200 XP

Prueba de conocimientos

5 minutos

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

Comprobación de conocimientos

1. El departamento de soporte técnico de TI quiere reducir las incidencias de soporte técnico del restablecimiento de contraseña. Sugiere que los usuarios inicien sesión tanto en las aplicaciones locales como en las basadas en la nube utilizando la misma contraseña. Su organización no tiene previsto usar Azure AD Identity Protection; así pues, ¿qué característica sería más fácil de implementar dados estos requisitos?

- ○ Federación
- ◉ Autenticación de paso a través

✔ **Autenticación de paso a través. La autenticación transferida (PTA) permite a los usuarios iniciar sesión en aplicaciones basadas en la nube y en entornos locales con las mismas contraseñas. Con PTA, los usuarios inician sesión mediante la validación de sus contraseñas directamente en la instancia local de Active Directory. PTA no proporciona informes de credenciales filtradas de Azure AD Identity Protection.**

- ○ Sincronización de hash de contraseña

2. ¿Qué herramienta puede usar para sincronizar las contraseñas de Azure AD con Active Directory local?

- ◉ Azure AD Connect

✔ **Azure AD Connect. La sincronización de Azure AD Connect es un componente principal de Azure AD Connect. Se encargan de todas las operaciones relacionadas con la sincronización de datos de identidad entre el entorno local y Azure AD.**

- ○ Servicios de federación de Active Directory

- ○ escritura diferida de contraseñas

3. ¿cuál de los siguientes protocolos de seguridad admite Azure AD?

- ○ Kerberos
- ◉ OAuth

  ✔ **OAuth se usa para la autorización.**
- ○ OpenID Connect

4. ¿Cuál de las siguientes es una opción de autenticación que se integra con Azure Active Directory, lo que requiere que use varios métodos diferentes, como el teléfono, para confirmar su identidad?

- ○ Claves de seguridad FIDO2
- ○ Aplicación Microsoft Authenticator
- ◉ Azure Active Directory Multi-Factor Authentication

  ✔ **Azure Active Directory Multi-Factor Authentication (MFA) es una excelente manera de proteger la organización, pero los usuarios a menudo se frustran con la capa de seguridad adicional además de tener que recordar sus contraseñas. Los métodos de autenticación sin contraseña resultan más cómodos, ya que la contraseña se quita y se reemplaza por algo que se tiene más algo que se es o se sabe. Las otras opciones son las de autenticación sin contraseña que se integran con Azure AD. Azure AD DS permite el uso de cifrados como NTLM v1 y TLS v1.**

Siguiente unidad: Resumen

Continuar >