**Introducción**

Este módulo está diseñado para equipar a los administradores con los conocimientos y aptitudes necesarios para administrar y proteger el acceso a las aplicaciones empresariales mediante Microsoft Enterprise Identity, lo que garantiza que las aplicaciones solo sean accesibles para los usuarios autorizados.

**Escenario**

Imagine que es un especialista en administración de identidades y acceso responsable de controlar y supervisar el acceso a las aplicaciones empresariales dentro de su organización. Su organización se basa en Microsoft Entra ID para la administración de identidades y acceso, y debe asegurarse de que el acceso a la aplicación es seguro y compatible con las directivas.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes pueden:

* Administre el acceso a las aplicaciones empresariales en Microsoft Entra ID, incluida la configuración de concesiones de permisos de OAuth para controlar el acceso a la aplicación.
* Administre registros de aplicaciones en Microsoft Entra ID para controlar la integración de aplicaciones con la plataforma de identidad.
* Configure los ámbitos de permisos de registro de aplicaciones para conceder el nivel correcto de acceso a los recursos para las aplicaciones.
* Administre el consentimiento del permiso de registro de aplicaciones para asegurarse de que los usuarios conocen y dan su consentimiento a los permisos solicitados por las aplicaciones.
* Administre y use entidades de servicio para automatizar la administración y las interacciones de aplicaciones.
* Administre las identidades administradas para recursos de Azure para mejorar la seguridad y simplificar la administración del acceso.

**Objetivos**

El módulo tiene como objetivo proporcionar a los participantes los conocimientos y aptitudes necesarios para administrar eficazmente el acceso a las aplicaciones dentro de Microsoft Enterprise Identity. Los participantes aprenderán a controlar el acceso a las aplicaciones empresariales, configurar registros de aplicaciones, administrar permisos y aprovechar las entidades de servicio e identidades administradas, garantizando en última instancia el acceso seguro y compatible a las aplicaciones para los usuarios autorizados.

**Administración del acceso a aplicaciones empresariales en Microsoft Entra ID, incluidas las concesiones de permisos de OAuth**

El acceso continuo a las aplicaciones, la evaluación del uso y la generación de informes siguen siendo un desafío después de que una aplicación se integra en el sistema de identidad de su organización. En muchos casos, los administradores de TI o el departamento de soporte técnico deben asumir un rol activo continuo en la administración del acceso a las aplicaciones. En ocasiones, la asignación la realiza un equipo de TI general o departamental. En ocasiones, se pretende que la decisión de asignación se delegue en el responsable de la toma de decisiones, lo que requiere su aprobación antes de que TI realice la asignación.

Otras organizaciones invierten en integración con un sistema automatizado existente de administración de identidades y acceso, como Control de acceso basado en rol (RBAC) o Control de acceso basado en atributos (ABAC). Tanto la integración como el desarrollo de reglas tienden a ser procesos especializados y caros. La supervisión o la generación de informes en cualquier enfoque de administración requieren su propia inversión aparte que resulta costosa y compleja.

**¿Cómo ayuda Microsoft Entra ID?**

Microsoft Entra ID admite una amplia administración de acceso para las aplicaciones configuradas, lo que permite a las organizaciones lograr fácilmente las directivas de acceso adecuadas, que van desde la asignación automática basada en atributos (escenarios ABAC o RBAC) hasta la delegación, pasando por la administración por parte del administrador. Con Microsoft Entra ID, se pueden conseguir fácilmente directivas complejas al combinar varios modelos de administración para una sola aplicación, e incluso se pueden volver a usar las reglas de administración entre aplicaciones con las mismas audiencias.

Con Microsoft Entra ID, los informes de asignación y uso están totalmente integrados, lo que permite a los administradores informar fácilmente sobre el estado y los errores de asignación, e incluso del uso.

**Asignación de usuarios y grupos a una aplicación**

La asignación de aplicaciones de Microsoft Entra se centra en dos modos de asignación principales:

* Asignación individual : un administrador de TI con permisos de administrador global de directorios puede seleccionar cuentas de usuario individuales y concederles acceso a la aplicación.
* Asignación basada en grupos (requiere Microsoft Entra ID P1 o P2) Un administrador de TI con permisos de administrador global de directorios puede asignar un grupo a la aplicación. El acceso de usuarios específicos se determina en función de si son miembros del grupo al momento de intentar acceder a la aplicación. En otras palabras, un administrador puede crear en la práctica una regla de asignación que diga "cualquier miembro actual del grupo asignado tiene acceso a la aplicación". Con esta opción de asignación, los administradores pueden beneficiarse de cualquier opción de administración de grupos de Microsoft Entra, incluidos grupos dinámicos basados en atributos, grupos externos del sistema (por ejemplo, Active Directory local o Workday) o grupos administrados por el administrador o por autoservicio. Un único grupo se puede asignar fácilmente a varias aplicaciones, lo que garantiza que las aplicaciones con afinidad de asignación puedan compartir reglas de asignación y así reducir la complejidad de la administración en general.

**Requerir la asignación del usuario a una aplicación**

Con algunos tipos de aplicaciones, existe la opción de requerir que los usuarios estén asignados a la aplicación. Al hacerlo, se impide que todos los usuarios puedan iniciar sesión, salvo aquellos que se asignen expresamente a la aplicación. Los siguientes tipos de aplicaciones admiten esta opción:

* Aplicaciones configuradas para el inicio de sesión único (SSO) federado con autenticación basada en SAML
* Application Proxy aplicaciones que usan la autenticación previa de Microsoft Entra
* Aplicaciones, que se crean en la plataforma de aplicaciones Microsoft Entra que usan Autenticación OAuth 2.0 / OpenID Connect después de que un usuario o administrador haya dado su consentimiento a esa aplicación. Determinadas aplicaciones empresariales ofrecen más control sobre quién puede iniciar sesión.

Cuando se requiere la asignación de usuarios, solo podrán iniciar sesión los usuarios que se asignen a la aplicación (ya sea a través de una asignación directa de usuarios o según la pertenencia a grupos). Estos pueden acceder a la aplicación desde el portal Mis aplicaciones o a través de un vínculo directo.

Cuando la asignación de usuarios no es necesaria, los usuarios sin asignar no ven la aplicación en su página Aplicaciones, pero sí pueden iniciar sesión en la aplicación propiamente dicha (esto se conoce también como inicio de sesión iniciado por SP). Otra opción es usar la dirección que aparece en URL de acceso de usuario en la página Propiedades de la aplicación (esto se conoce también como inicio de sesión iniciado por IDP). Para obtener más información sobre cómo requerir configuraciones de asignación de usuarios, consulte Configuración de una aplicación.

Esto no afecta a si una aplicación aparece o no en Aplicaciones. Las aplicaciones aparecen en los paneles de acceso Mis aplicaciones de los usuarios en el momento en que un usuario o un grupo se asigna a la aplicación en cuestión.

**Determinación de la experiencia del usuario para acceder a las aplicaciones**

Microsoft Entra ID ofrecevarias formas personalizables de implementar aplicaciones para los usuarios finales de su organización:

* Microsoft Entra Aplicaciones
* Iniciador de la aplicación Microsoft 365
* Inicio de sesión directo en aplicaciones (service-pr)
* Vínculos profundos a aplicaciones federadas, con contraseña o existentes

Puede decidir si los usuarios asignados a una aplicación empresarial pueden verla en la página Aplicaciones y en el iniciador de aplicaciones de Microsoft 365.

**Ejemplo: Asignación de aplicación compleja con Microsoft Entra ID**

Considere una aplicación como Salesforce. En muchas organizaciones, Salesforce se usa principalmente en los equipos de ventas y marketing. A menudo, los miembros del equipo de marketing tienen acceso privilegiado a Salesforce, mientras que los miembros del equipo de ventas tienen acceso limitado. En muchos casos, una amplia población de trabajadores de la información tiene acceso restringido a la aplicación. Las excepciones a estas reglas complican el asunto. Con frecuencia, es prerrogativa de los equipos líderes de marketing o de ventas conceder acceso a un usuario o cambiar su rol independientemente de estas reglas genéricas.

Con Microsoft Entra ID, las aplicaciones como Salesforce se pueden configurar previamente para el inicio de sesión único (SSO) y el aprovisionamiento automatizado. Después de configurar la aplicación, un administrador puede realizar la acción puntual de crear y asignar los grupos adecuados. En este ejemplo, un administrador puede ejecutar las siguientes asignaciones:

* grupos dinámicos para representar automáticamente a todos los miembros de los equipos de ventas y marketing con atributos como departamento o rol:  
  + Todos los miembros de los grupos de marketing se asignarían al rol "marketing" en Salesforce.
  + Todos los miembros de los grupos de equipo de ventas se asignarían al rol "ventas" en Salesforce. Para afinar más, se podrían usar varios grupos que representan los equipos de ventas regionales asignados a diferentes roles de Salesforce.
* Para habilitar el mecanismo de excepciones, se podría crear un grupo de autoservicio para cada rol. Por ejemplo, el grupo de "excepción de marketing de Salesforce" se puede crear como un grupo de autoservicio. El grupo se puede asignar al rol de marketing de Salesforce y los integrantes del equipo de liderazgo de marketing se pueden convertir en propietarios. Los miembros del equipo de liderazgo de marketing podrían agregar o quitar usuarios, establecer una directiva de unión o incluso aprobar o rechazar solicitudes de unión de usuarios individuales. Este mecanismo es posible mediante una experiencia adecuada del trabajador de la información en la que los propietarios o miembros no necesitan aprendizaje especializado.

En este caso, todos los usuarios asignados se aprovisionarían automáticamente en Salesforce. Como se añaden a grupos diferentes, la asignación de roles se actualizaría en Salesforce. Los usuarios pueden detectar Salesforce y acceder a esta aplicación mediante el portal Mis aplicaciones, los clientes web de Office o navegando a su página de inicio de sesión organizativa de Salesforce. Los administradores pueden ver fácilmente el estado de uso y asignación mediante los informes de Microsoft Entra.

Los administradores pueden emplear el acceso condicional de Microsoft Entra para establecer directivas de acceso para roles específicos. Estas directivas pueden incluir si se permite el acceso fuera del entorno corporativo e incluso los requisitos de la autenticación multifactor o de los dispositivo para obtener acceso en diversos casos.

**Acceso a aplicaciones de Microsoft**

Las aplicaciones de Microsoft (como Exchange, SharePoint, Yammer, etc.) se asignan y administran de manera algo diferente a las aplicaciones SaaS de terceros u otras aplicaciones que se integran con Microsoft Entra ID para el inicio de sesión único.

Hay tres maneras principales en que un usuario puede acceder a una aplicación publicada por Microsoft.

* En el caso de aplicaciones de Microsoft 365 u otros conjuntos de aplicaciones de pago, a los usuarios se les concede acceso mediante la asignación de licencias o mediante la funcionalidad de asignación de licencias basada en grupo.
* En el caso de aplicaciones que Microsoft o un tercero publica de manera gratuita para que todo el mundo las use, a los usuarios se les puede conceder acceso mediante consentimiento del usuario. Los usuarios inician sesión en la aplicación con su cuenta profesional o educativa de Microsoft Entra, que les permite tener acceso a un conjunto limitado de datos en sus cuentas.
* Además, en el caso de aplicaciones que Microsoft o un tercero publica de manera gratuita para que todo el mundo las use, a los usuarios se les puede conceder acceso mediante consentimiento del administrador. Esto significa que un administrador ha determinado que todos los miembros de la organización pueden usar la aplicación, por lo que inicia sesión en la aplicación con una cuenta de administrador global y concede acceso a todos ellos.

Algunas aplicaciones combinan estos métodos. Por ejemplo, algunas aplicaciones de Microsoft forman parte de una suscripción a Microsoft 365, pero siguen requiriendo consentimiento.

Los usuarios pueden acceder a las aplicaciones de Microsoft 365 a través de sus portales de Office 365 correspondientes. También puede mostrar u ocultar las aplicaciones de Microsoft 365 en la página Aplicaciones con el botón de alternancia de visibilidad de Office 365 en Configuración de usuario en su directorio.

Al igual que con las aplicaciones empresariales, puede asignar usuarios a determinadas aplicaciones de Microsoft a través del centro de administración de Microsoft Entra o mediante PowerShell.

**Administración de registros de aplicaciones en Microsoft Entra ID**

Al registrar una nueva aplicación en Microsoft Entra ID, se crea automáticamente una entidad de servicio para el registro de la aplicación. La entidad de servicio es la identidad de la aplicación en el inquilino de Microsoft Entra. El acceso a los recursos está restringido por los roles asignados a la entidad de servicio, lo que permite controlar a qué recursos pueden tener acceso y en qué nivel. Por motivos de seguridad, se recomienda usar siempre entidades de servicio con las herramientas automatizadas, en lugar de permitirles iniciar sesión con una identidad de usuario.

**Importante**

*En lugar de crear una entidad de servicio, considere el uso de identidades administradas para recursos de Azure para la identidad de la aplicación. Si el código se ejecuta en un servicio que admite identidades administradas y tiene acceso a recursos que admiten la autenticación de Microsoft Entra, las identidades administradas son la opción ideal para usted.*

**Requisitos previos**

Para registrar una aplicación en el inquilino de Microsoft Entra, necesita:

Una cuenta de usuario de Microsoft Entra. Si no la tiene, puede crear una cuenta gratis.

**Permisos necesarios para registrar una aplicación**

Debe tener permisos suficientes para registrar una aplicación en su inquilino de Microsoft Entra y asignar a la aplicación un rol en su suscripción de Azure. Para completar estas tareas, se necesita Application.ReadWrite.Allpermission.

**Registrar una aplicación con Microsoft Entra ID y crear una entidad de servicio**

1. Inicie sesión en el Centro de administración de Microsoft Entra como Administrador de aplicaciones en la nube.
2. Vaya a **Identidad** > **Aplicaciones** > **Registros de aplicaciones** y seleccione **Nuevo registro**.
3. Asigna un nombre a la aplicación, por ejemplo, «example-app».
4. Seleccione un tipo de cuenta compatible, que determinará quién puede usar la aplicación.
5. En **URI de redireccionamiento**, seleccione **Web** para indicar el tipo de aplicación que quiere crear. Escriba el URI al que se envía el token de acceso.
6. Seleccione **Registrar**.

Ha creado una aplicación de Microsoft Entra y una entidad de servicio.

**Asignación de un rol a la aplicación**

Para acceder a los recursos de la suscripción, debe asignar un rol a la aplicación. Decida qué rol ofrece los permisos adecuados para la aplicación.

Puede establecer el ámbito en el nivel de suscripción, grupo de recursos o recurso. Los permisos se heredan en los niveles inferiores del ámbito.

1. Inicie sesión en Azure Portal.
2. Seleccione el nivel de ámbito al que quiere asignar la aplicación. Por ejemplo, para asignar un rol en el ámbito de suscripción, busque y seleccione **Suscripciones**. Si no ve la suscripción que busca, seleccione el **filtro de suscripciones globales**. Asegúrese de que la suscripción que le interesa está seleccionada para el inquilino.
3. Seleccione **Access Control (IAM)** .
4. Seleccione **Agregar** y, luego, **Agregar asignación de roles**.
5. En la pestaña **Rol**, selecciona el rol que desea asignar a la aplicación en la lista. Por ejemplo, para que la aplicación ejecute acciones como reiniciar, iniciar y detener instancias, seleccione el rol **Colaborador**.
6. Seleccione el botón **Siguiente**.
7. En la pestaña **Miembros**. Seleccione **Asignar acceso a** y, a continuación, seleccione **Usuario**, **Grupoo Entidad de servicio**
8. Elija **Seleccionar miembros**. De manera predeterminada, las aplicaciones de Microsoft Entra no se muestran en las opciones disponibles. Al buscar la aplicación, búsquela por su nombre.
9. Seleccione el botón **Seleccionar** y, luego, **Review + assign** (Revisar y asignar).

La entidad de servicio está configurada. Puede empezar a usarla para ejecutar aplicaciones o scripts. Para **administrar** la entidad de servicio (permisos, permisos confirmados por el usuario, ver qué usuarios han dado su consentimiento, revisar permisos, ver información de inicio de sesión, etc.), vaya a **Aplicaciones empresariales**.

**Configuración de directivas de acceso sobre los recursos**

Es posible que deba configurar permisos adicionales sobre los recursos a los que la aplicación necesita acceso. Por ejemplo, también debe actualizar las directivas de acceso de un almacén de claves para proporcionar a la aplicación acceso a las claves, los secretos o los certificados.

Para configurar directivas de acceso:

1. Inicie sesión en Azure Portal.
2. Elija su almacén de claves y seleccione **Directivas de acceso**.
3. Seleccione **Agregar directiva de acceso** y, luego, seleccione la clave, el secreto y los permisos de certificado que quiere conceder a la aplicación. Seleccione la entidad de servicio que creó anteriormente.
4. Seleccione **Agregar** para agregar la directiva de acceso.
5. Seleccione **Guardar**.

**Configuración de los ámbitos del permiso de registro de aplicaciones**

Al registrar su API web y exponerla a través de ámbitos, asignando un propietario y una función de aplicación, puede proporcionar acceso basado en permisos a sus recursos a usuarios autorizados y aplicaciones cliente que acceden a su API.

**Registro de la API web**

El acceso a API requiere configurar los ámbitos y roles de acceso. Si quiere exponer sus API web de aplicaciones de recursos a aplicaciones cliente, configure los roles y ámbitos de acceso de la API. Si quiere que una aplicación cliente pueda acceder a una API web, configure permisos de acceso a la API en el registro de la aplicación.

Para proporcionar acceso con ámbito a los recursos de la API web, primero debe registrar la API en la plataforma de identidad de Microsoft.

Siga los pasos de la sección **Registro de una aplicación** en Inicio rápido: Registrar una aplicación con la plataforma de identidad de Microsoft.

Omita la sección **URI de redireccionamiento (opcional)**. No es necesario configurar un URI de redireccionamiento para las API web, ya que ningún usuario inicia sesión de forma interactiva.

**Asignar propietario de la aplicación**

En el registro de la aplicación, en Administrar, seleccione Propietarios y Agregar propietarios.

En la nueva ventana, busque y seleccione los propietarios que desea asignar a la aplicación. Los propietarios seleccionados aparecen en el panel derecho. Una vez hecho, confirme con Seleccionar. Los propietarios de la aplicación aparecerán ahora en la lista del propietario.

**Asignar rol de aplicación**

1. En el registro de la aplicación, en Administrar, seleccione Roles de la aplicación y Crear rol de aplicación.
2. A continuación, especifique los atributos del rol de aplicación en el panel Crear rol de aplicación. Para este tutorial, puede usar los valores de ejemplo o especificar los suyos propios.

| **Campo** | **Descripción** | **Los** |
| --- | --- | --- |
| Nombre para mostrar | Nombre del rol de aplicación | *Registros de empleados* |
| Tipos de miembros permitido | Especifica si el rol de aplicación se puede asignar a usuarios o grupos o aplicaciones | *Aplicaciones* |
| Value | Valor que se muestra en la notificación "roles" de un token | Employee.Records |
| Descripción | Una descripción más detallada de la función de la aplicación | *Las aplicaciones tienen acceso a los registros de empleados* |

1. Seleccione la casilla de verificación para habilitar la función de la aplicación.

**Agregar un ámbito**

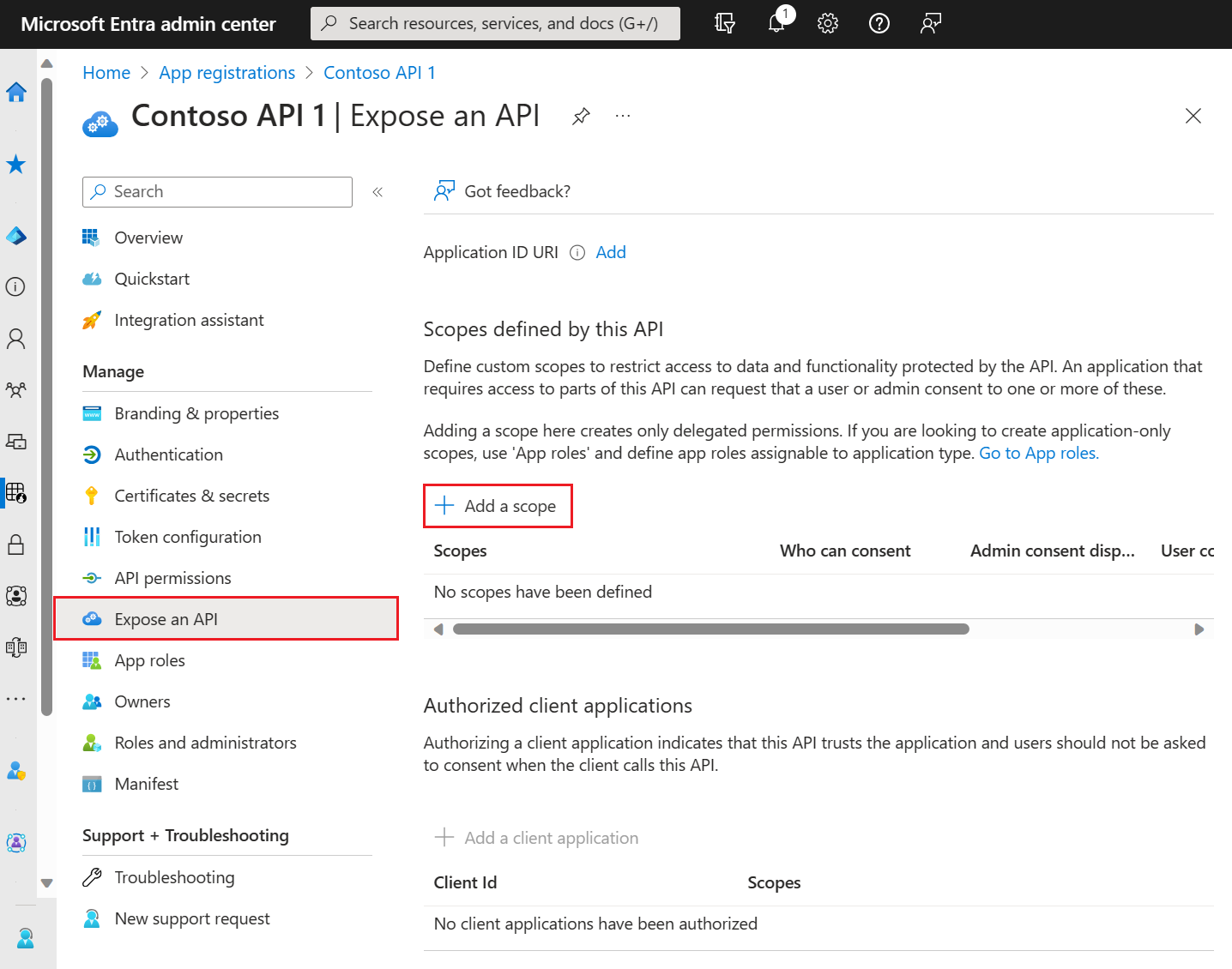
El código de las aplicaciones cliente solicita permiso para realizar operaciones definidas por la API web; para ello, pasa un token de acceso junto con sus solicitudes al recurso protegido (la API web). A continuación, la API web realiza la operación solicitada solo si el token de acceso que recibe contiene los ámbitos necesarios para la operación.

En primer lugar, siga estos pasos para crear un ámbito de ejemplo denominado Employees.Read.All:

1. Inicie sesión en el Centro de administración de Microsoft Entra como Administrador de aplicaciones en la nube.
2. Si tiene acceso a varios inquilinos, use el filtro Directorios + suscripciones del menú superior para seleccionar el inquilino que contiene el registro de la aplicación cliente.
3. Vaya a Identidad, Aplicaciones, Registros de aplicaciones y, a continuación, seleccione el registro de aplicaciones de la API.
4. Seleccione Exponer una API.
5. Seleccione Agregar, que se encuentra junto a URI de Id. de aplicación, en caso de que no haya configurado ninguno.

Puede usar el valor predeterminado de la identidad de cliente de la aplicación u otro patrón de URI de identificador de aplicación compatible. El URI de identificación de aplicación actúa como prefijo de los ámbitos a los que se hará referencia en el código de la API y debe ser único globalmente.

1. Seleccione Agregar un ámbito.



1. A continuación, especifique los atributos del ámbito en el panel Agregar un ámbito. Para este tutorial, puede usar los valores de ejemplo o especificar los suyos propios.

| **Campo** | **Valor de ejemplo** |
| --- | --- |
| Nombre de ámbito | Employees.Write.All |
| ¿Quién puede dar el consentimiento? | Solo administradores |
| Nombre para mostrar del consentimiento del administrador | Acceso de escritura a los registros de empleados |
| Descripción del consentimiento del administrador | Permite que la aplicación obtenga acceso de escritura a todos los datos de los empleados. |
| Nombre para mostrar del consentimiento del usuario | *Ninguno (deje este campo en blanco)* |
| Descripción del consentimiento del usuario | *Ninguno (deje este campo en blanco)* |

1. Establezca Estado en Habilitado y seleccione Agregar ámbito.
2. (Opcional) Para eliminar la solicitud de consentimiento por parte de los usuarios de su aplicación en los ámbitos que ha definido, puede preautorizar a la aplicación cliente para que acceda a su API web. Debe preautorizar únicamente a las aplicaciones cliente en las que confíe, ya que los usuarios no tendrán la oportunidad de rechazar el consentimiento.

* En Aplicaciones cliente autorizadas, seleccione Agregar una aplicación cliente
* Escriba el valor de Id. de aplicación (cliente) de la aplicación cliente que desea preautorizar. Por ejemplo, el de una aplicación web que ha registrado previamente.
* En Ámbitos autorizados, seleccione los ámbitos en que desea suprimir la solicitud de consentimiento y, después, seleccione Agregar aplicación.

Si ha seguido este paso opcional, la aplicación cliente será ya una aplicación cliente preautorizada (PCA) y no se pedirá a los usuarios su consentimiento al iniciar sesión en ella.

**Incorporación de un ámbito que requiera el consentimiento del administrador**

A continuación, agregue otro ámbito de ejemplo denominado Employees.Write.All para el que solo los administradores puedan dar su consentimiento. Los ámbitos que requieren el consentimiento del administrador se suelen usar para proporcionar acceso a operaciones de mayor privilegio y, a menudo, los usan aplicaciones cliente que se ejecutan como servicios back-end o demonios que no inician sesión de forma interactiva.

Para agregar el ámbito de ejemplo Employees.Write.All, siga los pasos de la sección **Incorporación de un ámbito** y especifique estos valores en el panel Agregar un ámbito:

| **Campo** | **Valor de ejemplo** |
| --- | --- |
| Nombre de ámbito | Employees.Write.All |
| ¿Quién puede dar el consentimiento? | Solo administradores |
| Nombre para mostrar del consentimiento del administrador | Acceso de escritura a los registros de empleados |
| Descripción del consentimiento del administrador | Permite que la aplicación obtenga acceso de escritura a todos los datos de los empleados. |
| Nombre para mostrar del consentimiento del usuario | *Ninguno (deje este campo en blanco)* |
| Descripción del consentimiento del usuario | *Ninguno (deje este campo en blanco)* |

Establezca Estado en Habilitado y seleccione Agregar ámbito.

**Administración del consentimiento de permisos del registro de aplicaciones**

Para acceder a un recurso protegido, como el correo electrónico o los datos del calendario, la aplicación necesita la autorización del propietario del recurso. El propietario del recurso puede dar su consentimiento o denegar la solicitud de la aplicación. Comprender estos conceptos básicos te ayudará a crear aplicaciones más seguras y confiables que solicitan solo el acceso que necesitan, cuando lo necesitan, de usuarios y administradores.

**Escenarios de acceso**

Como desarrollador de aplicaciones, debe identificar cómo accederá la aplicación a los datos. La aplicación puede usar el acceso delegado, actuar en nombre de un usuario que ha iniciado sesión o el acceso solo a la aplicación, actuando solo como identidad propia de la aplicación.

**Acceso delegado (acceso en nombre de un usuario)**

En este escenario de acceso, un usuario ha iniciado sesión en una aplicación cliente. La aplicación cliente accede al recurso en nombre del usuario. El acceso delegado requiere permisos delegados. Tanto el cliente como el usuario deben estar autorizados por separado para realizar la solicitud.

Para la aplicación cliente, se deben conceder los permisos delegados correctos. Los permisos delegados también se pueden denominar ámbitos. Los ámbitos son permisos para un recurso determinado que representan a qué puede acceder una aplicación cliente en nombre del usuario.

Para el usuario, la autorización se basa en los privilegios concedidos al usuario para que accedan al recurso. Por ejemplo, el usuario podría estar autorizado para acceder a los recursos de directorio mediante el control de acceso basado en rol (RBAC) de Microsoft Entra o para acceder a los recursos de correo y calendario mediante RBAC de Exchange Online.

**Acceso solo a la aplicación (acceso sin un usuario)**

En este escenario de acceso, la aplicación actúa por sí misma sin que ningún usuario haya iniciado sesión. El acceso a la aplicación se usa en escenarios como automatización y copia de seguridad. Por ejemplo, las aplicaciones que se ejecutan como servicios en segundo plano o demonios. Es adecuado cuando no es conveniente que un usuario específico haya iniciado sesión o cuando los datos necesarios no se puedan limitar a un solo usuario.

El acceso de solo aplicación usa roles de aplicación en lugar de ámbitos delegados. Cuando se concede a través del consentimiento, los roles de aplicación también se pueden denominar permisos de aplicaciones. Para el acceso de solo aplicación, se debe conceder a la aplicación cliente los roles de aplicación adecuados de la aplicación de recursos a la que llama para acceder a los datos solicitados.

**Tipos de permisos**

Los permisos delegados se usan en el escenario de acceso delegado. Son permisos que permiten a la aplicación actuar en nombre de un usuario. La aplicación nunca podrá acceder a nada a lo que los usuarios que han iniciado sesión no puedan acceder.

Por ejemplo, imagine una aplicación a la que se le ha concedido el permiso delegado Files.Read.All en nombre de Tom, el usuario. La aplicación solo podrá leer archivos a los que Tom puede acceder personalmente.

Los **permisos de aplicación**, en ocasiones denominados roles de aplicación, se usan en el escenario de acceso solo a la aplicación, sin que haya un usuario que haya iniciado sesión. La aplicación podrá acceder a los datos a los que está asociado el permiso. Por ejemplo, una aplicación a la que se le haya concedido el permiso Files.Read.All podrá leer cualquier archivo del inquilino. Solo un administrador o propietario de la entidad de servicio puede dar su consentimiento a los permisos de aplicación.

Hay otras maneras en las que se puede conceder autorización a las aplicaciones para el acceso solo a la aplicación. Por ejemplo, se puede asignar una aplicación a rol RBAC de Microsoft Entra.

**Comparación de permiso de aplicación y delegados**

| **Tipos de permisos** | **Permisos delegados** | **Permisos de aplicación** |
| --- | --- | --- |
| Tipos de aplicaciones | Aplicación web/móvil/de página única (SPA) | Web/Demonio |
| Contexto de acceso | Obtención del acceso en nombre de un usuario | Obtener acceso sin un usuario |
| ¿Quién puede dar el consentimiento? | Los usuarios pueden dar su consentimiento a sus datos Los administradores pueden dar su consentimiento a todos los usuarios | Solo el administrador puede dar consentimiento a |
| Métodos de consentimiento | Estático: lista configurada en el registro de aplicaciones Dinámico: solicitar permisos individuales en el inicio de sesión | SOLO estático: lista configurada en el registro de aplicaciones |
| Otros nombres | Ámbitos Ámbitos de permisos de OAuth2 | Roles de aplicación Permisos solo de aplicación |
| Resultado del consentimiento (específico de Microsoft Graph) | Concesión de permisos de OAuth2 | Asignación de roles de aplicación |

**Consentir**

Una manera en que se conceden permisos a las aplicaciones es a través del consentimiento. El consentimiento es un proceso en el que los usuarios o administradores autorizan a una aplicación el acceso a un recurso protegido. Por ejemplo, cuando un usuario intenta iniciar sesión por primera vez en una aplicación, la aplicación puede solicitar permiso para ver el perfil del usuario y leer el contenido del buzón del usuario. El usuario ve la lista de permisos que la aplicación solicita a través de un mensaje de consentimiento. Otros escenarios en los que los usuarios pueden ver un mensaje de consentimiento incluyen:

* Cuando se revoca el consentimiento concedido previamente.
* Cuando la aplicación se codifica para solicitar específicamente el consentimiento durante el inicio de sesión.
* Cuando la aplicación usa el consentimiento dinámico para solicitar nuevos permisos según sea necesario en el entorno de ejecución.

Los detalles clave de un mensaje de consentimiento son la lista de permisos que requiere la aplicación y la información del publicador

**Consentimiento del usuario**

El consentimiento del usuario se produce cuando un usuario intenta iniciar sesión en una aplicación. El usuario proporciona sus credenciales de inicio de sesión. Estas credenciales se comprueban para determinar si ya se ha concedido el consentimiento. Si no existe ningún registro anterior de consentimiento del usuario o administrador para los permisos necesarios, se muestra al usuario una solicitud de consentimiento y se le pide que conceda a la aplicación los permisos solicitados. En muchos casos, puede ser necesario que un administrador otorgue el consentimiento en nombre del usuario.

**Consentimiento del administrador**

Dependiendo de los permisos que se necesiten, es posible que algunas aplicaciones requieran que un administrador sea el que conceda consentimiento. Por ejemplo, los permisos de aplicación y muchos permisos delegados de alto privilegio solo se pueden conceder por un administrador. Los administradores pueden conceder consentimiento para sí mismos o para toda la organización.

**Autorización previa**

La autorización previa permite que un propietario de la aplicación de recursos conceda permisos sin necesidad de que los usuarios vean un mensaje de consentimiento para el mismo conjunto de permisos que se han autorizado previamente. De este modo, una aplicación que se ha autenticado previamente no pedirá a los usuarios que concedan su consentimiento a los permisos. Los propietarios de recursos pueden autorizar previamente las aplicaciones cliente en Azure Portal o mediante PowerShell y las API, como Microsoft Graph.

**Administración y uso de entidades de servicio**

**Registro de la aplicación**

Para delegar funciones de administración de identidades y acceso a Microsoft Entra ID, una aplicación debe registrarse con un inquilino de Microsoft Entra. Al registrar la aplicación con Microsoft Entra ID, va a crear una configuración de identidad para la aplicación que le permita integrarla con Microsoft Entra ID. Al registrar una aplicación, elige si es un inquilino único o multiinquilino y, si lo desea, puede establecer un URI de redirección. Puede encontrar instrucciones paso a paso sobre cómo registrar una aplicación en el inicio rápido del registro de aplicaciones.

Una vez completado el registro de la aplicación, tiene una instancia globalmente única de la aplicación (el objeto de aplicación) que reside en su directorio o inquilino principal. También tiene un identificador único global para la aplicación (el identificador de la aplicación o del cliente). Puede agregar secretos o certificados y ámbitos para que la aplicación funcione, personalizar la marca de la aplicación en el cuadro de diálogo de inicio de sesión y mucho más.

Al registrar una aplicación, se crean automáticamente un objeto de aplicación y un objeto de entidad de servicio en su inquilino principal. Si registra o crea una aplicación mediante las API de Microsoft Graph, la creación del objeto de entidad de servicio se hace en un paso independiente.

**Objeto de aplicación**

Una aplicación de Microsoft Entra se define por su objeto de aplicación único, que reside en el inquilino de Microsoft Entra donde se registró la aplicación (conocido como inquilino "principal" de la aplicación). El objeto de aplicación se usa como plantilla o plano técnico para crear uno o varios objetos de entidad de servicio. La entidad de servicio se crea en todos los inquilinos en los que se utiliza la aplicación. De forma similar a una clase en la programación orientada a objetos, el objeto de aplicación tiene algunas propiedades estáticas que se aplican a todas las entidades de servicio creadas (o instancias de aplicación).

El objeto de aplicación describe tres aspectos de una aplicación:

* Cómo el servicio puede emitir tokens para acceder a la aplicación
* Los recursos a los que es posible que la aplicación necesite acceder
* Las acciones que puede realizar la aplicación

Puede usar la página **registros de aplicaciones** en el Centro de administración de Microsoft Entra para enumerar y administrar los objetos de aplicación en el inquilino principal.

La **entidad de aplicación** de Microsoft Graph define el esquema para las propiedades de un objeto de aplicación.

**Objeto de entidad de servicio**

Para acceder a los recursos que están protegidos por un inquilino de Microsoft Entra, la entidad que requiere acceso debe estar representada por una entidad de seguridad. Este requisito es cierto para los usuarios (entidad de seguridad de usuario) y para las aplicaciones (entidad de servicio). La entidad de seguridad define la directiva de acceso y los permisos para el usuario o la aplicación de ese inquilino de Microsoft Entra. Esto habilita características básicas como la autenticación del usuario o de la aplicación durante el inicio de sesión y la autorización durante el acceso a los recursos.

Hay tres tipos de entidad de servicio:

* **Aplicación**: este tipo de entidad de servicio es la representación local o la instancia de aplicación de un objeto de aplicación global en un único inquilino o directorio. En este caso, una entidad de servicio es una instancia concreta creada a partir del objeto de aplicación, que hereda determinadas propiedades de ese objeto de aplicación. La entidad de servicio se crea en cada inquilino donde se usa la aplicación y hace referencia al objeto de aplicación único global. El objeto de entidad de servicio define lo que la aplicación puede hacer en el inquilino específico, quién puede acceder a la aplicación y a qué recursos tiene acceso la aplicación.

**Nota**

Cuando una aplicación tiene permiso para acceder a los recursos de un inquilino (tras el registro o consentimiento), se crea un objeto de entidad de seguridad de servicio. Cuando se registra una aplicación, se crea automáticamente una entidad de seguridad de servicio. También puede crear objetos de entidad de servicio en un inquilino mediante Azure PowerShell, la CLI de Azure, Microsoft Graph y otras herramientas.

* **identidad administrada**: este tipo de entidad de servicio se usa para representar una identidad administrada. Las identidades administradas eliminan la necesidad de que los desarrolladores administren las credenciales. Las identidades administradas proporcionan una identidad que usan las aplicaciones al conectarse a los recursos que admiten la autenticación de Microsoft Entra. Cuando se habilita una identidad administrada, se crea en el inquilino una entidad de servicio que representa esa identidad administrada. A las entidades de servicio que representan identidades administradas se les pueden conceder acceso y permisos, pero no se pueden actualizar ni modificar directamente.
* **Heredado**: este tipo de entidad de servicio representa una aplicación heredada (la que se ha creado antes de que se introdujeran o crearan registros de aplicaciones mediante experiencias heredadas). Una entidad de servicio heredada puede tener credenciales, nombres de entidad de servicio, direcciones URL de respuesta y otras propiedades que un usuario autorizado puede editar, pero no tiene un registro de aplicación asociado. La entidad de servicio solo se puede usar en el inquilino donde se creó.

La **entidad ServicePrincipal** de Microsoft Graph define el esquema para las propiedades de un objeto de entidad de servicio.

Puede usar la página **Aplicaciones empresariales** del centro de administración de Microsoft Entra para enumerar y administrar las entidades de servicio de un inquilino. Se pueden ver los permisos de la entidad de servicio, los permisos con consentimiento del usuario, los usuarios que han dado ese consentimiento, la información de inicio de sesión, etc.

**Relación entre los objetos de aplicación y las entidades de servicio**

El objeto de aplicación es la representación global de la aplicación para su uso en todos los inquilinos, y la entidad de servicio es la representación local para su uso en un inquilino específico. El objeto de aplicación actúa como la plantilla a partir de la cual se derivan las propiedades comunes y predeterminadas para su uso en la creación de objetos de entidad de servicio correspondientes.

Un objeto de aplicación tiene lo siguiente:

* Una relación 1:1 con la aplicación de software y
* Una relación 1:varios con sus objetos de entidad de servicio correspondientes

Debe crearse una entidad de servicio en cada inquilino donde se usa la aplicación. Esto permite establecer una identidad para el inicio de sesión o el acceso a los recursos que va a proteger el inquilino. Una aplicación de inquilino único tendrá solo una entidad de servicio (en su inquilino principal), que normalmente se crea y se consiente para su uso durante el registro de la aplicación. Una aplicación multiinquilino también tiene una entidad de servicio creada en cada inquilino donde un usuario de ese inquilino ha dado su consentimiento para su uso.

**Enumeración de entidades de servicio asociadas a una aplicación**

Puede encontrar las entidades de servicio asociadas a un objeto de aplicación.

Consecuencias de la modificación y eliminación de aplicaciones

Los cambios que realice en el objeto de aplicación también se reflejan en su objeto de entidad de servicio, solo en el inquilino principal de la aplicación (es decir, el inquilino en donde se registró). Esto significa que, al eliminar un objeto de la aplicación, también se eliminará su objeto de la entidad de servicio del inquilino principal. Sin embargo, restaurar ese objeto de aplicación mediante la interfaz de usuario de registros de aplicaciones no restaurará su entidad de servicio correspondiente.

En este escenario de ejemplo:

| **Step** | **Descripción** |
| --- | --- |
| 1 | El proceso de creación de los objetos de aplicación y de entidad de servicio del inquilino principal de la aplicación. |
| 2 | Cuando los administradores de Contoso y Fabrikam completan el consentimiento, se crea un objeto de entidad de servicio en el inquilino de Microsoft Entra de la empresa y se asignan los permisos que haya concedido el administrador. Tenga en cuenta también que la aplicación de recursos humanos podría estar configurada o diseñada para dar consentimiento a los usuarios para el uso individual. |
| 3 | Los inquilinos consumidores de la aplicación HR (Contoso y Fabrikam) tienen cada uno de ellos su propio objeto de entidad de servicio. Cada uno representa su uso de una instancia de la aplicación en tiempo de ejecución, que se rige por los permisos que consiente el administrador correspondiente. |

**Administrar identidades administradas de recursos de Azure**

Un desafío común para los desarrolladores es la administración de secretos, credenciales, certificados, claves, etc. que se usan para proteger la comunicación entre servicios. Las identidades administradas eliminan la necesidad de administrar las credenciales para los desarrolladores.

Aunque los desarrolladores pueden almacenar de forma segura los secretos en Azure Key Vault, los servicios necesitan una manera de acceder a él. Las identidades administradas proporcionan una identidad administrada automáticamente en Microsoft Entra ID para que las aplicaciones la utilicen al conectarse a los recursos que admiten la autenticación de Microsoft Entra. Las aplicaciones pueden usar identidades administradas para obtener tokens de Microsoft Entra sin necesidad de administrar credenciales.

**Estas son algunas de las ventajas de usar las identidades administradas**

* No es necesario administrar credenciales. Las credenciales ni siquiera están accesibles.
* Puede usar identidades administradas para autenticarse en cualquier recurso que admita la autenticación de Microsoft Entra, incluidas sus propias aplicaciones.
* Las identidades administradas se pueden usar sin costes adicionales.

**Tipos de identidad administrada**

Hay dos tipos de identidades administradas:

* **Asignadas por el sistema**. Algunos recursos de Azure, como las máquinas virtuales, permiten habilitar una identidad administrada directamente en el recurso. Cuando habilita una identidad administrada asignada por el sistema:  
  + Se crea una entidad de servicio de un tipo especial en Microsoft Entra ID para la identidad. La entidad de servicio está vinculada al ciclo de vida de ese recurso de Azure. Cuando se elimina el recurso de Azure, Azure elimina automáticamente la entidad de servicio automáticamente.
  + Por diseño, solo ese recurso de Azure puede usar esta identidad para solicitar tokens de Microsoft Entra ID.
  + Autorice a la identidad administrada para que pueda acceder a uno o varios servicios.
  + El nombre de la entidad de servicio asignada por el sistema siempre es el mismo que el nombre del recurso de Azure para el que se crea. En el caso de una ranura de implementación, el nombre de su identidad asignada por el sistema es <app-name>/slots/<slot-name>.
* **Asignadas por el usuario**. También es posible crear una identidad administrada como un recurso independiente de Azure. Puede crear una identidad administrada asignada por el usuario y asignársela a uno o varios recursos de Azure. Al habilitar una identidad administrada asignada por el usuario:
  + Se crea una entidad de servicio de un tipo especial en Microsoft Entra ID para la identidad. La entidad de servicio se administra por separado de los recursos que la usan.
  + Las identidades asignadas por el usuario se pueden usar en varios recursos.
  + Autorice a la identidad administrada para que pueda acceder a uno o varios servicios.

En la tabla siguiente, se muestran las diferencias entre los dos tipos de identidades administradas:

| **Propiedad** | **Identidad administrada asignada por el sistema** | **Identidad administrada asignada por el usuario** |
| --- | --- | --- |
| Creación | Se crea como parte de un recurso de Azure (por ejemplo, Azure Virtual Machines o Azure App Service). | Se crea como un recurso de Azure independiente. |
| Ciclo de vida | Se comparte el ciclo de vida con el recurso de Azure con el que se creó la identidad administrada. Si se elimina el recurso primario, se elimina también la identidad administrada. | Ciclo de vida independiente. Se debe eliminar explícitamente. |
| Uso compartido de recursos de Azure | No se puede compartir. Solo se puede asociar con un único recurso de Azure. | Se puede compartir. La misma identidad administrada asignada por el usuario se puede asociar con más de un recurso de Azure. |
| Casos de uso comunes | Cargas de trabajo que contiene un único recurso de Azure. Cargas de trabajo que necesitan identidades independientes. Por ejemplo, una aplicación que se ejecuta en una sola máquina virtual. | Cargas de trabajo que se ejecutan en varios recursos y pueden compartir una única identidad. Cargas de trabajo que necesitan autorización previa para un recurso seguro como parte de un flujo de aprovisionamiento. Cargas de trabajo donde los recursos se reciclan con frecuencia, pero los permisos deben permanecer coherentes. Por ejemplo, una carga de trabajo en la que varias máquinas virtuales tienen que acceder al mismo recurso. |

**¿Cómo se usan las identidades administradas de Managed Identities for Azure Resources?**

Siga los pasos siguientes para usar identidades administradas:

1. Cree una identidad administrada en Azure. Puede elegir entre la identidad administrada asignada por el sistema o por el usuario.
   * Cuando use una identidad administrada que haya asignado el usuario, asigne la identidad administrada a Azure Resource "de origen", como una máquina virtual, Azure Logic App o Azure Web App.
2. Autorice el acceso al servicio de "destino" para la identidad administrada y
3. Use la identidad administrada para acceder a un recurso. Para ello, puede usar el SDK de Azure con la biblioteca de Azure.Identity. Algunos recursos de "origen" ofrecen conectores que saben usar identidades administradas para las conexiones. En ese caso, usará la identidad como si esta fuera una característica de ese recurso de "origen".

**Recomendación sobre cuándo usar y configurar una instancia de Microsoft Entra Application Proxy, incluida la autenticación**

Microsoft Entra Application Proxy es una solución de acceso remoto segura y rentable a todas las aplicaciones locales. Proporciona una ruta de acceso de transición inmediata para las organizaciones de tipo "La Nube primero" para administrar el acceso a las aplicaciones locales heredadas que aún no pueden usar protocolos modernos.

Application Proxy se recomienda para dar a los usuarios remotos acceso a recursos internos. Application Proxy reemplaza la necesidad de una VPN o proxy inverso para estos casos de uso de acceso remoto. No está pensado para aquellos usuarios que están en la red corporativa. Estos usuarios que usan Application Proxy para el acceso a la intranet pueden experimentar problemas de rendimiento no deseado.

**Planeamiento de la implementación**

Requisitos previos:

Debe cumplir los siguientes requisitos previos antes de iniciar la implementación. Puede ver más información sobre cómo configurar su entorno, incluidos estos requisitos previos, en este tutorial.

* Conectores: Los conectores son agentes ligeros que puede implementar en:  
  + Hardware físico en el entorno local
  + Una VM hospedada en cualquier solución de hipervisor
  + Una VM hospedada en Azure para habilitar una conexión saliente con el servicio Application Proxy.
* Conectores de proxy de aplicaciones de Microsoft Entra.
  + Las máquinas del conector se deben habilitar para TLS 1.2 antes de instalar los conectores.
  + Si es posible, implemente los conectores en la misma red y segmento que los servidores de aplicaciones web de back-end. Es mejor implementar los conectores después de completar una detección de aplicaciones.
  + Se recomienda que cada grupo de conectores tenga al menos dos conectores para proporcionar alta disponibilidad y escala. Tener tres conectores es una situación óptima en caso de que necesite realizar tareas de servicio en una máquina en cualquier momento. Revise la tabla de capacidad de los conectores para obtener ayuda para decidir en qué tipo de máquina instalará conectores. Cuanto mayor sea la máquina, más búfer y mayor rendimiento tendrá el conector.
* Configuración de acceso a la red: los conectores de Microsoft Entra Application Proxy se conectan a Azure por HTTPS (puerto TCP 443) y HTTP (puerto TCP 80).  
  + La interrupción del tráfico TLS del conector no se admite y evitará que los conectores establezcan un canal seguro con sus respectivos puntos de conexión de Azure App Proxy.
  + Evite todo tipo de inspección insertada en las comunicaciones TLS salientes entre los conectores y Azure. La inspección interna entre un conector y las aplicaciones de back-end es posible, pero podría degradar la experiencia del usuario y, por lo tanto, no se recomienda.
  + Tampoco se admite, ni se necesita, el equilibrio de carga de los propios conectores.

**Consideraciones importantes antes de configurar Microsoft Entra Application Proxy**

Deben cumplirse los siguientes requisitos principales para configurar e implementar Microsoft Entra Application Proxy.

* Incorporación de Azure: Antes de implementar Application Proxy, las identidades de usuario se deben sincronizar desde un directorio local o bien se deben crear directamente desde los inquilinos de Microsoft Entra. La sincronización de identidades permite a Microsoft Entra ID realizar una autenticación previa de los usuarios antes de concederles acceso a aplicaciones publicadas en App Proxy y tener la información del identificador de usuario necesarios para realizar el inicio de sesión único (SSO).
* Requisitos de acceso condicional: No se recomienda el uso de Application Proxy para el acceso de intranet, ya que esto agrega una latencia que afectará a los usuarios. Es recomendable usar Application Proxy con las directivas de autenticación previa y acceso condicional para el acceso remoto desde Internet. Un enfoque para proporcionar acceso condicional para su uso en la intranet es modernizar las aplicaciones para que se puedan autenticar directamente con Microsoft Entra ID. Consulte Recursos para migrar aplicaciones a Microsoft Entra ID para obtener más información.
* Límites de servicio: Para protegerse frente al consumo excesivo de recursos por parte de inquilinos individuales, existen límites definidos por aplicación e inquilino. Para ver estos límites, consulte Restricciones y límites del servicio Microsoft Entra. Estos límites se basan en un banco de pruebas muy superior al volumen de uso típico y proporcionan un búfer suficiente para la mayoría de las implementaciones.
* Certificado público: Si usa nombres de dominio personalizados, deberá adquirir un certificado TLS/SSL. Según los requisitos de la organización, obtener un certificado puede llevar algún tiempo y se recomienda comenzar el proceso lo antes posible. Azure Application Proxy admite certificados estándar, comodín o basados en SAN. Para obtener más información, consulte Configuración de dominios personalizados con el proxy de aplicaciones de Microsoft Entra.
* Requisitos de dominio: El inicio de sesión único en las aplicaciones publicadas con la delegación restringida de Kerberos (KCD) requiere que el servidor que ejecuta el conector y el servidor que ejecuta la aplicación estén unidos a un dominio y formen parte del mismo dominio o los mismos dominios de confianza. Para obtener más información sobre el tema, consulte KCD para el inicio de sesión único con Application Proxy. El servicio de conectores se ejecuta en el contexto del sistema local y no debería configurarse para usar una identidad personalizada.
* Registros de DNS para direcciones URL  
  + Antes de usar dominios personalizados en Application Proxy, debe crear un registro CNAME en un DNS público, lo que permite a los clientes resolver la dirección URL externa y personalizada definida para la dirección predefinida de Application Proxy. Si no se pudiera crear un registro CNAME para una aplicación que use un dominio personalizado, los usuarios remotos no podrán conectarse a la aplicación. Los pasos necesarios para agregar registros CNAME pueden variar de un proveedor de DNS a otro, así que aprenda a administrar registros DNS y conjuntos de registros utilizando el Centro de administración de Microsoft Entra.
  + De forma similar, los hosts de conector deben poder resolver la dirección URL interna de las aplicaciones que se publican.
* Derechos y roles administrativos  
  + La instalación del conector requiere derechos de administrador local en el servidor Windows en que se instala. También requiere un mínimo de un rol de Administrador de la aplicación para autenticarse y registrar la instancia del conector para su inquilino de Microsoft Entra.
  + La publicación y administración de aplicaciones requiere el rol Administrador de la aplicación. Los administradores de aplicaciones pueden administrar todas las aplicaciones del directorio, incluidos los registros, configuraciones de SSO, asignaciones y configuración de licencias de usuario y de grupo, configuración del proxy de aplicación y consentimiento. No concede la capacidad de administrar el acceso condicional. El rol Administrador de aplicaciones en la nube tiene todas las funcionalidades del administrador de la aplicación, excepto que no se permite la administración de la configuración de Application Proxy.
* Licencias: Application Proxy está disponible a través de una suscripción Microsoft Entra ID P1 o P2.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. Un desarrollador quiere proporcionar acceso basado en permisos a los recursos de su API web a usuarios autorizados y aplicaciones cliente. ¿Cuál es el primer paso que deben realizar?**

1. Configuración de permisos para que la aplicación cliente acceda a la API en el registro de la aplicación
2. Creación de un rol de aplicación en el registro de aplicaciones
3. Registro de la API web con la plataforma de identidad de Microsoft

**2. Una organización quiere lograr fácilmente las directivas de acceso adecuadas para sus aplicaciones configuradas. ¿Qué servicio de Microsoft puede ayudarles a lograr esto?**

1. Microsoft Excel
2. Microsoft Word
3. Microsoft Entra ID

**3. Una empresa quiere asegurarse de que su aplicación web sea segura y esté protegida contra el acceso no autorizado. Quieren implementar un mecanismo de seguridad que permita a los usuarios autenticarse antes de acceder a la aplicación. ¿Cuál es el primer paso que deben realizar?**

1. Configuración de permisos para que la aplicación cliente acceda a la API en el registro de la aplicación
2. Registro de la API web con la plataforma de identidad de Microsoft
3. Implementación de un mecanismo de autenticación como OAuth u OpenID Connect

**4. Un desarrollador quiere proporcionar acceso basado en permisos a su API web. ¿Qué pasos deben seguir para lograr esto?**

1. El desarrollador debe crear un nuevo rol de aplicación para la API web.
2. El desarrollador debe configurar los permisos para que la aplicación cliente acceda a la API en el registro de la aplicación.
3. El desarrollador debe registrar la API web con la Plataforma de identidad de Microsoft, asignar un propietario, crear un rol de aplicación y agregar un ámbito.

**5. Un desarrollador debe almacenar de forma segura secretos en Azure Key Vault y permitir que los servicios accedan a ellos. ¿Cuál es la ventaja de usar identidades administradas?**

1. Las identidades administradas requieren que los desarrolladores administren las credenciales.
2. Las identidades administradas solo se pueden usar para autenticarse en los recursos de Microsoft Entra.
3. Las identidades administradas eliminan la necesidad de que los desarrolladores administren secretos, credenciales, certificados y claves que se usan para proteger la comunicación entre servicios.
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo se trata la administración del acceso a las aplicaciones en Microsoft Entra ID, incluido el control del acceso a aplicaciones empresariales, la administración de registros y permisos de aplicaciones, el uso de entidades de servicio y la configuración del Application Proxy de Entra para el acceso seguro.