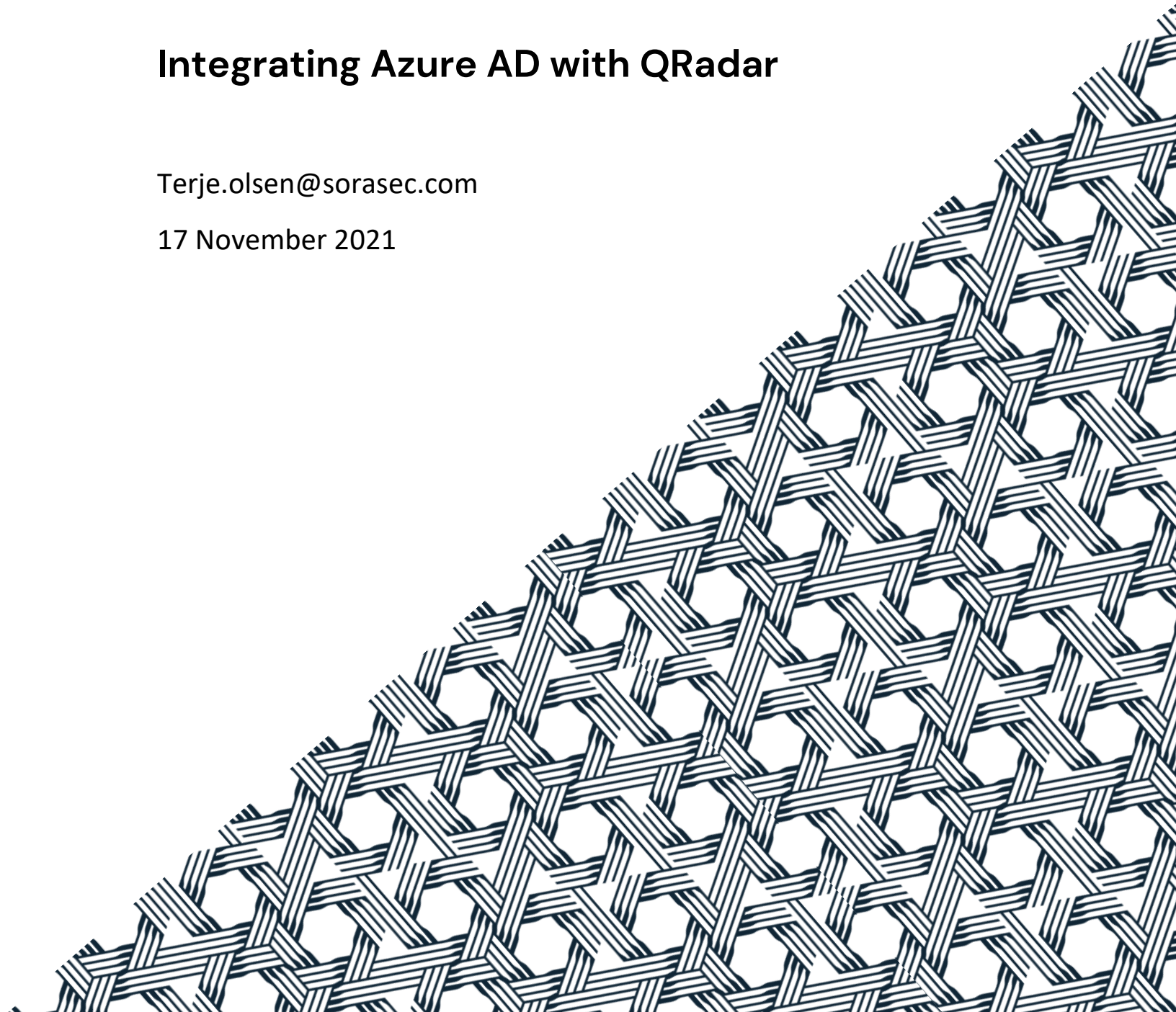
Integrating Azure AD with QRadar

Terje.olsen@sorasec.com

17 November 2021



Contents

Introduction

This article contains step-by-step instructions with screenshots on how to integrate IBM QRadar with Azure Active Directory using supported standard components. The screenshots were valid at the time of writing this article. There is vast amount of information on how to do parts of this integration, however I always end up with multiple pieces of information, articles, browser tabs and a set of Post its to remember the small details. And as always, the devil is in the details.

The following instructions is for demo purposes only and may not be valid in production scaled integrations. I have tried to explain the choices I have made during the preparation of this guide, but sometimes the choice is made for me – and I have not verified why someone else came to their conclusion.

This article comes without warranty and may be used on your own risk. I have done verification of all the steps, but there may be errors in the article. I would be grateful if you inform me about any errors or if you like the article that's always nice to hear.

This article covers specifically Azure Active Directory, however many components in Azure supports streaming events to Event Hub, so the usage of the steps in this guide is wider than just Active Directory. In QRadar there is a generic connector (Protocol) that connects to Azure Event Hubs.

High level tasks:

- Create Azure Event Hubs (Event Hubs Namespace and Event Hubs)
- Create Resource Group
- Create Azure Storage Account
- Configure Azure AD to Stream events to Event Hub
- Configure QRadar to subscribe to your Event Hub

Prerequisites

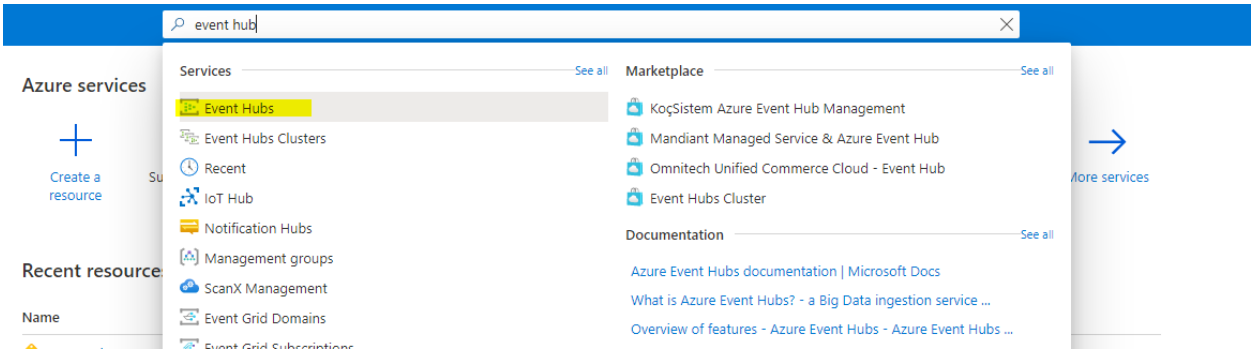
- Azure subscription with administrative rights
- Azure Active Directory
- Up to date QRadar installation with Internet connectivity
- The following Protocols and DSM must be installed:
    - Protocol Common RPM
    - DSM Common
    - Microsoft Azure Event Hubs Protocol RPM
    - Microsoft Azure Platform DSM RPM
    - Microsoft Azure Active Directory DSM RPM

The official IBM documentation on how to integrate QRadar with Azure Active Directory can be found here: https://www.ibm.com/docs/de/dsm?topic=microsoft-azure-active-directory

Create an Azure Event Hub

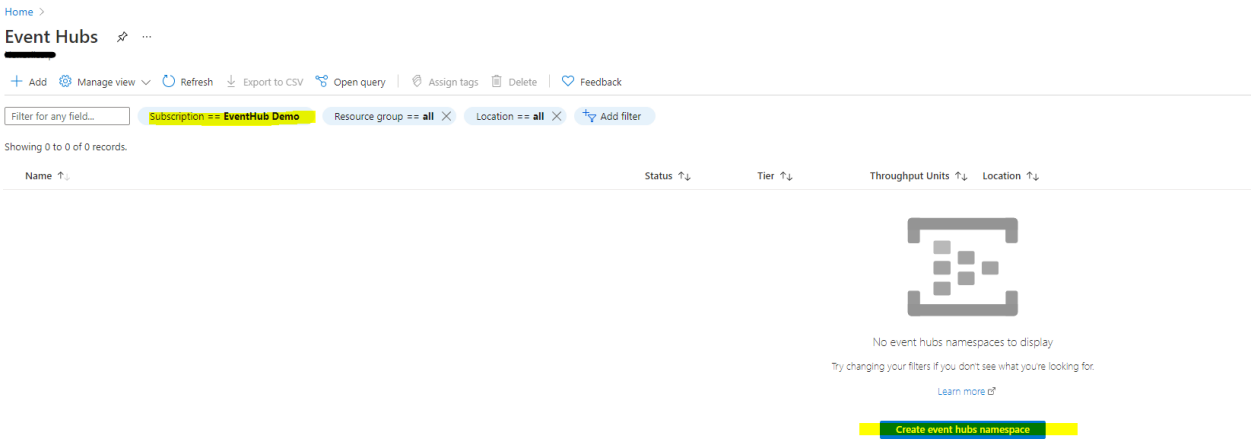
An Event Hub Namespace needs to be created first. Sometimes it's a bit challenging to understand if you have selected an Event Hub Namespace or an Event Hub in the Azure Portal.

Log into your Azure portal and look up the Event Hub service. Click on the Event Hubs icon. (marked in yellow)



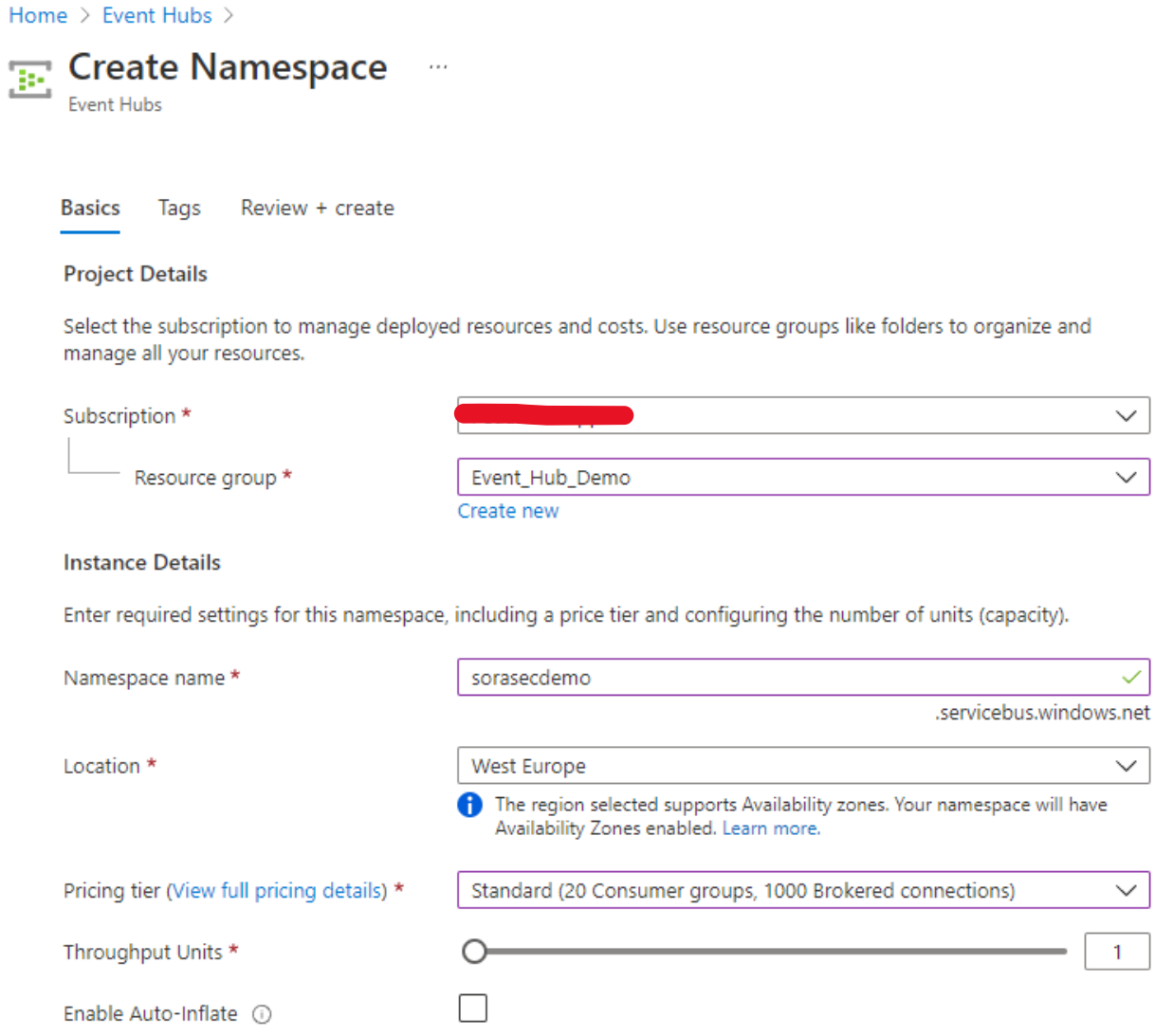
Create an Event Hub namespace

In the example below I have no Event Hubs or Event Hubs namespace. Create an Event Hub namespace first, marked in yellow.



If you are not familiar with the Azure Portal, a lesson learned from my side is to always check if the Subscription filter is set correctly if your organization have more than one Azure subscription.

Select Create an Event Hub Namespace:



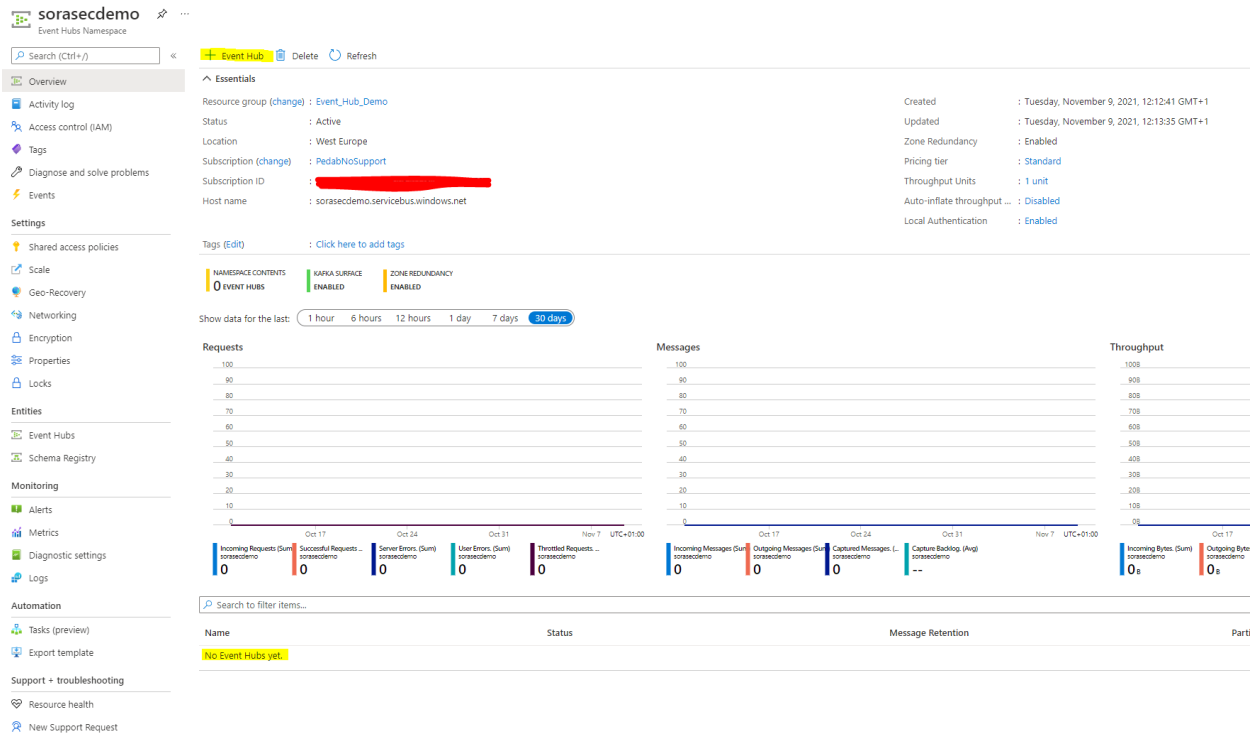
Notes:

- I created a new Resource Group in this Wizard
- Important - Pricing tier: We need more than 1 consumer group. Standard pricing tier is OK for this demo.
- Hit review and create the Event Hub namespace
- The deployment takes a couple of minutes to complete. Verify deployment progress before moving on to the next step.

Create an Event Hub

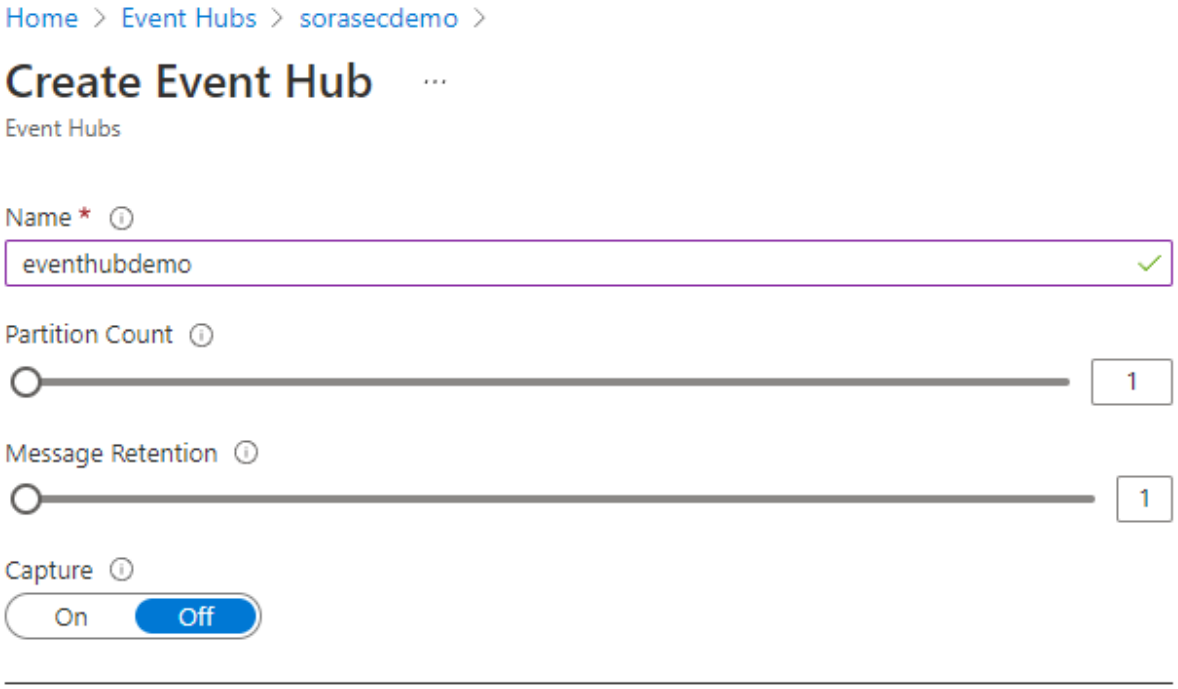
Open your newly created Event Hubs namespace.

In this picture you can see that there are no Event Hubs that exists. At a later stage in the process, you can verify if your new Event Hub has been created, and if there are any data sent to your Event Hub.



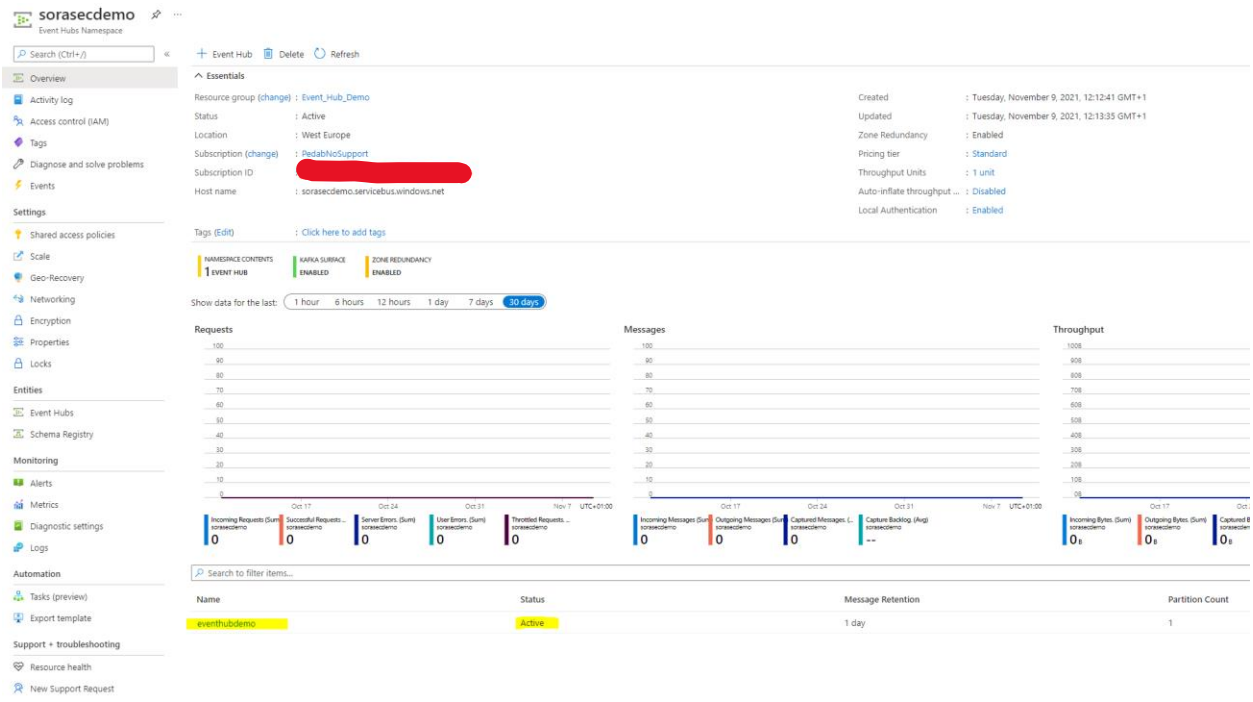
The next step is to add a new Event Hub, press the button +Event Hub (marked in yellow):

The next screen looks like this:



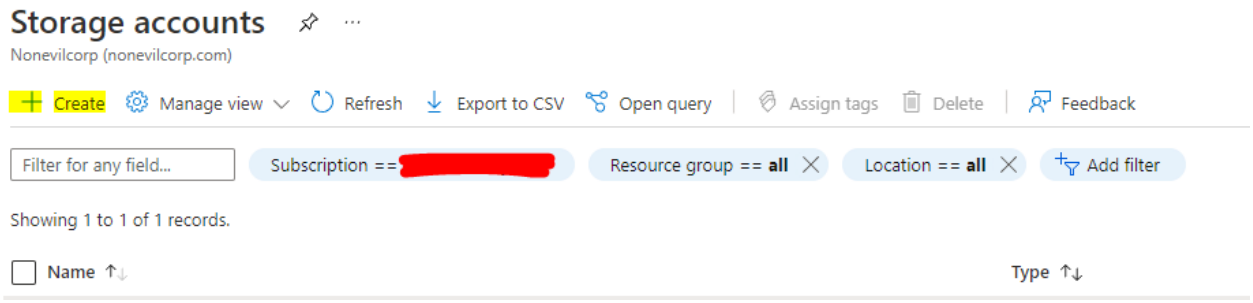
Notes: These settings does not affect the remaining workflow of this guide. Adapt the settings to fit your needs.

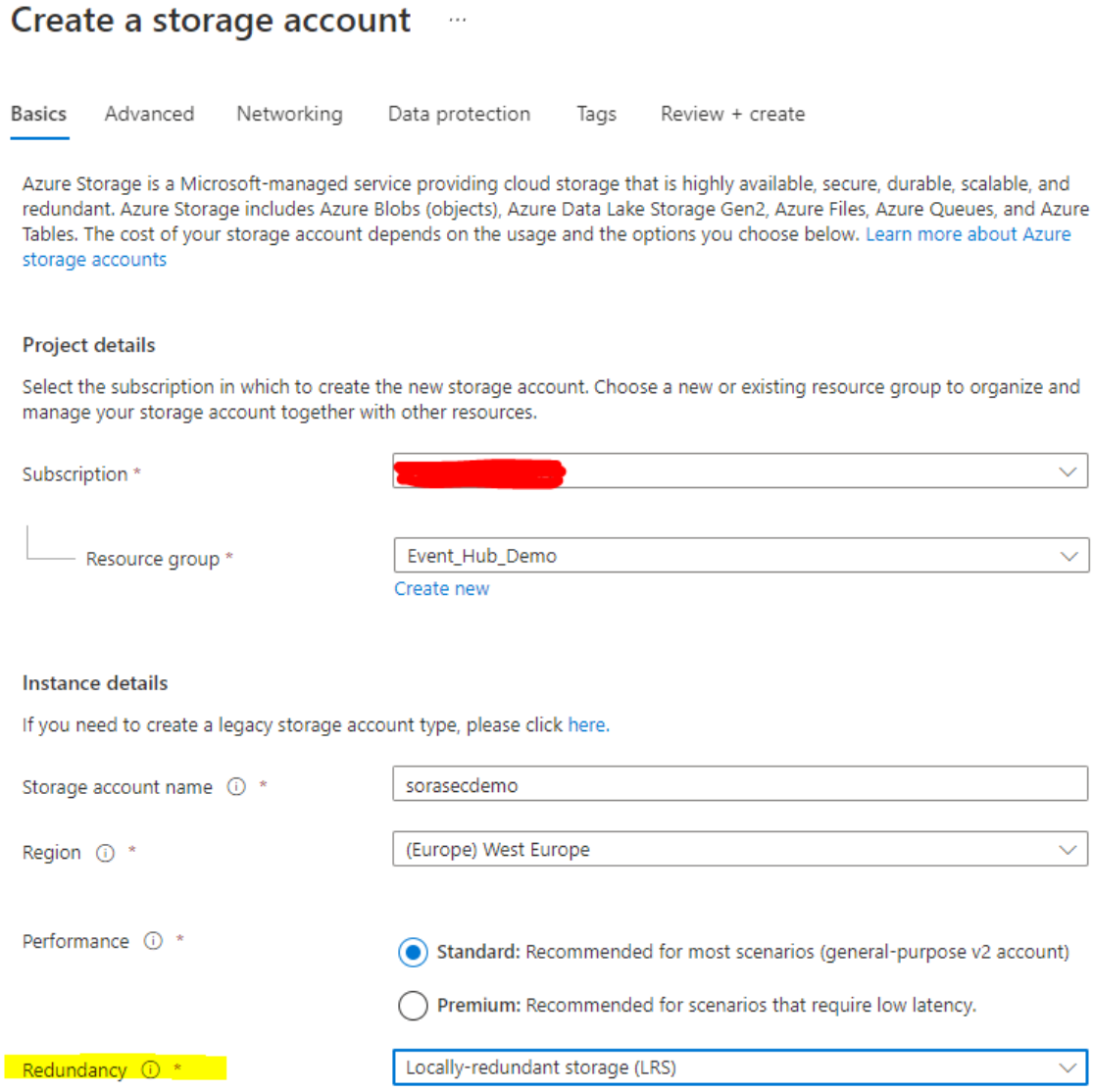
Verify in the Event Hub Namespace dashboard that your new Event Hub exists.



Create Azure Storage Account

Look up Storage accounts on the Azure Portal. Create a new Storage Account:



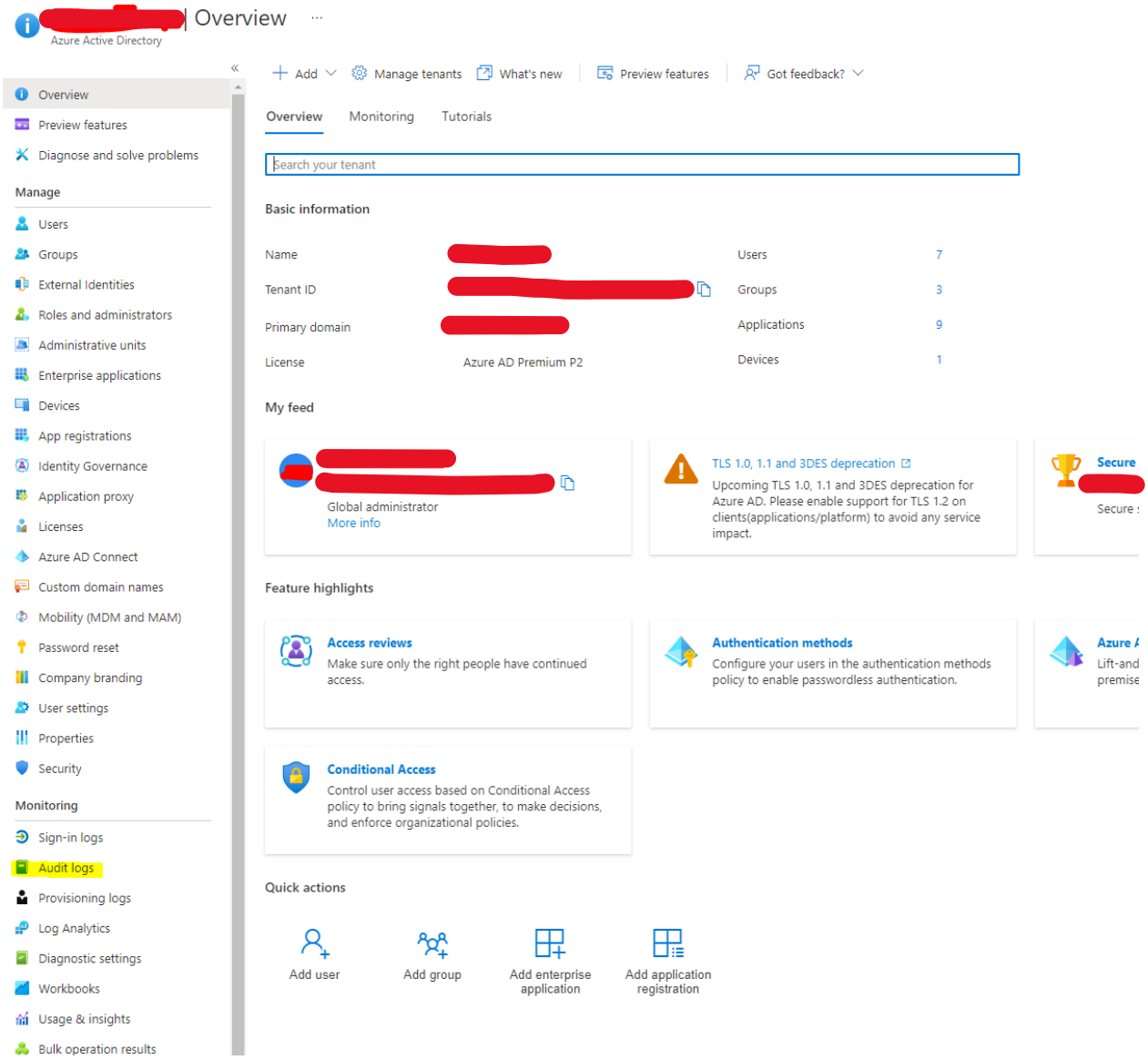


Notes: Verify your redundancy needs and replication policies for your business.

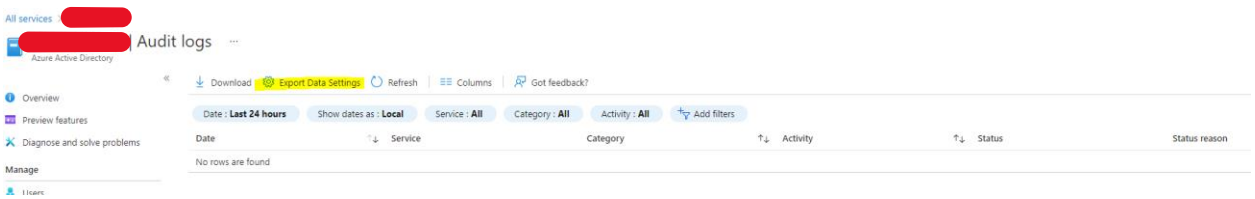
Verify that the storage account is created.

Configure Azure AD to Stream events to Event Hub

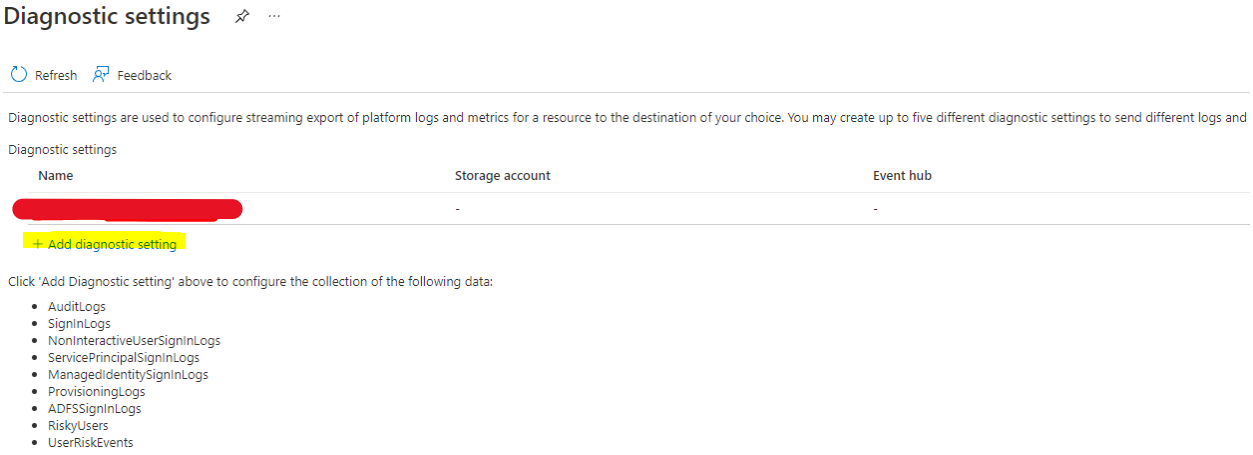
Open your Azure AD dashboard and open the Audit Logs configuration item:



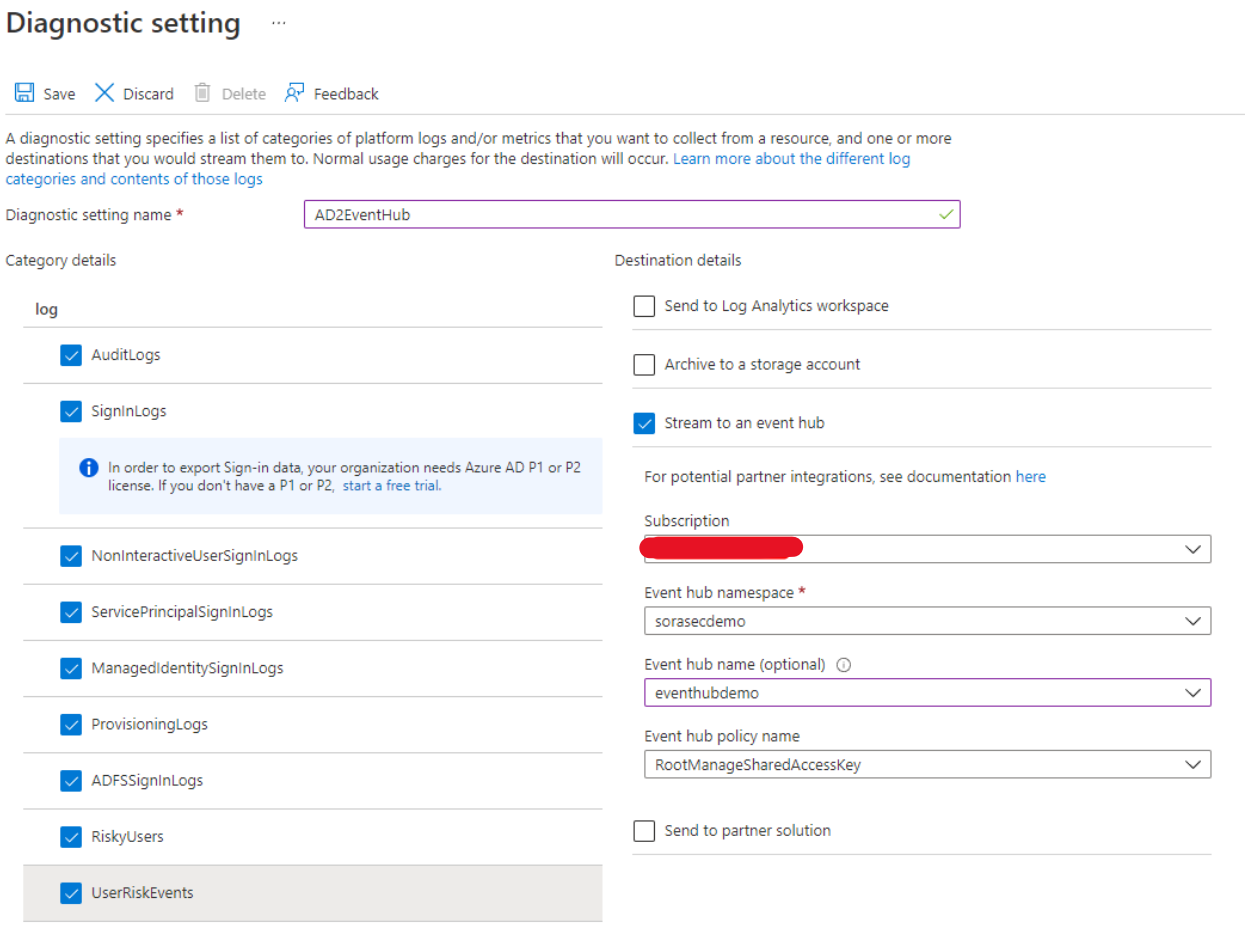
Go to Export Data Settings



Add diagnostic setting

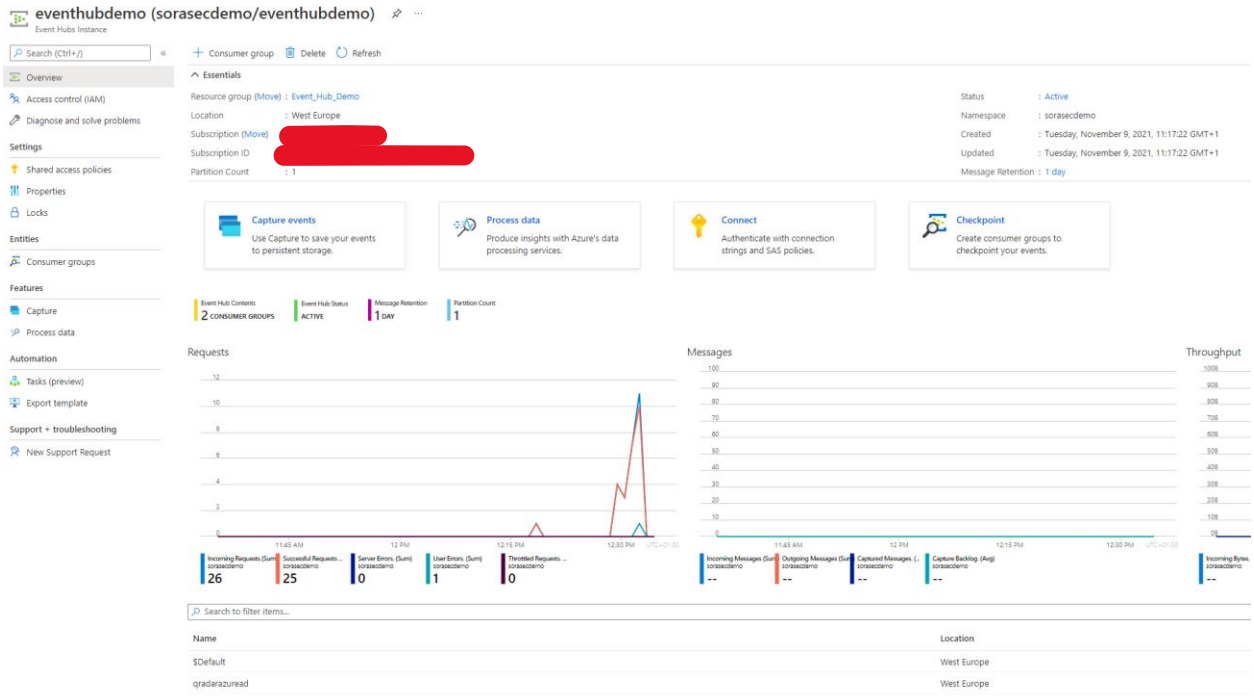


I selected all the audit event types to be sent to the Event Hub.



Verify that Azure AD sends data to the Event Hub.

Open the Event Hub dashboard and review if there any incoming requests. You may need to grab a coffee and wait for incoming requests if your Azure AD is not heavily used.

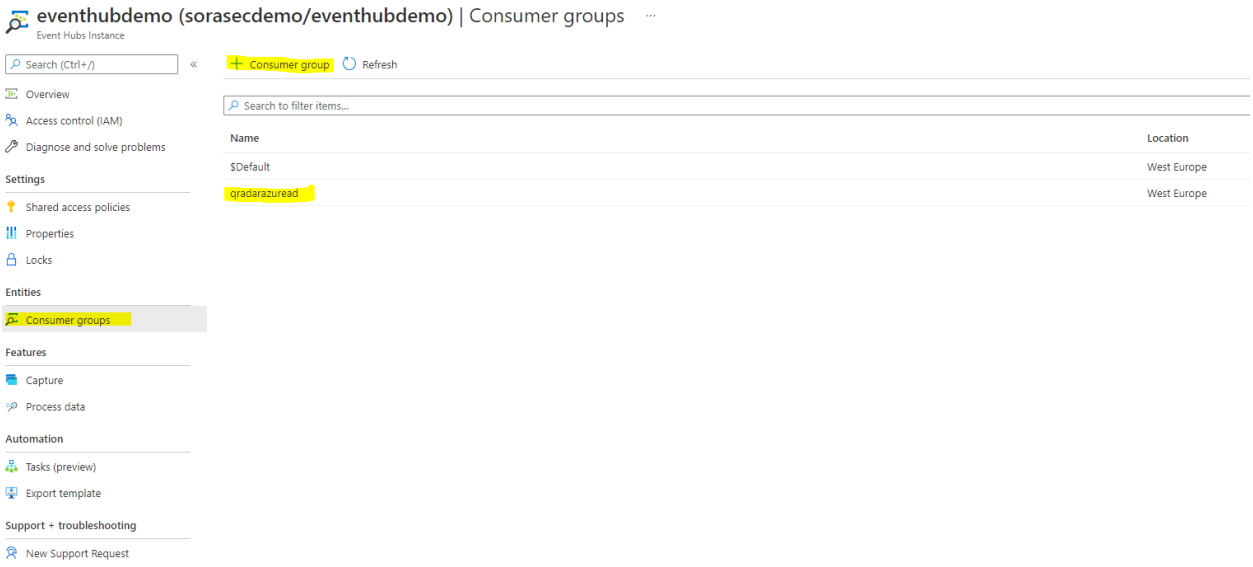


Important:

An Event Hub Consumer Group needs to be configured. QRadar uses this for session tracking. The *$Default* Consumer Group should not be used when setting up the Log Source in QRadar.

Add a new Consumer group

Open the Event Hub Namespace page, and select Consumer groups, and add a new Consumer group.



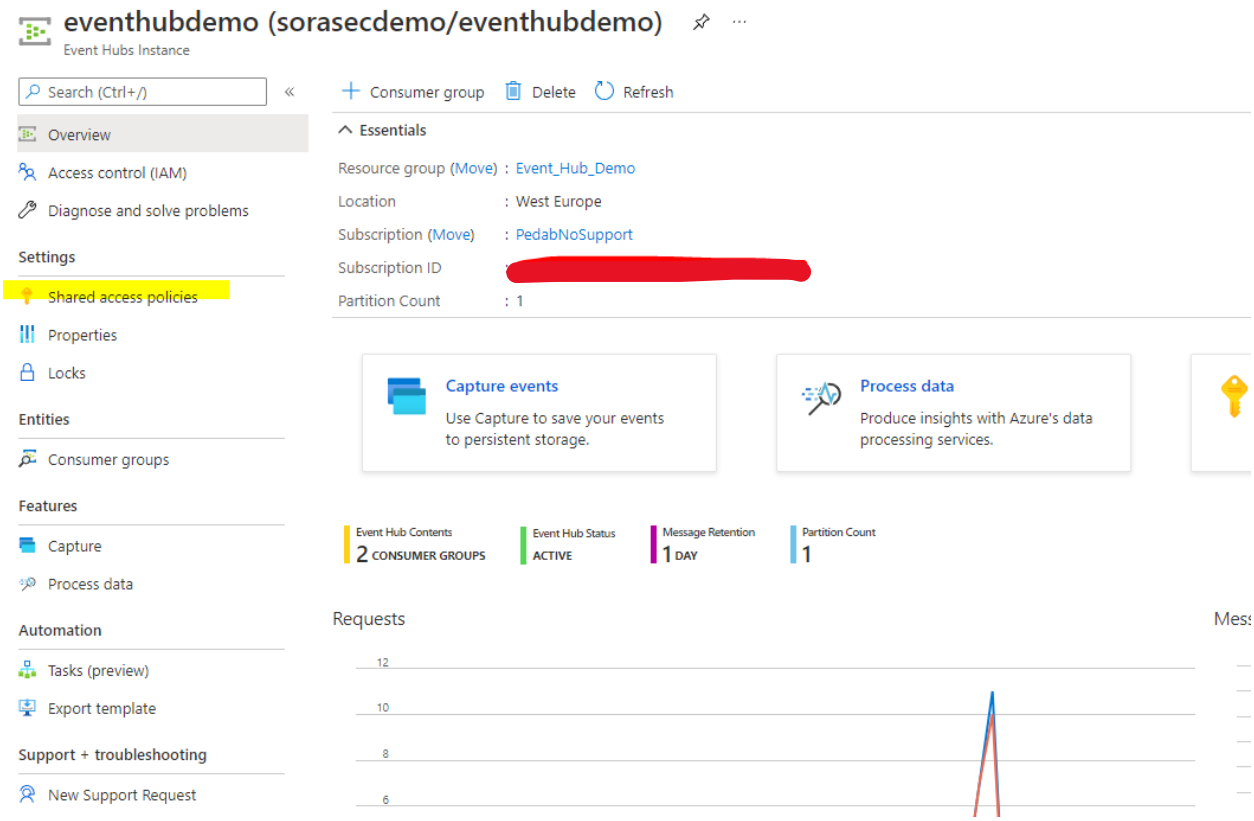
Shared access policy

We need to create a shared access policy to fetch our Event Hubs connection string. This connection string is needed when creating the Log Source in QRadar.

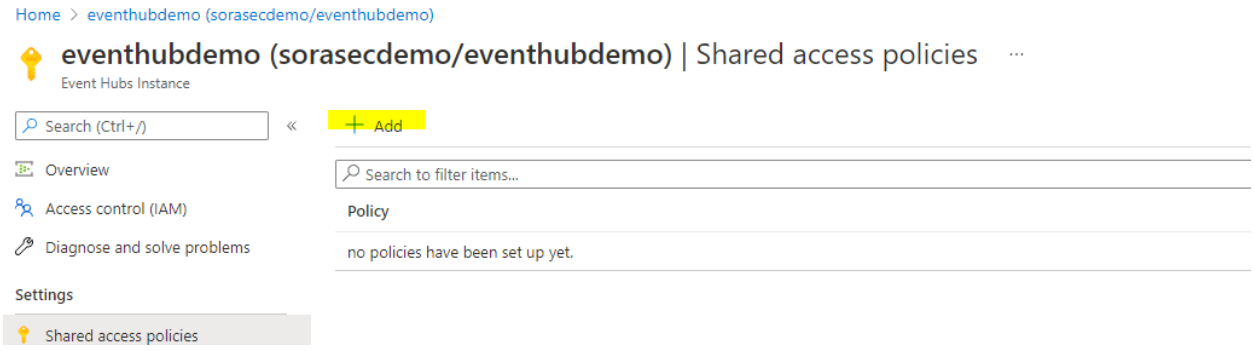
These steps are based on documentation from Microsoft:

https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-get-connection-string

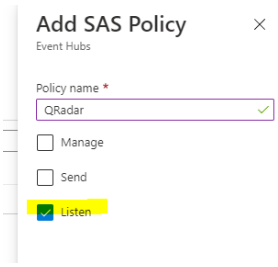
Go to the Event Hub dashboard, and go into the Shared access policies configuration item:



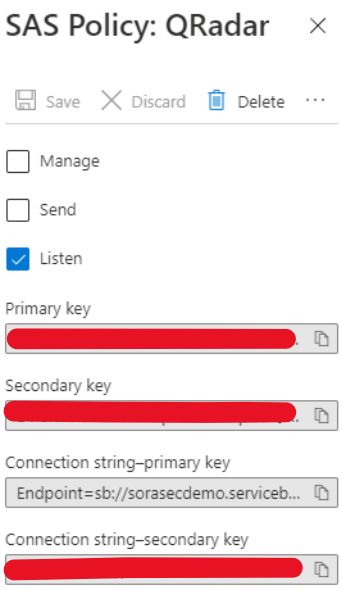
Add a Shared access policy:



Over to the right side on the screen a menu pops up:

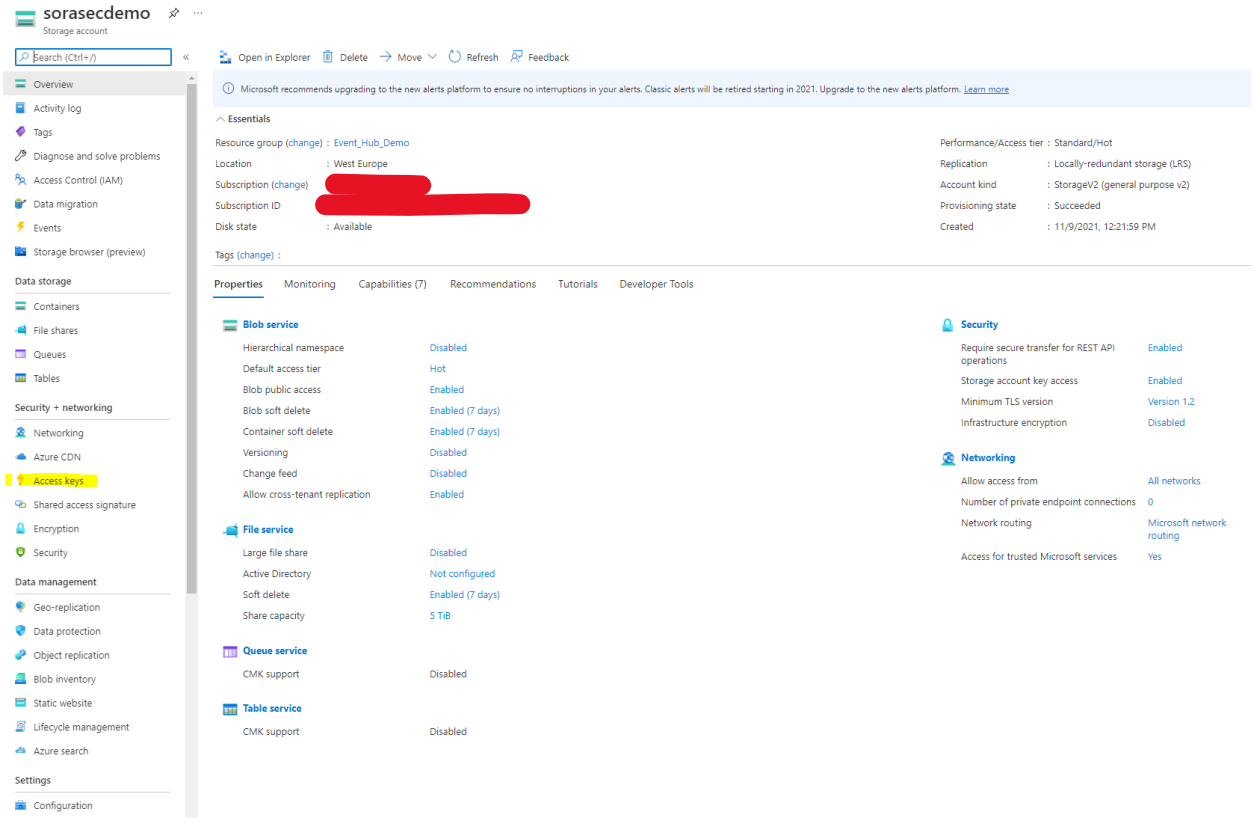


When the creation of the new policy completes, click on the policy and you will see some information pop-up on the right side of the screen. Copy-paste the "Connection string-primary key", this is needed during the Log Source configuration step in QRadar:

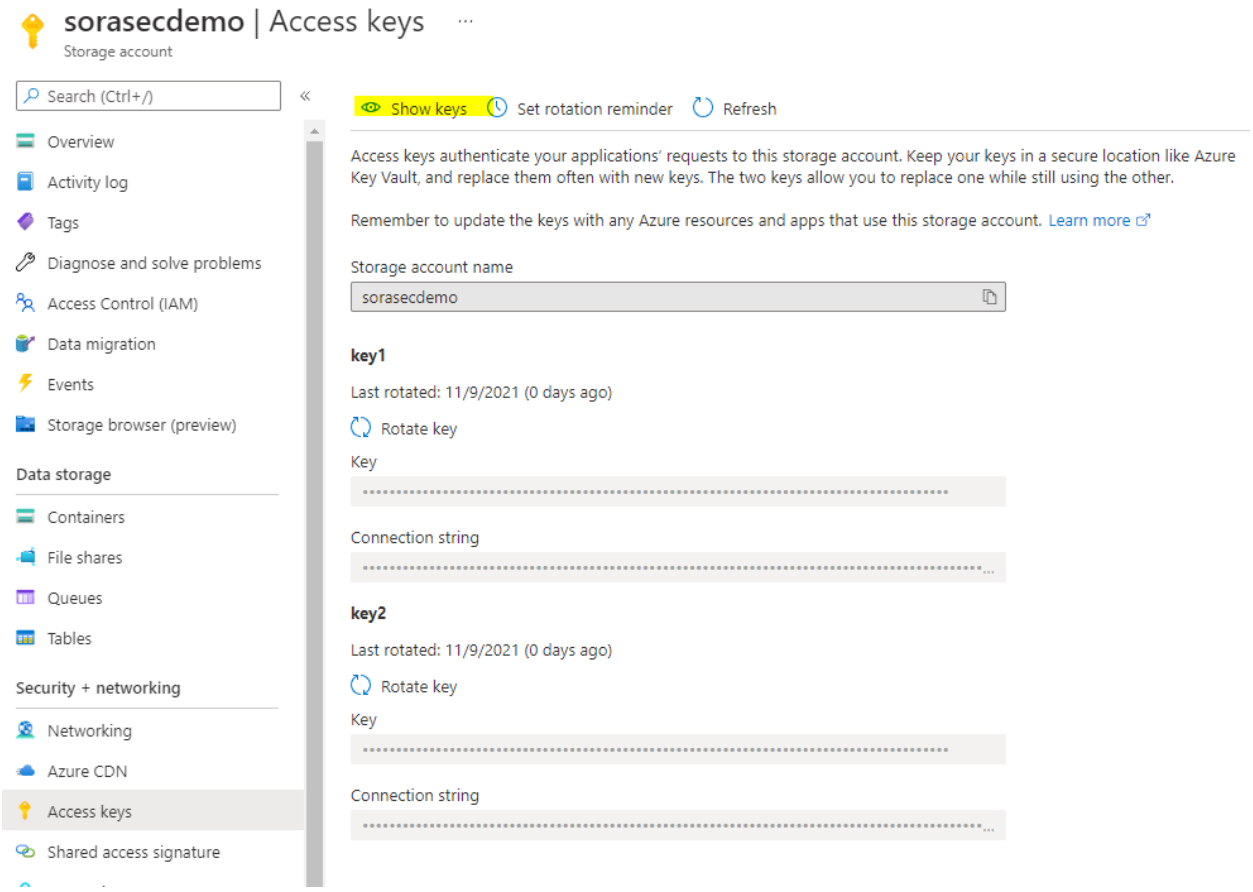


Locate your Storage Account Connection string

Go to your Storage Account, and click on the Access Keys configuration item:



Click the Show keys button:



The connection strings will be visible here. Copy-paste the Connection string for key1.

Connection string-primary key Sample syntax:

Endpoint=sb://<Namespace Name>.servicebus.windows.net/;SharedAccess KeyNam Key Name>;SharedAccessKey=<SAS Key>; EntityPath=<Event Hub Name>

This (hopefully) concludes the work needed in Azure.

Configure QRadar to subscribe to your Event Hub

The following steps is based on the official IBM documentation:

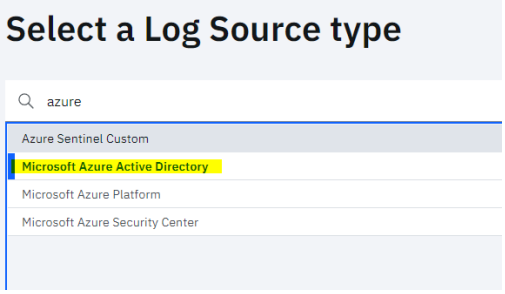
https://www.ibm.com/docs/de/dsm?topic=options-microsoft-azure-event-hubs-protocol-configuration

You will need the following information:

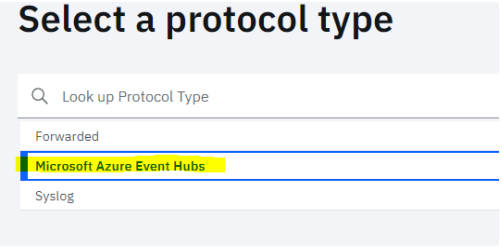
- Event Hub Connection String
- Consumer Group
- Storage Account Connection String

Open the Log Source Management app in QRadar and add a new Log Source

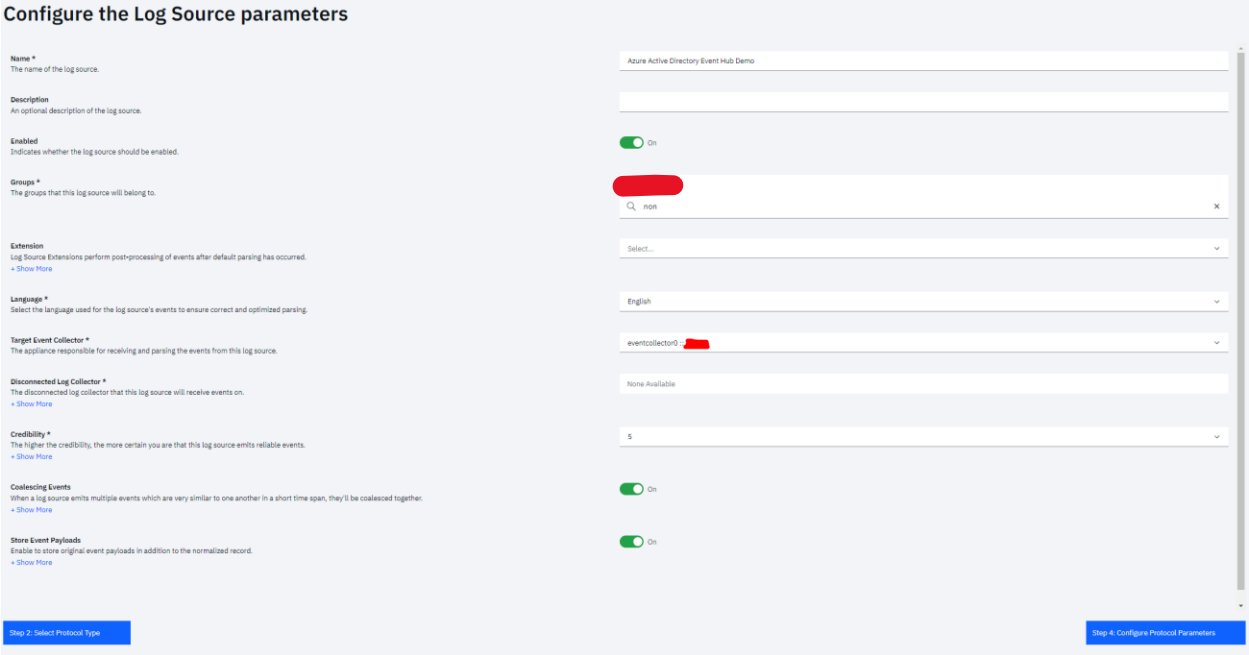
Use Microsoft Azure Active Directory as Log Source Type



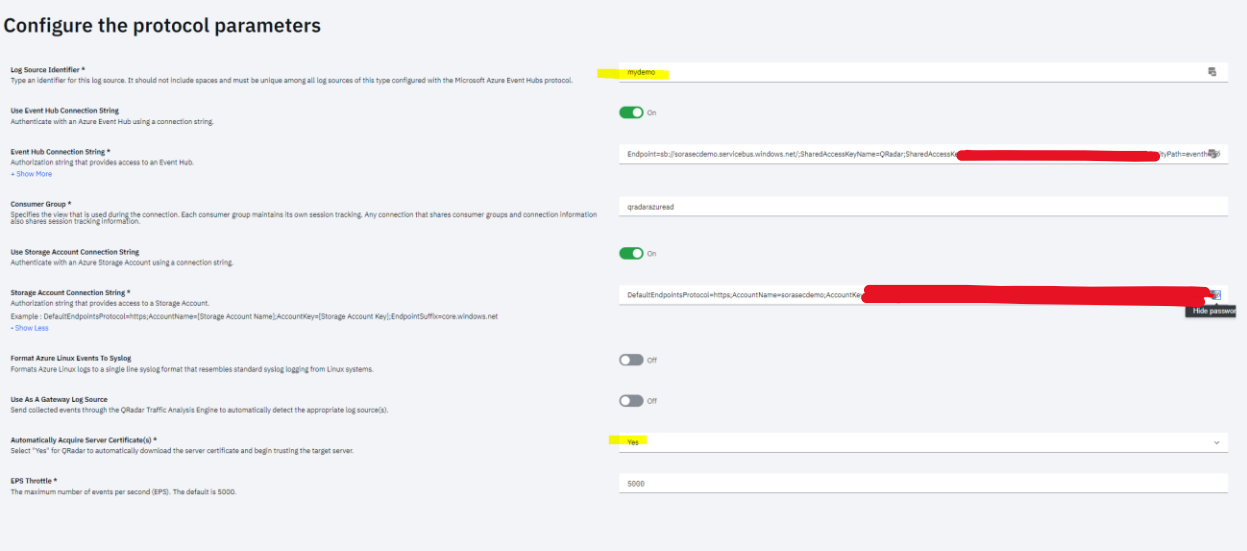
Use the Microsoft Azure Event Hubs as protocol type.



Configure the Log Source parameters

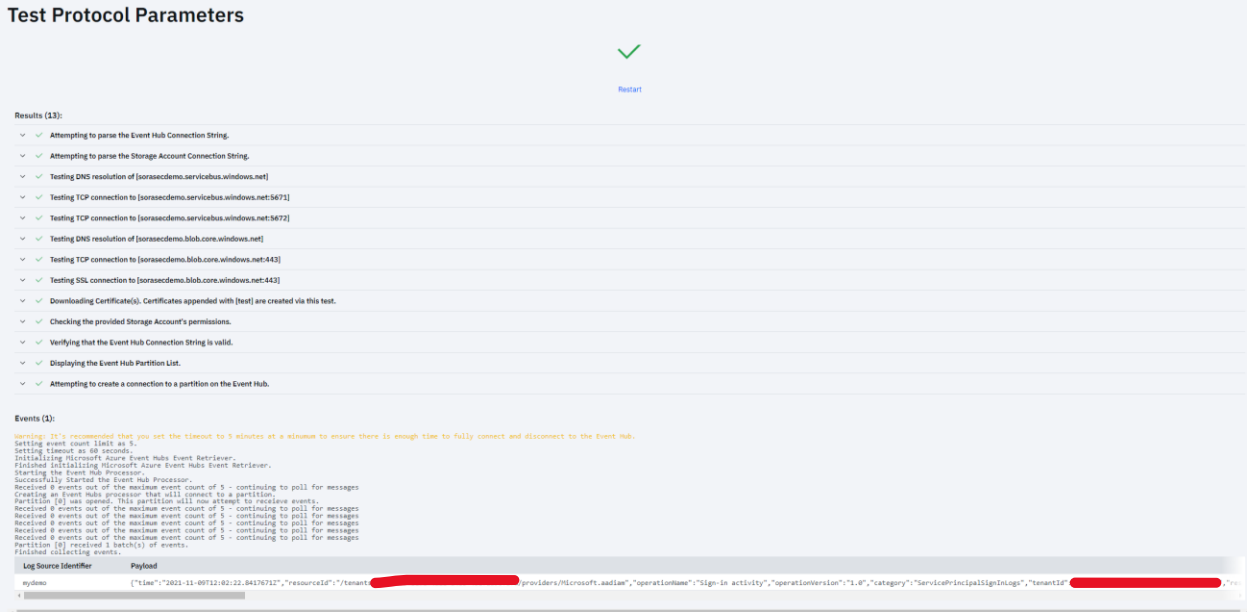


Go to the next page

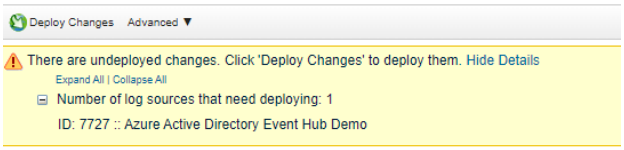


I opted to download the certificate from Azure automatically.

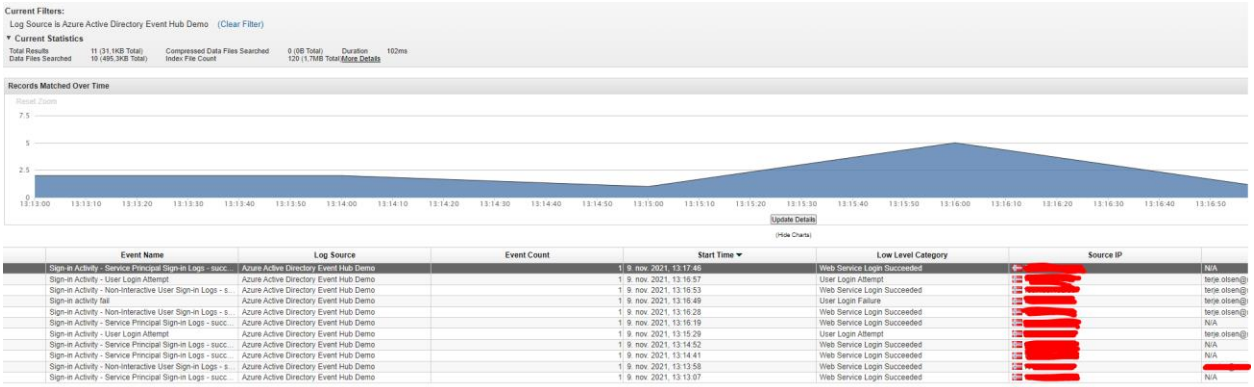
Use the Test Protocol Parameters feature, this will provide valuable information if some if the configuration items is misconfigured. You can see on the last line that an actual event from Azure Active Directory is received.



Save the Log Source. Remember to do a deploy in QRadar.



The last step is to check if the newly created Log Source contains any events from Azure Active Directory



Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP	
Sign-in Activity - Service Principal Sign-in Logs - succ...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:17:46	Web Service Login Succeeded	[redacted]	N/A
Sign-in Activity - User Login Attempt	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:16:57	User Login Attempt	[redacted]	terje.olsen@
Sign-in Activity - Non-Interactive User Sign-in Logs - s...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:16:53	Web Service Login Succeeded	[redacted]	terje.olsen@
Sign-in activity fail	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:16:49	User Login Failure	[redacted]	terje.olsen@
Sign-in Activity - Non-Interactive User Sign-in Logs - s...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:16:28	Web Service Login Succeeded	[redacted]	terje.olsen@
Sign-in Activity - Service Principal Sign-in Logs - succ...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:16:19	Web Service Login Succeeded	[redacted]	N/A
Sign-in Activity - User Login Attempt	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:15:29	User Login Attempt	[redacted]	terje.olsen@
Sign-in Activity - Service Principal Sign-in Logs - succ...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:14:52	Web Service Login Succeeded	[redacted]	N/A
Sign-in Activity - Service Principal Sign-in Logs - succ...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:14:41	Web Service Login Succeeded	[redacted]	N/A
Sign-in Activity - Non-Interactive User Sign-in Logs - s...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:13:58	Web Service Login Succeeded	[redacted]	[redacted]
Sign-in Activity - Service Principal Sign-in Logs - succ...	Azure Active Directory Event Hub Demo	1	9. nov. 2021, 13:13:07	Web Service Login Succeeded	[redacted]	N/A