Configuración de Servidor de Proyecto ATE TECNOLOGÍA en Google Cloud Platform

Versión 1.0 02-09-2022 Presentador Denis Arosquipa Mamani

TÉRMINOS DE CONFIDENCIALIDAD

La información contenida en el presente documento es propiedad de Denis Arosquipa Mamani (en adelante, DEAM). La información contenida se encuentra legalmente protegida por ser privilegiada y confidencial. Cualquier distribución, divulgación, reenvío, copia total o parcial, impresión, reproducción o uso indebido de esta información, sin la autorización expresa por escrito de **DEAM** queda estrictamente prohibida.

Por su parte, **DEAM** se compromete a no divulgar el contenido del presente documento, en lo referente a las necesidades y/o requerimientos específicos de u otro tema de negocios que hubiere sido mencionado en reuniones de trabajo previas.

A. ARQUITECTURA DEL PROYECTO

La arquitectura de los servicios instalados en Google Compute Platform son como sigue el diagrama:



Fig. 1. Arquitectura de la plataforma en GCP

El acceso al proyecto es por el dominio atetecnologia.com que se encuentra registrado y gestionado en Godaddy por DATGEO, todos los demás servicios se encuentran en GCP.

Se usa el Recurso Cloud DNS para usar el dominio con registro tipo A hacia la IP Estática de la VM Compute Engine. La VPC (Virtual Private Cloud) tiene dos subredes una publica y otra privada, la VM se encuentra en la subnet publica, la subnet privada se creó para futuros fines de usar otros recursos o servicios de GCP.

Se creó también un servicio de Cloud Storage para el uso de fotos y archivos TIFF relacionados al proyecto.

El Firewall creado solo permite conexiones por etiquetas de http (80), https (443) y ssh (22) y no son propias de la VM sino a nivel de red (cualquier ingreso a la red solo se permiten por los puertos mencionados como etiquetas)

DETAILS	OBSERVABILITY	OS INFO	SCREENSHOT			
Networkin	g					
Public DNS PTR	Record	None				
Total egress bai	ndwidth tier	-				
NIC type		-				
\rightarrow VIEW IN N	IETWORK TOPOLOGY					
Firewalls						
HTTP traffic		Off				
HTTPS traffic		Off				
Network tag	gs					
db-postgres	http https ssh					
Network int	erfaces					
Name 个	Network Sub	network	Primary internal IP address	Alias IP ranges	Stack Type	External IP address
<u>nic0</u>	dg-att-prod- dg-a vpc sub	att-prod- net-public	10.0.101.2		IPv4	att-prod-ip-public- 835ba62e (34.176.225.229)

Fig. 2. Detalles de la Máquina Virtual

En GCP para su desarrollo de recursos de infraestructura se basa y agrupa por proyectos y para ello se utilizó el proyecto ya creado atetecnologia:

Select a	\$ NEW PROJECT			
Search م				
RECENT	STARRED	ALL		
	Name		ID	
🗸 🏠 🐌	atetecnologia 🕜		atetecnologia	

Fig. 3. Selección del proyecto en GCP

Toda la infraestructura se instaló al proyecto atetecnologia.

1. IAM y Administración

Los recursos creados a nivel IAM:

Se crearon las siguientes cuentas de servicios:

- sa-ansible@atetecnologia.iam.gserviceaccount.com: Se creó para realizar las instalaciones de los softwares en la máquina virtual.
- sa-terraform@atetecnologia.iam.gserviceaccount.com: Se creo para realizar la instalación inicial de la arquitectura de los servicios con Terraform como son la máquina virtual, disco, cloud storage,Cloud SQL, la VPC, las Subnets, los firewalls y la IP estática.
- **sa-app-dat-geo-php@atetecnologia.iam.gserviceaccount.com**: Se creó para el uso de la aplicación PHP para conectarse al cloud storage.
- sa-gcsfuse@atetecnologia.iam.gserviceaccount.com: Se creó para montar el cloud storage en un directorio TIFF del proyecto GeoServer en la Máquina Virtual.

Service accounts for project "atetecnologia" vice account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service acc ization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service a = Filter Enter property name or value Email Name 🛧 Key ID eation date OAuth 2 Client ID Compute Engine default service account <u>€</u> 635656880121-No keys 105698703726503161816 compute@developer.gserviceaccount.com 107651069900766796378 95b9e3befc07caa487360295164db536e207c2ba Aug 30, 2022 $\mathbf{\mathbf{r}}$ 연<u>sa</u>tecnologia.iam.gserviceacco Ansible 107616608018614987352 Service Account for Terrfaform Aug 30, 2022 <u>•⊒ sa</u>-610856bded39095005abf1a63c7de4e9bb5e1350 : terraform@atetecnologia.iam.gserviceaccount.com Terraform Service Account for 🖭 sa-app-dat-geo-5ef14d5199c6f6acab88c19a5ef5e2bde929061a Sep 1, 2022 17545101543139285379 : ologia.iam.gserviceaccount.com dat-geo php Application DatGeo 111893812855616976422 **:** e502c386f466fda3b6932c23fb6018d2420735df Sep 4, 2022 e⊒ sagcsfuse@atetecnologia.iam.gserviceaccount.com acsfuse Account fo Storage with acsfuse

Fig. 4. Listado de Cuentas de Servicio (services account) en IAM

La cuenta de servicio **635656880121-compute@developer.gserviceaccount.com** es la que aparece por defecto de la cuenta GCP.

2. API y Servicios

Se activaron las siguientes Apis para la creación de toda la arquitectura:

Ţ Filtro	Filtro
Nombre	
Compute E	ngine API
Cloud Dom	ains API
Cloud DNS	API
API Gatewa	ay API
Cloud Depl	oyment Manager V2 API
Cloud Files	tore API
Network M	anagement API



3. Compute Engine

Las Instancias de VM se creó una máquina virtual con las siguientes características:

Nombre	dg-att-prod-vm0d02b235
ID de instancia	1038706855530088907
Zona	southamerica-west1-c
Tipo de máquina	e2-standard-4
vCPUs	4
Memory	16 GiB
Disco de arranque	50GB
Disco para base de datos	100GB

4. Cloud Storage

Se crearon dos bucket **stac-bucket-photos** y **stac-bucket-tiff** para el almacenamiento de fotos y archivos TIFF utilizados en el proyecto.

Nombre	stac-bucket-photos
Tipo Ubicación	southamerica-west1
Clase de Almacenamiento	Standard
Acceso público	No
Encriptaciòn	Gestionado por GCP

Nombre	stac-bucket-tiff
--------	------------------

Tipo Ubicación	southamerica-west1
Clase de Almacenamiento	Standard
Acceso público	No
Encriptaciòn	Gestionado por GCP

5. Redes de VPC

Se creó la VPC dg-att-prod-vpc con dos subredes en la region **southamerica-west1**, una subnet privada y otra pública, actualmente se usa la subnet pública y la subnet privada se dejaría para otros procesos y/o desarrollos que se necesite.

dg-att-	prod-vpc										
Subnet cr Custom su	reation mode										
Dynamic Global	routing mode										
VPC netw Disabled	vork ULA interr	al IPv6 range									
DNS serv None	er policy										
Maximun 1460	n transmission	unit									
SUBN	IETS S	TATIC INTERNAL IP	ADDRESSES	FIREWALLS ROUT	ES VPC NETWORK	PEERING PRIVATE SER	VICE CONNECTIO	N			
ADD SU	JBNET FL	OW LOGS 👻									
∓ Fił	iter Enter proj	perty name or value								0	III
∓ Fil	ter Enterprop Name ↑	perty name or value Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs	0	III
≂ Fil	ter Enter prop Name 个 dg-att- prod- subnet- private	Region southamerica- west1	Stack Type	Internal IP ranges	External IP ranges None	Secondary IPv4 ranges None	Gateway	Private Google Access Off	Flow logs 😧 Off	•	III

Fig. 6. Detalles del VPC dg-att-prod-vpc

Se creo una dirección IP estática (att-prod-ip-public-835ba62e) que es utilizada para la máquina virtual la IP es 34.176.225.229

IP addresses RESERVE EXTERNAL STATIC ADDRESS C REFRESH RELEASE ST					SE STATIC ADDR	ESS		E HELP ASSISTAL	NT SHOW INFO P/	
ALL	INTERN	AL IP ADDRESSES	EXTERNAL IP A	DDRESSES IF	V4 ADDRESSES	IPV6 AD	DRESSES			
∓ Fil	ter Enter prop	erty name or value								0
	Name	IP address	Access type	Region	Туре 🗸	Version	In use by	Subnetwork	VPC Network	Network Tier 🔞
	att-prod- ip-public- 835ba62e	34.176.225.229	External	southamerica- west1	Static	IPv4	VM instance dg-att-prod- vm0d02b235 (Zone southamerica- west1-c)			Premium

Fig. 7. Listado de IP creadas en la VPC

Se creo una regla de firewall con destinos de etiquetas, es decir que fácilmente cualquier máquina virtual se anexe al firewall por etiquetas de red, las reglas son:

VPC fi	PC firewall rules														
Firewall r traffic fro	ewall rules control incoming or outgoing traffic to an instance. By default, incoming Iffic from outside your network is blocked. Learn more														
Note: App	ste: App Engine firewalls are managed in the App Engine Firewall rules section 12.														
🥊 SMTP	SMTP port 25 disallowed in this project 🛛														
C REF	C REFRESH														
∓ Fil	ter Network :	projects/ateteo	cnologia/global/n	etworks/dg-att-	prod-vpc 🛞 Enter	property name or value	е					×	0	ш	
	Name	Туре	Targets	Filters	Protocols / ports	Action	Priority	Network 个	Logs	Hit count 🔞	Last hit 😯	Insights			
	att-prod-fw- allow-http	Ingress	http	IP ranges: I	tcp:80	Allow	1000	dg-att-prod- vpc	Off	_	-		~		
	att-prod-fw- allow-https	Ingress	https	IP ranges: I	tcp:443	Allow	1000	dg-att-prod- vpc	Off	_	_		~		
	att-prod-fw- allow- postgres	Ingress	db-postgres	IP ranges: (tcp:5432	Allow	1000	dg-att-prod- vpc	Off	-	-		~		
	att-prod-fw- allow-ssh	Ingress	ssh	IP ranges: I	tcp:22	Allow	1000	dg-att-prod- vpc	Off	_	-		~		
	att-prod-fw- allow-tomcat	Ingress	tomcat	IP ranges: I	tcp:8080	Allow	1000	dg-att-prod- vpc	Off	_	_		~		

Fig. 8. Identificación de los firewalls creados en la VPC

6. Monitoreo

Todos los servicios y/o recursos de GCP tienen disponibles paneles o dashboard de monitoreo y visibilidad por ejemplo de Capacidad de Disco, CPU, Memoria, etc:

VM Details RESET ZOO	M 1 HOUR 👻	I MANAGE VM SSH 🝷 SEND FEEDBACK 🗙
dg-att-prod-vm0d02b2	35	⊼
Installed agent	ot Detected INSTALL OPS AGENT	♠ Alerts → No open incidents
		Image: Second system Image: Second system No recent events Image: Second system
		Uptime Checks → No failed checks
Additional details: instance_id : 10 METRICS LOGS	338706855530088907 zone : southamerica-west1-c View Details	
CPU Processes	New Connections with VMs/External/Google Disk T	hroughput 😧 🚦
Memory Network Summary Packet Mirroring Disk	UTC-5 12:10 PM 12:20 PM 12:30 PM 12:40 PM 12:50 PM UTC-5	12:10 PM 12:20 PM 12:30 PM 12:40 PM 12:50 PM
Performance Capacity	Logs by Top Severity 😧 Disk Id	DPS @ 50%
ña nueva	UTC-5 12:10 PM 12:20 PM 12:30 PM 12:40 PM 12:50 PM UTC-5	12:10 PM 12:20 PM 12:30 PM 12:40 PM 12:50 PM

Fig. 9. Monitoreo y Visibilidad de los recursos de la Máquina Virtual.

7. Copias de seguridad de Discos

Existe dos discos duros configurados: uno es de la Máquina Virtual de 50Gb propio del boot o inicio de la máquina, donde se encuentra todas las configuraciones e instalaciones de los servicios, y el otro disco es de la base de datos de PostgreSQL que es la data propiamente. Estos discos se encuentran configurados para que se realice diariamente instantáneas o snapshots:

Use snaj persister	Jse snapshot schedules to regularly and automatically back up your zonal and regional versistent disks. <u>Learn more</u>												
SNAPSHOTS ARCHIVE SNAPSHOTS			PSHOTS S	NAPSHOT SCHEDULES									
Ŧ	ilter Enter pro	operty name or va	lue					0 III					
	Status	Name 🛧	Region	Schedule frequency (UTC)	Autodelete snapshots after	In use by		Creation time					
	٢	<u>schedule-</u> disk- postgres	southamerica- west1	Every day, starts between 8:00 AM and 9:00 AM	10 days	dg-att-pr	~	Sep 7, 2022, 11:42:18 PM UTC-05:00					
	٢	<u>schedule-</u> disk-vm	southamerica- west1	Every day, starts between 9:00 AM and 10:00 AM	10 days	dg-att-pr	~	Sep 7, 2022, 11:44:14 PM UTC-05:00					

Fig. 10. Monitoreo y Visibilidad de los recursos de la Máquina Virtual.

Las copias son realizadas en la misma región, no son multiregion:

- El disco de la VM de 50Gb se realiza de 9am a 10am horario UTC que serían de 4am a 5am
- El disco de PostgreSQL de 100Gb se realiza de 8am a 9am UTC que serían de 3am a 4am

Los archivos son generados hasta dentro de 10 días.

B. SOFTWARE INSTALADOS

El sistema operativo instalado fue Ubuntu 20.04.5 LTS (Focal Fossa):



Fig. 11. Versión del Sistema Operativo y Kernel de Linux instalados.

El servidor actualmente no tiene un antivirus instalado, es posible instalarlo dependiendo de la lógica o el flujo de negocios que se pretenda operar.

Por defecto la máquina virtual viene con el servicio de SSH para poder ingresar y gestionar la máquina, el ingreso a la máquina se pueden ingresar de varias formas:

 Con la misma cuenta de Gmail una vez ingresado a Google se ingresa a https://console.cloud.google.com y se tendrá acceso a todos los recursos de GCP, luego en la sección de Compute Engine -> Instancias de VM:

≡ Google Cloud	atetec	VIRTUAL MACHINES
Cloud overview	>	VM instances
C Recent	>	Sole-tenant nodes
View all products		Machine images TPUs
PINNED Pin your top products here		Committed use discounts Migrate to Virtual Machines
		STORAGE
Security	'	Disks
Anthos	>	Snapshots
COMPUTE		Images
Compute Engine	>	INSTANCE GROUPS
🚯 Kubernetes Engine		Hoalth chooks

Fig. 12. Menú de ingreso a la Máquina Virtual.

Seleccionamos la máquina virtual **dg-att-prod-vm0d02b235** y seleccionamos el botón de SSH:



Fig. 13. Botón de ingreso a la consola SSH de la Máquina Virtual.

Se iniciará en una nueva ventana el ingreso por SSH directamente.



Fig. 14. Consola Web de SSH de la Máquina Virtual.

 La otra forma de ingresar es por ssh directo desde la máquina local (con bash, cmd, powershell, git bash, putty, etc.). Es requisito que la llave pública de la máquina local este registrada en GCP en la misma instancia de VM, actualmente se tiene el usuario ubuntu registrado con la llave pública de momento para las instalaciones y configuraciones adicionales y adicional a ello con la IP publica que es 34.176.225.229

≡	Google Cloud so atete	nologia Q Search Products, resources, docs (/)	D
۲	Compute Engine	← dg-att-prod-v	ARN
Virtual	machines ^	DETAILS OBSERVABILITY OS INFO SCREENSHOT	
B	VM instances	Integrity Monitoring 🖗 On	
<u>ا</u>	Instance templates		-
8	Sole-tenant nodes	SSH Keys SSH keys	
=	Machine images	Username Key	
X	TPUs	ubuntu ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC67xbikMxII+ItyvO3vZt7dR/s01wJ5mH85golkqm4xu/VrmkwSJKPSkqOoeTx	т.
1%1	Committed use discounts	Block project-wide SSH keys Off	
Ø Migrate to Virtual Machin			
API and identity management		API and identity management	
	Disks	Service account None	
0	Snapshots	Management	1
¥.	Marketplace	Availability policies	
Ē	Release Notes	VM provisioning model 🚱 Standard	
		Preemptibility Off (Recommended)	
~			

Fig. 15. Clave pública registrada para el ingreso a la consola SSH.

Es posible reemplazar esa llave pública por la que utilicen finalmente.



Fig. 16. Consola SSH desde el computador o cliente.

Todos los softwares instalados se encuentran en la máquina virtual y a continuación lo detallamos:

1. **Nginx**: La versión es 1.18.0 y se instalaron las configuraciones por defecto y adicional a ello se configuró dos proxys que sirven a los servicios de PHP-FPM y a Tomcat.

ubuntu@att-vm0d02b235:~\$ nginx -V
nginx version: nginx/1.18.0 (Ubuntu)
built with OpenSSL 1.1.1f 31 Mar 2020
TLS SNI support enabled
configure arguments:with-cc-opt='-g -02 -fdebug-prefix-map=/build/nginx-7KvRN5/nginx-1.18.0=fstack-protector-strong -Wformat -Werror=format-security -fP
IC -Wdate-time -D_FORTIFY_SOURCE=2'with-ld-opt='-Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now -fPIC'prefix=/usr/share/nginxconf-path=/etc/nginx/ng
inx.confhttp-log-path=/var/log/nginx/access.logerror-log-path=/var/log/nginx/error.loglock-path=/var/lock/nginx.lockpid-path=/run/nginx.pidmodu
les-path=/usr/lib/nginx/moduleshttp-client-body-temp-path=/var/lib/nginx/bodyhttp-fastcgi-temp-path=/var/lib/nginx/fastcgihttp-proxy-temp-path=/var/lib
ib/nginx/proxyhttp-scgi-temp-path=/var/lib/nginx/scgihttp-uwsgi-temp-path=/var/lib/nginx/uwsgiwith-debugwith-compatwith-pcre-jitwith-http_ss
l_modulewith-http_stub_status_modulewith-http_realip_modulewith-http_auth_request_modulewith-http_v2_modulewith-http_dav_modulewith-http_sli
ce_modulewith-threadswith-http_addition_modulewith-http_gunzip_modulewith-http_gzip_static_modulewith-http_image_filter_module=dynamicwith-http_gunzip_modulewith-http_gzip_static_modulewith-http_image_filter_module=dynamicwith-http_graphical definition and the statementwith-http_graphical definition and the statementwith-http_gr
ttp_sub_modulewith-http_xslt_module=dynamicwith-stream=dynamicwith-stream_ssl_modulewith-mail=dynamicwith-mail_ssl_module
ubuntu@att-vm0d02b235:~\$

Fig. 17. Versión del NGINX instalado con sus módulos activos.

Proxy para atetecnologia.com:



```
location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi pass unix:/var/run/php/php8.1-fpm.sock;
        }
  listen 443 ssl; # managed by Certbot
  ssl_certificate /etc/letsencrypt/live/atetecnologia.com/fullchain.pem; # managed by Certbot
  ssl certificate key /etc/letsencrypt/live/atetecnologia.com/privkey.pem; # managed by Certbot
  include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
  ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}
server {
  if ($host = atetecnologia.com) {
     return 301 https://$host$request_uri;
  } # managed by Certbot
        server_name atetecnologia.com;
  listen 80:
  return 404; # managed by Certbot
```

Proxy para gs.atetecnologia.com:

cat /etc/nginx/conf.d/gs.atetecnologia.com.conf	
server { server_name gs.atetecnologia.com; location / {	
proxy_pass http://127.0.0.1:8080; proxy_pass_header Set-Cookie; proxy_set_header Host \$host; proxy_set_header X-Forwarded-Proto \$scheme; proxy_set_header X-Forwarded-For \$proxy_add_x_forwarded_for;	
<pre>} location /geoserver { proxy_pass http://127.0.0.1:8080/geoserver; proxy_pass_header Set-Cookie; proxy_set_header Host \$host; proxy_set_header X-Forwarded-Proto \$scheme; proxy_set_header X-Forwarded-For \$proxy_add_x_forwarded_for; }</pre>	

	error_log /var/log/nginx/gs.atetecnologia-error.log warn; access_log /var/log/nginx/gs.atetecnologia-access.log;
	listen 443 ssl; # managed by Certbot ssl_certificate /etc/letsencrypt/live/gs.atetecnologia.com/fullchain.pem; # managed by Certbot ssl_certificate_key /etc/letsencrypt/live/gs.atetecnologia.com/privkey.pem; # managed by Certbot include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}	
S	erver { if (\$host = gs.atetecnologia.com) { return 301 https://\$host\$request_uri; } # managed by Certbot
}	listen 80; server_name gs.atetecnologia.com; return 404; # managed by Certbot

En el documentRoot de atetecnologia.com se sirven los siguientes archivos:



Fig. 18. Directorio y archivos de atetecnologia.com.

Y en el gs.atetecnologia.com se sirven los archivos de GeoServer:



Fig. 19. Directorios y archivos de gs.atetecnologia.com

2. Certbot: Para la gestión de certificados para HTTPS se instalaron letsencrypt estos proporcionan durante 90 días renovables certificados gratis y tienen la encriptación máxima y semejante a certificados de paga con la diferencia que son firmados por LetsEncrypt. Actualmente la configuración que existe es para Nginx con los proxys mencionados y adicional a ello se configuró un proceso en el Cron para la renovación automática de los certificados. 3. **CronJob**: Las tareas programadas se encuentra con la cuenta del usuario root:



Fig. 20. Tareas programadas en el cron de Linux en la cuenta del usuario root.

Existe un proceso:

Renovación de SSL: cada 90 días el certificado vence y lo que hace la tarea es revisar todos los días a las 12 de media noche y 12:12 de media noche.

4. PHP: Se instalo la versión 8.1.9 con los siguientes módulos:



Fig. 21. Versión del PHP instalado

php -m	
[PHP Modules]	pdo_pgsql
calendar	pgsql
Core	Phar
ctype	posix
curl	readline
date	Reflection
exif	session
FFI	shmop
fileinfo	sockets
filter	sodium
ftp	SPL
gd	standard
gettext	sysvmsg

hash	sysvsem
iconv	sysvshm
intl	tokenizer
ison	Zend OPcache
libxml	zip
mbstring	zlib
mcrvpt	
openssl	[Zend Modules]
pentl	Zend OPcache
pcre	
PDO	
1.20	

5. **Python**: Se instalo la versión 3.10.4 con los siguientes módulos:

ubuntu@att-vm0d02b235:~\$ python -V Python 3.10.6 ubuntu@att-vm0d02b235:~\$

Fig. 22. Versión de Python instalado

pip list	
Package / Versión Pa	ackage / Versión
attrs19.3.0perAutomat $0.8.0$ Pillbeautifulsoup4 $4.8.2$ pipblinker 1.4 plocertifi2019.11.28prochardet $3.0.4$ psyClick 7.0 pyzcloud-init22.2pyzcolorama $0.4.3$ pyccommand-not-found 0.3 pycconfigobj $5.0.6$ Pyyconstantly $15.1.0$ Pyxcyplography 2.8 Pylcupshelpers 1.0 Pyrcycler $0.10.0$ pyrdbus-python $1.2.16$ Pyldefer $1.0.6$ pyrdistro $1.4.0$ pyrdistro-info $0.23ubuntu1$ Pyrentrypoints 0.3 pyrfuture $0.18.2$ pyrfuture $0.14.0$ pyrhtml5lib $1.0.1$ pyrhtplib2 $0.14.0$ pyrhyperlink $19.0.0$ pyridna 2.8 pyrimportlib-metadata $1.5.0$ Pyr	expect 4.6.0 llow 7.0.0 p 22.2.2 otly 4.4.1 otobuf 3.6.1 sycopg2 2.8.4 /asn1 0.4.2 /vasn1 1.6.2 /vcups 1.9.73 /gments 2.3.1 /gObject 3.36.0 /yHamcrest 1.9.0 /yWT 1.7.1 /macaroons 0.13.0 /yNACI 1.3.0 /QDenSSL 19.0.0 /yrsistent 0.15.5 /yserial 3.4 /thon-dateutil

ipython_genutils 0.2.0 Jinja2 2.10.1 jsonpatch 1.22 jsonpointer 2.0 jupyter-core 4.6.3 keyring 18.0.1 kiwisolver 1.0.1 language-selector 0.1 launchpadlib 1.10.13	requests-unixsocket 0.2.0 retrying 1.3.3 SecretStorage 2.3.1 service-identity 18.1.0 setuptools 45.2.0 simplejson 3.16.0 sip 4.19.21 six 1.14.0 sos 4.3 soupsieve 1.9.5
lazr restfulclient 0 14 2	ssh-import-id 5.10
iazr.uri 1.0.3	systema-python 234
lxml 4.5.0	traitlets 4.3.3
macaroonbakery 1.3.1	Twisted 18.9.0
MarkupSafe 1.1.0	ubuntu-advantage-tools 27.10
matplotlib 3.1.2	ufw 0.36
more-itertools 4.2.0	unattended-upgrades 0.1
nbformat 5.0.4	urllib3 1.25.8
netifaces 0.10.4	wadllib 1.3.3
numpy 1.17.4	webencodinas 0.5.1
oauthlib 310	wheel 0.37.1
OWSLID 0.19.1	zope.interface 4.7.1

6. **PostgreSQL Server**: La versión instalada es 14.2 en SQL Cloud con las siguientes extensiones:

postgres=# \dx			
List of installed extensions			
Name	Version	Schema	Description
plpgsql	1.0	pg_catalog	PL/pgSQL procedural language
postgis	3.2.3	public	PostGIS geometry and geography spatial types and functions
postgis_raster	3.2.3	public	PostGIS raster types and functions
postgis_topology	3.2.3	topology	PostGIS topology spatial types and functions
(4 rows)			
postgres=#			

Fig. 23. Listado de extensiones instaladas en el Postgres.

Se creó la base de datos dbgeo (sin tablas).

Actualmente PostgreSQL se encuentra configurado principalmente con los siguientes parametros:

/etc/postgresql/14/main/postgresql.conf
DB Version: 14 # OS Type: linux # DB Type: web # Total Memory (RAM): 1 GB # CPUs num: 2 # Data Storage: ssd

max connections = 200 shared buffers = 256MB effective cache size = 768MB maintenance_work_mem = 64MB checkpoint_completion_target = 0.9 wal_buffers = 7864kB default statistics target = 100 random page cost = 1.1effective_io_concurrency = 200 work mem = 1310kB min wal size = 1GB max_wal_size = 4GB max_worker_processes = 2 max_parallel_workers_per_gather = 1 max parallel workers = 2max_parallel_maintenance_workers = 1



7. Tomcat: La versión instalada es la 9 y se instaló para instalar el paquete de GeoServer en modo WAR. Se encuentra instalada como servicio. El servicio se encuentra instalado en /var/lib/tomcat9.Tomcat se encuentra como salida hacia un proxy con Nginx y sirve la aplicación en:

https://gs.atetecnologia.com

8. **GeoServer**: La versión instalada es 2.20 y se encuentra instalada como paquete WAR y se ejecuta en el servidor de aplicaciones Tomcat 9, los archivos se encuentran instalados en /var/lib/tomcat9/webapps/geoserver. La aplicación se consume en el proxy de Nginx con el dominio:

https://gs.atetecnologia.com/geoserver

9. **SFTP**: Se instalo FTP con acceso seguro SSH y los accesos a los usuarios se distribuyen en los siguientes directorios:



Fig. 24. Listado de archivos disponibles para los usuarios de FTP.

Los accesos son al proyecto web y al proyecto geoserver. Existen dos usuarios heine.valverde y fabio.ohara los directorios son los mismos. El directorio /home/usuario/atetecnologia.com es un directorio montado del directorio /app y el directorio /home/usuario/geoserver/data es un directorio montado del directorio /var/lib/tomcat9/webapps/geoserver/data/data y /home/usuario/geoserver/styles es un directorio montado del directorio /var/lib/tomcat9/webapps/geoserver/data/styles.

El directorio /var/lib/tomcat9/webapps/geoserver/tiff es un directorio montado del cloud storage con gcsfuse (driver herramienta) del bucket stac-bucket-tiff

El montado es permanente y configurado en el /etc/fstab



Fig. 25. Contenido actual del archivo /etc/fstab.

Y el directorio /mnt/disks/postgresql contiene la data de PostgreSQL la partición es un disco SSD externo montado de 100GB.

C. CREDENCIALES Y ACCESOS

Los accesos a los softwares instalados y/o configurados:

- 1. Por SSH: se accede por claves públicas o directamente por la cuenta del correo Gmail
- 2. Por SFTP: los accesos son al Host 34.176.225.229, puerto 22 los usuarios son dos:
 - Username: heine.valverde Password: CqZTEVzVF5PZ7Cu9hxRP\$
 - Username: fabio.ohara Password: JGhRmZwqR54L6RfxrkqH.
- 3. A GeoServer:
 - URL: <u>https://gs.atetecnologia.com/geoserver/</u>
 - Username: admin
 - Password: \$geoS3rv3r\$
- 4. PostgreSQL Server:
 - host: 34.176.225.229
 - user: root

- password: LxQpDN69T5zWyQRwwrHM
- database: dbgeo

D. RECOMENDACIONES

- Es recomendable activar notificaciones y/o alertas de consumos de memoria, cpu o espacio hacía correo electrónico o mensaje de texto.
- Es recomendable tener una integración y entrega continua de cambios en los aplicativos que se tenga en el servidor y asi por buenas prácticas evitar el ingreso directo por SSH o SFTP al servidor.
- A futuro es posible llevar a cabo dockerizar las aplicaciones instaladas en la VM y así migrar a un desarrollo serverless.