Módulo 10 Tarea colaborativa

Segundo Factor de Autentificación en Windows AD

Máster en Desarrollo Seguro y DevSecOps

Campus Internacional Ciberseguridad

José María Canto Ortiz

Tabla de contenido

Tabla de ilustraciones

Introducción

Tras el reciente incidente de *ramsonware* padecido por la empresa CompuSec S.L., ya solucionado por nuestros compañeros de respuesta ante incidentes y dentro de la estrategia de mejora de su infraestructura de seguridad, se están realizando algunas recomendaciones que quedan recogidas una serie de documentos, en este que nos ocupa se tratará de explicar como configurar el segundo factor de autentificación para usuarios en windows.

Se incluirán algunos scripts de automatización en PowerShell para la instalación de los servicios necesarios; también crear usuarios de forma automática dentro del dominio y como no activar el 2 factor de autentificación a los usuarios.

Montando la infraestructura

Se va a partir de la idea que existe un servidor Windows Server 2016 o 2022 instalado y no necesariamente con el Directorio Activo instalado e incluso sin la interfaz gráfica, es decir que sea un server core.

Debido a que para poder configurar el segundo factor de autentificación integrado dentro del dominio, hay que hacerlo a través de Azure, se va a comenzar por esa parte.

Desde hace un tiempo, Microsoft ha sustituido *Azure Active Directory* por una evolución que engloba más productos como es *Microsoft Entra*. Azure proporciona dos soluciones para implementar servicios de directorio e identidad:

- Usar *Microsoft Entra ID* para crear un dominio de Directorio Activo en la nube y conectarlo a su dominio local de Directorio Activo. *Microsoft Entra Connect* integra los directorios locales con *Microsoft Entra ID*.
- Ampliar la infraestructura existente del Directorio Activo local a *Azure* mediante la implementación de una máquina virtual en *Azure* que ejecute los Servicios de Dominio de Directorio Activo como un controlador de dominio. Son posibles diversas variantes de esta arquitectura:
    - Crear un dominio en *Azure* y unirlo al bosque del Directorio Activo local.
    - Crear un bosque independiente en *Azure* en el que confíen los dominios del bosque local.
    - Replicar una implementación de Servicios de federación de Directorio Activo (*AD FS*) en Azure.

Se exponen ahora algunas ventajas e inconvenientes de estas distintas posibilidades de cara al despliegue en Azure.

Integración de dominios locales con Microsoft Entra ID

Utilizar *Microsoft Entra ID* para crear un dominio en *Azure* y vincularlo a un dominio de *AD* local. El directorio de *Microsoft Entra* no es una extensión de un directorio local. Por el contrario, es una copia que contiene los mismos objetos e identidades. Los cambios realizados en estos elementos locales se copian en *Microsoft Entra ID*, pero los realizados en *Microsoft Entra ID* no se replican al dominio local.

También se puede usar *Microsoft Entra ID* sin utilizar un directorio local. En este caso, *Microsoft Entra ID* actúa como el origen principal de toda la información de identidad, en lugar de contener los datos replicados desde un directorio local. Entre sus ventajas se encuentra:

- No es necesario mantener una infraestructura de AD en la nube. Microsoft Entra ID es un servicio que administra y mantiene completamente Microsoft.
- Microsoft Entra ID proporciona la misma información de identidad que está disponible en el entorno local.
- La autentificación puede tener lugar en Azure, lo que reduce la necesidad de que las aplicaciones y los usuarios externos se pongan en contacto con el dominio local.

Entre sus inconvenientes podrían indicarse:

- Se debe configurar la conectividad con el dominio local para mantener sincronizado el directorio de *Microsoft Entra*.
- Puede que sea necesario volver a escribir las aplicaciones para permitir la autentificación mediante *Microsoft Entra ID*.
- Si desea autenticar el servicio y las cuentas del equipo, tendrá también que implementar Microsoft Entra Directory Domain Services.

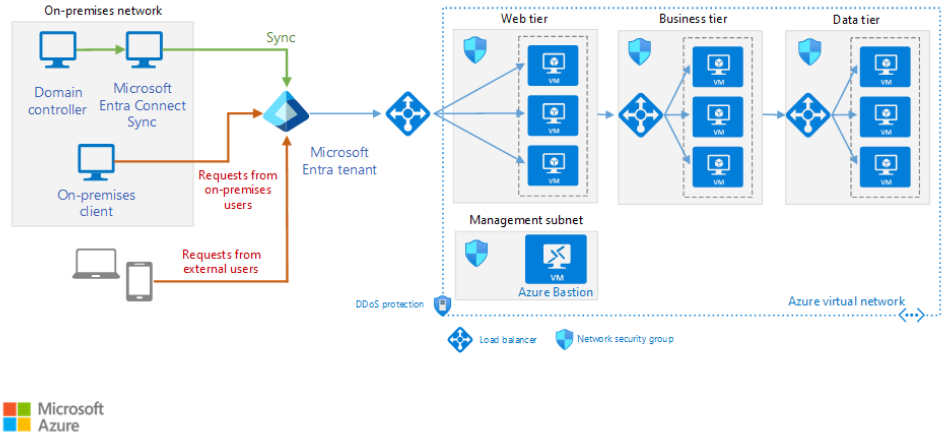

Ilustración 1: Arquitectura de Integración de dominios locales de AD con Microsoft Entra ID

AD DS en Azure unido a un bosque local

Se puede implementar servidores de Servicios de dominio de *Active Directory (AD DS)* en Azure, creando un dominio en *Azure* y uniéndolo al bosque de *AD* local.

Se puede tener en cuenta esta opción si tiene que usar características de *AD DS* que no están implementadas actualmente por *Microsoft Entra ID*. Entre sus ventajas se encuentra:

- Proporciona acceso a la misma información de identidad que está disponible en el entorno local.
- Puede autenticar las cuentas de usuario, servicio y equipo de forma local y en *Azure*.
- No es necesario administrar un bosque de *AD* independiente. El dominio de *Azure* puede pertenecer al bosque local.
- Puede aplicar la directiva de grupo definida por objetos de directiva de grupo local al dominio de *Azure*.

Entre sus inconvenientes podrían indicarse:

- Debe implementar y administrar sus propios servidores y dominios de *AD DS* en la nube.
- Puede haber cierta latencia de sincronización entre los servidores de dominio en la nube y los servidores que se ejecutan en el entorno local.

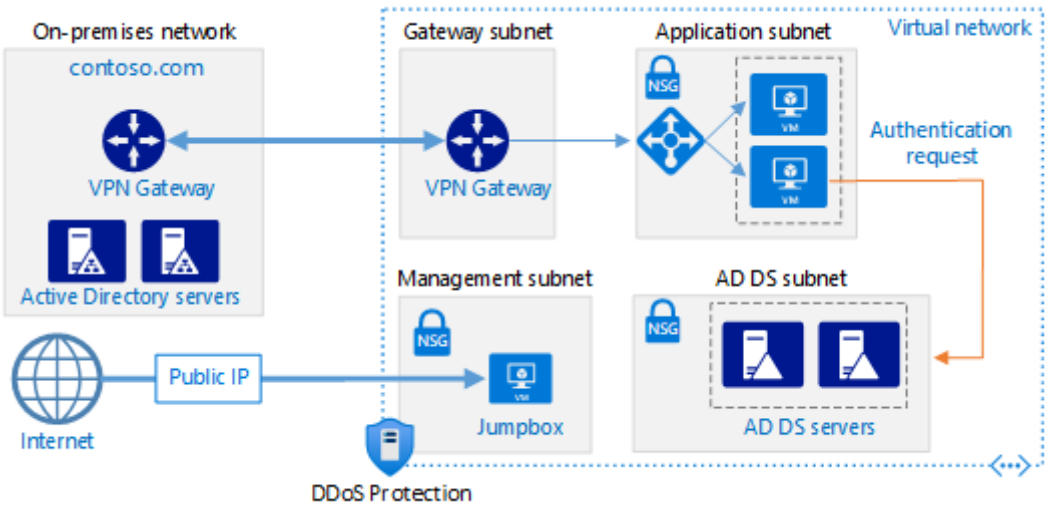

Ilustración 2: Arquitectura de la integración de AD DS en Azure unido a un bosque local

Active Directory Domain Services en Azure con un bosque independiente

Se puede implementar servidores de *AD Domain Services (AD DS)* en *Azure*, pero creando un bosque independiente de *Active Directory* que esté separado del bosque local. Todos los dominios del bosque local confían en este bosque.

Los usos habituales de esta arquitectura incluyen el mantenimiento de la separación de seguridad de objetos e identidades mantenida en la nube y la migración de dominios individuales del entorno local a la nube. Entre sus ventajas se encuentra:

- Se pueden implementar identidades locales y separar las identidades que son solo de *Azure*.
- No es necesario realizar la replicación del bosque local de *AD* a *Azure*.

Desafíos

- La autenticación en *Azure* de las identidades locales requiere saltos de red adicionales a los servidores de *AD* local.
- Se debe implementar servidores y bosques propios de *AD DS* en la nube y establecer las relaciones de confianza adecuadas entre los bosques.

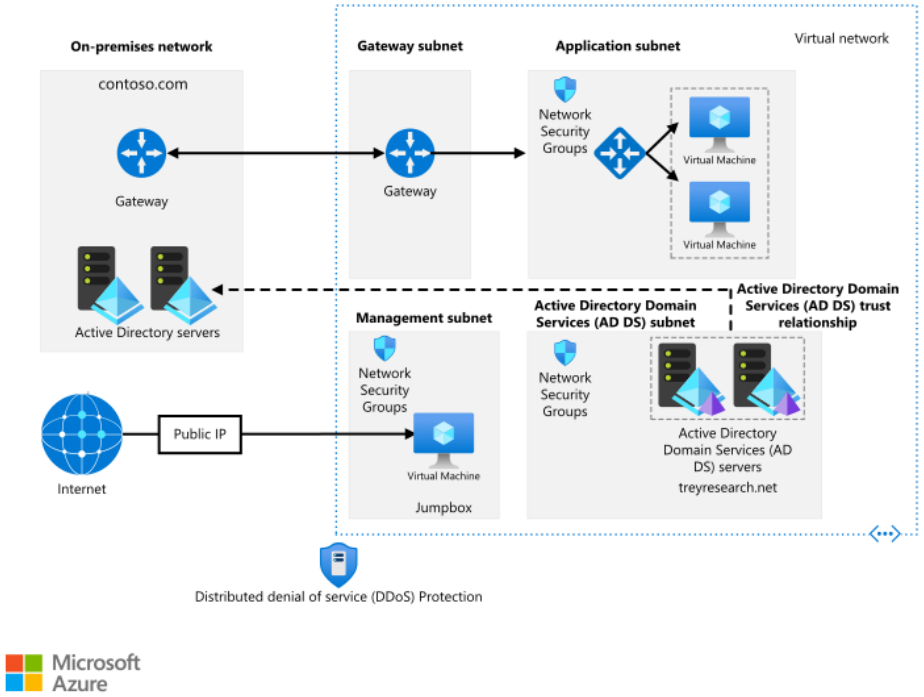

Ilustración 3: Arquitectura de la integración de AD DS en Azure con un bosque independiente

Extensión de AD FS a Azure

Se puede replicar una implementación de Servicios de federación de *Active Directory (AD FS)* a *Azure*, para realizar la autenticación y la autorización federadas de los componentes que se ejecutan en *Azure*.

Usos habituales de esta arquitectura:

- Autentificar y autorizar a los usuarios de organizaciones asociadas.
- Permitir a los usuarios autenticarse en exploradores web que se ejecutan fuera del firewall de la organización.
- Permitir a los usuarios conectarse desde dispositivos externos autorizados, como dispositivos móviles.

Como ventajas se podrían indicar:

- Puede aprovechar las aplicaciones basadas en notificaciones.
- Ofrece la posibilidad de confiar la autentificación a asociados externos.
- Compatibilidad con un gran conjunto de protocolos de autentificación.

Y entre sus inconvenientes:

- se deben implementar sus propios servidores de *AD DS*, *AD FS* y de proxy de aplicación web de *AD FS* en *Azure*.
- Esta arquitectura puede ser difícil de configurar.

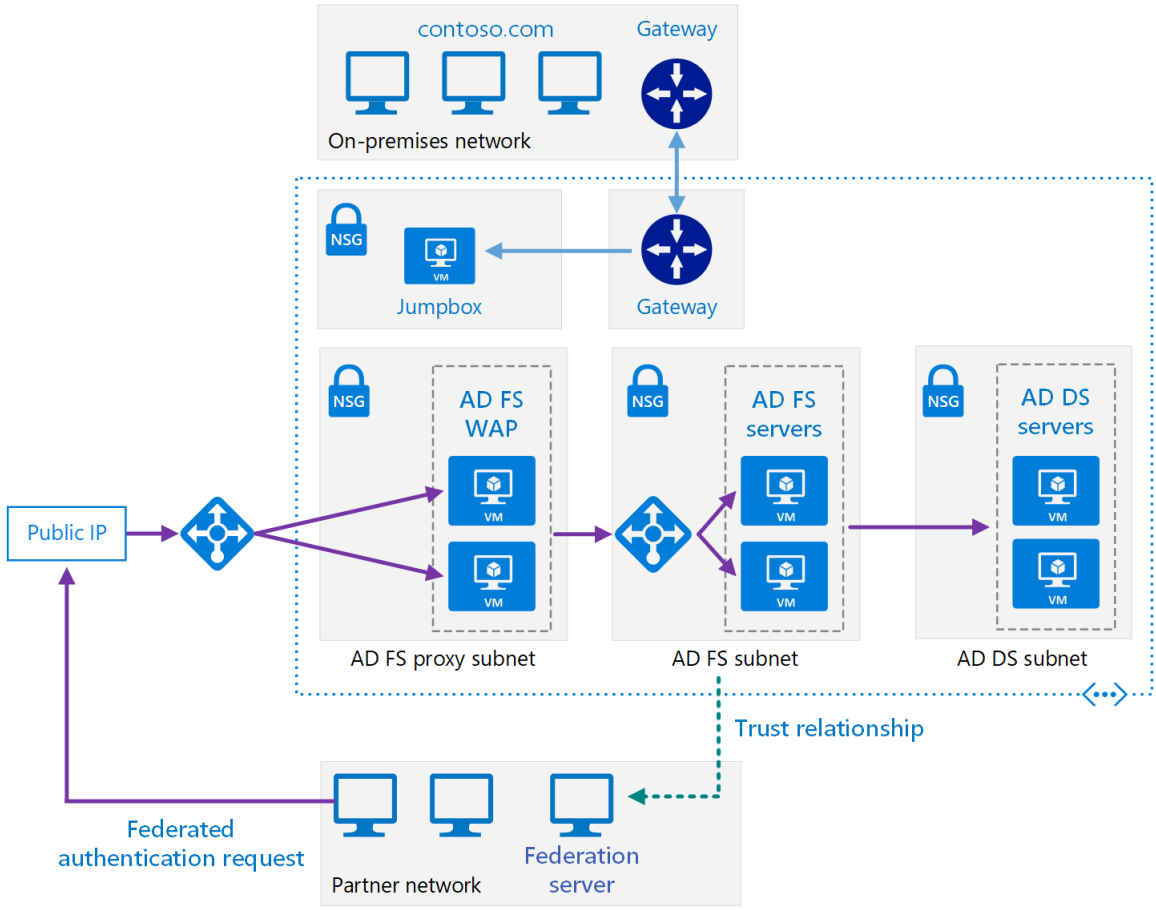

Ilustración 4: Arquitectura implementación replicación AD FS a Azure

Por la estructura actual del cliente, se podría escoger la primera opción, que es la integrar el dominio local con *Entra ID.* El problema con esa selección, sería que hay que tener en cuenta que los cambios se deben aplicar siempre en el dominio local, para que se apliquen en *Azure*, pero si se hace al revés no se aplican al dominio local. Además puede ocurrir que como se está en proceso de crecimiento, esta modalidad se vaya volviendo cada vez más complicada de gestionar.

Debido a estas razones, se considera que la mejor opción sería la replicación de los servicios de federación de Active Directory (*AD FS*) a Azure, aunque es la solución más compleja de configurar.

El cliente tiene un dominio configurado en su red y todo está integrado en el mismo, usuarios equipos, etcétera. Como paso previo a realizar la integración con Azure, con el objetivo siempre de implementar el segundo factor de autentificación, es necesario instalar una serie de roles en el dominio.

Paso 1 Instalar La autoridad de certificación

Para configurar AD FS es necesario indicar un certificado digital, para ello se va a crear uno desde la autoridad de certificación, pero antes es necesario instalar el rol necesario. Para

comenzar la instalación pulsa primero en *agregar roles y características* desde el *Administrador del servidor* y una vez que se está situado en la ventana para para la selección de los roles a instalar seleccionamos: *Servicios de certificados de Active Directory*, al pulsar indicará que se van a instalar una característica necesarias en el rol. Esta característica es *Herramientas de administración de entidades de certificación*.

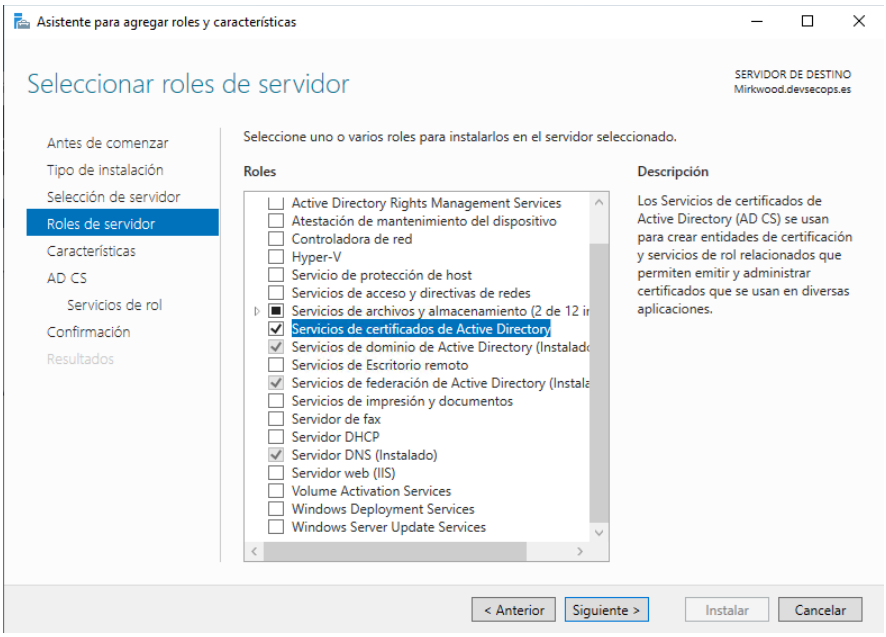

Ilustración 5: Selección del rol para servicios de certificados de AD

Ahora al pulsar en el botón *Siguiente*, se puede comprobar las características que nos indicó antes que se iban a instalar con el rol, *Herramientas de administración de entidades de certificación*.

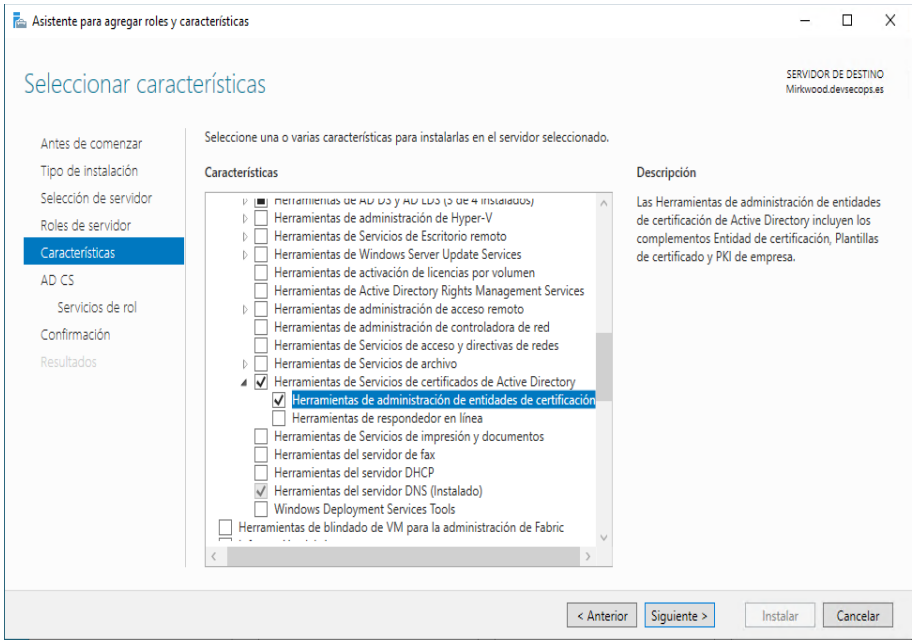

Ilustración 6: Característica agregada con el rol servicios de certificados AD

Tras pulsar de nuevo en el botón *Siguiente*, al avanzar se llega a otra ventana en la que se puede seleccionar los servicios de rol que se deseen instalar, en el caso que nos ocupa sólo se dejará seleccionado *Entidad de certificación*.

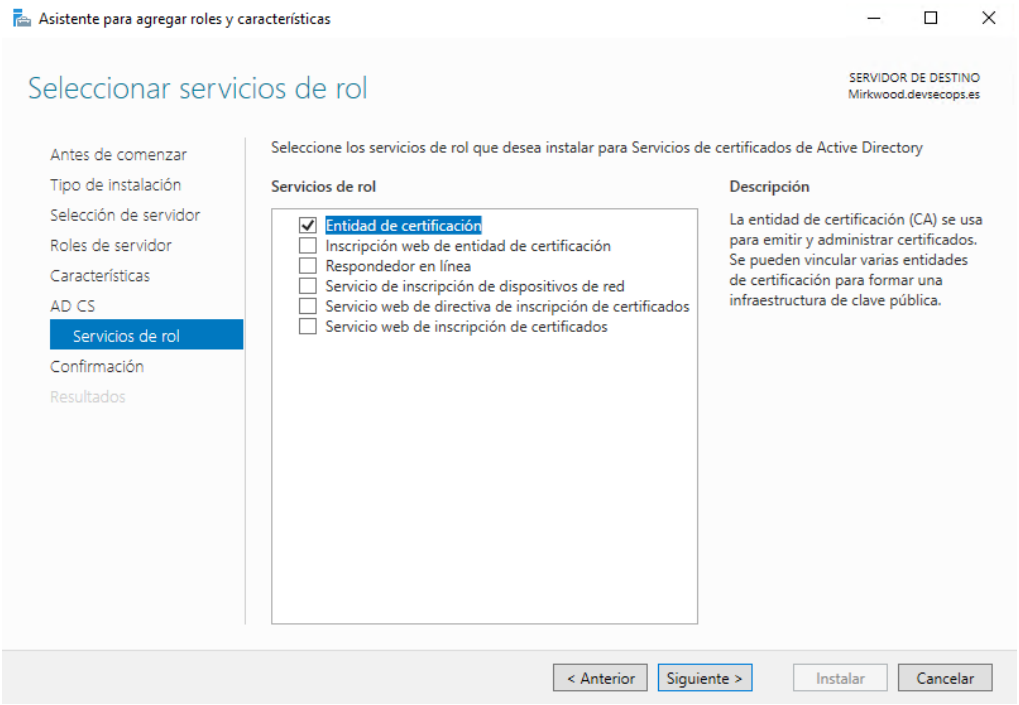

Ilustración 7: Servicios del rol a instalar para Servicios de certificados de Active Directory

De los demás servicios no se selecciona ninguno porque no se necesitan para la emisión del certificado que se desea. Tras pulsar de nuevo en el botón *Siguiente* aparece la ventana de resumen de la instalación y se pulsa en Instalar, comenzando dicho proceso.

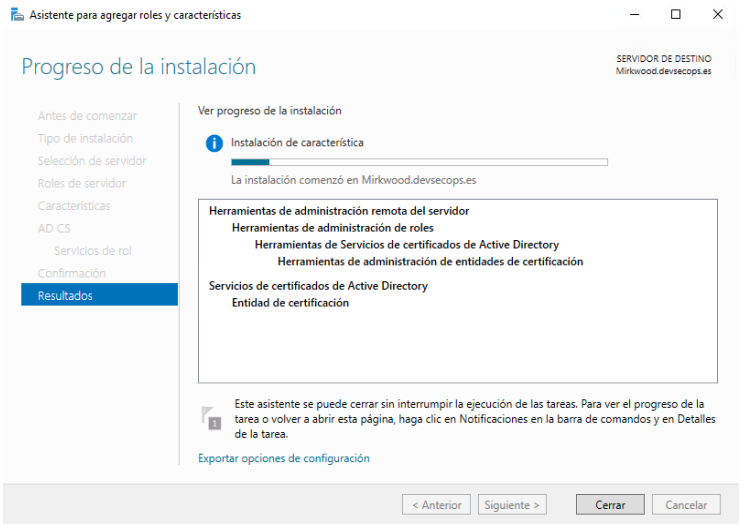

Ilustración 8: Comienzo instalación AD CS

Paso 2 Configurar AD CS

Para configurar los *Servicios de certificados de Active Directory*, desde el *Administrador del servidor*, se puede observar que hay un signo de exclamación la lado del icono de notificaciones o tareas en la parte derecha de la ventana, si se pulsa, se puede observar que está reclamando que se configure el servicio. Pulsando sobre dicha opción, empieza el proceso .

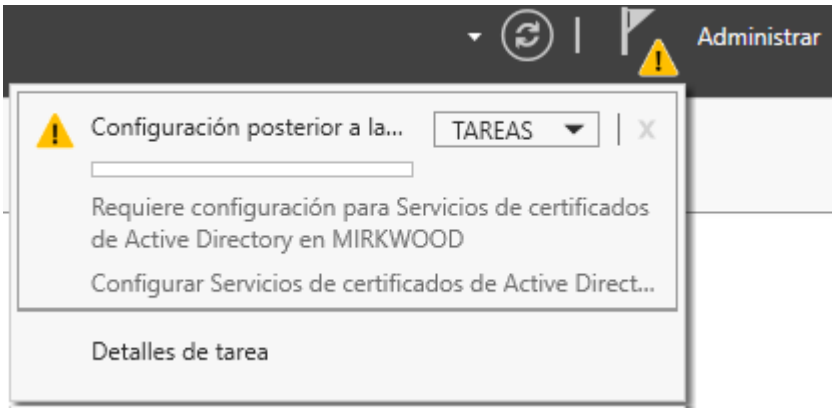

Ilustración 9: Notificación para configurar AD CS

Lo primero que se solicita es que se indiquen las credenciales a utilizar, por defecto aparece el usuario que está validado en el servidor, pero si se quiere utilizar otra, bien porque se haya creado un usuario específico para ese servicio o alguna otra razón, pulsando el botón *Cambiar...* se puede indicar otro usuario.

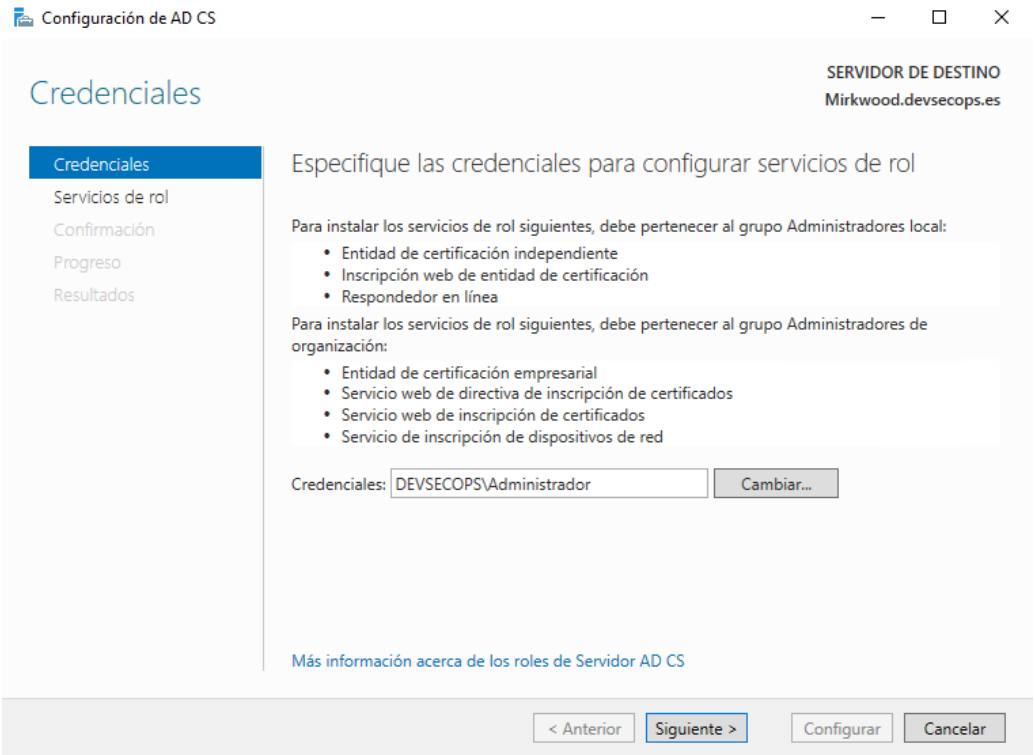

Ilustración 10: Indicar credenciales para configurar servicios de rol de AD CS

En la siguiente ventana se seleccionan los servicios de rol que se van a configurar, que como solo se ha instalado Entidad de certificación, se marca y se pulsa en el botón Siguiente.

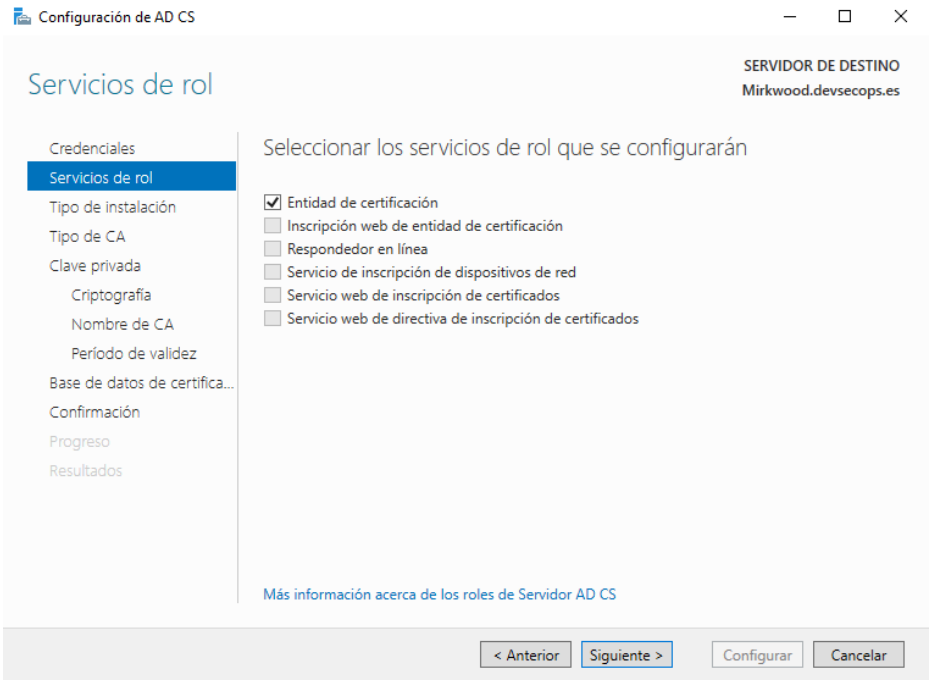

Ilustración 11: Roles de servidor AD CS a configurar

Las siguientes opciones, referentes a las entidades de certificación, se dejan tal y como aparecen indicadas por defecto. Llegando a la ventana de clave privada, aquí se pregunta si se desea crear una clave privada o usar una ya existente, en este caso, como no hay ninguna anterior, se deja la opción de crear una clave privada nueva.

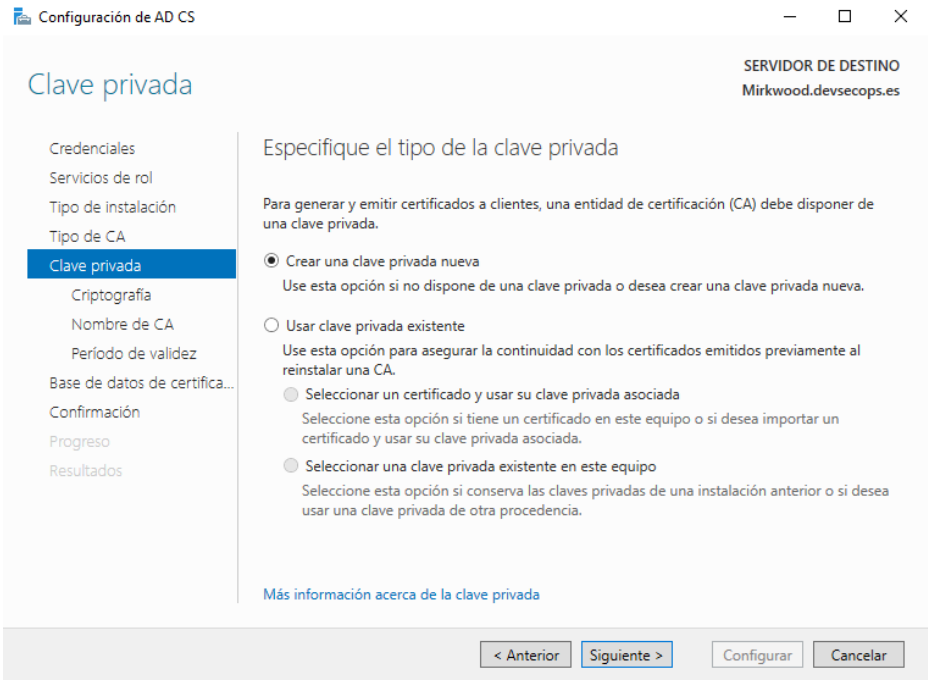

Ilustración 12: Tipo de clave privada en la configuración de AD CS

Seguidamente, se selecciona la entidad de certificación y el algoritmo hash a utilizar, en este caso, en lugar de dejar SHA256, se ha seleccionado SHA512, para que genere un hash un poco más grande, en vez de 32 bytes de 64 bytes.

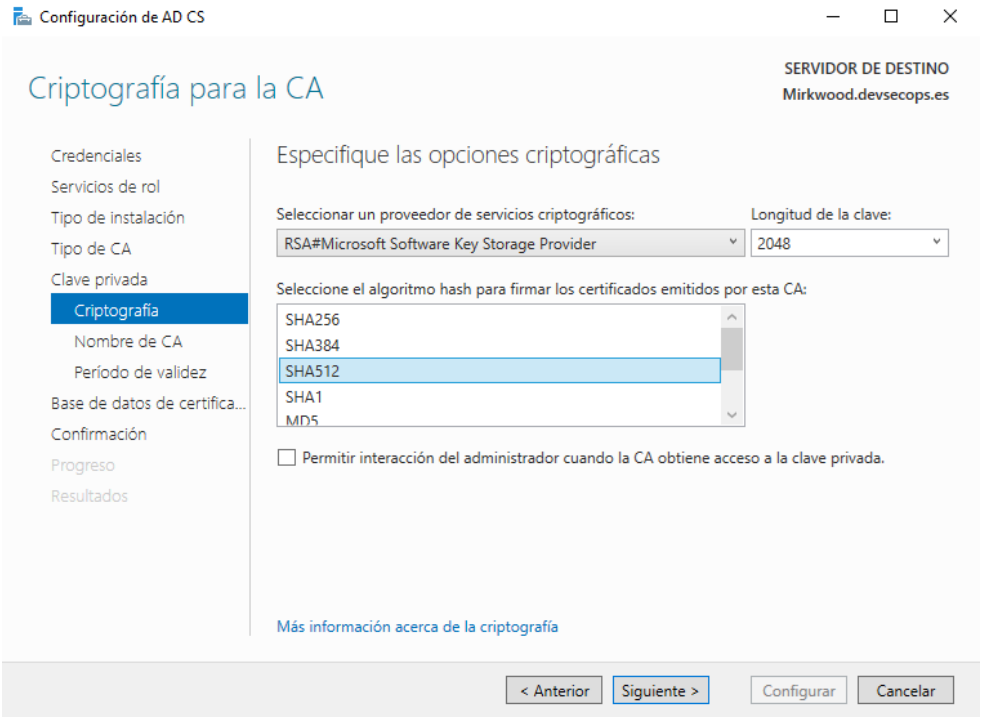

Ilustración 13: Elección algoritmo hash para la entidad de certificación

Tras indicar esta información, se solicita indicar un nombre para la entidad de certificación, que se puede cambiar.

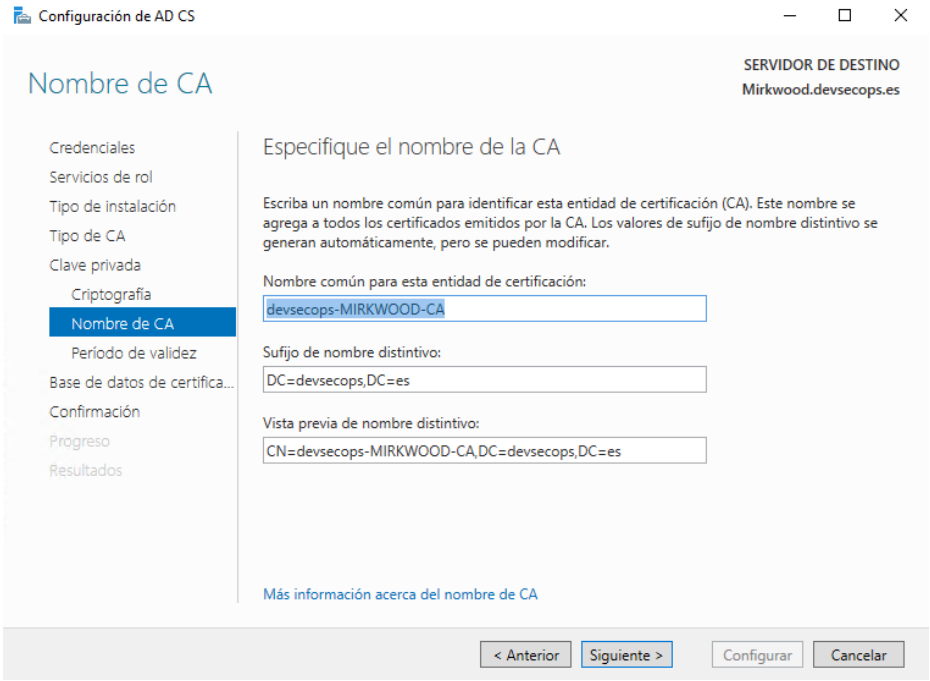

Ilustración 14: Nombre de la entidad de certificación

Posteriormente, se pide que se indique el periodo en el que será válido el certificado emitido por la entidad de certificación, se deja por defecto en 5 años pero se podría ampliar o reducir.

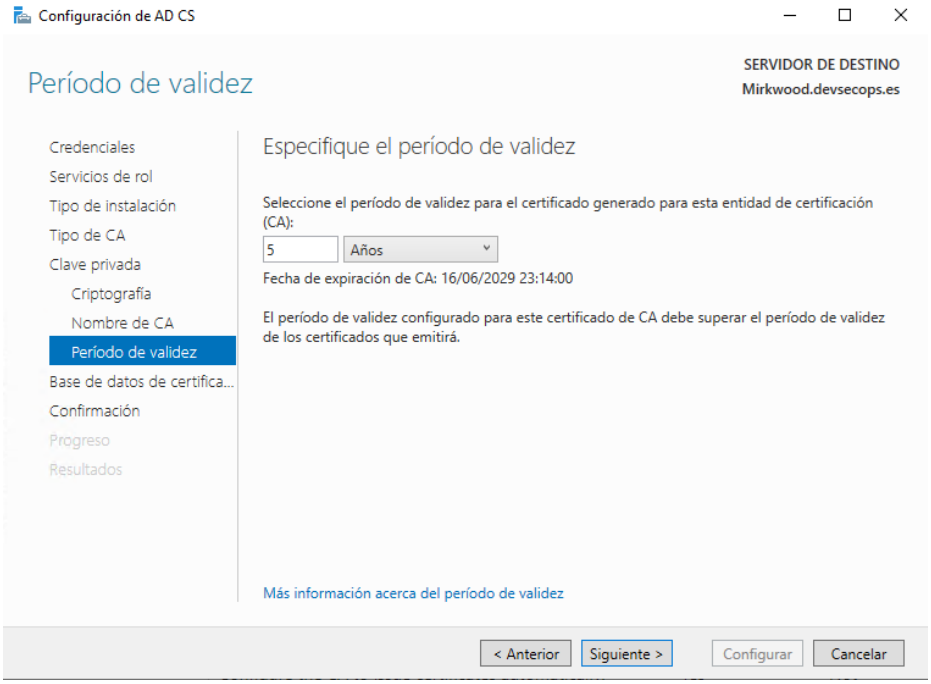

Ilustración 15: Periodo validez certificado

Por último se pide confirmar o cambiar la ruta donde se ubicará la base de datos de certificados y se muestra un resumen con los valores indicados.

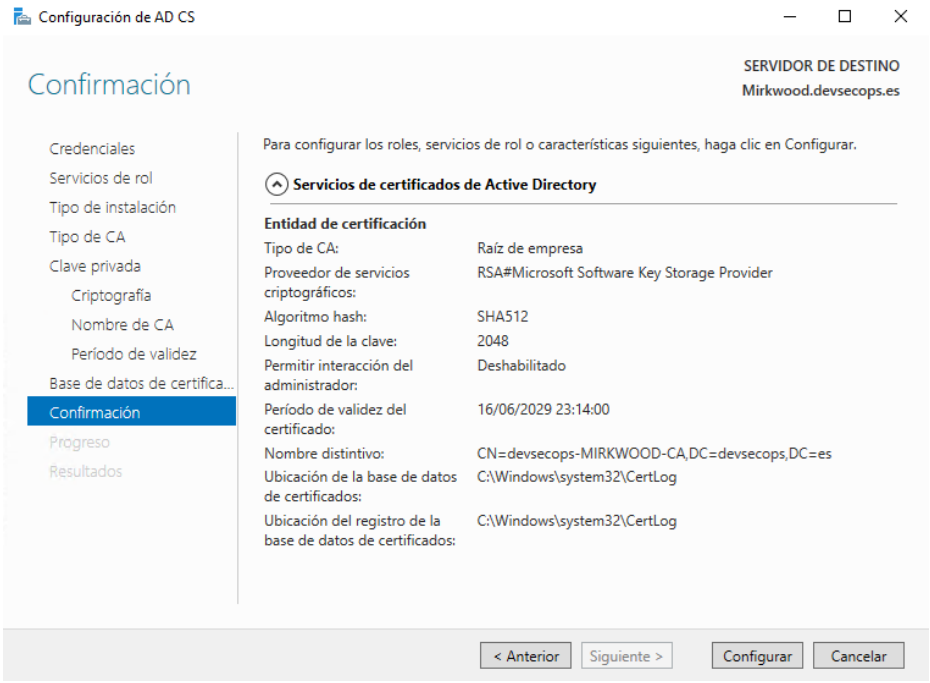

Ilustración 16: Resumen configuración AD CS

Paso 3 Crear certificado

Para comenzar con el proceso, se puede acceder a la *Entidad de Certificación* desde el *Administrador del servidor* o se puede situar en *herramientas administrativas de Windows* y acceder a dicha herramienta.

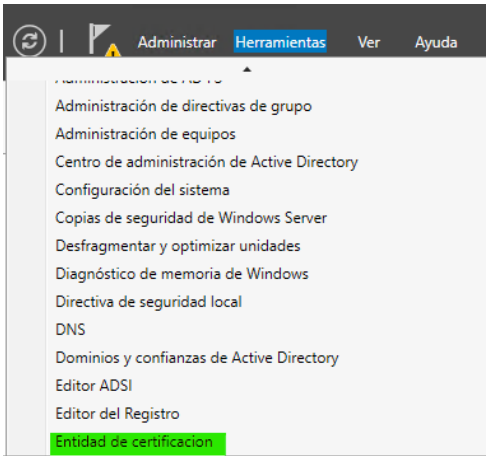

Ilustración 17: Accediendo Entidad de certificación

Una vez dentro de la entidad de certificación, se debe crear una plantilla de certificado, para ello, hay que desplegar el nombre de la entidad de certificación, en este caso, *devsecops-MIRKWOOD-CA*, y pulsar con el botón derecho del ratón sobre *Plantillas de certificado*, en el menú que aparece, pulsar en *Administrar*.

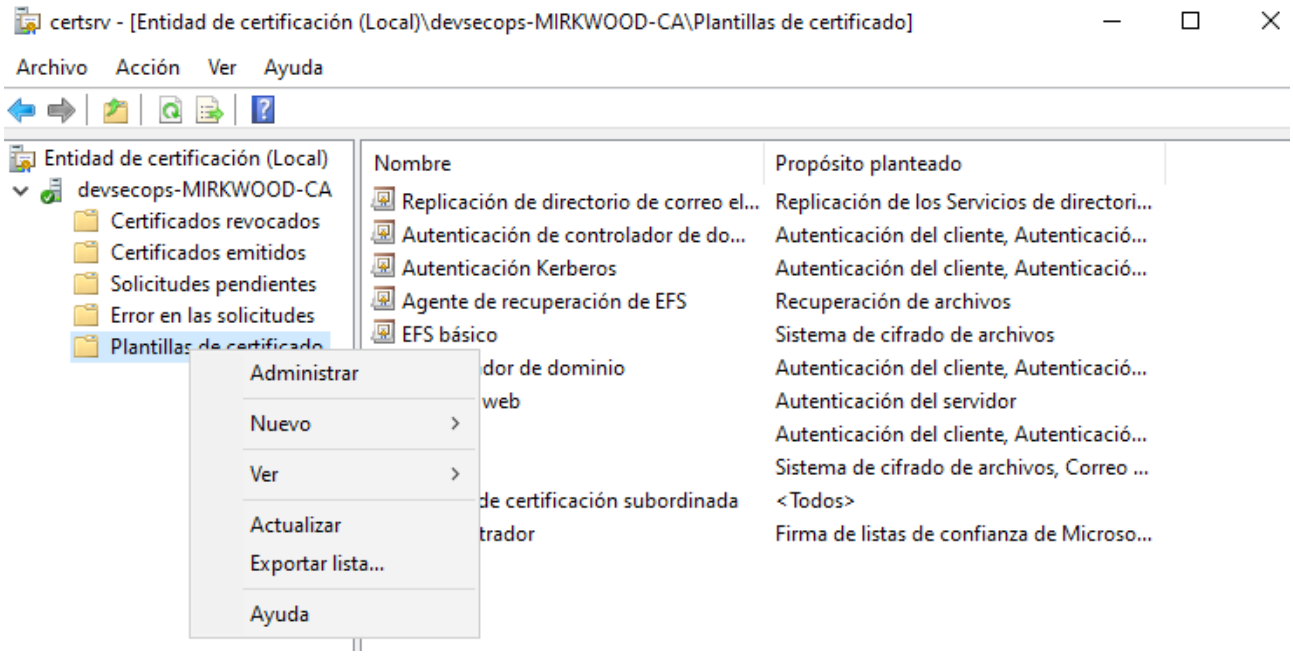

Ilustración 18: Entidad de Certificación

Esta acción abre otra herramienta, la *consola de plantillas de certificado.* Aquí se busca la plantilla *servidor web* y se pulsa con el botón de derecho del ratón sobre ella; en el menú que aparece se debe seleccionar *Plantilla duplicada.*

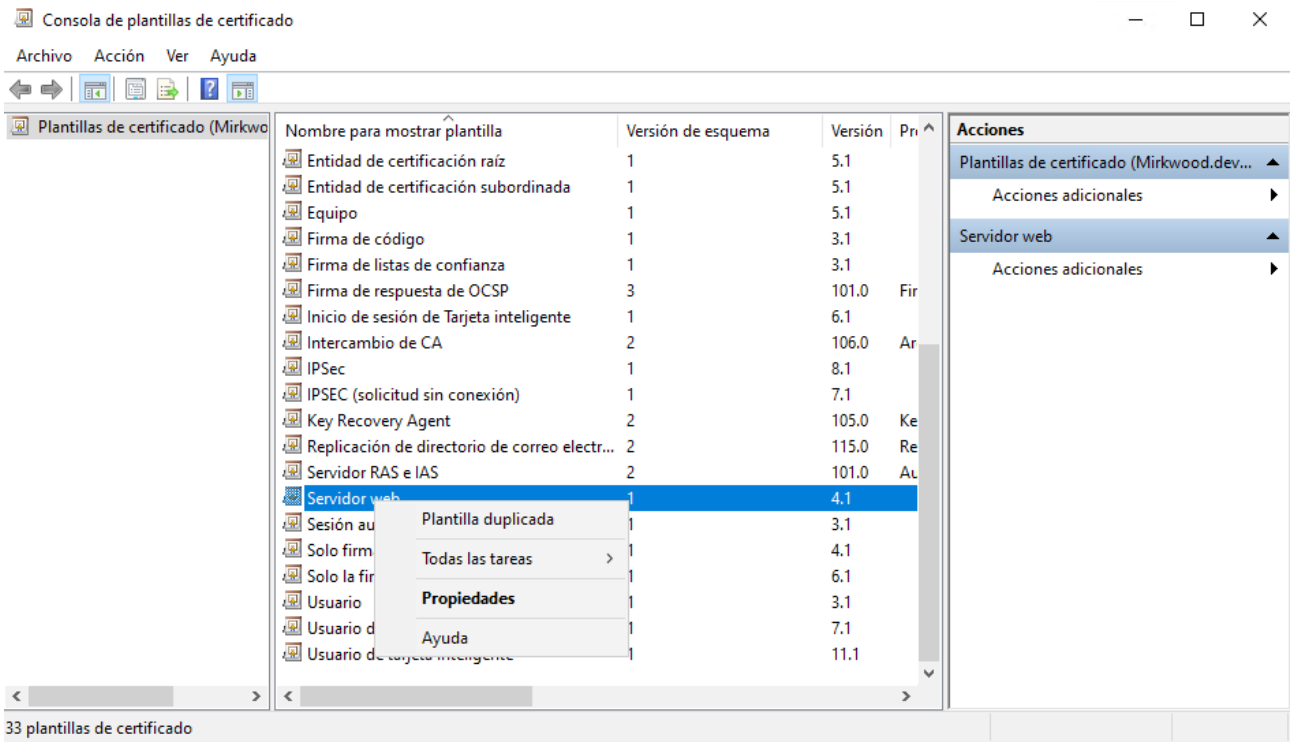

Ilustración 19: Consola de plantillas de certificado duplicación de certificado

Ahora si se desea, se le puede cambiar el nombre a esta plantilla duplicada, desde la pestaña *General* de la misma se indica el nombre que se quiera, recomendable que sea algo descriptivo y se pulsa el botón de *Aplicar*. También en la pestaña de *nombre del sujeto* se comprueba que está marcado la opción "*Proporcionado por el solicitante*". Seguidamente se selecciona la pestaña *Tratamiento de la solicitud* y se marca la casilla "Permitir que la clave privada se pueda exportar". Esto es **importante** porque si hay más servidores de federación, se necesitara este certificado, que se exportará desde el primer servidor *AD FS* y se importará en el resto. Por último se necesita dar permiso al servidor para inscribirse en el certificado, para ello hay que situarse en la pestaña seguridad y agregar el servidor y asegurarse que tiene los permisos de lectura y inscribirse. Si hubiera más servidores de federación, se deben agregar aquí también.

La creación de una plantilla de certificado, al igual que las plantillas de directivas, y otras muchas, permite que cuando se necesite crear un nuevo certificado de las mismas características se utilice y todos esos certificados creados partiendo de la misma plantilla, tendrán las mismas características de entrada, luego quizás, habrá parámetros que se les tengan que modificar.

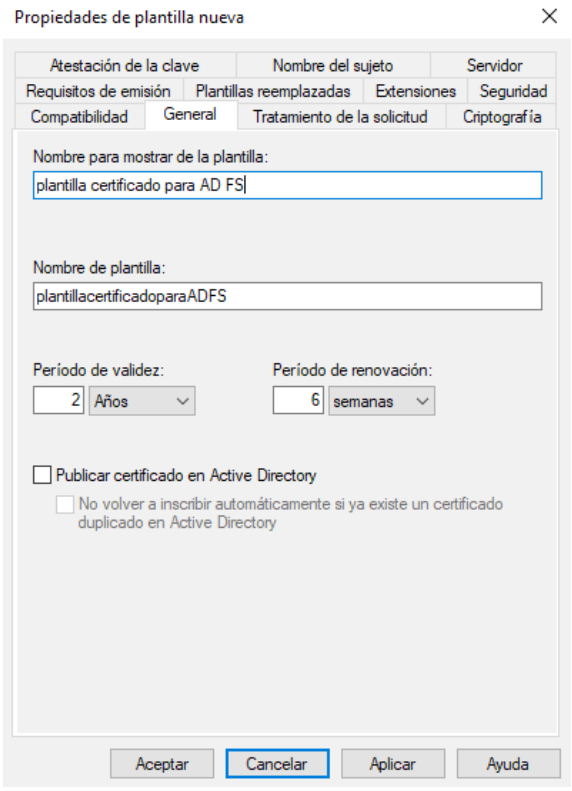

Ilustración 20: Nombre de la plantilla de certificado

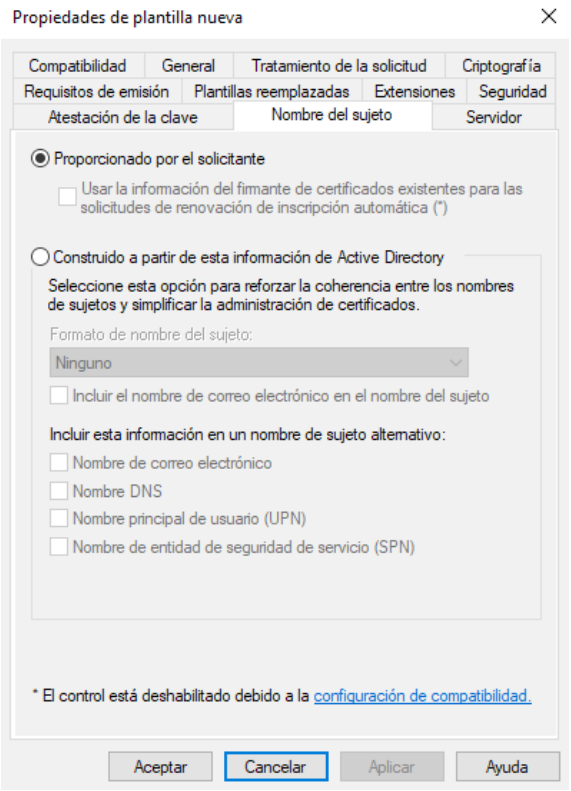

Ilustración 21: nombre del sujeto de la plantilla de certificado

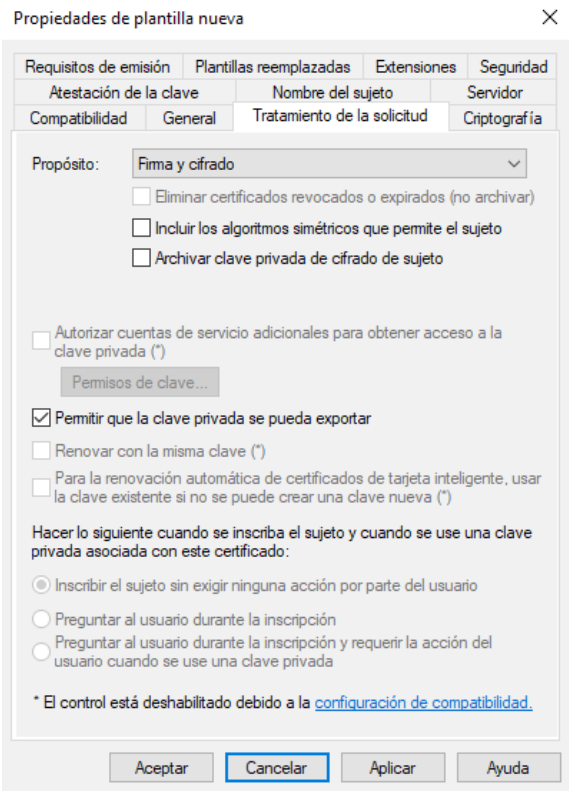

Ilustración 22: Exportación clave privada en la plantilla de certificado

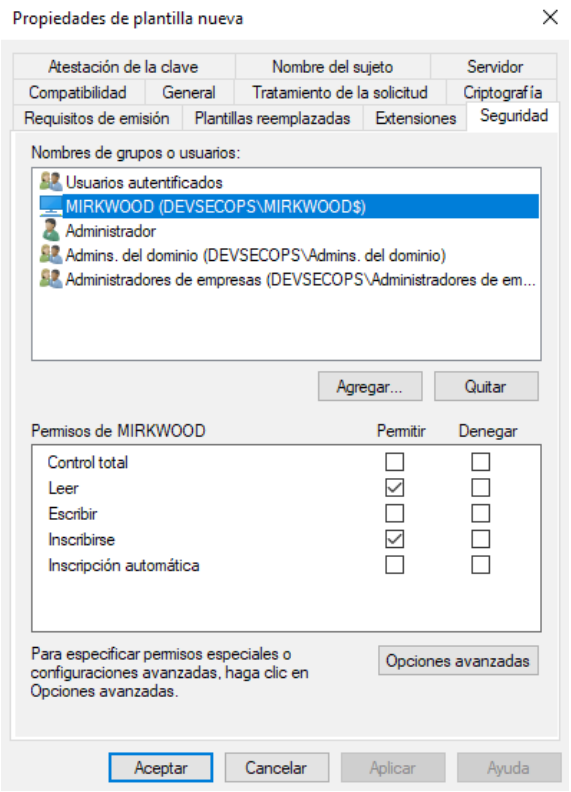

Ilustración 23: Seguridad de la plantilla de certificado

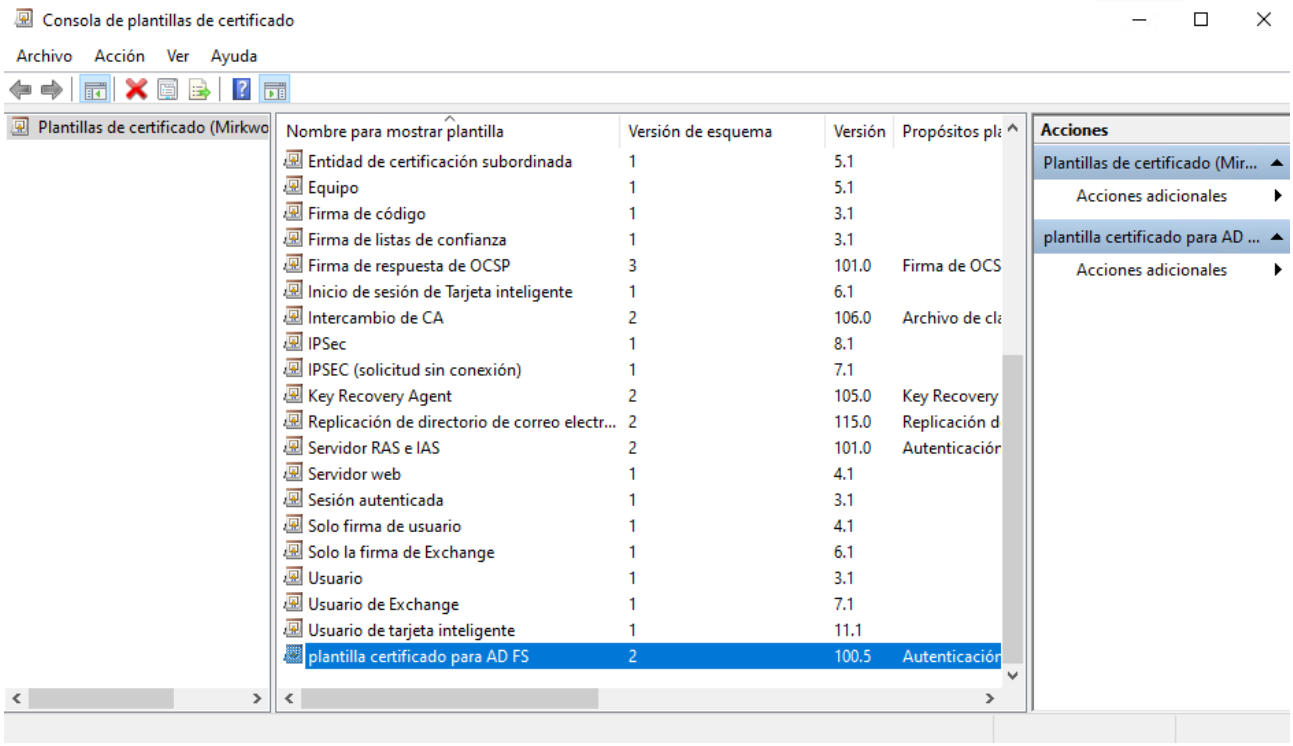

Ilustración 24: Plantilla creada para AD FS en la consola de plantillas de certificado

Con la plantilla ya creada, se cierra la ***consola de plantillas de certificados*** y se vuelve a la **Entidad de certificación**. Ahora en las *plantillas de certificado*, se pulsa en nuevo y se selecciona *"Plantilla de certificado que se va a emitir"*.

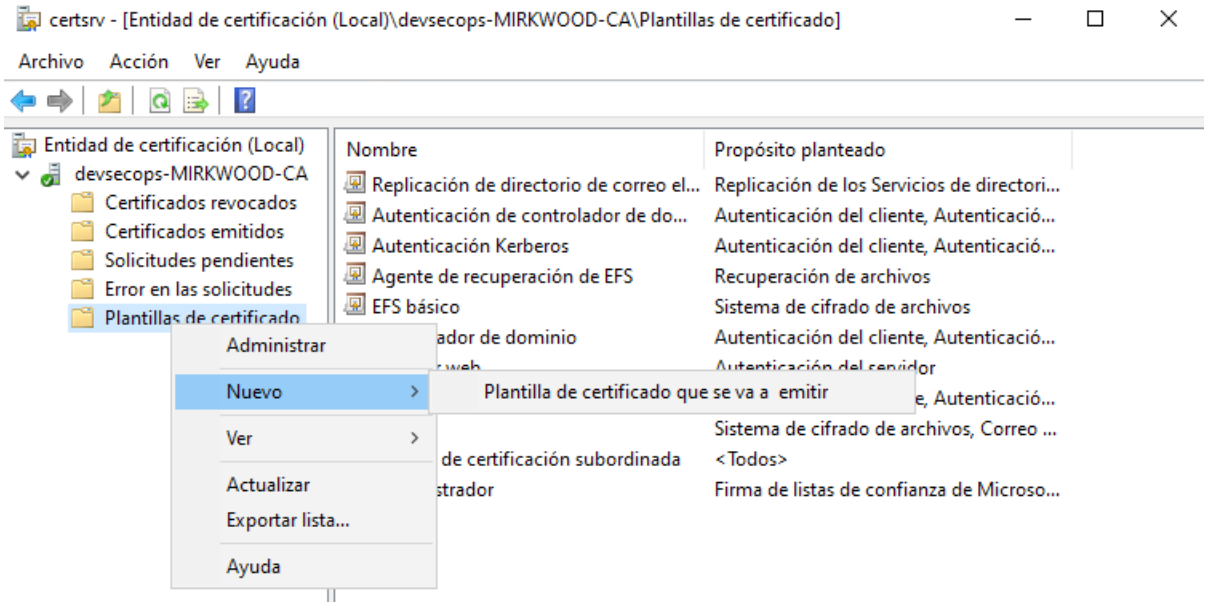

Ilustración 25: Plantilla de certificado a emitir

Y se selecciona la plantilla creada antes, así ya aparecerá en el apartado de Plantillas de certificado de la Entidad de certificación.

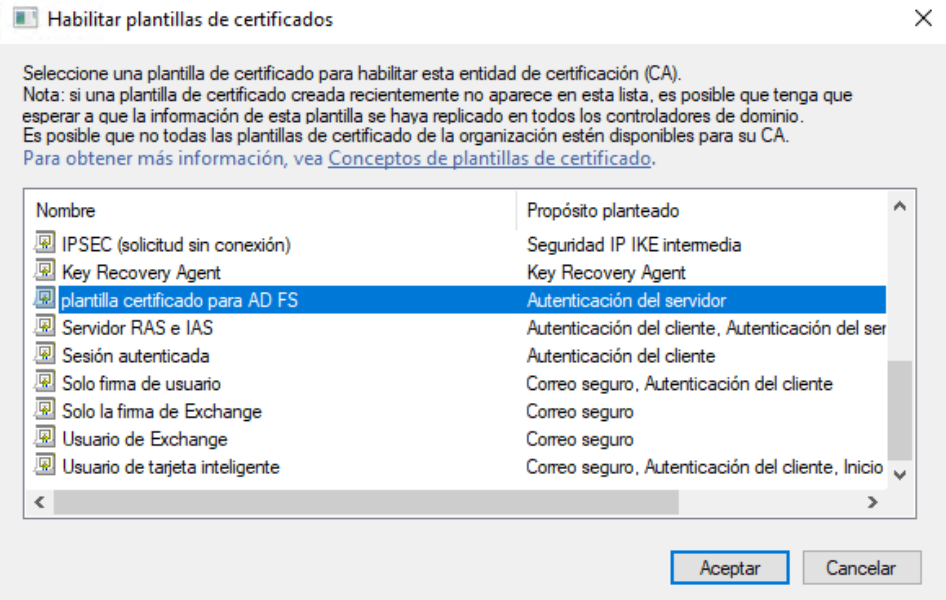

Ilustración 26: Habilitar plantilla de certificado para AD FS

Con esto hecho, se pasaría a crear el certificado propiamente dicho. Para crearlo, se abren los certificados por ejemplo desde la consola de administración MMC, se despliega el apartado certificados y en Personal > Certificados se pulsa en *Solicitar nuevo certificado…* comenzando un asistente para su creación.

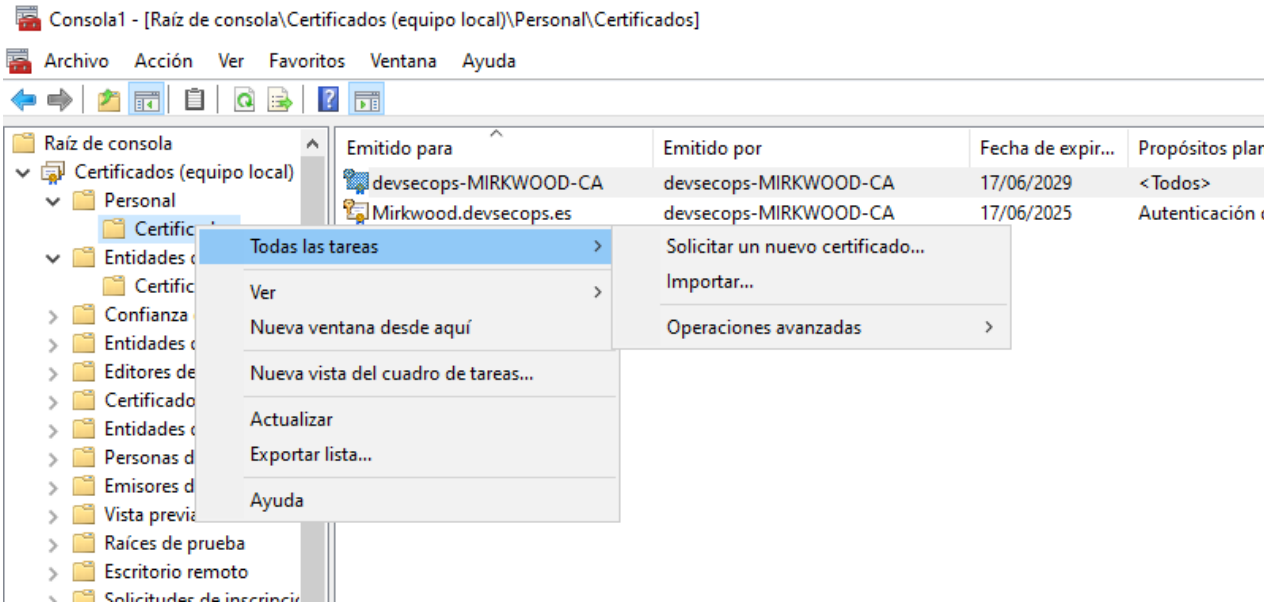

Ilustración 27: Creando nuevo certificado

En dicho asistente se llega al siguiente apartado donde se debe seleccionar la directiva de inscripción, como puede observarse aparece la plantilla anteriormente creada, se debe marcar. Es importante pulsar sobre el enlace que aparece debajo en el que se indica *"Se necesita más información para inscribir este certificado. Haga clic aquí para configurar los valores".*

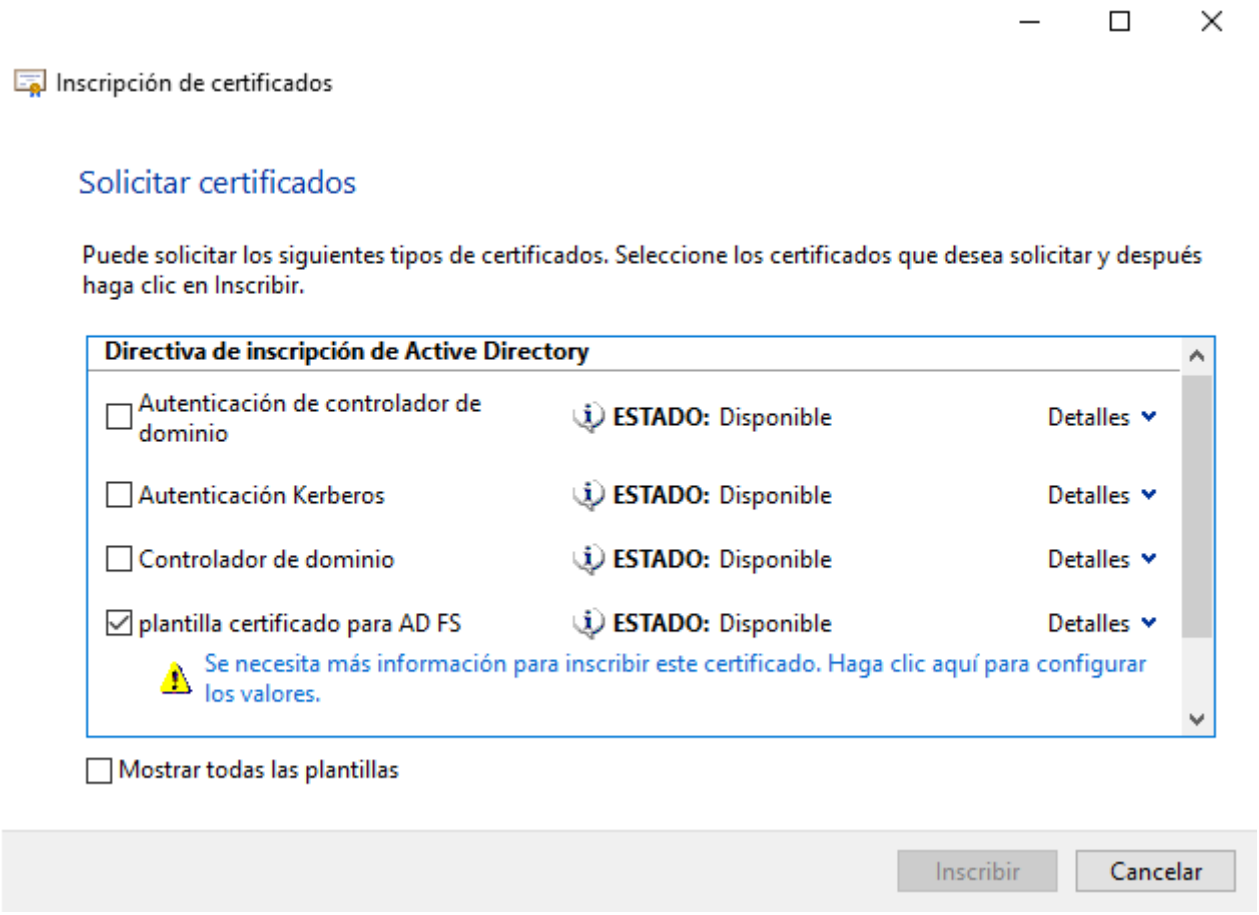

Ilustración 28: Selección de la plantilla AD FS creada en la solicitud de nuevo certificado

Al pulsar en ese enlace aparecen las propiedades del certificado, como se puede observar, aparecen en la pestaña Sujeto, de nuevo el símbolo de exclamación. Aquí debemos indicarle el nombre y un nombre alternativo. Se selecciona primero en tipo *nombre común* y se introduce el nombre del servicio *AD FS* que desee en el campo Valor y haga clic en *Agregar*. Para el nombre alternativo, se va a seleccionar *DNS* en el tipo y en valor se indica el mismo nombre que se ha indicado antes. El nombre alternativo no es necesario, pero por precaución se a añadido.

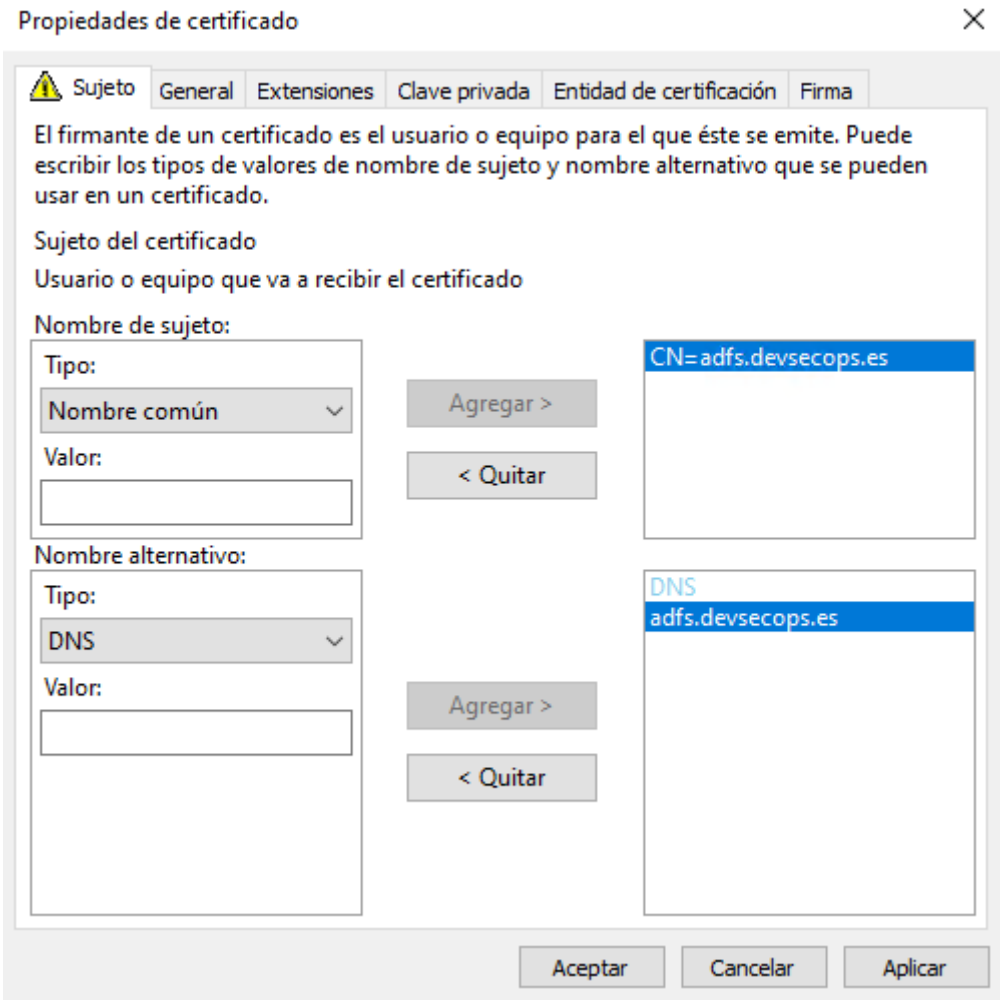

Ilustración 29: Propiedades del nuevo certificado

Con esto quedaría solventado la solicitud de más información que indicaba en la ventana anterior. Se debe acceder a la pestaña *Clave privada* para asegurarse que la clave privada es exportable.

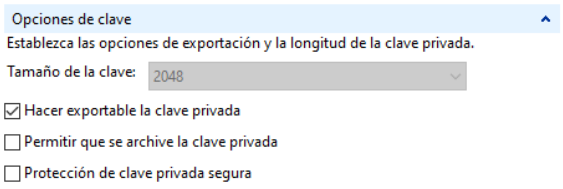

Ilustración 30: Habilitada la exportación de la clave privada

Ahora solo falta pulsar en el botón *Inscribir* y ya quedará creado el certificado y aparece en la relación de los mismos.

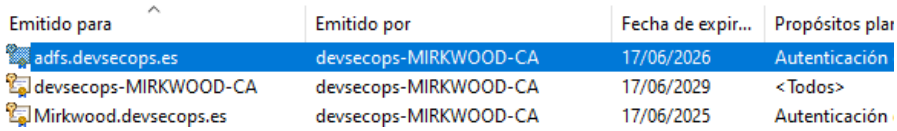

Ilustración 31: Certificados creados

Ahora se podría exportar dicho certificado, si se desea configurar más de un servidor de federación o si el servidor de federación es distinto del servidor con el rol de *Servicios de certificados.* Para ello se pulsaría con el botón derecho del ratón sobre el certificado y se selecciona *Todas las tareas* > *Exportar.*

Paso 4 Instalar AD FS en local

El cliente tiene un dominio configurado en su red y todo está integrado en el, usuarios equipos, etcétera. Como paso previo a realizar la integración con Azure, con el objetivo siempre de implementar el segundo factor de autentificación, se va a instalar *AD FS* en el dominio. AD FS habilita la identidad federada y la administración del acceso mediante el uso compartido seguro de identidades digitales en los límites empresariales y de seguridad. Además, amplía la capacidad de usar la funcionalidad de **inicio de sesión único** que está disponible dentro de un único límite de seguridad o empresarial a las aplicaciones accesibles desde Internet para permitir a clientes, asociados y proveedores una experiencia de usuario simplificada al acceder a las aplicaciones basadas en web de una organización.

En principio se va a instalar *AD FS* en el controlador de dominio principal. Para ello, se pulsa primero en *agregar roles y características* desde el *Administrador del servidor* y una vez que se está situado en la ventana para para la selección de los roles a instalar se selecciona: *Servicios de federación de Active Directory*, tras lo cual se pulsa el botón siguiente y se pasa a la ventana de selección de las características a instalar, de las que no se marca ninguna.

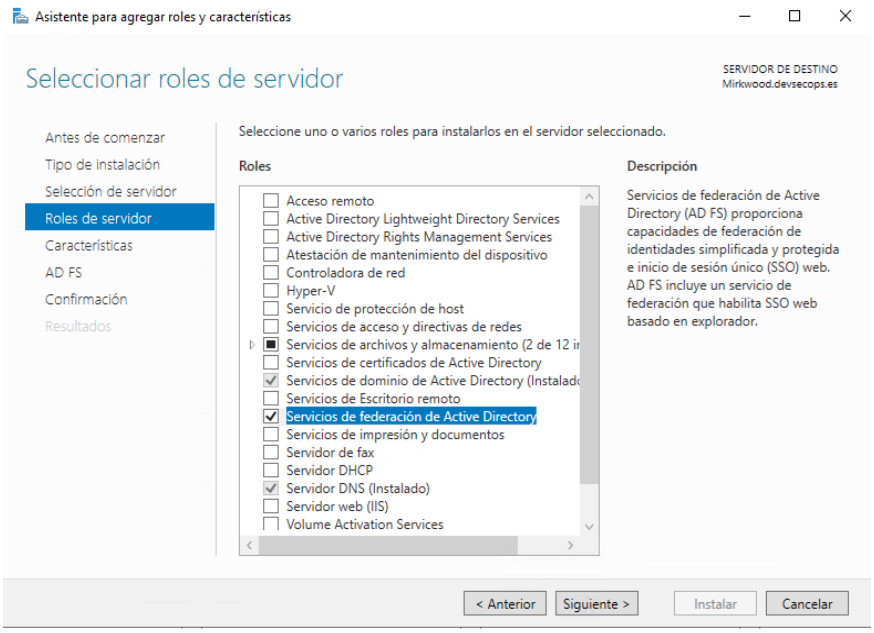

Ilustración 32: Selección del rol para AD FS

Avanzando por las siguientes ventanas se llega a la de confirmación de la instalación de estos servicios y se pulsa el botón de instalar, comenzando la instalación propiamente dicha.

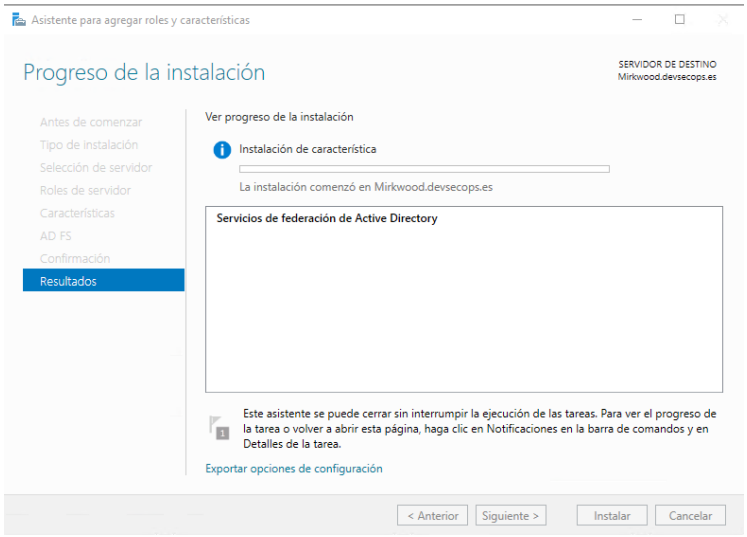

Ilustración 33: Comienzo instalación de AD FS

Terminado el proceso de instalación y aunque no es necesario, se reinicia el servidor.

Paso 5 configurar AD FS

Al arrancar de nuevo el servidor tras el reinicio anterior, para configurar los *Servicios de federación de Active Directory*, desde el *Administrador del servidor*, se puede observar que hay un signo de exclamación la lado del icono de notificaciones o tareas en la parte derecha de la ventana, si se pulsa, se puede observar que está reclamando que se configure el servicio. Pulsando sobre dicha opción, empieza el proceso.

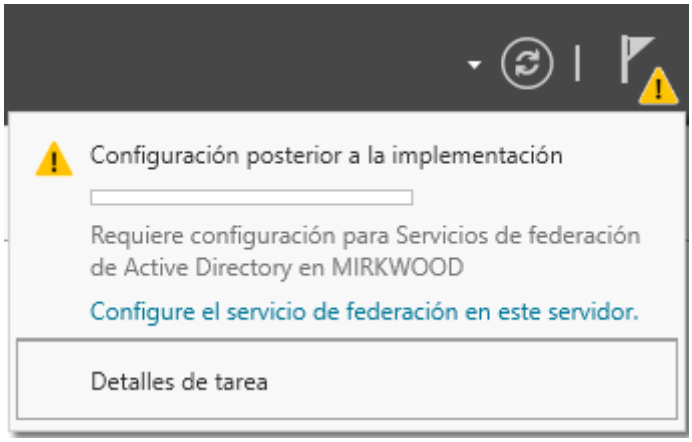

Ilustración 34: Notificación para configurar AD FS

Al iniciar este nuevo asistente, lo primero que solicita es si se desea crear el primer servidor de una granja de servidores de federación, que es la opción que se dejará puesto que no existe aún dicha granja. La segunda opción se escogería en el caso que ya haya otros servidores de federación integrados en una granja y se desee agregar uno más, a continuación se pulsa en el botón *Siguiente*.

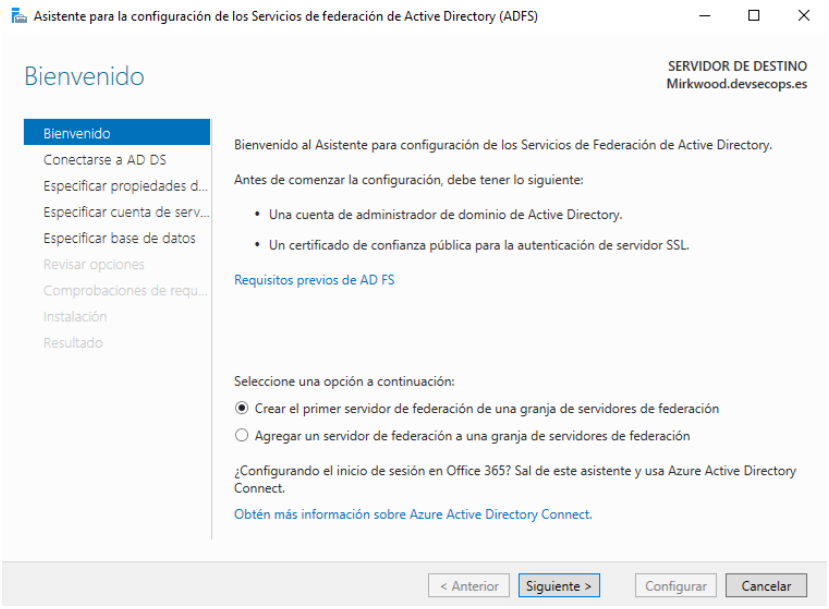

Ilustración 35: Creación del primer servidor de federación

A continuación se solicita un usuario con permisos de administrador en Active Directory, por defecto se asigna el usuario con el que se haya iniciado sesión, pero se puede cambiar por otro. Cambiado o no, seguidamente se pulsa el botón *Siguiente* para continuar con la configuración.

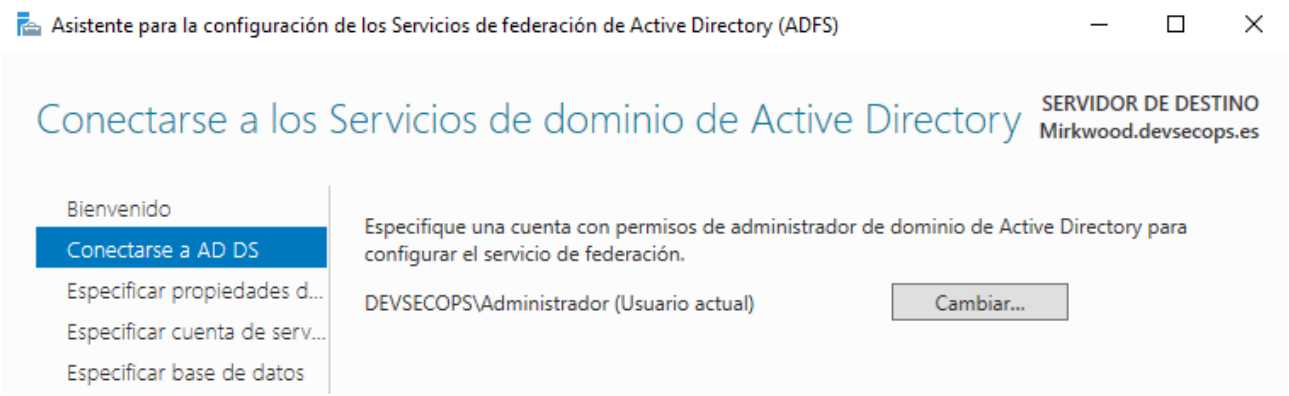

Ilustración 36: Solicitud de cuenta con permisos de administración

En el siguiente apartado, se debe seleccionar el certificado a utilizar, que es el que se ha creado en el Paso 3 Crear certificado, el nombre del servicio de federación y el nombre que se va a mostrar cuando los usuarios inicien sesión. Indicado estos datos se pulsa de nuevo en el botón *Siguiente*.

Ilustración 37: Propiedades del servicio AD FS

A continuación, se solicita que se indique una cuenta de servicio. Hay dos opciones, crear una cuenta de servicio administrada de grupo o indicar una cuenta de usuario del dominio o una de servicio ya existente. Indicado este dato se pulsa de nuevo el botón Siguiente.

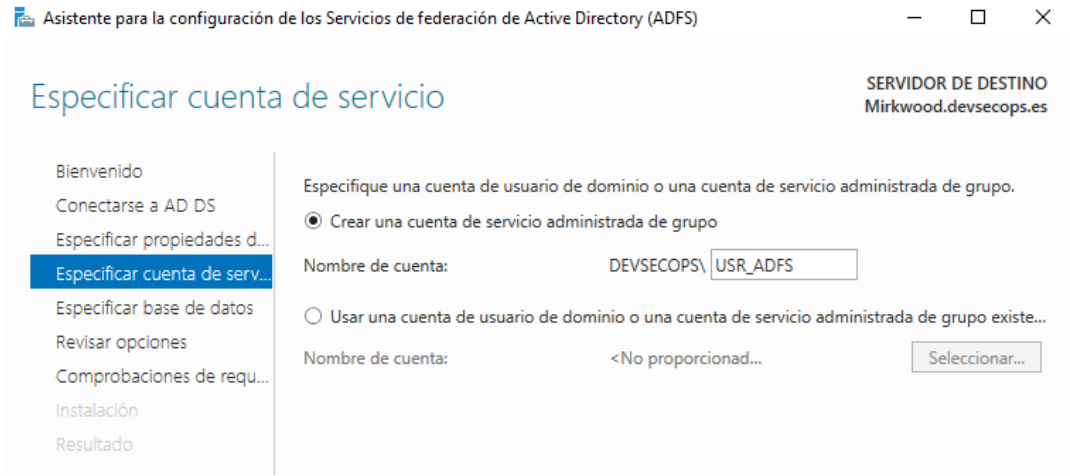

Ilustración 38: Indicar la cuenta de servicio para AD FS

Por último, antes de realizar la configuración en sí misma, se solicita que se indique la base de datos a utilizar para guardar la configuración de *AD FS*. Si dentro de la infraestructura se posee algún servidor *SQL Server*, se podría indicar para usarlo o por el contrario, crear una base de datos interna. En este caso, como no se ha instalado ningún *SQL Server* se selecciona la opción de la base de datos interna. Para continuar como siempre se pulsa el botón de *Siguiente*.

Ilustración 39: Indicar la Base de datos para guardar datos de AD FS

Tras esto, aparecen en forma de resumen las opciones indicadas y posteriormente se realiza la comprobación de requisitos y se indica que ya se puede configurar AD FS pulsando el botón Configurar.

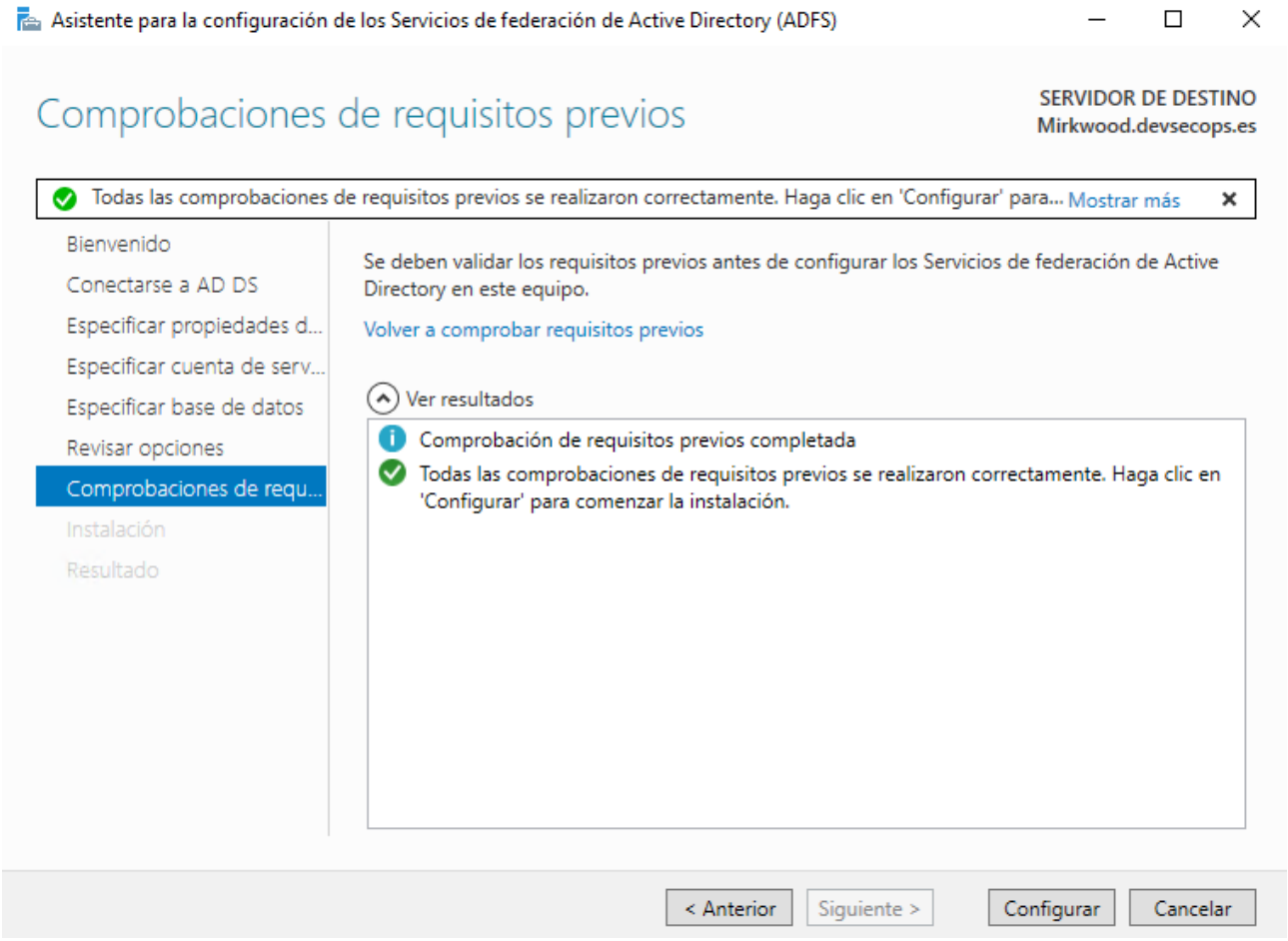

Ilustración 40: Últimas comprobaciones antes de configurar AD FS

El proceso comienza y al terminar se reinicia forzosamente el servidor.

Paso opcional habilitar la página de inicio de sesión

Esto no tendría nada que ver con lo que se está configurando, se incluye como curiosidad, con el siguiente comando de PowerShell, se habilitaría dicha página de inicio.

```
PS C:\Users\Administrador> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
```

Esto permitiría iniciar sesión en el dominio desde un navegador.

Paso 6 Instalación y configuración Microsoft Entra Connect

Antes de proceder a su instalación, es importante realizar una serie de pasos en el portal de Azure. Una vez que se haya dado de alta y se tenga un inquilino o tenant, hay que crear una cuenta de **administrador de identidades híbridas**. Esta cuenta se usa para crear la cuenta del conector de *Microsoft Entra* durante la instalación de *Microsoft Entra Connect*. La cuenta del conector de *Microsoft Entra* se usa para escribir información en *Microsoft Entra ID*. Es importante realizar esto, puesto que no se puede usar la cuenta de Microsoft que se utilizó para darse de alta en Azure.

Para crear una cuenta de administrador de identidad híbrida se debe iniciar sesión en el *centro de administración de Microsoft Entra*, una vez dentro, hay que situarse en **Identidad > Usuarios > Todos los usuarios** y ahí seleccionar *Nuevo usuario* > *Crear nuevo usuario*. En el panel *Crear nuevo usuario*, se debe asignar un Nombre para mostrar y un Nombre principal de usuario para el nuevo usuario. Va a crear la cuenta de administrador de identidad híbrida para el inquilino. Se pude indicar una contraseña o dejar que el sistema genere una temporal.

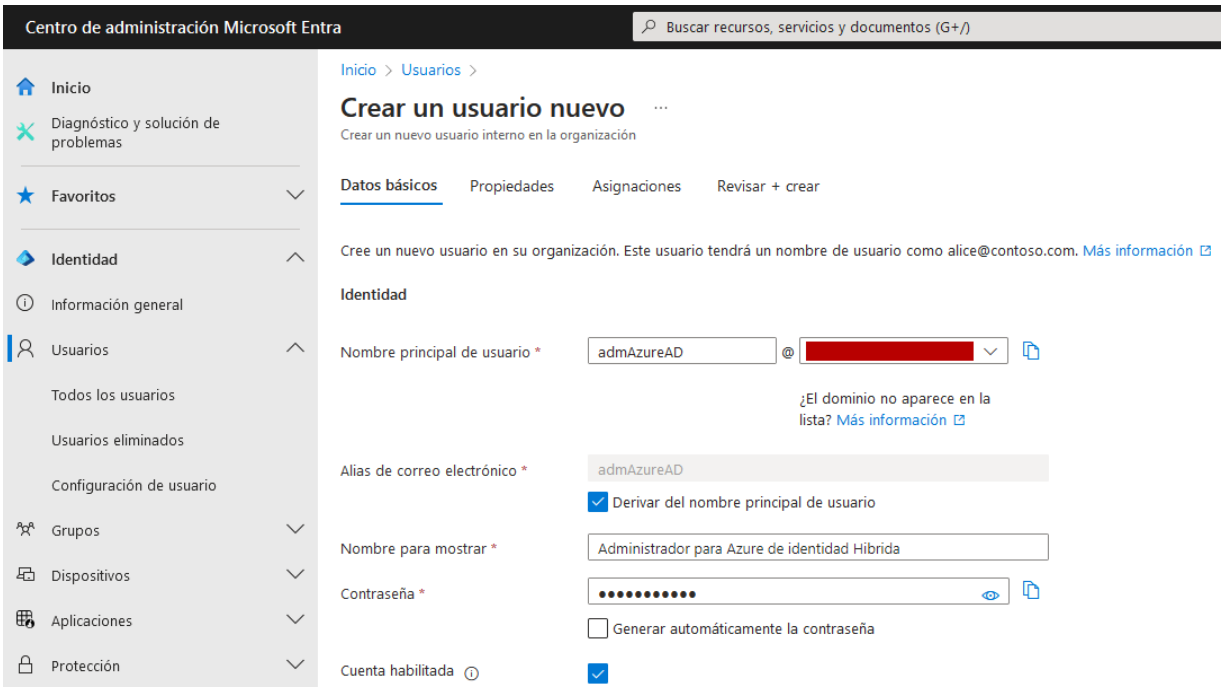

Ilustración 41: Crear un usuario en Microsoft Entra

En el panel o pestaña **Asignaciones**, seleccionar **Agregar rol** y ahí buscar y seleccionar *Administrador de identidades híbridas*. Como puede observarse en la siguiente imagen.

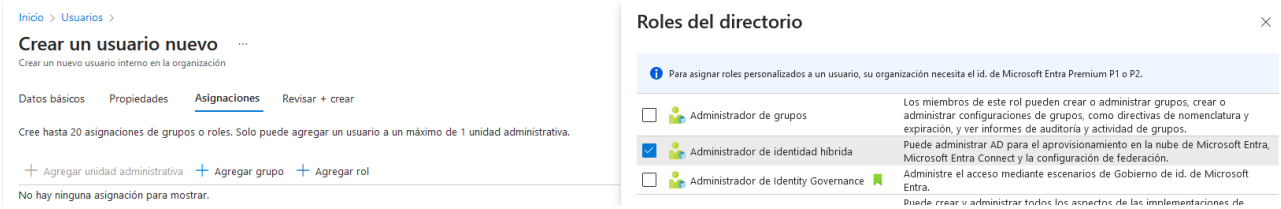

Ilustración 42: Asignación del rol al usuario a crear en Microsoft Entra

Asignado este rol, se selecciona *Revisar + crear* para ver un resumen de los datos del usuario.

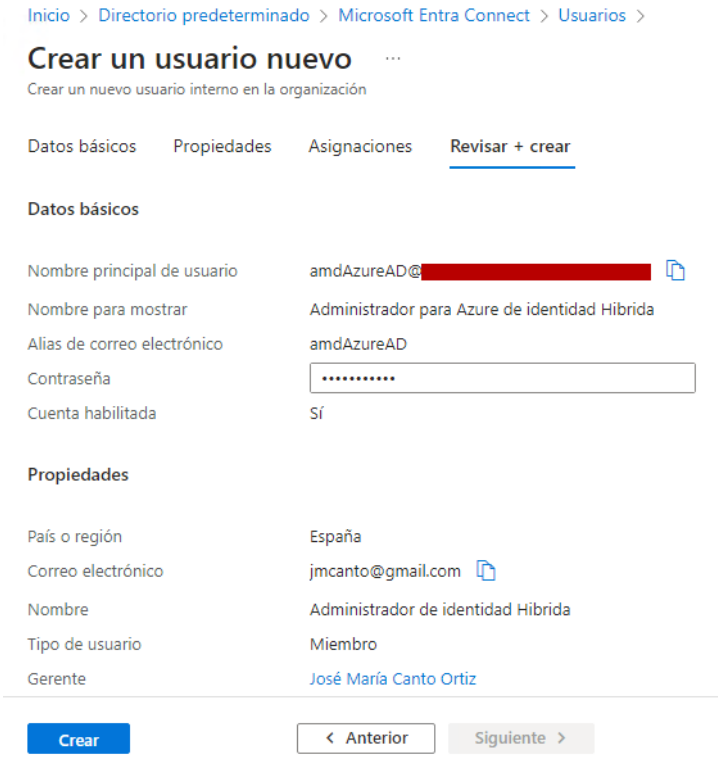

Ilustración 43: Resumen usuario a crear en Microsoft Entra

A continuación, se pulsa en el botón **Crear** que esta en la parte inferior.

Ahora se debe iniciar sesión en myapps.microsoft.com con la nueva cuenta de Administrador de identidad híbrida y la contraseña temporal. Elija una nueva contraseña para la cuenta de Administrador de identidades híbridas y cambie la contraseña. Probablemente sea necesario instalar en el dispositivo móvil la app *Microsoft Authenticator*. Concluido esto, se puede iniciar la instalación de *Microsoft Entra Connect.*

Ya que se tiene al inquilino y una cuenta de administrador de identidad híbrida, el siguiente paso es agregar el dominio personalizado, para que *Azure* pueda comprobarlo.

Para ello, hay que situarse en menú de la izquierda en **Identidad > Configuración > Nombres de dominio**. Y una vez ahí, seleccionar **Agregar dominio personalizado**.

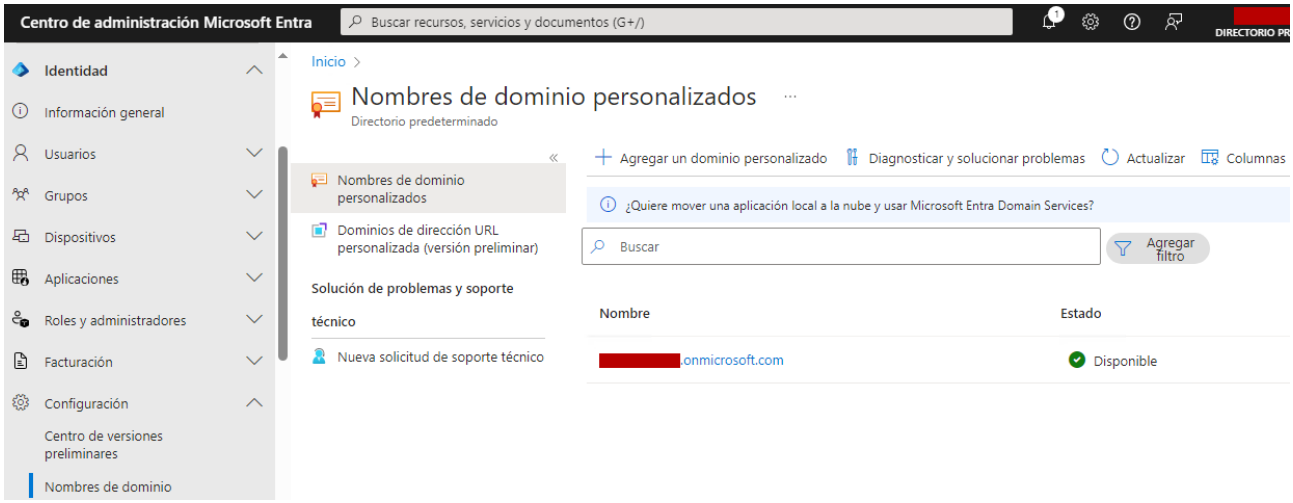

Ilustración 44: Crear nombre de dominio personalizado

Después hay que escribir el nombre del dominio personalizado y, luego, seleccionar *Agregar dominio*. En Nombre de dominio personalizado se muestra la información *TXT o MX*. Debe agregar esta información al servidor DNS donde esté creada la zona DNS de dicho dominio, que normalmente será uno del registrador de dominios donde se hizo dicho registro.

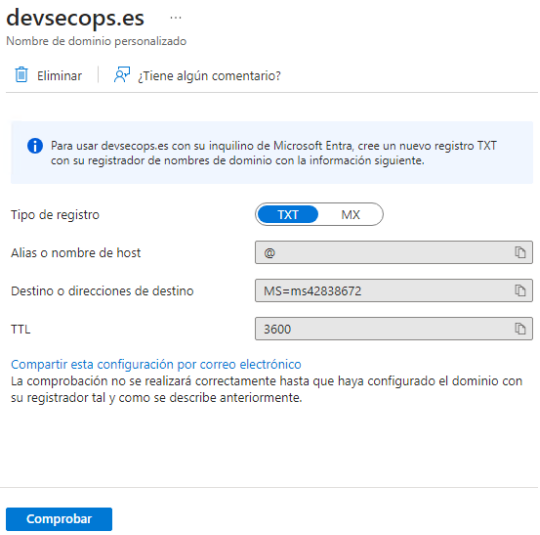

Ilustración 45: Datos a indicar en la zona DNS en el registrador del dominio

Microsoft Entra Connect sustituye a *Azure AD Connect* pero su funcionamiento es similar, para instalarla se accede a la url: https://www.microsoft.com/en-us/download/details.aspx?id=47594. De hecho en la instalación aparece el nombre de Azure AD Connect, en lugar del nuevo nombre. Una vez descargado dicho software, se inicia dicha instalación.

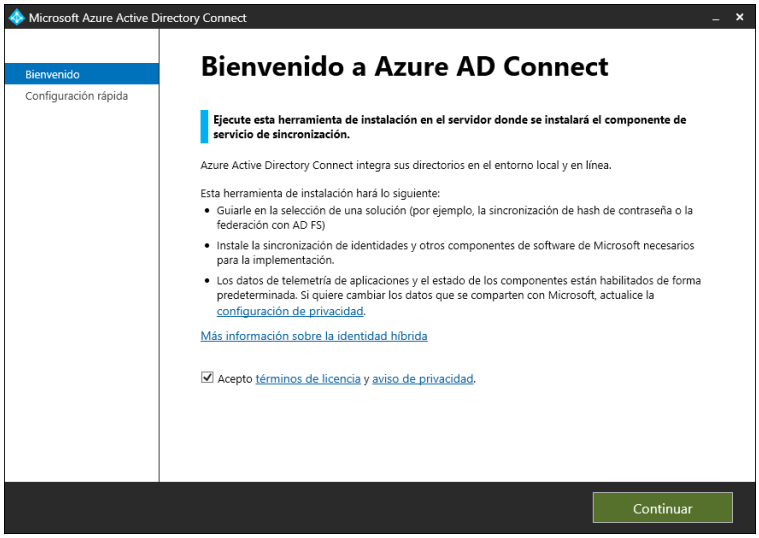

Ilustración 46: Comienzo instalación Azure AD Connect

En Bienvenida, active la casilla para aceptar los términos de licencia y, luego, seleccione Continuar. En Configuración rápida, seleccione **Personalizar**.

En la siguiente ventana, *Instalar componentes necesarios,* seleccione **Instalar**. En Inicio de sesión de usuario, seleccione *Federación con AD FS* y, luego, seleccione *Siguiente*.

En *Conectar con Azure AD*, hay que escribir el nombre de usuario y la contraseña de la cuenta de administrador de identidad híbrida que creó anteriormente y, luego, seleccione *Siguiente*.

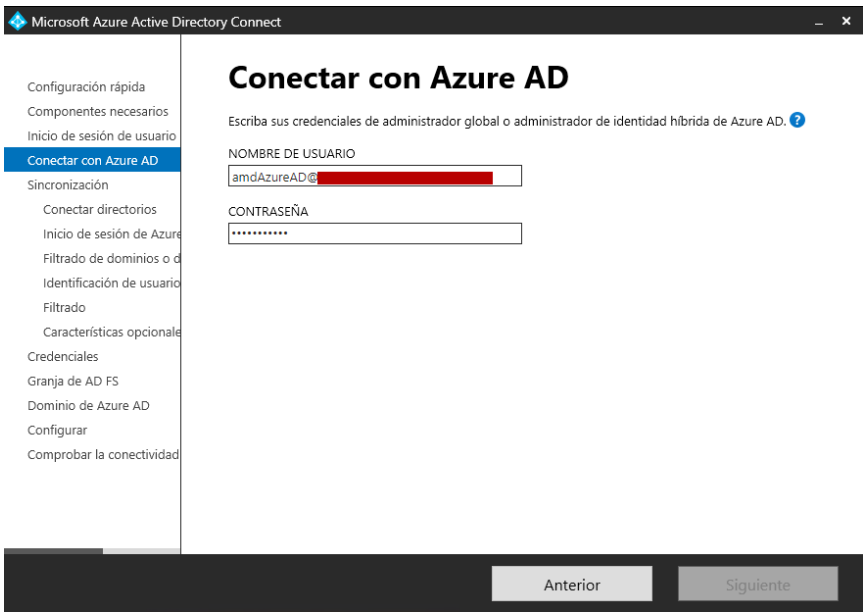

Ilustración 47: Indicar datos usuario administrador de identidad híbrida

En la siguiente ventana, *Conectar sus directorios*, seleccione del desplegable el dominio y pulse en *Agregar directorio*.

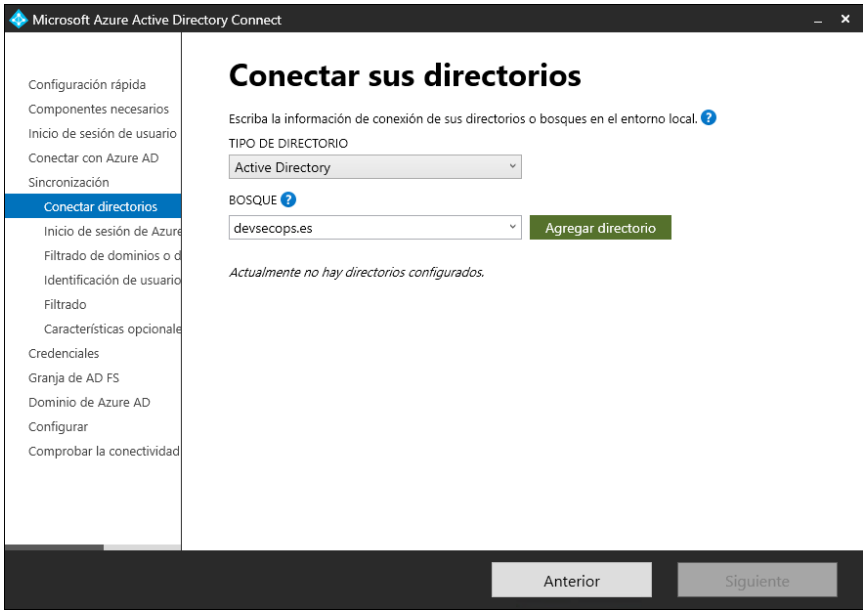

Ilustración 48: Conectar el directorio local

A continuación se pedirá que se seleccione entre las opciones crear una cuenta AD o utilizar una existente. Se recomienda seleccionar ***Crear una cuenta de AD*** y escriba el nombre de usuario y la contraseña del administrador del dominio, con lo que se crea una cuenta específica para esto. Seleccione Aceptar. Y tras unos segundos aparecerá el directorio agregado. Tras esto, seleccione *Siguiente*.

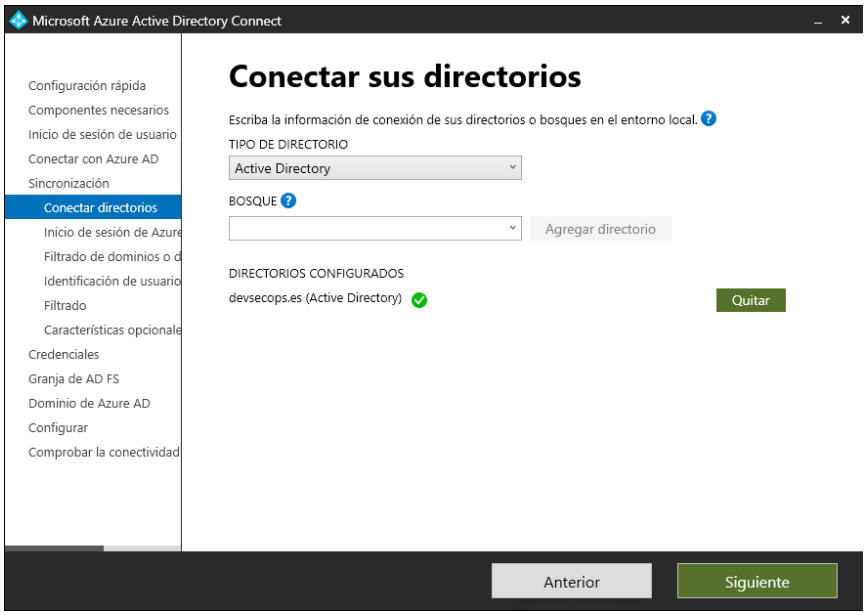

Ilustración 49: Directorio local conectado

La siguiente ventana trata de Configuración de inicio de sesión de *Azure AD / Microsoft Entra*, seleccione **Continuar sin relacionar todos los sufijos UPN con los dominios verificados** y a continuación pulsar Siguiente.

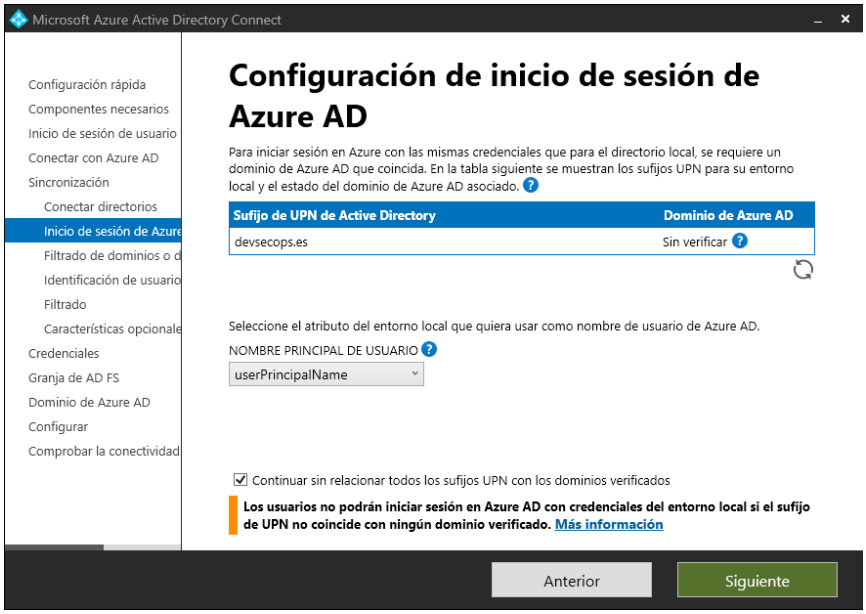

Ilustración 50: Configuración de inicio de sesión en Azure AD

En la ventana *Filtrado de dominios y unidades organizativas*, se deja tal y como aparece, seleccione *Siguiente*.

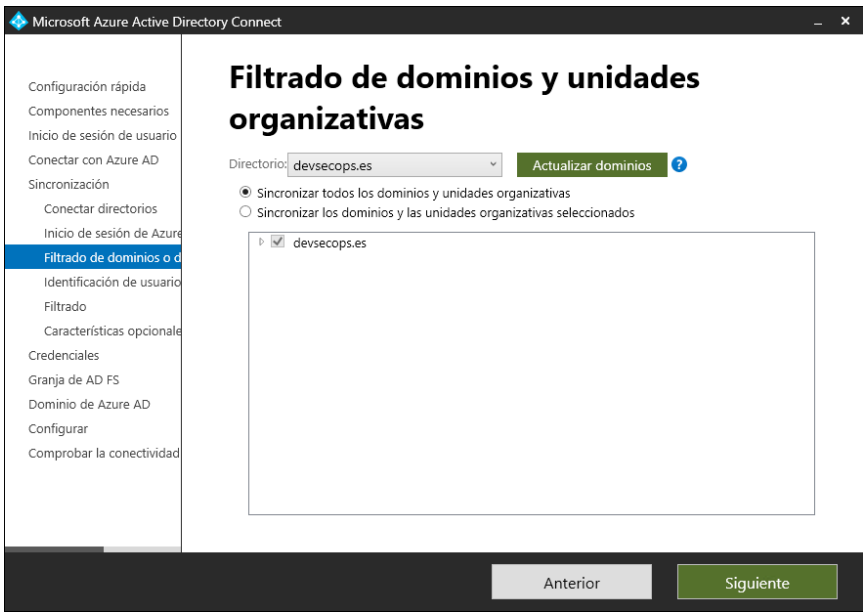

Ilustración 51: Filtrado de dominios y unidades

En Identificación de forma exclusiva de usuarios, no se cambia nada, seleccione *Siguiente*.

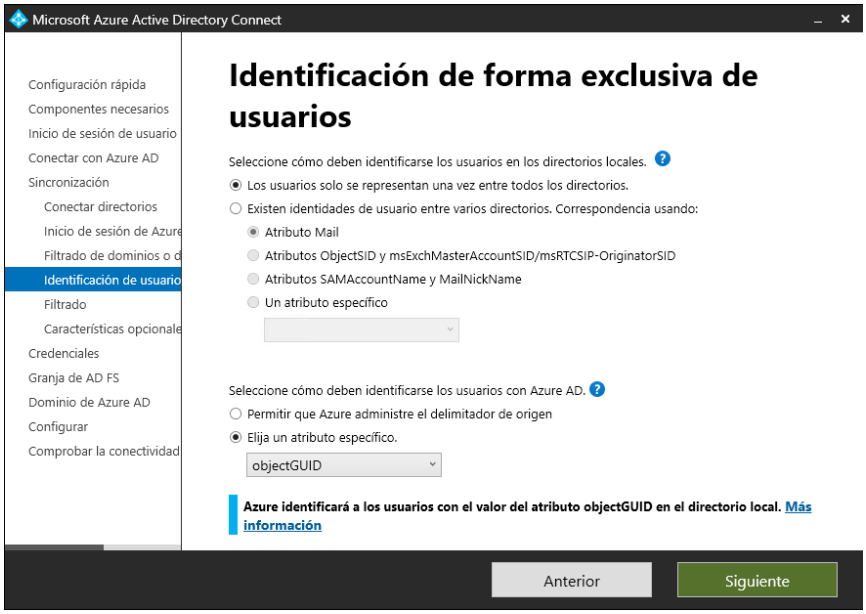

Ilustración 52: Identificación exclusiva de usuarios

Tanto en *Filtrar usuarios y dispositivos* como en *Características opcionales*, no se selecciona ninguna opción distinta de las que aparecen por defecto, con lo que en ambas se debe pulsar en *Siguiente*.

En *Credenciales de administrador* de dominio, escriba el nombre de usuario y la contraseña del administrador de dominio y, luego, haga clic en *Siguiente*.

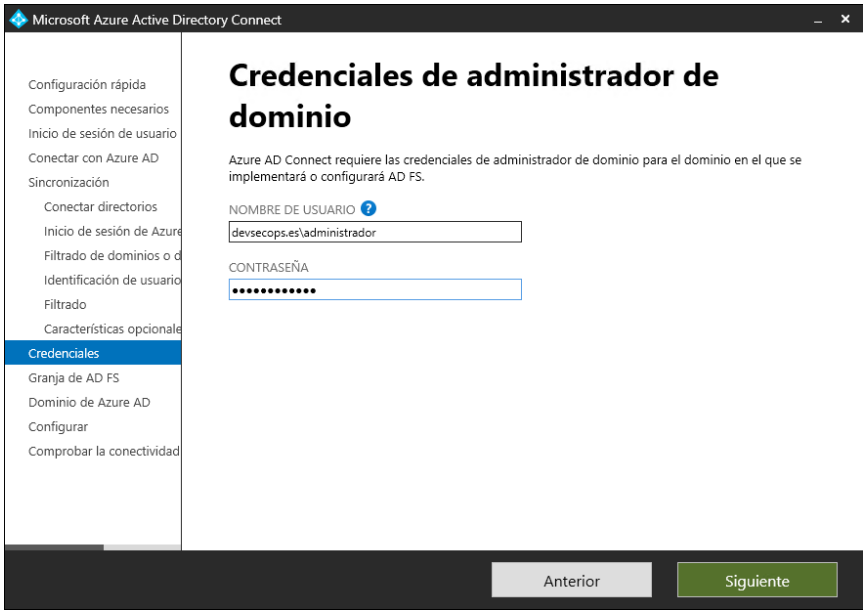

Ilustración 53: Indicar datos del administrador de dominio para enlazar AD FS con Azure

En Granja de AD FS, como ya existe una granja, se deja seleccionada la opción Usar una granja de AD FS asegúrese de que la opción Configurar una nueva granja de servidores de AD FS esté seleccionada.

Script de instalación y configuración servicios

Este script se encarga de ir comprobando los servicios necesarios para la posterior comprobación del segundo factor de autentificación en los usuarios. Entre las tareas que puede realizarse en el se encuentra:

- Arrancar el servicio de Active Directory si está parado.
- Instalar un controlador de dominio de solo lectura (secundario).
- Instalar Active Directory y DNS en caso de no estarlo.
- Instalar un controlador de dominio.

El script tiene tres parámetros que se pueden incluir en la ejecución del mismo se definen en el script de esta forma:

```
param([string]$instalarDC, [string]$instalarAD, [string]$instalarFS)
```

Siendo cada uno:

- -instalarDC: con un valor de *"si"* o *"s"*, asigna al servidor que ejecuta el script el rol de controlador de solo lectura (secundario)
- -instalarAD: si su valor es *"si"* o *"s"*, instala Active Directory y asigna el rol de controlador de dominio principal al servidor. Se instala también el DNS.
- -InstalarFS: si su valor es *"si"* o *"s"*, instala los servicios de AD CS y AD FS generando certificado.

Con este comando se le asigna al servidor el rol de controlador de dominio de solo lectura:

```
Install-ADDSDomainController -DomainName $nombreDominio `
 -ReplicationSourceDC $controladorDominio.Name `
 -Credential (Get-Credential)
```

Así se crea un controlador de dominio principal:

```
Install-ADDSDomainController -DomainName $nombreDominio `
 -InstallDNS `
 -CreateDNSDelegation `
 -Credential (Get-Credential)
```

Parámetros incluidos en ambas ejecuciones del ***Install-ADDSDomainController***:

- *-ReplicationSourceDC*: especifica el nombre del controlador de dominio que se utilizará como origen para replicar en este controlador de dominio.
- *-InstallDNS*: instala y configura el servicio Servidor DNS en el controlador de dominio.
- *-CreateDNSDelegation*: crea una delegación DNS que hace referencia al nuevo servidor

DNS que se instala junto con el controlador de dominio. Sólo es válido para el DNS integrado en *Active Directory*.

- *-Credential*: especifica el nombre de usuario y la contraseña que corresponden a la cuenta utilizada para instalar el controlador de dominio. Al usarlo junto con *Get-Credential*, se solicita usuario y clave para instalar el servicio.

De esta otra forma se instala *Active Directory* y el servidor DNS:

```
Add-WindowsFeature -name AD-Domain-Services, DNS `
 -IncludeAllSubFeature -IncludeManagementTools -Restart
```

Para instalar AD CS e incluir las herramientas de administración, se utiliza este comando:

```
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
```

Los *servicios de federación* (AD FS), se instalan de esta forma con sus herramientas de administración:

```
Install-WindowsFeature ADFS-Federation -IncludeManagementTools
```

Para crear un certificado auto firmado se puede realizar de esta forma:

```
$certificado = New-SelfSignedCertificate `
 -DnsName $nombreADFS `
 -CertStoreLocation "Cert:\LocalMachine\My"
```

Los parámetros usados son los siguientes:

- *-DnsName:* indica uno o más nombres DNS (en este caso uno) para poner en la extensión de nombre alternativo del certificado. El primer nombre DNS también se guarda como nombre de asunto. Si no se especifica ningún certificado de firma, el primer nombre DNS también se guarda como Nombre del Emisor.

- *-CertStoreLocation*: Especifica el almacén de certificados en el que se almacenará el nuevo certificado.

La granja para los servidores de AD FS se puede crear de esta forma:

```
Install-AdfsFarm -CertificateThumbprint $huellaCert `
 -FederationServiceDisplayName $nombreaMostrar `
 -FederationServiceName $nombreADFS `
 -ServiceAccountCredential $serviceAccount
```

Lo que hace es crear el primer nodo de una nueva granja de servidores de federación. Los parámetros indicados son:

- *-CertificateThumbprint*: Especifica la huella digital de un certificado X.509 de clave pública digital. Esta huella se obtiene del certificado creado anteriormente.

- *-FederationServiceDisplayName*: indica el nombre a mostrar.

- *-FederationServiceName*: especifica el nombre del Servicio de Federación de *Active Directory*.

- *-ServiceAccountCredential*: indica la cuenta de *Active Directory* bajo la que se ejecuta el servicio *AD FS.*

El enlace con *Azure* se realiza utilizando el módulo *Graph ya que MSOnline* está obsoleto.

Script creación usuarios

Este script se realiza considerando el escenario en el que se ha migrado de un sistema antiguo y se tienen los usuarios del servidor o dominio almacenados en un fichero de formato CSV para importarlo en *Active Directory* una vez montada la infraestructura. El script leerá dicho fichero y creará los usuarios en el domino y les asignará un grupo.

La lectura del fichero se realiza mediante el comando **Import-Csv**, que básicamente crea objetos personalizados en formato tabla a partir de los elementos de un archivo CSV. El parámetro más importante es *-Path* que se indica la ruta del fichero. Si el delimitador fuera distinto de la coma, se podría utilizar el parámetro *-Delimiter*.

```
$Users = Import-Csv -Path $csvPath
```

Este objeto *$Users* se recorre con un bucle *foreach* en el que para cada elemento se van realizando una serie de comprobaciones, antes de crear el usuario: como si ya está creado el usuario o si la unidad organizativa es correcta.

La comprobación de la existencia, o no del usuario, se ha incluido de esta forma:

```
if (-not (Get-ADUser -Filter "SamAccountName -eq '$($User.SamAccountName)'")) {
```

Se utiliza el método **Get-ADUser** incluyendo un filtro que comprueba si el nombre de la cuenta de usuario (*SamAccountName*) es igual al que tiene el elemento guardado. En caso que no coincidan, indica que el usuario no existe y se procede a su creación.

La unidad organizativa se comprueba con el comando **Get-ADOrganizationalUnit**, de esta forma:

```
$ou = Get-ADOrganizationalUnit -Filter "DistinguishedName -eq '$rutaOU'" -ErrorAction Stop
```

La comprobación se hace de forma similar a la del usuario, se incluye un filtro donde se comprueba si el atributo DistinguishedName coincide con el indicado en el elemento, si coincide entonces se puede indicar que la unidad organizativa existe.

Para crear los usuarios en el dominio se utiliza el comando **New-ADUser**, en el caso que nos ocupa de la siguiente forma:

```
New-ADUser -Name "$nombre $apellido" `
 -DisplayName "$nombre $apellido" `
 -SamAccountName $nombreCuenta `
 -UserPrincipalName $usuarioPrincipal `
 -GivenName "$nombre" `
 -Surname "$apellido" `
 -Description "$($User.Description)" `
 -AccountPassword $SecurePassword `
 -Enabled $true `
 -Path "$rutaOU" `
 -ChangePasswordAtLogon $true `
 -PasswordNeverExpires $false `
 -Server $dominio.DnsRoot
```

Los parámetros indicados son:

- *-Name*: establece la propiedad Nombre de un usuario.
- *-DisplayName*: especifica el nombre para mostrar del usuario.
- *-SamAccountName*: indica el nombre de la cuenta de usuario.
- *-UserPrincipalName*: establece el nombre de usuario principal (*UPN*) en el formato *<usuario>@<nombre de dominio DNS>*.
- *-GivenName*: indica el nombre del usuario.
- *-Surname*: apellidos del usuario.
- *-Description*: se indica la descripción del usuario.
- *-AccountPassword*: especifica un nuevo valor de contraseña para una cuenta. Este valor se almacena como una cadena cifrada.
- *-Enabled*: indica si la cuenta se va a crear habilitada o no.
- *-Path*: se indica la ruta de la unidad organizativa o contenedor donde se crea el nuevo usuario.
- *-ChangePasswordAtLogon*: indica si la contraseña debe cambiarse en el primer intento de inicio de sesión.
- *-PasswordNeverExpires*: especifica si la contraseña de una cuenta puede caducar. Este parámetro no se puede establecer a verdadero ($true o 1) para una cuenta que también tenga la propiedad *ChangePasswordAtLogon* establecida en verdadero, es decir no se puede establecer que la contraseña nunca caduca, cuando se ha indicado que la contraseña se debe cambiar en el siguiente inicio de sesión.
- *-Server*: se indica la instancia de *AD DS* a la que conectarse, proporcionando uno de los siguientes valores: nombre de dominio o servidor de directorio correspondiente.

Para la asignación del grupo de usuarios se utiliza el comando **Add-ADGroupMember** y en el script se ha indicado de la siguiente forma:

```
Add-ADGroupMember `
    -Identity $User.Group `
    -Members $User.SamAccountName
```

Los parámetros utilizados son:

- *-Identity*: se especifica un grupo de *Active Directory* ya existente
- -Members: se indica uno o varios usuarios, separados por comas para añadirlos al grupo indicado en el parámetro anterior. En este caso, solamente se indica un nombre de cuenta.

Como posible mejora al script de creación de usuarios, se encuentran:

- Introducción de una función para generar una clave aleatoria que cumpla las restricciones.
- Enviar correo electrónico con los datos de acceso del usuario o a su superior.

Script comprobación usuarios activado 2FA

El siguiente script obtiene todos los usuarios del dominio y va comprobando para cada uno de ellos si tienen el segundo factor de autentificación activado.