Access Management and Vulnerability

Thursday, July 1, 2021

**Location: WebEx**

**Attendees:**

Participants (9) 
Q Search 
Oluwaseyi Mafi 
Host, me 
Aerozona Obiadazie 
David Dessommes 
Jason Nazare 
Maria Braun 
Moriah Striegel 
Olivia Lawson 
Sivashankari Shanmugam 
Tyrell Jarrett 

**AGENDA:**

For GCP. The authentication is via Google IAM, and via google service account. We have multiple Azure groups and the users will be part of those groups. They will be segregated depending on their task. If it's development team, there is operation team (they have their azure groups) Engineering groups, testers, users associated. They are directly sync with google services. (Azure platform)

A pipeline account - in prod environment. There are certain task that have couple tactical solutions with respect to scheduling. Having an end to end service. Dep Ops environment.

There is an on prem group. To have the authentication. For example, Say Siva, is Trying to create a pipeline group. Then linked to GCP projects. The dev environment project.

**Change management alongside Access management?**

Any google level service, the Enterprise cloud engineering team is notified.

**Can you provide info on Pre-prod Environment/New access, how that was created?**

Not sure. We can provide information.

**Is there doc CVS health, google cloud users, and their privilege?**

Yes, high level information. We can provide this document. Jason ask to be specific on when this information will be provided. Would it be after the walkthrough?

How they manage the process, different projects.

High Explanat-o 
rilr rdil 
uest High-Lev 
pl. - with 
dp- de 
count. 
ect 
NOTE: this 
pattern be the 
ple 2021 -ea-es 
the big dif 
NOTE: project_narne should not repeat, resources for everything in t 
NOTE: type should not repeat within a project, required re 
NOTE: role name should not repeat within the resource-name 
x block. 
and 
PseudOCOde for requests: 
edp-proiect-nare-l 
1 
grantæ-l th 
grantæ-2 
grantæ-l 
ran-tæ-2 
r.ntæ-x 
grantæ-x (this can repe t 
can 
role-name-x 
grantee 
gran-tee 
grantee 
resource-name -2 
role-name-I 
grantee-I 
antæ•x 
grantæ-x 
1 con 
rep 
for - 
for 
many 
Enablement 
serviceusae.eoogleapis.com 
SGI - 
p dp-dev-eds-dataprocwkr*dp-dev-eds.iam 
++gcp-edp-deu 
-d ed 
-eds lam _ gserul 
dataprcc. aamin 
ecentedmeontdd@eap-dev-eds.iam.eserviceaccount.com 
gcentedmconpddéedp-dev-eds 
dataproc Viewer 
scentedmeontddée 
gcentedmconpddée 
gcentedmeontddéedp-de 
gcentedmconpddßedp-de 
cloudsql_ admin 
cloudsql_ client 
gcentedmconpdd@edp-dev-eds.iam.gserviceaccount.com 

What is included in the above image. Anything that has CVS.com will be azure group. The active directory group. We create request. Once created, we check to see if they are activated. That is how we validate.

Microsoft Azure 
services, 
CVS Health I Overview 
€3 What's 
@aetna 
Got 
ard 
uministratiE units 
kpp registratWE 
Overvi 
NC ræults 
No ræults 
Monitoring 
Tutorials 
S\wwin 
gcp 
app registrations 
the CVS He.lth 
43 

For groups. What are the different service account? All the different service, you will see the user, the admin etc. It is a very elaborate task. Two teams involved. They work together and this is how they are given provisioning.

**Jason: If we select the azure group, do they show the service accounts?**

They are maintained by the GCP IAM.

Also looking into Access Now? Going through the manual piece. There is a manual process that happens? Google IAM or our enterprise IAM?

The cloud engineers are the super admin. They have main access.

Google Cloud Platform 
Select from 
CVS* EALTH.COM 
E DASHBO 
Project info 
'roject 
dp dc.' stomgc 
10 
rojcct 
121014S995 
GO to project Settings 
Resources 
App Ergine 
do not 
Compute Enqir* 
"u cJo not to 
p Type here search 
u•amh and 
STARRED 
digital 
ELI P 
NEB PROJECT 
82272536460 
68C7S741313g 
accsnssssno 
26210273407 
orm status 
"X" billing 
ed#avfrants 
OPEN 
lie 
CUSTOMIZE 
PM 

We get access from the EDP level and down. Anything at the top level, it's the cloud engineering In access now, we let them know the access now groups and complete, so they sync it and it's attached to the project. From that point on, it is part of the google IAM provisioning. We only have a view/read access. I can see the different services accounts, what are the different roles etc. If its management admin, they have added layer of access.

PERMISSIONS 
RECOMMENDATIONS HISTORY 
Permissions for project "edp-dev-storage" 
this and cf its Leam 
ROLES 
1 
= Filter Enter o r 
lope r. 
0 
212169448995@ 
708183-10526. 
co 
Compute 
Engine default 
Sew i æ 
&Jild So-vice 
Sto Admi n 

Only have read access privilege (Image above)

**Do we know who is behind the Service now account?**

The service account are associated to the EDP group.

**Provisioning process**

Going through Aetna access now. Who request and who manages the group listing. But the cloud engineering are the ones who do the seek out once the groups are created. That's what's done by cloud engineering. And once complete, the next level would be done by EDP IAM admin at the project level.

**Recertification process?**

The group is created in the first place then the groups have their own access. The accounts are being brought by the solution engineering. Each groups have dedicated solution engineers. They also make sure which group and level of privileges. Goes into multiple rounds of discussion. As scope expands, they might have a version 10, 11 etc. We maintain this in a separate template and maintaining in Rally. The team uses this info and that's how they pick up.

Deprovisioning Process?

In access now request, and depending on management approval. One or two days. Usually, and SLA of one day is a good estimate. Once a group is created, the cloud engineer syncs up. Depends upon the maturity of the template. Each of these roles is put in place depending on understand. If it is a new team, the template might be pushed back. Say it’s a version 7,

**Any instances?**

It is managed by Access Now.

Google Cloud Platform 
IAM g Admin 
ntiry & 
'olicy TrubleshmtB 
ti PC-IiCieS 
ice Accounts 
Identity Federat, 
Release Notes 
Q s urces 
-2 REMCVE 
IAM 
PERMISSIONS 
•2 ADD 
RECOMMENDATIONS HISTORY 
sto a d m m 
corn 
cloudSQL Auth 
proxy 
Ser. & 
Pub.:Sub Admin 
Pmjcct Admin 
So-.'icc 'dmin 
Storage 
aigcuer,• Job user 
cloud SOL Client 
SQL user 
CVS 
Tech 
VPC 
EDP 
EDP 

**Are we sending logs to anyone to monitor for user activity and outliers?**

All google services and activities are captures in google login. Any activity is captured in login. Say it’s a new project in QA environment or development enjoyment. We need to enable the logs. Logging is captured. All the services, the logs are sent to Splunk (Enterprise supporting monitoring system). They support not just EDP but other enterprise. The tenant will configure their logging. Each client can have their specific….Say they need to configure and email, etc. Not sure what the alerts are, the logs are getting sent to Splunk. Anything specific o CDR, we can follow up with the CDR team.

**Who gets the alerts?**

**Can you give us a POC?**

Yes we can. We can reach out to the team who can provide us with information.

**The Logs from GCP to Splunk? Manual or automated?**

At project level, they go automatically. We give input say for instance these logs need more access, depends on what the use cases are.

**GCP to Splunk? Is that done nightly?**

I think it goes instantaneously. We can get more information on this. The SLAs. I won't say real time, but not batch also.

**Who can make edits to Data in CDR?**

Come back to azure already groups. From the storage layer, whatever the azure already group, if they have read access, depending on the user group and level of access they have. Maybe if we have a prod level of access.

**Can we get # of users who can make edits rights?**

Yes, we can provide information on this.

----------------------------------------------------------------------------------

Vulnerability Management. We will need to schedule a different time to go over this piece.