Guía 6 – Configuración del firewall para el acceso de los clientes al Servicio AD

GUÍA 6 – CONFIGURACIÓN DEL FIREWALL PARA EL ACCESO DE LOS CLIENTES AL SERVICIO AD 1

DESCRIPCIÓN DEL ESCENARIO 1
INFORMACIÓN TÉCNICA DEL SERVICIO AD 2
SOLUCIÓN: 4
1. Crear los objetos para el servicio AD y SAMBA 4
2. Establecer comunicación desde los clientes de la LAN2 13
Paso 3 - Ingrese con los usuarios del dominio 17

Descripción del escenario

Se desea configurar el router srvext de forma que permita el acceso de los clientes ubicados en la red LAN02 (192.168.50.0) al servidor DC que se encuentra en la LAN01 (192.168.60.2)

- Dominio: empresay.com.sv
- Crear un objeto servicio con los puertos a utilizarse para Active Directory y SAMBA (Kerberos, DS, SMB/CIFS)
- Crear dos reglas para permitir el tráfico desde la red LAN02 al DC (Domain Controller)

Se puede utilizar como destino la dirección 192.168.60.0 en lugar de la dirección 192.168.60.2
Se recomienda utilizar BGIfo en las pantallas de los clientes Windows.

Prerequisitos

Información Técnica del servicio AD

Los servicios que provee Active Directory son:
Información tomada y modificada de https://technet.microsoft.com/es-es/library/dd578336(v=ws.10).aspx

1. **Active Directory Domain Services**. Servicios de dominio de Active Directory (**AD DS**) para almacenar datos de directorio y administrar la comunicación entre cuentas de usuarios y dominios, incluso procesos de inicio de sesión de usuarios, autenticación y búsquedas en directorios.
2. **Active Directory Lightweight Directory Services**. Active Directory Lightweight Directory Services (AD LDS), es un servicio de directorio del Protocolo ligero de acceso a directorios (LDAP) que ofrece una compatibilidad flexible para aplicaciones habilitadas para el uso de directorios, sin las restricciones de los Servicios de dominio de Active Directory (**AD DS**).
3. **Active Directory Federation Services**. Servicios de federación de Active Directory (**AD FS**) son las tecnologías de inicio de sesión único (SSO) web para autenticar a un usuario en varias aplicaciones web durante una única sesión en línea.
4. **Active Directory Certificate Services**. Servicios de certificados de Active Directory (**AD CS**) permite crear, distribuir y administrar certificados de claves públicas personalizados.
5. **ctive Directory Rights Management Services**. Active Directory Rights Management Services (**AD RMS**) permite proteger la información y trabajar con aplicaciones compatibles con AD RMS para ayudar a proteger la información digital del uso no autorizado.

En el caso de Zentyal solo los primeros dos servicios del AD pueden ser configurados, es decir solo se podrá configurar el AD DS y el AD LDS.

El servicio AD DS proporciona una base de datos distribuida que almacena y administra información acerca de los recursos de red y datos específicos de las aplicaciones con directorio habilitado. Los administradores pueden usar AD DS para organizar los elementos de una red (por ejemplo, los usuarios, los equipos y otros dispositivos) en una estructura de contención jerárquica. La estructura de contención jerárquica incluye el bosque de Active Directory, los dominios del bosque y las unidades organizativas de cada dominio. El servidor que ejecuta AD DS se llama controlador de dominio DC. Tomado de: https://technet.microsoft.com/es-es/library/cc731053(WS.10).aspx

El servicio AD LDS es un servicio de directorio del protocolo ligero de acceso a directorios (LDAP) que ofrece una compatibilidad flexible para aplicaciones habilitadas para el uso de directorios, sin las dependencias que se requieren para los Servicios de dominio de Active Directory (AD DS). AD LDS ofrece la mayoría de las funciones de AD DS, aunque no exige la implementación de dominios ni de controladores de dominio. Es posible ejecutar varias instancias de AD LDS de forma simultánea en un único equipo, siempre que haya un esquema administrado de forma independiente para cada instancia de AD LDS. Tomado de: https://technet.microsoft.com/es-es/library/cc754361(v=ws.10).aspx

El servicio de Sistema de archivos distribuido (DFS) administra los volúmenes lógicos distribuidos de una red de área local o amplia (LAN o WAN) y es necesario para el recurso compartido SYSVOL de Microsoft® Active Directory®. DFS es un servicio distribuido que integra recursos compartidos de archivo dispares en un solo espacio de nombre lógico.

ADWS es un servicio de Windows que proporciona una interfaz de servicio web para instancias del servicio de directorio de AD DS y AD LDS, y para instantáneas de Active Directory que se ejecutan en el mismo servidor de Windows Server 2008 R2 que ADWS. ADWS se instala automáticamente al agregar los roles de servidor de AD DS o AD LDS al servidor de Windows Server 2008 R2. Tomado de: https://technet.microsoft.com/es-es/library/cc731053(v=ws.10).aspx

Más información de servicios y puertos para los servidores Microsoft
https://www.trucoswindows.net/forowindows/temas/servicios-protocolos-y-puertos.19072/

Puertos que se requiere para el servicio SAMBA en Linux
https://blogs.itpro.es/rtejero/2014/02/11/restringir-el-trafico-rpc-de-los-controladores-de-dominio-a-un-puerto-o-puertos-determinados/

Cómo funcionan los puertos RPC
https://blogs.itpro.es/rtejero/2014/02/11/restringir-el-trafico-rpc-de-los-controladores-de-dominio-a-un-puerto-o-puertos-determinados/

Ver el tipo de DFS que se tiene
https://blogs.itpro.es/rtejero/2014/09/08/replica-de-sysvol-con-dfs-r-o-con-frs-cual-tengo-yo-activada/

Particiones Active Directory
La base de datos Active Directory está dividida en varias particiones lógicas:

- **Esquema**: esta partición contiene todas las clases de objetos y atributos que es posible crear en el directorio Active Directory. Esta partición es única en el bosque y se replica en el conjunto de los controladores de dominio.
- **Configuración**, esta partición contiene toda la información sobre los dominios, los sitios, la programación de replicaciones y la topología del bosque. Esta partición es única en el bosque y se replica en el conjunto de los controladores de dominio.
- **Dominio**: esta partición contiene todos los objetos que existen en un dominio. Cada dominio posee su propia partición de dominio.

Proceso para autenticar un usuario:

1. El usuario se autentica en el dominio y la información de conexión se registra en un controlador de dominio.
2. El servidor Kerberos valida la información comunicada por el diente y le devuelve un token de acceso también llamado TGT.
3. El servidor de autenticación emite una solicitud Kerberos presentando el TGT del usuario a un controlador de dominio.
1. 4 El controlador de dominio responde al usuario comunicándole un TGS.
4. El usuario presenta el TGS al servidor de archivos que valida. a continuación, el acceso del usuario.
5. El usuario puede en adelante abrir los recursos disponibles en el servidor de archivos.

Solución:

1. Crear los objetos para el servicio AD y SAMBA

Paso 1 – Requisitos previos

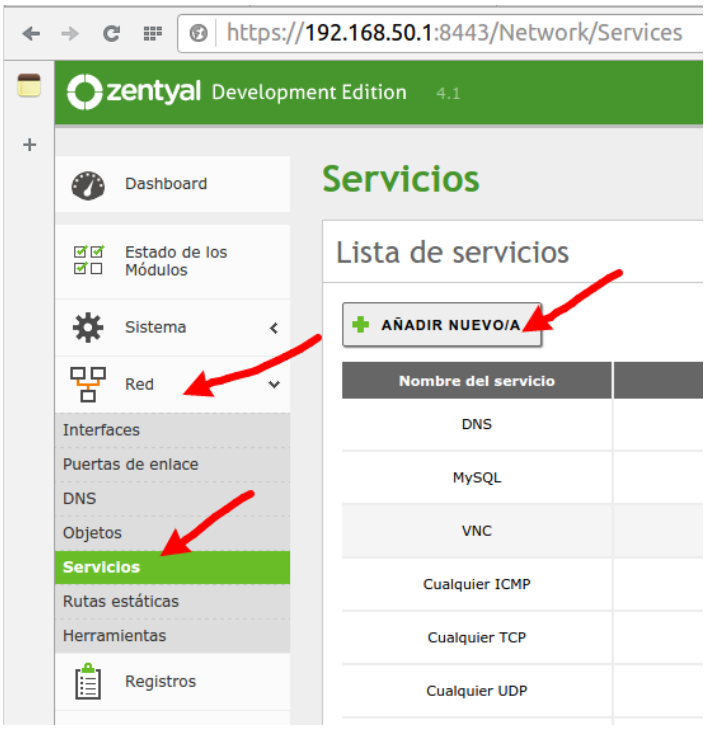
Es necesario que se cuente con:

- Conexión libre a Internet.
- El router **srvext** instalado y configurado correctamente.
- El DC "Cotrolador de Dominio" **srvint** instalado correctamente.
- Al menos dos clientes Windows 7.
- Haber conectado un cliente Windows 7 en el segmento de la red LAN01
- Comunicación entre las dos redes.

Paso 2 – Agregar los servicios requeridos

2.1 Ingrese a la aplicación web del equipo **srvext**
En la consola del sistema: usuario1/123456 (el usuario con el cual se instaló Zentyal)
En la herramienta web: administrador/123456

2.2 Seleccione el menú "**Red**"
2.3 Seleccione "**Servicios**"
2.4 Dar un clic en el botón "**+ Añadir nuevo/nueva**"



2.5 Nombrar el nuevo objeto servicio

Nota: Se agruparán los servicios de AD y Samba para facilitar la administración.

Completar el formulario con los siguientes datos:

- Nombre del servicio: AD y Samba
- Descripción: Active Directory y Sam

2.6 Dar clic en botón "**+ Añadir**"

2.7 Seleccionar el botón "Configuración"

Nombre del servicio	Descripción	Configuración
DNS	Servicio de Resolución de Nombres	
MySQL	Servidor MySQL o MariaDB	
VNC	Servicio de pantalla	
AD y SAMBA	Active Directory y SAMBA	
Cualquier ICMP	Cualquier paquete ICMP	
Cualquier TCP	Cualquier puerto TCP	
Cualquier UDP	Cualquier puerto UDP	
Cualquiera	Cualquier protocolo y puerto	
DHCP	Protocolo de Configuración de Máquinas Dinámico	

2.8 Agregar los puertos

Debido a que el Active Directory y el servidor SAMBA requieren varios protocolos, se crearán los servicios listados en el siguiente cuadro.

Los siguientes cuadros han sido generados a partir de la información disponible en: https://technet.microsoft.com/es-es/library/dd772723(v=ws.10).aspx

Autenticación de usuarios y equipos		
Protocolo	**Puerto**	**Servicio**
TCP y UDP	53	DNS
TCP y UDP	88	Kerberos
UDP	389	LDAP
TCP y UDP	445	SMB/CIFS/SMB2
TCP dinámico		RPC

Catálogo global		
Protocolo	**Puerto**	**Servicio**
TCP	3268	GC
TCP	3269	GC SSL

Directivas de grupo		
Protocolo	**Puerto**	**Servicio**
TCP	389	LDAP
TCP	345	SMB
TCP y UDP dinámicos		DCOM, RPC, EPM

Servicios web de Active Directory		
Protocolo	Puerto	Servicio
TCP	9389	SOAP

Relaciones de Confianza		
Protocolo	**Puerto**	**Servicio**
TCP y UDP	53	DNS
TCP y UDP	88	Kerberos
UDP	138	Servicio de datagramas de NetBIOS
TCP y UDP	389	LDAP
TCP-NP y UDP-NP	445	Administrador de cuentas de seguridad (SAM), LSA
TCP	636	LDAP SSL
TCP	3268	GC
TCP	3269	GC SSL
TCP	135, 49152–65535	RPC, EPM

DFS – Sistema de archivos distribuido		
Protocolo	Puerto	Servicio
TCP, UDP	138	Servicio de Datagrama de NetBIOS
TCP	139	Servicio de Sesión NetBIOS
TCP, UDP	389	Servidor LDAP

TCP	445	SMB
TCP	135	RPC
TCP	Aleatorio	Puertos altos TCP asignados aleatoriamente

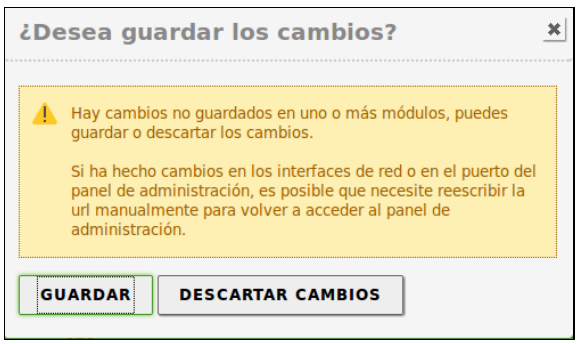
Cuadro No. 1 Listado de puertos y servicios para el servicio AD y Samba

Al final los puertos deberán aparecer de la siguiente manera:

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	53
TCP/UDP	cualquiera	88
TCP	cualquiera	135
UDP	cualquiera	137:138
TCP	cualquiera	139
TCP/UDP	cualquiera	389
TCP	cualquiera	445
TCP/UDP	cualquiera	464
TCP	cualquiera	636
TCP	cualquiera	1024
TCP	cualquiera	3268:3269

2.8 Dar clic en botón guardar

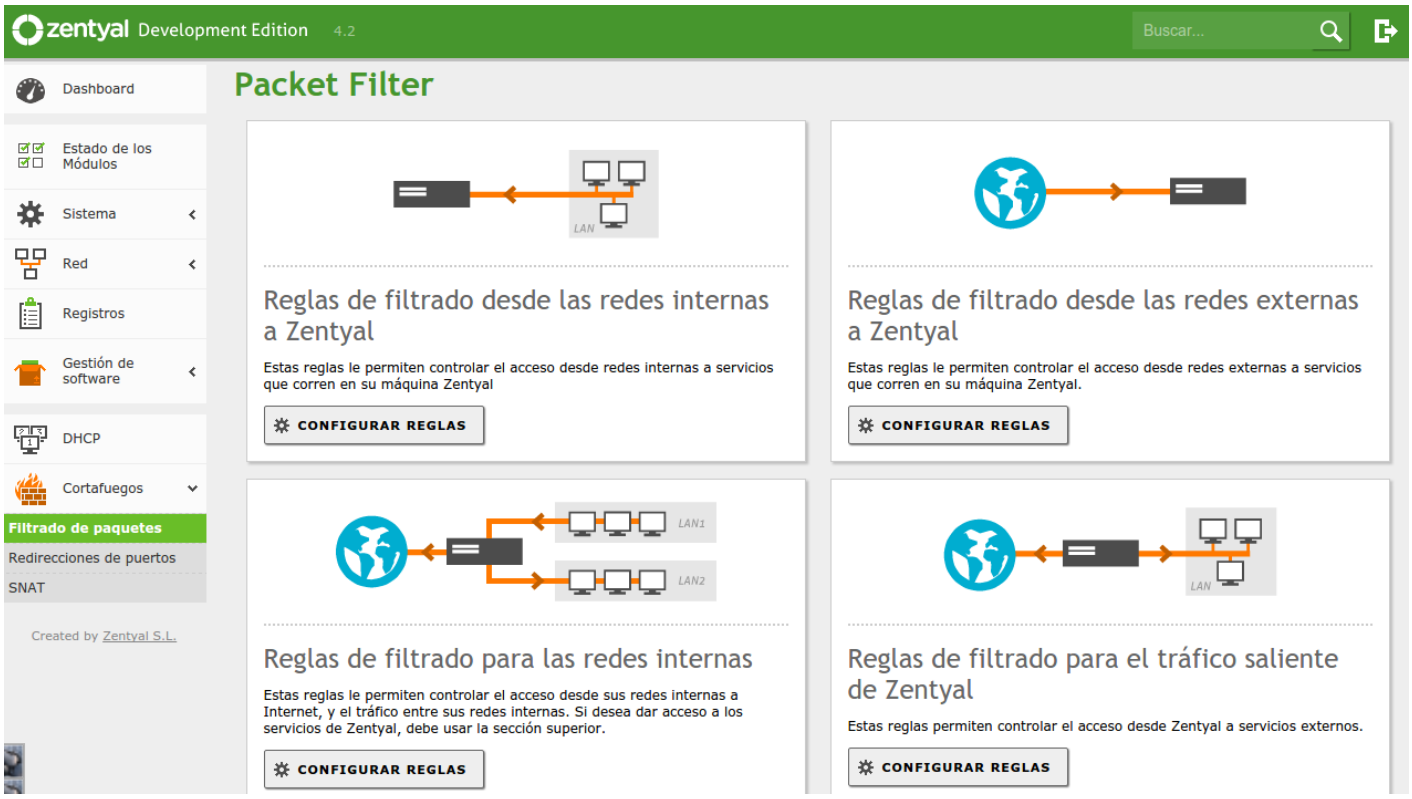
2.9 Confirmar los cambios



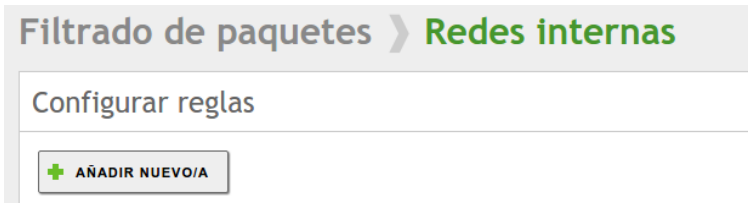
Paso 3 – Crear las reglas del firewall

3.1 Expandir el menú “Cortafuegos”

3.2 Dar clic en botón “Configurar reglas” de la opción “Reglas de filtrado para las redes internas”

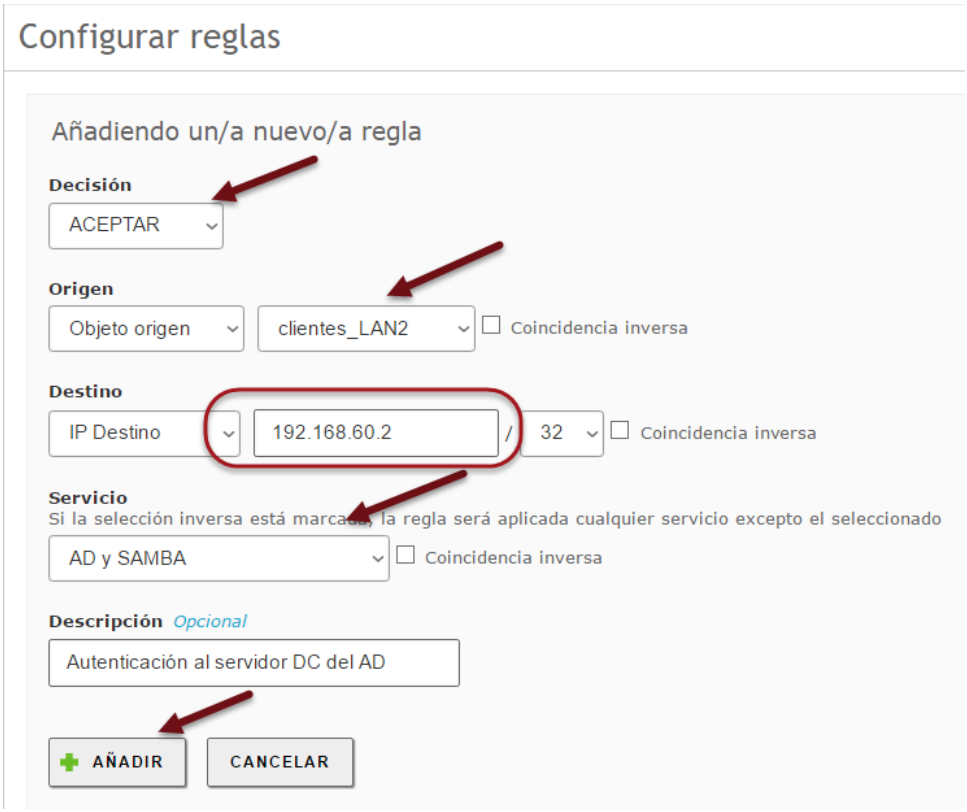


3.4 Dar clic en el botón “+ Añadir nuevo/a”



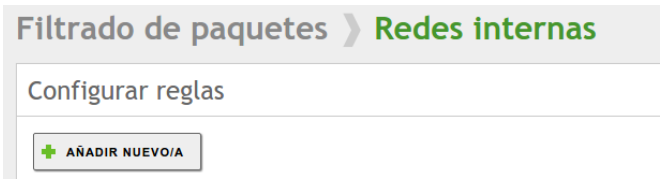
3.5 Definir las opciones de la regla de conexión desde los clientes al servidor srvint para AD y SMB

- Tipo de permiso: Aceptar (permitir)
- Tráfico origen: clientes_LAN2 (o bien la red 192.168.50.0/24)
- Tráfico destino: 192.168.60.2/32
- Servicio: AD y SAMBA (creado previamente)
- Descripción: Autenticación al servidor DC



3.6 Dar clic en el botón “+Añadir”

3.7 Dar clic en el botón “+ Añadir nuevo/a”



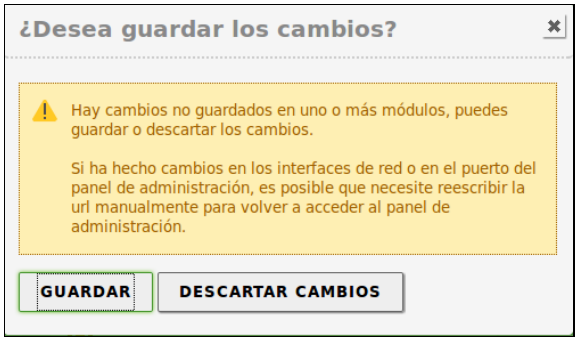
3.8 Definir las opciones de la regla de conexión desde el DC hacia los clientes AD

- Tipo de permiso: Aceptar (permitir)
- Tráfico origen: 192.168.60.2/24
- Tráfico destino: clientes_LAN2 (o bien 192.168.50.0/24)
- Servicio: AD y SAMBA (creado previamente)
- Descripción: Respuesta de autenticación de DC del AD hacia clientes LAN2

3.9 Verificar que se hayan creado las reglas

3.10 Dar clic en botón guardar

3.11 Confirmar los cambios



Paso 4 - Establecer comunicación desde los clientes de la red LAN02 al DC

4.1 Verificar la comunicación desde el cliente05 (equipo Windows 7)

```
C:\Users\usuario1\Desktop>ipconfig

Configuración IP de Windows
Adaptador de Ethernet Lan0:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.50.15
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.50.1
   Sufijo DNS específico para la conexión. . :  empresay.com.sv

C:\Users\usuario1\Desktop>ping 192.168.50.1 -n 2

Haciendo ping a 192.168.50.1 con 32 bytes de datos:
Respuesta desde 192.168.50.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.50.1: bytes=32 tiempo<1m TTL=64


C:\Users\usuario1\Desktop>ping 192.168.60.1 -n 2

Haciendo ping a 192.168.60.1 con 32 bytes de datos:
Respuesta desde 192.168.60.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.60.1: bytes=32 tiempo<1m TTL=64
. . .

C:\Users\usuario1\Desktop>ping 192.168.60.2 -n 2

Haciendo ping a 192.168.60.2 con 32 bytes de datos:
Respuesta desde 192.168.60.2: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.60.2: bytes=32 tiempo<1m TTL=63
. . .
```

4.2 Verificar la resolución de nombres

```
C:\Users\usuario1\Desktop>nslookup empresay.com.sv
Servidor:  srvint.empresay.com.sv
Address:  192.168.60.2

Nombre:  empresay.com.sv
Address:  192.168.60.2


C:\Users\usuario1\Desktop>ping empresay.com.sv -n 2
```

```
Haciendo ping a empresay.com.sv [192.168.60.2] con 32 bytes de datos:
Respuesta desde 192.168.60.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.60.2: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 192.168.60.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Nota si tiene problemas de comunicación utilizando el DHCP, utilice una dirección IPv4 estática de la red LAN02

Paso 5 – Verificar la conexión a la base de datos LDAP del DC desde la red LAN02

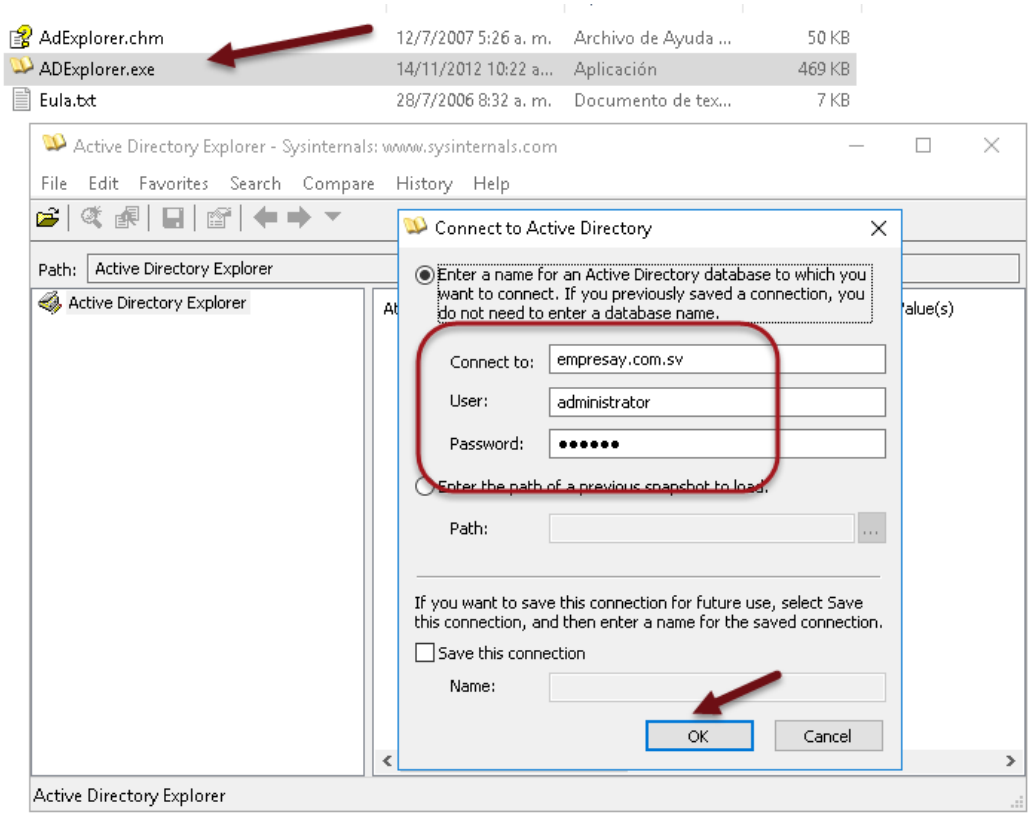
Para verificar que existe comunicación se deberá utilizar el programa ADExplorer disponible en: https://technet.microsoft.com/en-us/sysinternals/adexplorer.aspx

5.1 Descargue el programa ADExplorer

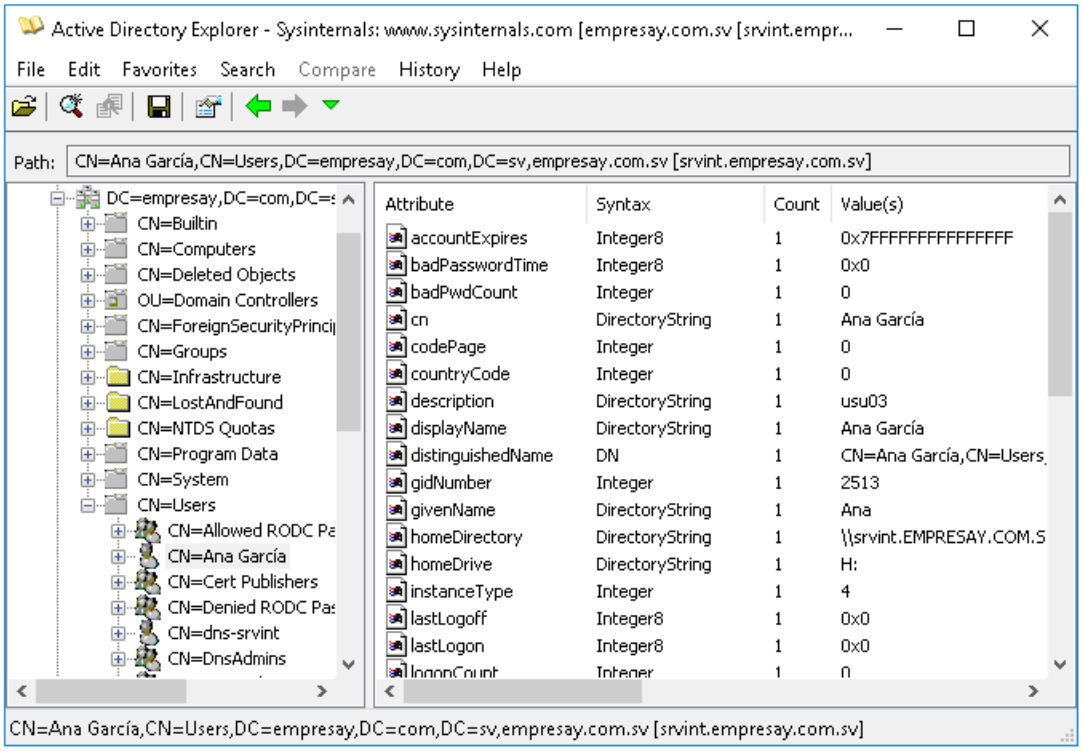
5.2 complete la pantalla de autenticación

- Connect to: **empresay.com.sv**
- User: **administrator**
- Password: **123456**

5.3 Dar un clic en el botón “OK”



5.4 Verifique que se ha conectado.



Nota: Si existe un problema para autenticarse y ver la base de datos, verifique las reglas de filtrado.

2. Establecer comunicación desde los clientes de la LAN2

Paso 1 Abra la herramienta de conexión al AD

Panel de control / Sistema / Configuración avanzada del sistema

Paso 2 – Seleccionar la ficha "Nombre de equipo" de Propiedades del Sistema

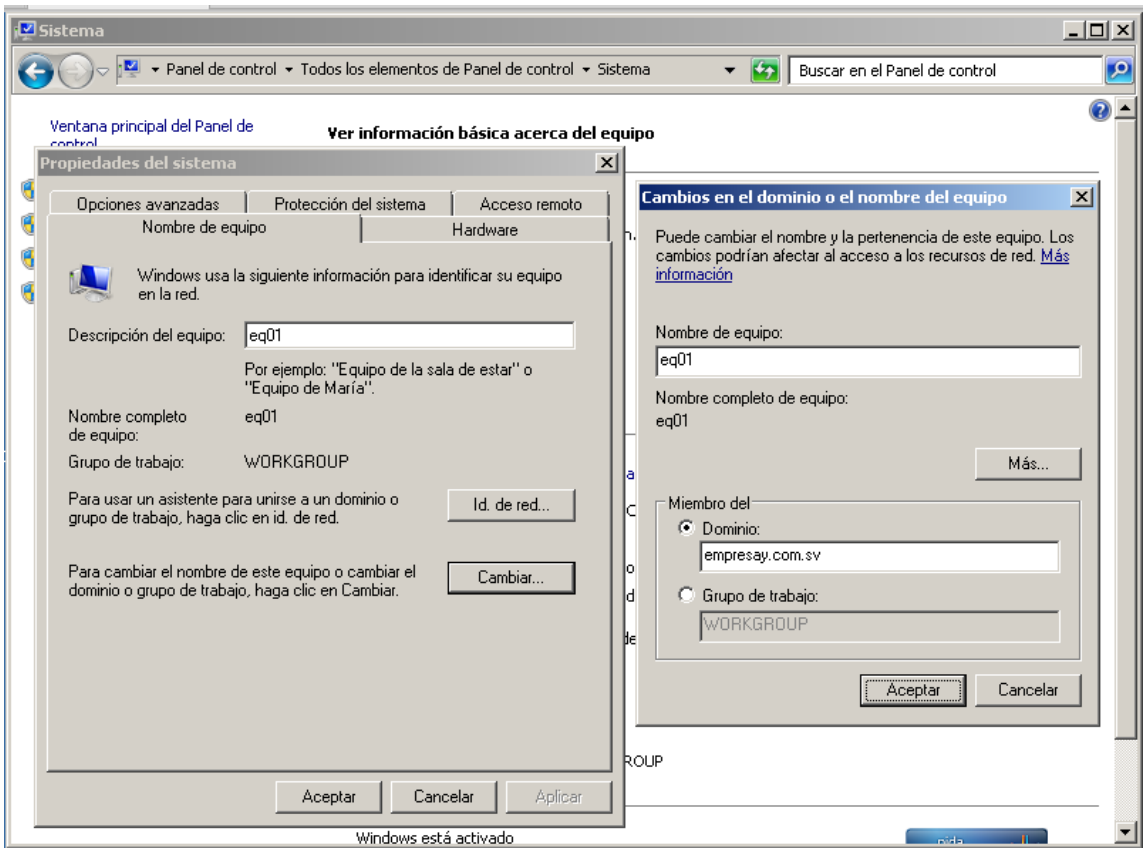
2.1 Dar clic en botón "Cambiar"

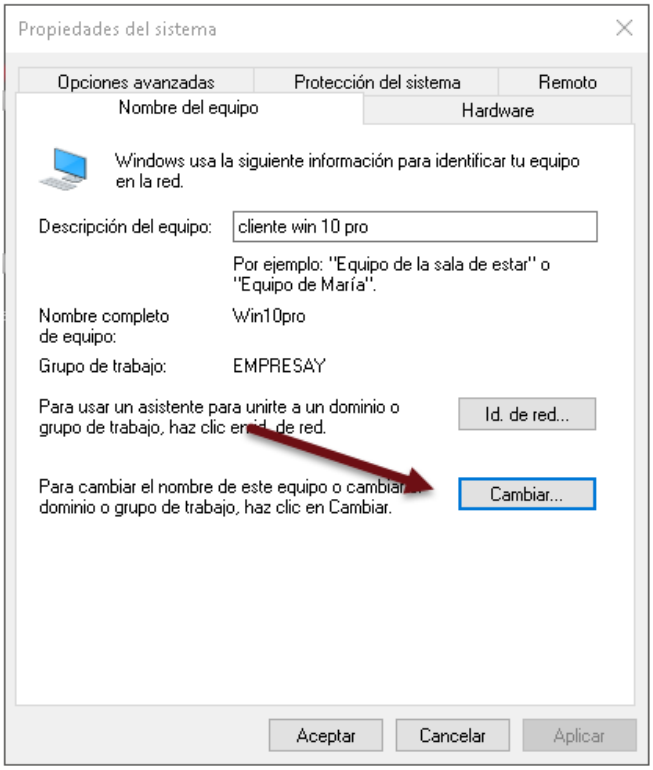
2.2 Activar la opción Dominio

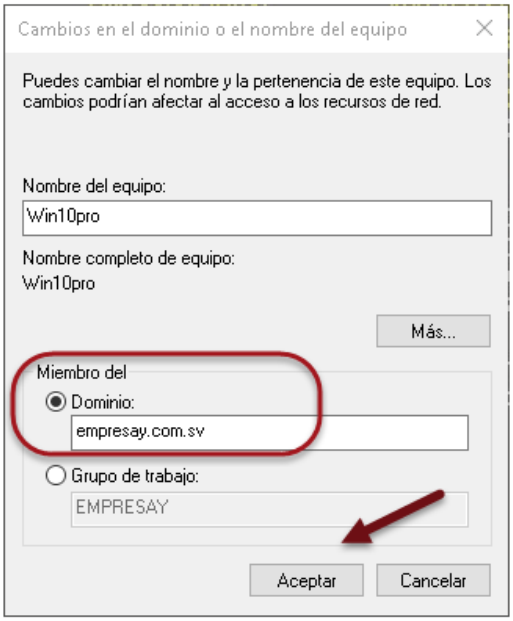
2.3 Escribir el nombre del dominio: **empresay.com.sv**

2.4 Dar clic en el botón "**Aceptar**"

A continuación, se muestran las pantallas para Windows 7 profesional y Windows 10 profesional respectivamente.

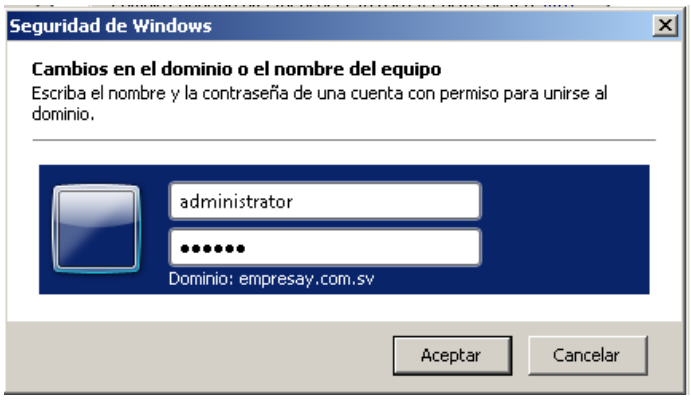


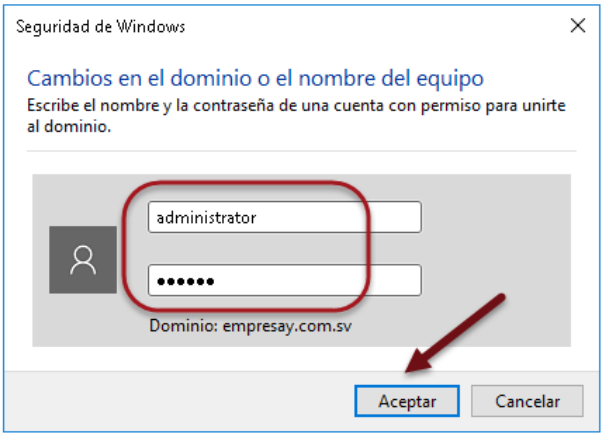




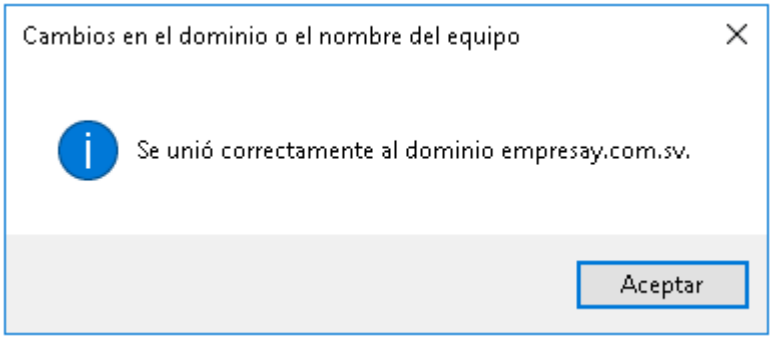
2.5 Definir la cuenta con privilegios para la administración del AD
Si proceso de comunicación es correcto parecerá una pantalla para colocar las credenciales del usuario con privilegios de administración.

Usuario: **admiistrator**
Contraseña: **123456**

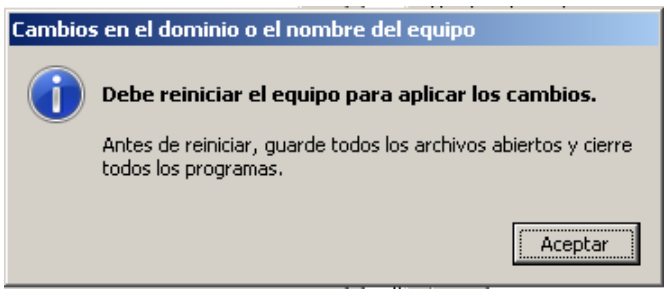


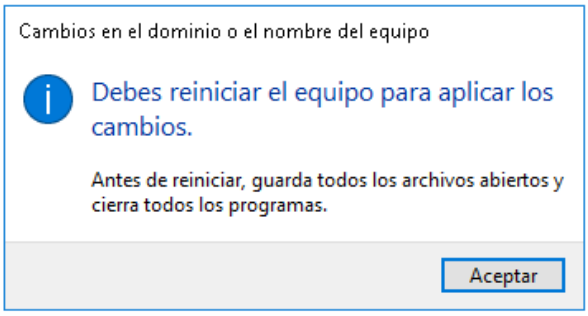


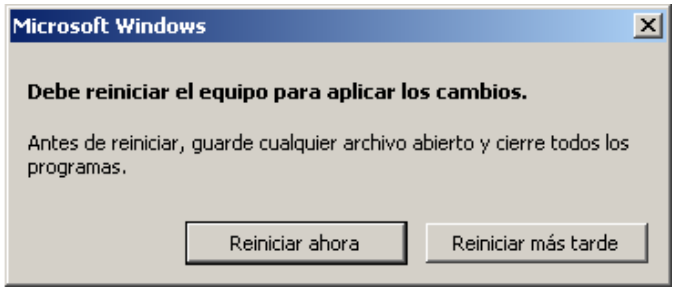
Nota: si no aparece la pantalla de autenticación, puede que existan problemas de configuración IPv4, de resolución de nombres, de firewall, Mala configuración del AD, falta de contraseña del usuario administrator, etc.

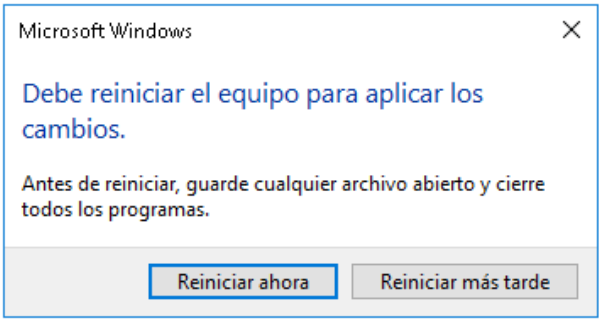


2.6 Reinicie el equipo para ingresar al dominio

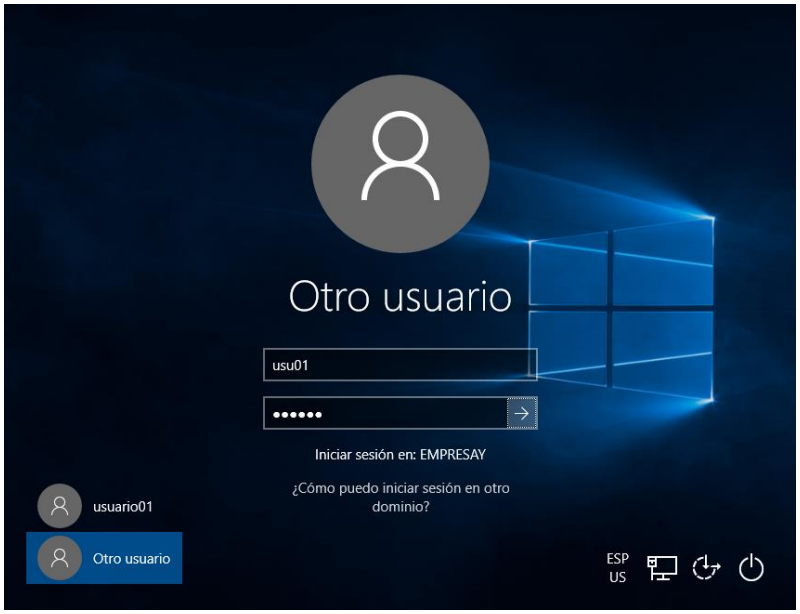








2.8 Verifique el ingreso.



Paso 3 - Ingrese con los usuarios del dominio

Para probar de acceso

No.	Nombre de usuario	Nombre	Apellido	Descripción	Contraseña	Grupo
1	usu01	Juan	Pérez	Usu01	123456	ventas
2	usu02	Pedro	Pobre	Usu02	123456	ventas
3	usu03	Ana	García	Usu03	123456	ventas
4	usu04	Ricardo	Tapia	Usu04	123456	compras
5	usu05	Bruno	Díaz	Usu05	123456	compras
6	usu06	Bárbara	Gordon	Usu06	123456	compras
7	usu07	Libre	Libre	Usu07	123456	bodega
8	usu08	Libre	Libre	Usua08	123456	bodega
9	usu09	Libre	Libre	Usu09	123456	bodega