

*n*Lighten™

Azure Event Hub Logging

This solution requires the use of **Azure Event Hub** for the activity, sign-in, and/or audit logs, as well as access to a **storage blob**. If you do not have such an event hub set up, please refer to the [Create an Azure event hub quick start](#) documentation for details. You will then need to refer to the [instructions on sending activity logs](#) to the event hub.

1. From your Azure portal [Event Hub](#), select the event hub to monitor. Click **Shared access policies**.

Click the default policy that appears, named **RootManageSharedAccessKey** and then click to copy the Connection string-primary. This will be sent to Cybraics.

SAS Policy: Ro

Save × Discard

Manage

Send

Listen

Primary key
ItnGqj5rkn4LlkXUafe7IMf

Secondary key
4BCzZfm6Ofx0G3ZQbDlu

Connection string-primary
Endpoint=sb://eh-diag-p

Connection string-second
Endpoint=sb://eh-diag-p

2. Navigate to **Activity Logs** and then click **Diagnostics settings**.

Activity log ✨ ...

Activity Edit columns Refresh Diagnostics settings Download as CSV Logs Pin current filter

Search Quick Insights

Management Group : **None** Subscription : **CDCA Appliance** Event severity : **All** Timespan : **Last 6 hours**

Click **Add diagnostic setting** and name it `cybraics-diagnostic`. Under Log select **Administrative, Security, Alert**.

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 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 * ✓

Category details

log

Administrative

Security

ServiceHealth

Alert

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

Choose **Stream to an event hub** and select the corresponding subscription, event Hub and event Hub policy name previously created.

Destination details

Send to Log Analytics

Archive to a storage account

Stream to an event hub

For potential partner integrations, see documentation [here](#)

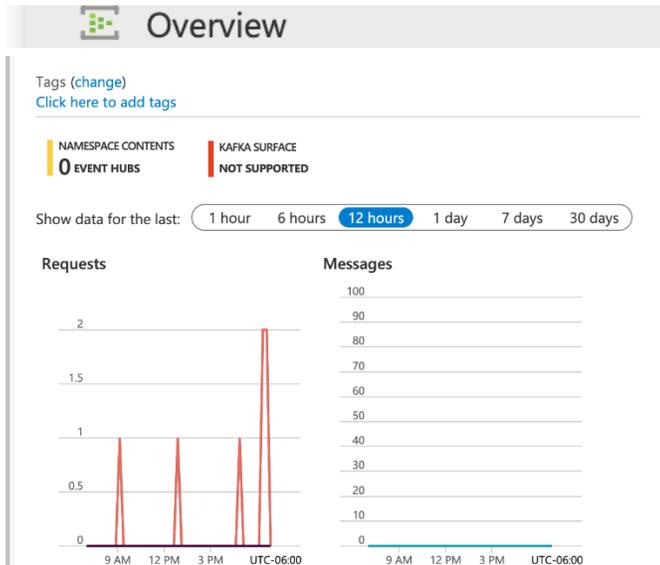
Subscription

Event hub namespace *

Event hub name (optional) ⓘ

Event hub policy name

Click **Save**, then optionally navigate back to **event hub** to see the event metrics coming in under the **Overview** section.



- Next, we need to create a storage account. A storage account is used to store a record of messages in the event of a system outage. A public IP is needed and whitelisted with Cybraics IP address. If this is not permitted in your environment, we can implement a private solution. Navigate to **Storage accounts** and create a new one.

Create a unique name and corresponding region. **Standard** and **Locally-redundant storage (LRS)** **Create a storage account** ...

Basics Advanced Networking Data protection Tags Review + create

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 field can contain only lowercase letters and numbers. Name must be between 3 and 24 characters.

Region ⓘ *

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

Redundancy ⓘ *

Under **Networking** select Public endpoint (all networks)

Create a storage account ...

Basics • Advanced **Networking** Data protection Tags Review + create

Network connectivity

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

Connectivity method *

- Public endpoint (all networks)
- Public endpoint (selected networks)
- Private endpoint
- i All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. [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

Select the newly created storage account, **Networking** → **Firewalls and virtual networks**.
Choose **Select networks** and restrict to 18.218.9.120

<<

Firewalls and virtual networksPrivate endpoint connectionsCustom domain

SaveDiscardRefresh

Allow access from

All networks Selected networks

i Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

| Virtual Network | Subnet | Address range | Endpoint Status |
|----------------------|--------|---------------|-----------------|
| No network selected. | | | |

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

Add your client IP address ('76.120.51.20') ⓘ

Address range

| | |
|--------------|--------------------------------------|
| 18.218.9.120 | 🗑️ |
|--------------|--------------------------------------|



Send the following parameters to Cybraics via encrypted email.

Eventhub name containing the activity logs

eventhub: "eh-cybraics"

Consumer group name that has access to the event hub.

consumer_group: "\$Default"

The connection string required to communicate with Event Hubs

connection_string: "Endpoint=sb://myconnection.servicebus.windows.net/;SharedAccessKeyName=mykey;SharedAccessKey=1234zklr7bPyFR0cH28gKiGDwzRLRJ5ZjnvCZxqITk="

The name of the storage account the state/offsets will be stored and updated

storage_account: "sa-cybraics"

The storage account key, this key will be used to authorize access to data in your storage account

storage_account_key: "1234667T8yiw2Vg0jth9R39IvYw1vechg3TUtMYMpP7TZND+9IUxrAhF9nrNkx0Bi7Ybw6rQuV06wcasadSd=="