

ESPECIALIZACIÓN

Ingeniería de datos con Azure

Curso: Microsoft Azure & ETL Fundamentals

Docente: Richard Tadeo Zenteno

REGLAS



Se requiere **puntualidad** para un mejor desarrollo del curso.



Para una mayor concentración **mantener silenciado el micrófono** durante la sesión.



Las preguntas se realizarán **a través del chat** y en caso de que lo requieran **podrán activar el micrófono**.



Realizar las actividades y/o tareas encomendadas en **los plazos determinados**.



Identificarse en la sala Zoom con el primer nombre y primer apellido.

ITINERARIO

*07:00 PM – 07:30 PM **Soporte técnico DMC***

*07:30 PM – 08:50 PM **Agenda***

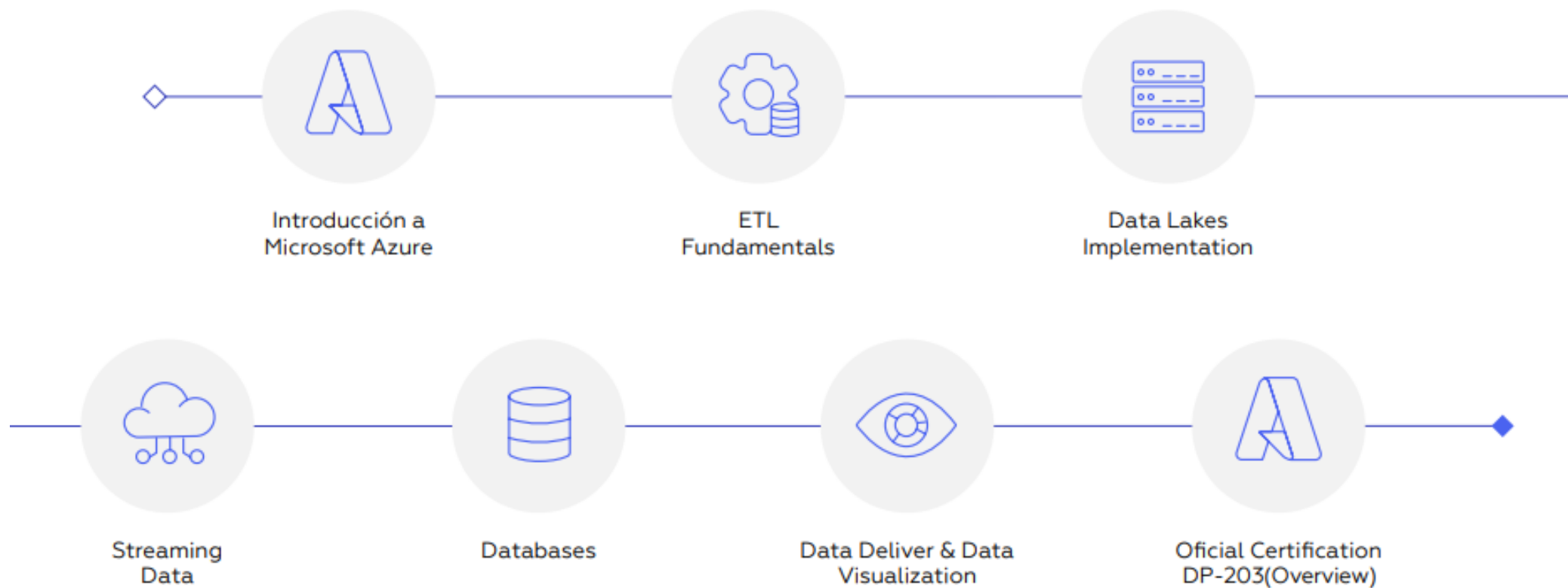
*08:50 PM – 09:00 PM **Pausa Activa***

*09:00 PM – 10:30 PM **Agenda***

Horario de Atención Área Académica y Soporte

Lunes a Viernes 09:00 am a 10:30 pm / Sábado 09:00 am a 02:00pm

MALLA CURRICULAR



CERIFICACIÓN FINAL
por **Aprobación** de la Especialización en **Ingeniería de Datos con Microsoft Azure** (48 horas académicas)

CONTENIDO



Introducción a Microsoft Azure

- Introducción a Cloud Computing. Proveedores de servicios Cloud, On-Premise vs. On-Cloud, principales servicios, descripción de los modelos de costos.
- Identity and Access Management (IAM). Overview de los roles principales, ejemplos de gestión de permisos.



ETL Fundamentals

- Introducción a las soluciones ETL. Definición, descripción de sus etapas.
- Introducción a los servicios Azure Data Factory y Data Flow. Características generales, casos de uso.
- Taller: Implementación de un ETL Básico con Azure.



Data Lakes Implementation

- Introducción a Data Lakes. Definición, arquitectura, capas (Raw, Stage, Analytics).
- Introducción a los servicios Azure Blob Storage y Storage Account.
- Taller: Implementación de un Datalake en Azure.

CONTENIDO



Streaming Data

- Introducción a procesamiento de datos Batch y Streaming. Diferencias Near-Real-Time y Real-Time.
- Introducción a IoT. Definición, uso de sensores, aplicaciones.
- Revisión de servicios: Azure EventHubs y IoT Hub. Características generales, ejemplos de implementación y uso.
- Taller: Manejo de Streaming al Data.



Databases

- Introducción a las bases de datos Relacionales y No-Relacionales. Definición, características, casos de uso.
- Azure SQL Database for MariaDB. Descripción y características generales.
- Azure SQL Database for PostgreSQL. Descripción y características generales.
- Azure SQL Database for CosmosDB. Descripción y características generales.
- Taller: Diseño de una base de datos relacional y técnicas para poblarla.



Data Deliver & Data Visualization

- Azure Synapse Analytics. Propósito del servicio, características generales.
- Fabric. Propósito del servicio, características generales.
- Taller: Conexión de Power BI a servicios de datos de Azure.

AGENDA

01

Accesos Azure

02

Identify and Access
Management
(IAM) y RBAC

03

Revisión de
prompts para IA
Assistance
(ChatGPT y otros)

04

Laboratorio 02:
Configuración de
IAM

Acceso a las aplicaciones de Azure

Hay dos conceptos fundamentales que deben entenderse al hablar sobre identidad y acceso: la autenticación (AuthN) y la autorización (AuthZ).

- **¿Qué es la autenticación?**
- Determina si el usuario es quien dicen ser.
- **¿Qué es la autorización?**
- Especifica a qué datos puede acceder y qué puede hacer con ellos

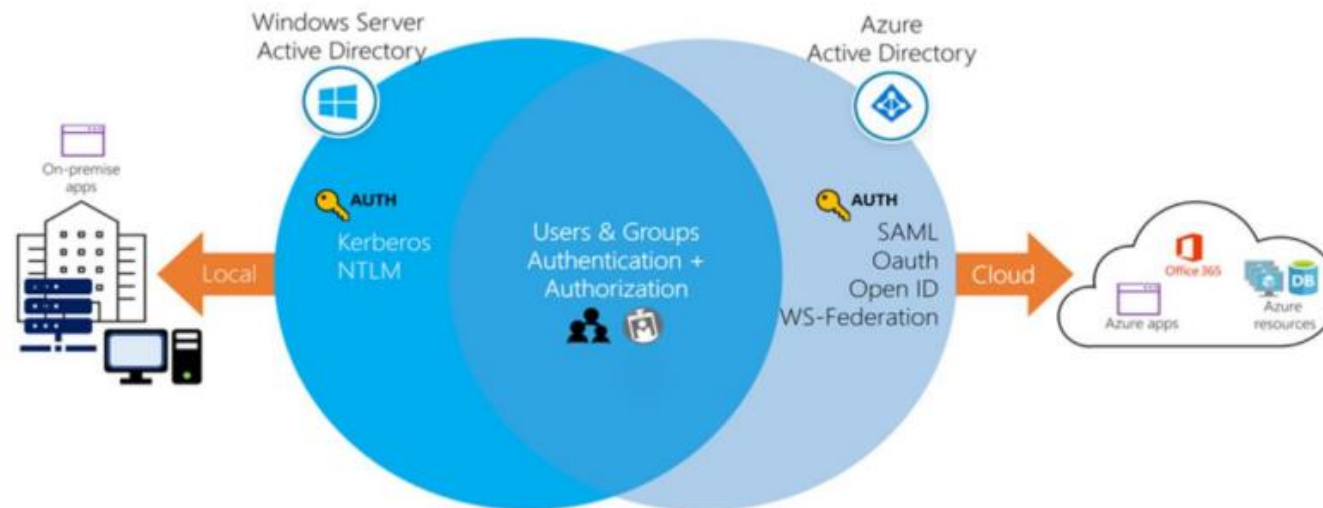


Azure Active Directory

Proporciona servicios de identidad que permiten a los usuarios iniciar sesión y acceder tanto a las aplicaciones en la nube de Microsoft como a las que desarrolle personalmente. También verá cómo admite Azure AD el inicio de sesión único (SSO).

¿Qué diferencia hay entre Azure AD y Active Directory?

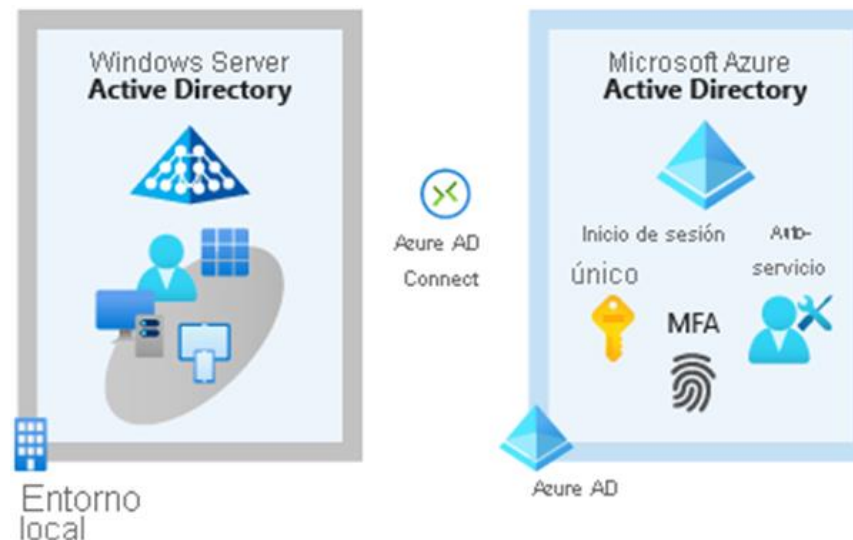
Active Directory ejecutado en Windows Server proporciona un servicio de administración de acceso e identidades administrado por su propia organización. Azure AD es un servicio de administración de acceso e identidades basado en la nube de Microsoft.



¿Cómo se puede conectar Active Directory con Azure AD?

La conexión de Active Directory con Azure AD permite proporcionar una experiencia de identidad coherente a los usuarios.

Hay varias maneras de conectar la instalación de Active Directory existente con Azure AD. Quizás el método más popular es usar Azure AD Connect.



¿Quién usa Azure AD?

Azure AD es para:

- **Administradores de TI:** Utilizan Azure AD para controlar el acceso a aplicaciones y recursos según las necesidades empresariales.
- **Desarrolladores de aplicaciones:** Pueden añadir funcionalidades a sus aplicaciones, como SSO, usando Azure AD y las credenciales existentes de los usuarios.
- **Usuarios:** Gestionan sus identidades, incluyendo el autoservicio de restablecimiento de contraseña sin necesidad de intervención del soporte técnico.
- **Suscriptores de servicios en línea:** Usuarios de Microsoft 365, Office 365, Azure y Dynamics CRM Online ya utilizan Azure AD.
 - Un **inquilino** representa una organización, separado de otros inquilinos, con su propia identidad.
 - Cada inquilino de Microsoft 365, Office 365, Azure y Dynamics CRM Online es automáticamente un inquilino de Azure AD.

Que servicios proporciona:

- **Autenticación:** Verificación de identidad, restablecimiento de contraseña, autenticación multifactor y bloqueo inteligente.
- **SSO:** Un solo identificador y contraseña para múltiples aplicaciones, simplificando la gestión de accesos.
- **Administración de aplicaciones:** Gestión de aplicaciones en la nube y locales con SSO y otras herramientas.
- **Administración de dispositivos:** Registro y gestión de dispositivos con herramientas como Microsoft Intune y directivas de acceso condicional.

Características de Azure AD

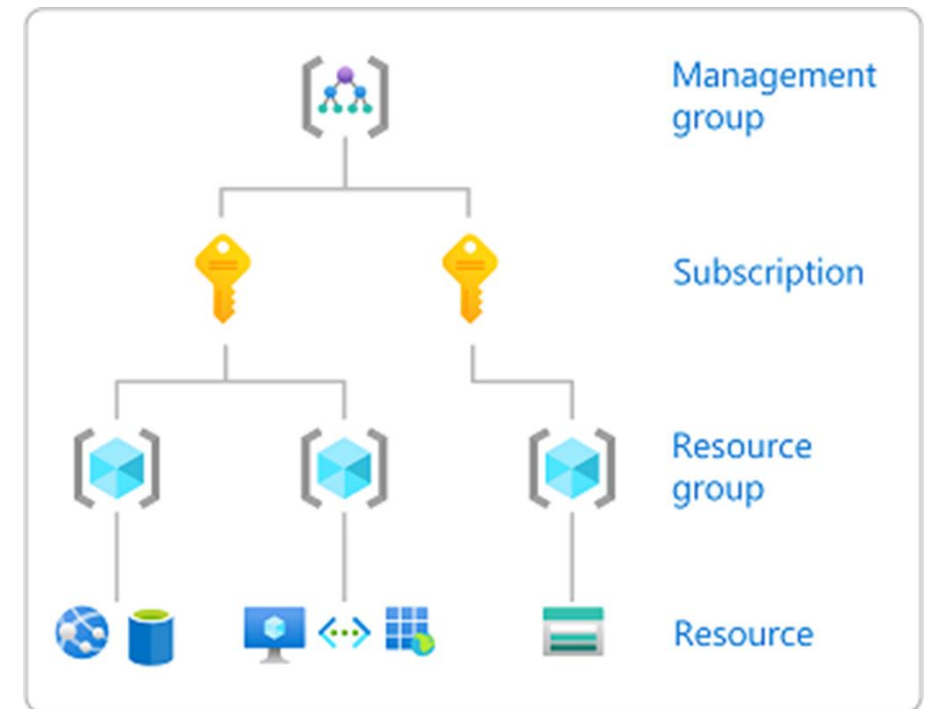
- ✓ El inicio de sesión único (SSO) permite a los usuarios iniciar sesión una vez y utilizar esa credencial para acceder a varios recursos y aplicaciones.
- ✓ Azure AD Multi-Factor Authentication proporciona seguridad adicional para las identidades, ya que se requieren dos o más elementos para una autenticación completa. En general, la autenticación multifactor puede incluir algo que el usuario sabe, algo que tiene y algo que es.
- ✓ El acceso condicional es una herramienta que Azure AD usa para permitir o denegar el acceso a los recursos en función de señales de identidad, como la ubicación del usuario.



IAM - Administración de Identidad y Acceso

Se refiere a un conjunto de herramientas y servicios que permiten gestionar quién tiene acceso a los recursos de Azure, qué pueden hacer con esos recursos y a qué áreas específicas pueden acceder. Aquí tienes un resumen de sus principales características:

- **Control de Acceso Basado en Roles (RBAC):** Permite asignar roles específicos a usuarios, grupos o aplicaciones para controlar el acceso a los recursos de Azure1.
- **Azure Active Directory (Azure AD):** Proporciona servicios de identidad y acceso, incluyendo autenticación multifactor, gestión de identidades y acceso condicional2.
- **Protección de Identidad:** Utiliza herramientas para defenderse contra intentos de inicio de sesión malintencionados y proteger las credenciales con controles de acceso basados en el riesgo2.
- **Identidades Administradas:** Facilita la gestión de identidades para aplicaciones que se ejecutan en Azure, eliminando la necesidad de gestionar credenciales directamente



RBAC – Control De Acceso Basado En Roles

- RBAC es la **gestión del acceso a los recursos de la nube**. Es una función **fundamental y crítica**.
- Es un **sistema de autorización** que proporciona una administración de acceso detallada de los recursos en Azure.
- El control de acceso basado en roles (RBAC) **permite administrar quién tiene acceso** a los recursos, **qué pueden hacer** y **a qué áreas tienen acceso** en Azure.



RBAC – Control De Acceso Basado En Roles

Los elementos que participan en RBAC son:

1

Entidad de Seguridad (Security Principal)

Objeto que representa algo que solicita acceso a recursos. Ejs.: Usuario, grupo, Entidad de servicio (Service Principal), Identidad administrada (Managed Identity).

2

Definición de roles (Role definition)

Colección de permisos que enumera las operaciones que se pueden realizar.
Ejs.: Lector (Reader), Colaborador (Contributor), Propietario (Owner), Administrador de acceso de usuario (User access administrator).

3

Alcance (Scope)

Límite para el nivel de acceso que se solicita.
Ejs.: Grupo de administración, Suscripción, Grupo de recursos, recurso.

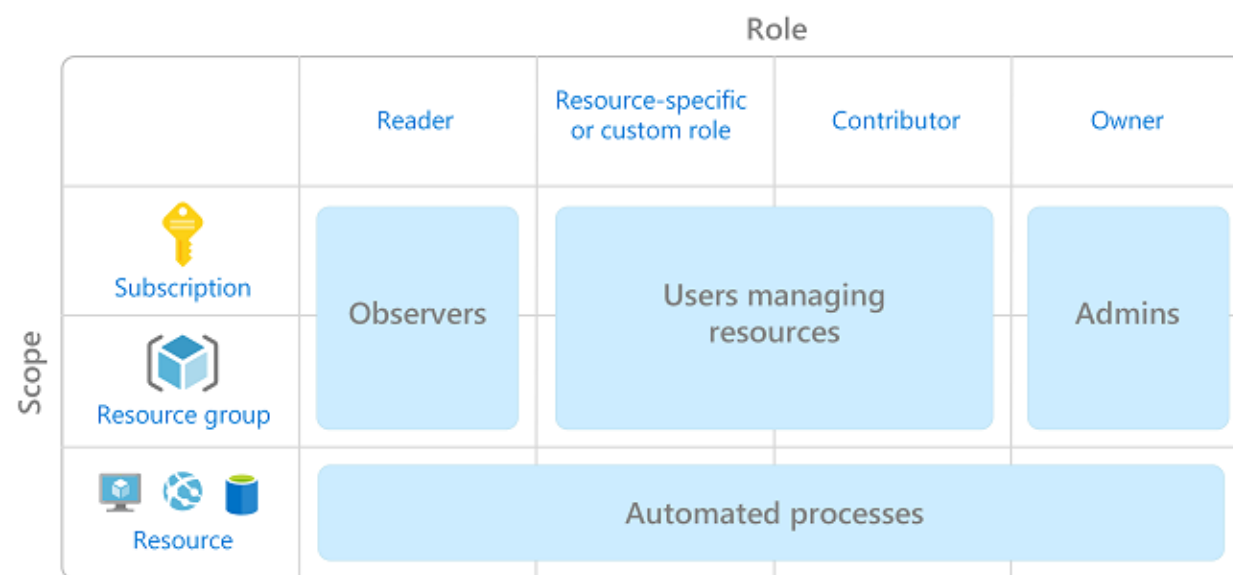
4

Asignación (Assignment)

Adjuntar una definición de rol a una entidad de seguridad en un ámbito particular.

Modelo RBAC

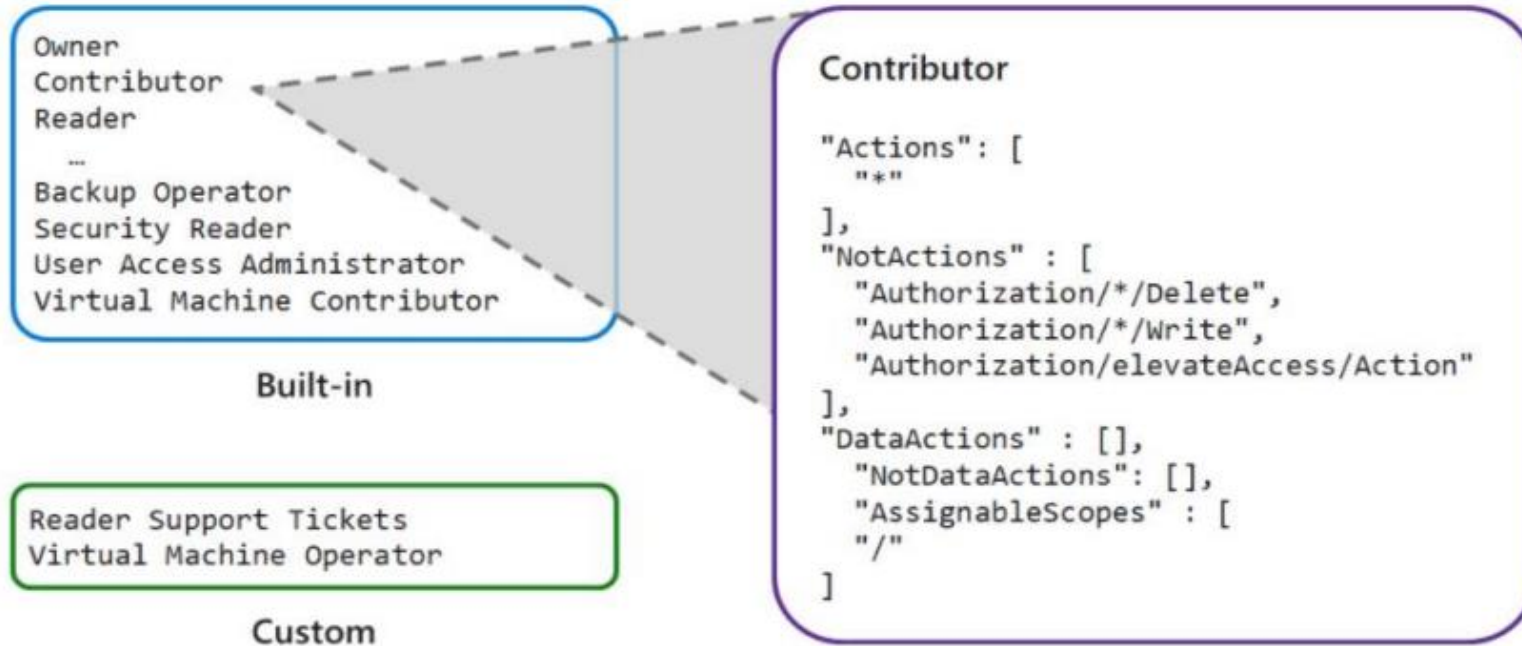
Rol	Descripción
Propietario	Acceso total para gestionar todos los recursos, incluyendo asignación de roles.
Colaborador	Acceso total para gestionar todos los recursos, sin poder asignar roles.
Lector	Ver todos los recursos, sin poder hacer cambios.
Administrador de acceso	Gestionar el acceso de usuarios a los recursos de Azure con RBAC.
Administrador de acceso de usuario	Gestionar el acceso de usuarios a los recursos de Azure.



[Azure built-in roles - Azure RBAC | Microsoft Learn](#)

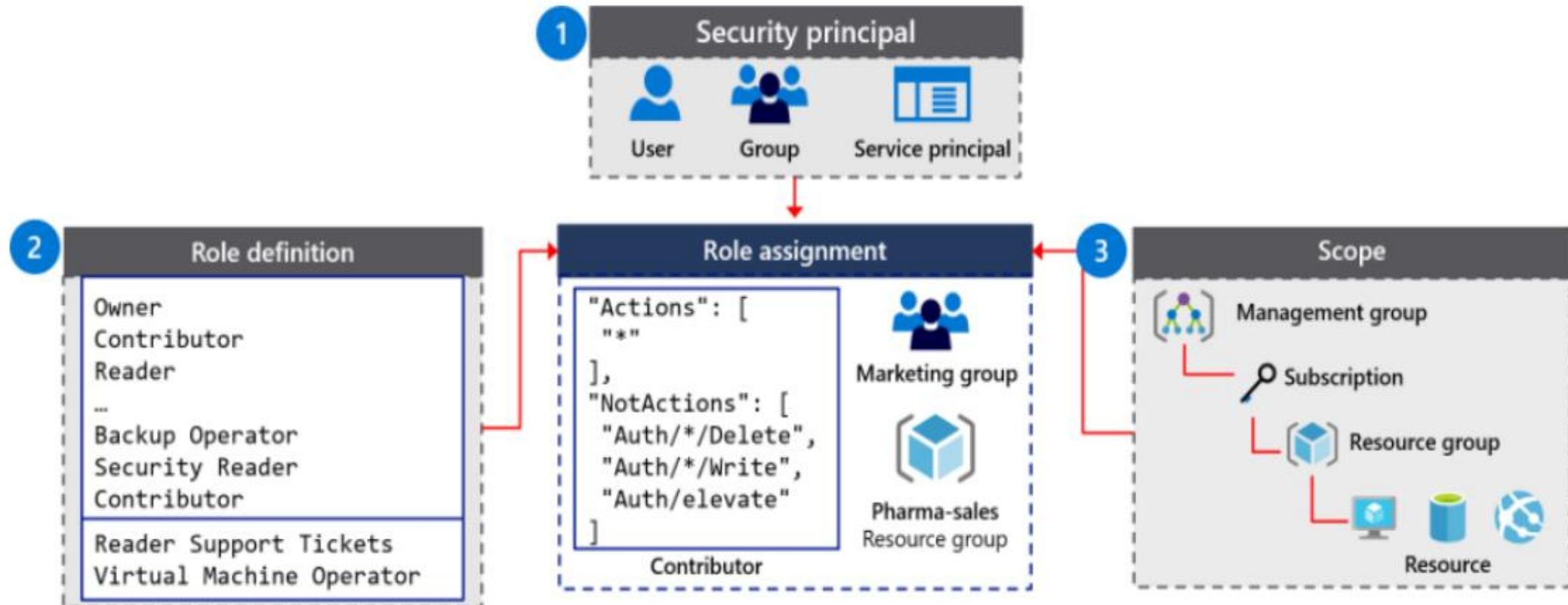
RBAC – Definición de Roles

Definición de roles



Cada rol es un conjunto de propiedades definidas en un file JSON, que incluye **Nombre, ID y descripción**. También incluye **permisos autorizados** (acciones), **permisos denegados** (no acciones), y **alcance** (acceso de lectura, etc.) para el rol.

RBAC – Proceso de asignación de Roles



RBAC VS. AZURE AD ROLES

AZURE RBAC ROLES

- Administrar accesos a los recursos de Azure.
- El alcance puede ser especificado a múltiples niveles (management group, suscripción, grupo de recursos, recurso).
- Se puede acceder a la información por roles a través de: Portal de Azure, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API.
- Ejemplos Reader, Contributor, Owner, etc.

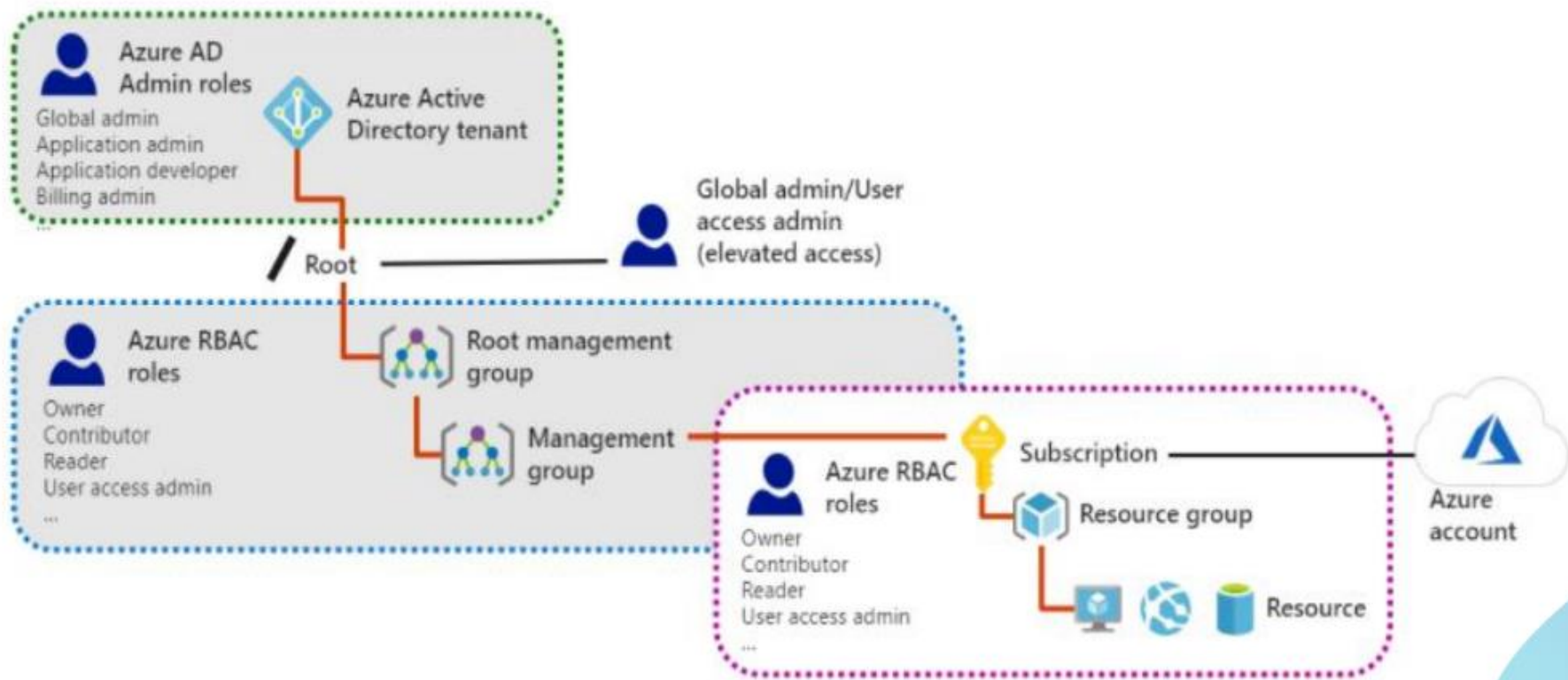
AZURE AD ROLES

- Administrar accesos a los recursos de Azure AD.
- El alcance es a nivel de Tenant.
- Se puede acceder a la información por roles a través de: Portal admin de Azure, Portal admin de Microsoft 365, Microsoft Graph Azure AD PowerShell.
- Ejemplos Global Administrator, Global Reader, Application Administrator, etc.

RBAC Autenticación

RBAC incluye muchos roles integrados (built-in).

Para administrar recursos en Azure AD, como usuarios, grupos y dominios, existen **varios roles de administrador de Azure AD**.



TALLER DIRIGIDO: Revisión de prompts para IA Assistance (ChatGPT y otros)

Se refiere al proceso de evaluar y mejorar las instrucciones o preguntas (prompts) que se utilizan para interactuar con modelos de inteligencia artificial. Este proceso es importante porque la calidad y claridad de los prompts pueden influir significativamente en la calidad de las respuestas que genera la IA.

Algunos aspectos clave de la revisión de prompts incluyen:

- ✓ **Claridad:** Asegurarse de que el prompt sea claro y fácil de entender.
- ✓ **Especificidad:** Proporcionar suficiente contexto o detalles para guiar a la IA hacia la respuesta deseada.
- ✓ **Objetivo:** Definir claramente el propósito del prompt para que la IA pueda alinearse con las expectativas del usuario.
- ✓ **Pruebas:** Realizar pruebas con diferentes formulaciones de prompts para identificar cuáles generan las mejores respuestas.

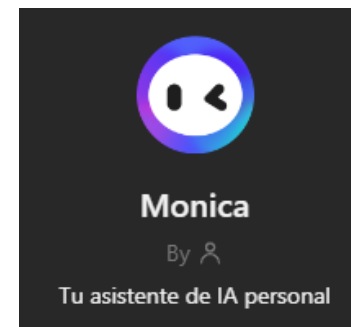


[ChatGPT](#)



Su complemento de IA para el día a día

[Copilot \(microsoft.com\)](#)



[Chat - Monica](#)

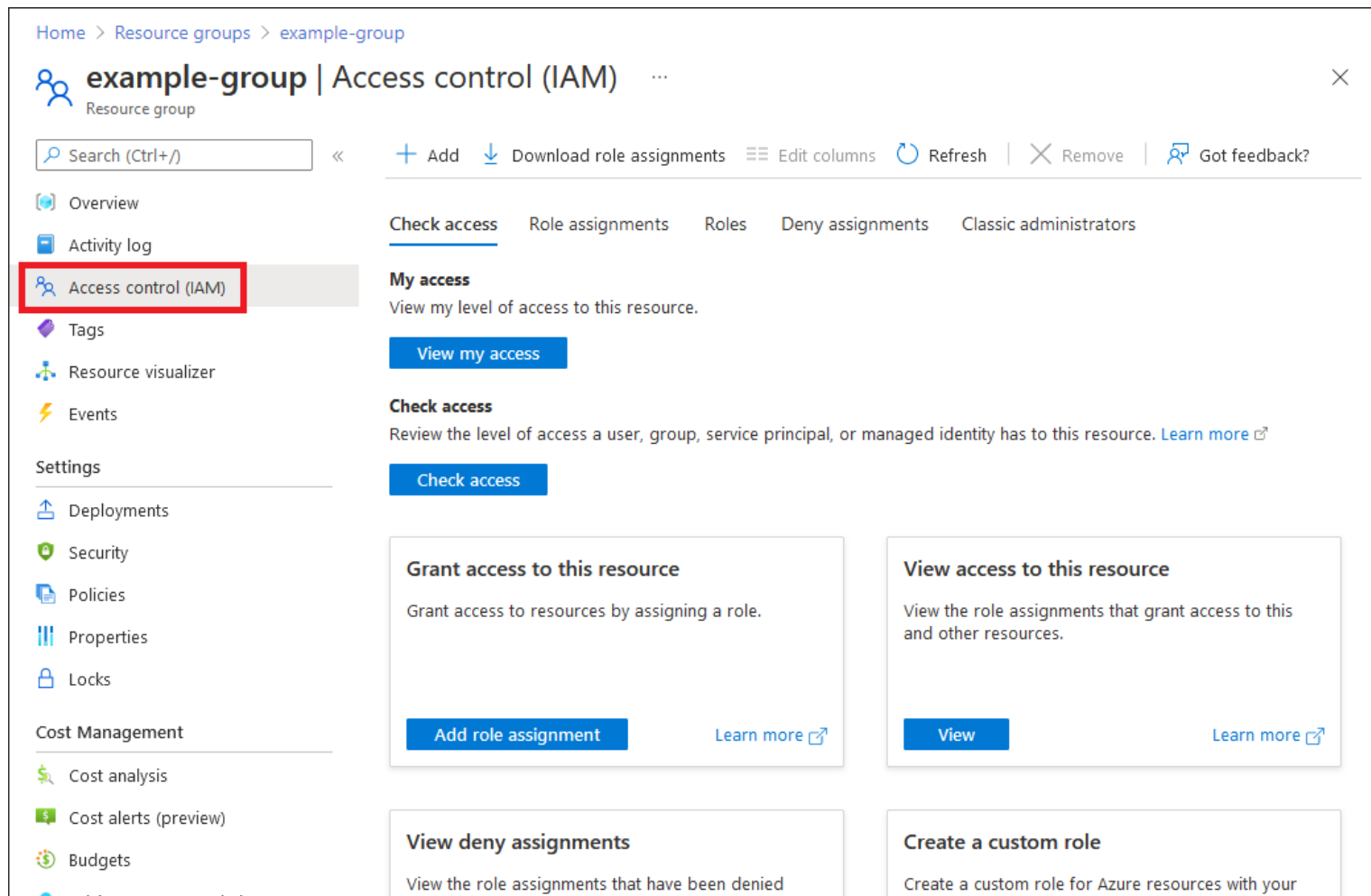
LABORATORIO: Configuración de IAM

Entra ID (IAM) :

[AZ-104-MicrosoftAzureAdministrator](https://github.com/microsoftlearning/AZ-104-MicrosoftAzureAdministrator)
 [\(microsoftlearning.github.io\)](https://github.com/microsoftlearning/AZ-104-MicrosoftAzureAdministrator)

RBAC:

[AZ-104-MicrosoftAzureAdministrator](https://github.com/microsoftlearning/AZ-104-MicrosoftAzureAdministrator)
 [\(microsoftlearning.github.io\)](https://github.com/microsoftlearning/AZ-104-MicrosoftAzureAdministrator)



The screenshot shows the Azure Portal interface for the 'example-group' resource group, specifically the 'Access control (IAM)' page. The left-hand navigation pane is visible, with 'Access control (IAM)' highlighted by a red rectangle. The main content area displays the 'Access control (IAM)' page, which includes a search bar, a list of actions (Add, Download role assignments, Edit columns, Refresh, Remove, Got feedback?), and a list of tabs (Check access, Role assignments, Roles, Deny assignments, Classic administrators). The 'Check access' tab is selected, showing 'My access' and 'Check access' sections. The 'Grant access to this resource' section is visible, with a button to 'Add role assignment' and a 'Learn more' link. The 'View access to this resource' section is also visible, with a 'View' button and a 'Learn more' link. The 'View deny assignments' section is partially visible at the bottom, with a 'View the role assignments that have been denied' link. The 'Create a custom role' section is also partially visible at the bottom, with a 'Create a custom role for Azure resources with your' link.

RONDAS DE PREGUNTAS



¡GRACIAS!

