CYBRAICS

nLighten™

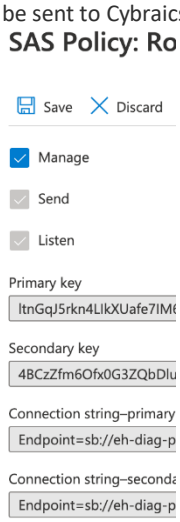
Azure Event Hub Logging

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.

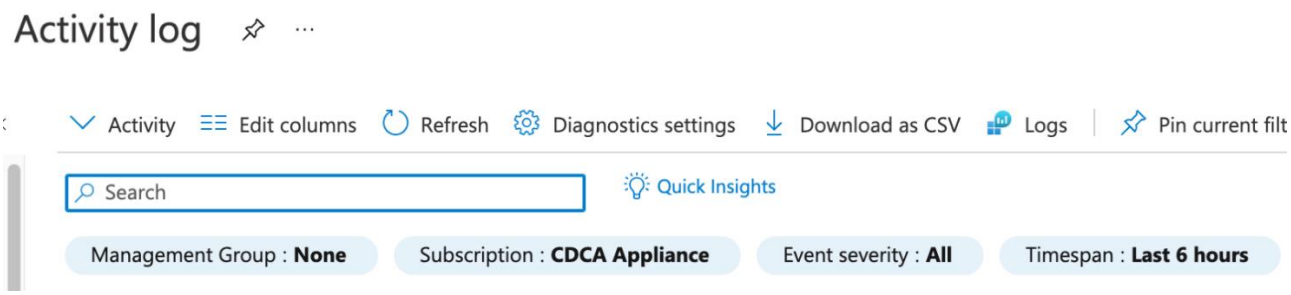
1. From your Azure portal Event Hub, select the event hub to monitor.

Click **Shared access policies**.

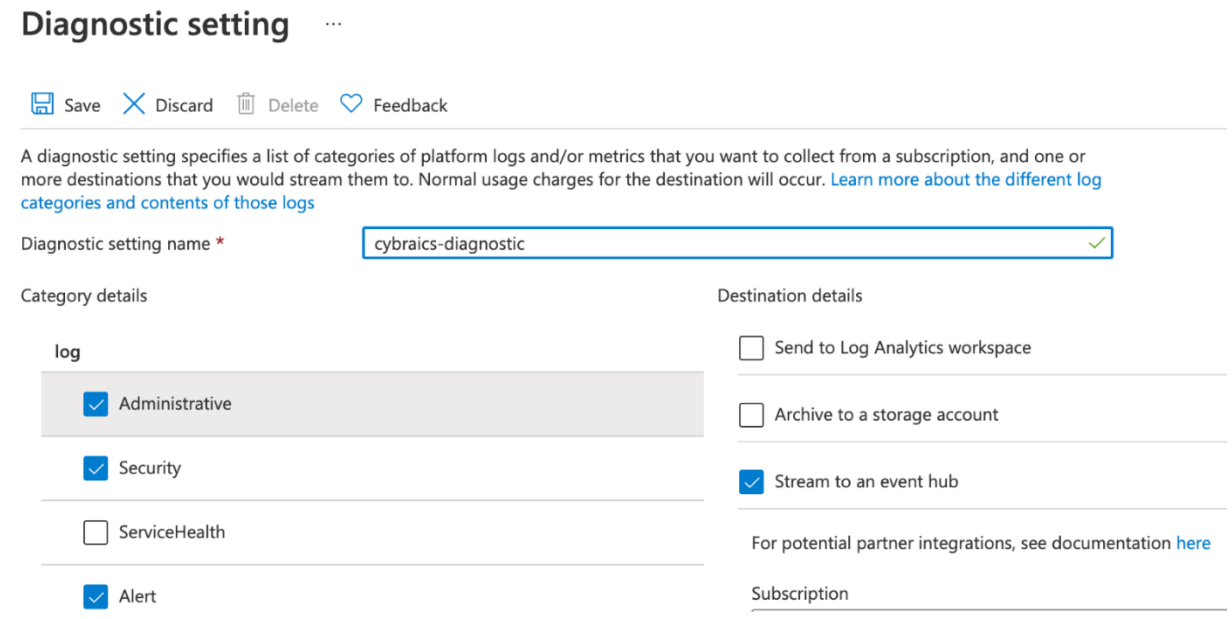
Click the default policy that appears, named **RootManageSharedAccessKey** and then click to copy the Connection string-primary. This will be sent to Cybraics.



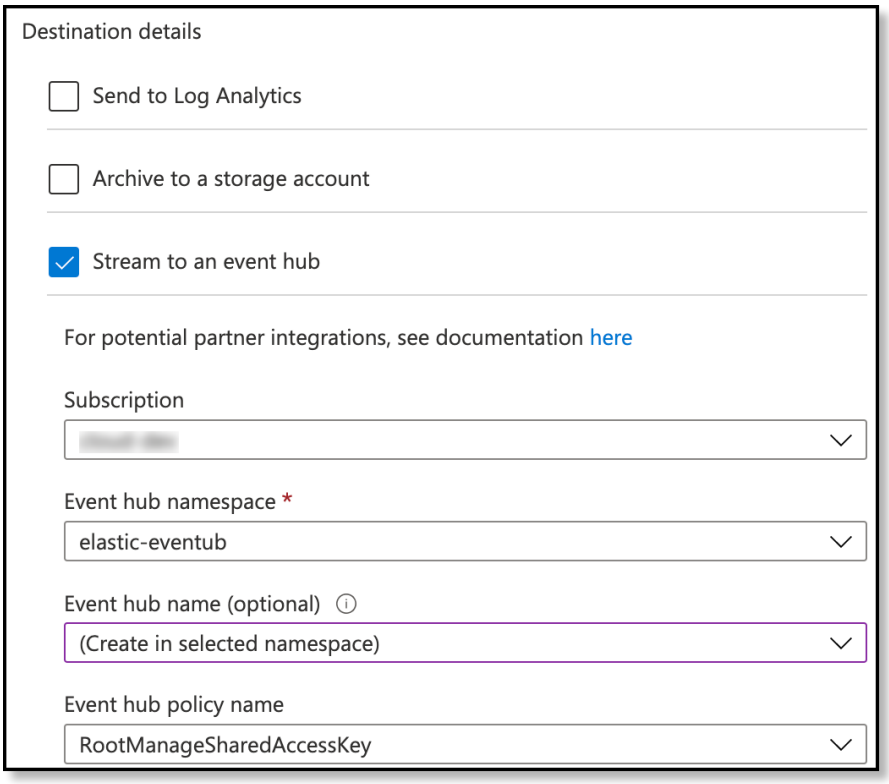
2. Navigate to **Activity Logs** and then click **Diagnostics settings**.



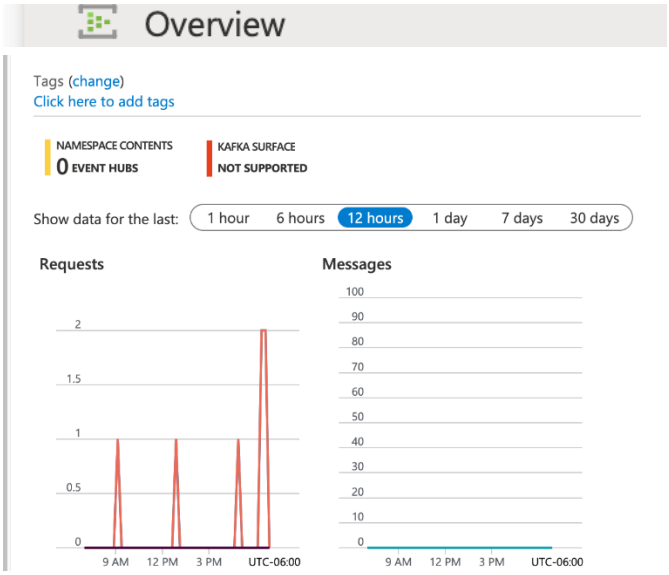
Click **Add diagnostic setting** and name it cybraics-diagnostic. Under Log select **Administrative, Security, Alert**.



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

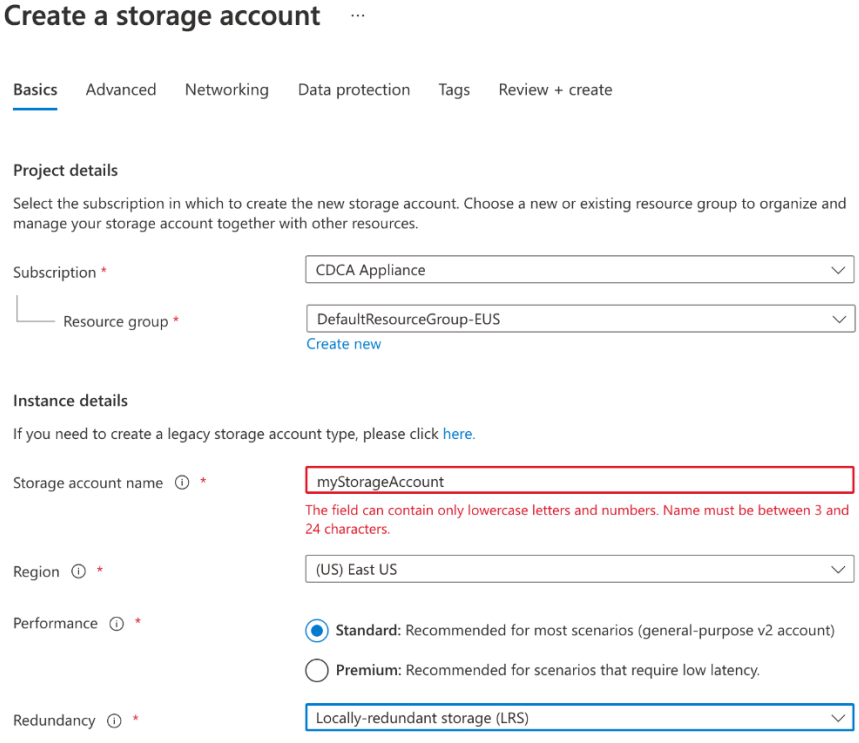


Click **Save,** then optionally navigate back to **event hub** to see the event metrics coming in under the **Overview** section.

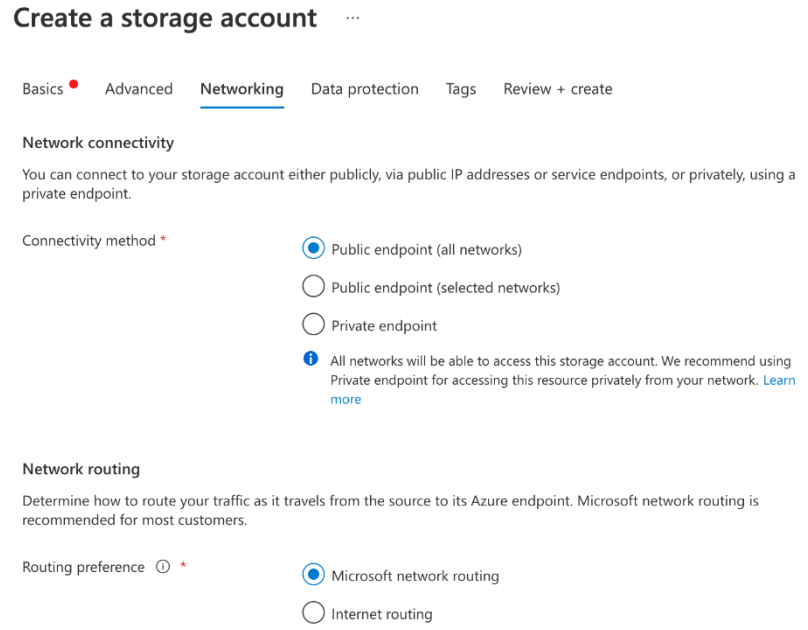


3. Next, we need to create a storage account. A storage account is used to store a record of messages in the event of a system outage. A public IP is needed and whitelisted with Cybraics IP address. If this is not permitted in your environment, we can implement a private solution. Navigate to **Storage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

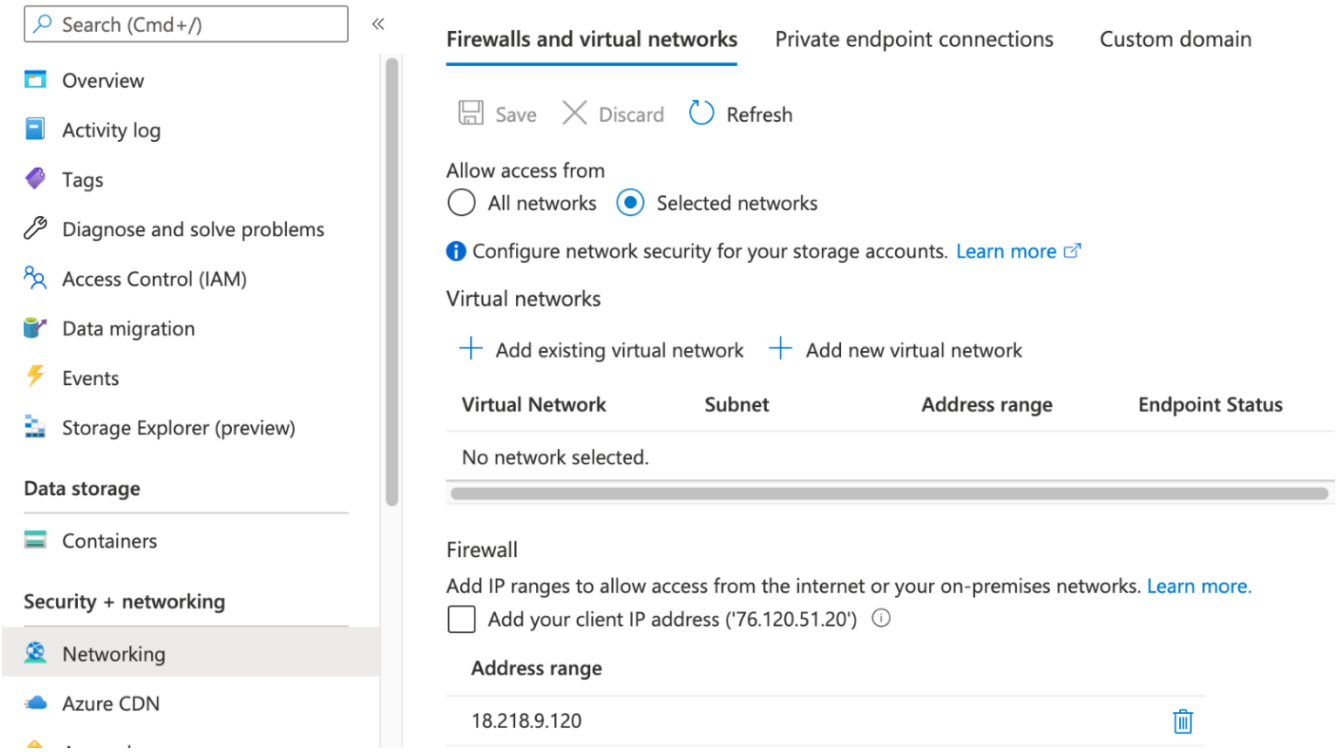
Create a unique name and corresponding region. **Standard** and **Locally-redundant storage (LRS)**



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



Select the newly created storage account, **Networking → Firewalls and virtual networks.**
Choose **Select networks** and restrict to 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=1234zkpLr7bPyFR0cH28gKiGDwzRLRJ5ZjnvCZxqlTk="

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+9IUxrAhF9nrNkxoBi7Ybw6rQuV06wcasadSd=="