

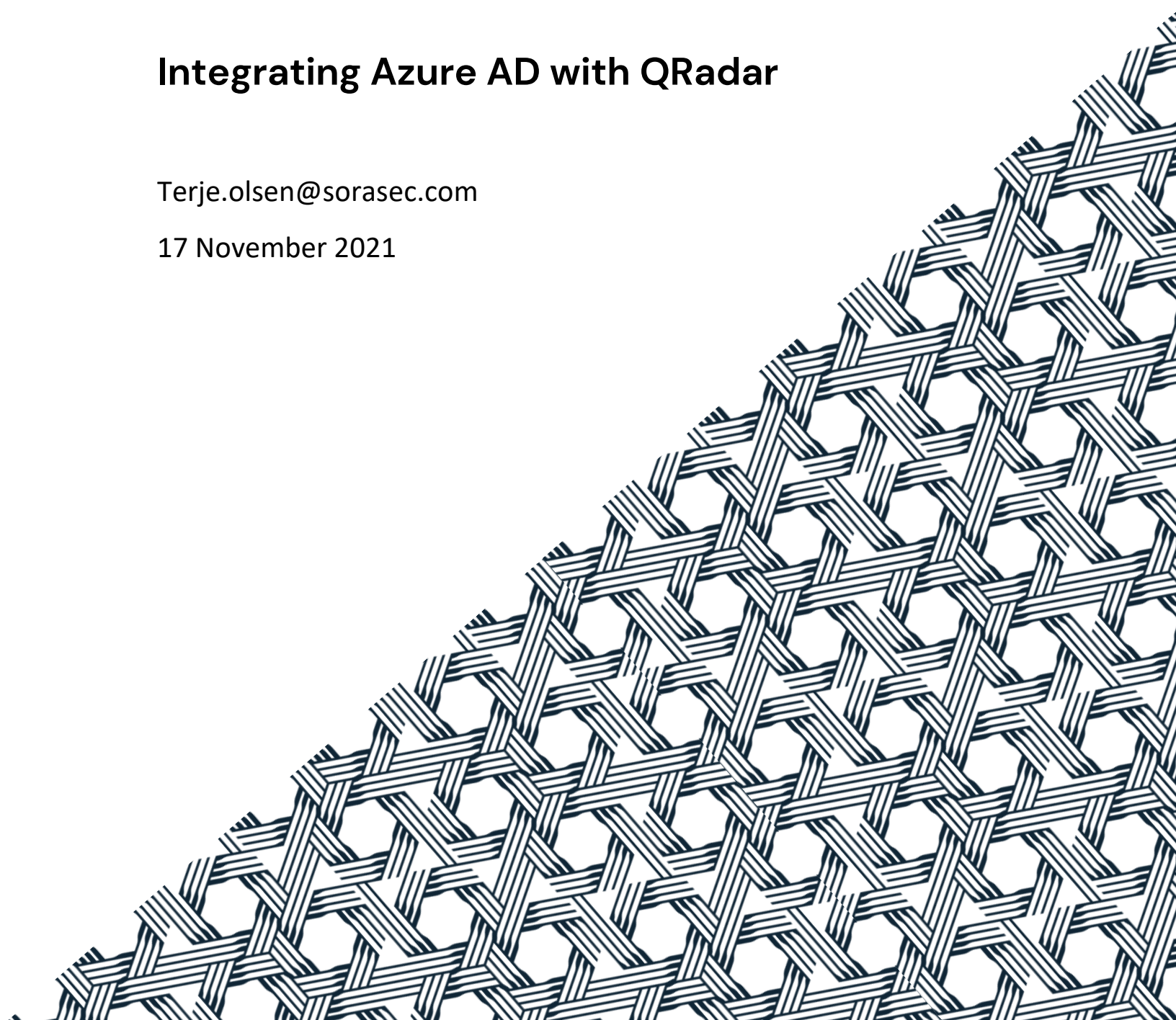


sorasec
BUSINESS IT SECURITY

Integrating Azure AD with QRadar

Terje.olsen@sorasec.com

17 November 2021





Contents

Introduction	3
High level tasks:.....	4
Prerequisites	4
Create an Azure Event Hub.....	5
Create an Event Hub namespace.....	5
Create an Event Hub	7
Create Azure Storage Account.....	10
Configure Azure AD to Stream events to Event Hub	12
Configure QRadar to subscribe to your Event Hub	21
Open the Log Source Management app in QRadar and add a new Log Source.....	21



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

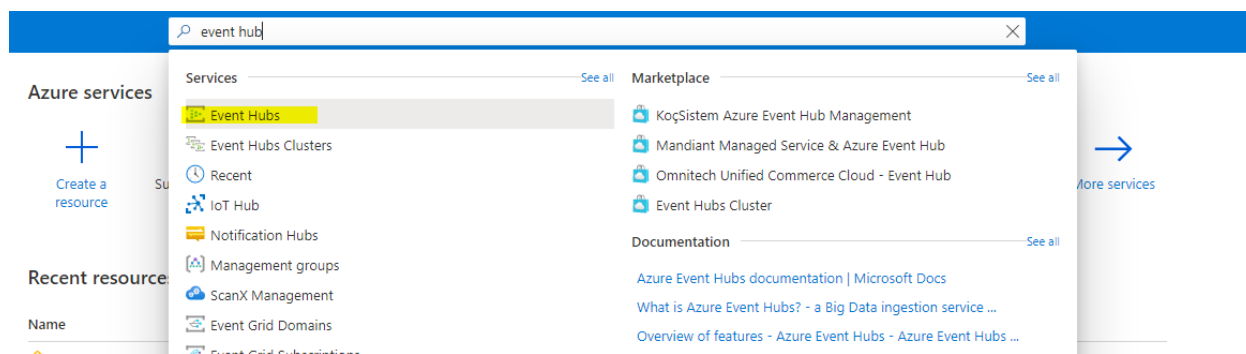
The official IBM documentation on how to integrate QRadar with Azure Active Directory can be found here: <https://www.ibm.com/docs/de/dsm?topic=microsoft-azure-active-directory>



Create an Azure Event Hub

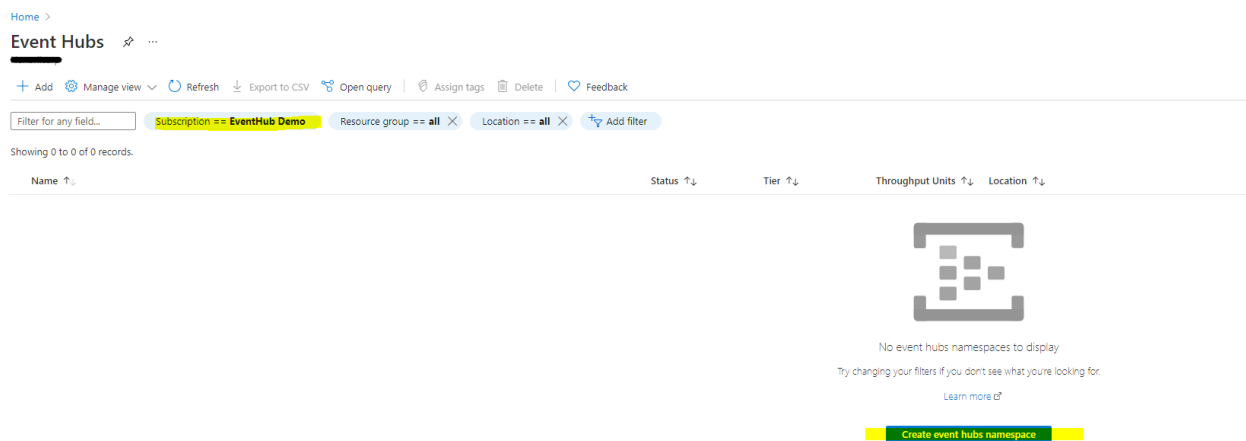
An Event Hub Namespace needs to be created first. Sometimes it's a bit challenging to understand if you have selected an Event Hub Namespace or an Event Hub in the Azure Portal.

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:

[Home](#) > [Event Hubs](#) >

Create Namespace ... Event Hubs

Basics Tags Review + create

Project Details

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

Subscription *

Resource group * [Create new](#)

Instance Details

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

Namespace name *

Location *
 ⓘ The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more.](#)

Pricing tier ([View full pricing details](#)) *

Throughput Units *

Enable Auto-Inflate ⓘ

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 screenshot shows the Azure portal interface for an Event Hubs namespace named 'sorasecdemo'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings, Shared access policies, Scale, Geo-Recovery, Networking, Encryption, Properties, Locks, Entities, Event Hubs, Schema Registry, Monitoring, Alerts, Metrics, Diagnostic settings, Logs, Automation, Tasks (preview), Export template, Support + troubleshooting, Resource health, and New Support Request.

The main content area displays the 'Essentials' section for the namespace, including:

- Resource group (change): Event_Hub_Demo
- Status: Active
- Location: West Europe
- Subscription (change): PedabNoSupport
- Subscription ID: [Redacted]
- Host name: sorasecdemo.servicebus.windows.net
- Created: Tuesday, November 9, 2021, 12:12:41 GMT+1
- Updated: Tuesday, November 9, 2021, 12:13:35 GMT+1
- Zone Redundancy: Enabled
- Pricing tier: Standard
- Throughput Units: 1 unit
- Auto-inflate throughput...: Disabled
- Local Authentication: Enabled

Below the essentials, there are three monitoring charts: Requests, Messages, and Throughput. All charts show zero activity for the selected time range (30 days). The Requests chart shows metrics for Incoming Requests (Sum), Successful Requests, Server Errors (Sum), User Errors (Sum), and Throttled Requests. The Messages chart shows Incoming Messages (Sum), Outgoing Messages (Sum), and Captured Messages (Avg). The Throughput chart shows Incoming Bytes (Sum) and Outgoing Bytes.

At the bottom, there is a table for Event Hubs with the following columns: Name, Status, Message Retention, and Part. The table is currently empty, with a message 'No Event Hubs yet.' displayed in a yellow box.

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



The next screen looks like this:

[Home](#) > [Event Hubs](#) > [sorasecdemo](#) >

Create Event Hub ...

Event Hubs

Name * ⓘ

eventhubdemo ✓

Partition Count ⓘ

1

Message Retention ⓘ

1

Capture ⓘ

On Off

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.

sorasecdemo Event Hubs Namespace

Search (Ctrl+F) | + Event Hub | Delete | Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Events

Settings

- Shared access policies
- Scale
- Geo-Recovery
- Networking
- Encryption
- Properties
- Locks

Entities

- Event Hubs
- Schema Registry

Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

Resource health

New Support Request

Essentials

Resource group (change): Event_Hub_Demo
Status: Active
Location: West Europe
Subscription (change): RedabNOSupport
Subscription ID: [REDACTED]
Host name: sorasecdemo.servicebus.windows.net

Created: Tuesday, November 9, 2021, 12:12:41 GMT+1
Updated: Tuesday, November 9, 2021, 12:13:35 GMT+1
Zone Redundancy: Enabled
Pricing tier: Standard
Throughput Units: 1 unit
Auto-inflate throughput: Disabled
Local Authentication: Enabled

Tags (Edit): [Click here to add tags](#)

NAMESPACE CONTENTS: 1 EVENT HUB | KAFKA SOURCE: DISABLED | ZONE REDUNDANCY: ENABLED

Show data for the last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

Requests | **Messages** | **Throughput**

0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0

Name	Status	Message Retention	Partition Count
eventhubdemo	Active	1 day	1



Create Azure Storage Account

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

Storage accounts

Nonevilcorp (nonevilcorp.com)

Create Manage view Refresh Export to CSV Open query | Assign tags Delete | Feedback

Filter for any field... Subscription == Resource group == all Location == all Add filter

Showing 1 to 1 of 1 records.

Name Type



Create a storage account ...

Basics Advanced Networking Data protection Tags Review + create

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 *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

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

Redundancy ⓘ *

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:

Basic information

Name	[REDACTED]	Users	7
Tenant ID	[REDACTED]	Groups	3
Primary domain	[REDACTED]	Applications	9
License	Azure AD Premium P2	Devices	1

My feed

- Global administrator [REDACTED]
- TLS 1.0, 1.1 and 3DES deprecation**
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
- Secure**
Secure :

Feature highlights

- Access reviews**
Make sure only the right people have continued access.
- Authentication methods**
Configure your users in the authentication methods policy to enable passwordless authentication.
- Azure / Lift-and-premise**
- Conditional Access**
Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Quick actions

- Add user
- Add group
- Add enterprise application
- Add application registration

Go to Export Data Settings

Export Data Settings

Date: Last 24 hours | Show dates as: Local | Service: All | Category: All | Activity: All | Add filters

Date	Service	Category	Activity	Status	Status reason
No rows are found					



Add diagnostic setting

Diagnostic settings [↗](#) [...](#)

[Refresh](#) [Feedback](#)

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

Diagnostic settings

Name	Storage account	Event hub
[REDACTED]	-	-

[+ Add diagnostic setting](#)

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

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents



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

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 * AD2EventHub ✓

Category details

log

AuditLogs

SignInLogs

i 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

RiskyUsers

UserRiskEvents

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

[Redacted] ▾

Event hub namespace *

sorasecdemo ▾

Event hub name (optional) ⓘ

eventhubdemo ▾

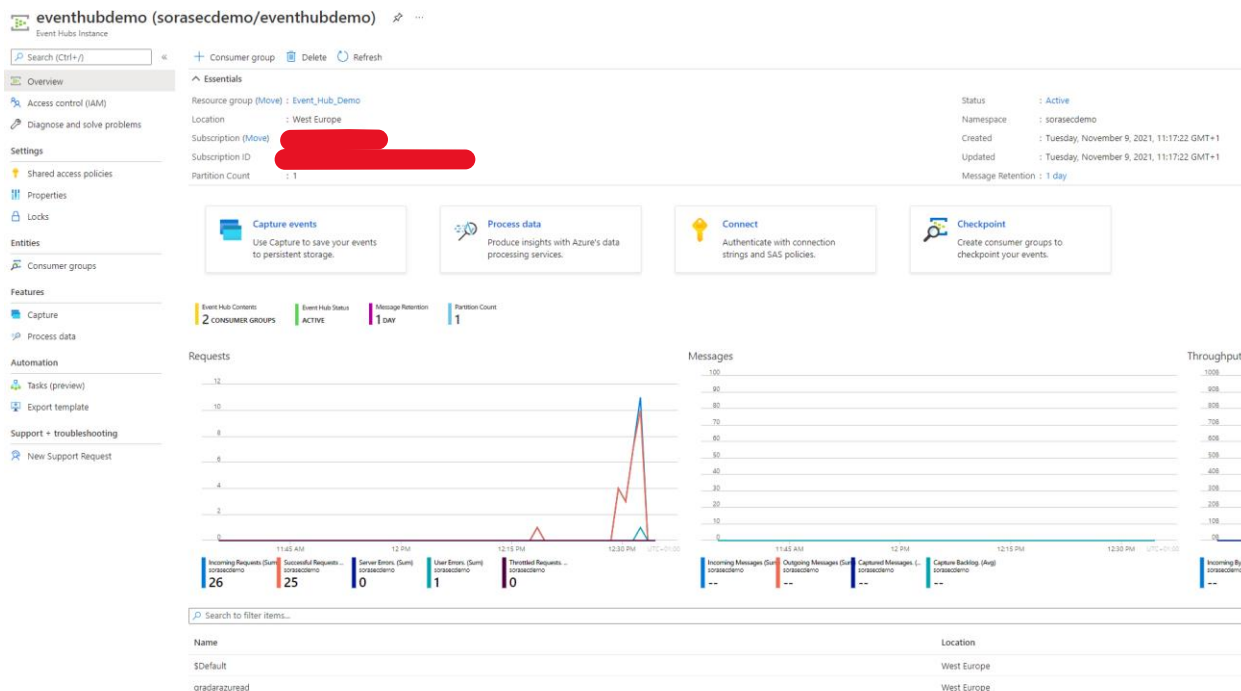
Event hub policy name

RootManageSharedAccessKey ▾

Send to partner solution

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.

eventhubdemo (sorasecdemo/eventhubdemo) | Consumer groups

Search (Ctrl+F) << Consumer group Refresh

Search to filter items...

Name	Location
\$Default	West Europe
qradarazuread	West Europe

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:

eventhubdemo (sorasecdemo/eventhubdemo) Event Hubs Instance

Search (Ctrl+/) << + Consumer group Delete Refresh

Overview

Access control (IAM)

Diagnose and solve problems

Settings

Shared access policies

Properties

Locks

Entities

Consumer groups

Features

Capture

Process data

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Essentials

Resource group (Move) : Event_Hub_Demo

Location : West Europe

Subscription (Move) : PedabNoSupport

Subscription ID : [REDACTED]

Partition Count : 1

Capture events
Use Capture to save your events to persistent storage.

Process data
Produce insights with Azure's data processing services.

Event Hub Contents: 2 CONSUMER GROUPS

Event Hub Status: ACTIVE

Message Retention: 1 DAY

Partition Count: 1

Requests

Mess

Add a Shared access policy:

Home > eventhubdemo (sorasecdemo/eventhubdemo)

eventhubdemo (sorasecdemo/eventhubdemo) | Shared access policies Event Hubs Instance

Search (Ctrl+/) << + Add

Overview

Access control (IAM)

Diagnose and solve problems

Settings

Shared access policies

Search to filter items...

Policy

no policies have been set up yet.



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:

Essentials

Resource group (change) : Event_Hub_Demo
Location : West Europe
Subscription (change) : [REDACTED]
Subscription ID : [REDACTED]
Disk state : Available

Performance/Access tier : Standard/Hot
Replication : Locally-redundant storage (LRS)
Account kind : StorageV2 (general purpose v2)
Provisioning state : Succeeded
Created : 11/9/2021, 12:21:59 PM

Properties | Monitoring | Capabilities (7) | Recommendations | Tutorials | Developer Tools

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob public access	Enabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)
Versioning	Disabled
Change feed	Disabled
Allow cross-tenant replication	Enabled

File service

Large file share	Disabled
Active Directory	Not configured
Soft delete	Enabled (7 days)
Share capacity	5 TiB

Queue service

CMK support	Disabled
-------------	----------

Table service

CMK support	Disabled
-------------	----------

Security

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

Networking

Allow access from	All networks
Number of private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes



Click the Show keys button:

The screenshot shows the Azure portal interface for the 'sorasecdemo' storage account. The left-hand navigation pane is visible, with 'Access keys' selected. The main content area displays the 'Access keys' page. At the top, there is a search bar and a 'Show keys' button (highlighted in yellow), along with 'Set rotation reminder' and 'Refresh' buttons. Below this, there is a brief explanation of access keys and a 'Learn more' link. The 'Storage account name' is shown as 'sorasecdemo'. Two keys are listed: 'key1' and 'key2'. Each key entry includes a 'Rotate key' button, the last rotation date (11/9/2021), and fields for the 'Key' and 'Connection string'. The 'Key' and 'Connection string' fields are currently obscured by grey bars.

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 KeyName=<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>

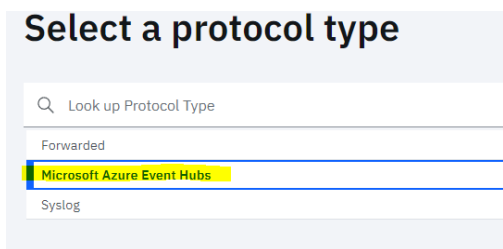
You will need the following information:

- 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

Configure the Log Source parameters

Name *
The name of the log source.
Azure Active Directory Event Hub Demo

Description
An optional description of the log source.

Enabled
Indicates whether the log source should be enabled.
 On

Groups *
The groups that this log source will belong to.
[Redacted]

Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.
[+ Show More](#)

Language *
Select the language used for the log source's events to ensure correct and optimized parsing.
English

Target Event Collector *
The appliance responsible for receiving and parsing the events from this log source.
eventcollector0 [Redacted]

Disconnected Log Collector *
The disconnected log collector that this log source will receive events on.
[+ Show More](#)

Credibility *
The higher the credibility, the more certain you are that this log source emits reliable events.
[+ Show More](#)

Coalescing Events
When a log source emits multiple events which are very similar to one another in a short time span, they'll be coalesced together.
 On

Store Event Payloads
Enable to store original event payloads in addition to the normalized record.
 On

[Step 2: Select Protocol Type](#) [Step 4: Configure Protocol Parameters](#)

Go to the next page

Configure the protocol parameters

Log Source Identifier *
Type an identifier for this log source. It should not include spaces and must be unique among all log sources of this type configured with the Microsoft Azure Event Hubs protocol.
mydemo

Use Event Hub Connection String
Authenticate with an Azure Event Hub using a connection string.
 On

Event Hub Connection String *
Authorization string that provides access to an Event Hub.
Endpoint=stj[sorasecdemo.servicebus.windows.net];SharedAccessKeyName=QRadar;SharedAccessKey=[Redacted];Path=eventhubs

Consumer Group *
Specifies the view that is used during the connection. Each consumer group maintains its own session tracking. Any connection that shares consumer groups and connection information also shares session tracking information.
qradarazread

Use Storage Account Connection String
Authenticate with an Azure Storage Account using a connection string.
 On

Storage Account Connection String *
Authorization string that provides access to a Storage Account.
DefaultEndpointProtocol=https;AccountName=sorasecdemo;AccountKey=[Redacted]

Format Azure Linux Events To Syslog
Formats Azure Linux logs to a single line syslog format that resembles standard syslog logging from Linux systems.
 Off

Use As A Gateway Log Source
Send collected events through the QRadar Traffic Analysis Engine to automatically detect the appropriate log source(s).
 Off

Automatically Acquire Server Certificate(s) *
Select "yes" for QRadar to automatically download the server certificate and begin trusting the target server.
Yes

EPS Throttle *
The maximum number of events per second (EPS). The default is 5000.
5000

I opted to download the certificate from Azure automatically.



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

Test Protocol Parameters

✓
Restart

Results (13):

- ✓ Attempting to parse the Event Hub Connection String.
- ✓ Attempting to parse the Storage Account Connection String.
- ✓ Testing DNS resolution of [sorasecdemo.servicebus.windows.net]
- ✓ Testing TCP connection to [sorasecdemo.servicebus.windows.net:5671]
- ✓ Testing TCP connection to [sorasecdemo.servicebus.windows.net:5672]
- ✓ Testing DNS resolution of [sorasecdemo.blob.core.windows.net]
- ✓ Testing TCP connection to [sorasecdemo.blob.core.windows.net:443]
- ✓ Testing SSL connection to [sorasecdemo.blob.core.windows.net:443]
- ✓ Downloading Certificate(s). Certificates appended with [test] are created via this test.
- ✓ Checking the provided Storage Account's permissions.
- ✓ Verifying that the Event Hub Connection String is valid.
- ✓ Displaying the Event Hub Partition List.
- ✓ Attempting to create a connection to a partition on the Event Hub.

Events (1):

```
Warning: It's recommended that you set the timeout to 5 minutes at a minimum to ensure there is enough time to fully connect and disconnect to the Event Hub.
Setting event count limit to 5.
Setting timeout to 60 seconds.
Initializing Microsoft Azure Event Hubs Event Retriever.
Finished initializing Microsoft Azure Event Hubs Event Retriever.
Starting the Event Hub Processor.
Successfully started the Event Hub Processor.
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Creating an event hubs processor that will connect to a partition.
Partition [0] was opened. This partition will now attempt to receive events.
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Received 0 events out of the maximum event count of 5 - continuing to poll for messages
Partition [0] received 3 batch(es) of events.
Finished collecting events.
```

Log Source Identifier	Payload
mydemo	{"time": "2021-11-09T12:02:22.841767Z", "resourceId": "/tenant [redacted] providers/Microsoft.aad1ad", "operationName": "Sign-In activity", "operationVersion": "1.0", "category": "ServicePrincipalSignInLogs", "tenantId": "[redacted]"}

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

Deploy Changes Advanced ▾

⚠ There are undeployed changes. Click 'Deploy Changes' to deploy them. [Hide Details](#)

Expand All | Collapse All

☑ Number of log sources that need deploying: 1

ID: 7727 :: Azure Active Directory Event Hub Demo



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

