# BEYOND IDENTITY EVENTS DATA INTEGRATION WITH GOOGLE PUBSUB

# 1 Table of Contents

2	INTRODUCTION	2	
2.1	Авоит		2
2.2	Prerequisites		2
3	GOOGLE PUBSUB CONFIGURATION	2	
3.1	CREATE A NEW PROJECT		3
3.2	Create a new Topic		5
3.3	CREATE GCP SERVICE ACCOUNT		8
3.4	Generate a service account key and download the JSON file.		10
4	BEYOND IDENTITY CONFIGURATION	12	
5	Appendix	12	

# 2 Introduction

#### 2.1 About

This guide provides instructions on how to:

• Integrate BI events data with Google PubSub

### 2.2 Prerequisites

Ensure that you have the following:

• You have a tenant configured for your organization and able to enroll users.

# 3 Google PubSub Configuration

- Create a new project
- Create a new Topic and default Subscription
- Create a GCP service account and grant it an IAM role that allows publishing to a Pub/Sub topic of your choice

Generate a key and download the JSON representation. Share this JSON file with BI SME, Topic name
and list of event types interested in. The appendix section explains how to get the event types

## 3.1 Create a new project

Access console.google.com with admin credentials. Click on "Create a project" under IAM & Admin menu.

≡	Google Cloud Platform	n :	🗣 bi-pubsub 👻	
51	Cloud overview	>		
	View all products			
PINN	ED			
θ	IAM & Admin	>	IAM	
	Billing		Identity & Organization	
API	APIs & Services	>	Policy Troubleshooter	
2	Marketplace		Policy Analyzer	
۲	Compute Engine	>	Service Accounts	
	Cloud Storage	>	Workload Identity Federation	
11	VPC network	>	Labels	
	Kubernetes Engine	>	Settings	
	BigQuery	\$	Privacy & Security	
Ś	SOL	*	Identity-Aware Proxy	
~	Socurity		Audit Logs	
	Security	7	Manage Resources	
17			Create a Project	
Q	Google Maps Platfor	>	Asset Inventory	
MORE	PRODUCTS V		Essential Contacts	
			Groups	

Early Access Center

Quotas

In the "New Project" screen, type in a project name for example bi-pubsub. Choose organization and location to suit your GCP configuration. Click "Create"

Project name *	
bi-pubsub	Ø
Project ID: bi-pubsub-349815. It cannot be chang	jed later. EDIT
Project ID: bi-pubsub-349815. It cannot be chang Organization *	ed later. EDIT
Project ID: bi-pubsub-349815. It cannot be chang Organization * zeropw.com Select an organization to attach it to a project. Th	red later. EDIT
Project ID: bi-pubsub-349815. It cannot be chang Organization * zeropw.com Select an organization to attach it to a project. Th — Location *	red later. EDIT
Project ID: bi-pubsub-349815. It cannot be chang Organization * zeropw.com Select an organization to attach it to a project. Th Location *	ed later. EDIT

## 3.2 Create a new Topic

Enter "project" in the search box . In the drop-down search results, select the project you created under "PROJECTS , FOLDERS & ORGANIZATIONS."

Q billing projects

#### **PRODUCTS & PAGES**



Create a Project IAM & Admin

**Billing projects** Billing



. .

**Project Settings** Cloud Volumes



**Project Settings** Cloud Volumes

#### **DOCUMENTATION & TUTORIALS**



Create an Artifact Registry repository for Java. Interactive Tutorial



Project | Config Connector Documentation Documentation

Projects | Cloud Storage Documentation

#### **PROJECTS, FOLDERS & ORGANIZATIONS**



**ADFS** Integration Project - adfs-integration

bi-pubsub Project - bi-pubsub

After selecting the project, in the search box type "topics". In the drop-down search results, select "Topics".



On the Topics screen, click "CREATE TOPIC"

≡	Google Cloud Platform	🐉 bi-pubsub 🔻	
**** ****	Pub/Sub	Topics 🛑 🛨 CREATE TOPIC	DELETE

Enter a name for the Topic ID for example "bi-data-export-pub-sub". Leave "Add a default subscription" selected. This will create a subscription automatically. Click "CREATE TOPIC".

Create a topic	
A topic forwards messages from publishers to	o subscribers.
Topic ID * bi-data-export-pubsub	0
Topic name: projects/bi-pubsub/topics/bi-data-e	export-pubsub
Add a default subscription	
🔲 Use a schema 🛛 😮	
Set message retention duration (not free)	0
Use a customer-managed encryption key (	(CMEK)
	CANCEL CREATE TOPIC

You will see the topic created with a default subscription. The default subscription created is "projects/bi-pubsub/subscriptions/bi-data-export-pubsub-sub"

	n 🛟 bi-pubsub 👻	Q Search project	x ~				
Pub/Sub	← bi-data-export-pubsub  ✓ EDIT + TRIGGER CLOUD F	unction 👌 import 👻 👕 delete					
Topics Subscriptions	Export options have moved to the Create subscription dropdown menu under the Subscriptions tab below.						
Snapshots	Topic details						
Schemas	Topie name projects i/e publiculo regiont publiculo 🕤						
Lite Reservations							
Lite Topics	Export to BigQuery ×	Export to Cloud Storage ×					
	cieste a batallow job to export bata to a bigquery table.	Create a balance point data to a text or Ano me in crood storage.					
	EXPORT TO BIGQUERY	EXPORT TO TEXT EXPORT TO AVRO					
			✓ 1 hour 6 hours 1 day 7 days 30 days F	RESET ZOOM			
	Publish message request count	:	Werage message size	I			
	Requests/sec	Bytes					
	▲ No data is available for the selected time	1.0 0.8		1.00B 0.758			
		ed time frame. 0.6 0.4 0.2		0.508			
	11:15 11:20 11:25 11:30 11:35 11:40 11:45	11:50 11:55 12 PM 12:05 12:10 0	11:15 11:20 11:25 11:30 11:35 11:40 11:45 11:30 11:35 12:PM 12:05 12:10	0			
	Encryption key Google-managed						
	Schema name – Message encoding –						
	Labels -						
	SUBSCRIPTIONS SNAPSHOTS MESSAGES	tream of maccanes sublished to a size topic. You can also steam messages to	Biofluseu or Ploud Starsan hu constian a sub-existion from a Ploud Datafleu inh Loan mere				
	CREATE SUBSCRIPTION ·	icon or mossiges passings to a great oper, for our and another mossinges to	allifers har anone numbershoren under a nanne annen bar <del>vennumen</del> t.				
	The Filter subscriptions						
	Subscription ID  Subscription name						
Delases Notes	projecta/orpuosuo/subscription/	an-ann milianagg					
E Release Notes	A new topic and a new subactription has been successfully created DEFAULS 🗙						
4							

#### 3.3 Create GCP service account

The service account is used BI event integration code to authenticate to Google PubSub. In the Google cloud console, select your project and select "Service Accounts" under "IAM & Admin". Click "CREATE SERVICE ACCOUNT" in menu.

	Google Cloud Platform	🕽 bi-pubsub 👻					
	IAM & Admin	Service accounts	TE + MAN/	AGE ACCESS C REFRESH			
+•	IAM	Service accounts for project "bi-pubsub"					
Θ	Identity & Organization	A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems run					
ગ	Policy Troubleshooter	Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation					
Ę	Policy Analyzer	= Filter Enter property name or value					
	Organization Policies	Email	Status	Name 🕇 🛛 🖸			
$\rightarrow$	Service Accounts	asdfasdf@bi-pubsub.iam.gserviceaccount.com		asdfasdf			
-		bi-dataexport-pusher-926@bi-pubsub.iam.gserviceaccount.com	$\bigcirc$	bi-dataexport-pusher			
	Workload Identity Federation	□ 의 bi-dataexport-pusher-2@bi-pubsub.iam.gserviceaccount.com	$\bigcirc$	bi-dataexport-pusher-2			
•	Labels	□ ➡ byndid-staging-okta@bi-pubsub.iam.gserviceaccount.com		byndid-staging-okta			
_	-	□ 🖻 dmd-test@bi-pubsub.iam.gserviceaccount.com	<b>S</b>	dmd-test d			
	lags	☐ 🖻 firebase-adminsdk-ssrb4@bi-pubsub.iam.gserviceaccount.com	<b>S</b>	firebase-adminsdk F			
\$	Settings	pusher-test-subscription@bi-pubsub.iam.gserviceaccount.com	<b>S</b>	pusher-test-subscription			
Ø	Privacy & Security	D 🖻 pusher-test-tenant-1@bi-pubsub.iam.gserviceaccount.com	<b>S</b>	pusher-test-tenant-1			
~	,	<b>—</b>	-				

In the "Create service account" screen, enter a name for the service account, for example bi-data-export-sa. The Service account ID and the email address are automatically filled in. Enter description in Service account description and click "CREATE AND CONTINUE"



Under "Grant this service account access to project" click on the Role drop-down and select "Pub/Sub Publisher". Click "Done"



3.4 Generate a service account key and download the JSON file.

Navigate to the service account you created in IAM & Admin=>Service accounts

≡	Google Cloud Platform	🐉 bi-p	ubsub 🔫			Q Search service principal		×			
θ	IAM & Admin	Servio	CREATE SERVICE ACCOUNT	TE 🔩 MANA	IGE ACCESS C REFRESH	H Contraction of the second					
•±	IAM	Service accounts for project "bi-pubsub"									
Θ	Identity & Organization	A servio	i service account represents a Google Cloud service identity, such as code numning on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.								
٩	Policy Troubleshooter	Organizi	Organization policies can be used to secure service accounts and block risky service account features, such as automatic MM Grants, key creation-upload, or the creation of service accounts entirely. Learn new about service account organization policies.								
6	Policy Analyzer	Ŧ	₹ Filter Enter property name or value								
	Organization Policies		Email	Status	Name 个	Description	Key ID		Key creation date	OAuth 2 Client ID	Actions
•B	Service Accounts	-	9월 asdfasdf@bi-pubsub.iam.gserviceaccount.com	0	asdfasdf		192922695b390b6ed05ed516	43c4f0282ccf7e4b	May 6, 2022	108488006593442253561 6	:
-	Westland Identity Federation		월 bi-data-export-sa⊗bi-pubsub.iam.gserviceaccount.com	0	bi-data-export-sa	access to bi-data-export-pubsub	No keys			106347024534821878078 6	:

Click on the service account. Select "Create New Key" under "Add key" drop-down/

🛟 bi-pubsub 👻	<b>Q</b> Search service principal	× •	
← bi-data-export-sa			
DETAILS PERMISSIONS KEYS METRICS LOGS			
Keys			
Service account keys could pose a security risk if compromised. We recommend you	avoid downloading service account keys and instead use the <u>Workload Identity Federation</u> . You can lea	m more about the best way to authenticate service accounts on Google Cloud here.	
Add a new key pair or upload a public key certificate from an existing key pair.			
Block service account key creation using organization policies. Learn more about setting organization policies for service accounts			
ADD KEY 👻			
Create new key Key creation date Key expiration date			
Upload existing key			

In the pop-up screen, select "JSON" key type. Click "CREATE"

Create private key for "bi-data-export-sa"				
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.				
Key type				
● JSON				
Recommended				
O P12				
For backward compatibility with code using the P12 format				
CANCEL				

The JSON file will be saved to your computer. Share this file securely with BI SME

Priva	te key saved to your computer	
<b>A</b>	bi-pubsub-57d8868ecdc5.json allows access to your cloud resources, so store it securely. Learn more best prac	tices
		CLOSE

# 4 Beyond Identity Configuration

In BI admin console, navigate to "Integrations", "SIEM". Click on "Add SIEM integration", In "ADD SIEM integration" pop up, choose "Cloud Pub/Sub"

BEYOND IDENTITY		
MONITORING	OIDC SAML WS FED ENDPOINT MANAGEMENT OKTA	
TENANT	SIEM Integrations	FILTER BY Select Filter Add SIEM Integration
<ul> <li>Users</li> <li>Groups</li> </ul>	Edit Elastic Saarch Integration  regu-cassini-elastic-siem  (ACTIVE) Jan 09. 2023, IIS59 AM	Ø
Integrations     Policy     Settings	Edit Splunk Heightiten Cassini-splunk-enterprise Add SIEM Integration Cassini-splunk-enterprise ACTIVE) bec 21, 2022, 1082,244	Ø
	Edit Datadog Integration         SIEM Provider         Log Integration           Cassini-events-adatadog-siem         Log Integration         Cog Integration           CASTIN/FYET Derivation         Cog Integration         Cog Integration	Ø
	Designed to provide reliable, many-to-many, asystchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages	

In "Add SIEM integration" screen, provide a name, the topic name from section 3.2. For the service account upload the file from section 3.4. In events drop down window select all events or only the events interested in. Make the "Status", " Active". Click on "Save changes"



# 5 Appendix

How to get event types?

- Access <a href="https://developer.beyondidentity.com/reference/getevents">https://developer.beyondidentity.com/reference/getevents</a>
- Scroll down the page and under "Responses" look for "200". Click on the button to the right of description

#### RESPONSES

200 Retrieve the given page of events for the given tenant over the given window.	× × × × × × × × × × × × × × × × × × ×
<ul> <li>400</li> <li>Bad request.</li> </ul>	لا <sup>7</sup>

• This will pop-up the screen as shown below. All event types are listed under "event type" string required

# Response • 200 ¢

TOTES THAT HATCHING HER SET TO HERCHING SOTTAIL THAT GOT HIM OF HIM

data from a process not controlled by Beyond Identity.

actor object

The entity whose action caused the event to be emitted.

ACTOR OBJECT

event\_type string required

The type of the event.

USER\_AUTHENTICATION OIDC\_INBOUND OIDC\_COMPLETE WSFED\_INBOUND WSFED\_COMPLETE SAML\_INBOUND SAML\_COMPLETE ADD\_DEVICE POLICY TENANT\_CREATED GROUP\_CHANGE USER\_CHANGE GROUP\_MEMBERSHIP\_CHANGE CONTINUOUS\_AUTHENTICATION DEVICE\_CREDENTIAL\_CHANGE BOOTSTRAP\_INBOUND BOOTSTRAP\_COMPLETE BOOTSTRAP\_KEY\_ROTATION AUTHSERVER\_ACCESS AUTHSERVER\_DIRECTORY\_ACCESS AUTHORIZE\_CONTEXT\_ACCESS APPLICATION\_ACCESS TENANT\_CHANGE OIDC\_CLIENT\_CHANGE CONSOLE\_SSO\_IDP\_CHANGE CONSOLE\_SSO\_OIDC\_AUTH\_CONFIG\_CHANGE CONSOLE\_SSO\_SAML\_AUTH\_CONNECTION\_CHANGE SAML\_CONNECTION\_CHANGE OKTA\_DESKTOP\_LOGIN\_CONFIGURATION\_CHANGE OKTA\_EVENT\_HOOK\_CONFIGURATION\_CHANGE POLICY\_CHANGE OKTA\_REGISTRATION\_ATTRIBUTE\_CONFIGURATION\_CHANGE GPG\_KEY\_CHANGE ENROLLMENT\_CHANGE REALM\_CHANGE SCIM11\_PROVIDER\_CHANGE SCIM20\_PROVIDER\_CHANGE OUTBOUND\_ATTRIBUTE\_UPDATE CREDENTIAL\_CHANGE CREDENTIAL BINDING JOB CHANGE AUTHENTICATOR INVOCATION ATTEMPT

X

+