Consideración de la autenticación

De forma predeterminada, el acceso a los recursos de servicios de Azure AI se restringe mediante claves de suscripción. La administración del acceso a estas claves es una consideración principal para la seguridad.

Regeneración de claves

Debe volver a generar las claves periódicamente para protegerse frente al riesgo de que usuarios no autorizados compartan o accedan a estas claves. Puede regenerar claves mediante Azure Portal o mediante el comando de la interfaz de la línea de comandos (CLI) de Azure `az cognitiveservices account keys regenerate`.

Cada servicio de AI se proporciona con dos claves, lo que le permite regenerar claves sin interrupción del servicio. Para realizar esta acción:

1. Si usa ambas claves en producción, cambie el código para que solo esté en uso una clave. Por ejemplo, configure todas las aplicaciones de producción para que usen la clave 1.
2. Regenere la clave 2.
3. Cambie todas las aplicaciones de producción para que usen la clave 2 recién regenerada.
4. Regenere la clave 1.
5. Por último, actualice el código de producción para usar la nueva clave 1.

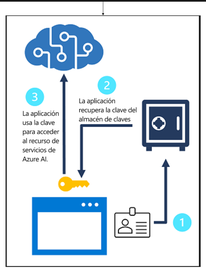
Por ejemplo, para regenerar claves en Azure Portal, puede hacer lo siguiente:

1. En Azure Portal, vaya al panel Claves y punto de conexión del recurso.
2. A continuación, seleccione **Regenerar Key1** o **Regenerar Key2**, en función de la que quiera regenerar en el momento.

Protección de las claves con Azure Key Vault

Azure Key Vault es un servicio de Azure en el que puede almacenar secretos de forma segura (como contraseñas y claves). Se concede el acceso al almacén de claves a las *entidades de seguridad*, que se pueden considerar como identidades de usuario autenticadas mediante Microsoft Entra ID. Los administradores pueden asignar una entidad de seguridad a una aplicación *(en cuyo caso se conoce como entidad de servicio)* para definir una *identidad administrada* para la aplicación. A continuación, la aplicación puede usar esta identidad para acceder al almacén de claves y recuperar un secreto al que tiene acceso. Controlar el acceso al secreto de esta manera minimiza el riesgo de que se vea comprometido si se codifica de forma rígida en una aplicación o se guarda en un archivo de configuración.

Puede almacenar las claves de suscripción de un recurso de servicios de AI en Azure Key Vault y asignar una identidad administrada a las aplicaciones cliente que necesitan usar el servicio. A continuación, las aplicaciones pueden recuperar la clave cuando sea necesario desde el almacén de claves, sin riesgo de exponerla a usuarios no autorizados.



Autenticación basada en tokens

Al usar la interfaz de REST, algunos servicios de AI admiten (o incluso *requieren*) la autenticación basada en tokens. En estos casos, la clave de suscripción se presenta en una solicitud inicial para obtener un token de autenticación, que tiene un período válido de 10 minutos. Las solicitudes posteriores deben presentar el token para validar que el autor de la llamada se ha autenticado.

> **Sugerencia**
>
> Cuando se usa un SDK, este controla las llamadas para obtener y presentar un token.

Autenticación de Microsoft Entra ID

Los servicios de Azure AI admiten la autenticación de Microsoft Entra ID, lo que le permite conceder acceso a entidades de servicio específicas o identidades administradas para las aplicaciones y servicios que se ejecutan en Azure.

Autenticación mediante entidades de servicio

El proceso general para autenticarse en los servicios de Azure AI mediante entidades de servicio es el siguiente:

Creación de un subdominio personalizado

Puede crear un subdominio personalizado de diferentes maneras, como Azure Portal, la CLI de Azure o PowerShell.

Por ejemplo, puede crear un subdominio mediante PowerShell en Azure Cloud Shell. Para ello, seleccione la suscripción con el siguiente comando:

```
PowerShell                                                    Copiar

Set-AzContext -SubscriptionName <your-Subscription-Name>
```

A continuación, cree el recurso de servicios de Azure AI que especifique un subdominio personalizado mediante la ejecución de lo siguiente:

```
PowerShell                                                    Copiar

$account = New-AzCognitiveServicesAccount -ResourceGroupName <your-resource-group-name> -name <your-account-na
```

Una vez creado, el nombre del subdominio se devolverá en la respuesta.

Asignación de un rol a una entidad de servicio

Ha creado un recurso de Azure AI que está vinculado a un subdominio personalizado. A continuación, asigne un rol a una entidad de servicio.

Para empezar, deberá registrar una aplicación. Para ello, ejecute el siguiente comando:

```
PowerShell                                                    Copiar

$SecureStringPassword = ConvertTo-SecureString -String <your-password> -AsPlainText -Force

$sp = New-AzureADApplication -DisplayName <your-app-display-name> -IdentifierUris <your-app-uris> -PasswordC
```

Esto crea el recurso de aplicación.

A continuación, use el comando **New-AzADServicePrincipal** para crear una entidad de servicio y proporcionar el identificador de la aplicación:

```
PowerShell                                                    Copiar

New-AzADServicePrincipal -ApplicationId <app-id>
```

Por último, asigne el rol **Usuarios de Cognitive Services** a la entidad de servicio mediante la ejecución de:

```
PowerShell                                                    Copiar

New-AzRoleAssignment -ObjectId <your-service-principal-object-id> -Scope <account-id> -RoleDefinitionName "Cog
```

Autenticar mediante identidades administradas

Las identidades administradas vienen en dos tipos:

- **Identidad administrada asignada por el sistema**: Se crea una identidad administrada y se vincula a un recurso específico, como una máquina virtual que necesita acceder a los servicios de Azure AI. Cuando se elimina el recurso, también se elimina la identidad.
- **Identidad administrada asignada por el usuario:** La identidad administrada se crea para que sea utilizable por varios recursos en lugar de estar vinculado a uno. Existe independientemente de cualquier recurso único.

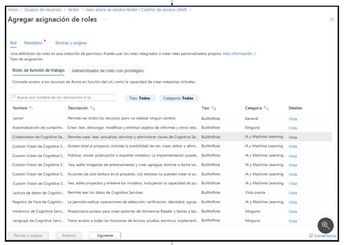
Puede asignar cada tipo de identidad administrada a un recurso durante la creación del recurso o después de que ya se haya creado.

Por ejemplo, supongamos que tiene una máquina virtual en Azure que pretende usar para el acceso diario a los servicios de Azure AI. Para habilitar una identidad asignada por el sistema para esta máquina virtual, primero debe asegurarse de que la cuenta de Azure tiene el rol Colaborador de máquina virtual. A continuación, puede ejecutar el siguiente comando mediante la CLI de Azure en el terminal de Azure Cloud Shell:

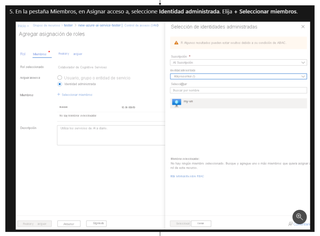
```
Azure CLI                                                     Copiar

az vm identity assign -g <my-resource-group> -n <my-vm>
```

A continuación, puede conceder acceso a los servicios de Azure AI en Azure Portal mediante lo siguiente:

1. Vaya al recurso de servicios de Azure AI que quiere conceder acceso a la identidad administrada de la máquina virtual.
2. En el panel de información general, seleccione **Control de acceso (IAM)**.
3. Seleccione **Agregar** y, después, **Agregar asignación de roles.**
4. En la pestaña Rol, seleccione **Colaborador de Cognitive Services.**



5. En la pestaña Miembros, en Asignar acceso a, seleccione **Identidad administrada**. Elija + **Seleccionar miembros**.

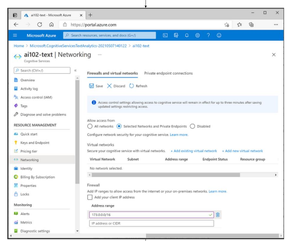


6. Asegúrese de que la suscripción está seleccionada en el menú desplegable Suscripción. Y en Identidad administrada, seleccione **Máquina virtual**.
7. Seleccione la máquina virtual de la lista y seleccione **Seleccionar**.
8. Por último, seleccione **Revisar y asignar** para revisar y, a continuación, **Revisar y asignar** de nuevo para finalizar.

Implementación de seguridad de red

Aplicación de restricciones de acceso a la red

De forma predeterminada, se puede acceder a los servicios de Azure AI desde todas las redes. Algunos recursos de servicios de Azure AI concretos (como **Azure AI Face**, **Azure AI Vision** y otros) se pueden configurar para restringir el acceso a direcciones de red específicas, ya sean de la Internet pública o de redes virtuales.



Con las restricciones de red habilitadas, un cliente que intente conectarse desde una dirección IP no permitida recibirá un error de **Acceso denegado.**