ADVANCED ACCESS INDETITY MANAGEMENT MODEL ON AWS (IAM)

*Analysis and development of a proposed multilevel security model based on the advanced access identity management model

1st Freddy Leonel Pachacama
dept. Computer´s Science Application of Operating Systems
Sangolquí, Ecuador
flpachacama@espe.edu.ec

1st Kevin Quimuña
dept. Computer´s Science Application of Operating Systems
Sangolquí, Ecuador
kfquimuna@espe.edu.ec

***Abstract*—The purpose of this project is to implement a multilevel security model based on the organizational structure of the company Cayambito dedicated to has to offer traditional products of the sector. This through Aws as advanced access identity management tool, it is intended to also make known what it consists of and how a directory server. Within this framework it will be seen how to create a directory structure, database and its setting. The practical part will consist of the application of the theoretical part in an example of operation using two computers for this purpose in order to see the process of authentication. At the end of the project, a vision of what can be applied (IAM) will be obtained, as well as the recommendations necessary for its implementation.**

***Index Terms*—IAM, Security Multilevel, Method, Organization, hierarchy.**

I. GOALS

A. General

Analyze and develop a proposal for an advanced identity access management model (IAM)

B. Specific

Select a business model organization based on from which a hierarchy of levels of access to the information of the institution

Preparate an access and permission matrix according to the established hierarchy.

II. THEORETICAL FRAMEWORK

A. Advanced access identity management model

Also known as MLS (Multiple Level Security), is a type of security policy that classifies users into different security levels, allowing access simultaneous to different users with different permissions and making sure that each user accesses those resources that you are authorized to and in the manner that you are authorized to, for therefore it is a technology that allows to protect secrets and thus prevent any user from accessing certain information whose access you are not allowed. Security technology multilevel classifies the data using the information security levels: (Highest) Top secret, (High) Secret, (Lower) Confidential, (Lower) Unclassified. One is for refer to a system that is adequate to protect itself of subversion and has robust mechanisms for separating of information, that is, reliable. The other refers to a computer application that will require it to be strong enough to protect itself from subversion and which means adequate mechanisms to separate domains of information.

B. IAM

AWS identity and access management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage the permissions that control which AWS resources users can access.

III. MATERIALS

- Laptops
- Windows 11 Operating System
- Internet Access
- AWS account

IV. Instructions

A. Business Model

- Select a business model or organization. Cayambito is an Ecuadorian company dedicated to the production and distribution of traditional sweets with high quality standards at an affordable price, allowing wholesale and retail purchases.

Fig. 1. Cayambito Logo

- Establish a hierarchy of levels of access to the information of the institution.

The company hierarchy is as follows:

B. Company Matrix

- Prepare an access and permissions matrix according to the established hierarchy.

After analyzing the hierarcgy, the matrix of according to the levels that belong.

C. Basic implementation to demonstrate the model according to the levels in AWS.

- *Steps:*

1. We create an AWS account.
2. We create imagine to EC2 and S3
3. We are going to create new users, and we go to the IAM part.
4. We enter the username and select the type of access, finally we give a password.
5. On the next page we add the permissions, we can associate it to a group or give permissions to only one user.
6. We can add tags where they are labeled to each infrastructure of our company.
7. At the end we will have the review screen where we can see all the configurations that we have given to our user.
8. Once our user has been created, we can verify that it was created correctly simply by entering AWS again with the newly created account.

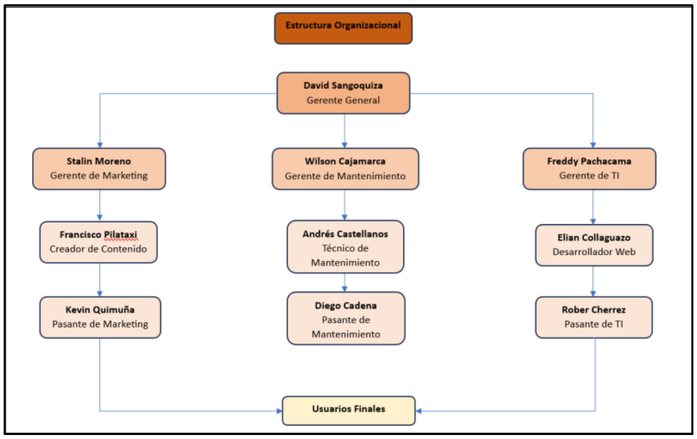
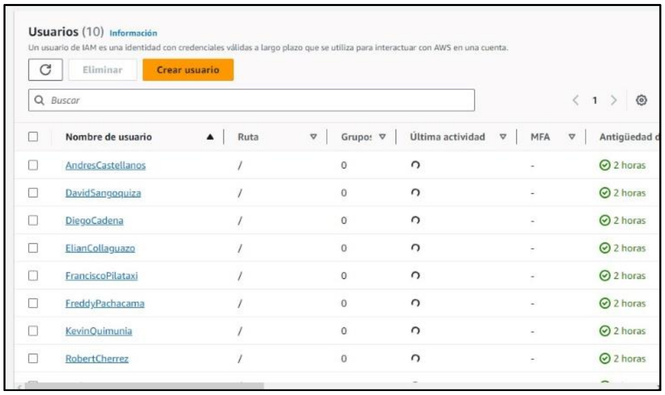


Fig. 2. Cayambito Hierarchy

	Ultra secreto (A1)	Secreto (A2)	Confidencial (B1)	No clasificado (C)
Departamento de Marketing	Informe de Estrategia de Producto	Campaña de Marketing Confidencial	Investigación de Mercado Anónima	Videos Publicitarios
Departamento de Mantenimiento		Plan de Mantenimiento de Equipos Críticos	Registro de Mantenimiento Preventivo	
Departamento de TI	Arquitectura de Red y Seguridad	Política de Acceso a Datos de Usuarios	Guía de Respaldo y Recuperación	Página Web

Fig. 3. Cayambito Matrix



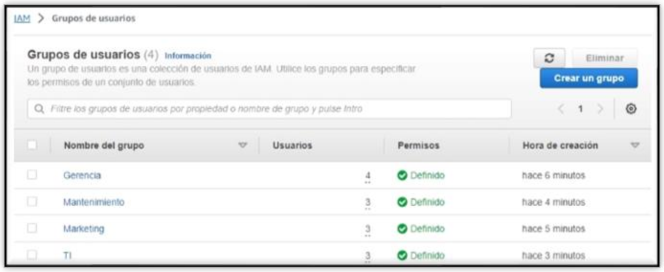
Usuarios (10) Información

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

Buscar

☐	Nombre de usuario	Ruta	Grupos	Última actividad	MFA	Antigüedad d
☐	AndresCastellanos	/	0		-	2 horas
☐	DavidSangoquiza	/	0		-	2 horas
☐	DiegoCadena	/	0		-	2 horas
☐	ElianCollaguazo	/	0		-	2 horas
☐	FranciscoPilataxi	/	0		-	2 horas
☐	FreddyPachacama	/	0		-	2 horas
☐	KevinQuimunia	/	0		-	2 horas
☐	RobertCherrez	/	0		-	2 horas

Fig. 4. Step 1



IAM > Grupos de usuarios

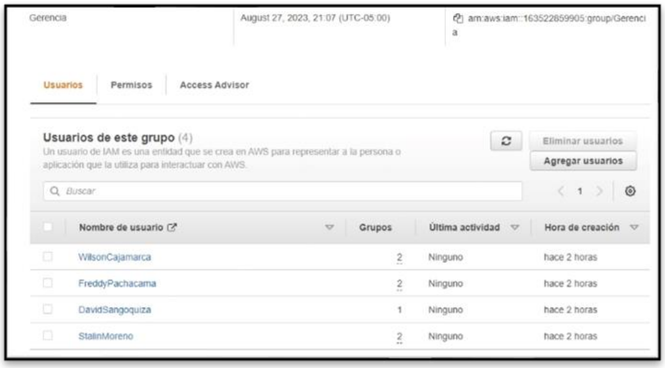
Grupos de usuarios (4) Información

Un grupo de usuarios es una colección de usuarios de IAM. Utilice los grupos para especificar los permisos de un conjunto de usuarios.

Filtre los grupos de usuarios por propiedad o nombre de grupo y pulse Intro

☐	Nombre del grupo	Usuarios	Permisos	Hora de creación
☐	Gerencia	4	Definido	hace 6 minutos
☐	Mantenimiento	3	Definido	hace 4 minutos
☐	Marketing	3	Definido	hace 5 minutos
☐	TI	3	Definido	hace 3 minutos

Fig. 5. Step 2



Gerencia | August 27, 2023, 21:07 (UTC-05:00) | arn:aws:iam::163522859905:group/Gerencia

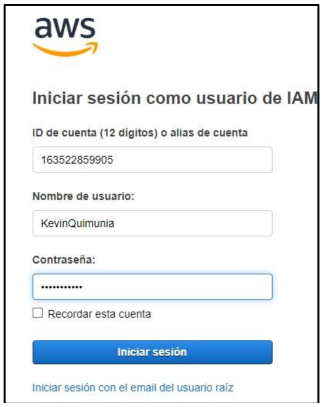
Usuarios de este grupo (4)

Un usuario de IAM es una entidad que se crea en AWS para representar a la persona o aplicación que la utiliza para interactuar con AWS.

Buscar

☐	Nombre de usuario	Grupos	Última actividad	Hora de creación
☐	WilsonCajamarca	2	Ninguno	hace 2 horas
☐	FreddyPachacama	2	Ninguno	hace 2 horas
☐	DavidSangoquiza	1	Ninguno	hace 2 horas
☐	StalinMoreno	2	Ninguno	hace 2 horas

Fig. 6. Step 3



Iniciar sesión como usuario de IAM

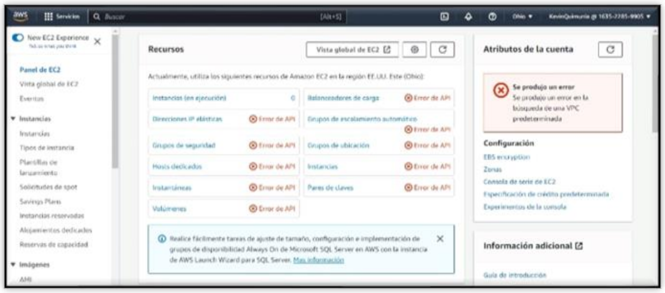
ID de cuenta (12 dígitos) o alias de cuenta: 163522859905

Nombre de usuario: KevinQuimunia

Contraseña: ••••••••••••

☐ Recordar esta cuenta

Fig. 7. Step 4



Recursos

Actualmente, utiliza los siguientes recursos de Amazon EC2 en la región EE.UU. Este (Ohio):

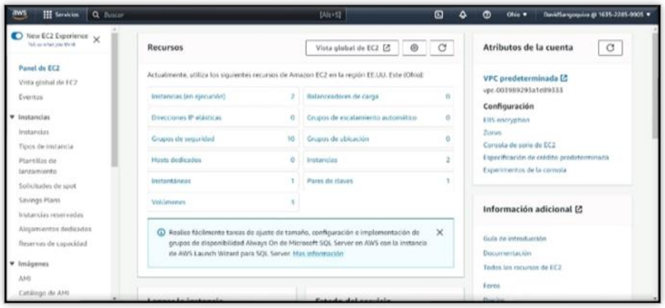
Instancias (en ejecución)	0	Balanceadores de carga	Error de API
Direcciones IP elásticas	Error de API	Grupos de escalamiento automático	Error de API
Grupos de seguridad	Error de API	Grupos de ubicación	Error de API
Hosts dedicados	Error de API	Instancias	Error de API
Instantáneas	Error de API	Pares de claves	Error de API
Volúmenes	Error de API		

Realice fácilmente tareas de ajuste de tamaño, configuración e implementación de grupos de disponibilidad Always On de Microsoft SQL Server en AWS con la instancia de AWS Launch Wizard para SQL Server. Más información

Atributos de la cuenta

Se produjo un error
Se produjo un error en la búsqueda de una VPC predeterminada

Fig. 8. Step 5



Recursos

Actualmente, utiliza los siguientes recursos de Amazon EC2 en la región EE.UU. Este (Ohio):

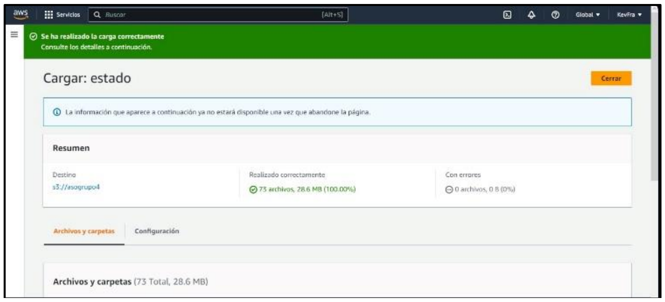
Instancias (en ejecución)	2	Balanceadores de carga	0
Direcciones IP elásticas	0	Grupos de escalamiento automático	0
Grupos de seguridad	10	Grupos de ubicación	0
Hosts dedicados	0	Instancias	2
Instantáneas	1	Pares de claves	1
Volúmenes	5		

Realice fácilmente tareas de ajuste de tamaño, configuración e implementación de grupos de disponibilidad Always On de Microsoft SQL Server en AWS con la instancia de AWS Launch Wizard para SQL Server. Más información

Atributos de la cuenta

VPC predeterminada
vpc-003989293a1e89333

Fig. 9. Step 6



Se ha realizado la carga correctamente
Consulte los detalles a continuación.

Cargar: estado

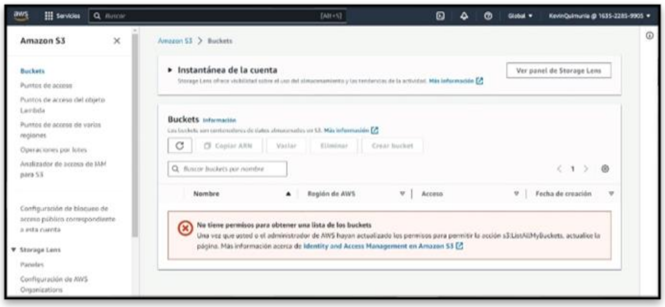
La información que aparece a continuación ya no estará disponible una vez que abandone la página.

Resumen

Destino	Realizado correctamente	Con errores
s3://asogrupo4	73 archivos, 28.6 MB (100.00%)	0 archivos, 0 B (0%)

Archivos y carpetas (73 Total, 28.6 MB)

Fig. 10. Step 7


Servicios
Buscar
[Alt+S]
Global
KevinQuimuria @ 1635-2285-9905
Amazon S3
Buckets
Puntos de acceso
Puntos de acceso del objeto Lambda
Puntos de acceso de varias regiones
Operaciones por lotes
Analizador de acceso de IAM para S3
Configuración de bloqueo de acceso público correspondiente a esta cuenta
Storage Lens
Paneles
Configuración de AWS Organizations
Amazon S3 > Buckets
Ver panel de Storage Lens
Copiar ARN
Vaciar
Eliminar
Crear bucket
Buscar buckets por nombre
Nombre
Región de AWS
Acceso
Fecha de creación

Instantánea de la cuenta
Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de la actividad. Más información

Buckets Información
Los buckets son contenedores de datos almacenados en S3. Más información

No tiene permisos para obtener una lista de los buckets
Una vez que usted o el administrador de AWS hayan actualizado los permisos para permitir la acción s3:ListAllMyBuckets, actualice la página. Más información acerca de Identity and Access Management en Amazon S3

Fig. 11. Step 8

CONCLUSIONS

- It can be concluded that when carrying out this project we have knowledge of the most important theoretical concepts related to the advanced access methodology in AWS.
- After the installation tests, configurations and user creations, it is possible to understand and know how important, useful and practical it is to have a directory of users, in the case given of a company, or as of any other type of information.
- In AWS we find several preconfigured access lists, which can be used to practice giving access to users or groups of users.

RECOMMENDATIONS

- Always keep in mind how far the free limit in AWS goes in order to avoid unnecessary expenses.
- In case it is difficult to carry out the practice, there are several tutorials on digital platforms with very good explanations.
- For the creation of users, it is advisable to take into account what permissions you want to give and for whim that user will be directed.

REFERENCES

[1] J. Lopez, “Seguridad multinivel´´, April 2008
[2] G. Tugurium, “Bell-LaPadula model´´, December 2005
[3] I. S. Jacobs “phpLDAPadmin”, September 2007