Gestión de usuarios y acceso

Como propietario o administrador de la cuenta, puede añadir las personas de su organización a la cuenta de IBM Cloud y, a continuación, asignarles permisos de acceso utilizando roles que proporcionen acceso a los servicios que necesitan.

Gestión de usuarios en IBM Cloud

Las personas que trabajen en inCloud Pak para Data as a Service deben tener un IBMid válido y ser miembros de la cuenta IBM Cloud. De forma alternativa, deben tener un ID válido en un registro de usuarios soportado. La gestión de usuarios incluye añadir usuarios a la cuenta y, a continuación, asignar los roles adecuados para proporcionar acceso a los servicios y acciones que necesitan.

Gestión de accesos mediante IBM Cloud Identity and Access Management (IAM)

Puede controlar las acciones que un usuario puede realizar para un servicio específico asignando permisos con IBM Cloud IAM. Puede crear grupos de acceso de usuario que contengan roles para proporcionar permisos a los usuarios. También puede asignar roles y permisos a usuarios individuales. Si es necesario, puede crear roles personalizados para satisfacer los requisitos empresariales.

Añadir usuarios a la cuenta

Como **Administrador**, puede añadir las personas de su organización que necesitan acceso a Cloud Pak for Data as a Service a la cuenta de IBM Cloud y, a continuación, asignarles los roles adecuados para sus tareas.

1. Añada usuarios no administrativos a la cuenta IBM Cloud y asígneles grupos de acceso o funciones para que puedan trabajar en Cloud Pak for Data as a Service. Los nuevos usuarios reciben una invitación por correo electrónico para unirse a la cuenta. Deben aceptar la invitación para añadirse a dicha cuenta.

2. Configure grupos de acceso para simplificar los permisos y la asignación de roles. Consulte Configuración de grupos de acceso.

Añada usuarios no administrativos a su cuenta de IBM Cloud

Puede invitar a los usuarios a su cuenta de IBM Cloud enviando una invitación por correo electrónico. El usuario acepta la invitación para unirse a la cuenta. Debe asignarles roles (o grupos de acceso) para proporcionar los permisos necesarios para trabajar en Cloud Pak for Data as a Service. Para una asignación de rol de

línea base, puede proporcionar permisos mínimos asignando los roles siguientes en la pantalla **Gestionar > Acceso (IAM) > Usuarios > Invitar a usuarios > Política de acceso** en IBM Cloud:

Tabla 1. Roles mínimos para nuevos usuarios de Cloud Pak for Data as a Service

Nivel	**Rol**	**Descripción**
Acceso a grupo de recursos	**Visor**	Puede ver pero no modificar grupos de recursos
Acceso de servicio	**Lector**	Puede realizar acciones de sólo lectura dentro de un servicio
Acceso de plataforma	**Visor**	Puede ver pero no modificar instancias de servicio

Un método conveniente para asignar roles es crear grupos de acceso y asignar nuevos usuarios a uno o más grupos de acceso. Se proporcionan ejemplos de grupos de acceso básicos como sugerencias sobre cómo empezar con los grupos de acceso. Consulte Ejemplo de grupos de acceso de IAM. Puede asignar los nuevos usuarios al grupo **CPD-Common-User** para proporcionar permisos mínimos.

Posteriormente, puede asignar roles o grupos de acceso específicos en función de las tareas que realice el usuario en Cloud Pak for Data as a Service.

Pertenencia a la cuenta de IBM

Para estar autorizado para Cloud Pak for Data as a Service, los usuarios deben tener IBMid existentes. Si el usuario invitado no tiene un IBMid, se crea para él cuando se une a la cuenta.

Asignación de roles

Los grupos de acceso agilizan las asignaciones de roles agrupando permisos para un gran número de usuarios. Cree un grupo y asigne políticas y reglas al grupo. Cuando asigna usuarios a un grupo de acceso, se les otorga acceso en función de los parámetros del grupo. Todos los miembros de un grupo de acceso tienen los

mismos permisos de acceso y todos los miembros se actualizan cuando se edita la política.

Después de crear un conjunto de grupos de acceso, siga estos pasos para añadir usuarios como miembros de un grupo de acceso:

1. En Cloud Pak for Data as a Service, pulse **Administración > Acceso (IAM)** para abrir la página **Gestionar acceso y usuarios** para su cuenta de IBM Cloud .
2. Pulse **Usuarios > Invitar a usuarios**.
3. Especifique una o más direcciones de correo electrónico separadas por comas, espacios o saltos de línea. El límite es de 100 direcciones de correo electrónico. Los valores se aplican a todas las direcciones de correo electrónico.
4. Pulse el mosaico **Grupos de acceso** y seleccione uno o más grupos de acceso y, a continuación, pulse **Añadir**. Los grupos de acceso se crean antes de añadir usuarios. Consulte Configuración de grupos de acceso de IAM y Grupos de acceso de IAM de ejemplo.
5. Pulse **Invitar** para enviar una invitación por correo electrónico a cada dirección de correo electrónico. El usuario se asigna al grupo de acceso cuando acepta la invitación para unirse a la cuenta.

De forma alternativa, puede asignar permisos mínimos a usuarios individuales:

1. En Cloud Pak for Data as a Service, pulse **Administración > Acceso (IAM)** para abrir la página **Gestionar acceso y usuarios** para su cuenta de IBM Cloud .
2. Pulse **Usuarios > Invitar a usuarios+**.
3. Especifique una o más direcciones de correo electrónico separadas por comas, espacios o saltos de línea. El límite es de 100 direcciones de correo electrónico. Los valores se aplican a todas las direcciones de correo electrónico.
4. Pulse el mosaico **Política de acceso** .
5. Seleccione los servicios a los que desea asignar acceso y haga clic en **Siguiente**.
6. Seleccione los recursos a los que desea asignar acceso y haga clic en **Siguiente**.

7. Opcional: para **acceder al grupo de recursos**, seleccione **Visor**. Pulse **Siguiente**.
8. Para **Roles y acción**, elija los permisos mínimos siguientes:
    - En la sección **Acceso de servicio** , seleccione **Lector**
    - En la sección **Acceso a plataformas**, seleccione **Visor**.
9. Haga clic en **Revisar** para revisar la configuración y editarla, si es necesario.
10. Pulse **Añadir** para guardar la política.
11. Pulse **Invitar** para enviar una invitación por correo electrónico a cada dirección de correo electrónico. Las políticas se asignan a los usuarios cuando aceptan la invitación para unirse a la cuenta.

Niveles de roles de acceso de usuario en Cloud Pak for Data as a Service

Cada usuario de Cloud Pak for Data as a Service tiene varios niveles de roles con los permisos o acciones correspondientes. Los permisos determinan qué acciones puede realizar un usuario en la plataforma o en un servicio. Algunos roles se establecen en IBM Cloud, y otros se establecen en Cloud Pak for Data as a Service.

El propietario o administrador de la cuenta de IBM Cloud establece los roles de acceso de plataforma y servicio de Identity and Access (IAM) en la cuenta de IBM Cloud . Los administradores de espacios de trabajo establecen las funciones de los colaboradores para los espacios de trabajo, por ejemplo, los proyectos.

Es necesario estar familiarizado con la característica de IBM Cloud IAM, grupos de acceso, roles de plataforma y roles de servicio para configurar el acceso de usuario para Cloud Pak for Data as a Service. Consulte la documentación de IBMIBM Cloud: Acceso IAM para obtener una descripción de los roles de IBM Cloud IAM Platform y Service.

En lugar de asignar a cada usuario individual un conjunto de roles, puede crear grupos de acceso para consolidar acciones para un grupo de usuarios. Los grupos de acceso (también denominados grupos de usuarios) contienen roles y permisos correspondientes que desea asignar a un grupo de usuarios. Los grupos de acceso agilizan las asignaciones de roles organizando permisos para varios usuarios.

Esta ilustración muestra los diferentes niveles de roles asignados a cada usuario para que puedan trabajar en Cloud Pak for Data as a Service.

Niveles de roles en Cloud Pak for Data as a Service

Los niveles de roles son:

- Los roles de acceso de IAM Platform determinan los permisos para la cuenta de IBM Cloud . Se necesita al menos el rol de **Visor** para trabajar con servicios.
- Los roles de acceso deIAM Service determinan los permisos dentro de los servicios.
- Los roles de colaborador del espacio de trabajo determinan qué acciones tiene permiso para realizar dentro de los espacios de trabajo en Cloud Pak for Data as a Service. Los espacios de trabajo son proyectos, espacios de despliegue, catálogos, categorías y vistas virtuales.

Roles de acceso a la plataforma IAM

Los roles de acceso de IAM Platform se asignan y gestionan en la cuenta de IBM Cloud .

Los roles de acceso de IAM Platform proporcionan permisos para gestionar la cuenta de IBM Cloud y para acceder a servicios dentro de Cloud Pak for Data as a Service. Los roles de acceso de plataforma son **Visor**, **Operador**, **Editor**y **Administrador**. Los roles de plataforma están disponibles para todos los servicios en IBM Cloud.

El rol de **Visor** tiene permisos mínimos de solo vista. Los usuarios necesitan al menos el rol de **Visor** para ver los servicios en Cloud Pak for Data as a Service. Un **Visor** puede:

- Ver, pero no modificar, las instancias de servicio y los activos disponibles
- Asociar servicios con proyectos.
- Conviértase en colaboradores de los proyectos o catálogos.
- Cree proyectos, espacios de despliegue y catálogos si se le han asignado los permisos adecuados para Cloud Object Storage.

El rol de **Operador** tiene permisos para configurar instancias de servicio existentes. Un **Operador** puede:

- Configurar y operar, pero no aprovisionar, instancias de servicio de Data Virtualization.

- Ver paneles de servicio para Data Virtualization.

El rol **Editor** proporciona acceso a estas acciones:

- Todos los permisos del rol Visor.
- Suministrar instancias de servicios.
- Actualizar planes para instancias de servicio.

El rol de **Administrador** proporciona los mismos permisos que el rol **Propietario** para la cuenta. Con el rol de **Administrador** puede:

- Todos los permisos de visor, operador y editor.
- Realizar todas las acciones de gestión de servicios.
- Añadir usuarios a la cuenta de IBM Cloud y asignar roles
- Realizar tareas administrativas en Cloud Pak for Data as a Service
- Gestionar servicios para Cloud Pak for Data as a Service
- Configurar grupos de acceso
- Crear roles de servicio personalizados.

Para comprender los roles de acceso a la plataforma IAM, consulte Documentos de IBM Cloud: ¿Qué es IBM Cloud Identity and Access Management?.

Roles de acceso a servicio de IAM

Los roles de servicio se aplican a servicios individuales y definen las acciones permitidas dentro del servicio. El servicio IBM Cloud Pak for Data contiene funciones y permisos que se aplican a IBM watsonx.data intelligence y watsonx.ai Studio. Consulte Funciones y permisos de usuario para IBM watsonx.data intelligence y watsonx.ai Studio. IBM Cloud Object Storage tiene su propio conjunto de roles de acceso al Servicio. Consulte Configuración de IBM Cloud Object Storage para su uso con Cloud Pak for Data as a Service.

La siguiente tabla muestra los permisos de las funciones de acceso de Servicio para **IBM Cloud Pak for Data** para categorías, catálogos, proyectos y productos de datos:

Tabla 1. Roles de acceso a IAM Service para IBM Cloud Pak for Data

Rol	Categorías	Catálogos	Productos de datos	Proyectos
Gestor	Gestionar	Gestionar	Gestionar	Gestionar
CloudPak Data Steward	Acceso	Acceso	Ninguna	Ninguna
CloudPak Data Engineer	Acceso	Acceso	Ninguna	Ninguna
CloudPak Data Scientist	Ninguna	Acceso	Ninguna	Ninguna
Administrador de informes	Ninguna	Acceso	Ninguna	Ninguna
Analista de calidad de datos deCloudPak	Ninguna	Ninguna	Ninguna	Ninguna

Para obtener una lista completa de los permisos y las acciones asociadas a estas funciones, consulte Funciones y permisos de usuario.

La tabla siguiente muestra los permisos para los roles de acceso de IAM Service para **Todos los servicios habilitados para identidad y acceso** para categorías y catálogos:

Tabla 2. Roles de acceso de IAM Service para todos los servicios habilitados para identidad y acceso

Rol	Categorías	Catálogos
Gestor	Gestionar	Gestionar

Tabla 2. Roles de acceso de IAM Service para todos los servicios habilitados para identidad y acceso

Rol	Categorías	Catálogos
Escritor	Ninguna	Gestionar
Lector	Ninguna	Vista

Roles de colaborador de espacio de trabajo

Su rol en un espacio de trabajo específico determina las acciones que puede realizar en dicho espacio de trabajo. Los roles de IAM no afectan a su rol dentro de un espacio de trabajo. Por ejemplo, puede ser el **Administrador** de la cuenta de Cloud, pero esto no le convierte automáticamente en administrador de un proyecto o catálogo. El rol de colaborador **Admin** para un proyecto (u otro espacio de trabajo) debe asignarse explícitamente. Del mismo modo, los roles son específicos de cada proyecto. Es posible que tenga un rol de **Administrador** en un proyecto, lo que le da un control total sobre el contenido de dicho proyecto, incluyendo la gestión de colaboradores y activos. Pero puede tener el rol de **Visor** en otro proyecto, que solo le permite ver el contenido de dicho proyecto.

Muchos espacios de trabajo tienen estos roles:

- **Administrador**: Controlar activos, colaboradores y valores en el espacio de trabajo.
- **Editor**: Controlar activos en el espacio de trabajo.
- **Visor**: Ver el espacio de trabajo y su contenido.

Creación de roles de acceso de usuario personalizados en IBM Cloud IAM

Si necesita roles de acceso de usuario con permisos diferentes a los roles predefinidos, puede crear roles personalizados en IBM Cloud.

Creación de roles personalizados

Las funciones predefinidas podrían no cubrir las necesidades exactas de su empresa. En este caso, puede crear roles personalizados para un servicio habilitado para IAM. Los roles personalizados se pueden asignar a grupos de

acceso o a usuarios individuales. Los roles personalizados pueden combinar cualquier número de permisos (también denominados acciones) para un servicio específico. Se debe añadir al menos una acción de nivel de servicio para crear el nuevo rol.

Permisos necesarios

Para crear, editar o suprimir roles personalizados en IBM Cloud, debe tener los siguientes roles y permisos de gestión de cuentas de IBM Cloud :

- **Editor** -Puede editar y actualizar el nombre de visualización del rol, la descripción y las acciones correlacionadas con él.
- **Administrador** : puede crear, editar, actualizar y suprimir roles personalizados y asignar acceso a los usuarios.

Para crear un rol de IAM Service personalizado:

1. Vaya a **Administración > Acceso (IAM)**. A continuación, seleccione **Roles** en la consola de IBM Cloud.
2. Pulse **Crear**.
3. Escriba un nombre para el rol. El nombre es necesario y puede tener hasta 50 caracteres de longitud. Los usuarios ven este nombre de rol en la consola de IBM Cloud cuando asignan acceso al servicio.
4. Introduzca un ID para el rol. Este ID es necesario y se utiliza en el CRN, que es leído por las API. El ID de la función debe comenzar con una letra mayúscula y utilizar sólo caracteres alfanuméricos. Este ID debe tener 30 caracteres o menos y no se puede actualizar.
5. Opcional: Especifique una descripción que ayude a los usuarios a identificar el rol. Esta descripción también se muestra en la consola cuando un usuario asigna el acceso al servicio.
6. Seleccione el servicio para el que el rol proporcionará acceso. Para IBM watsonx.data intelligence y watsonx.ai Studio, seleccione el servicio IBM Cloud Pak for Data.
7. Revise las acciones disponibles y pulse **Añadir** para todas las acciones que desee en el nuevo rol. Debe añadir al menos una acción para crear con éxito el nuevo rol. Las acciones corresponden a los permisos que asignará a los usuarios. Las acciones tienen el ámbito de Plataforma o Servicio tal como se muestra en la columna **Tipo** .
8. Pulse **Crear** cuando haya terminado de añadir acciones.

Si edita un rol personalizado, los cambios se aplican inmediatamente a todos los grupos de acceso y a todas las personas a las que se les ha asignado el rol.

Si elimina un rol personalizado, se elimina automáticamente de cualquier política de acceso que lo utilice. Se eliminará el acceso del usuario para dicha acción. Si un servicio elimina una acción que ha utilizado en un rol personalizado, es posible que el rol personalizado no sea válido.