[Publish] - Access and User Management in AWS IAM Identity Center

Su entorno de AWS Landing Zone Accelerator (LZA) utiliza AWS IAM Identity Center (antes conocido como AWS Single Sign-On) para gestionar el acceso a las cuentas de AWS y asignar permisos a través de usuarios, grupos y conjuntos de permisos administrados de forma centralizada.

Este documento explica cómo se crean y gestionan los usuarios, cómo se otorgan los permisos, cómo acceder a AWS por primera vez y cómo su equipo puede personalizar los roles y el acceso en el futuro.

1. ¿Qué es AWS IAM Identity Center?

AWS IAM Identity Center proporciona una forma centralizada de gestionar el acceso en todo su entorno de AWS. Con IAM Identity Center, los usuarios pueden:

- Acceder a múltiples cuentas de AWS con un solo inicio de sesión.
- Ser asignados a roles a través de conjuntos de permisos.
- Ser agrupados en equipos con derechos de acceso similares mediante grupos.

Documentación de AWS:

What is IAM Identity Center?

2. Grupos Existentes en IAM Identity Center

Los siguientes grupos han sido creados en su entorno para simplificar y estandarizar la gestión de acceso. Estos grupos le permiten asignar permisos a múltiples usuarios a la vez sin necesidad de configurar a cada individuo por separado.

Nombre del Grupo	Descripción
`AWSControlTowerAdmins`	Privilegios de administrador para las cuentas principales (core) y aprovisionadas de AWS Control Tower
`AWSLogArchiveViewers`	Acceso de solo lectura a la cuenta de archivo de registros (log archive)
`AWSSecurityAuditors`	Acceso de solo lectura a todas las cuentas para auditorías de seguridad
`AWSAuditAccountAdmins`	Privilegios de administrador para la cuenta de auditoría (audit)
`AWSSecurityAuditPowerUsers`	Acceso de usuario avanzado (power user) a todas las cuentas para auditorías de seguridad
`AWSServiceCatalogAdmins`	Privilegios de administrador para la fábrica de cuentas (account factory) en AWS Service Catalog
`AWSLogArchiveAdmins`	Privilegios de administrador para la cuenta de archivo de registros (log archive)

`AWSAccountFactory`	Acceso de solo lectura a la fábrica de cuentas (account factory) en AWS Service Catalog

Estos grupos se gestionan manualmente y pueden ser ampliados, modificados o eliminados según las necesidades de su organización.

Documentación de AWS:

Managing Groups

3. Cómo se Otorgan los Permisos

Los permisos en AWS IAM Identity Center se otorgan utilizando **conjuntos de permisos** (*permission sets*). Estos definen las acciones que un usuario o grupo puede realizar en una cuenta de AWS.

- Los usuarios o grupos son asignados a cuentas y se les otorga uno o más conjuntos de permisos.
- En su configuración actual, alejandro.cabrera@sanchezgrupo.com ha sido asignado al grupo `AWSControlTowerAdmins`, otorgándole acceso administrativo completo en todas las cuentas gestionadas por Control Tower.

Documentación de AWS:

Assign User Access to AWS Accounts

4. Aceptar su Invitación de Acceso a AWS

Cuando se cree su cuenta de usuario, recibirá un correo electrónico de AWS IAM Identity Center con un asunto como:

"Invitation to AWS IAM Identity Center"

Para comenzar:

1. Abra el correo electrónico y haga clic en el enlace **Accept Invitation**.
2. Cree su contraseña y complete la configuración de MFA (Autenticación Multifactor).
3. Será redirigido al Portal de Usuario de IAM Identity Center.

URL del Portal:

```
https://d-906638b178.awsapps.com/start
```

> Este es el valor genérico. Puede ser personalizado una sola vez y no se puede cambiar posteriormente. Avíseme si desea cambiarlo.
>
> Valor sugerido: https://grupo-sanchez.awsapps.com/start

Documentación de AWS:

Sign in to the IAM Identity Center User Portal

5. Gestión y Personalización del Acceso

Puede gestionar el acceso de los usuarios de las siguientes maneras:

- Agregar nuevos usuarios o grupos.
- Crear conjuntos de permisos personalizados (p. ej., `ReadOnly`, `Developer`).
- Cambiar qué usuarios o grupos tienen acceso a qué cuentas de AWS.

Todos los cambios se pueden realizar a través de la Consola de IAM Identity Center o programáticamente mediante la CLI de AWS.

Documentación de AWS:

Manage Permission Sets

6. Próximos Pasos

- Agregar usuarios adicionales.
- Definir el tipo de acceso a las cuentas de AWS a través de los grupos creados en SSO Identity Center.
- Usted podrá cambiar permisos, crear grupos adicionales y gestionar el acceso según sea necesario en el futuro.