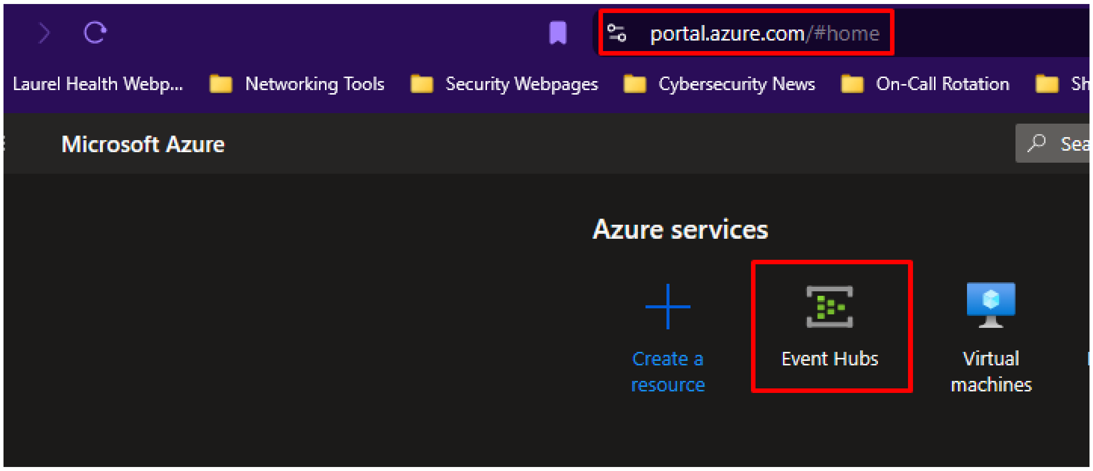
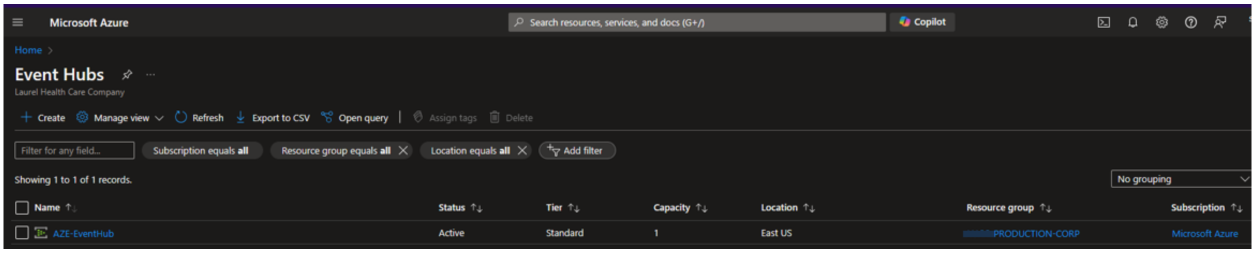
AZE-EventHub Configuration on InsightIDR Documentation

- Azure Event Hubs as a centralized service to collect data and logs from other Azure services.
- AZE-Event Hubs is connected to a collector that was installed on KodeDC1 (10.33.1.94).
- IDR-AzureShareAccessKey: p/mc9IOSUC7hzgy989L5m9zLBDp3mivsH+hgfdhsertr

1. Event Hub can be found at *https://portal.azure.com/#home*

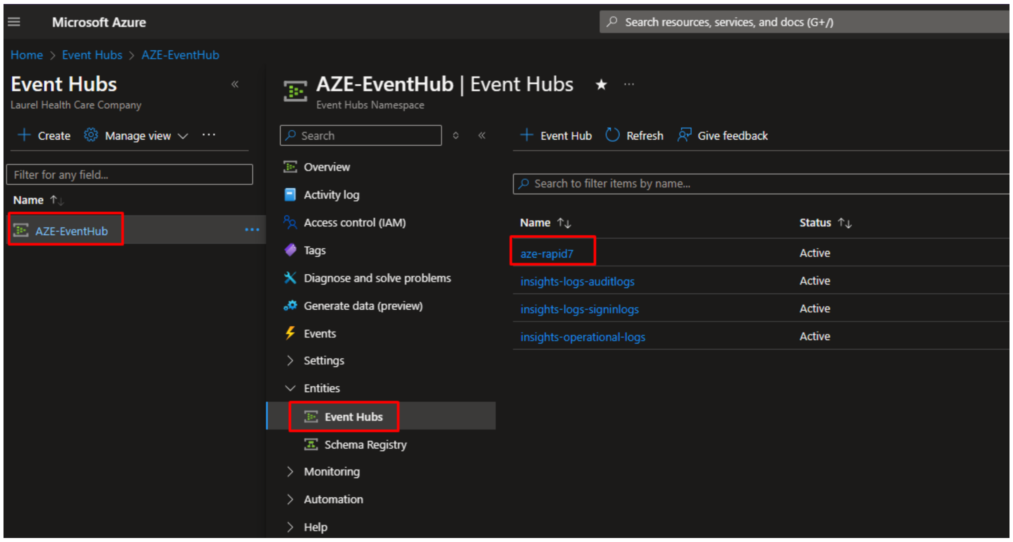




Showing 1 to 1 of 1 records.

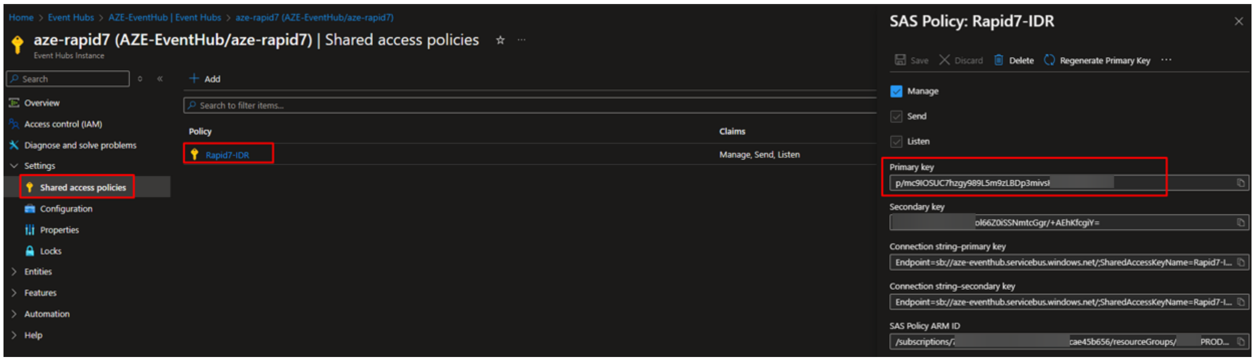
Name	Status	Tier	Capacity	Location	Resource group	Subscription
AZE-EventHub	Active	Standard	1	East US	[redacted]PRODUCTION-CORP	Microsoft Azure

2. Under Entity > Events Hubs > aze-rapid7



Name	Status
aze-rapid7	Active
insights-logs-auditlogs	Active
insights-logs-signinlogs	Active
insights-operational-logs	Active

3. Go to Share access policies. The Shared Access Policies key is the “Primary Key”



Home > Event Hubs > AZE-EventHub | Event Hubs > aze-rapid7 (AZE-EventHub/aze-rapid7)

aze-rapid7 (AZE-EventHub/aze-rapid7) | Shared access policies

Event Hubs Instance

Policy	Claims
Rapid7-IDR	Manage, Send, Listen

SAS Policy: Rapid7-IDR

☑ Manage

☑ Send

☑ Listen

Primary key

p/mc9IOSUC7hzgy989L5m9zLBDp3mivsl[redacted]

Secondary key

[redacted]ol66Z0iSSNmtcGgr/+AEhKfcgiY=

Connection string–primary key

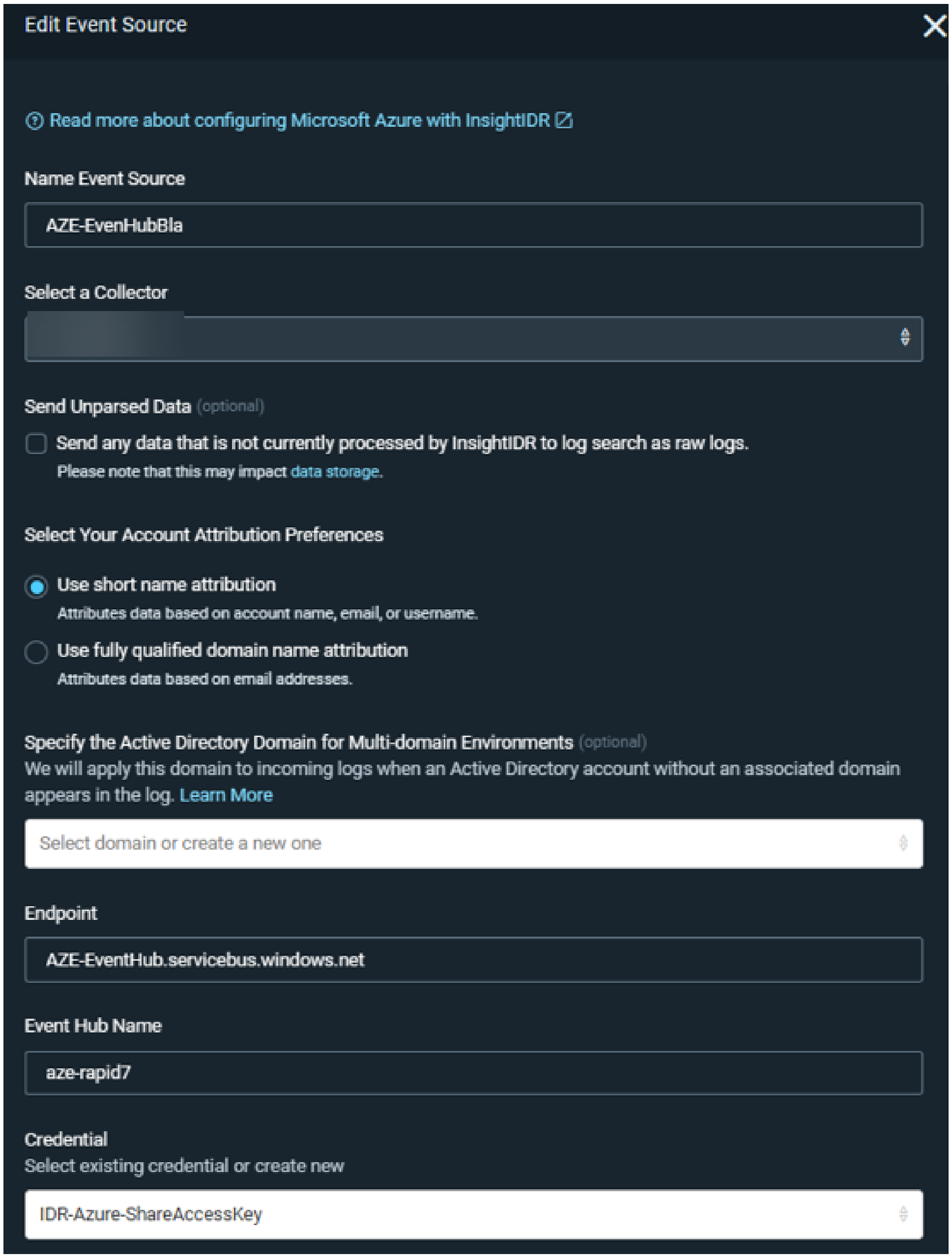
Endpoint=sb://aze-eventhub.servicebus.windows.net/;SharedAccessKeyName=Rapid7-I...

Connection string–secondary key

Endpoint=sb://aze-eventhub.servicebus.windows.net/;SharedAccessKeyName=Rapid7-I...

SAS Policy ARM ID

/subscriptions/[redacted]cae45b656/resourceGroups/[redacted]PROD...



Edit Event Source

Read more about configuring Microsoft Azure with InsightIDR

Name Event Source

AZE-EvenHubBla

Select a Collector

[redacted]

Send Unparsed Data (optional)

□ Send any data that is not currently processed by InsightIDR to log search as raw logs.
Please note that this may impact data storage.

Select Your Account Attribution Preferences

● Use short name attribution
Attributes data based on account name, email, or username.

○ Use fully qualified domain name attribution
Attributes data based on email addresses.

Specify the Active Directory Domain for Multi-domain Environments (optional)
We will apply this domain to incoming logs when an Active Directory account without an associated domain appears in the log. Learn More

Select domain or create a new one

Endpoint

AZE-EventHub.servicebus.windows.net

Event Hub Name

aze-rapid7

Credential
Select existing credential or create new

IDR-Azure-ShareAccessKey

Version	Date	Author	Status	Notes
1.0	07/22/2024	Soklim Seang	Draft	Initial document creation.
1.1				