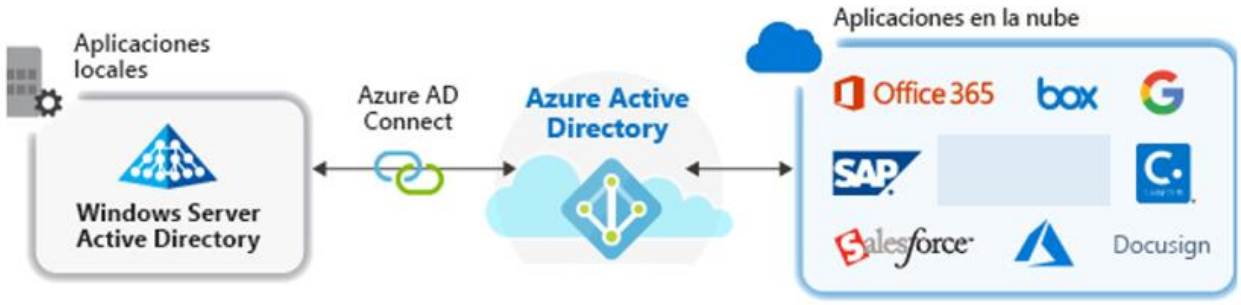
1. OBJETIVO

Informar el método de integración de aplicaciones con Azure Active Directory (Azure AD)

2. TÉRMINOS Y DEFINICIONES

Azure AD proporciona la administración de identidades para aplicaciones. La integración de Azure AD ofrece a los usuarios una experiencia de inicio de sesión simplificada y ayuda a que las aplicaciones se ajusten a las directivas de TI.



La plataforma de identidad de Microsoft simplifica la autenticación para los desarrolladores de aplicaciones, ya que ofrece la identidad como servicio, con compatibilidad con protocolos estándares del sector, como OAuth 2.0 y OpenID Connect, además de bibliotecas de código abierto para distintas plataformas para poder empezar a programar rápidamente.

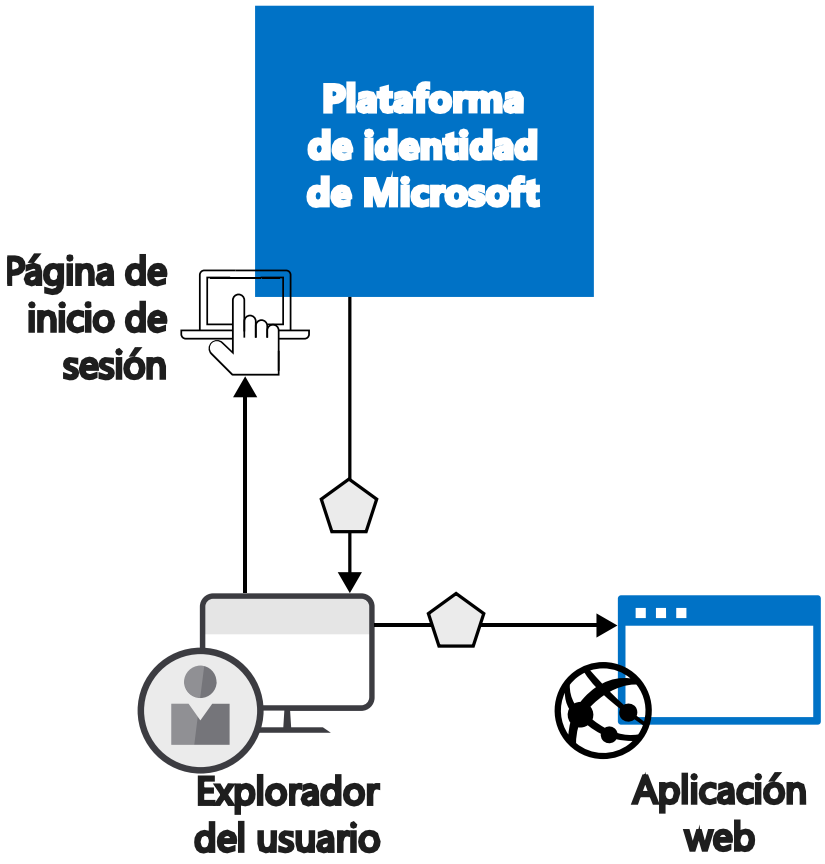
Hay dos casos de uso principales en el modelo de programación de la plataforma de identidad de Microsoft:

- Durante un flujo de concesión de autorización de OAuth 2.0: cuando el propietario del recurso autoriza a la aplicación cliente, lo que permite al cliente acceder a los recursos del propietario del recurso.
- Durante el acceso a los recursos por el cliente: cuando lo implementa el servidor de recursos, mediante el uso de los valores de notificación presentes

en el token de acceso para tomar decisiones de control de acceso basadas en ellos.

Aspectos básicos de la autenticación en la plataforma de identidad de Microsoft

Veamos el escenario más básico en el que es necesario identificarse: un usuario de un explorador web debe autenticarse en una aplicación web. El siguiente diagrama muestra este escenario:



Esto es lo que necesita saber sobre los distintos componentes que se muestran en el diagrama:

- La plataforma de identidad de Microsoft es el proveedor de identidades. El proveedor de identidades es el responsable de comprobar la identidad de los usuarios y las aplicaciones que existen en el directorio de una organización y

de emitir tokens de seguridad tras la autenticación correcta de dichos usuarios y aplicaciones.

- Cualquier aplicación que necesite externalizar la autenticación a la plataforma de identidad de Microsoft se debe registrar en Azure Active Directory (Azure AD). Azure AD registra la aplicación y la identifica de forma única en el directorio.
- Los desarrolladores pueden usar las bibliotecas de autenticación de código abierto de la plataforma de identidad de Microsoft para facilitar la autenticación, ya que administran los detalles de los protocolos para el usuario. Para más información, consulte las bibliotecas de autenticación v2.0 y las bibliotecas de autenticación v1.0 de la plataforma de identidad de Microsoft.
- Una vez autenticado el usuario, la aplicación debe validar el token de seguridad de este para garantizar que la autenticación se realizó correctamente. Puede encontrar guías de inicio rápido, tutoriales y ejemplos de código en una variedad de lenguajes y marcos que muestran lo que debe hacer la aplicación.
    - Para crear rápidamente una aplicación y agregar funcionalidad similar a obtener tokens, actualizar tokens, iniciar la sesión de un usuario, mostrar información de usuario y mucho más, vea la sección **Inicios rápidos** de la documentación.
    - Para obtener procedimientos detallados basados en un escenario para tareas de autenticación principales para desarrolladores, como obtener tokens de acceso y usarlos en las llamadas a Microsoft Graph API y otras API, implementar el inicio de sesión con Microsoft con una aplicación tradicional basada en explorador web mediante OpenID Connect y más, consulte la sección **Tutoriales** de la documentación.

    - Para descargar ejemplos de código, vaya a GitHub.
- El flujo de solicitudes y respuestas del proceso de autenticación lo determina el protocolo de autenticación que usó, como OAuth 2.0, OpenID Connect, WS-Federation o SAML 2.0. Para más información sobre los protocolos, consulte la sección **Conceptos > Protocolo de autenticación** de la documentación.

En el escenario de ejemplo anterior, puede clasificar las aplicaciones según estos dos roles:

- Aplicaciones que necesitan acceso seguro a recursos
- Aplicaciones que desempeñan el rol del propio recurso

3. INSTRUCCIONES GENERALES

La plataforma de identidad de Microsoft es una evolución de la plataforma para desarrolladores de Azure Active Directory (Azure AD). Permite a los desarrolladores compilar aplicaciones que inicien sesión en todas las identidades de Microsoft, obtener tokens para llamar a las API de Microsoft, como Microsoft Graph, o a otras API que los desarrolladores hayan creado. El punto de conexión de la Plataforma de identidad de Microsoft consta de lo siguiente:

Servicio de autenticación compatibles con los estándares OAuth 2.0 y OpenID Connect que permite a los desarrolladores autenticar identidades de Microsoft como las siguientes:

Cuentas profesionales o educativas (aprovisionadas a través de Azure AD)

Cuentas personales de Microsoft (por ejemplo, Skype, Xbox y Outlook.com)

Cuentas locales y sociales (a través de Azure AD B2C)

Bibliotecas de código abierto: bibliotecas de autenticación de Microsoft (MSAL) y compatibilidad con cualquier otra biblioteca que cumpla con los estándares.

Portal de administración de aplicaciones: una experiencia de registro y configuración basada integrada en Azure Portal, junto con las demás funcionalidades de administración de Azure.

PowerShell y API de configuración de aplicaciones: permite la configuración mediante programación de las aplicaciones a través de la API de REST (Microsoft Graph y Azure Active Directory Graph 1.6) y PowerShell, para que pueda automatizar las tareas de DevOps.

Contenido para desarrolladores: documentación conceptual y de referencia, ejemplos de inicio rápido, ejemplos de código, tutoriales y guías paso a paso.
La Plataforma de identidad de Microsoft ofrece a los desarrolladores una perfecta integración con las innovaciones en el espacio de identidad y seguridad, como la autenticación sin contraseña, la autenticación de nivel superior y el acceso condicional. No es necesario que implemente esta funcionalidad manualmente: las aplicaciones integradas de manera nativa con la Plataforma de identidad de Microsoft aprovechan estas innovaciones.

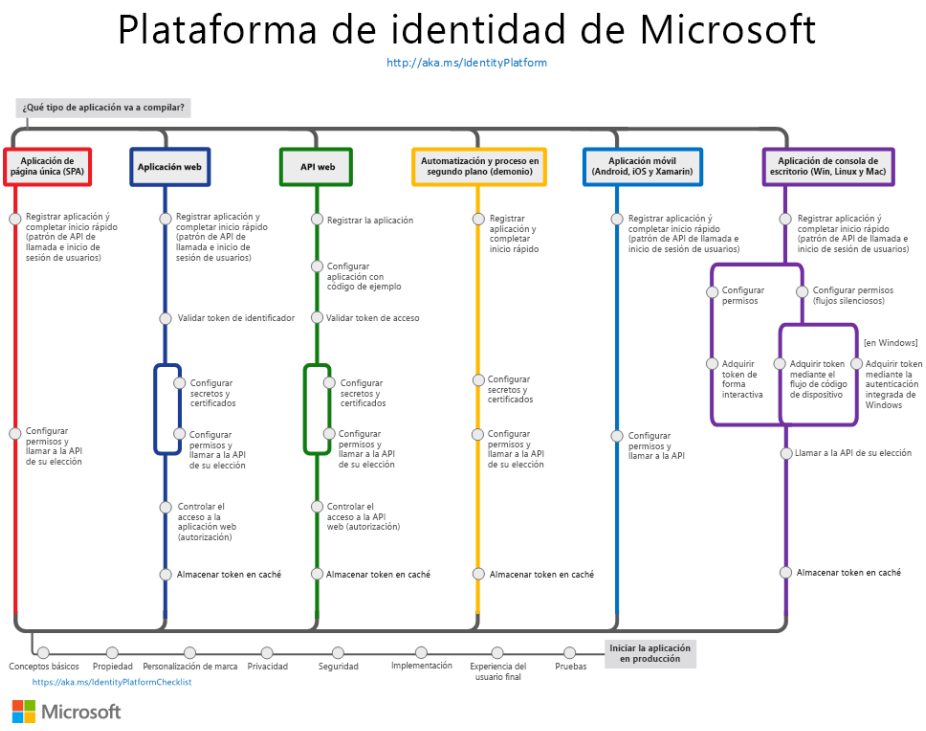
Con la Plataforma de identidad de Microsoft, puede escribir código una vez y llegar a cualquier usuario. Puede compilar una aplicación una sola vez y conseguir que funcione en muchas plataformas, o bien compilar una aplicación que funcione como un cliente, así como una aplicación de recursos (API).

Elija un escenario que se aplique a su trabajo: cada ruta de acceso de escenario tiene un inicio rápido y una página de información general para ayudarle a ponerse en marcha en cuestión de minutos:

- Compilación de una aplicación de una sola página
- Compilación de una aplicación web que permite iniciar sesión a los usuarios
- Compilación de una aplicación web que llama a las API web

- Compilación de una API web protegida
- Compilación de una API web que llama a las API web
- Compilación de una aplicación de escritorio
- Compilación de una aplicación demonio
- Compilación de una aplicación móvil

En el gráfico siguiente se describen escenarios comunes de aplicaciones de autenticación: úselo como referencia al integrar la Plataforma de identidad de Microsoft con su aplicación.



Información y referencias:

https://docs.microsoft.com/es-es/azure/active-directory/develop/v2-overview

https://docs.microsoft.com/es-es/azure/active-directory/develop/authentication-scenarios

Octubre - 2019