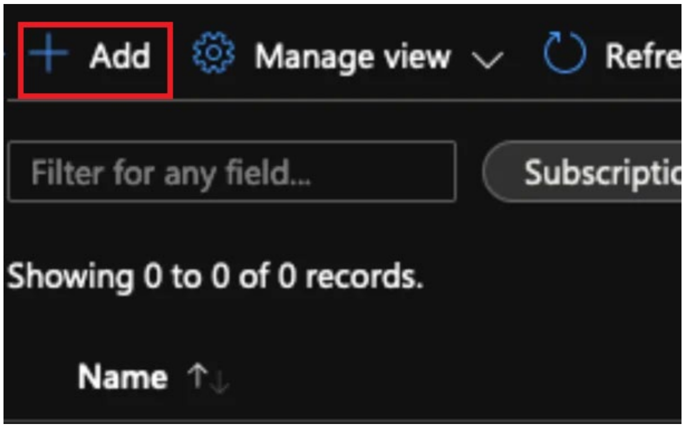
Region * : (US) East US

4. Click on "Create Tags" and then "Review and Create."
   a. Tag creation is optional.

5. With the Resource Group created, proceed to **"All Services"** and select **Analytics** to create the **Event Hub** Name Space.

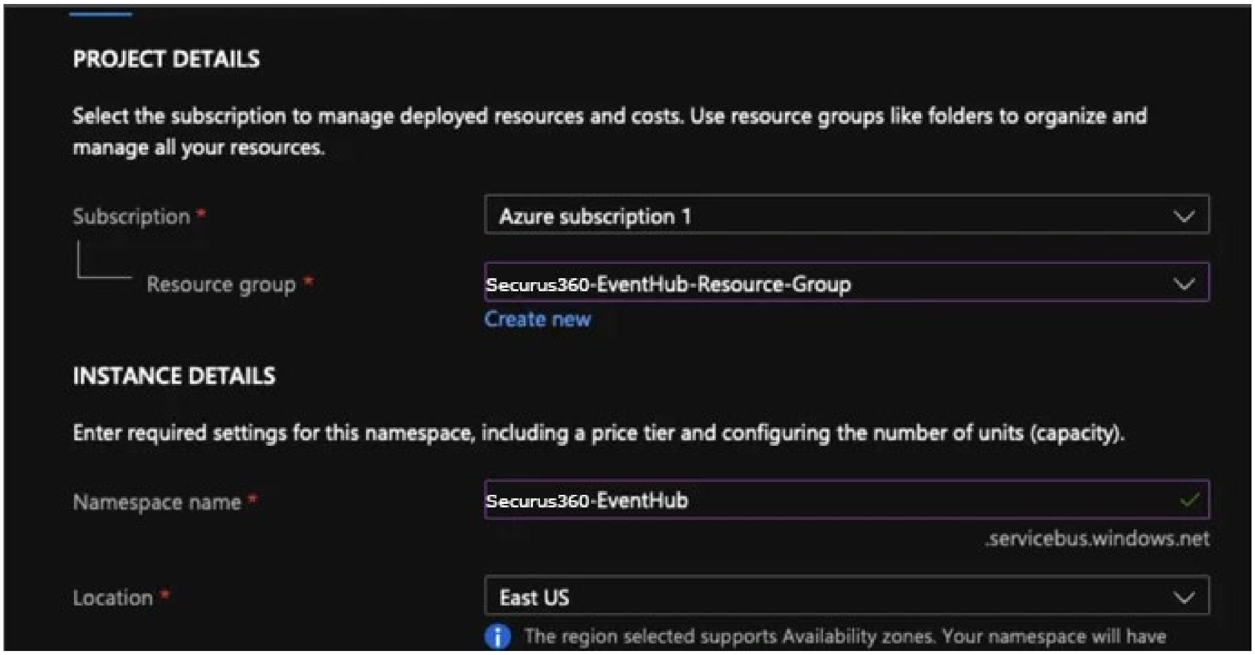


6. Click "Add" in the upper left-hand portion of the screen under Event Hubs.



Showing 0 to 0 of 0 records.

7. Give the Event Hub the previously-created Resource Group and provide a name for the Name Space. For Pricing, **Basic** or **Standard** are acceptable.



PROJECT DETAILS

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

Subscription * Azure subscription 1

Resource group * Securus360-EventHub-Resource-Group

INSTANCE DETAILS

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

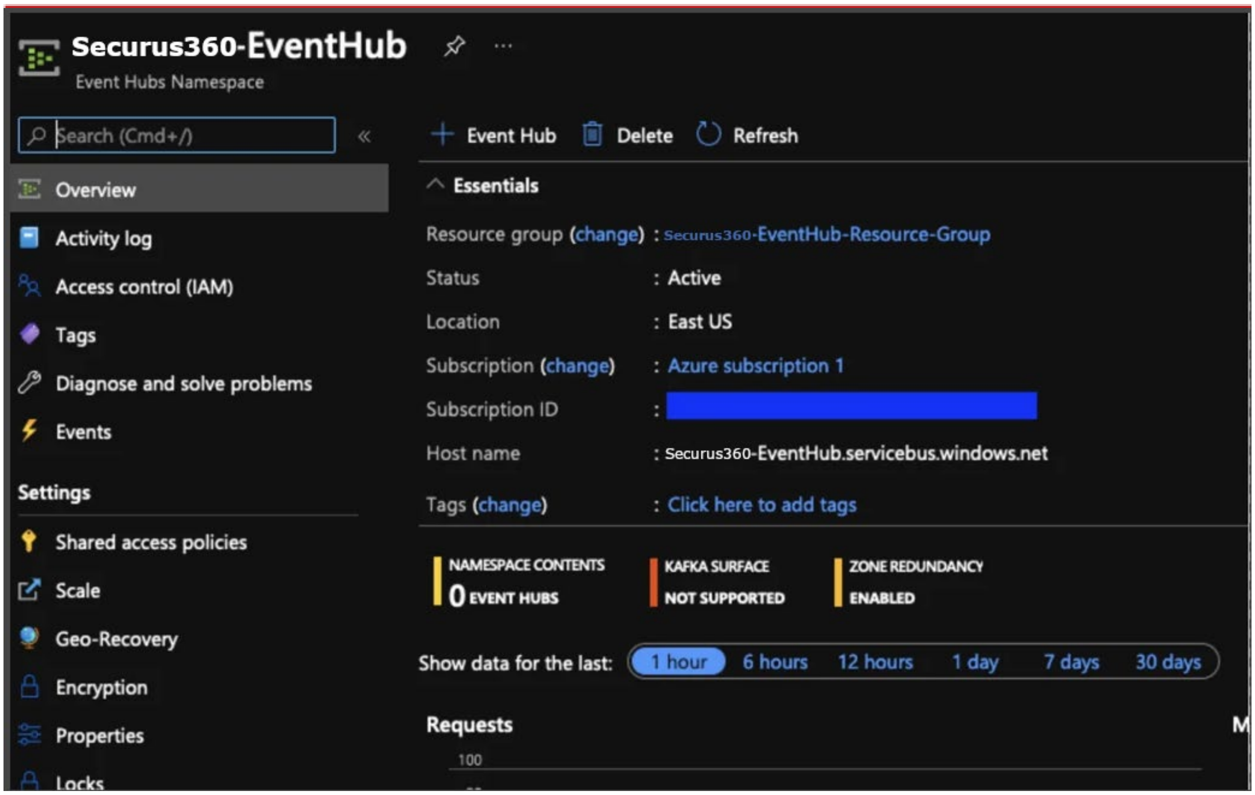
Namespace name * Securus360-EventHub .servicebus.windows.net

Location * East US

The region selected supports Availability zones. Your namespace will have

8. Click "Review + Create" and then "Create" when the hub is validated, or click "Next" if tags need to be created, then proceed to review and create and wait for deployment to complete.

9. Once the deployment is finished, click "Go to resource" and verify the namespace is properly created.



Resource group (change) : Securus360-EventHub-Resource-Group

Status : Active

Location : East US

Subscription (change) : Azure subscription 1

Subscription ID : [redacted]

Host name : Securus360-EventHub.servicebus.windows.net

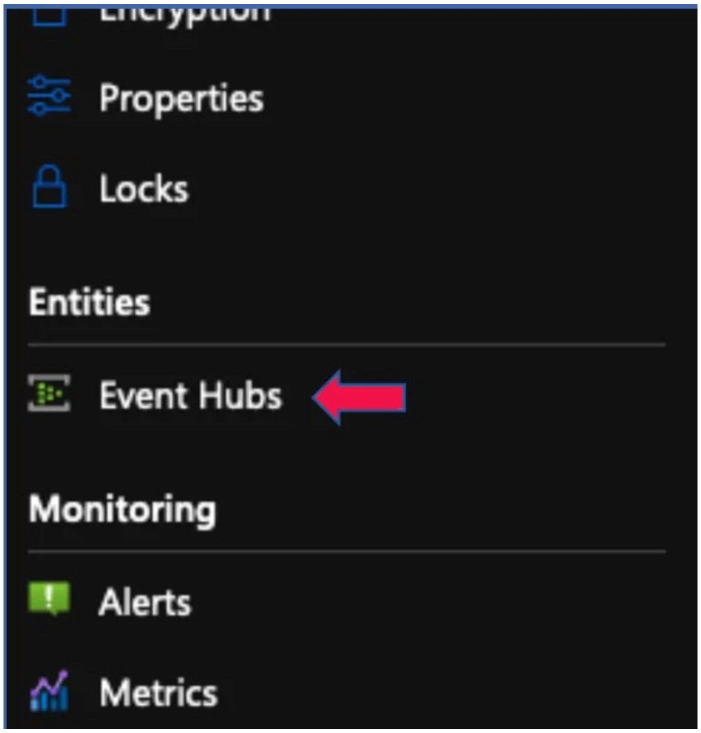
Tags (change) : Click here to add tags

NAMESPACE CONTENTS 0 EVENT HUBS

KAFKA SURFACE NOT SUPPORTED

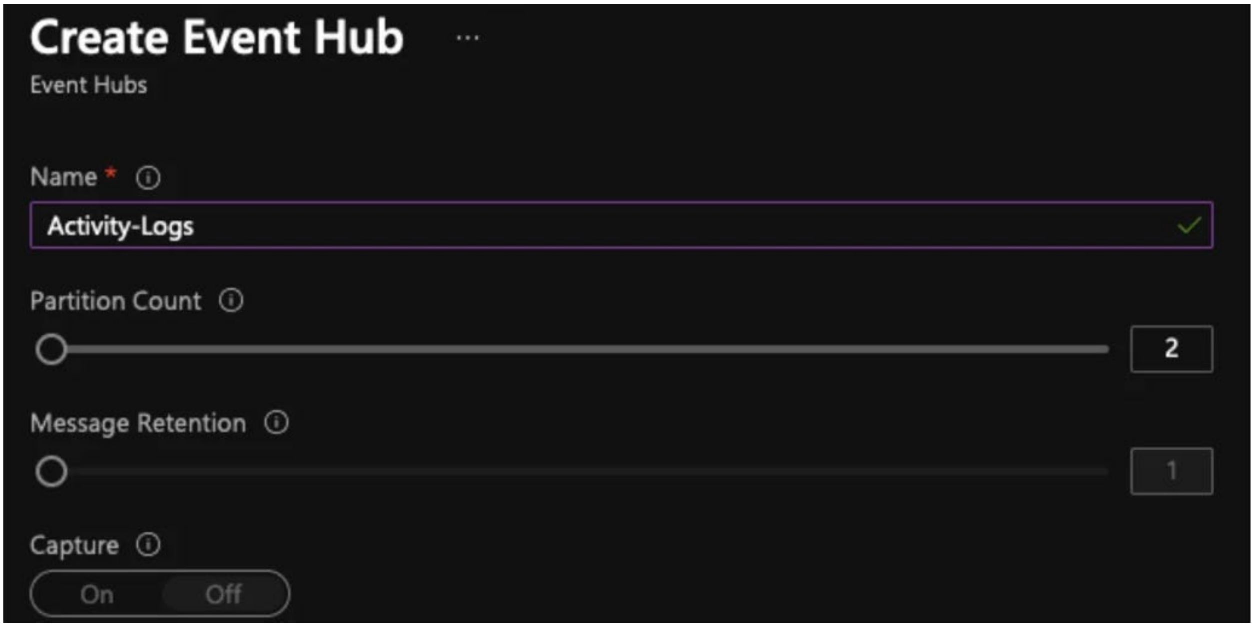
ZONE REDUNDANCY ENABLED

10. Now that the name space is created, proceed to create the event hub for log collection.



11. Once on the Event-Hubs page, click "+ Event Hub"
    a. These steps will be repeated for:
        i. Activity Logs
        ii. Sign-in Logs/Audit Logs
        iii. Optional – Platform Logs
        iv. Optional – Endpoint Logs

12. Provide the name of the event hub.



Create Event Hub ...

Event Hubs

Name * ⓘ

Activity-Logs ✓

Partition Count ⓘ

2

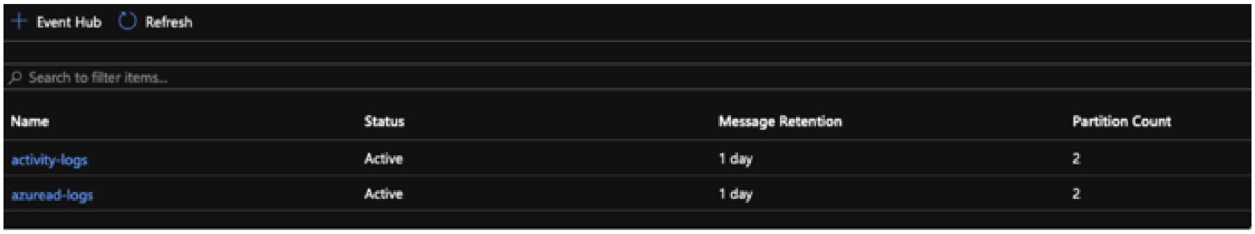
Message Retention ⓘ

1

Capture ⓘ

On Off

13. Once the hubs have been completed, the list should look similar to the image below.
    a. AzureAD-Logs will contain the logs for Audit and Sign-In

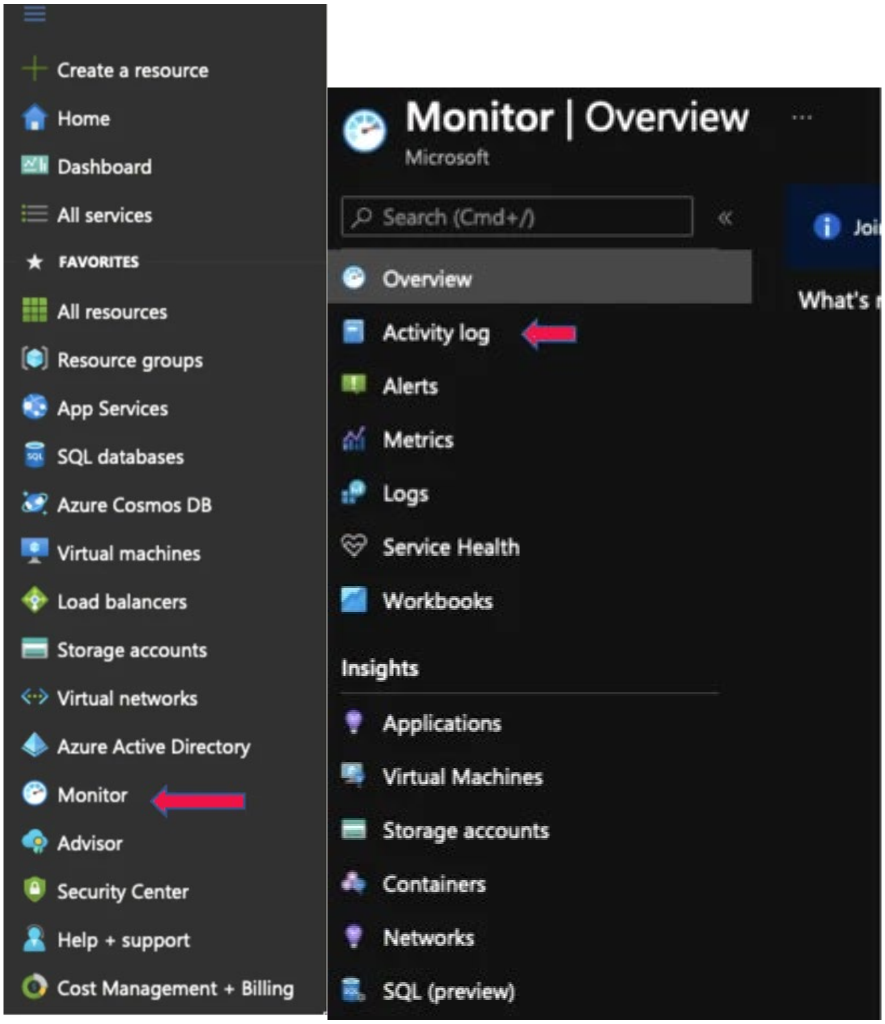


| Name | Status | Message Retention | Partition Count |
|---|---|---|---|
| activity-logs | Active | 1 day | 2 |
| azuread-logs | Active | 1 day | 2 |

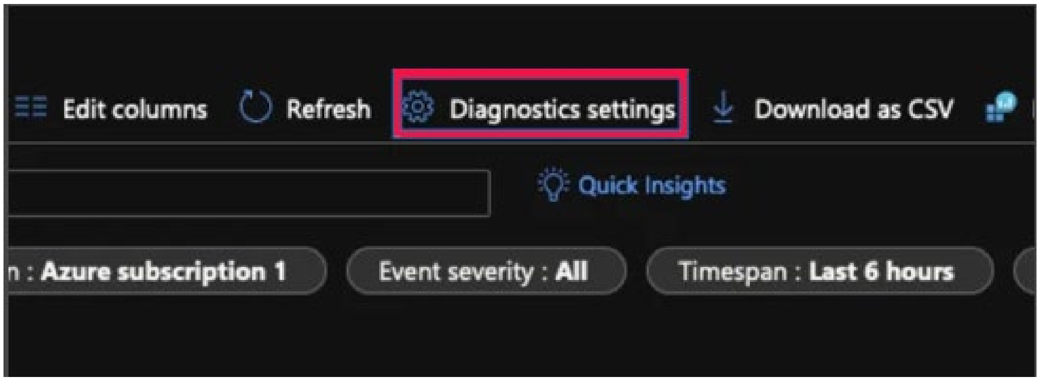
14. Now that the event hubs have been created, the next step is to export data to the Hubs.

## Activity Logs

1. Go to "Monitor" (left-hand menu) and select "Activity Logs."



2. Once on the activity logs page, click "Diagnostics settings."

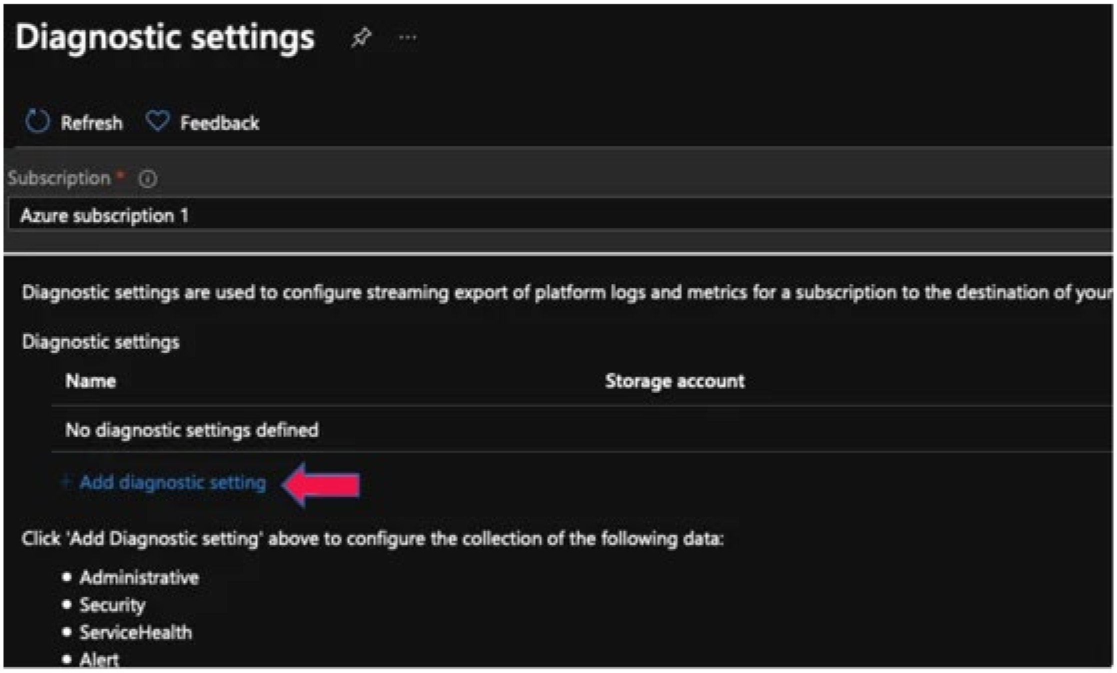


n : Azure subscription 1

Event severity : All

Timespan : Last 6 hours

3. Select the subscription that was used for the creation of the Event Hub Name Space and then select "+ Add diagnostic setting".



Diagnostic settings

Subscription *

Azure subscription 1

Diagnostic settings are used to configure streaming export of platform logs and metrics for a subscription to the destination of your

Diagnostic settings

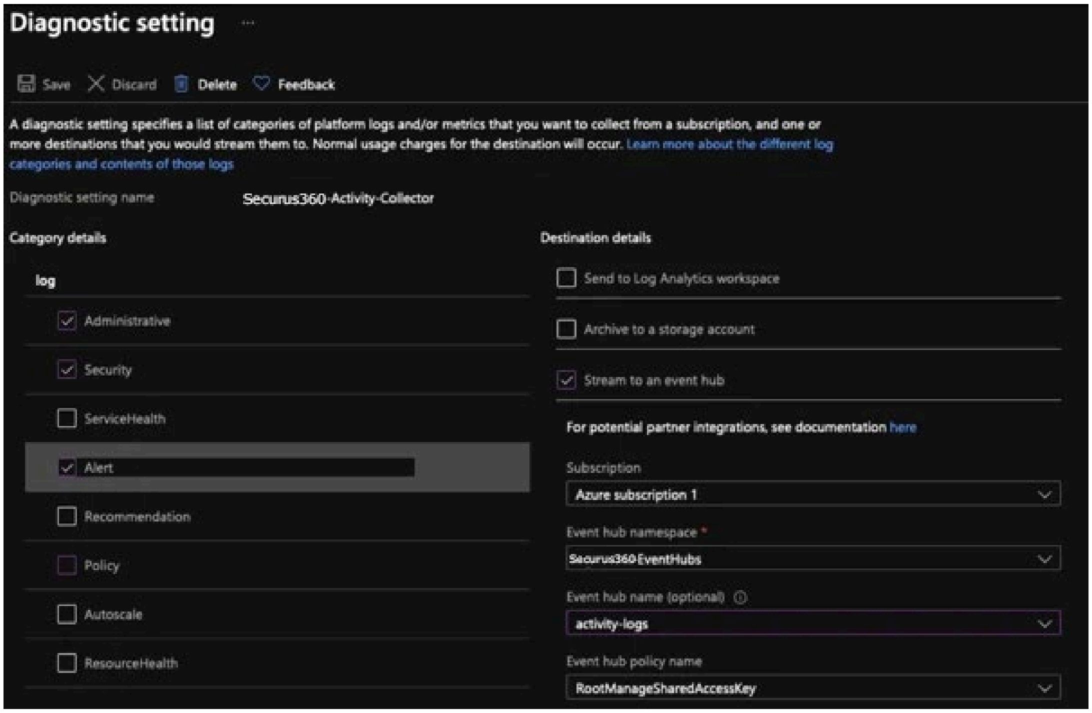
| Name | Storage account |
|---|---|
| No diagnostic settings defined | |

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Administrative
- Security
- ServiceHealth
- Alert

4. Select the required settings for the collection of Activity Logs as displayed in the image below.



Diagnostic setting

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a subscription, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name: Securus360-Activity-Collector

Category details

log

- ☑ Administrative
- ☑ Security
- □ ServiceHealth
- ☑ Alert
- □ Recommendation
- □ Policy
- □ Autoscale
- □ ResourceHealth

Destination details

- □ Send to Log Analytics workspace
- □ Archive to a storage account
- ☑ Stream to an event hub

For potential partner integrations, see documentation here

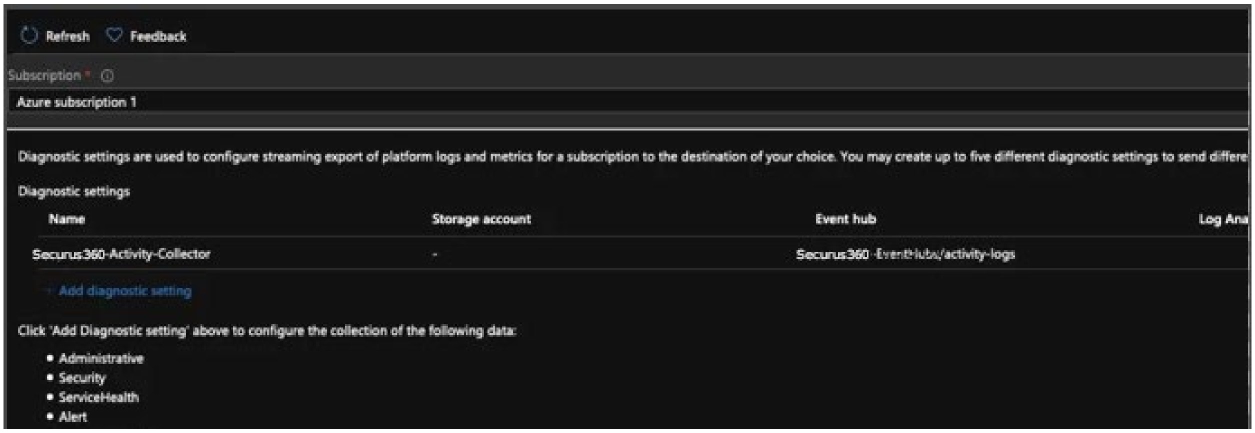
Subscription: Azure subscription 1

Event hub namespace *: Securus360EventHubs

Event hub name (optional): activity-logs

Event hub policy name: RootManageSharedAccessKey

5. Once the settings are set, click "Save" in the upper left of the screen then go back to the diagnostic settings and confirm the settings are in place.



Subscription *

Azure subscription 1

Diagnostic settings are used to configure streaming export of platform logs and metrics for a subscription to the destination of your choice. You may create up to five different diagnostic settings to send differe

Diagnostic settings

| Name | Storage account | Event hub | Log Ana |
|---|---|---|---|
| Securus360-Activity-Collector | - | Securus360-EventHubs/activity-logs | |

Click 'Add Diagnostic setting' above to configure the collection of the following data:

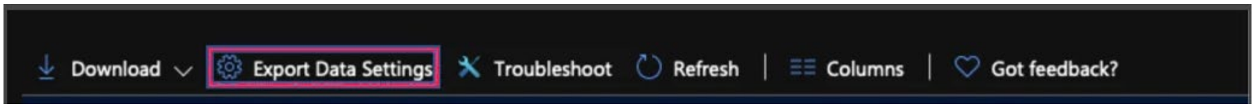
- Administrative
- Security
- ServiceHealth
- Alert

## Sign-In/Audit Logs

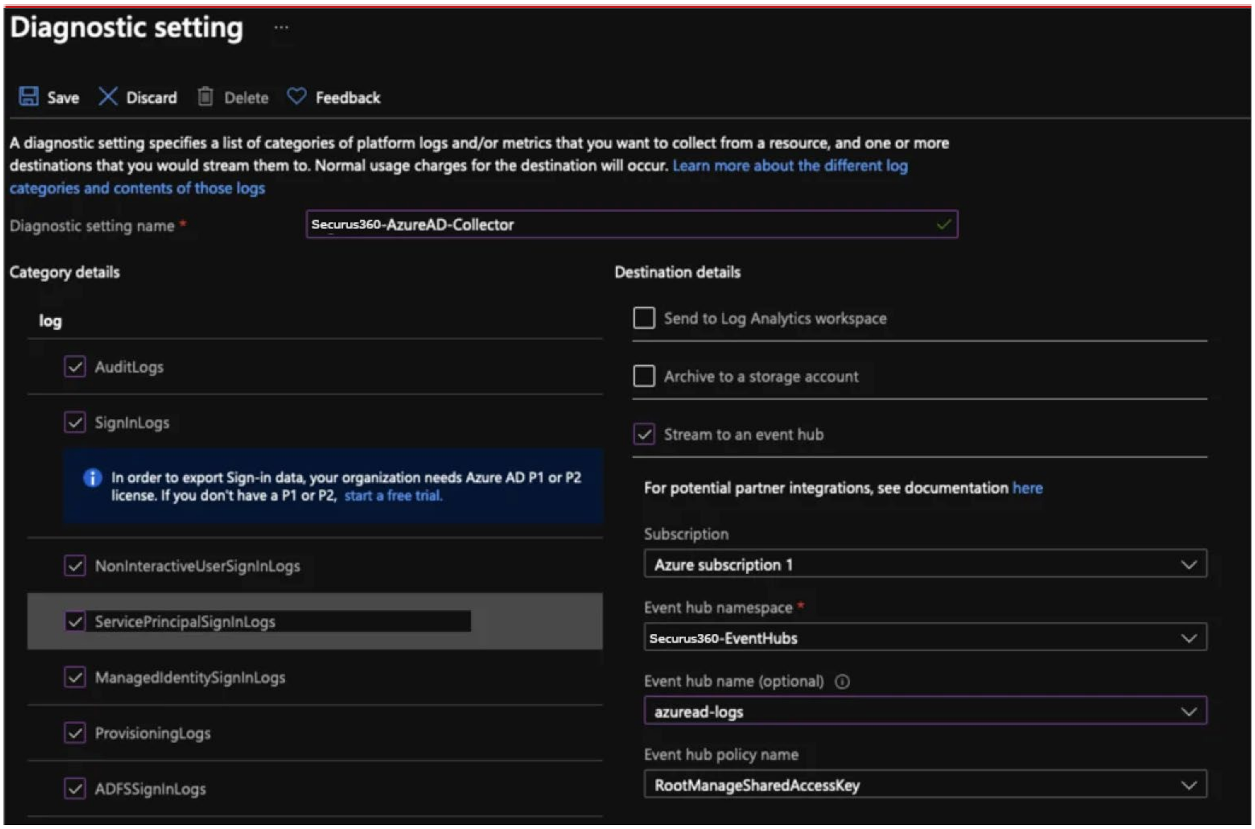
1. Go to "Azure Active Directory" in the left-hand menu.

2. Select "Sign-ins."

3. Go to "Export Data Settings" in the top left of the screen.



4. Proceed to set the diagnostic settings to reflect the image below.



Diagnostic setting ...

Save | Discard | Delete | Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * Securus360-AzureAD-Collector

Category details

log

☑ AuditLogs

☑ SignInLogs

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

☑ NonInteractiveUserSignInLogs

☑ ServicePrincipalSignInLogs

☑ ManagedIdentitySignInLogs

☑ ProvisioningLogs

☑ ADFSSignInLogs

Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☑ Stream to an event hub

For potential partner integrations, see documentation here

Subscription: Azure subscription 1

Event hub namespace *: Securus360-EventHubs

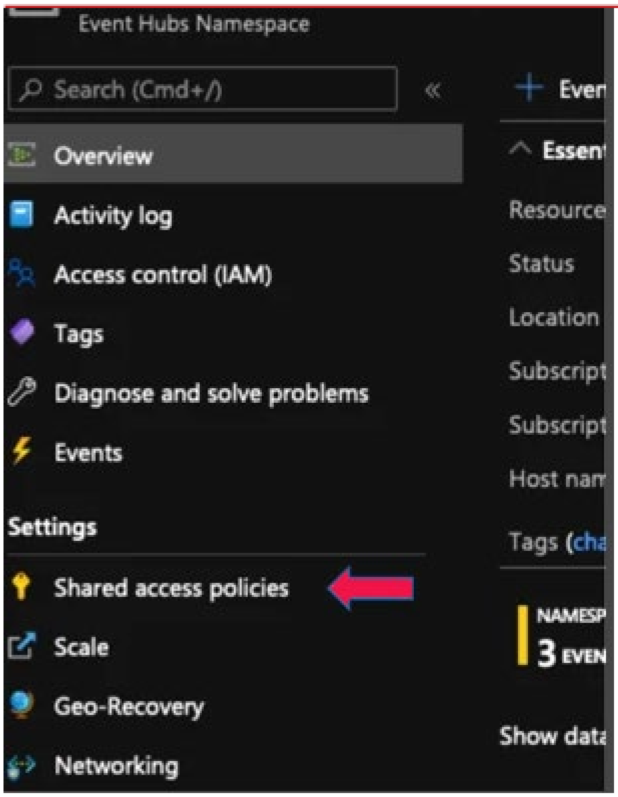
Event hub name (optional): azuread-logs

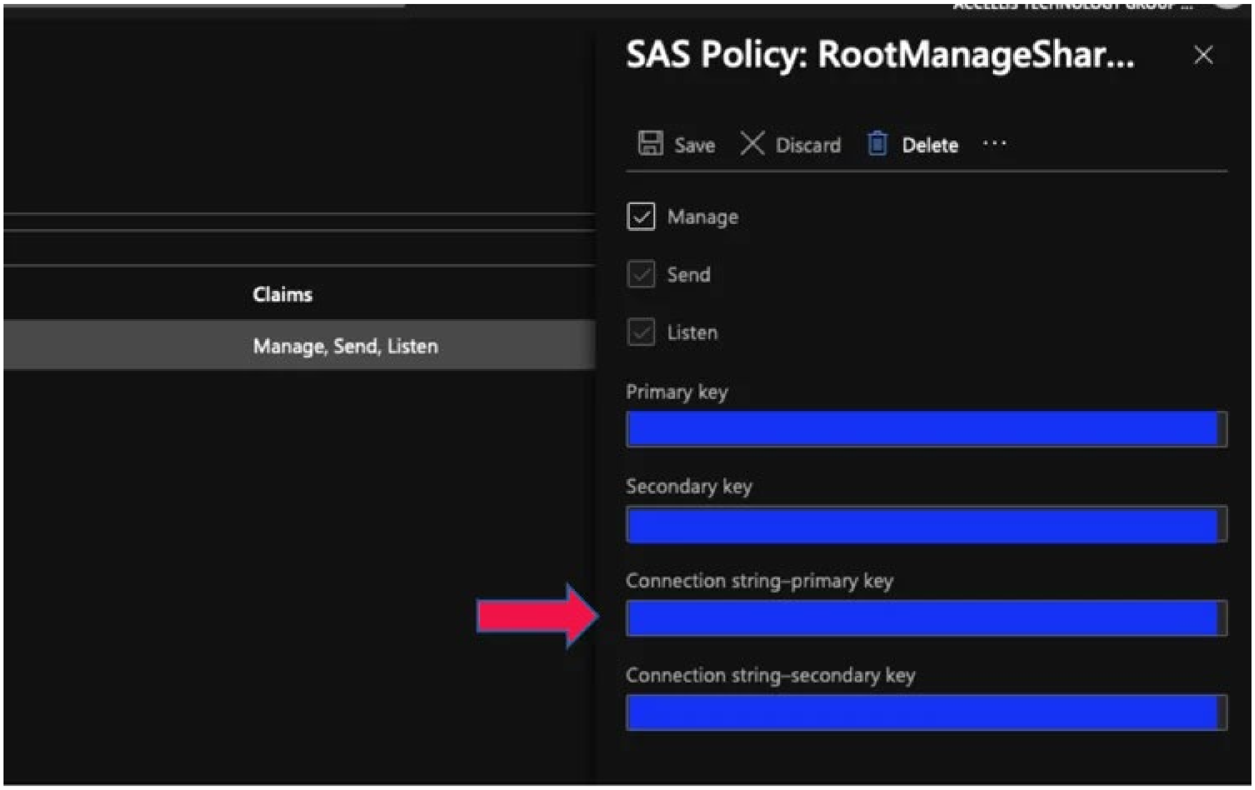
Event hub policy name: RootManageSharedAccessKey

## Required Information

Below is the information Seucurs360 requires in order for the collector to be able to connect to the Event Hubs and retrieve data.

1. Event Hub Connection String
   a. This can be found in the Event Hub NameSpace under "Shared Access Policies."
   b. Then select "RootManageSharedAccessKey" and copy the connection string-primary key, which will be sent back to Securus360




SAS Policy: RootManageShar...

| Claims |
|---|
| Manage, Send, Listen |

☑ Manage

☑ Send

☑ Listen

Primary key

[redacted]

Secondary key

[redacted]

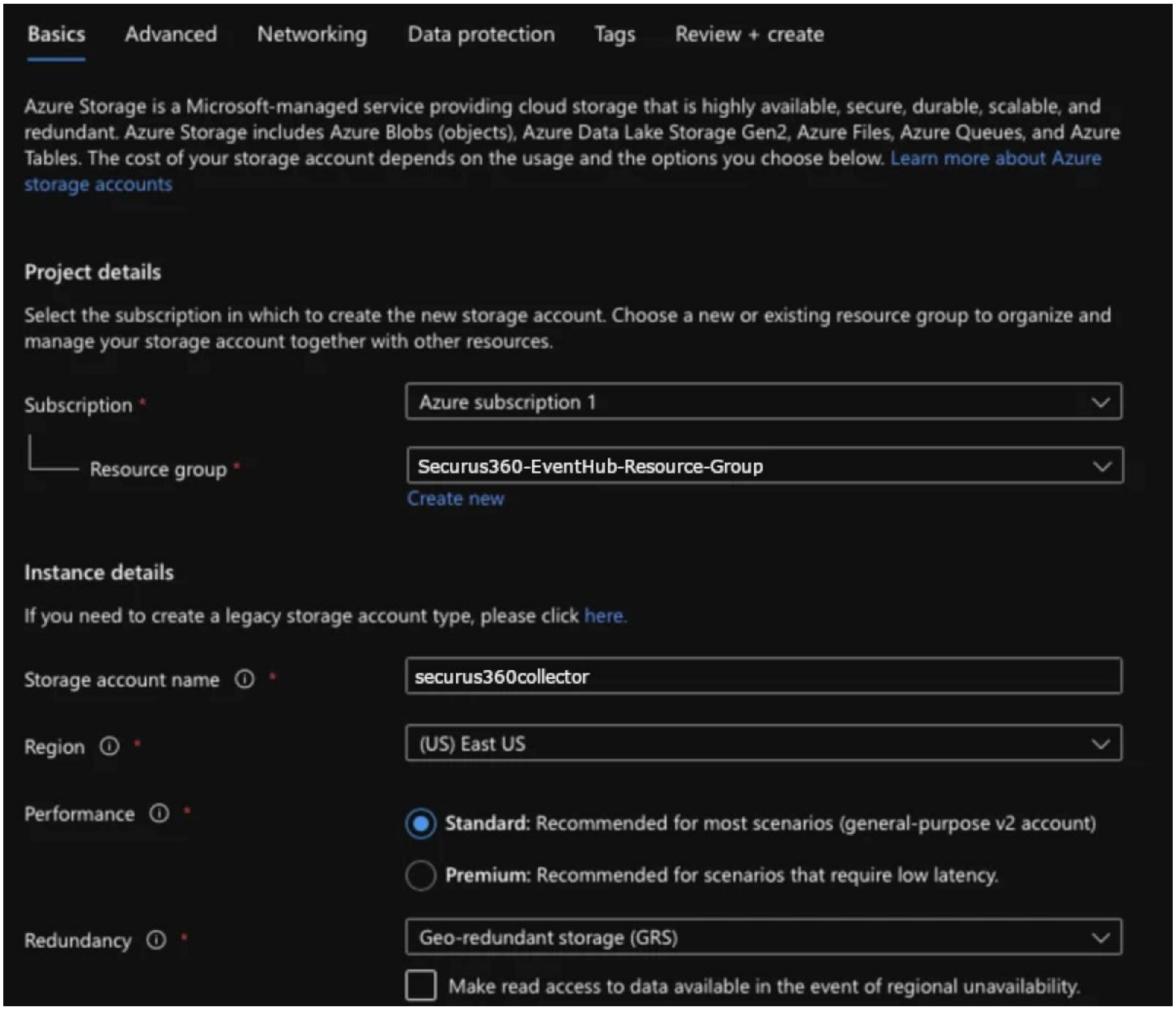
Connection string–primary key

[redacted]

Connection string–secondary key

[redacted]

2. Storage Account
    a. In order to allow the collector to keep track of the events, a storage account is needed in order to allow write back.
    b. To create a storage account, go to All Services > Storage > Storage Accounts.
    c. Then select "Create Storage Account" and use the settings reflected below.



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 *: Azure subscription 1

Resource group *: Securus360-EventHub-Resource-Group

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name *: securus360collector

Region *: (US) East US

Performance *:

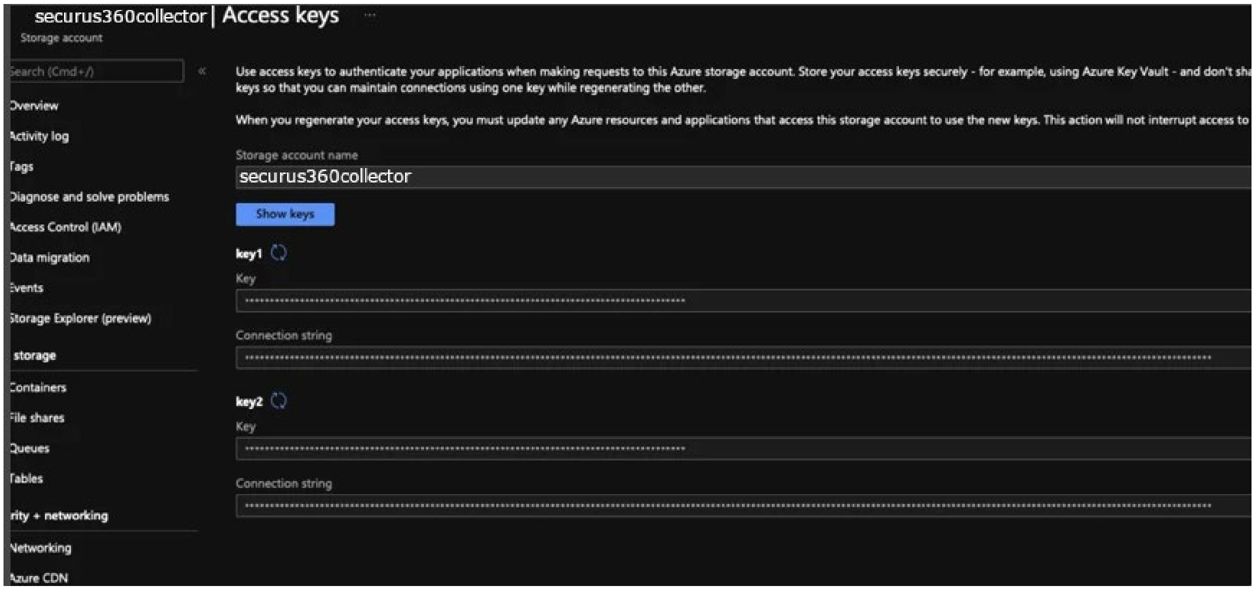
● Standard: Recommended for most scenarios (general-purpose v2 account)

○ Premium: Recommended for scenarios that require low latency.

Redundancy *: Geo-redundant storage (GRS)

□ Make read access to data available in the event of regional unavailability.

d. Click "Review Create".
e. Proceed to review the setup storage account and go to "Access Keys".
f. Here, you will need to copy the storage account name and the values in key1.



securus360collector | Access keys

Storage account

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't sha keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to

Storage account name: securus360collector

key1
Key
Connection string

key2
Key
Connection string

3. Securus360 will also need the event hub names (not the name of the event hub namespace).

4. Once complete, please upload the requested items to the Sharepoint link provided by Securus360:

   - Event Hub Connection String
   - Event Hub Names (not the name of the event hub namespace).
   - RootManageSharedAccessKey

5. Then send an email to support@securus360.com to let us know that it has been successfully uploaded. Securus360 will confirm we have received the file as quickly as possible. After we confirm receipt, you can then opt to securely delete the file from wherever it was saved locally, such as an internal disk or a flash drive.