

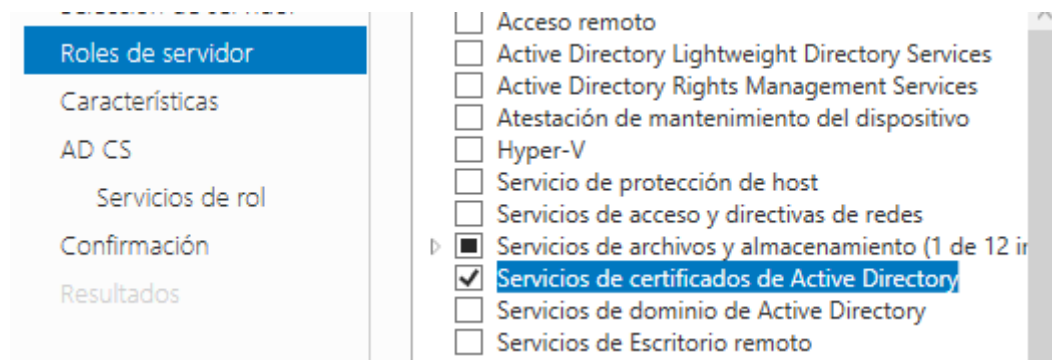
TEMA 2: Administración de credenciales de acceso a sistemas

Práctica 2.7: Creación de una PKI en Windows

En este caso vamos a mostrar como instalar una CA en un entorno Windows para poder emitir certificados y utilizarlos en los servicios de Windows.

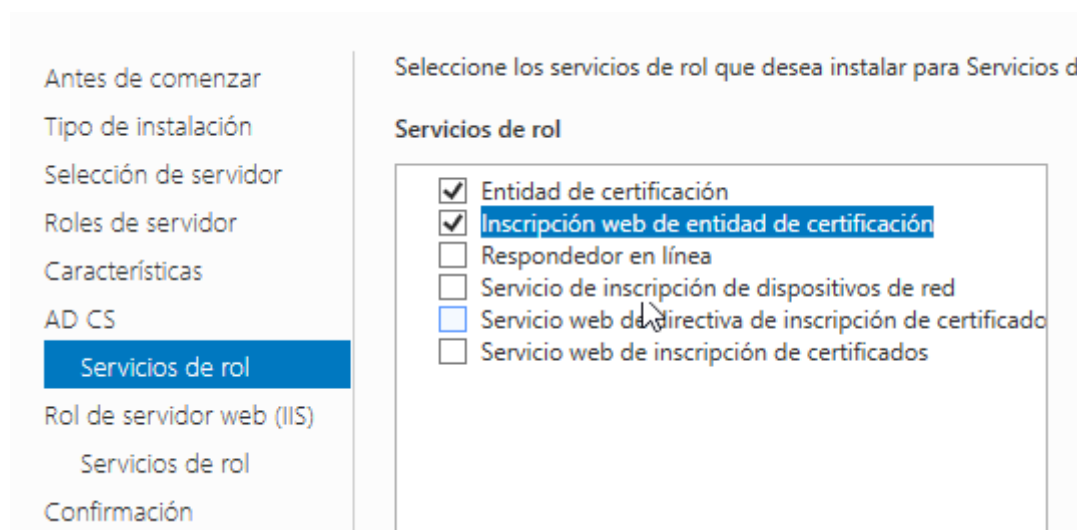
Desde el panel de administrador del servidor haremos una nueva instalación basada en características o en roles.

Y seleccionaremos “Servicios de certificados de Active Directory”

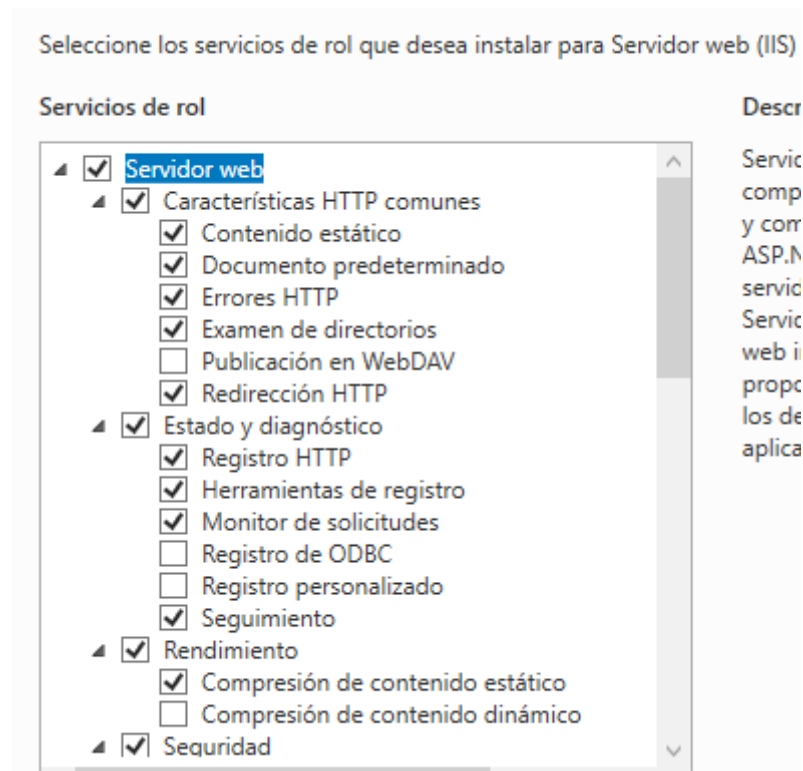


Servicios de certificados de Active Directory (AD CS) proporciona la infraestructura de certificados para habilitar escenarios como redes inalámbricas seguras, redes privadas virtuales, IPSec, protección de acceso a redes (NAP) y el sistema de cifrado de archivos (EFS).

Seleccionaremos los servicios de rol siguientes



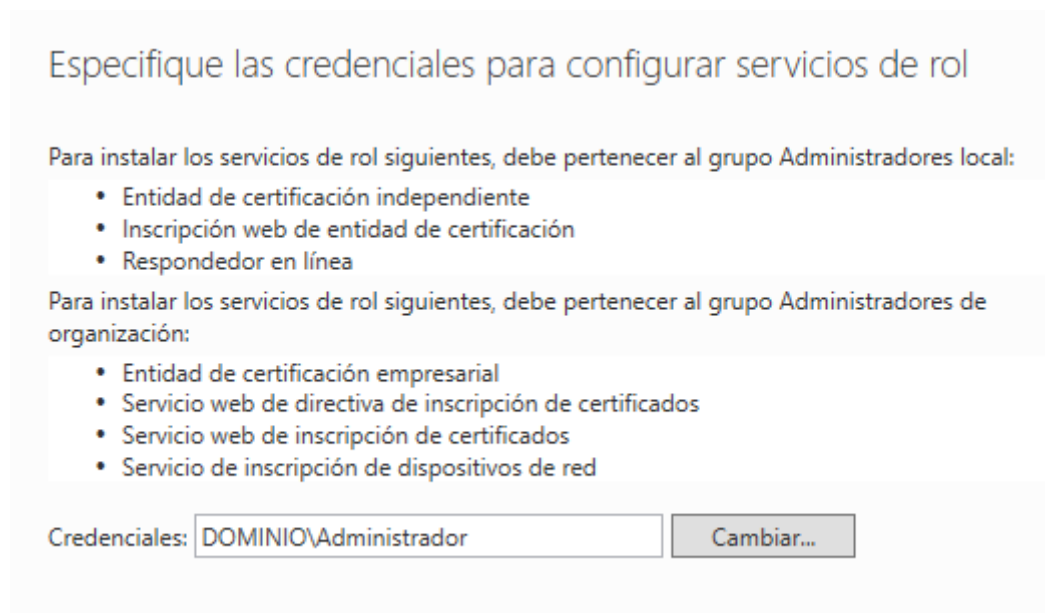
Dejaremos los servicios de rol para el Servidor web (IIS) como vienen por defecto.



Y procedemos a instalar.

Seguidamente procedemos a configurar los servicios de rol instalados.

Durante el asistente dejamos las opciones por defecto



Y seleccionamos los servicios a configurar

Servicios de rol

SERVIDOR DE DESTINO
AD01.dominio.local

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez

Seleccionar los servicios de rol que se configurarán

- ☒ Entidad de certificación
- ☒ Inscripción web de entidad de certificación
- ☐ Respondedor en línea
- ☐ Servicio de inscripción de dispositivos de red
- ☐ Servicio web de inscripción de certificados
- ☐ Servicio web de directiva de inscripción de certificados

Realizamos una instalación de CA empresarial

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso

Especifique el tipo de instalación de la CA

Las entidades de certificación (CA) empresariales pueden usar Servicios de dominio de Active Directory (AD DS) para simplificar la administración de los certificados. Las CA independientes no usan AD DS para emitir ni administrar certificados.

- ☒ CA empresarial
Las CA empresariales deben pertenecer al dominio y normalmente están en línea para emitir certificados o directivas de certificados.
- ☐ CA independiente
Las CA independientes pueden pertenecer a un grupo de trabajo o a un dominio. No requieren AD DS y se pueden usar sin conexión a la red (sin conexión).

Y seleccionamos el tipo de CA raíz.

Tipo de CA

SERVIDOR DE DESTINO
AD01.dominio.local

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso

Especifique el tipo de CA

Al instalar Servicios de certificados de Active Directory (AD CS), crea o amplía una jerarquía de infraestructura de clave pública (PKI). Se sitúa una CA raíz en la parte superior de la jerarquía de PKI, que emite su propio certificado autofirmado. Una CA subordinada recibe un certificado de la CA inmediatamente superior en la jerarquía de PKI.

- ☒ CA raíz
Las CA raíz son las primeras y puede que las únicas configuradas en una jerarquía de PKI.
- ☐ CA subordinada
Las CA subordinadas requieren una jerarquía de PKI establecida y están autorizadas a emitir certificados de la CA inmediatamente superior en la jerarquía.

Seleccionamos crear una clave privada nueva.

Configuración de AD CS

SERVIDOR DE DESTINO
AD01.dominio.local

Clave privada

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA
- Clave privada**
- Criptografía
- Nombre de CA
- Período de validez

Especifique el tipo de la clave privada

Para generar y emitir certificados a clientes, una entidad de certificación (CA) debe disponer de una clave privada.

☒ Crear una clave privada nueva
Use esta opción si no dispone de una clave privada o desea crear una clave privada nueva.

☐ Usar clave privada existente
Use esta opción para asegurar la continuidad con los certificados emitidos previamente al reinstalar una CA.

Y dejamos las opciones criptográficas por defecto

Configuración de AD CS

SERVIDOR DE DESTINO
AD01.dominio.local

Criptografía para la CA

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA
- Clave privada
- Criptografía**
- Nombre de CA
- Período de validez
- Base de datos de certifica...
- Confirmación
- Progreso

Especifique las opciones criptográficas

Seleccionar un proveedor de servicios criptográficos: RSA#Microsoft Software Key Storage Provider Longitud de la clave: 2048

Seleccione el algoritmo hash para firmar los certificados emitidos por esta CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Permitir interacción del administrador cuando la CA obtiene acceso a la clave privada.

Y especificamos un nombre para la CA. En este caso lo dejamos por defecto.

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Resultados

Especifique el nombre de la CA

Escriba un nombre común para identificar esta entidad de certificación (CA). E agregue a todos los certificados emitidos por la CA. Los valores de sufijo de nombre generan automáticamente, pero se pueden modificar.

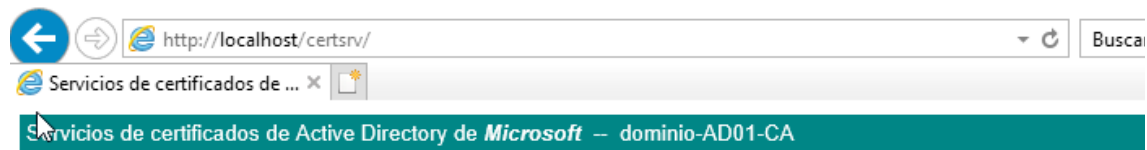
Nombre común para esta entidad de certificación:
dominio-AD01-CA

Sufijo de nombre distintivo:
DC=dominio,DC=local

Vista previa de nombre distintivo:
CN=dominio-AD01-CA,DC=dominio,DC=local

Seguimos el asistente hasta finalizar la instalación.

Cuando finalice tendremos instalada nuestra CA y podremos crear certificados mediante un explorador web entrando en la dirección <http://localhost/certsrv/>



Página principal

Use este sitio web para solicitar un certificado para su explorador web, programa cliente de correo electrónico, puede confirmar su identidad ante otras personas con las que se comunica vía web, filtrar el tipo de certificado que solicite, realizar otras tareas de seguridad.

También puede usar este sitio web para descargar certificados de entidad de certificación (CA), certificados de revocación (CRL) o ver el estado de una solicitud pendiente.

Para obtener más información acerca de Servicios de certificados de Active Directory, vea [Documentación de Active Directory](#).

Seleccione una tarea:

[Solicitar un certificado](#)

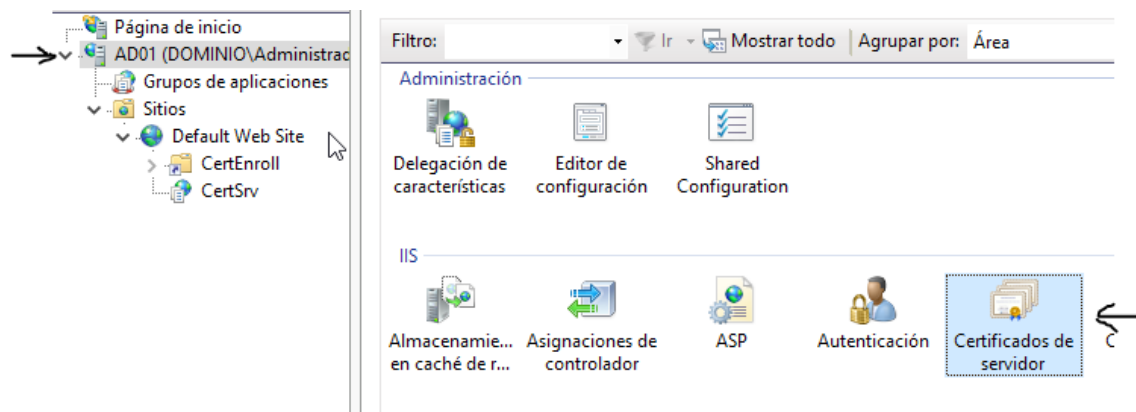
[Ver el estado de una solicitud de certificado pendiente](#)

[Descargar un certificado de CA, cadena de certificados o lista de revocación](#)

Si intentamos crear un certificado vía web, nos aparecerá un mensaje de advertencia que nos dice que nuestro sitio web necesita estar configurado para usar https.

Vamos a proceder a solucionar esto.

Nos dirigimos a nuestro servidor IIS y si seleccionamos "Certificados de servidor" dentro de "AD01".



Vemos que tenemos un certificado AD01.dominio.local emitido por nuestra propia CA.

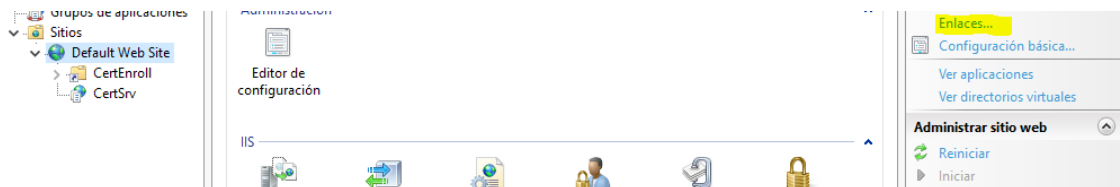


Certificados de servidor

Utilice esta característica para solicitar y administrar certificados que el servidor web puede usar con sitios web configurados para SSL.

Filtro:	Mostrar todo	Agrupar por:	Sin agrupar
Nombre	Emitido para	Emitido por	Fecha de expira
	dominio-AD01-CA AD01.dominio.local	dominio-AD01-CA dominio-AD01-CA	10/01/2026 23:4 10/01/2022 23:3

Vamos a asignar ese certificado a la página por defecto en el puerto 443. Para ello, seleccionamos “Default Web Site” y pinchamos sobre Enlaces...

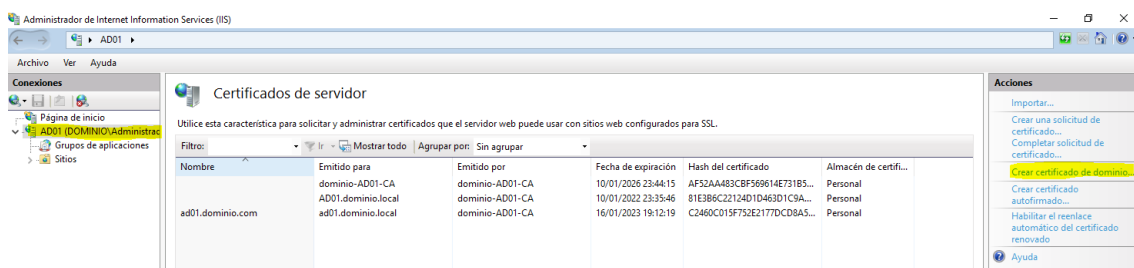


Y ahora si accedemos con un explorador a <https://localhost/certsrv> vemos que nos aparece la misma página desde la que podremos emitir certificados autofirmados.

Practica 2.8: Configuración de dominios en IIS con SSL

Vamos a crear dos certificados para los dominios “dominio1.com” y “dominio2.com” de dos maneras distintas.

La primera será desde el servidor IIS mediante la opción “Crear certificado de dominio”. Para ello nos dirigimos al IIS y pinchando sobre el nombre, en las acciones disponibles seleccionamos “Crear certificado de dominio...”



En el asistente rellenamos los campos con los datos sobre el dominio1.com



Propiedades de nombre distintivo

Especifique la información requerida para el certificado. Estado o provincia y Ciudad o localidad deben ser nombres oficiales y no deben contener abreviaturas.

Nombre común:	<input type="text" value="dominio1.com"/>
Organización:	<input type="text" value="Empresa"/>
Unidad organizativa:	<input type="text" value="Sistemas"/>
Ciudad o localidad:	<input type="text" value="Albacete"/>
Estado o provincia:	<input type="text" value="España"/>
País o región:	<input type="text" value="ES"/>

Y seleccionamos la entidad certificadora que hemos instalado en el servidor.



Entidad de certificación en línea

Especifique la entidad de certificación de su dominio que firmará el certificado. Se requiere un nombre descriptivo que debería ser fácil de recordar.

Especifique una entidad de certificación en línea:

<input type="text" value="dominio-AD01-CA\AD01.dominio.local"/>	<input type="button" value="Seleccionar..."/>
---	---

Ejemplo: NombreDeEntidadDeCertificación\NombreDeServidor

Nombre descriptivo:

Para el segundo certificado, en este caso, nos dirigimos a nuestro IIS y pinchando sobre el nombre del servidor, en la sección “Acciones”, seleccionamos “Crear solicitud certificado”

Acciones
Importar...
Crear una solicitud de certificado...
Completar solicitud de certificado...
Crear certificado de dominio...
Crear certificado autofirmado...
Habilitar el reenlace automático del certificado renovado
? Ayuda

Rellenamos los campos, poniendo como nombre común dominio2.com

Solicitar certificado



Propiedades de nombre distintivo

Especifique la información requerida para el certificado. Estado o provincia y Ciudad o localidad deben ser nombres oficiales y no deben contener abreviaturas.

Nombre común:	<input type="text" value="dominio2.com"/>
Organización:	<input type="text" value="Empresa"/>
Unidad organizativa:	<input type="text" value="Sistemas"/>
Ciudad o localidad:	<input type="text" value="Albacete"/>
Estado o provincia:	<input type="text" value="España"/>
País o región:	<input type="text" value="ES"/>



Entidad de certificación en línea

Especifique la entidad de certificación de su dominio que firmará el certificado. Se requiere un nombre descriptivo que debería ser fácil de recordar.

Especifique una entidad de certificación en línea:

dominio-AD01-CA\AD01.dominio.local

Seleccionar...

Ejemplo: NombreDeEntidadDeCertificación\NombreDeServidor

Nombre descriptivo:

dominio2.com



Propiedades de proveedor de servicios criptográficos

Seleccione un proveedor de servicios criptográficos y una longitud en bits. La longitud en bits de la clave de cifrado determina la seguridad de cifrado del certificado. Cuanto mayor sea la longitud en bits, más segura. Sin embargo, una longitud en bits grande puede mermar el rendimiento.

Proveedor de servicios criptográficos:

Microsoft RSA SChannel Cryptographic Provider

Longitud en bits:

1024

Le ponemos un nombre al archivo de la solicitud.

Solicitar certificado



Nombre de archivo

Especifique un nombre para la solicitud de certificado. Esta información se puede enviar a una entidad de certificación para que la firme.

Especificar un nombre de archivo para la solicitud de certificado:

C:\Users\Administrador\Desktop\dominio2.com_csr.txt



Seguidamente nos dirigimos a nuestro servidor de certificados vía web y seleccionamos la segunda opción.

Browser address bar: <https://localhost/certsrv/certreq.asp> Error de certificado Buscar...

Servicios de certificados de Active Directory de Microsoft – dominio-AD01-CA

Solicitud de certificado avanzada

La directiva de la CA determina los tipos de certificados que puede solicitar. Haga clic en una de las siguientes opciones para:

- [Crear y enviar una solicitud a esta CA.](#)
- [Enviar una solicitud de certificado con un archivo codificado en base64 CMC o PKCS #10 o una solicitud de renovación con un archivo codificado en base64 PKCS #7.](#)

Copiamos el texto del archivo dominio2.com_csr.txt

Servicios de certificados de Active Directory de Microsoft – dominio-AD01-CA

Enviar una solicitud de certificado o una solicitud de renovación

Para enviar una solicitud guardada a la CA copie una solicitud de certificado codificado en base64 (servidor web) en la casilla de solicitudes guardadas.

Guardar solicitud:

Codificado en Base64
Solicitud de certificado
(CMC o
(PKCS #10 o
PKCS #7):

```
tyKUNjEv2cPVu/5/hDH+FqfN6yNXTArLFvNdF49b:  
adtjN/8xOUiKLHoLb+GVCe4C1oVmJK5C1ecKUJY9:  
kQPN6fU7pzVOp3kO7J/9pbnjEr/PG1qCB1lsElsg:  
tvL0+vLfhtPlKeLDDUJch9pDB5BG1zG8Q==  
-----END NEW CERTIFICATE REQUEST-----
```

Plantilla de certificado:

Servidor web

Atributos adicionales:

Atributos:

Enviar >

Y nos descargamos el certificado emitido en formato .cer

Servicios de certificados de Active Directory de *Microsoft* – dominio-AD01-CA

Certificado emitido

Se emitió el certificado que ha solicitado.

☒ Codificado en DER o ☐ Codificado en Base64



[Descargar certificado](#)

[Descargar cadena de certificados](#)

Para finalizar, nos dirigimos a nuestro IIS y completamos la solicitud del certificado.

Completar solicitud de certificado

?

×



Especificar respuesta de entidad de certificación

Complete una solicitud de certificado creada previamente recuperando el archivo que contiene la respuesta de la entidad de certificación.

Nombre del archivo que contiene la respuesta de la entidad de certificación:

C:\Users\Administrador\Downloads\certnew.cer

...

Nombre descriptivo:

dominio2.com

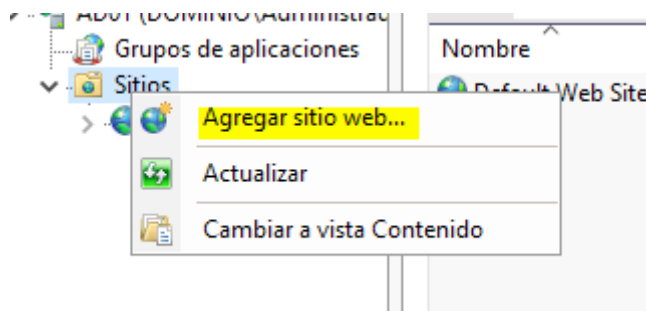
Seleccione un almacén de certificados para el nuevo certificado:

Personal

Aceptar

Cancelar

Llegados a este punto solamente nos queda crear los sitios web y asignarles un certificado.



Agregar sitio web

Nombre del sitio:

dominio1.com

Grupo de aplicaciones:

dominio1.com

Seleccionar...

Directorio de contenido

Ruta de acceso física:

C:\www\dominio1.com

...

Autenticación de paso a través

Conectar como...

Probar configuración...

Enlace

Tipo:

https

Dirección IP:

Todas las no asignadas

Puerto:

443

Nombre de host:

dominio1.com

☒ Requerir indicación del nombre de servidor

☐ Deshabilitar HTTP/2

☐ Deshabilitar la asociación de OCSP

Certificado SSL:

dominio1.com

Seleccionar...

Ver...

☒ Iniciar sitio web inmediatamente

Aceptar

Cancelar