Guía de Infraestructura Tecnológica con Windows Server 2012
Un Enfoque Empresarial

Alfonso Aníbal Gujarro Rodríguez
Fausto Raúl Orozco Lara
Miguel Alfonso Molina Calderón
Johana Elisabeth Trejo Alarcón

compAs

Guía de Infraestructura Tecnológica con Windows Server 2012 Un Enfoque Empresarial

Autores:

Alfonso Aníbal Guijarro Rodríguez
Fausto Raúl Orozco Lara
Miguel Alfonso Molina Calderón
Johana Elisabeth Trejo Alarcón

Guía de Infraestructura Tecnológica con
Windows Server 2012
Un Enfoque Empresarial

Autores:
Alfonso Aníbal Guijarro Rodríguez
Fausto Raúl Orozco Lara
Miguel Alfonso Molina Calderón
Johana Elisabeth Trejo Alarcón

Primera edición: diciembre 2018

ISBN: 978-9942-33-083-3

Diseño de portada y diagramación:
Grupo Compás
Este texto ha sido sometido a un proceso de evaluación por pares externos
con base en la normativa del editorial

Cita.
Guijarro, A, Orozco, F, Molina, M, Trejo, J (2018) Guía de Infraestructura Tecnológica con Windows Server 2012. Un Enfoque Empresarial, Editorial Grupo Compás, Guayaquil Ecuador, 298 pag

Tabla de Contenido

Unidad I

Generalidades Windows Server 2012

Unidad II

Windows Server 2012

Unidad III

Active Directory Servicios de dominio y Administración de objetos

Unidad IV

Servidor DHCP

Unidad V
Configuraciones de Red y Servidores DNS

Unidad VI
Servidores de Archivos
DFS y NTFS

Unidad VII
GPO Directivas de Grupo

Unidad VIII
Política de Seguridad
Implementando GPO

Unidad IX
Monitorización y Seguimiento del Servidor

Unidad X
WSUS distribución y administración de actualizaciones

Unidad XI
Zona Desmilitarizada

Unidad XII
Zona WAN Firewall Endian

Tabla de Figuras

Unidad

I

Unidad I

Generalidades Windows Server 2012

1. Introducción

Windows Server 2012, probablemente sea la versión más importante en la plataforma de servidores realizada por Microsoft y presentada oficialmente en septiembre del año 2012, este sistema operativo, incorpora la experiencia de implementación y ejecución en la nube, para servicios públicos o privados en los soporte de los servidores. Windows Server 2012, brinda a los clientes una arquitectura en la nube múltiples, escalable y dinámica que ayuda a los usuarios a conectarse a través de diferentes locaciones.

Como parte de las implementaciones de TI (Tecnología de información), responde con mayor eficiencia y agilidad a las necesidades de trabajo y negocio se puede acceder a entornos de trabajo personalizados desde cualquier lugar, cuenta con una nueva interfaz de usuario innovadora, potentes herramientas de administración, compatibilidad mejorada con Windows PowerShell, almacenamiento, virtualización y cientos de nuevas características, trabaja en redes, Windows Server 2012 puede ayudar a ofrecer más servicios en el menor tiempo, reduciendo los costos de implementación.

También se diseñó para la nube desde cero y proporciona una base para la creación de soluciones en nube tanto públicas como privadas para que las empresas puedan aprovechar los numerosos beneficios que este servicio ofrece (Mitch Tulloch & Anne Hamilton, 2012).

El sistema podrá administrar grandes servidores de nubes públicas, hasta servidores de pequeñas nubes privadas, las funciones de virtualización son a través Hipervisor (Hyper-V Versión 3), no es solo una característica de sistema operativo sino parte integral de la manera de hacer despliegue con la arquitectura de Windows Server. Desde la perspectiva de la escalabilidad, la infraestructura de TI, ha considerado que el sistema podrá soportar 4 Teras de RAM y 640 procesadores lógicos, mientras que en las capacidades de virtualización se asignará 160 procesadores virtuales y con una memoria de 512 GB a cada máquina virtual y disponibilidad con un hipervisor versión 3, de igual manera han confirmado que no funcionaran las máquinas virtuales con arquitecturas de 32 bits ni en procesadores Itanium. Por último tenemos que destacar las innovaciones las capas de almacenamiento, con una nueva mejora en la gestión de archivos en el sistema tales como el Resilient File System

(ReFS) y el NTFS en Windows Server 2012, con mayor fiabilidad en estructuras de disco, compatibilidad con APIs, elasticidad y recuperaciones integradas, tecnologías existentes. (Lello, 2012)

Este libro proporciona una descripción técnica de Windows Server 2012 y está destinado a ayudar a los profesionales de TI a familiarizarse con las capacidades de la plataforma.

1.1. Historia

En una revisión rápida se encuentra que el primer Windows Server fue lanzado en febrero 17 del año 2000 con una modificación de nomenclatura para el sistema NT. Así, mismo Windows 5.0 NT pasó a ser conocido como Windows 2000. Luego fue sustituido por Windows XP para computadoras de escritorios en octubre del año 2001, luego se lanza Microsoft Windows Server 2003 en abril 2003 para servidores; su creación representa un empeño para la unión entre los dos sistemas operativos distintos como Windows NT y Windows 9x. Luego de esto Salió Windows 2008 Server el cual fue conocido como Windows Server "Longhorn" hasta mayo 16 del 2007, cuando Bill Gates informo el título oficial (Windows 2008 Server) el cual fue lanzado febrero 27 del 2008. (Rodríguez V. , 2015)

Posterior a eso se desarrolla por su nombre representativo que lanzo Microsoft conocido como Windows Server 8. No obstante en abril 17 del 2012 la compañía dio a conocer el nombre oficial del software Windows Server 2012. La versión primera de Microsoft Windows Server 2012 nombrada como Developer Preview, dirigida a los desarrolladores, habilitado para suscriptores de MSDN. Desde ese entonces ya estaban presentes la interfaz de usuario, así como el Administrador de Servidores (para la aplicación gráfica utilizada para administración de servidores) además se cuenta con características nuevas.

En febrero 16 de 2012 Microsoft, dio a conocer que la edición del sistema Developer Preview, que una vez instalada con ciertas actualizaciones, expiraría el enero 15 del 2013 en lugar de la fecha prevista inicialmente en abril 08 del 2012. En enero 13 de 2102 se lanzó la construcción 8180 la cual comprendían la versión del sistema Developer Preview, lo cual contenían algunas revisiones a la interfaz del

Administrador de Servidores y los Espacios de Almacenamiento. (Mitch Tulloch & Anne Hamilton, 2012)

En febrero 29 del 2012 microsoft, lanzó versión beta Windows 8 para consumidores, a diferencia del software Developer Preview, los Consumidores Preview lanzó Windows Server 2012 para el público. La versión del lanzamiento Release Candidate (RC), Windows Server 2012 publicado en mayo 31 del 2012, junto RC con la versión Release Preview Windows 8. La última versión para la elaboración (RTM) publicado en agosto 1 del 2012 y estuvo a disposición general en septiembre 04 del 2012. Finalmente Windows Server 2016 actualmente existe más versiones Windows Server pero por ahora nos enfocaremos solo en Windows Server 2012. La figura 1.1 da a conocer algunas interfaces de Windows server.

Figura 1. 1 Interfaz Gráfica Windows Server

1.2. Roles y Características

1.2.1. Roles

(Zambrano, 2015) los roles se utilizan para organizar la funcionalidad del sistema operativo, las funciones principales del servidor, los servicios con los que cuenta, que puede ser llamados como servicios de rol y pueden ser necesarios en servicios específicos. Por ejemplo DHCP o DNS no se necesitan servicio adicional, en el archivo de servicio que compone entre otros servicios adicionales. La idea es que el rol elegido se encargue exclusivamente de los programas necesarios.

Los roles disponibles para Windows Server 2012 son los siguientes:

- ✓ Acceso remoto.
- ✓ Servidor DNS.
- ✓ Servidor DHCP.
- ✓ Servidor Web.
- ✓ Gestión de servicios derechos de Active Directory.
- ✓ Servicio de acceso y directiva de redes.
- ✓ Servicios de escritorio remoto.
- ✓ Hipervisor (Hyper-V).
- ✓ Servidor de Fax.
- ✓ Servidor de aplicaciones.
- ✓ Servicios de actualización de Windows Server.
- ✓ Servidor Volumen Activación Servicios.
- ✓ Servicio de certificados de Active Directory.
- ✓ Servicios de impresión y documentos.
- ✓ Servicios de directorio ligero de Active Directory.
- ✓ Servidor Active Directory de dominio.
- ✓ Implementación de servicios en Windows.
- ✓ Servicios de archivos y almacenamientos.

(Patricia Gonzalez, 2015) contribuye con otra definición sobre un rol, en el cual podemos definir que un rol consiste en una función principal de

un servidor, en este se puede instalar uno o varios roles según decidan los administradores del sistema, dejando en claro que cada rol puede incluir uno o varios servicios de instalación opcionales.

En cuanto a las direcciones IP, se puedes elegir de un grupo de direcciones que son determinados por el administrador, de esta forma ningún cliente puede tener acceso o disponer de una IP duplicada. A continuación se definen algunas definiciones de roles que brinda Windows server para un ambiente de producción.

1.2.2. Rol del servidor DNS

El rol de un servidor DNS, es considerado como un sistema para asignar servicios de red y nombres a equipos que organizan dichos nombres en un dominio de jerarquía, tal como se muestra en la figura 1.2. La asignación del servicio de DNS, se puede emplear en las redes TCP/IP como Internet, cuando busca un dominio o el nombre de un equipos mediante los nombres descriptivos. También es utilizado cuando un usuario especifica el DNS de un algún equipo dentro de una aplicación, los clientes y los servidores DNS cooperan para realizar la búsqueda más rápido por nombre, y esta se asocia a la información del equipo, como su dirección IP o los servicios que presta a la red. Este proceso se denomina como resoluciones de nombres. (Patricia Gonzalez, 2015)

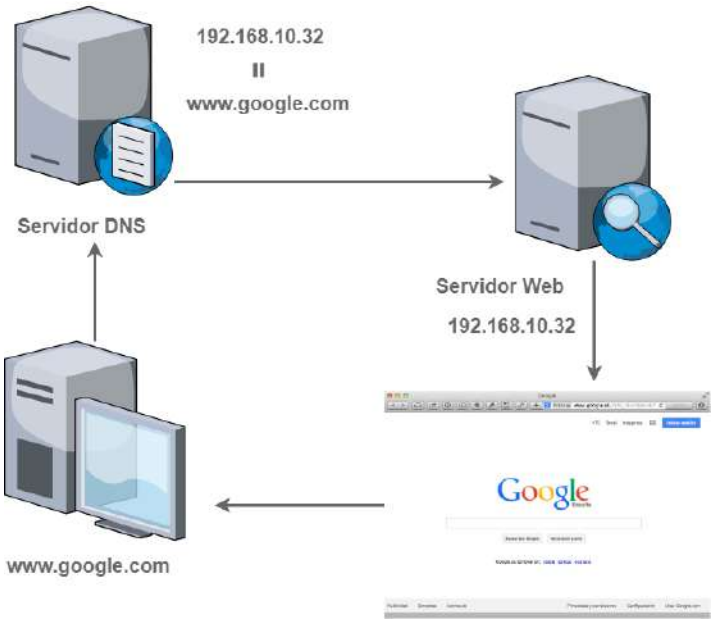


Figura 1. 2: Servidor DNS

1.2.3. Servidor DHCP

DHCP, es en realidad una herramienta de distribuciones de direcciones IP de red diseñada para trabajar sobre TCP (Protocolo de control de transmisión) y el IP (Protocolo de Internet), estos dos protocolos forman TCP/IP que se utilizan para conectar dispositivos en una red, es común emplearlos en las redes cuando el tamaño de los host aumenta, un ejemplo claro en una red corporativa tal como se muestra en la figura 1.3.

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red. (Smith, 2018)

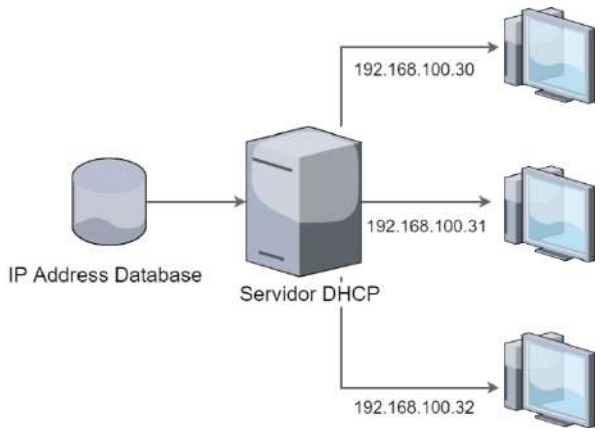


Figura 1. 3: Servidor DHCP

1.2.4. Servidor Web (IIS)

El rol del servidor web, conocido en los productos Microsoft como el servicio de IIS (Internet Information Service) o comúnmente llamado servicio Web, este nos proporciona una plataforma extensible, modular, segura y fácil de administrar para el albergue seguro de servicios, sitios web y aplicaciones. El IIS 8 puede compartir información entre los usuarios del Internet, como por ejemplo un extranet o intranet ver figura 1.4. Además es considerada como una plataforma web con la unión que integra ASP.NET, IIS, PHP, servicios de FTP y Windows Communication Foundation (WCF).

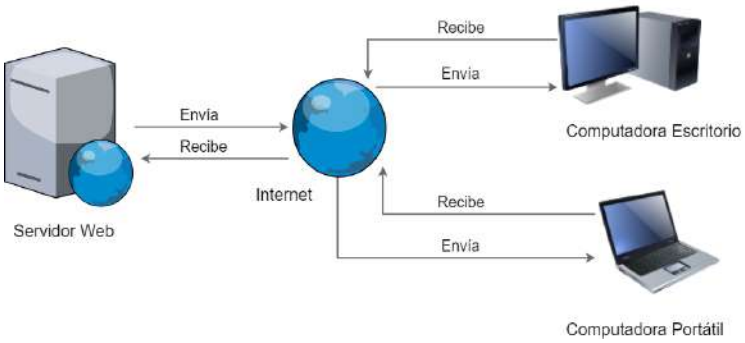


Figura 1. 4: Servidor Web

1.2.5. Window Server Update Services

WSUS en español Servicios de actualizaciones de Windows Server, nos permite que los administradores de información de las tecnologías desarrollen actualizaciones más recientes en el software de Microsoft en los equipos del sistema operativo ver figura 1.5. Mediante WSUS, los administradores pueden establecer actualizaciones a través de equipos conectando a la red.

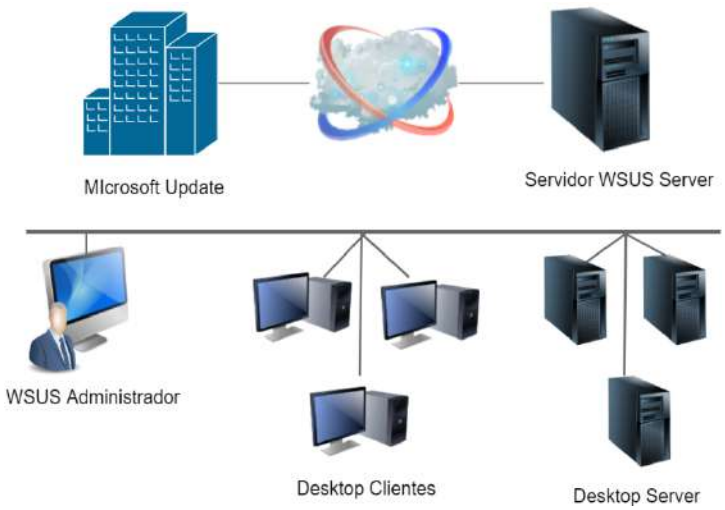


Figura 1. 5: Servicios de actualizaciones de Windows

1.2.6. Servicios de impresión y documentación

Este es otro de los servicios de mayor demanda en los servidores de Microsoft, permite compartir impresoras y escáneres en una red, es decir, configurar los servidores de digitalización e impresión, así como centralizar las tareas de impresoras de red y la administración previa de los escáneres, también se puede realizar tareas mediante los complementos de Administración de impresión y digitalización de MMC

(Microsoft Consola de Administración), en la figura 1.6 se ilustra el concepto, estos pueden ser usados como complementos para supervisar impresoras y escáneres en la red y para digitalización de los servidores.

El rol de estos servicios incluye cuatro recursos en la cual, los tres primeros proporcionan funcionalidad a un servidor de impresión, mientras que el último Servidor distribuido de digitalización, proporciona una funcionalidad de digitalización del servidor. (Patricia Gonzalez, 2015)

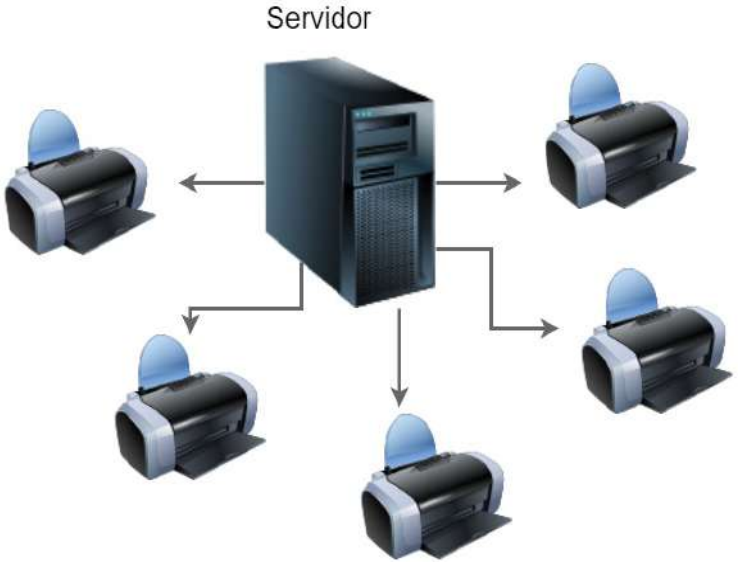


Figura 1. 6: Servicios de impresión y documentación

1.2.7. Servidor de aplicación

Servidor de aplicación ofrece la elaboración de aplicaciones de negocio basadas en servidor estas se encuentran personalizadas, el diseño de un entorno integrado permite flexibilidad a los administradores de sistema, este servicio responde a solicitudes que envían a través de las redes desde cualquier cliente remoto en la figura 1.7, se ilustra el servidor de aplicaciones.

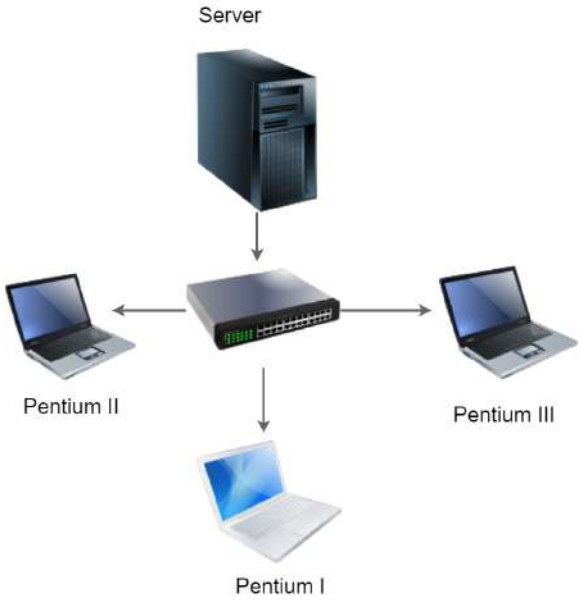


Figura 1. 7: Servidor de aplicación

1.2.8. Servicios de Directorio Activo de dominio

Conocido como el Servicio Active Directory de dominio, facilita un almacenamiento de datos distribuidos, facilita la administración de los recursos de red y las aplicaciones de directorio habilitado. El administrador puede usar el servicio Active Directory de dominio para organizar los elementos de una red especificas (por ejemplo, los equipos y usuarios) en una organización jerárquica de contención. La organización jerárquica incluye unidades organizativas de cada dominio, bosques de los dominios y Active Directory de bosquejos ver figura 1.8. Se ejecuta AD DS en el servidor conocido como controlador de dominio.

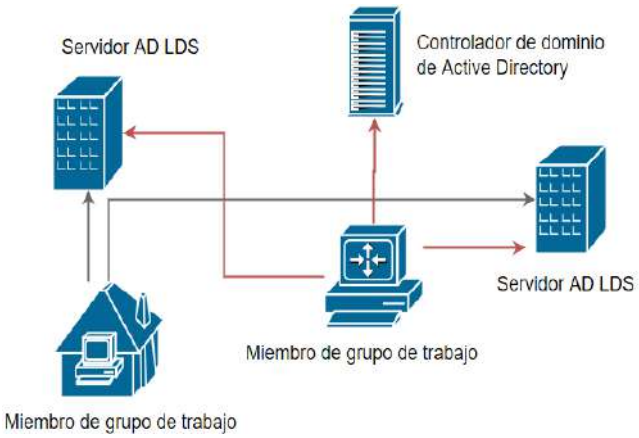


Figura 1. 8: Servidor Active Directory de dominio

1.2.9. Hyper-V

El rol Hyper-V permite crear y administrar un entorno informático de virtualización mediante la tecnología de virtualización integrada en Windows Server 2012. Hyper-V virtualiza el hardware con el fin de proporcionar un entorno en el que sea posible ejecutar varios sistemas operativos al mismo tiempo en un equipo físico, ejecuta cada uno de ellos en una propia máquina virtual.

Las máquinas virtuales implementa un Hyper-V en términos de particiones, es decir una unidad lógica de aislamiento que es admitida por un hipervisor ejecutada en cada sistema operativo invitado. Para que esto sea posible debe tener una partición primaria en una instancia de hipervisor ver la figura 1.9, el software de virtualización se ejecuta en la participación principal y tiene acceso directo a los dispositivos de hardware. (López, 2017)

Tomando en cuenta que la partición primaria crea particiones secundarias que alojan los sistemas operativos invitados utilizando la API hypercall, que es la interfaz de programación de aplicaciones expuesta por Hyper-V.

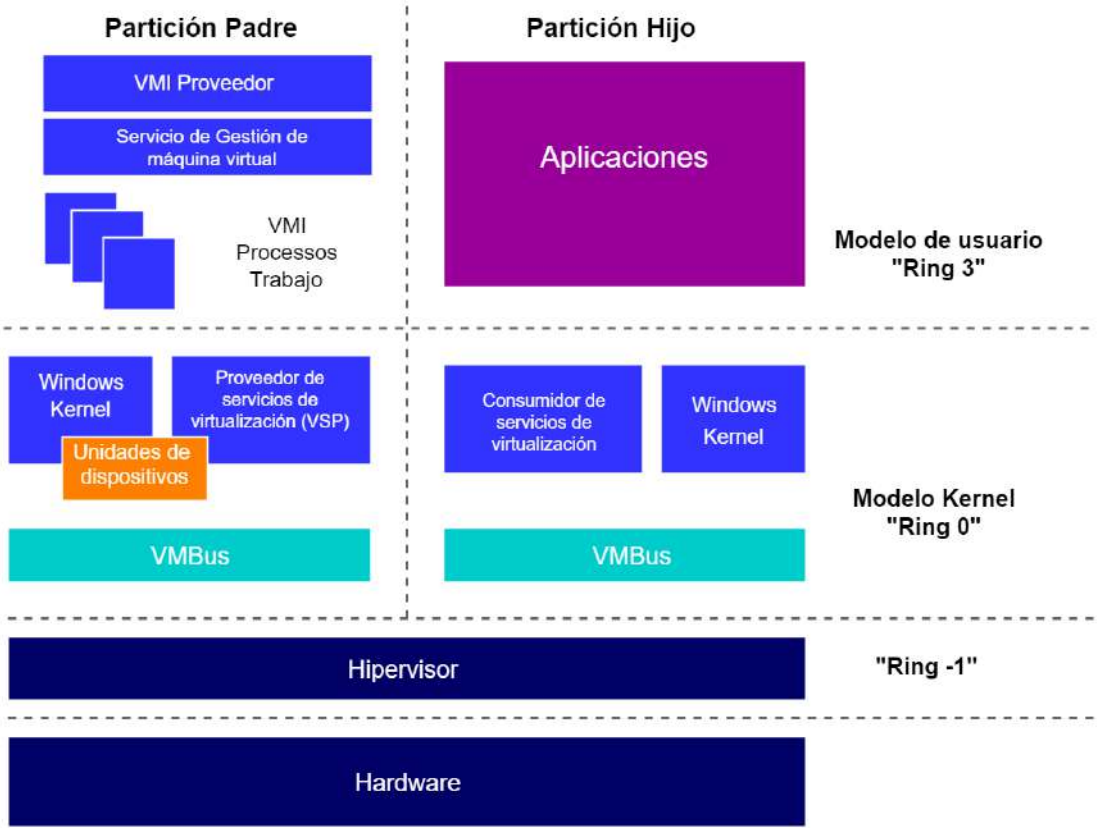


Figura 1. 1: Hyper-V

1.2.10. Servicios de directorio ligero de Active Directory (AD LDS)

Es un servicio de directorio del Protocolo ligero de acceso a directorios (LDAP) del sistema operativo Windows Server 2012, ofrece una compatibilidad flexible para aplicaciones habilitadas para el uso de directorios, sin las dependencias ni las restricciones relacionadas con los dominios de los Servicios de dominio.

AD LDS proporciona almacenamiento y recuperación de datos a aplicaciones habilitadas para el uso de directorios, sin las dependencias necesarias 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. (Microsoft, 2016)

AD LDS y AD DS pueden ejecutarse simultáneamente en la misma red. Además, AD LDS admite usuarios de grupos de trabajo y de dominio simultáneamente, como se muestra en la figura 1.10.

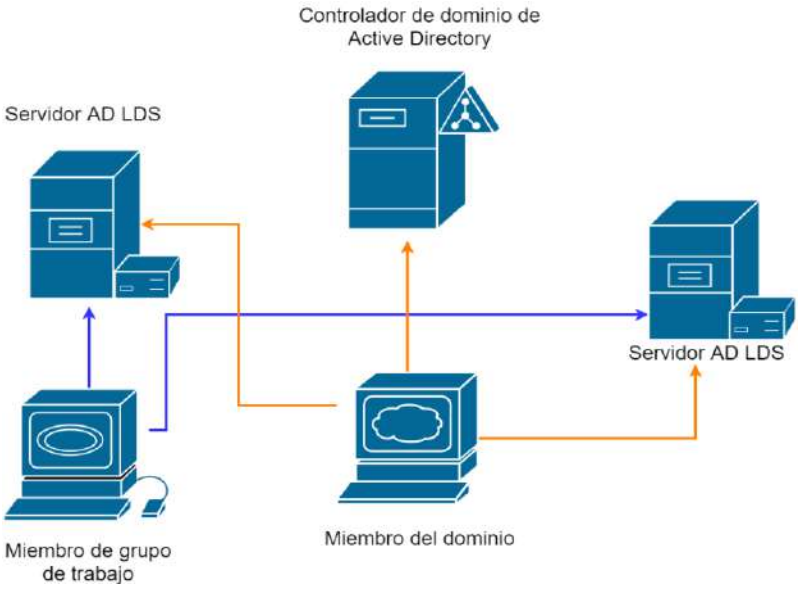


Figura 1. 2: Servicios de directorios de Active Directory

1.2.11. Servicios de archivos y almacenamiento

El rol del Servicios de archivos y almacenamiento, están instalados de forma predeterminada, pero sin servicios de rol adicionales. Esta funcionalidad permite usar el Administrador del servidor o Windows PowerShell para administrar la funcionalidad de almacenamiento de sus servidores. Sin embargo, para configurar o administrar un servidor de archivos, debemos usar el asistente para agregar roles y características en el administrador del servidor, tal como muestra la figura 1.12.

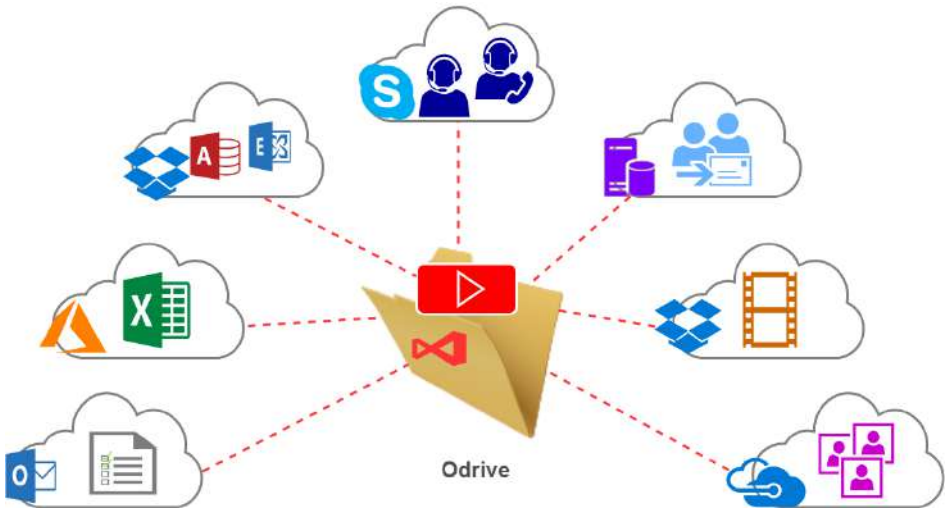


Figura 1. 3: Servidores de archivos y almacenamientos

1.3. Características

Además de los roles y servicios de roles, también están las características. Se trata de componentes independientes de las funciones del servidor, pero que pueden ser necesarios para dar apoyo a los roles. Por ejemplo, el directorio activo, es una función para determinadas instalaciones, puede ser necesario la instalación de un componente independiente llamado WINS, en este caso se trata de una características. (Zambrano, 2015)

Las características disponibles en Windows Server 2012 son:

- ✓ Microsoft .NET Framework 3.5 y Microsoft .NET Framework 4.5.
- ✓ Windows PowerShell.
- ✓ Servicio de transferencia inteligente en segundo plano (BITS).
- ✓ Cifrado de unidad BitLocker.
- ✓ Desbloqueo de BitLocker en red.
- ✓ BranchCache.
- ✓ Protocolo de puente del centro de datos.
- ✓ Clúster de conmutación por error.
- ✓ E/S de múltiples rutas.
- ✓ Equilibrio de carga de red.
- ✓ Protocolo de resolución de nombres de mismo nivel.
- ✓ Experiencia de calidad de audio y vídeo de Windows (qWave).
- ✓ Compresión diferencial remota.
- ✓ Servicios simples de TCP/IP.
- ✓ Proxy RPC sobre HTTP.

- ✓ Servidor SMTP.
- ✓ Servicio SNMP.
- ✓ Cliente Telnet.
- ✓ Servidor Telnet.
- ✓ Cliente TFTP.
- ✓ Windows Internal Database.
- ✓ Windows PowerShell Web Access.
- ✓ Administración de almacenamiento basada en directivas de Windows.
- ✓ Extensión WinRM de IIS.
- ✓ Servidor WINS.
- ✓ Compatibilidad con WoW64.
- ✓ Cliente NFS.
- ✓ Data Center bridging.
- ✓ Almacenamiento mejorado.
- ✓ Administración de directivas de grupo.
- ✓ Servidor de administración de direcciones IP.
- ✓ Cliente de impresión en Internet.
- ✓ Servicio de nombres de almacenamiento de internet (iSNS).
- ✓ Monitor de puerto LPR.
- ✓ Media Foundation.
- ✓ Message Queuing.
- ✓ NBL Equilibrio de carga de red.
- ✓ Asistencia Remota.
- ✓ RPC sobre el proxy HTTP.
- ✓ Subsistema para aplicaciones UNIX.
- ✓ Copia de seguridad de Windows Server.
- ✓ Administrador de recursos del sistema de Windows.
- ✓ Visor de XPS.

(Calderon, 2015) se refiere a que características, es un componente de software que proporciona funciones adicionales. Las características, entre las que podemos citar el cifrado de unidad BitLocker o Copias de Seguridad de Windows Server, se pueden instalar independientemente de los roles de servidor y de los servicios de rol.

Puede haber varias características instaladas en un equipo o ninguna, dependiendo de su configuración. Este tipo de funcionalidades, no tiene requerimientos ya que normalmente las características se instalan automáticamente cuando agregas un rol a la máquina como ya se ha indicado anteriormente en el proceso de instalación de los roles.

El método de instalación es muy sencillo, en la pantalla de administración del servidor, seleccionamos a agregar Rol o característica, pulsamos siguiente hasta llegar a la pantalla de características, seleccionamos la opción a instalar y damos clic al botón de instalar. A veces se requiere reiniciar la máquina para que los cambios surtan efecto, pero lo normal es que una vez finalizada la instalación, la característica esté en funcionamiento. En las cuales tenemos:

- ✓ BitLocker o unidades de codificación: Activar o desactivar el nivel de cifrado del disco o volumen.

- ✓ De conmutación por error: Se utiliza para configurar el clúster de servidores, lo que aumenta la fiabilidad, los servidores que proporcionan servidor de copia de seguridad.

- ✓ Política de Grupo de Gestión: Una consola de administración utilizada para implementar la directiva de grupo en una red de organizaciones.

- ✓ Servicios de tinta y de escritura a mano: Permite la red de apoyo a la entrada de lápiz y reconocimiento de escritura así como ecuaciones matemáticas.

- ✓ Cliente de impresión en Internet: Configurar el soporte para el usuario para conectarse e imprimir en impresoras locales o de Internet, utilizando el protocolo de impresión de Internet (IPP).

- ✓ Network Load Balancing (NLB): Se utiliza para equilibrar la carga de trabajo a través de múltiples servidores que ejecutan aplicaciones de usuario. Aplicaciones responden independientemente a cada petición del cliente, por lo que es posible que varios servidores para equilibrar las solicitudes de cliente.

- ✓ Asistencia remota: Permite el soporte a los clientes que envían las invitaciones, la prestación de asistencia a distancia, puede acceder el cliente de escritorio como si estuviera sentado en el propio ordenador.

- ✓ Herramientas de administración remota del servidor: Permite la gestión remota de los servidores que ejecutan Windows Server 2008 R2 y Windows Server 2012. También pueden administrar el servidor de Windows Server 2003 hasta que se conectan a ellos, a través de un servidor que ejecuta Windows Server 2008 R2 o Windows Server 2012.

- ✓ Simple Mail Transfer Protocol: Se utiliza para configurar un servidor para enviar mensajes.

- ✓ Cliente Telnet, el servidor Telnet: Permite la instalación de servidores de apoyo libre y utiliza el acceso a archivos a través del protocolo Telnet. El cliente Telnet se utiliza para conectarse al servidor Telnet.

- ✓ Windows PowerShell: Proporciona una interfaz de línea de comandos para ejecutar comandos o secuencias de comandos para realizar tareas administrativas.

- ✓ Seguridad de Windows Server: Utilizar para copia de seguridad de un servidor de Windows y, si es necesario, para restaurar una copia de seguridad después de un fallo del servidor.

- ✓ Administrador de recursos del sistema de Windows (WSRM) - Le permite configurar la asignación de CPU y RAM recursos tanto del servidor.

- ✓ Wireless Local Área Network Service (LAN): Configurar el servicio de LAN inalámbrica para habilitar un servidor para comunicarse mediante una tarjeta de red inalámbrica.

- ✓ Windows en Windows (WOW) 64 Soporte: Server 2012 servidor de 64 bits de Windows para utilizar esta función para permitir que las aplicaciones se ejecutan en 32 bits.

1.4. Novedades

Son muchas las novedades aportadas por esta versión de Microsoft Windows Server. (Zambrano, 2015) , las principales son:

- En relación al Directorio Activo (Active Directory) ha aumentado la posibilidad de automatización de tareas administrativas gracias al uso de los scripts.
- Posibilidad de cifrado del espacio de disco duro utilizado y no solo el cifrado de todo el volumen.
- Administración de direcciones IP, conocido como IPAM, es una nueva característica que aporta la posibilidad de supervisar y administrar de manera, personalizada una infraestructura basada en direcciones IP.
- Microsoft Internet Explorer 10.

Bibliografía

Calderon, J. M. (16 de Febrero de 2015). Roles y características de Windows server 2012 R2. Obtenido de http://administraciondesistemaoperativo. com/2014/11/roles-y-caracteristicas-de-windows.html

Lello, R. D. (27 de Abril de 2012). Windows Server 2012. Obtenido de http://www.radians.com.ar/?p=1644

López, J. M. (06 de Enero de 2017). Hyper-V, la máquina virtual de Microsoft. Obtenido de https://hipertextual.com/2017/01/hyper-v-maquina-virtual-microsoft

Microsoft. (19 de Agosto de 2016). Introducción a AD LDS. Obtenido de http://forsenergy.com/es-es/adam/html/d2b337b3-47e7-458c-b5a4-9e3d14a08078.htm

Mitch Tulloch & Anne Hamilton. (2012). Introducing Windows Server 2012 (Vol. I). (V. Woolley, Ed.) Washington: Diane Kohnen, S4Carlisle Publishing Services.

Patricia Gonzalez, J. M. (16 de Febrero de 2015). Roles y características de Windows server 2012 R2. Obtenido de Administración de Sistema Operativo: http://administraciondesistemaoperativo.com/2014/11/roles-y-caracteristicas-de-windows.html

Rodríguez, V. (10 de Diciembre de 2015). Windows Server 2012. Obtenido de https://www.VinceR336/windows-server-2012-56034208

Rodríguez, X. (Noviembre de 2012). Windows Server 2012. Obtenido de Air Computers: http://air-computers.com/air/ofertas/airofertas/paper-windows-server12.pdf

Smith, C. (17 de febrero de 2018). Servidor DHCP. Obtenido de IT Analysis, Business insight: http://wireless.cubava.cu/ubiquiti-configurando-ap-con-dhcp/

Zambrano, L. (01 de Marzo de 2015). Roles y Características de Windows Server 2012. Obtenido de Administración de Sistemas Operativos: https://administracionsistemasoperativos201415.roles.com/2015/03/01/roles-y-caracteristicas/

Unidad

II

Unidad II

Windows Server 2012 Instalación

2. Requisitos de Instalación

Antes de realizar la instalación de Windows Server 2012, se debe tomar en cuenta ciertas características que debe poseer el equipo para que el software a ser instalado funcione de manera óptima y no presente inconvenientes a la hora de su utilización. (Microsoft, 2013).

En este caso particular, se cuenta con los recursos descritos a continuación, los cuales cumplen con las características tabla 2, que se ajustan a las necesidades por las cuales se requiere instalar Windows Server 2012. Software utilizado:

- VMware Workstation.
- ISO de Windows Server 2012.

Para una instalación el servidor debe contar con las siguientes características:

Tabla 2: Requisitos del sistema para Windows Server 2012 Essentials

Componente	Mínimo	Recomendado	Máximo
socket CPU	1.4 GHz (procesador de 64 bits) o más rápido para un solo núcleo 1.3 GHz (procesador de 64 bits) o más rápido para múltiples núcleos	3.1 GHz (procesador de 64 bits) o multi-core más rápido	2 enchufes
Memoria (RAM)	2 GB 4 GB si implementa Windows Server Essentials como una máquina virtual	16 GB	64 GB
Discos duros y espacio de almacenamiento disponible	Disco duro de 160 GB con una partición de sistema de 60 GB		Sin límite

Los requisitos de hardware tabla 2.1, recomendados admiten límites máximos de usuario y dispositivo.

Tabla 2.1: Requisitos de hardware y software adicionales para Windows Server 2012

Componente	Descripción
Adaptador de red	Adaptador Gigabit Ethernet (10/100 / 1000baseT PHY / MAC)
Internet	Algunas funciones pueden requerir acceso a Internet (se pueden aplicar tarifas) o una cuenta de Microsoft
Sistemas operativos de cliente soportados	Windows 10, Windows 8, Windows 7, Macintosh OS X versiones 10.5 a 10.8. Nota: Algunas características requieren ediciones profesionales o superiores. 1 GB de espacio disponible en el disco duro (una parte de este disco se liberará después de la instalación)
Enrutador	Un enrutador o firewall que admite IPv4 NAT o IPv6
Requerimientos adicionales	Unidad de DVD-ROM

Essentials

Los requisitos reales, variarán según la configuración del sistema así como las aplicaciones y características que elija instalar. El rendimiento del procesador depende no solo de la frecuencia de reloj del procesador, sino también del número de núcleos y del tamaño del caché del procesador.
Los requisitos de espacio de almacenamiento para la partición del sistema son aproximados. Es posible que se requiera espacio de almacenamiento adicional, si está instalando a través de una red (Microsoft, 2013).

2.1. Versiones Disponibles

2.1.1. Windows Server Datacenter

Para entornos en la nube privada altamente virtualizados, permitirá correr un número ilimitado de instancias virtuales, es decir, para un entorno altamente virtualizados que requiera características de alta disponibilidad, incluida la agrupación en clústeres, como muestra la figura 2.1

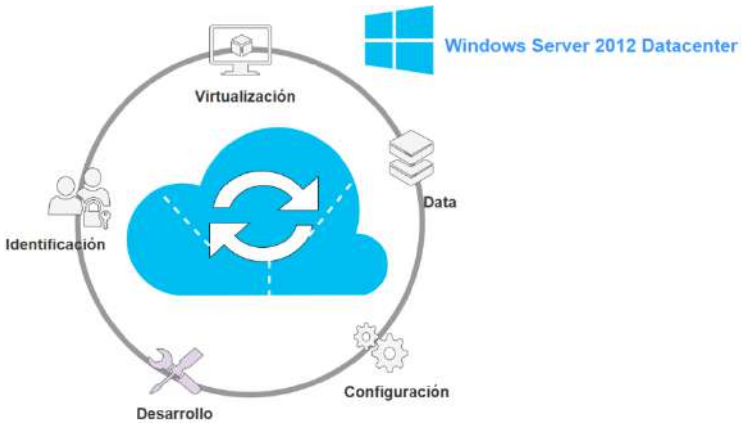


Figura 2. 1: Windows Server DataCenter

2.1.2. Windows Server Standard

Para entornos no virtualizados o poco virtualizados, contará con todas las funcionalidades de servidor y permitirá ejecutar dos instancias virtuales (ver figura 2.2).

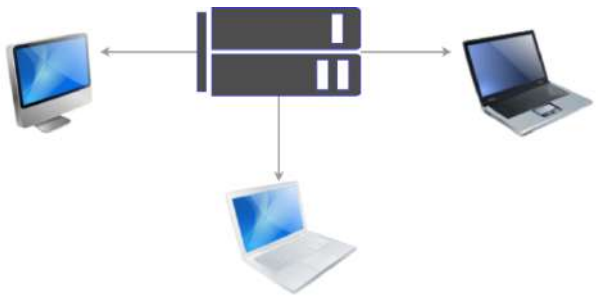


Figura 2. 2: Windows Server Standard

2.1.3. Windows Server Essentials

Para las pequeñas empresas con hasta 25 usuarios trabajando en servidores de hasta dos procesadores. Las funciones de virtualización han sido deshabilitadas (ver figura 2.3) (Iriarte, 2013).

Figura 2. 3: Windows Server Essentials

2.1.4. Windows Server Foundation

Para las pequeñas empresas con hasta 15 usuarios trabajando en servidores de un solo procesador. Las funciones de virtualización han sido deshabilitadas (ver figura 2.4).

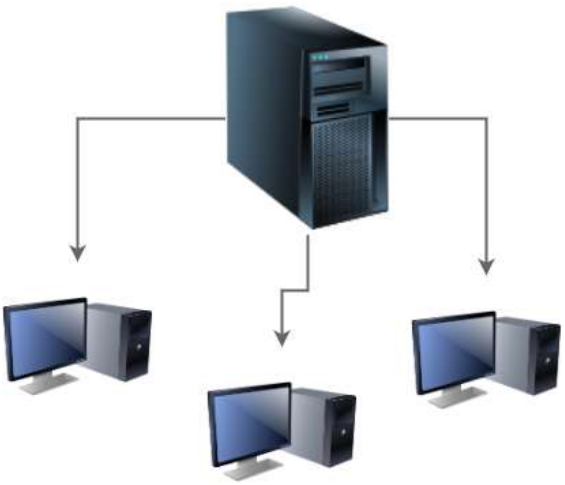


Figura 2. 4: Windows Server Foundation

Según (Iriarte, 2013) nos detalla las características que poseen las distintas versiones en el rol de un servidor (ver tabla 2.2). Sin embargo en la tabla 2.2.1 se aprecia el detalle de los servicios y aplicaciones de Windows server.

Tabla 2.2: Rol de Servidores de Windows Server diferentes versiones

Rol de servidor	Standard/Datacenter	Essentials	Fundation
Servicios de dominio de Active Directory	Completo	Instalado y configurado automáticamente	Debe ser la raíz de un bosque y dominio
Servicios de certificado de Active Directory	Completo	Instalado y configurado automáticamente. Limitado	Limitado
Servicios de Federación de Active Directory	Completo	No disponible	No disponible
Directorio Ligero de Active Directory	Completo	Completo	Completo
Servicios de "Rights Managemen"	Completo	Completo	Completo

Tabla 2.2.1: Servicios y Aplicaciones de Windows Server

Rol de servidor	Standard/DataCenter	Essentials	Fundation
Aplicaciones	Completo	Instalado y configurado automáticamente	Completo
DHCP/DNS	Completo	Completo	Completo
Servidor de Fax	Completo	Completo	Completo
Servidor de ficheros	Completo	Instalado y configurado automáticamente. Limitado a una raíz DFS	Limitado a una raíz DFS
Hyper-V	Completo	No disponible	No disponible
RDS	Completo	Instalado y configurado automáticamente. Limitado a 250 conexiones RRAS	Limitado a 50 conexiones RRAS

Servicios Web	Completo	Instalado y configurado automáticamente.	Completo
WSUS	Completo	Completo	Completo
Administrar servidores	Completo	Completo	Completo
PowerShell	Completo	Completo	Completo

2.2. Preparando la máquina virtual

La máquina virtual nos proporciona una herramienta de virtualización de sistema operativo en una máquina host. La aplicación se llama hipervisor y puede crear máquinas virtuales (VM) completas con administración de sonido, video, red, RAM, discos duros, procesadores, entre otros.

2.2.1. VMware Workstation

Aunque esta herramienta pertenece otro fabricante existe una alta demanda en el mercado ecuatoriano por el uso de esta producto, VMware Workstation puede interceptar dispositivos USB cuando están conectados al sistema operativo invitado. El software permite que varias máquinas virtuales se inicien simultáneamente, pausadas para reanudarlas más adelante, y así sucesivamente. Finalmente, VMware Workstation proporciona a los usuarios una conexión VNC para el acceso remoto al escritorio del sistema invitado y, por lo tanto, facilita las demostraciones de software en un sistema operativo limpio. (Verdezoto, 2017)

Es decir que es un emulador de computadoras, que permite crear máquinas virtuales en las cuales puedes instalar sistemas operativos como si fueran máquinas físicas.

Cabe señalar que pese a que los productos Microsoft soportan Hyper-v, en este trabajo se utilizó VMware Workstation 14 pro, tomando en cuenta que para su utilización el software requiere un procesador AMD o Intel, compatible solo para sistema operativo de 64 bits, velocidad de núcleo de 1,3 GHz o superior.

2.2.2. Requisitos de VMware Workstation

Para preparar el software lo primero que se debe hacer es, asegurar que la computadora cumpla los requisitos para la instalación, tal como muestra la tabla 2.3

Tabla 2.3: Requisitos del software

Requisitos para la instalación	
Ediciones Windows	Windows 10 Pro
Procesador	Intel Pentium CPU 3825U @1,90 GHz
Memoria RAM	4,00 GB
Tipo de sistema	Sistema operativo de 64 bits, procesador x64
Lápiz y entrada táctil	La entrada táctil o manuscrita no está disponible
Nombre del equipo	DESKTOP-33K3VHF
Nombre completo del equipo	DESKTOP-33K3VHF
Grupo de trabajo	WORKGROUP

Entramos la página oficial https://www.vmware.com/products/workstation-pro.html (VMare), dirigirnos en login para iniciar sesión en la caso de no tener cuenta creamos, acabando de iniciar sesión dirigirse en productos y opción descarga estos nos sirve para descargar el software (ver figura 2.5). (VMware, 2017)

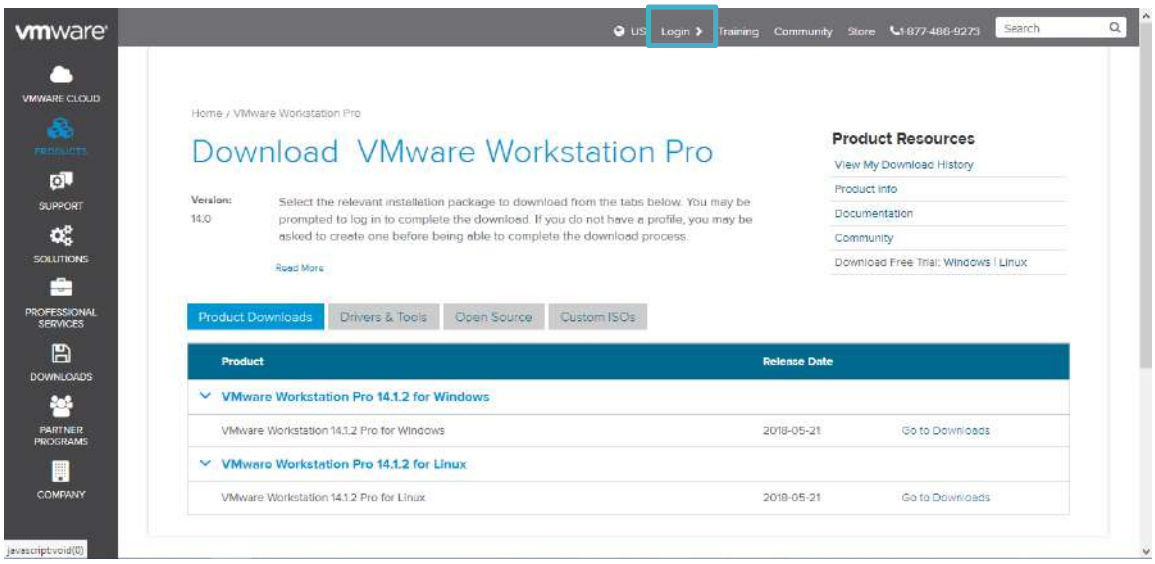


Figura 2. 5: Download VMware Workstation

2.2.3. Instalación del VMware Workstation

Luego de descargar el producto del sitio web, automáticamente la descarga se guarda en la computadora, luego se dirige en mi pc, opción descarga y se muestra el software descargado, comenzamos la instalación a ejecutar el programa haciendo doble clic en el software que descargamos, en el cual nos aparece un cuadro de dialogo de solicitud el permiso para que comience la instalación, luego de solicitar el permiso le damos clic en botón siguiente como se muestra la figura 2.6.

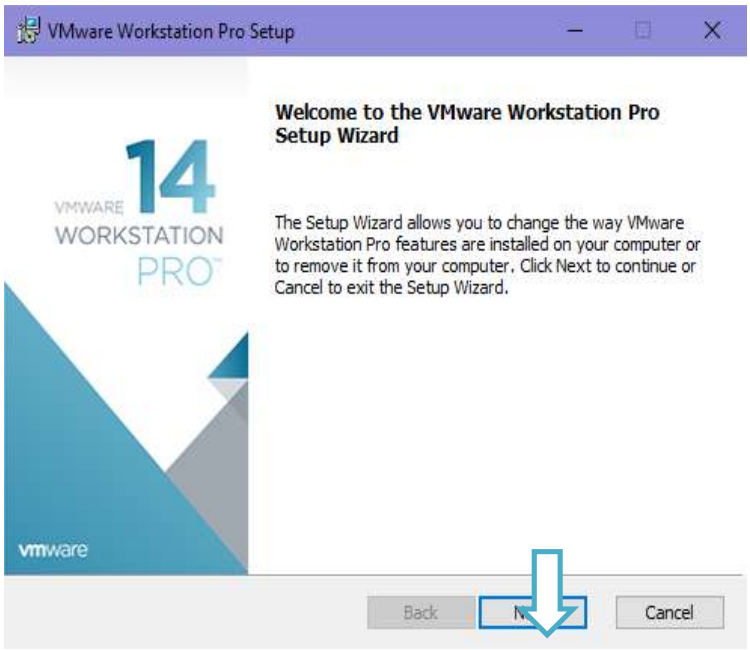


Figura 2. 6: Previa instalación del Software

Para comenzar la instalación del producto, se mostrará el término de la licencia donde debemos aceptar el término de la licencia, clic en opción continuar ver figura 2.7.

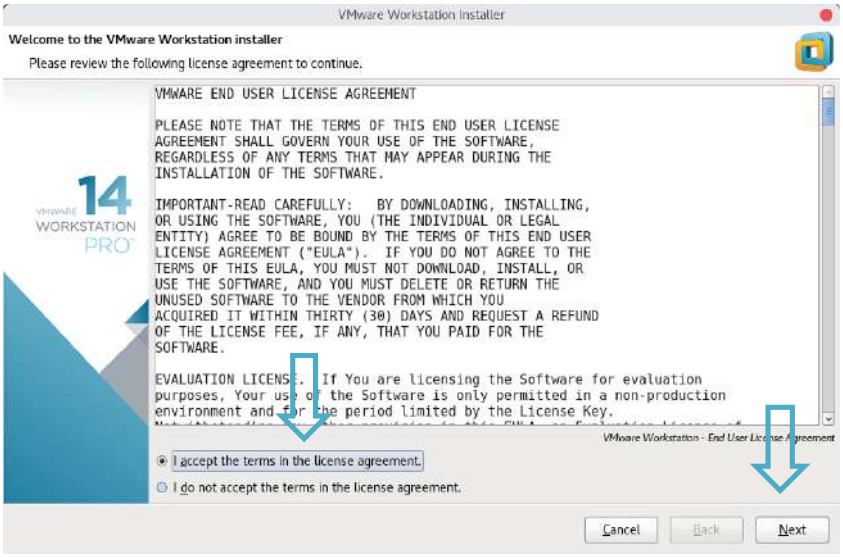


Figura 2. 7: Aceptación de los términos del software

Luego se mostrará un cuadro con dos opciones la primera Typical y las segunda Custom, elegimos la opción Typical, damos clic en siguiente y a continuación pedirá que ingrese la licencia del software, ya ingresado la licencia damos enter y finalizar, como nos muestra en la figura 2.8 ya tenemos instalado VMware Workstation para luego instalar el Windows Server 2012.

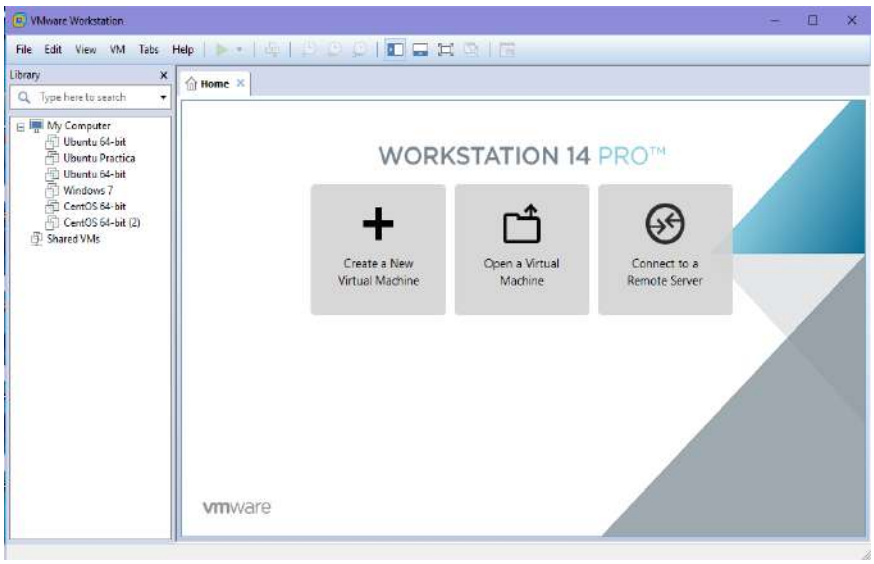


Figura 2. 8: VMware Workstation pro 14 instalado

2.2.4. Creación de una máquina virtual

Una vez instalado el software de virtualización, para crear una máquina virtual procedemos a la instalación de Windows Server 2012, cabe recalcar que para instalar el sistema operativo debemos tener descargado el archivo .iso Winows Server 2012. Damos clic Create a New Virtual Machine (Crear nueva máquina virtual) como mostramos en la figura 2.9, luego se abrirá una nueva ventana en la cual dejamos en Custom y damos clic en Next o siguiente como se muestra la figura 2.10.

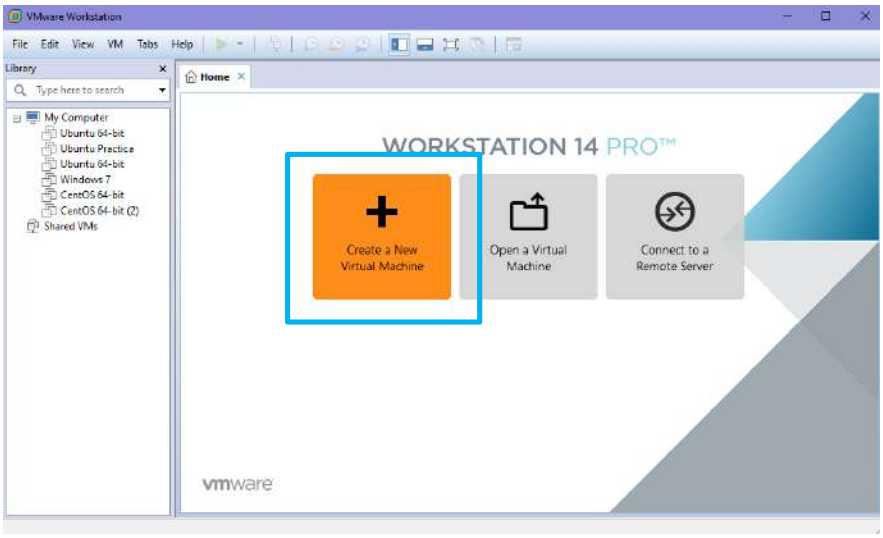


Figura 2. 9: Crear una máquina virtual

Typical, se instalada de manera predeterminada del sistema, en cambio Custom se instala de una manera avanzada es decir, en esta opción puede elegir el número de procesadores que deseo usar, la memoria RAM entre otras.

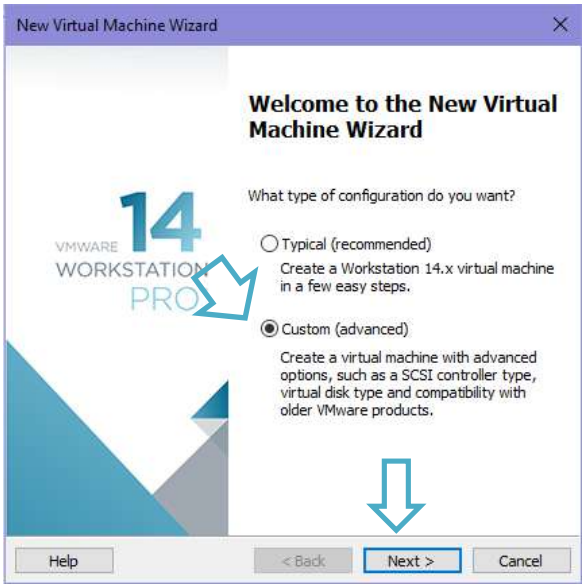


Figura 2. 10: Tipo de configuración máquina virtual

Después de seleccionar la configuración de la máquina virtual, mostrará una nueva ventana en la que colocaremos la imagen .iso de Windows server 2012 y pulsamos Next como vemos en la figura 2.11.

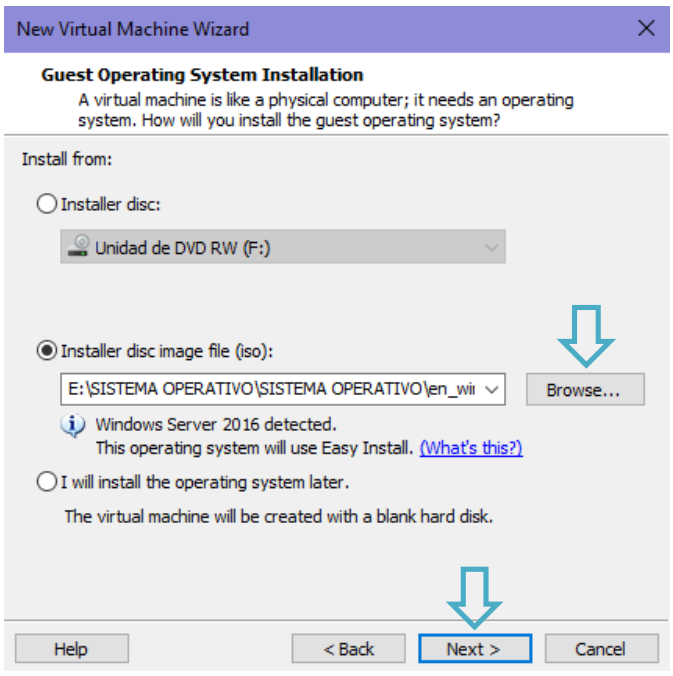


Figura 2. 11: Seleccionar la imagen iso

En la siguiente ventana permitirá mostrar la ubicación en la que se almacenara, si no se desea cambiar de ubicación se la dejara por defecto y pulsaremos Next ver figura 2.12.

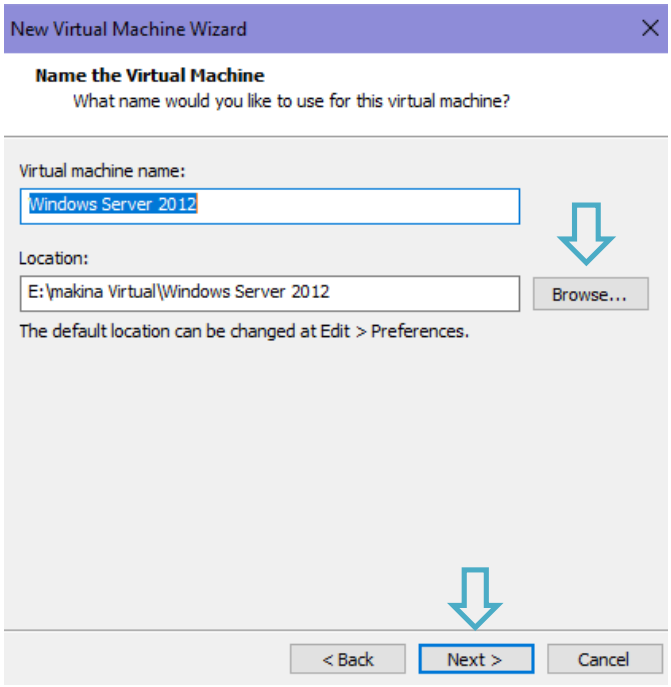


Figura 2. 12: Seleccionar la ubicación almacenada Windows Server 2012

Nos mostrará una ventana en la cual pedirá que especifique el números de procesadores de la máquina virtual ya introducido la cantidad de procesadores que utilizar, damos clic en siguiente y luego pediría que especifique la cantidad de memoria que usará, en este caso colocare 2 Gb y le damos clic en siguiente, así sucesivamente, luego veremos que en la siguiente, ventana podemos escoger el tamaño del disk hard en el que instalara el sistema dejamos por defecto la casilla marcada y pulsamos siguiente como se muestra en la figura 2.13.

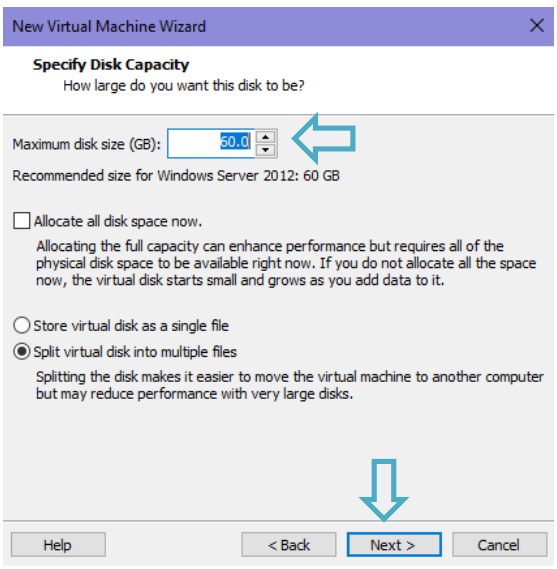


Figura 2. 13: Especificando la capacidad del disco Windows Server 2012

Finalmente aparecerá una ventana ver figura 2.14, en la que nos muestra las características de la máquina que hemos creado y pulsaremos Finish.

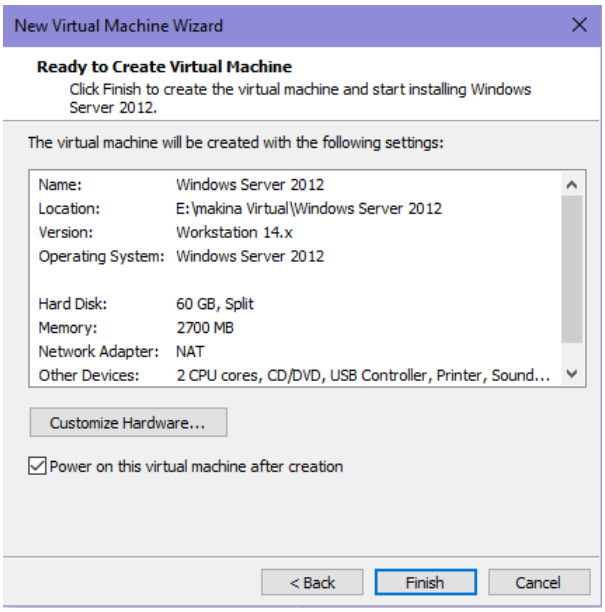


Figura 2. 14: Características de la instalación Windows Server 2012

Finalmente la máquina virtual se enciende para comenzar a realizar la instalación del sistema operativo Windows Server 2012.

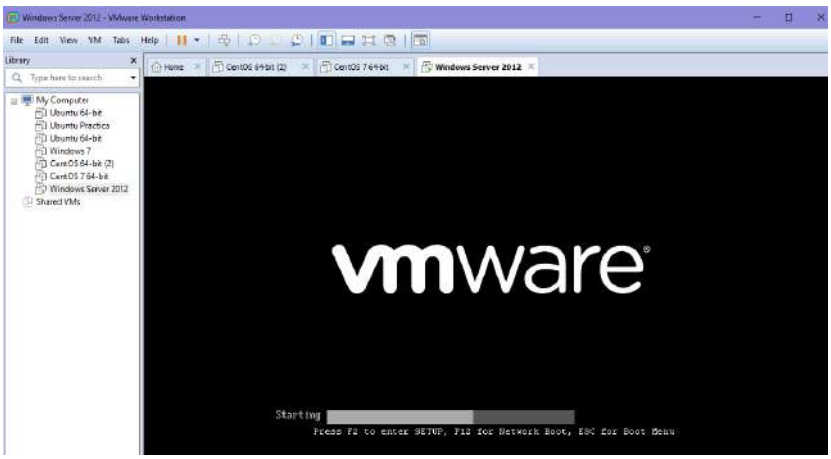


Figura 2. 15: Encendiendo la máquina virtual Windows Server 2012

2.3. Instalación Windows Server 2012

Windows Server 2012, es el sistema operativo basado en 64 bits, está diseñado para plataformas x64. (Valdés, 2015). Para comenzar a instalar Windows Server 2012 en la máquina virtual se realiza los pasos mostrados en la secuencia que sigue:

1. Una vez cargando el sistema mostrara una pantalla en donde indica que idioma deseamos instalar, el formato de la hora y el método de entrada, como podemos observar en la figura 2.16.

Figura 2. 16: Configuración Windows Server 2012

2. Ya configurando el sistema operativo le damos clic en siguiente y comenzara la instalación del sistema operativo.

Figura 2. 17: Instalando Windows Server 2012

3. Luego pedirá que ingresemos la licencia Windows Server 2012, seleccionamos y damos clic en siguiente, luego seleccionamos la categoría de instalación que usaremos el modo gráfico le damos clic en siguiente.

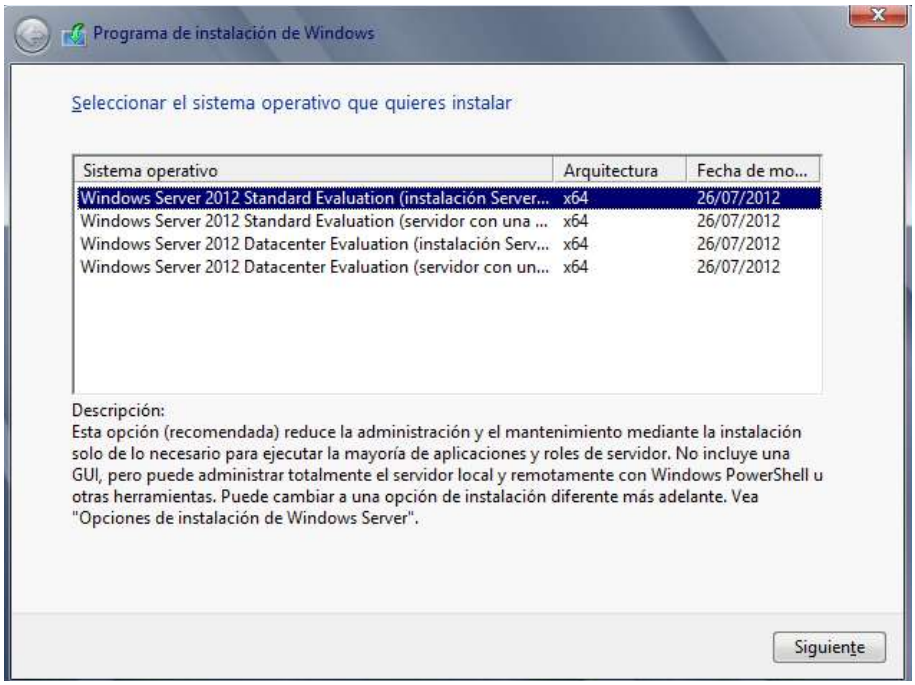


Figura 2. 18: Seleccionar el tipo de instalación Windows Server 2012

4. Aceptamos los términos de la licencia.

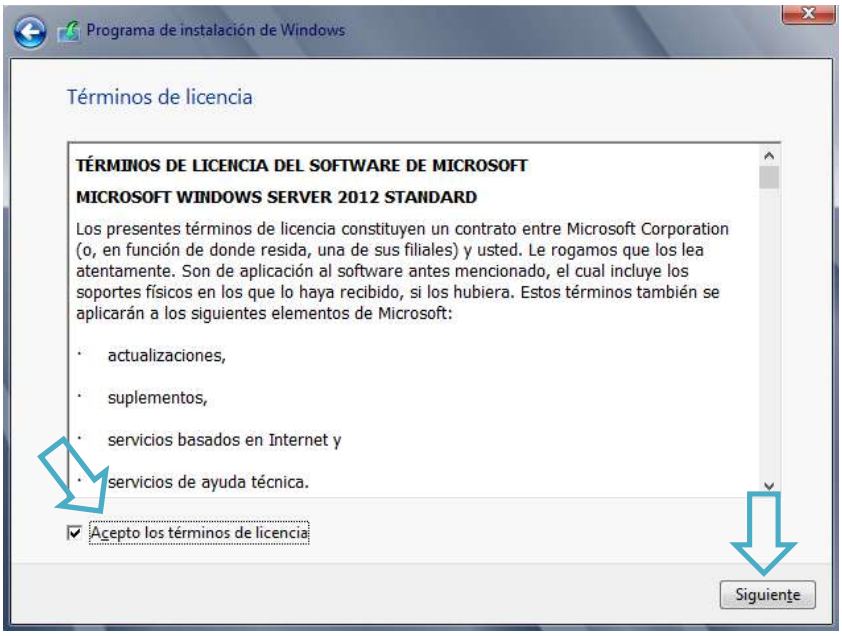


Figura 2. 19: Término de licencia Windows Server 2012

5. Colocamos el modo personalizados para elegir las particiones de las unidades del disk hard del sistema operativo, para configurar las particiones le damos clic opción nuevo muestra una ventana

donde debemos indicar la cantidad de memoria que queremos usar en las dos particiones, luego pulsamos siguiente como se muestra la figura 2.20.

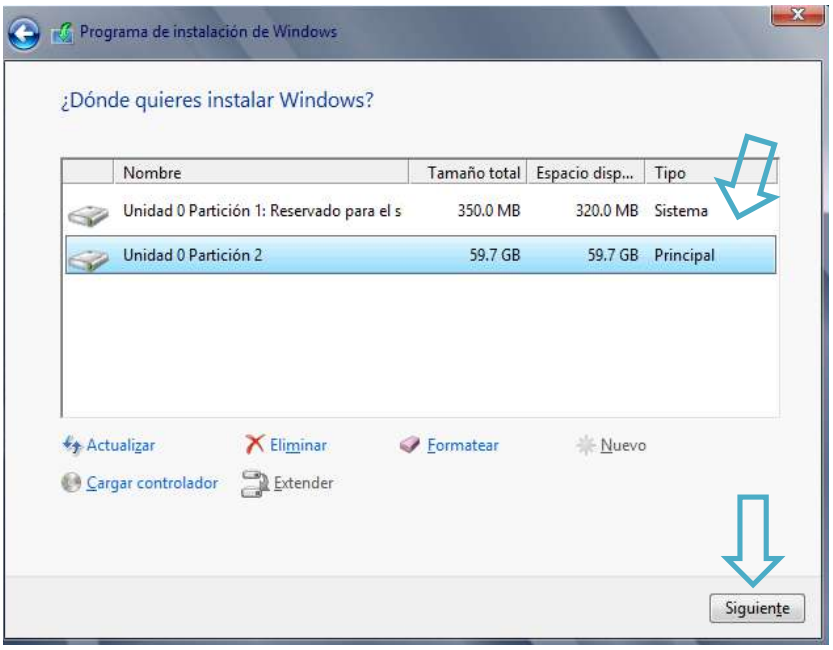


Figura 2. 20: Particiones del disco duro Windows Server 2012

6. Comenzamos la instalación de nuestro sistema operativo Windows Server 2012.

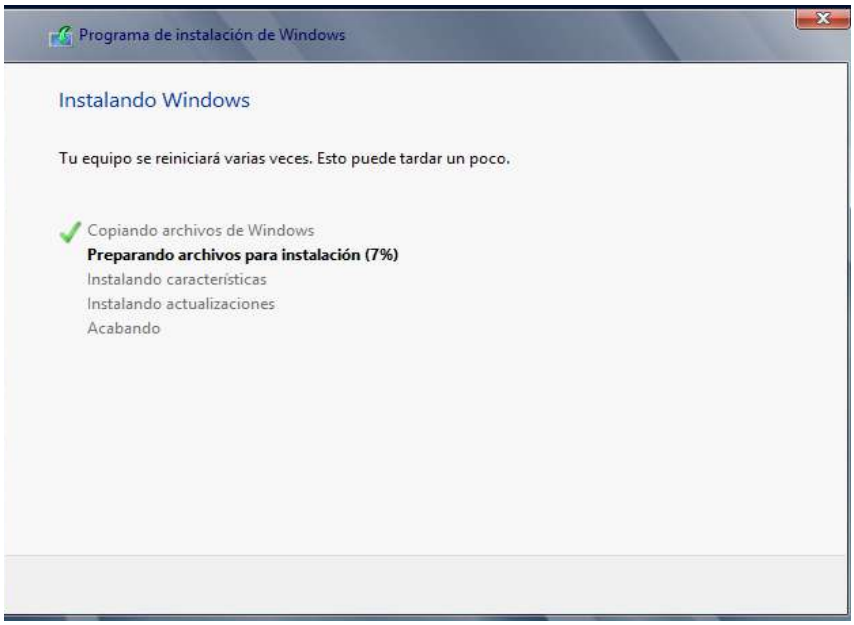


Figura 2. 21: Comenzando la instalación de Windows Server 2012

7. Una vez finalizada la instalación, el sistema se prepara para las primeras configuraciones. Luego el sistema se reiniciará y me pedirá que cree una clave como administrador, cli en finalizar como se observa la figura 2.22.

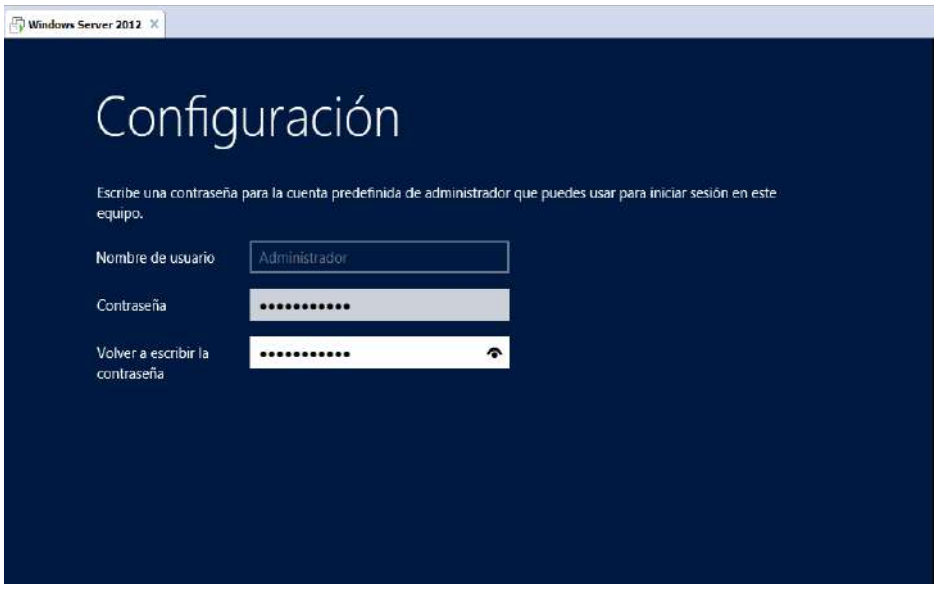


Figura 2. 22: Creando contraseña para iniciar sesión Windows Server 2012

8. Presionar las teclas CTRL+ALT+DELETE para dar inicio a la primera sesión, ingresamos la contraseña y listo tenemos nuestro sistemas operativo instalado.

Figura 2. 23: Windows Server 2012

Bibliografía

Iriarte, M. A. (26 de Septiembre de 2013). Instalación e Introducción básica de Windows Server 2012 . Obtenido de https://es.slideshare.net/mike741/instalacion-y-administracion-basica-de-windows-server-2012

Microsoft. (19 de Noviembre de 2013). Requisitos del sistema para Windows Server 2012 R2 Essentials. Obtenido de https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-essentials-sbs/dn383626(v=ws.11)

Valdés, E. (13 de Enero de 2015). Sistema Operativo Windows Server 2012. Obtenido de https://www.administracionderedes.com/sistema-operativo-windows-server-2012/

Verdezoto, C. (24 de Abril de 2017). VMware Workstation Pro 14 Serial key. Obtenido de Full Free Activation: http://www.nomorebuy.com/2017/10/vmware-workstation-pro-14.html

VMware. (09 de Agosto de 2017). VMare Workstation . Obtenido de https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html

Unidad

III

Unidad III

Active Directory Servicios de dominio y Administración de objetos

3. Introducción

El Directorio Activo o Active Directory (AD) es una base de datos de información sobre usuarios, computadoras, impresoras y casi cualquier objeto que pueda ser implementado dentro de una empresa. Ofrece a los usuarios el acceso a diferentes recursos de una red mediante un único inicio de sesión. Esto reduce considerablemente el número de contraseñas facilitando la administración de usuarios por parte del administrador. (González, 2014)

No obstante, cualquier objeto de la red, solo puede existir dentro de un dominio. Los dominios se usan para agrupar objetos relacionados, con el fin de reflejar la red de una organización. Cada dominio que se crea almacena información acerca de los objetos que contiene. Cada dominio representa un límite de seguridad. El acceso a los objetos dentro de cada dominio se controla mediante entradas de control de acceso (ACE, Access Control Entries) contenidas en listas de control de acceso (ACL, Access Control Lists).

El Sistema de Nombres de Dominio (DNS), es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a una red. Este sistema asocia información variada con nombres de dominios, asignados a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres en identificadores binarios asociados a los equipos con el propósito de poder localizarlos y direccionarlos. (González, 2014)

Las consultas DNS se resuelven de diferentes formas. A veces, un cliente responde a una consulta localmente mediante la información almacenada en la cache obtenida de una consulta anterior. Un servidor DNS, también puede consultar o ponerse en contacto con otros servidores DNS en nombre del cliente solicitante para resolver el nombre por completo y, a continuación, enviar una respuesta al cliente. DNS utiliza los protocolos TCP y UPD en el puerto 53 para servir las peticiones. Generalmente la mayoría de las consultas DNS consisten en un solo paquete UDP enviado por el cliente seguido de un paquete UPD de respuesta generado por el servidor. TCP se utiliza en los casos en que la respuesta excede de los 512 bytes.

A continuación, se detallan los pasos para instalar Active Directory y poder generar un nuevo dominio en el servidor. También se realiza la

instalación de un servidor DNS y se habilitan las actualizaciones dinámicas.

3.1.1. Estructura

Active Directory está basado en una serie de estándares llamados X.500, aquí se encuentra una definición lógica a modo jerárquico. Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios. (Solanes, 2016)

3.1.2. Objetos

Estos objetos se conocen como objetos esquema, o metadata, y existen para poder extender el esquema o modificarlo cuando sea necesario.

3.1.3. Funcionamiento

Su funcionamiento es similar a otras estructuras de LDAP (Lightweight Directory Access Protocol), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. Una de sus ventajas es la sincronización presente entre los distintos servidores de autenticación de todo el dominio. De esta forma, es posible crear recursos (como carpetas compartidas, impresoras de red, etc.) y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito.

3.1.4. Intercambio entre dominios

Para permitir que los usuarios de un dominio accedan a recursos de otro dominio, Active Directory usa una relación de confianza (en inglés, trust). La relación de confianza, es creada automáticamente cuando se crean nuevos dominios. Los límites de la relación de confianza no son marcados por dominio, sino por el bosque al cual pertenece. (Solanes, 2016)

3.2. Zona de configuración LAN

Este escenario estructura la zona de configuración LAN, con interfaz de red perteneciente a la eth0 del servidor firewall, va a estar conformada por: dos servidores Windows Server 2012, un switch y un pc. El primer servidor Windows server 2012 se llama SRV-DC-01, contiene los siguientes servicios: DA, GPO, DHCP, DNS, WINS, IIS. El segundo servidor Windows server 2012 se llama SRV-DC-02, contiene los siguientes servicios: DA, GPO, DHCP, DNS, WINS. Como se observa en la Figura 3.1 Ambos servidores son controladores de dominio. El nombre del pc es pc-01, representa a los 50 ordenadores que existen en la empresa, el switch pertenece a la capa de acceso, los Switchs de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Esta propuesta pretende mostrar el paso a paso de la configuración de cada servicio solicitado, así como el levantamiento de un controlador de dominio en ambos servidores.

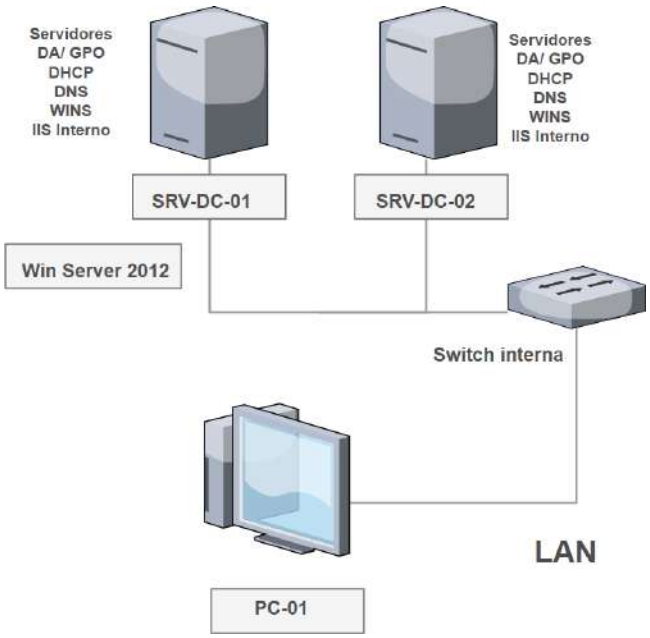


Figura 3. 1: Zona de configuración LAN

¿Sabías Qué?

3.3. Instalación del controlador de dominio

Active Directory permite administrar las identidades en Windows Server 2012 junto al resto de identidades dispersas en otros sistemas y plataformas, incluida la implementación de directivas de seguridad y acceso a otros recursos. Como resultado, Active Directory puede ser utilizado como un depósito global para las identidades, información sobre autenticación y autorización que puede ser extendida a otras aplicaciones, sistemas y plataformas. (Moreno, 2012)

Si se conectan más de dos ordenadores en una red LAN, se necesitan otros componentes de red como concentradores, switches, puentes de red y conmutadores que funcionan como elementos de acoplamiento y nodos de distribución.

Iniciaremos con la instalación del controlador de dominio siguiendo estos pasos:

1. En equipo hacemos clic derecho elegimos la opción propiedades, aparecerá la ventana de propiedades del sistema le daremos clic en cambiar configuración ver la figura 3.2.

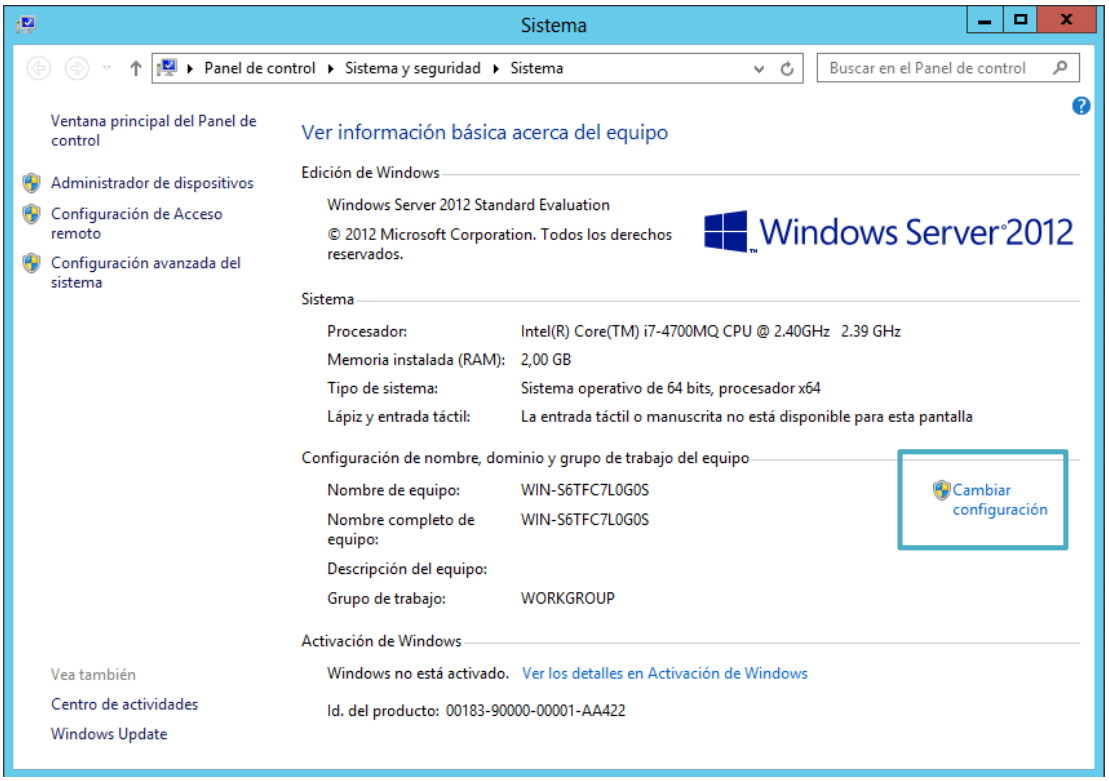


Figura 3. 2: Configuración Windows Server 2012

2. Se abrirá una nueva ventana en la cual damos clic en cambiar ver figura 3.3.

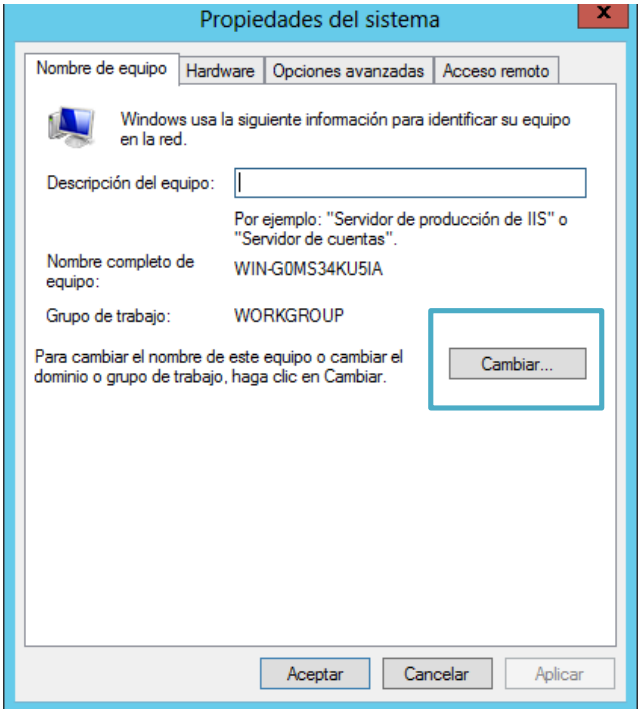


Figura 3. 3: Propiedades del sistema

3. En la nueva ventana asignamos un nombre, el cual será para este caso SrvDC01. Damos clic en aceptar ver figura 3.4.

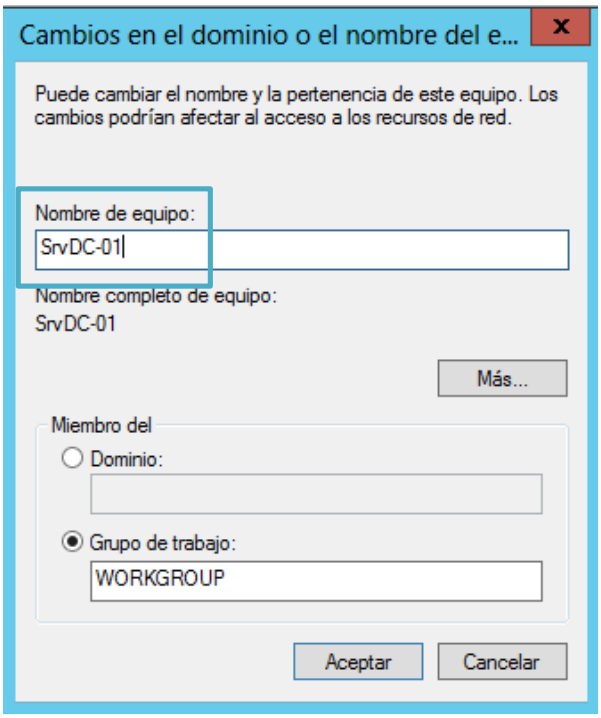


Figura 3. 4: Asignación del nombre del dominio

4. Antes de reiniciar el equipo, asignamos una dirección ip, para esto iremos al centro de redes en recursos compartidos, y hacemos clic en la opción cambiar configuración del adaptador ver figura 3.5.

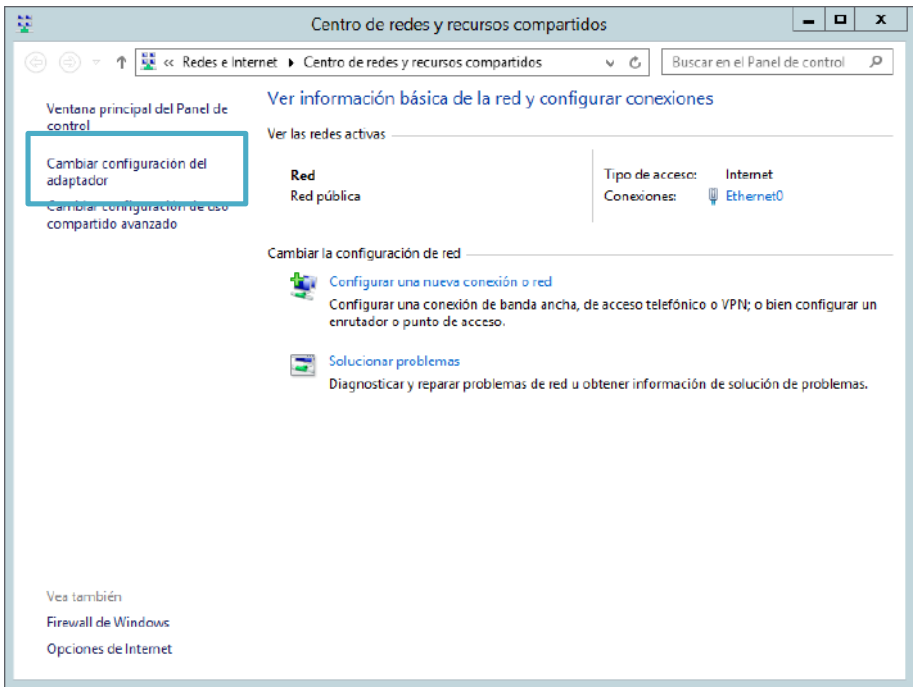


Figura 3. 5: Centro de recursos compartidos

5. Aparecerá una nueva ventana de conexiones de red, clic derecho y en la cinta de opciones elegimos propiedades como se muestra la figura 3.6.

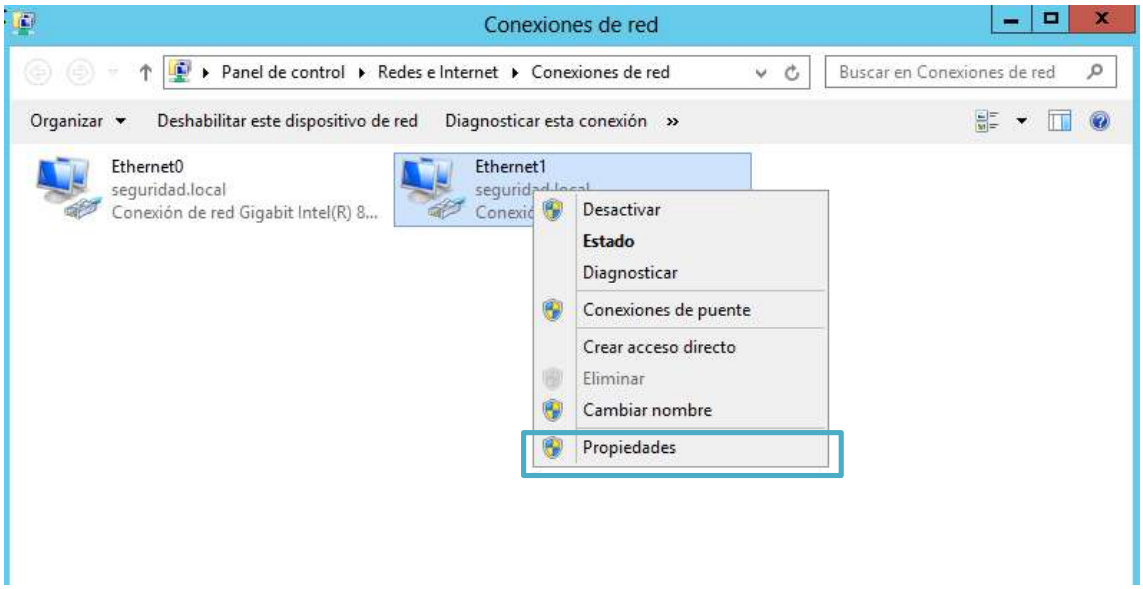


Figura 3. 6: Conexiones de redes

6. En la nueva ventana deshabilitamos la opción ipv6.

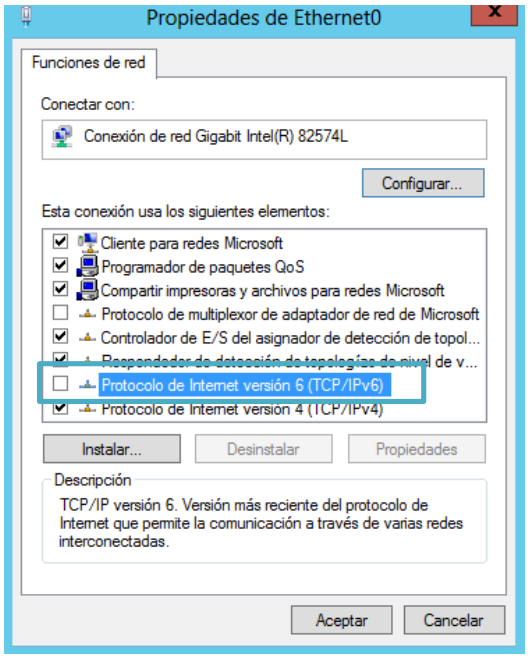


Figura 3. 7: Desabilitación TCP/IPv6

7. Luego elegimos la opción ipv4 y damos clic en propiedades y en las propiedades asignamos la dirección IP 192.168.239.12 dejamos por defecto la máscara y como servidor DNS dejamos la misma dirección IP ver figura 3.8 como se muestra figura 3.8.

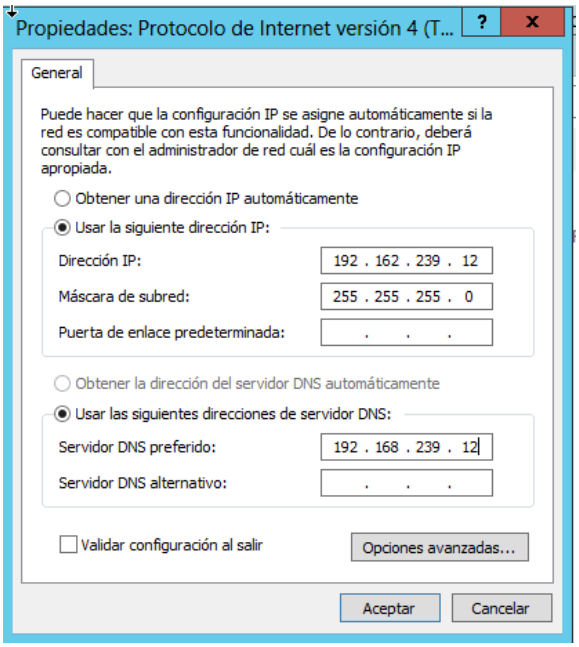


Figura 3. 8: Propiedades del Protocolo IPv4

8. Luego damos clic en aceptar y ahora procedemos a reiniciar el servidor, nuestro siguiente paso será instalar el controlador de dominios para ello debemos dar ir al administrador de servidor como lo vemos acontinuación ver la figura 3.9.

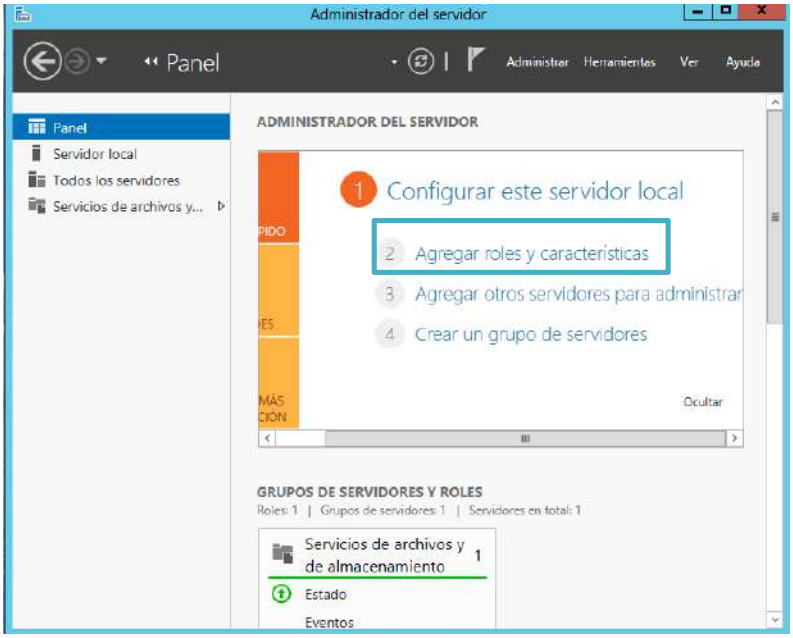


Figura 3. 9: Administrador del servidor

9. Hacemos clic en agregar roles y caracteristicas nos aparecerá una ventana y escojemos la opción siguiente haciendo un clic ver figura 3.10.

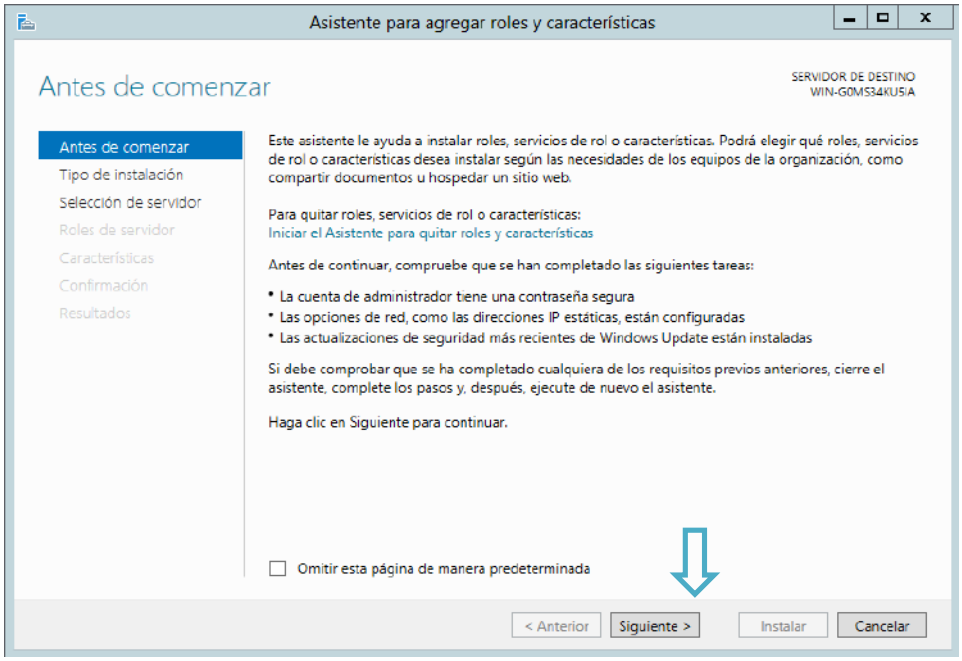


Figura 3. 10: Asistente para agregar roles y características

10. Nos aparecerá el tipo de instalación, elegir la instalación basada en características o en roles dar clic en siguiente como se muestra en la figura 3.11.

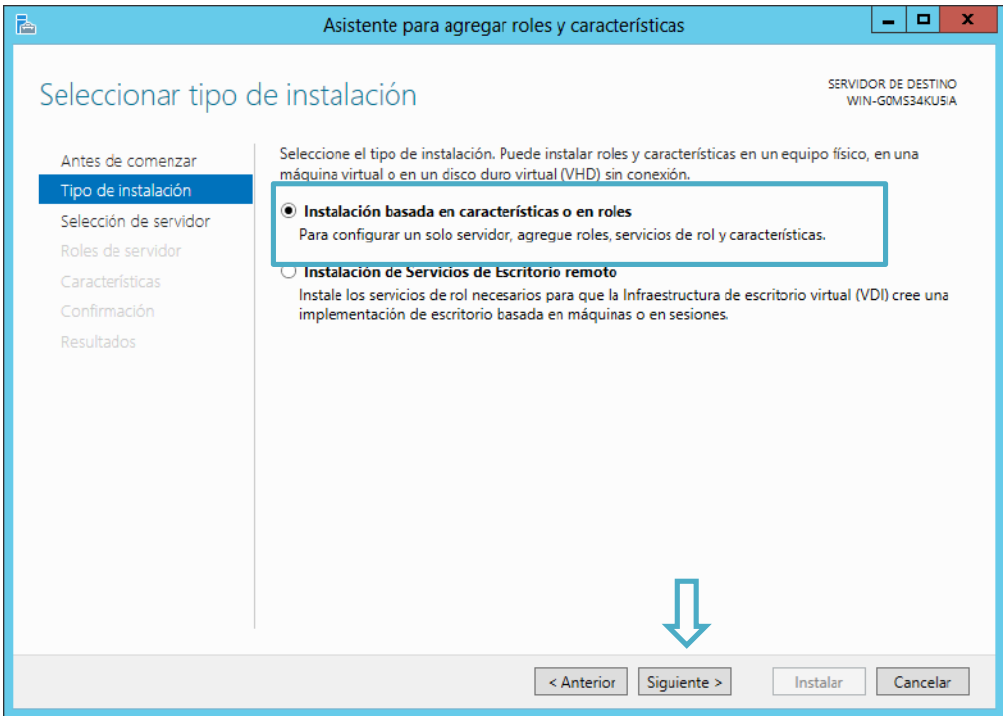


Figura 3. 11: Seleccionar tipo de instalación

11. En la siguiente opción, aparecerá selección de servidor, confirmamos que sea el nombre que se le asignó a la IP y haremos clic en siguiente ver la figura 3.12.

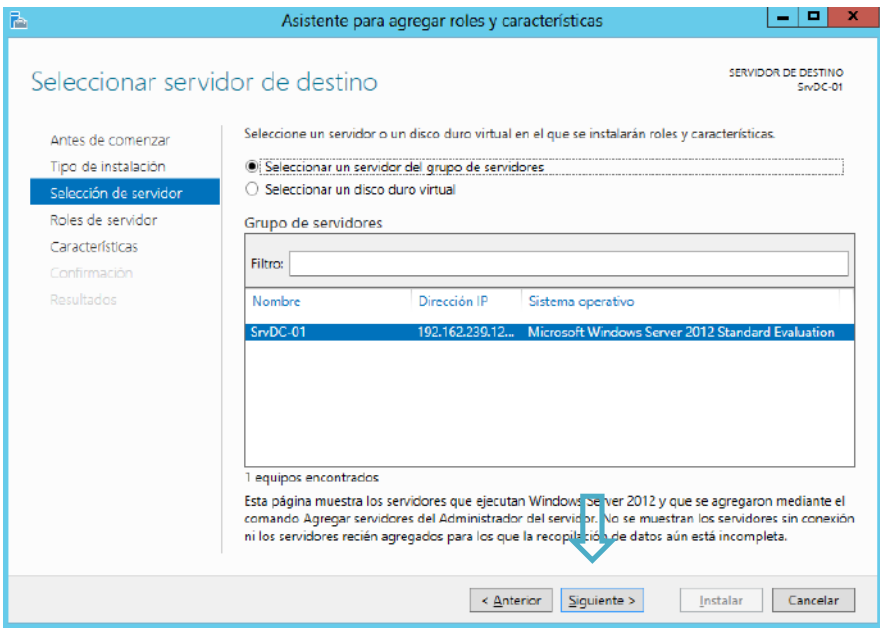


Figura 3. 12: Seleccionar el servidor

12. Ahora activamos la casilla de servicios de dominio.

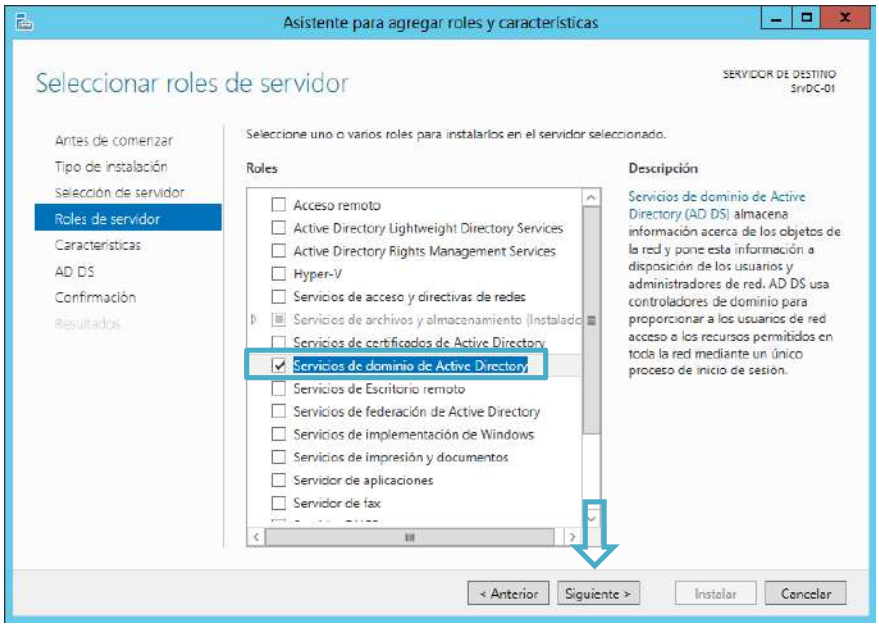


Figura 3. 13: Roles de servidores

13. Se abrirá otra ventana hacemos clic en agregar características y luego clic en siguiente ver figura 3.14.

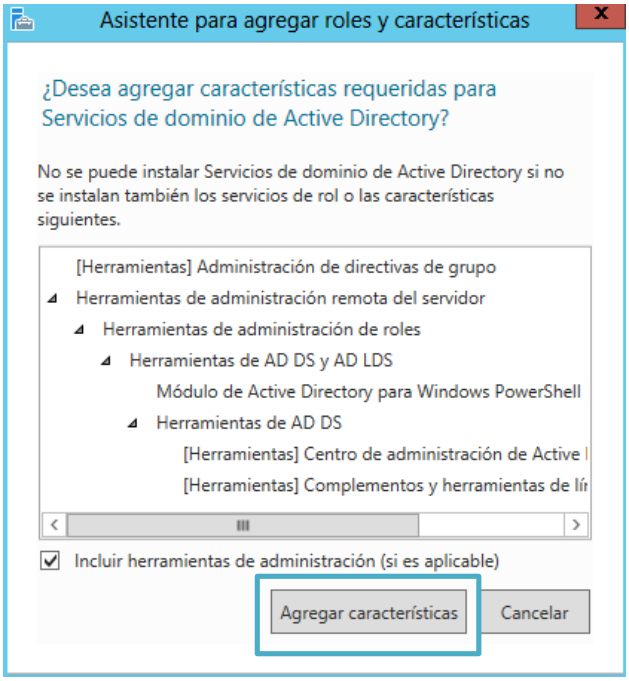


Figura 3. 14: Asistencia para agregar roles y características

14. Dejamos las características que están por defecto y hacemos clic en siguiente ver figura 3.15.

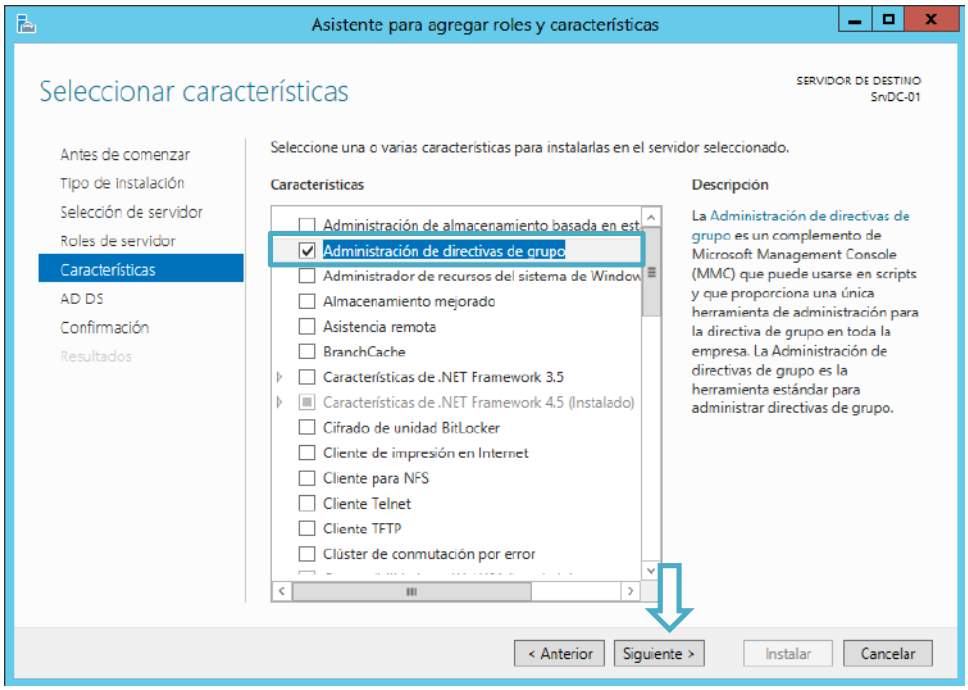


Figura 3. 15: Seleccionar características

15. Nos aparecerá el AD DS solo daremos clic en siguiente ver figura 3.16.

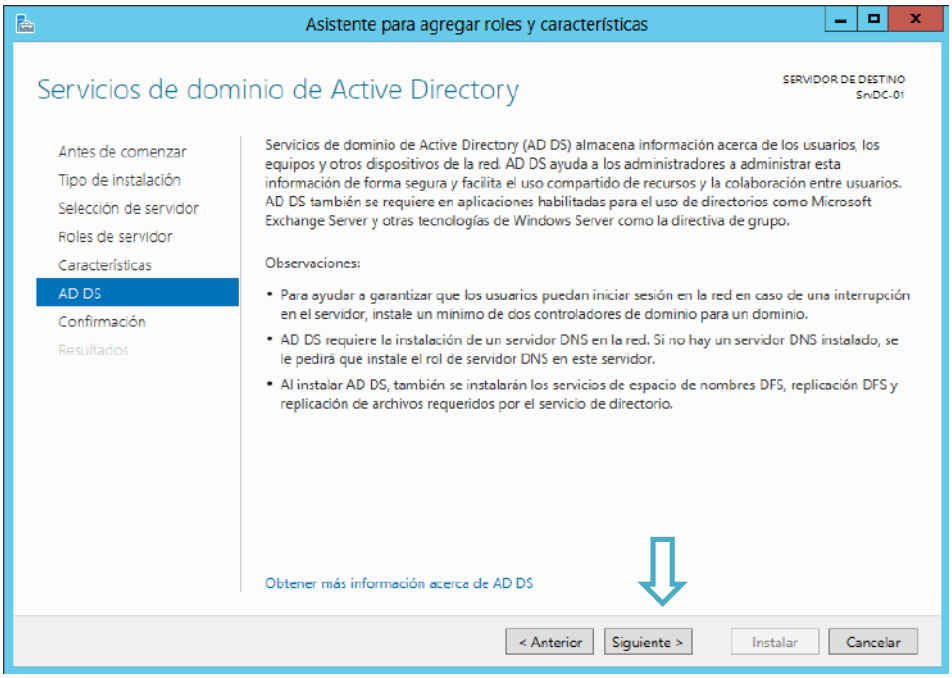


Figura 3. 16: Servicios de dominio de Active Directory

16. En el siguiente paso en la confirmación hacemos clic en instalar ver figura 3.17.

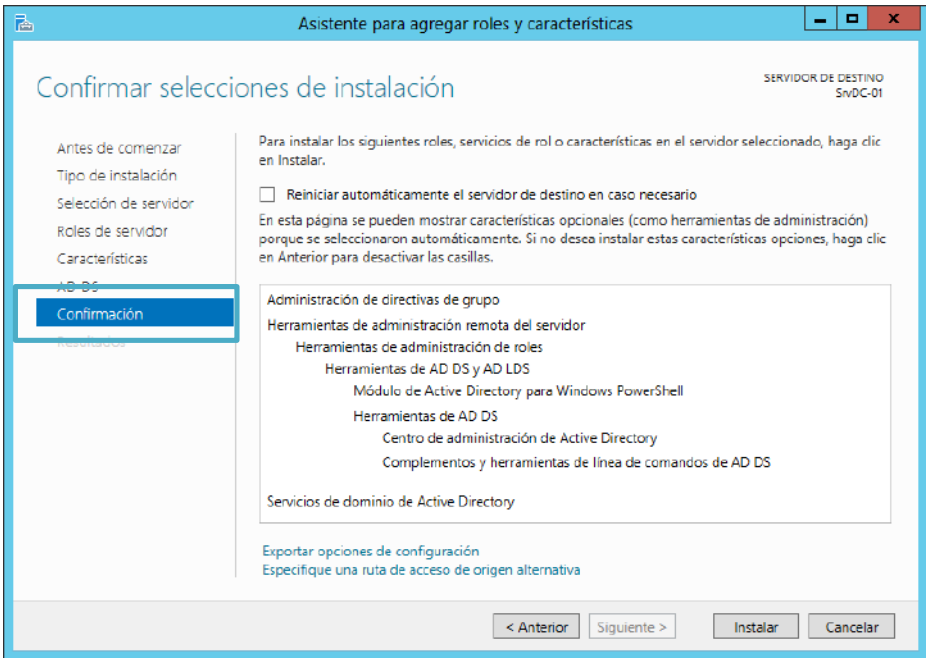


Figura 3. 17: Confirmar selecciones de instalación

17. Luego iniciará el proceso de instalación esperamos que cargue y finalice ver figura 3.18.

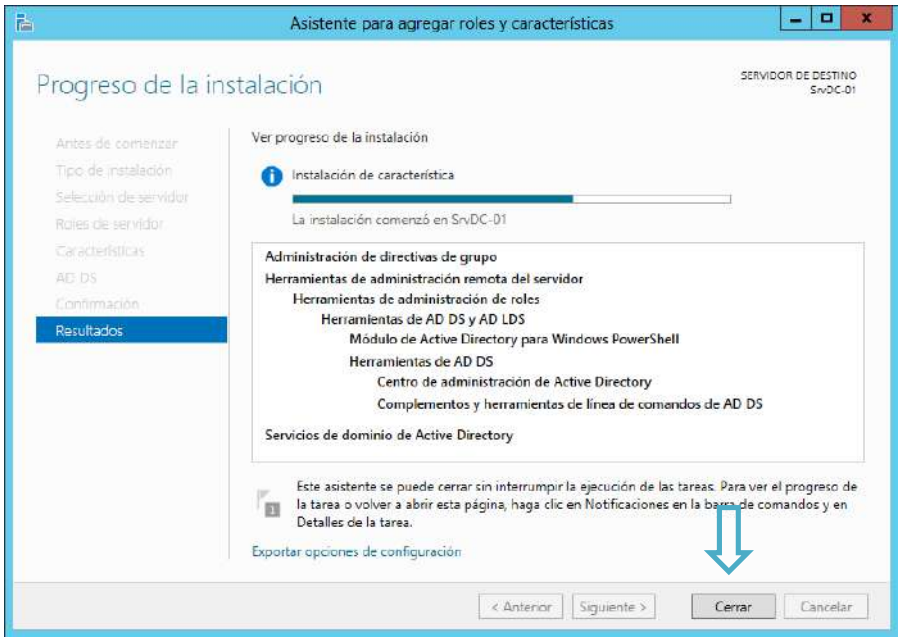


Figura 3. 18: Progreso de la instalación

18. Una vez finalizada la instalación damos clic en promover este servidor a controlador de dominio ver figura 3.19.

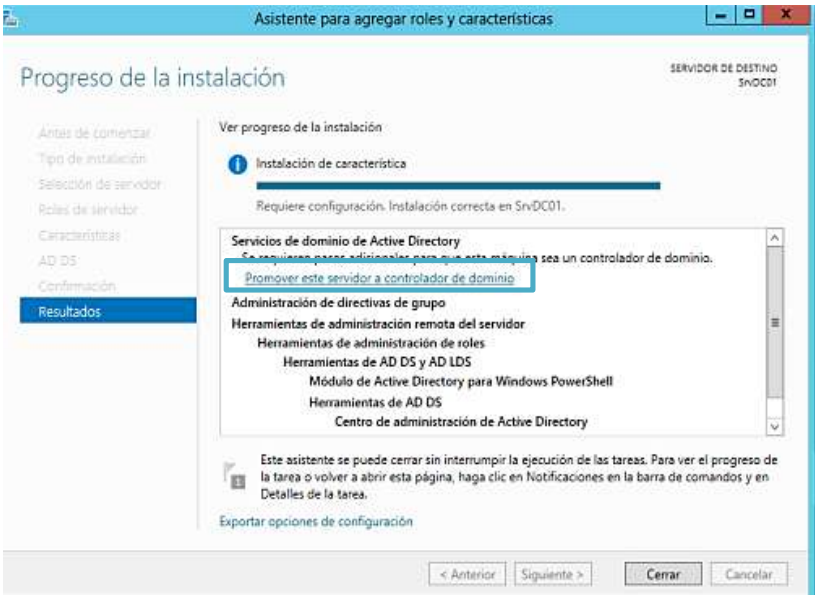


Figura 3. 19: Completando la instalación

19. Aparecerá una ventana y elegimos la opción agregar un nuevo bosque. Colocaremos un nuevo nombre en este caso será seguridad.local y damos clic en siguiente ver figura 3.20.

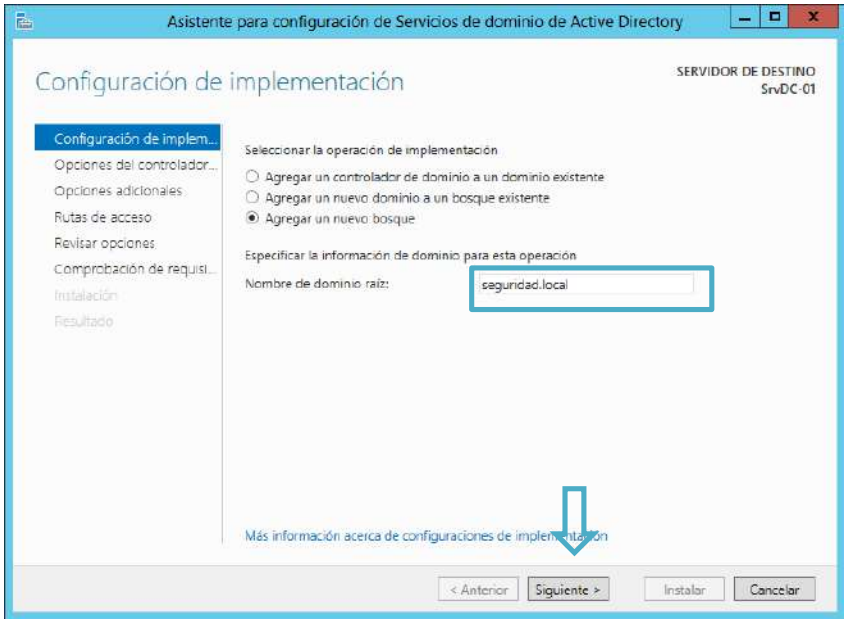


Figura 3. 20: Configurando la implementación

20. Dejamos por defecto las casillas marcadas y colocaremos una contraseña esto será útil para el modo restauración de directorio y luego damos clic en siguiente ver figura 3.21.

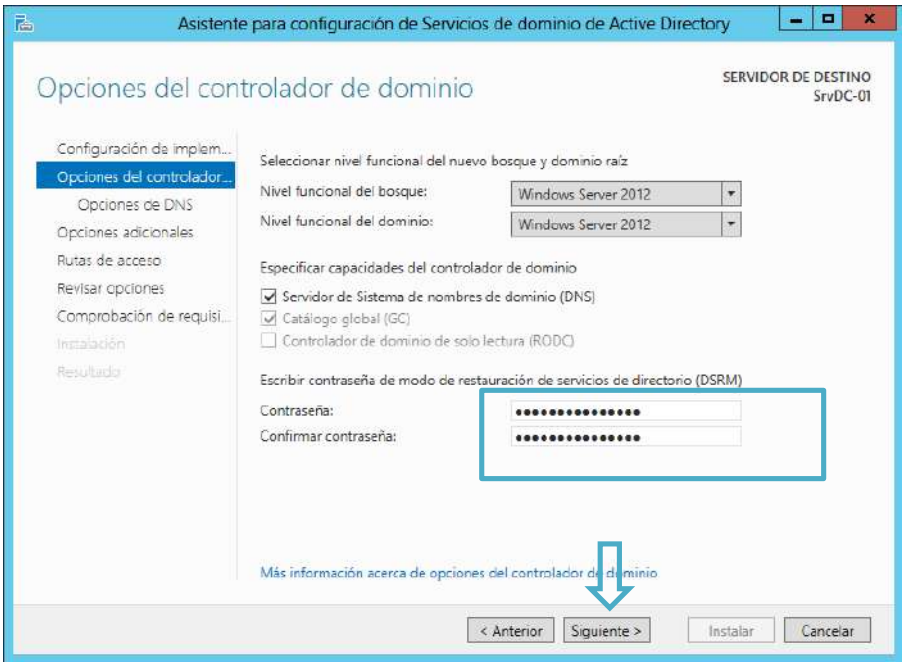


Figura 3. 21: Opciones del controlador de dominio

21. En la parte de opciones de DNS haremos Clic en siguiente ver figura 3.22.

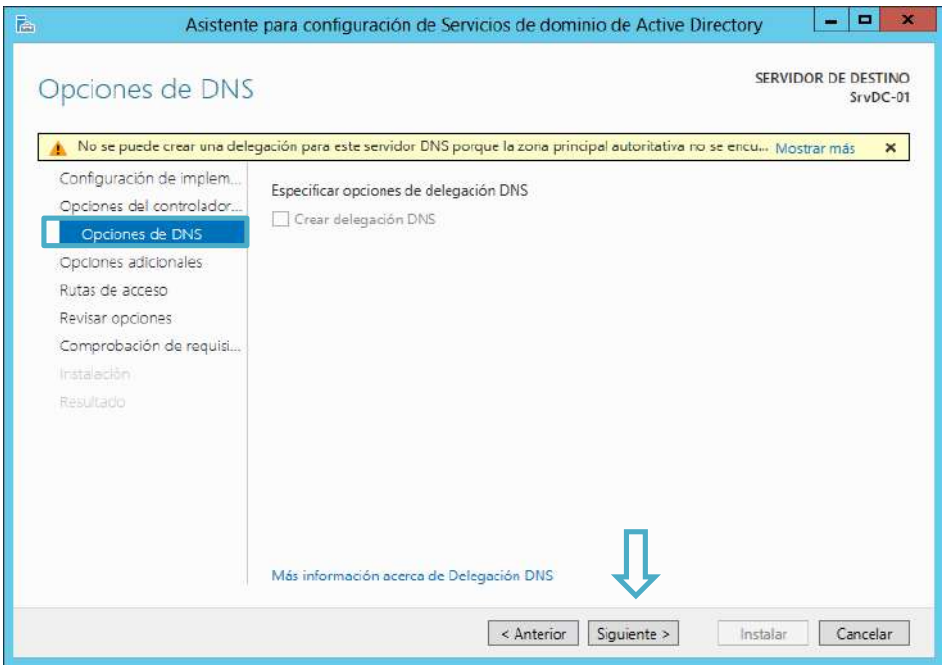


Figura 3. 22: Opciones de DNS

22. En la siguiente ventana aparecerá el nombre netbios, este nombre se utiliza para autenticar en la red sin necesidad de utilizar el nombre completo del dominio en este caso será seguridad, y damos clic en siguiente y nos mostrará la opción rutas de acceso nos aparecerá la ruta por defecto de donde se almacenará la base de datos, los archivos de registro y la carpeta de sysvol, haremos clic en siguiente ver figura 3.23.

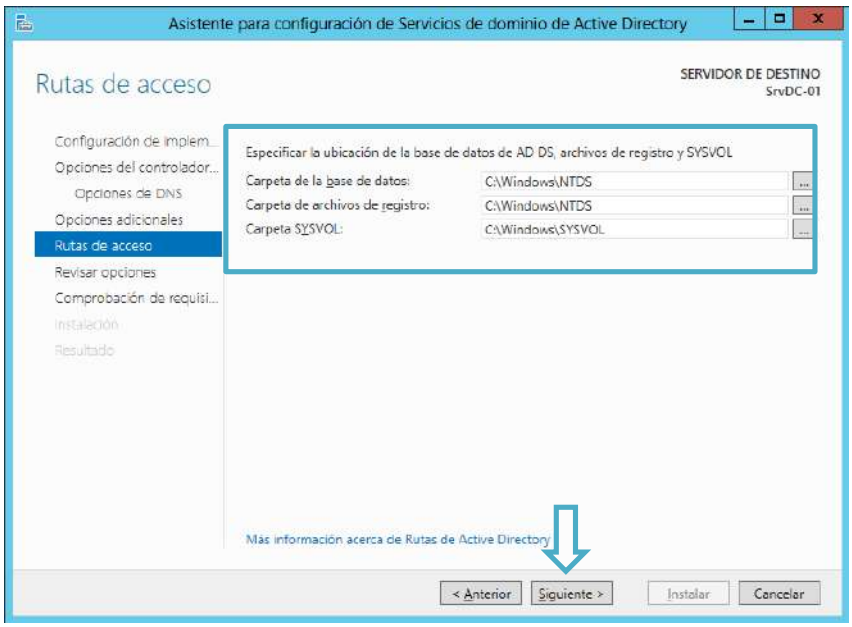


Figura 3. 23: Ruta de acceso

23. Nos mostrara un resumen de la configuración que hemos realizado y un script que podría omitir todos los pasos que hemos realizado ver figura 3.24.

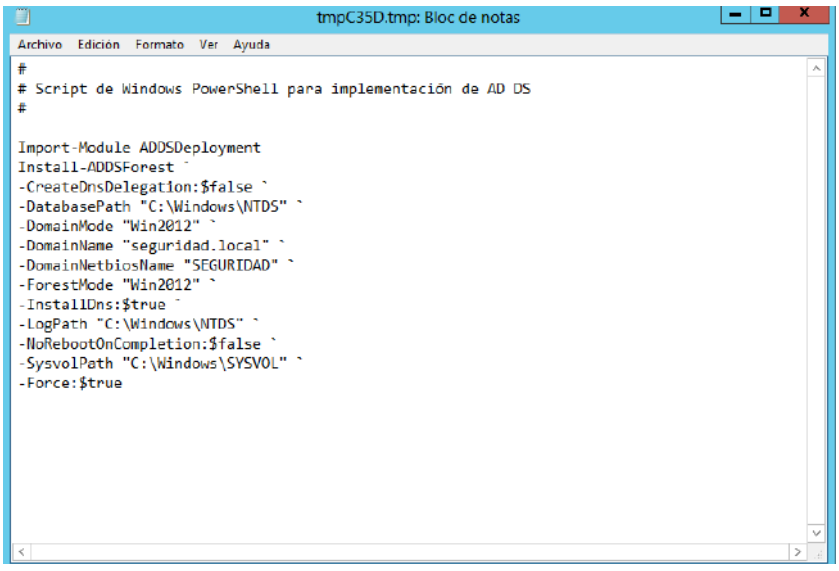


Figura 3. 24: Script para la implementación PowerShell

24. Como no es el caso en que hemos realizado el script podemos cerrar y dar clic en continuar ver figura 3.25.

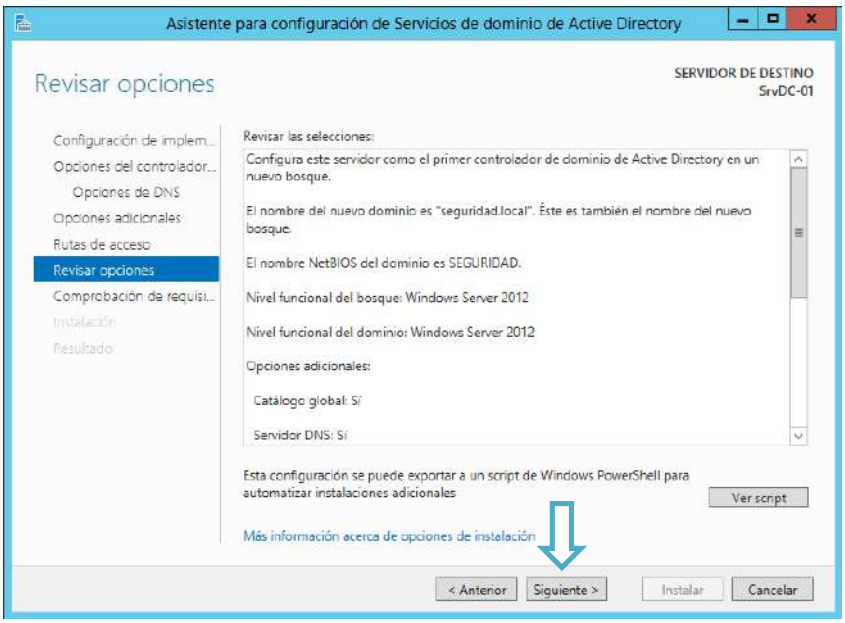


Figura 3. 25: Revisar Opciones

25. Esperamos a que los pre-requisitos de carguen y se validen. Una vez validados los pre-requisitos damos clic en instalar ver figura 3.26.

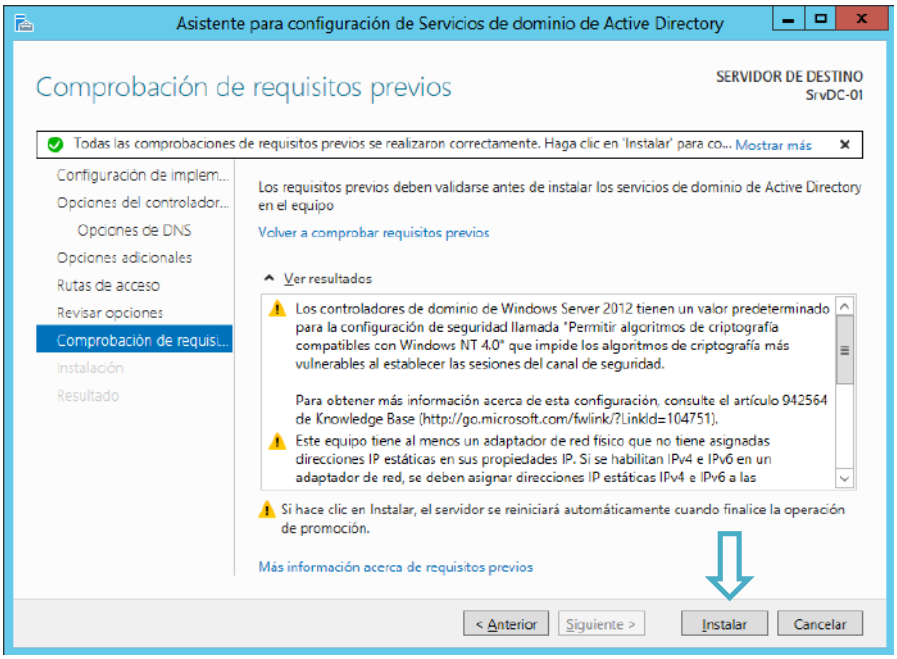


Figura 3. 26: Comprobación de requisitos previos

26. Una vez completa la configuración nos pedirá reiniciar el sistema hacemos clic en reiniciar ver figura 3.27.

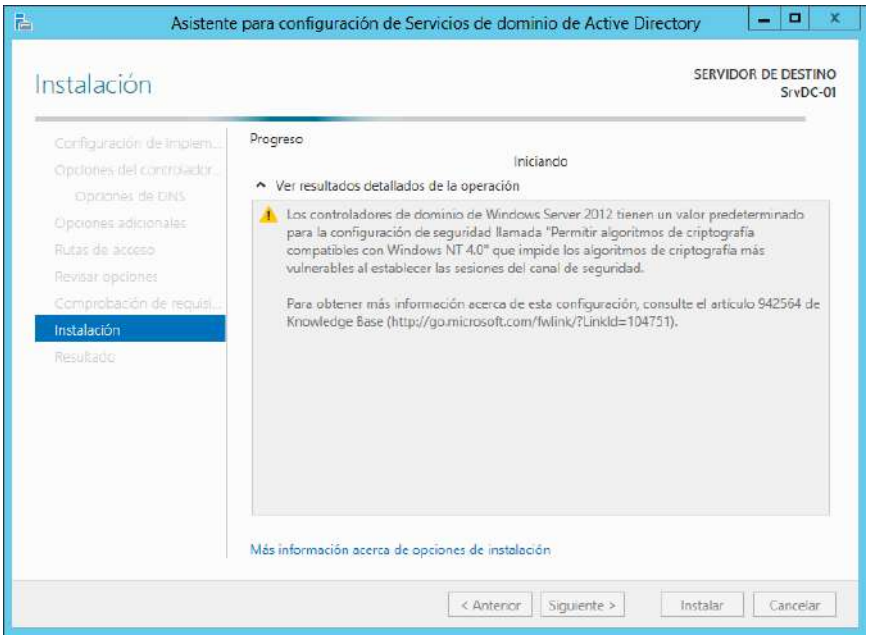


Figura 3. 27: Instalación controladores de dominio

27. Una vez que se reinicie el sistema aparecerá el nombre que fue asignado para el servidor ver figura 3.28.

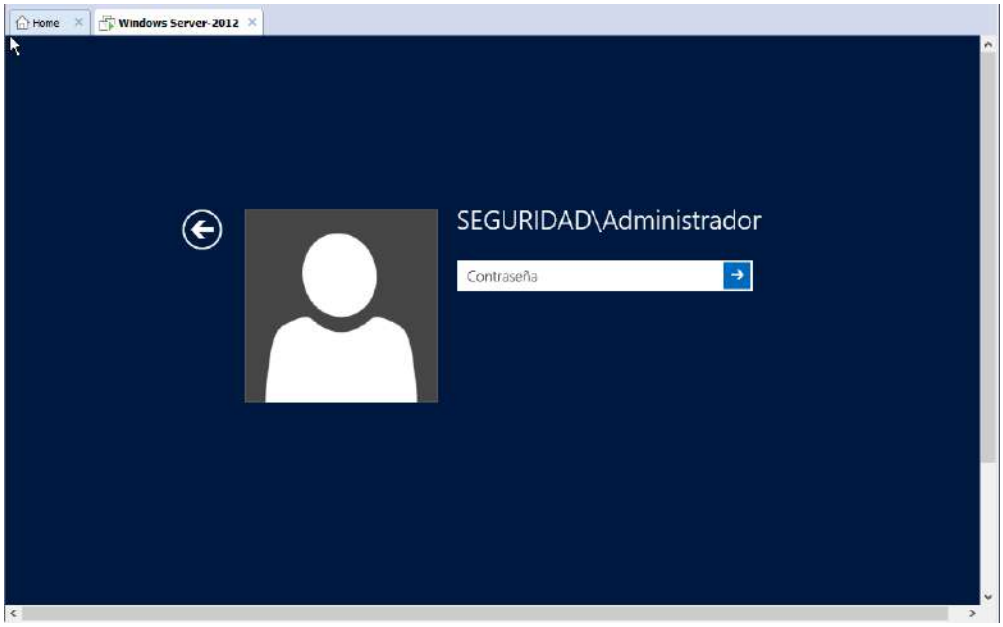


Figura 3. 28: Visualización del nombre asignado por el servidor

28. Ingresaremos y realizamos la verificación de la post instalación del rol. Por defecto cuando se instala un rol por primera vez la dirección de DNS se cambia por la dirección local del servidor ver

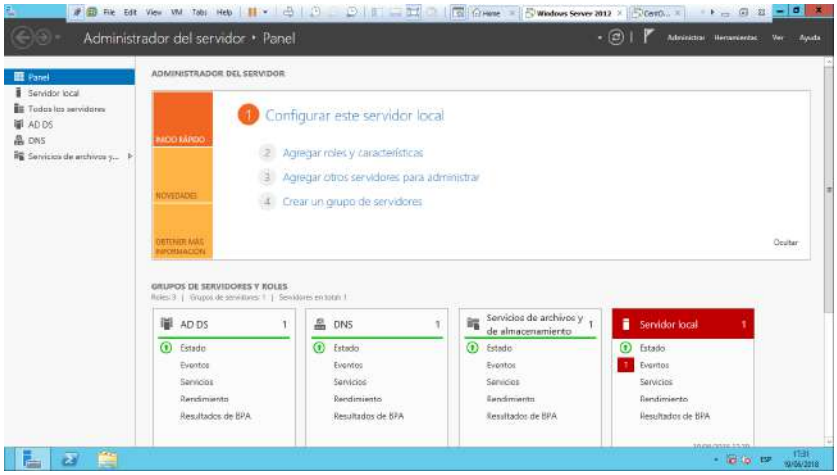


figura 3.29.

29. Para ello vamos a cambiar la IP que sale por defecto 127.0.0.0, la cambiaremos por la 192.168.239.12 porque esa IP, fue asignada en los pasos anteriores:
    - Vamos a la parte de administrador de redes damos clic derecho en la red.
    - Vamos a ipv4 y propiedades (Cuando enumeren los pasos pongan el número de pasos que hay que repetir) nos fijaremos que la dirección de DNS se ha cambiado reemplazaremos por la dirección IP asignada y damos clic en aceptar ver figura 3.40.

Figura 3. 29: Verificación de la instalación DNS

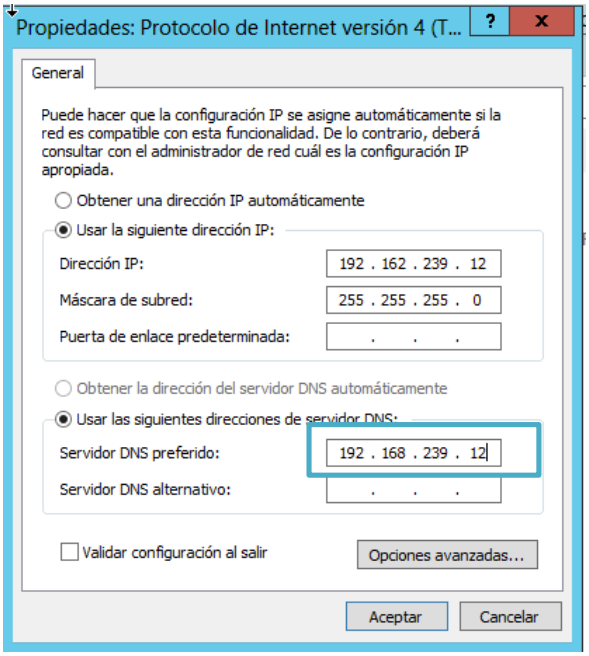


Figura 3. 30: Propiedades Protocolo de Internet IPv4

30. El servicio DNS es importante para el buen funcionamiento del servicio de dominio para ello vamos a verificar que esté funcionando correctamente. Ingresamos al administrador de servicios a la pestaña herramientas y escogemos DNS y damos clic ver figura 3.31, como podemos ver el servicio DNS esta iniciado y correctamente funcionando.

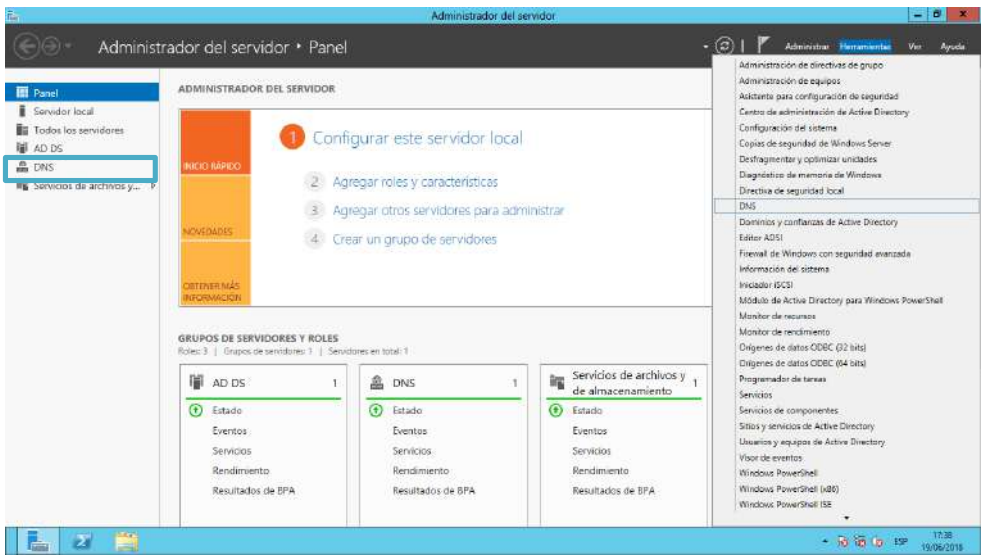


Figura 3. 31: Herramientas del administrador del servidor

31. Ahora vamos a revisar que el servicio esté funcionando correctamente, presionamos win+r o ejecutar y abrimos cmd(consola), escrribimos nslookup ver figura 3.32.

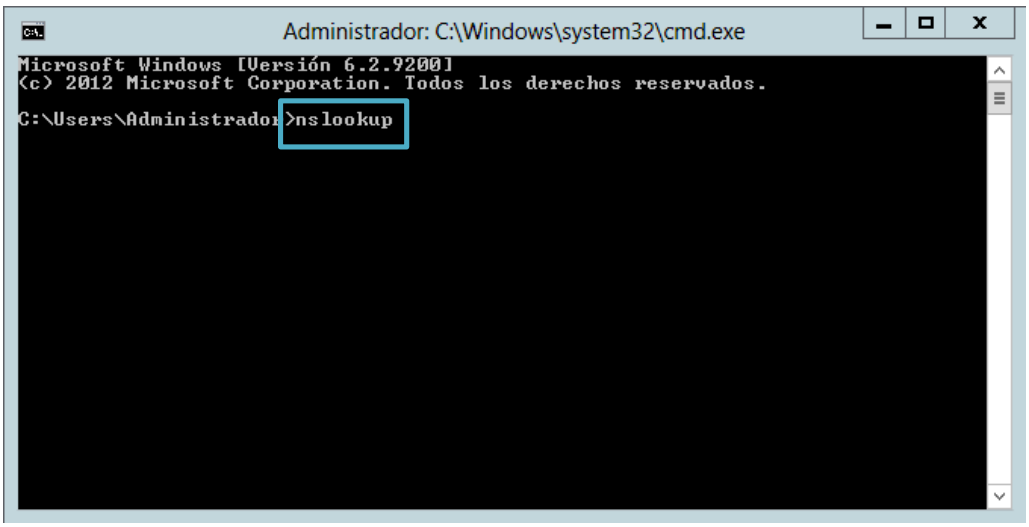


Figura 3. 32: Cmd Windows Server 2012

32. Como vemos se indica un Unknow esto pasa, porque el servidor no reconoce la ip 192.168.239.12, ver figura 3.33.

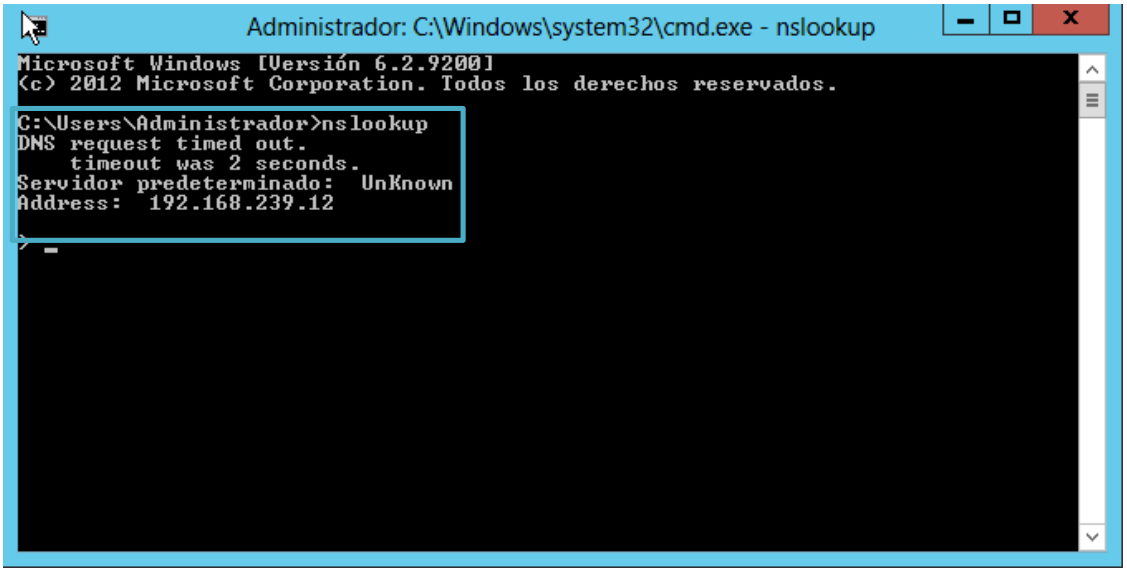


Figura 3. 33: Cmd no reconoce IP

33. Para solucionar este inconveniente vamos a crear una zona de reversa inversa, para ello vamos al administrador de DNS y damos clic derecho en Zona de búsqueda inversa y presionamos nueva zona ver figura 3.34.

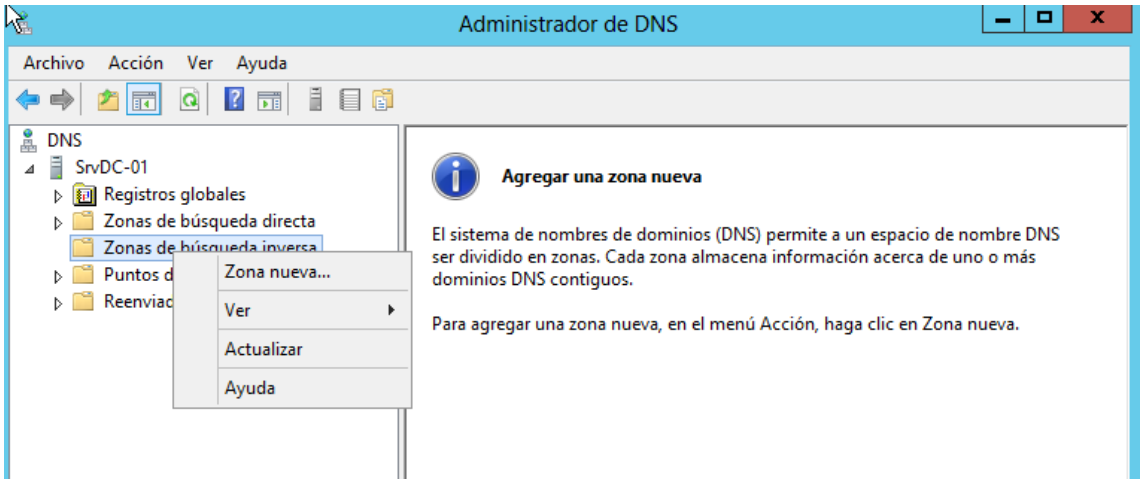


Figura 3. 34: Administrador del DNS

34. Muestra una venta para la creación de nueva zona damos clic en siguiente ver figura 3.35.

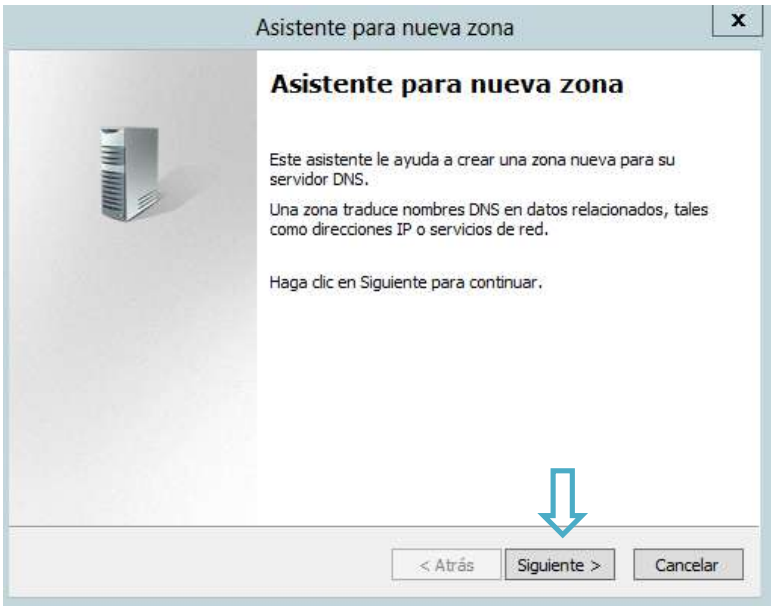


Figura 3. 35: Asistente para ámbito

35. Marcamos la casilla indicando que la zona es primaria y que se va a almacenar en el directorio activo y damos clic en siguiente ver figura 3.36.

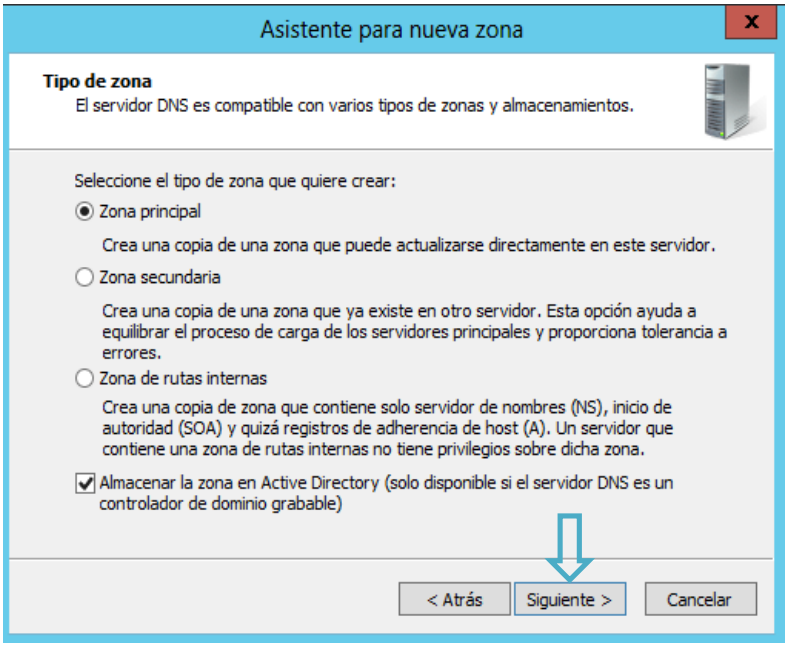


Figura 3. 36: Seleccionar tipo de zona

36. Marcamos la opción que indique que la zona está disponible para todos los servidores DNS, que se ejecutan en controladores de dominio en este caso el controlador de dominio es seguridad.local y hacemos clic en siguiente ver figura 3.37.

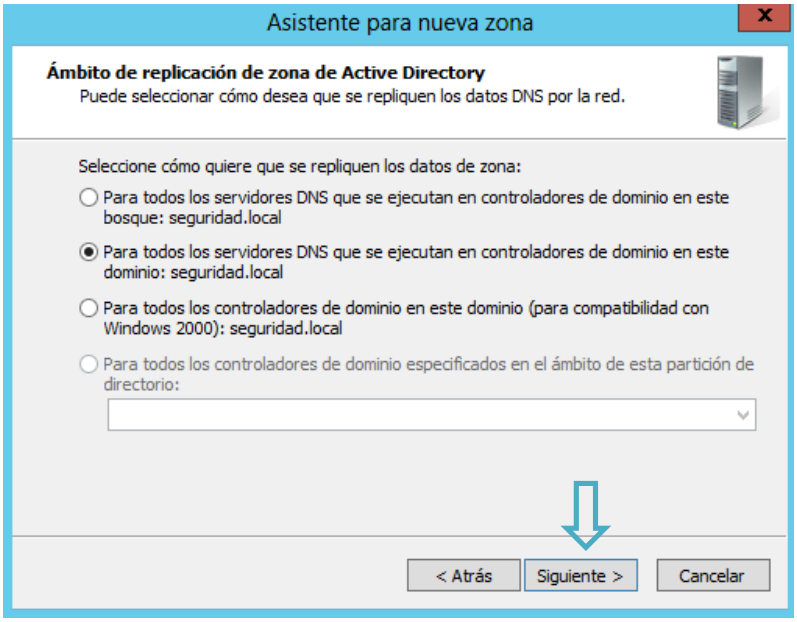


Figura 3. 37: Ámbito de replicación de zona de Active Directory

37. Dejamos marcada la opción zona de búsqueda inversa ipv4 y clic en siguiente.

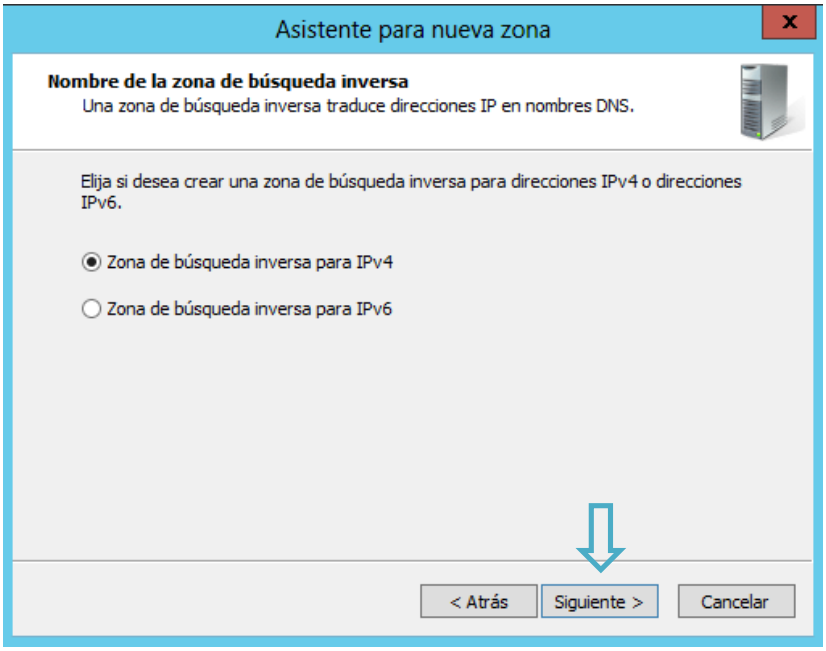


Figura 3. 38: Nombre de la zona de búsqueda inversa

38. Aparecerá una opción en la que ingresaremos los 3 octetos que serán los que no cambian en este caso 192.168.239 y clic en siguiente ver figura 3.39.

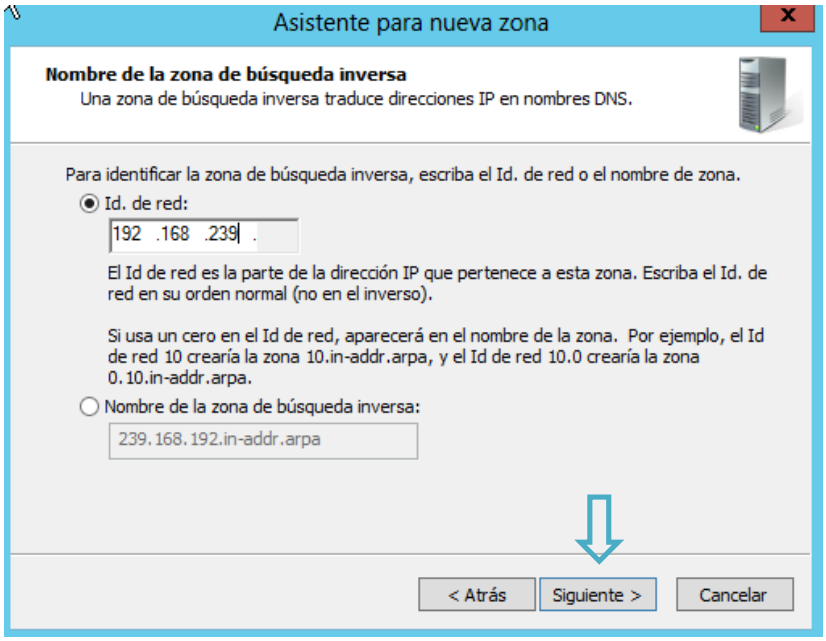


Figura 3. 39: Digitamos la IP de la red

39. Dejamos marcada la casilla que va a permitir actualizaciones dinámicas seguras (esto quiere decir que solamente se van a

crear los registros automáticos de aquellos equipos que estén dentro del dominio, es decir que un servidor Linux o cliente Linux no va a utilizar DNS, ya que hay se debe realizar el registro manualmente) damos clic en siguiente ver figura 3.40.

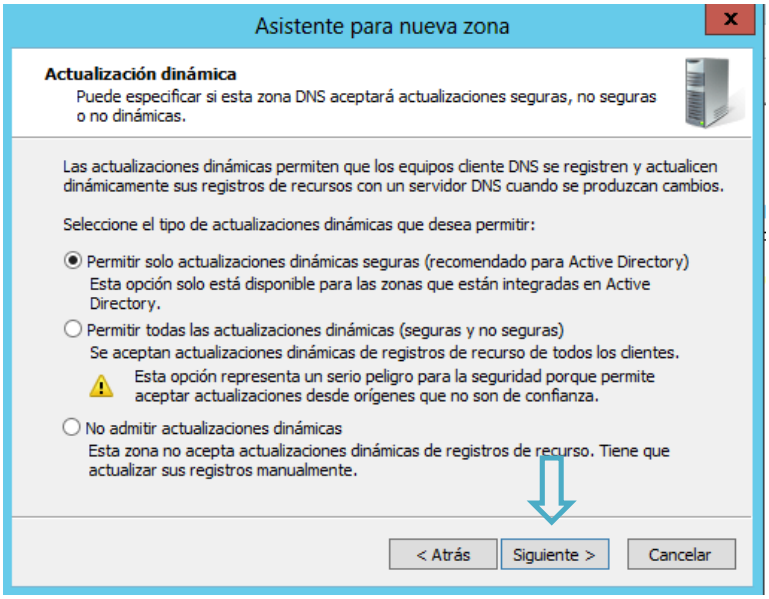


Figura 3. 40: Actualización dinámica

40. Luego hacemos clic en finalizar.

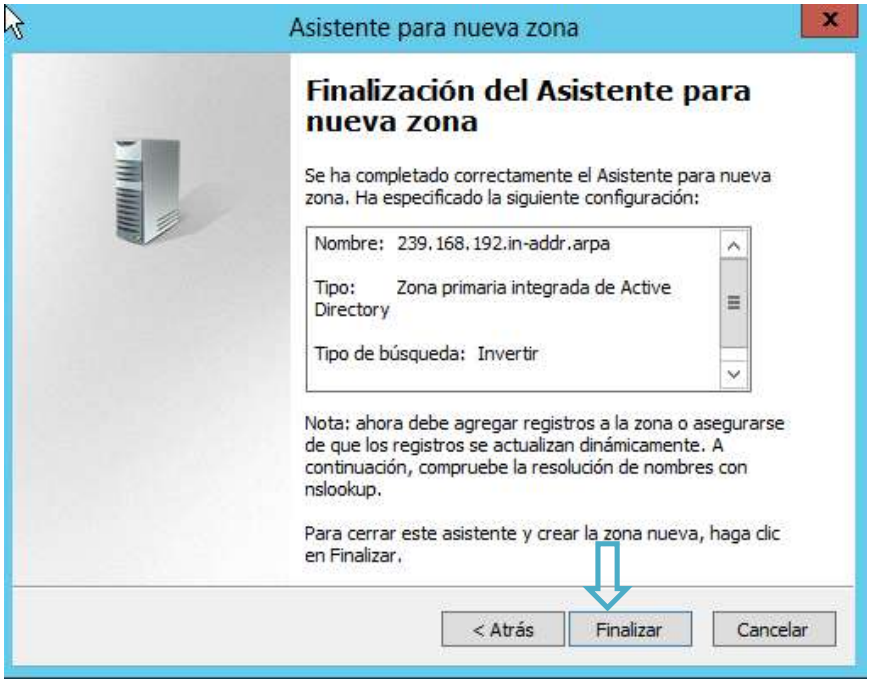


Figura 3. 41: Finalización del Asistente nueva zona

41. Una vez creada la zona de búsqueda de inversa hay que actualizar o crear el registro PTR ver figura 3.42.

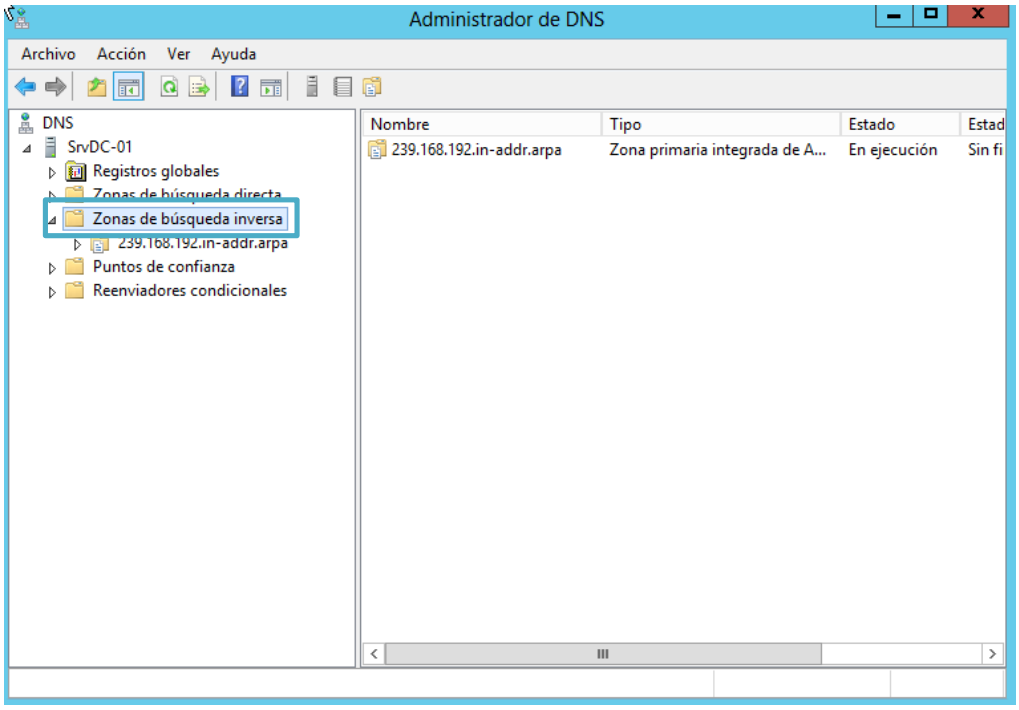


Figura 3. 42: Zona de búsqueda inversa

42. Para esto vamos a la zona seguridad.local damos doble clic sobre el registro de controlador.

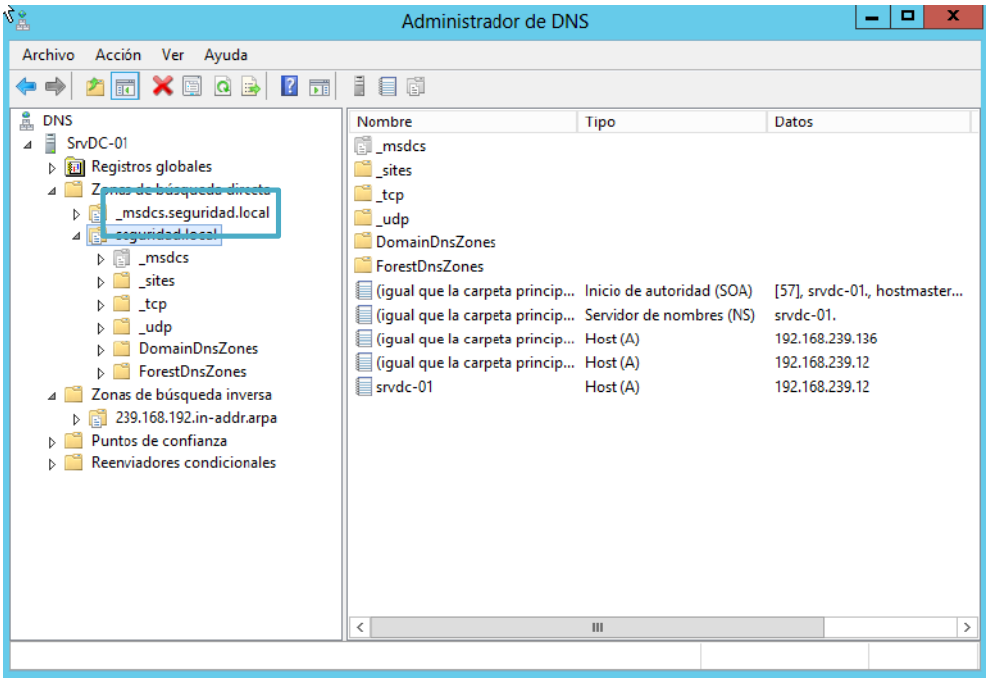


Figura 3. 43: Zona de búsqueda directa

43. Mostrará una ventana en la que marcaremos la opción de actualizar registro PTR y damos clic en aplicar y aceptar.

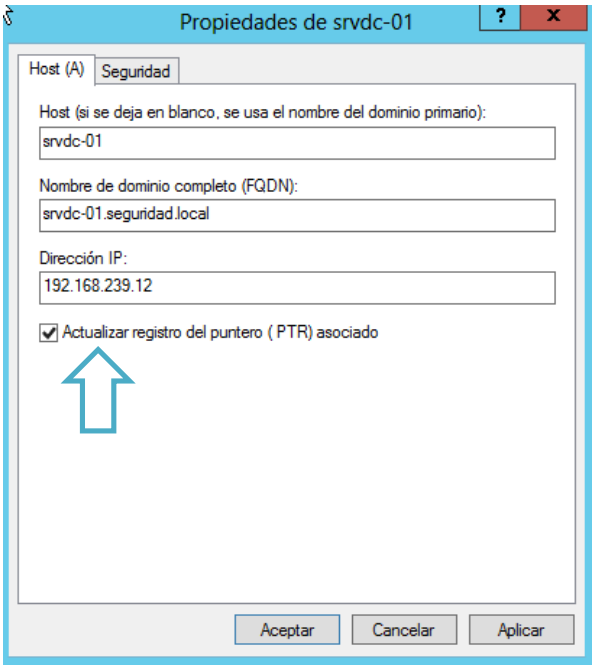


Figura 3. 44: Propiedades de SrvDC-01

44. Dirigir a nuestra zona de búsqueda de inversa y nos debería mostrar nuestro registro PTR.

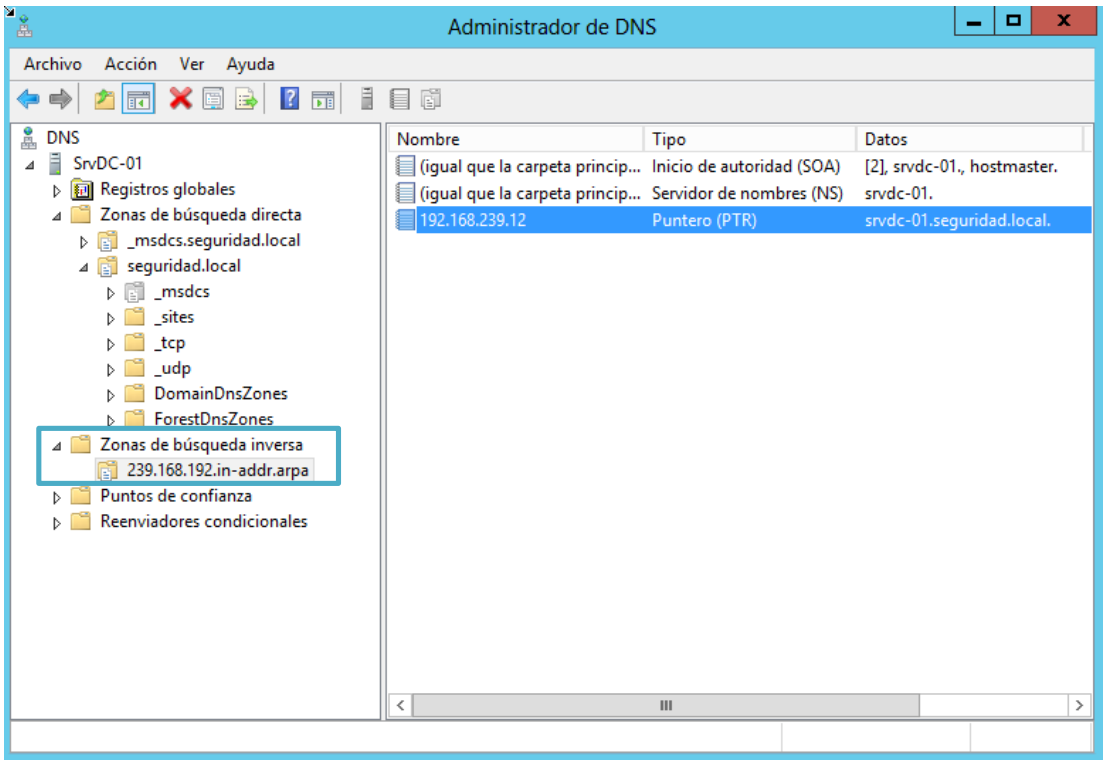


Figura 3. 45: IP zona de búsqueda inversa

45. Dirigirse nuevamente a nuestra venta de comandos y ejecutamos nuevamente el comando nslookup.

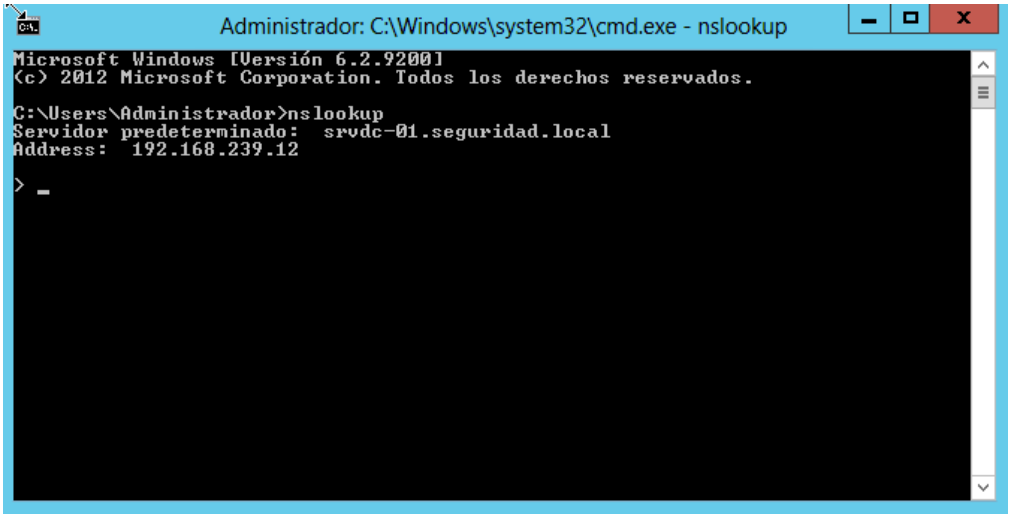


Figura 3. 46: Cmd ejecutando el comando nslookup

Como podemos observar en la figura anterior nuestro servidor está correctamente instalado y hemos finalizado la configuración del controlador de servidor de dominio.

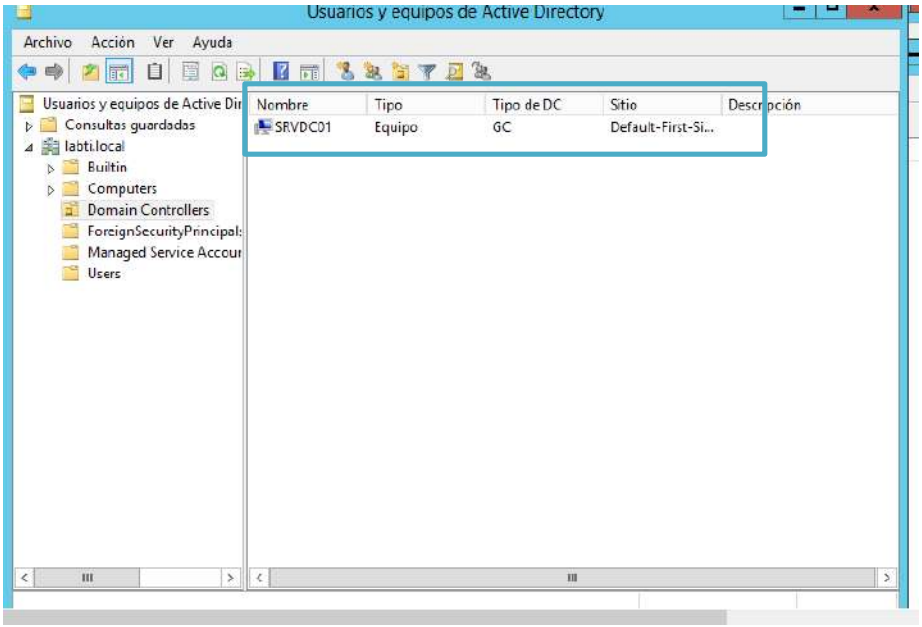


Figura 3. 47: Controladores de dominio

¿Sabías Qué?

3.4. Unión de controladores de dominio

Esta propuesta pretende mostrar el paso a paso de la unión de dos controladores de dominio que pertenecen a los servidores de la zona LAN (SrvDC-01/SrvDC-02), para que exista una replicación de las configuraciones e informaciones o datos en ambos servidores.

Los servidores Windows server 2012 de la zona LAN (SrvDC-01/SrvDC-02), sus direcciones IP son las siguientes respectivamente: 192.168.239.12/24 y 192.168.0.19, ambos pertenecen a la interfaz de red eth1 del servidor firewall ubicado en la Zona WAN de la red.

> Un controlador de dominio controla la autenticación, autorización, mantiene el ciclo de vida de la seguridad de las identidades en una compañía.

3.4.1. Pasos para unir controladores de dominio

Para unir los controladores de ambos servidores pertenecientes a la zona LAN utilizar los siguientes pasos:

1. En el panel del administrador del servidor SrvDC-02, clic en configuración posterior, clic en promover este servidor a controlador de dominio. Como se observa en la Figura 3.48.

Figura 3. 48: Menú principal

2. Habilitar la opción "agregar un controlador de dominio a un dominio existente", escribir el nombre del dominio del primer servidor seguridad.local, clic en cambiar. Como se observa en la Figura 3.49.

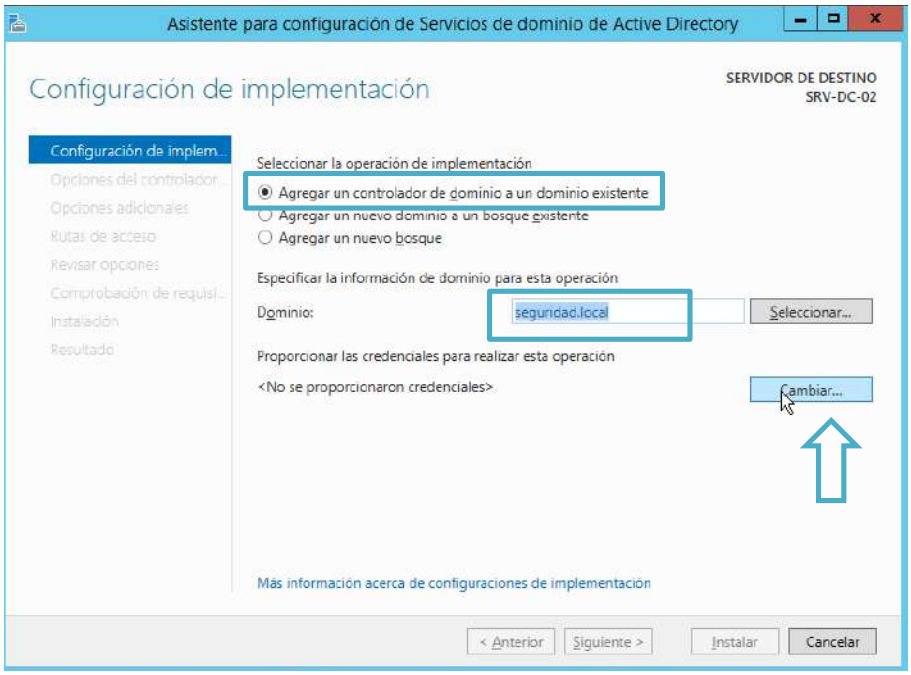


Figura 3. 49: Configuración de implementación

3. Ingresar como administrador al sistema para proporcionar las credenciales a la implementación, escribir SEGURIDAD\Administrador, contraseña, clic en aceptar y clic en siguiente. Como se observa en la Figura 3.50.

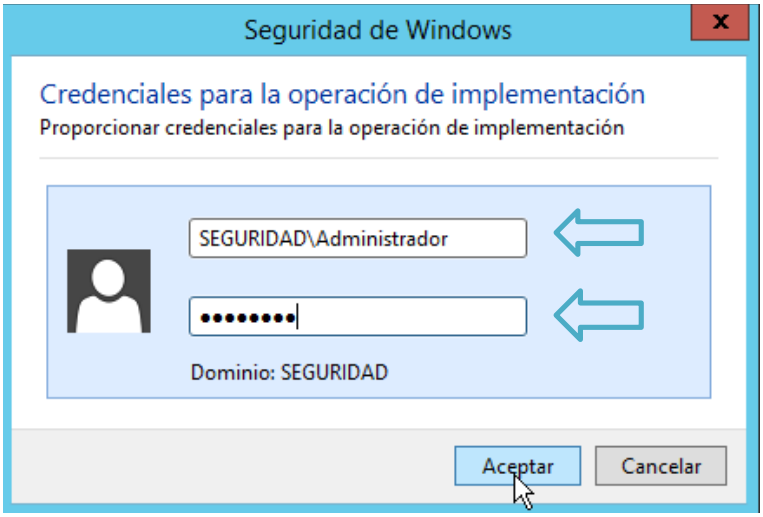


Figura 3. 50: Credenciales para la operación de implementación

4. En opciones del controlador de dominio habilitar el servidor del sistema, el catalogo global, desactivar el controlador de dominio de solo lectura, escribir la contraseña, clic en siguiente. Como se observa en la Figura 3.51.

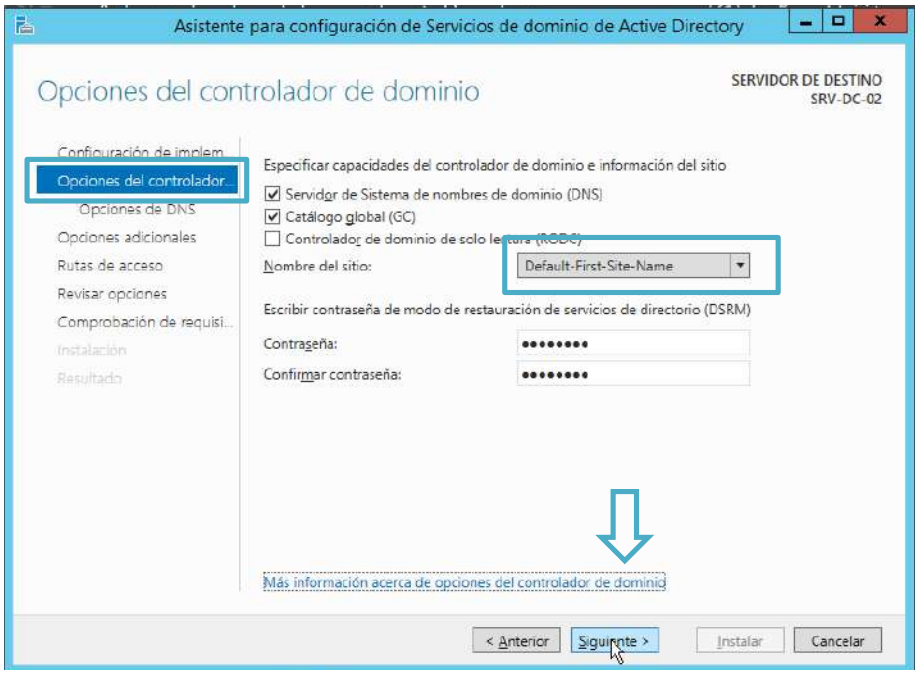


Figura 3. 51: Opciones del controlador de dominio

5. Como opciones adicionales, escribir la ruta de configuración, el nombre del primer servidor y el nombre del dominio, clic en siguiente. Como se muestra en la figura 3.52.

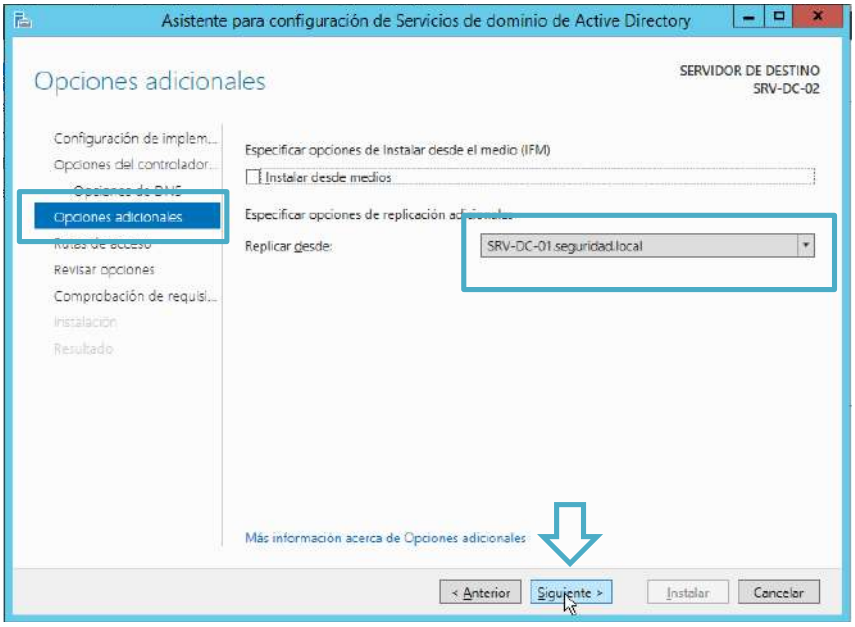


Figura 3. 52: Opciones adicionales

6. En rutas de acceso, especificar la ubicación de la base de datos del Active Directory, clic en siguiente. Como se observa en la Figura 3.53.

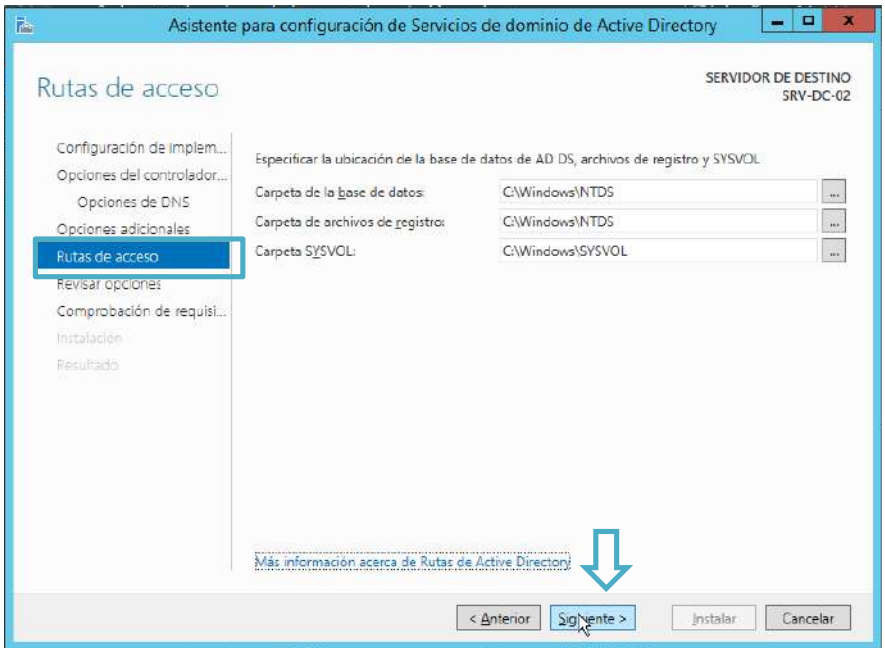
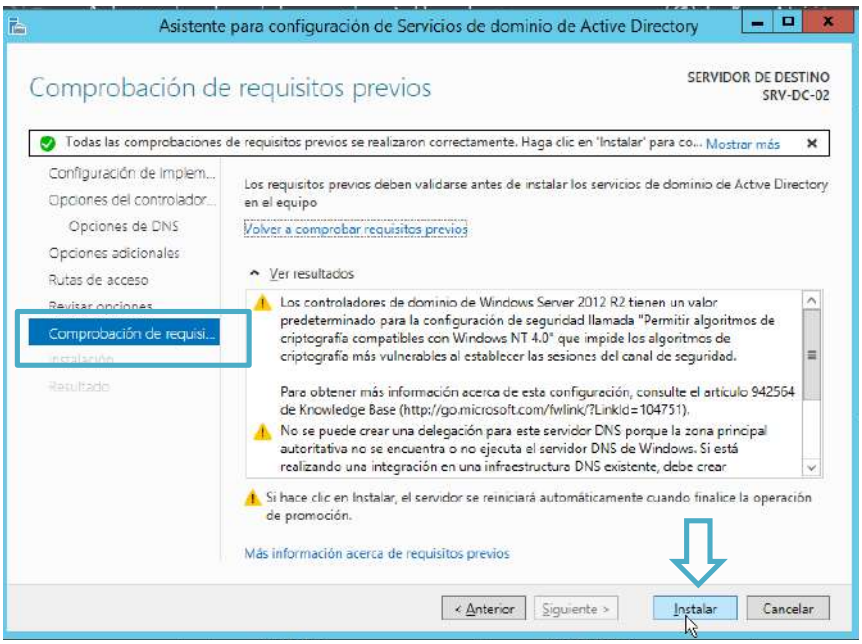


Figura 3. 53: Rutas de acceso

7. En la ventana revisar opciones, verificar toda información realizada, clic en siguiente, realizar la comprobación de requisitos previos, dar clic en instalar. Como se observa en la Figura 3.54, luego el equipo se reiniciara para guardar todos los cambios realizados, dar clic en cerrar.



z

¿Sabías Qué?

pertenecientes a una misma zona puedan comunicarse entre sí, al igual que con las demás zonas.

Figura 3. 54: Requisitos previos

3.5. Duplicando el controlador del dominio

El propósito de clonar un controlador de dominio, es que puede implementar una restauración rápidamente durante la recuperación de desastres, mediantes la restauración de los servicios de dominio de Active Directory. Para poder clonar necesitas, tener instalado el hipervisor, luego de esos seguimos los siguientes pasos que debes realizar para clonear un controlador de domino:

1. Dirigirse herramienta opción Usuarios y Equipos Active Directory y buscamos donde dice dominio controlador aparecerá un equipo que fue el que creamos al principio para colonearlo dentro de ese equipo que creamos clic derecho propiedades ver figura 3.55.

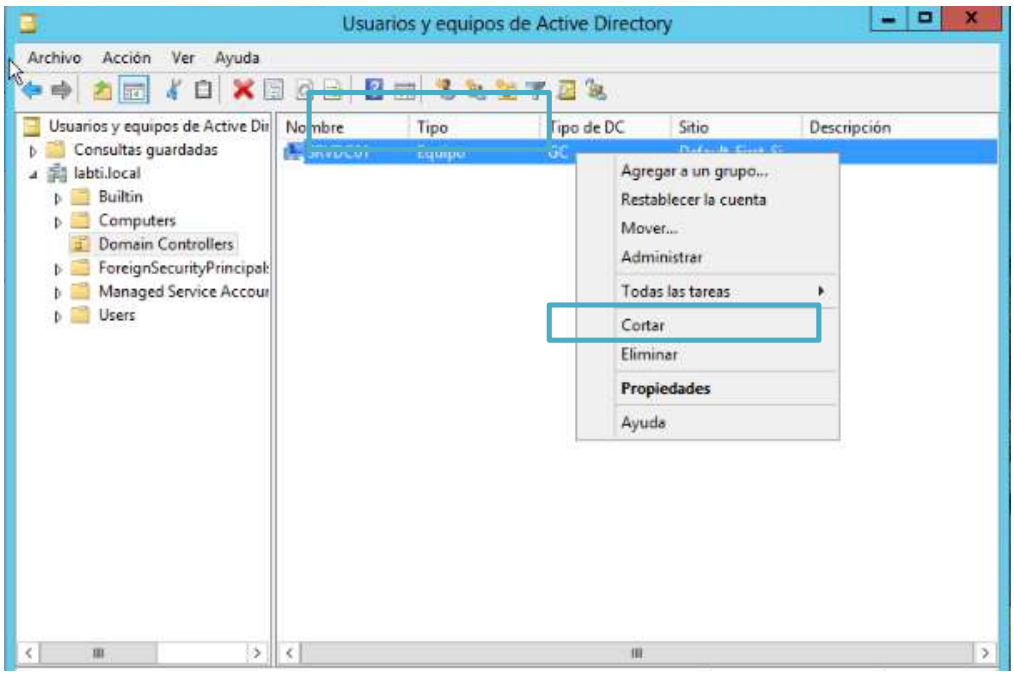


Figura 3. 55: Usuarios y equipos Active Directory

2. Luego se mostrará una ventana donde seleccionar grupos opciones avanzadas buscamos la opción controladores de dominio clonables aceptar ver figura 3.56.

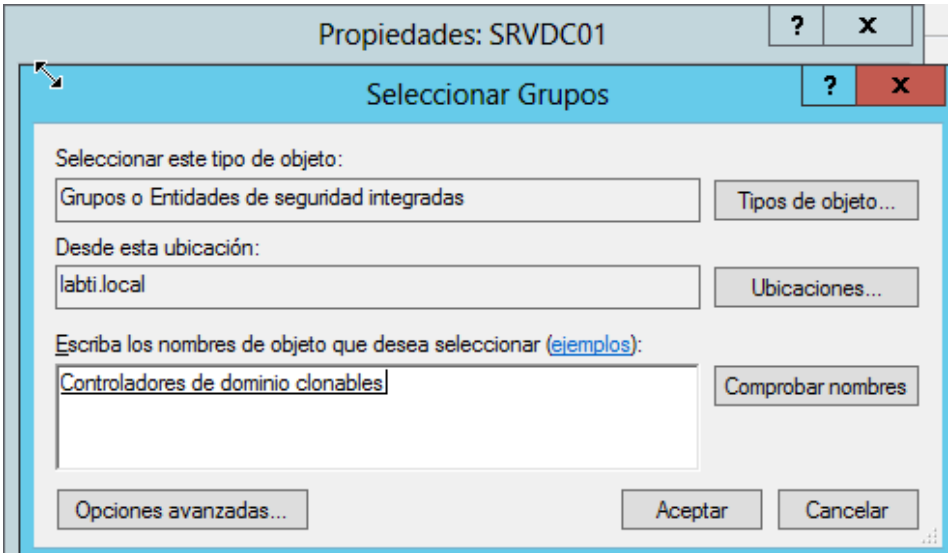


Figura 3. 56: Seleccionar Grupos

3. Clic en acepar luego aplicar, como observamos en la siguiente figura ya estamos listos para clonar ver figura 3.57.

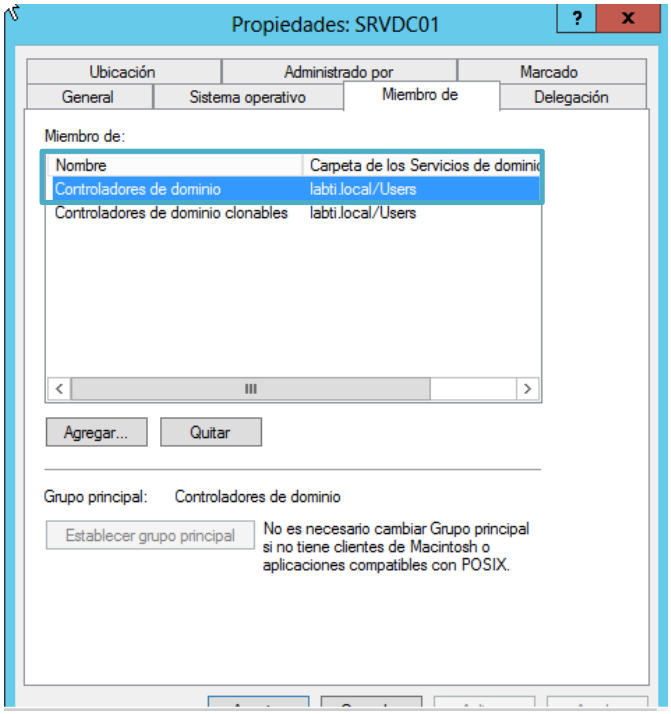


Figura 3. 57: Miembros de controladores de dominio

4. Abrimos la ventana Windows PowerShell y digitamos los siguientes comandos Get-ADDCCloningExcludeApplicationList ver figura 3.58.

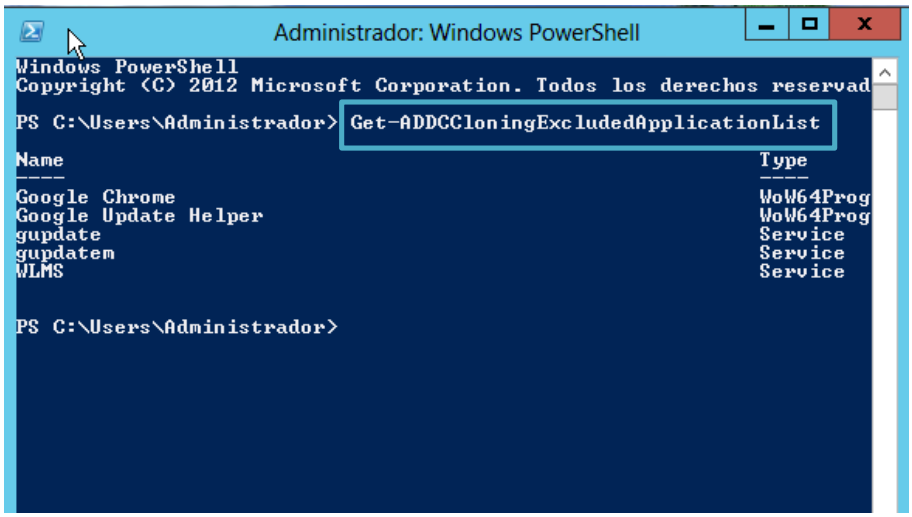


Figura 3. 58: Administrar Windows PowerShell

5. Reiniciamos el servidor para que actualice sus credenciales con la pertenencia al grupo. En cada Controlador de Dominio tenemos un archivo con la estructura necesaria, sólo debemos personalizarlo.

Hay que ejecutar como administrador el Notepad, y haciendo que muestre todos los tipos de archivos abrir uno llamado SampleDCCloneConfig.xml que se encuentra en C:\Windows\System32. Copia ese archivo XML y lo pego el contenido del archivo ya modificado resaltando lo que he agregado; este archivo debemos guardarlo en C:\Windows\NTDS con el nombre DCCloneConfig.xml (Delprato, 2013) como se muestra la figura 3.59.

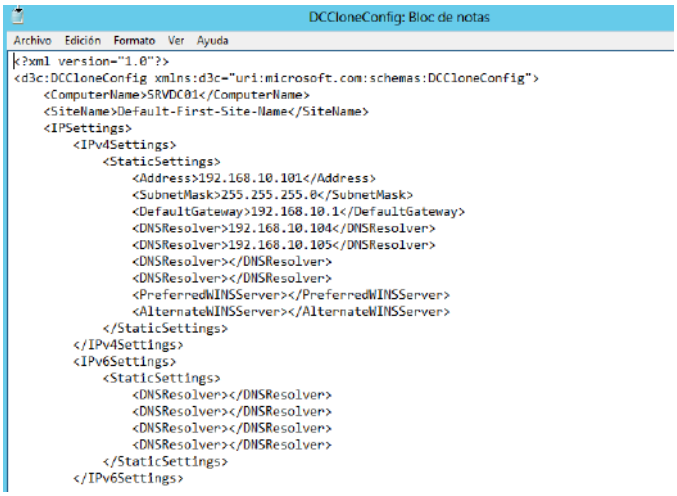


Figura 3. 59: Configurando el archivo XML con nuestra IP para clonar

6. Luego nos dirigimos usuarios y equipos de Active Directory buscamos el administrador en este caso es labti.local clic derecho maestro de operaciones esto permite asignar grupos RID a otros controladores de dominio.

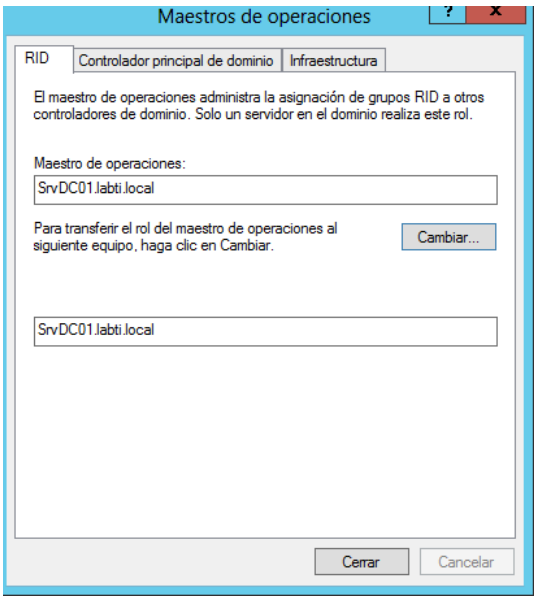


Figura 3. 60: Maestro de operaciones

7. Luego nos dirigimos al Hyper-V en la parte derecha escogemos opción crear una máquina virtual clonables y damos clic en siguiente ver figura 3.61.

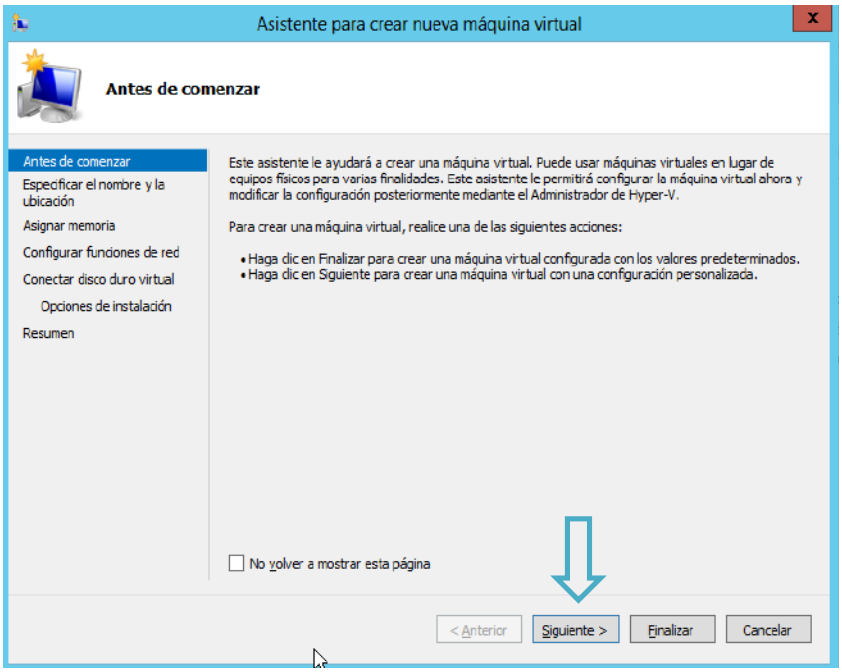


Figura 3. 61: Crear una máquina virtual

8. Introducimos el nombre de la máquina y la ubicación donde se guardará Hyper-V, ver figura 3.62.

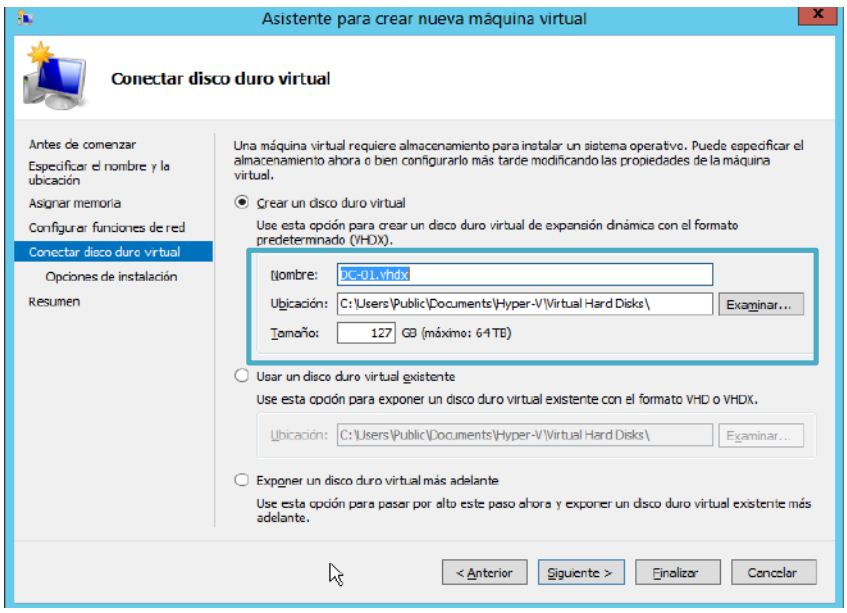


Figura 3. 62: Creando un disco duro virtual

9. Mostrará un resumen de la creación de la máquina virtual, le dar clic en finalizar como se muestra la figura 3.63.

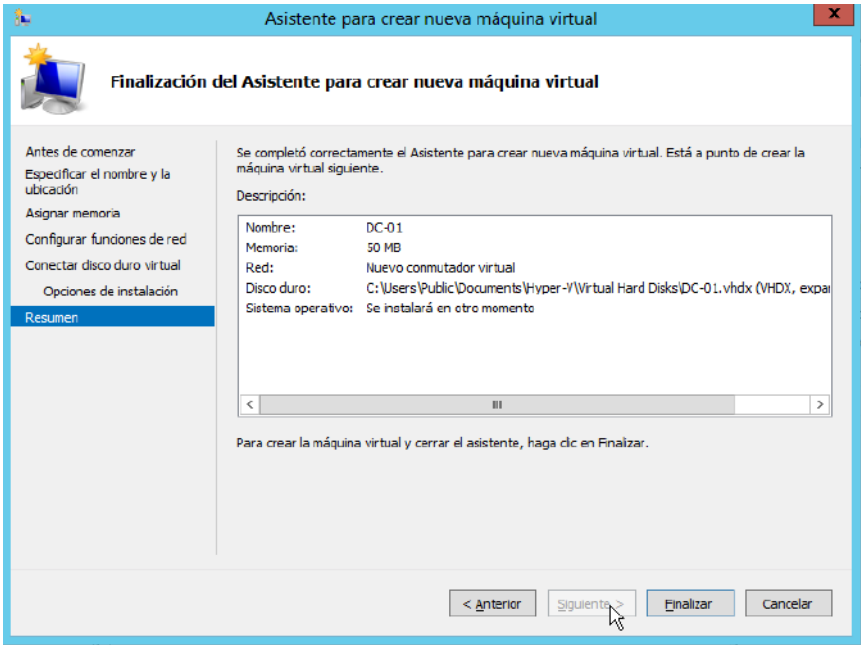


Figura 3. 63: Finalización crear máquina virtual

10. Como podemos observar ya creamos la máquina virtual en el administrador de Hyper-V ver figura 3.64.

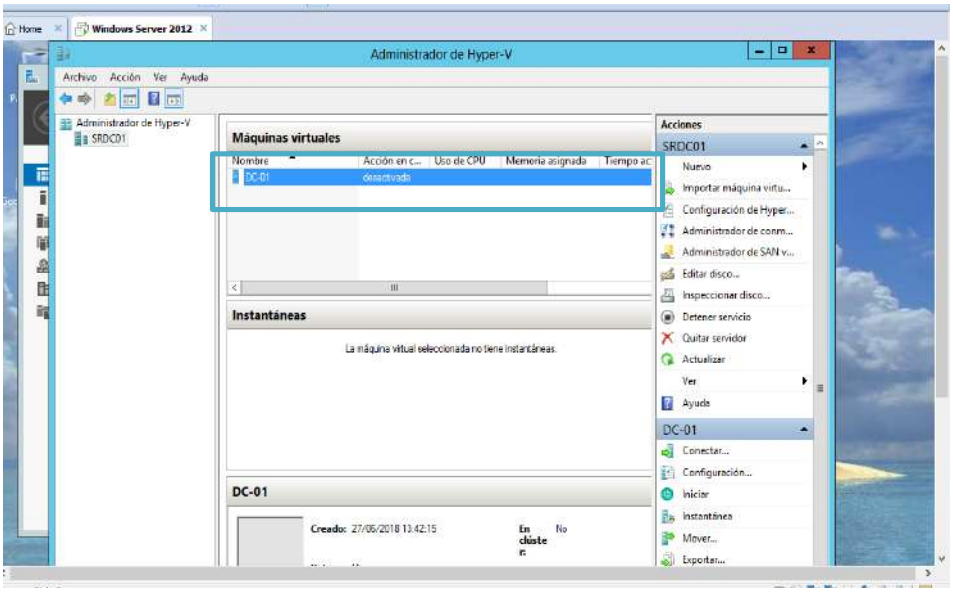


Figura 3. 64: Máquina virtual Hyper-V

11. Dirigimos en la parte derecha DC-01 exportamos y colocamos el archivo o carpeta que queremos exportar es decir carpeta clonada y exportamos como se muestra la figura 3.65.

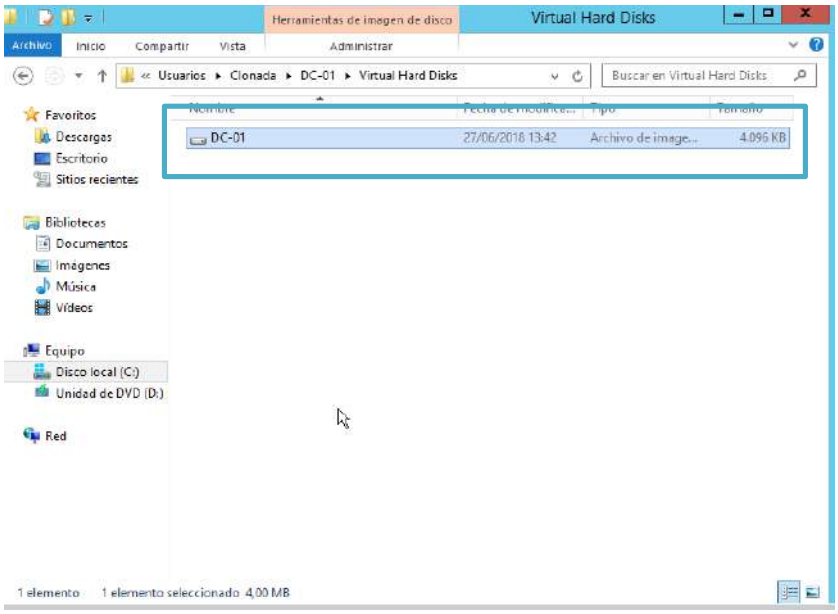


Figura 3. 65: Clonando la máquina virtual DC-01

12. Luego vamos a importar la máquina virtual DC-01 damos siguiente nuevamente siguiente y al finalizar mostrara un resumen de la asistencia de importaciones ver figura 3.66.

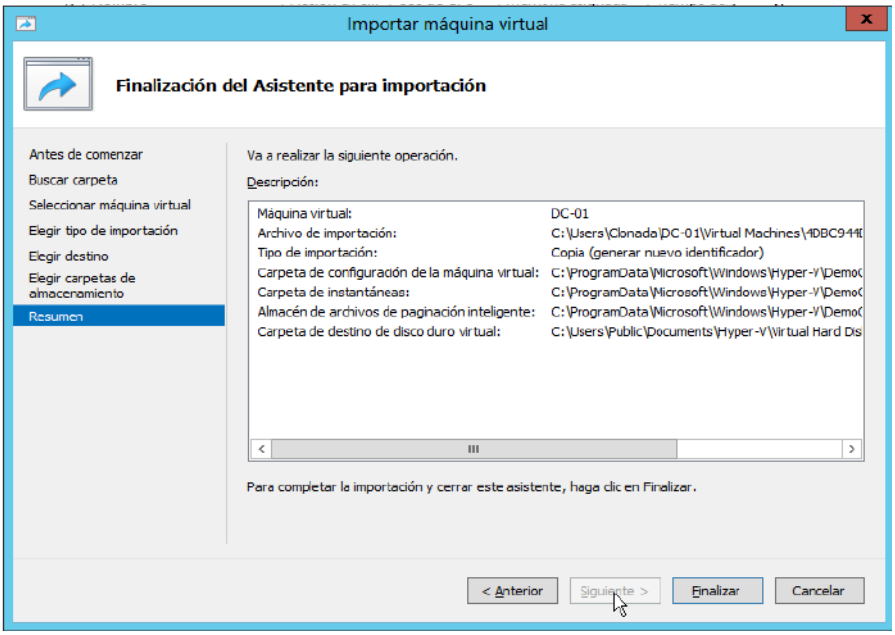


Figura 3. 66: Finalización la importación máquina virtual

13. Luego reiniciamos el equipo para que comience la clonación.

Figura 3. 67: Clonación controlador de dominio

3.6. Usuario de Dominio

Los dominios de usuario son un SecurityPattern común que permite a los usuarios poseer objetos y aun así poder compartirlos en la medida exacta que deseen. Pero cuál sería su definición, podría decir que es un conjunto de objetos sobre los que tienen control total. Si un sistema obedece a los ideales por ejemplo Seguridad , este es el subgrafo de objetos directamente debajo del usuario. Tenga en cuenta que un objeto puede pertenecer a más de un dominio de usuario. Es decir, los dominios de usuario pueden superponerse.

Crear usuario en Windows Server 2012, así como en cualquier otro Server, es algo muy simple y a la vez muy útil y necesario para poder llevar a cabo una buena administración de los usuarios que pertenecen a nuestro dominio. (Gutierrez, 2017)

Para eso seguimos los siguientes pasos:

1. Entramos en el administrador de servidor, dar clic en herramientas y luego presionamos usuarios y equipos de active Directory.
   Clic en nuestro controlador de dominio muestra un listado de opciones ahora para crear un usuario lo podemos realizar dentro de User pero como preferencia cree una unidad organizativa para ello me dirige a labti.local clic derecho nuevo objeto y unidad organizativa como se muestra la figura 3.68.

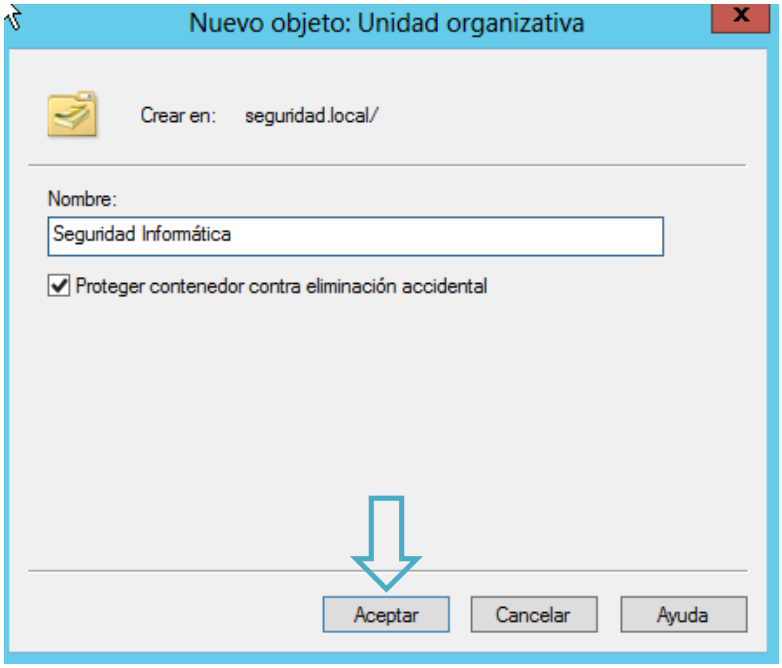


Figura 3. 68: Creación Unidad Organizativa

2. Listo ya tenemos nuestra unidad organizativa creada para así realizar la práctica.

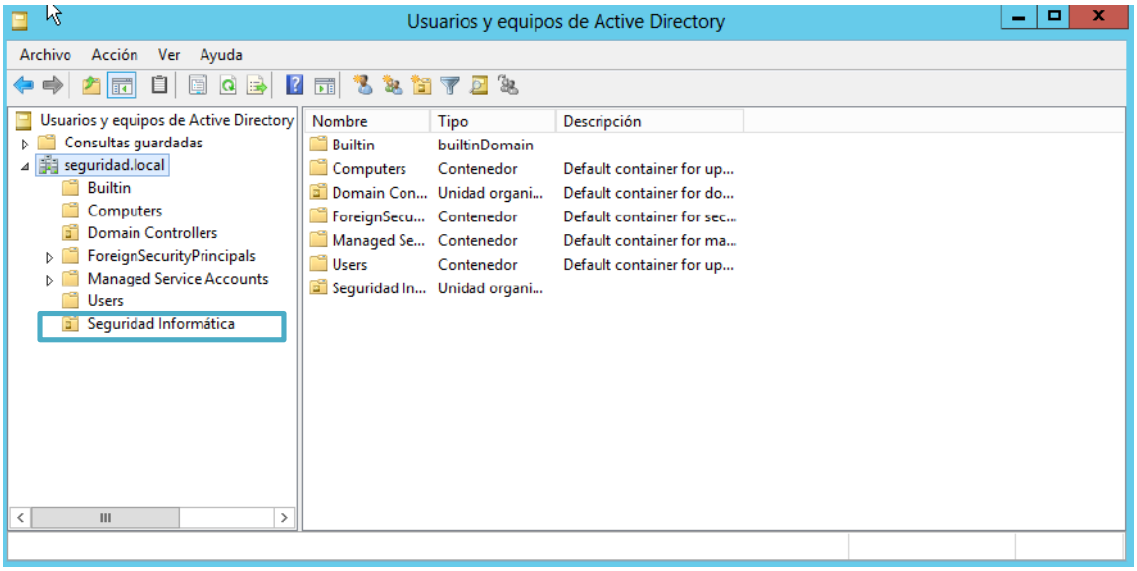


Figura 3. 69: Seguridad Informática creada

3. Dentro de la unidad organizativa le damos clic derecho nuevo objeto y usuario en la cual nos aparecerá que ingresemos los datos respectivos para la ceración de un usuario como se muestra la figura 3.70.

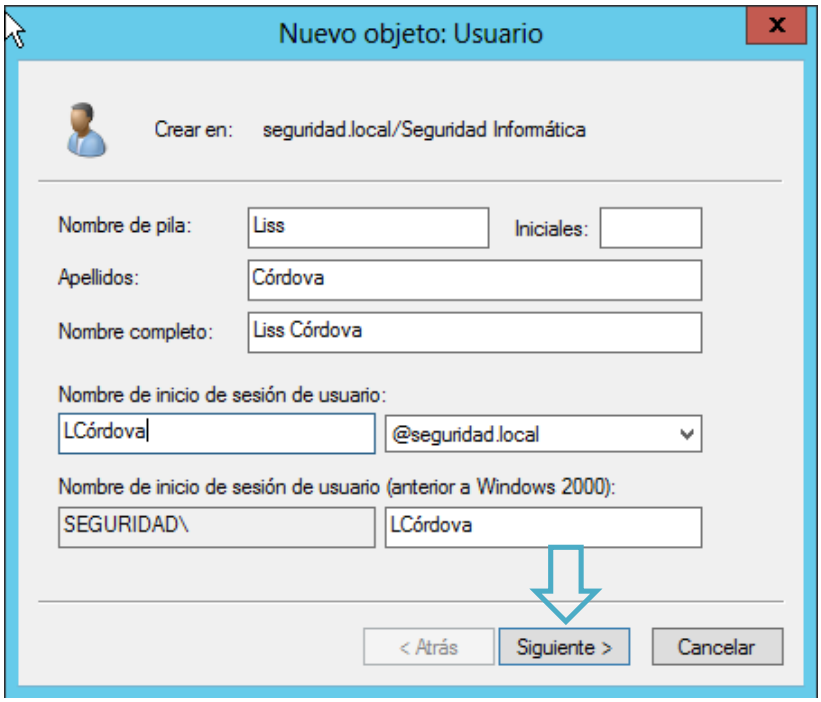


Figura 3. 70: Creación de un usuario

4. Luego nos pedirá que ingresemos la contraseña.

Figura 3. 71: Ingresando contraseña

5. Luego nos dará un resumen del proceso de la creación del usuario como se muestra la figura 3.72.

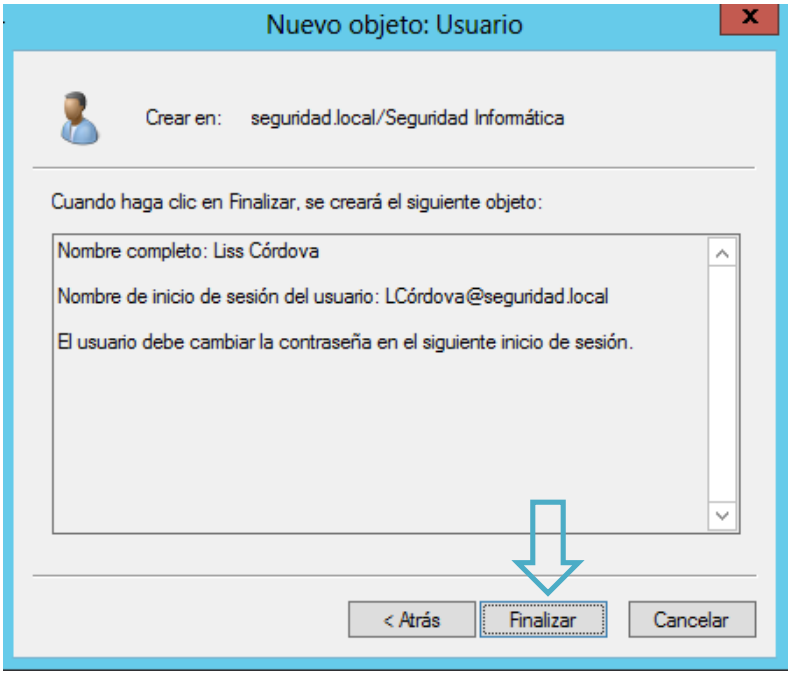


Figura 3. 72: Resumen del usuario

6. Listo ya tenemos el usuario creado.

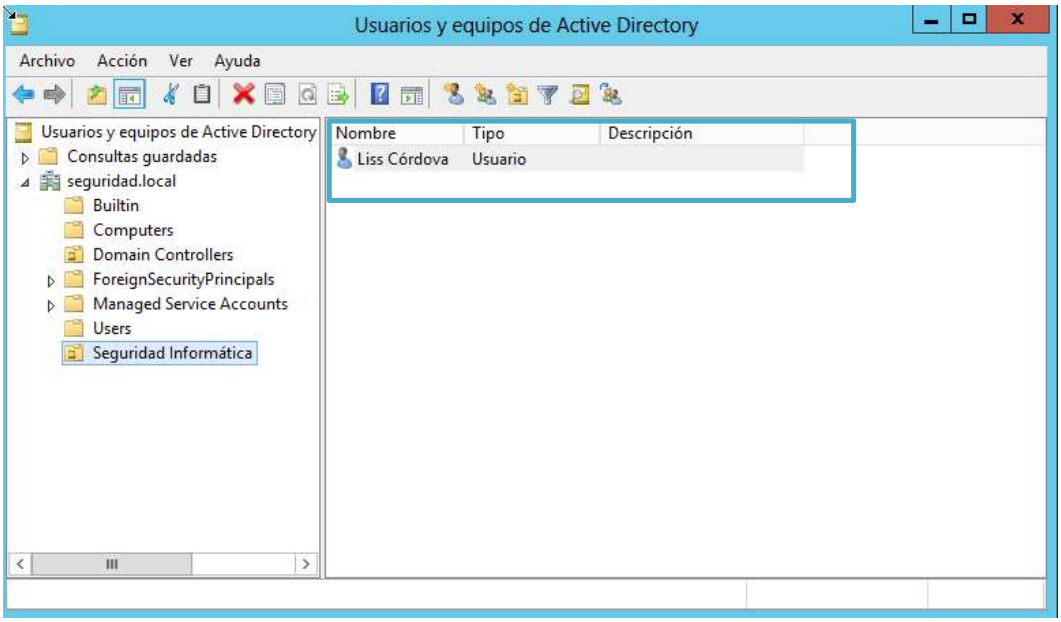


Figura 3. 73: Usuario Creado

3.7. Grupos Active Directory

Active Directory (AD) o Directorio Administrativo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Para agregar un grupo realizamos los siguientes pasos:

1. Nos dirigimos en la unidad organizativa que se llamara Seguridad Informática luego clic derecho y opción grupo como se muestra la figura 3.74.

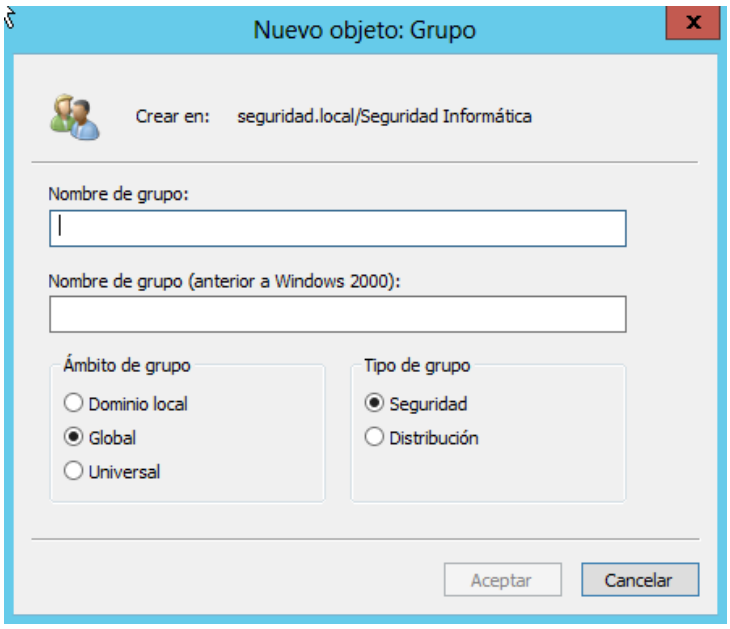


Figura 3. 74: Creación de un grupo

2. Llenamos los campos para crear el grupo y aceptamos, como se muestra la figura 3.75.

Figura 3. 75: Llenando los campos para creación de usuario

3. Listo se creó el grupo que se llama seguridad, ver figura 3.76.

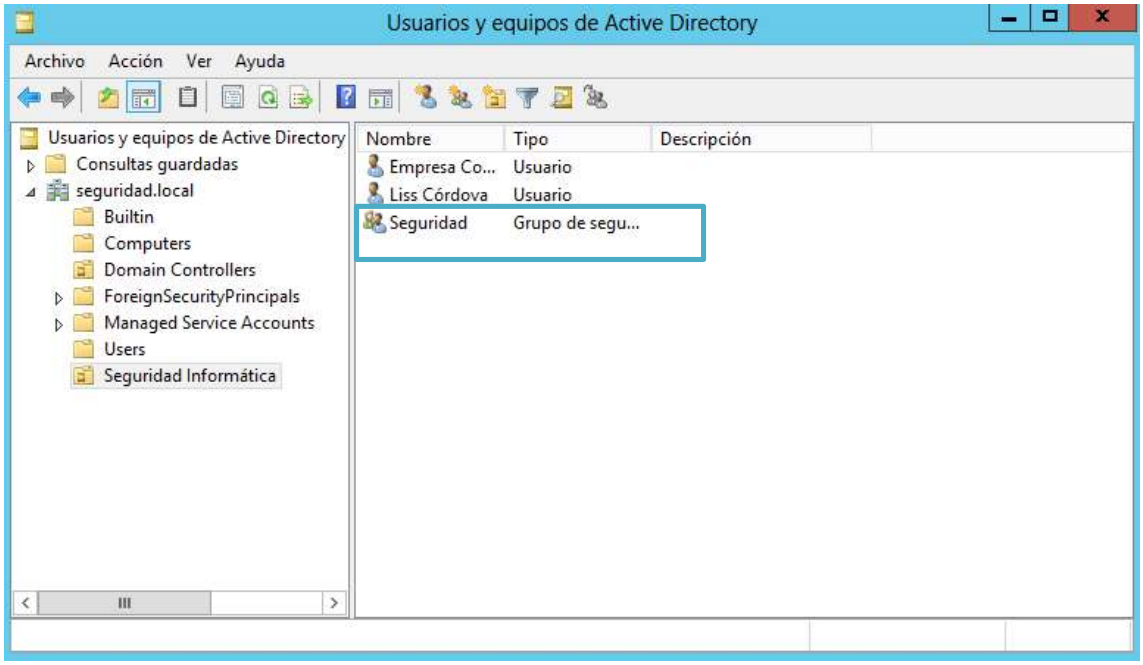


Figura 3. 76: Grupo creado

4. Dirigimos al usuario que creamos este caso Empresa Comisariato, clic derecho agregar un grupo, seleccionamos el grupo este caso seguridad y aceptamos, ver figura 3.77.

Figura 3. 77: Selección de Grupos

5. El usuario fue agregado con éxito al grupo, ver figura 3.78.

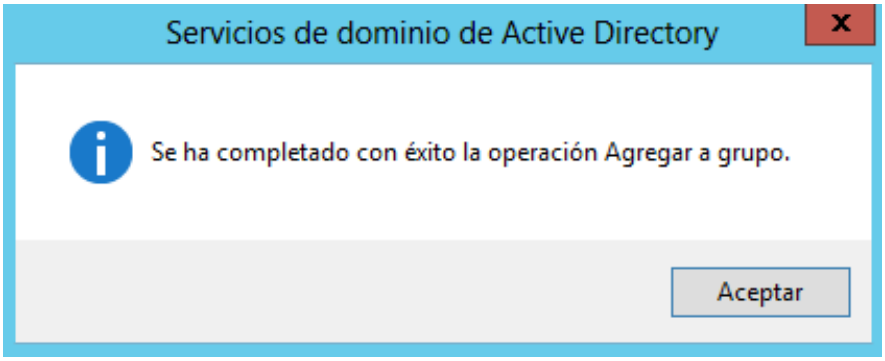


Figura 3. 78: Completando la agrupación del grupo

6. Ahora nos dirigimos al grupo de seguridad y confirmamos si en la opción miembro esta agregado el usuario y listo ya estamos agregados en un grupo.

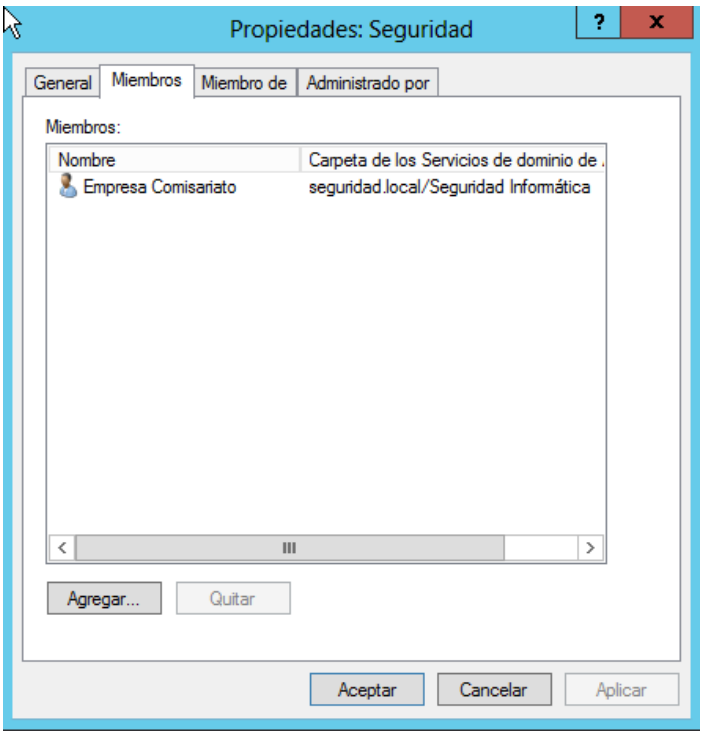


Figura 3. 79: Comprobando si el usuario esta agregado al grupo

¿Sabías Qué?

7. Por último, se procederá a agregar un equipo. Para esto se debe ir a la PC-01, que es la PC cliente.

NOTA:

Siguiendo el mismo procedimiento de agregar usuarios a un grupo se puede agregar los usuarios que queramos tener en los grupos que necesitemos.

Lo que se hará es iniciar sesión en la PC-01 con el usuario creado (Joshua Sailema). Para esto se inicia sesión con el nombre de usuario jsailema@seguridad.local y su respectiva contraseña.

Los nombres de inicio de sesión de usuario tienen la estructura de un correo electrónico. Estos deben seguir un patrón predefinido. En nuestro caso se colocará la inicial del primer nombre del usuario seguido del primer apellido, todo en minúscula. Luego viene el símbolo @ y el nombre del dominio: seguridad.local.
Ejemplo:
Usuario: Empresa Corporativa;
Nombre de inicio de sesión: Coporativa@seguridad.local

Antes de esto debe conocer que la PC-01 debe estar agregada al dominio seguridad.local. Para eso se deben cumplir los siguientes pasos:

a) En la PC-01 se ubica en Panel de control→Sistema y Seguridad→Sistema.
b) Se busca la información del sistema donde dice: Configuración de nombre, dominio y grupo de trabajo del equipo. Aquí se da clic en la opción: Cambiar configuración.
c) Clic en el botón cambiar. Se selecciona la opción Miembro del dominio y se escribe el nombre de dominio: seguridad.local. y clic en aceptar. Como se observa en las Figura 3.90 y 3.91.

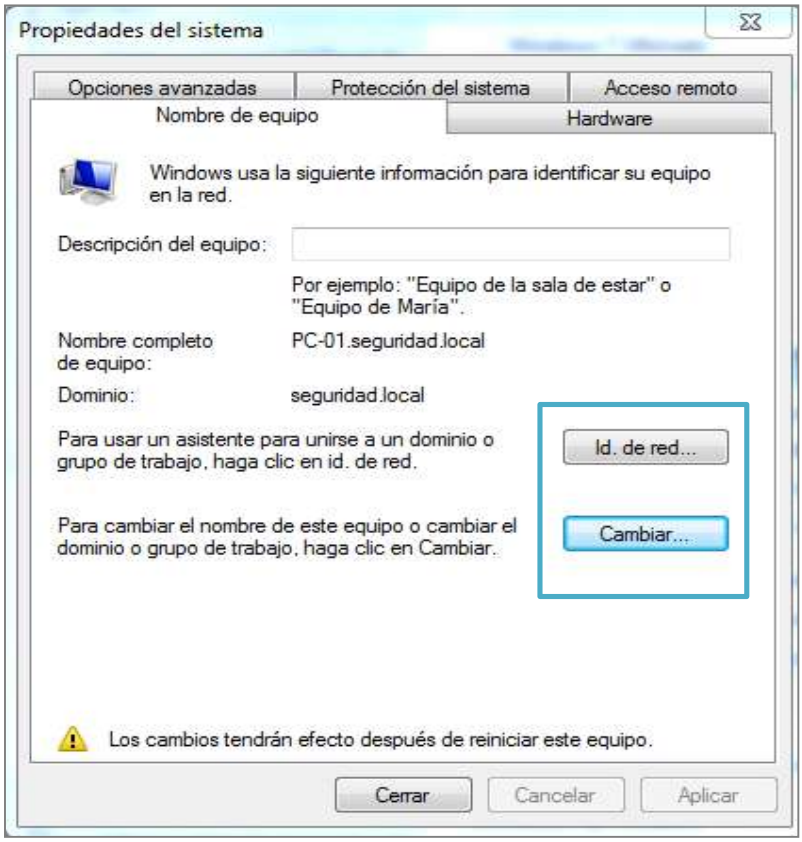


Figura 3. 80: Unión de dominio seguridad.local Parte 1

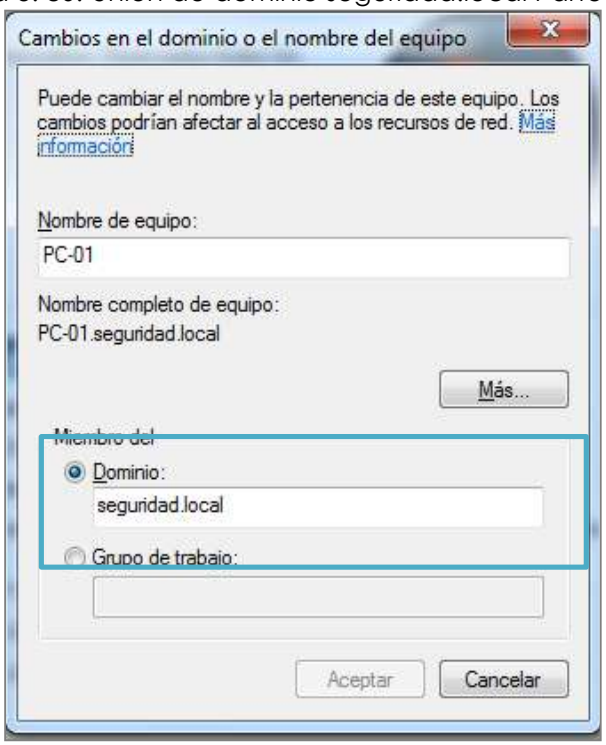


Figura 3. 81: Unión al dominio.local Parte 2

d) Este es el momento de unir este equipo al dominio. Este equipo PC-01 se agregará al DA y para efectuar esta operación en el siguiente paso se abrirá un cuadro donde nos pedirá iniciar sesión con un usuario que pertenezca al dominio seguridad.local, en este caso, este usuario es: jsailema@seguridad.local, se coloca su contraseña respectiva y se hace clic en aceptar. Saldrá un mensaje que confirmará que el equipo se ha unido correctamente al dominio. Como se observa en la Figura 3.82

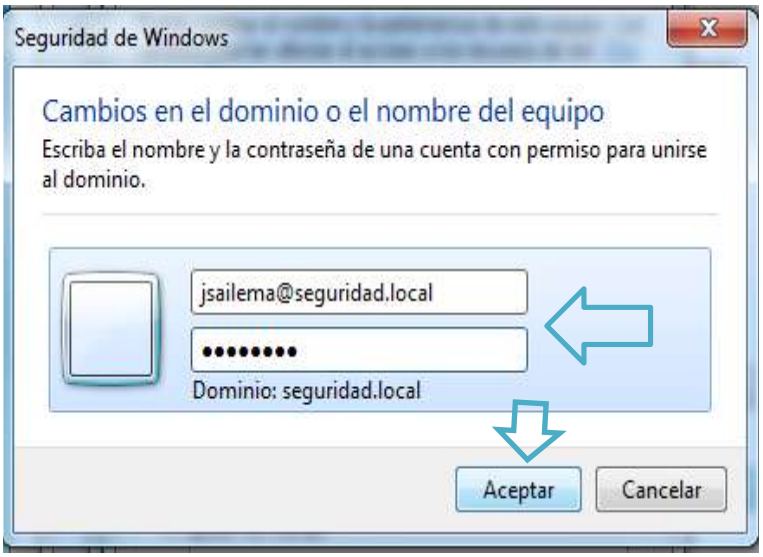


Figura 3. 82: Unión de dominio seguridad.local Parte 3

e) Por último, el equipo se reiniciará para poder efectuar todos los cambios. Una vez reiniciado el equipo, se procede a iniciar sesión, se escoge la opción "otro usuario" y se escribe el nombre de usuario y contraseña y listo. Como se observa en la Figura 3.81.

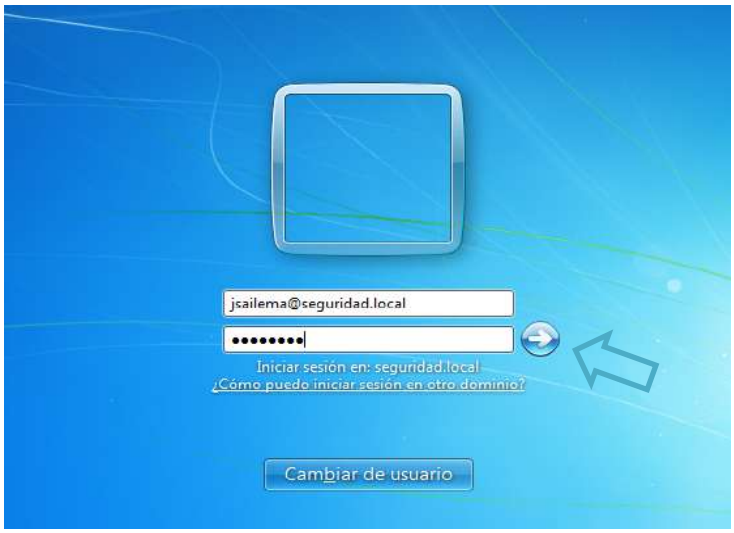


Figura 3. 83: Inicio de sesión en el equipo PC-01

f) Ahora que se ha hecho todos los pasos para unir el pc al dominio, se procede ir al Servidor SrvDC-01 y se dirige a la ruta: Administrador del servidor→Herramientas→Usuarios y Equipos de Active Directory. Una vez aquí se procede ir a la ruta: Usuarios y Equipos de Active directory →seguridad.local → Computers y en la parte derecha de la ventana se debe verificar que el Equipo PC-01 haya sido agregado. Como se observa en la figura 3.84.

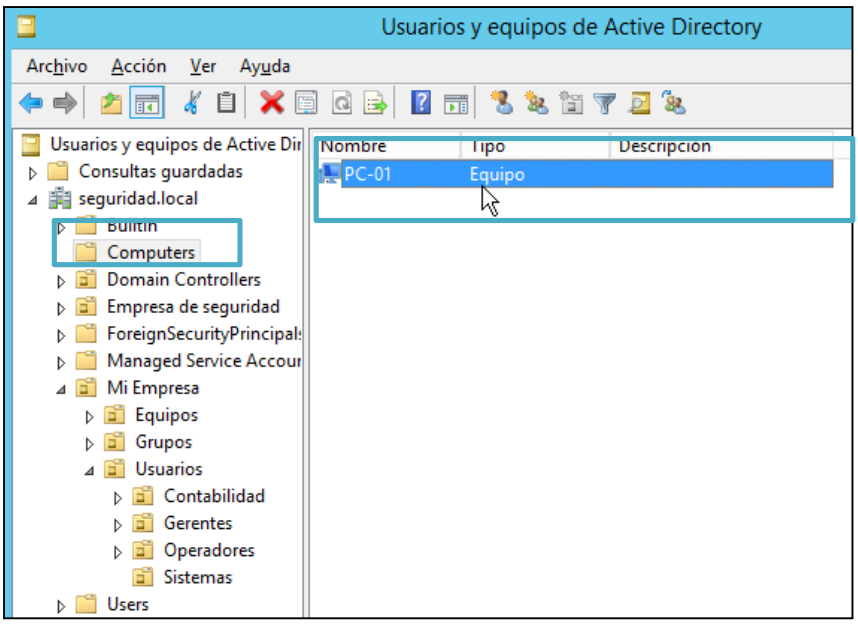


Figura 3. 84: Equipo añadido al dominio

g) Y finalmente, se selecciona la PC-01 y sin soltar el cursor del mouse, se arrastra el pc hasta la carpeta equipos de la unidad organizativa Empresa de Seguridad. Como se observa en la Figura 3.85.

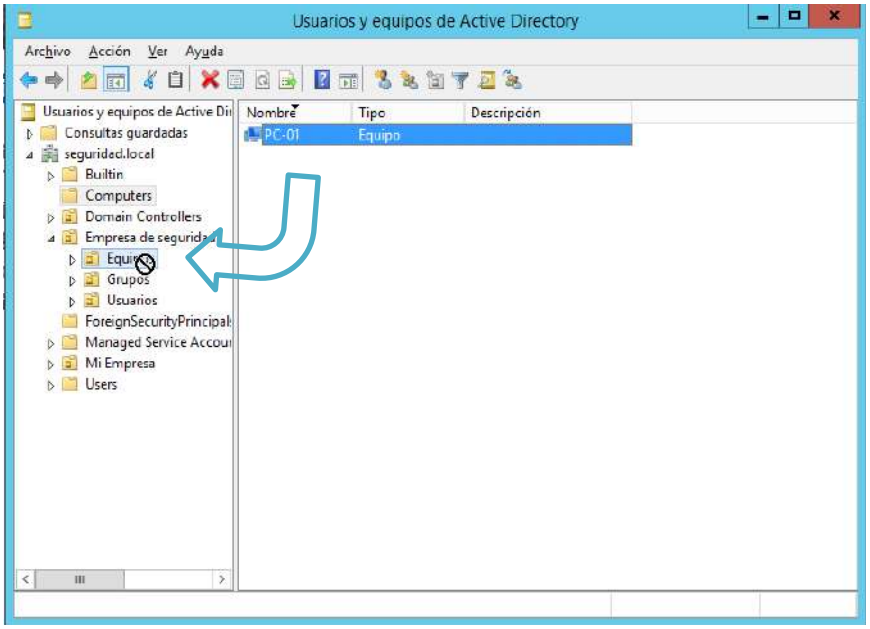


Figura 3. 85: Mover el equipo a carpeta Equipos

h) Aparecerá un mensaje de advertencia, se procede a dar clic en sí. Observe la Figura 3.86.

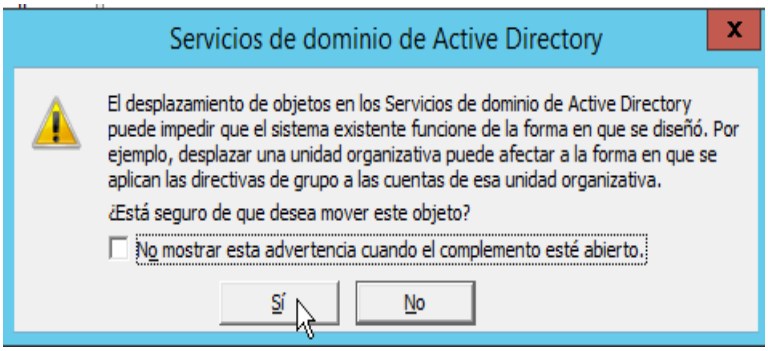


Figura 3. 86: Mensaje de advertencia

Y listo, de esta manera se tiene de una manera organizada los usuarios, equipos y grupos dentro de la organización.

3.8. Herramientas de administración

Una herramienta de administración de servidor remoto (RSAT), permite a los administradores de TI, administrar roles y características en Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 y Windows Server 2008 R2 de forma remota desde un equipo que está ejecutando. (Microsft, 2018)

En las RSAT versiones de herramientas de Windows 10, Windows 8.1 y Windows 8, vuelven a todo habilitado de forma predeterminada. Puede abrir Windows activar o desactivar las características para deshabilitar herramientas que no desea utilizar. En 10 de RSAT para Windows, así como Windows 8.1 y Windows 8, tener acceso a herramientas basadas en GUI en el menú Herramientas en la consola del administrador del servidor.

Es decir, que es un conjunto de herramienta gráfica para la administración remota de servidores que podemos instalar de una máquina, que no sea necesariamente de un servidor. Con este conjunto de herramienta podemos llevar acabo la administración y gestión de una forma amigable.

En este caso esta herramienta viene por defecto en el sistema operativo Windows Server 2012 para entrar hay que ir al buscador de server y poner herramientas de administración como se muestra en la figura.

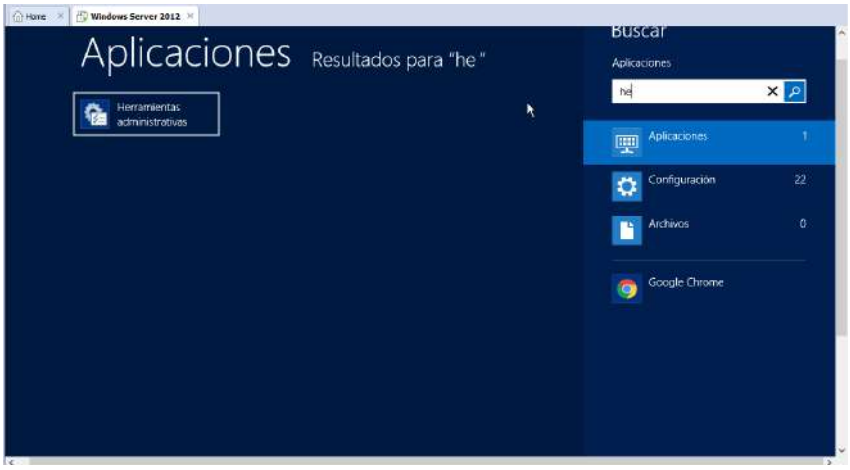


Figura 3. 87: Localizado la herramienta administrativas

Luego de localizar la herramienta le damos clic y nos mostrara la siguiente pantalla.

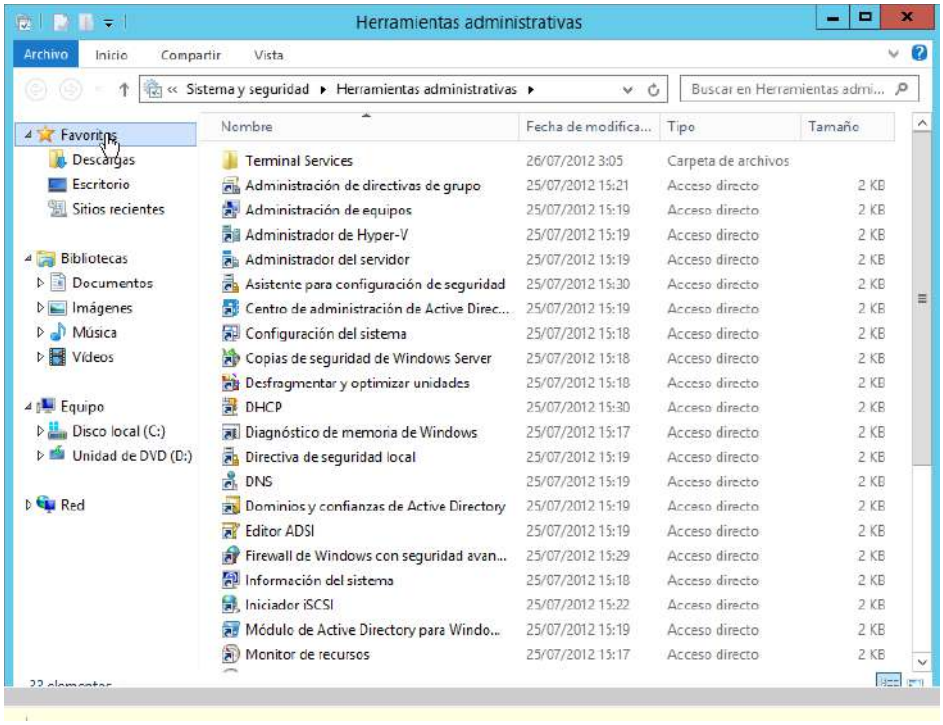


Figura 3. 88: Herramientas Administrativas

Para tener acceso rápido a cualquier servidor, dar clic en cualquiera de esas opciones por ejemplen DHCP y me mostrará la siguiente figura 3.88.

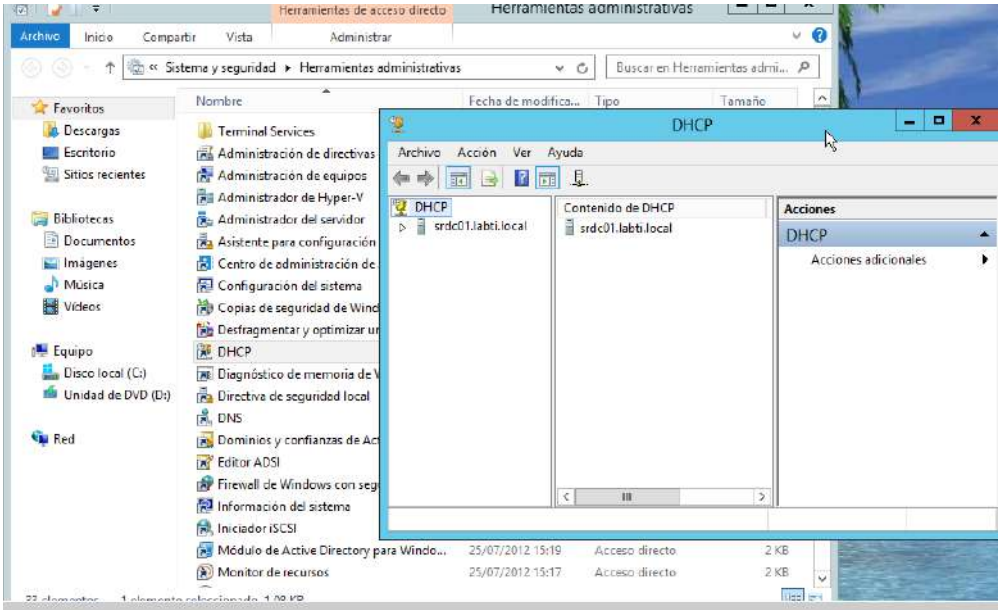


Figura 3. 89: DHCP

Bibliografía

Delprato, G. (13 de Julio de 2013). Clonar un controlador de dominio virtual. Obtenido de Windows Server: https://windowserver.com/2012/07/13/windows-server-2012-clonar-un-controlador-de-dominio-virtual/

González, C. (03 de Septiembre de 2014). Administración de sistemas corporativos basados en windows 2012 server active directory. (A. d. Directory, Productor) Recuperado el 25 de Junio de 2018, de https://www.support.net/cefespinoza/administracin-de-sistemas-corporativos-basados-en-windows-2012-server-active-directory

Gutiérrez, R. (18 de Julio de 2017). Crear usuario en windows server 2012. Obtenido de http://www.ramongutierrez.net/windows/windows-server-2012/crear-usuario-en-windows-server-2012/

Microsoft. (18 de Abril de 2018). Herramientas de administración de servidor remoto (RSAT) para sistemas operativos Windows.

Obtenido de https://support.microsoft.com/es-ec/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems

Moreno, C. (Febrero de 2012). Instalación Active Directory. Obtenido de https://cmunozblog.files.com/2016/08/instalacion_active_directory2.pdf

Solanes, J. M. (5 de septiembre de 2016). Introducción a Active Directory. Obtenido de JMSolanes: https://www.jmsolanes.net/es/introduccion-active-directory/

Unidad

IV

Unidad IV

Servidor DHCP

4. Introducción

DHCP proporciona parámetros de configuración para los servidores de Internet en un modelo de cliente-servidor. Los hosts del servidor DHCP asignan direcciones de red y entregan parámetros de configuración a otros hosts (clientes). (Azure, 2018)

DHCP consiste en dos componentes: un protocolo para entregar parámetros de configuración específicos del host desde un servidor a un host y un mecanismo para la asignación red direccionamientos a los hosts.

DHCP admite tres mecanismos para la asignación de direcciones IP:

Asignación automática: en la que se asigna una dirección IP permanente al cliente.

Asignación dinámica: en la que la dirección se asigna en un intervalo de tiempo limitado (una "concesión").

Asignación manual: en la que el administrador de red asigna la dirección manualmente.

Entrega de parámetros de configuración, el cliente envía un mensaje para solicitar parámetros de configuración y el servidor responde con un mensaje que transmite los parámetros deseados al cliente.

El formato de los mensajes DHCP, se basa en el formato de los mensajes BOOTP debido a los siguientes motivos:

1. Desde el punto de vista del cliente, DHCP es una extensión del mecanismo BOOTP . Este comportamiento permite a los clientes existentes
   de BOOTP interoperar con servidores DHCP sin requerir ningún cambio en el software de inicialización de los clientes.
2. DHCP admite el comportamiento del agente de retransmisión BOOTP .

DHCP no requiere un servidor en cada subred. Para permitir escala y economía, DHCP puede funcionar a través de enrutadores o mediante la intervención de agentes de retransmisión BOOTP . Un agente real escucha los mensajes DHCP y los reenvía a (y a otros segmentos de

red). Esto elimina la necesidad de tener un servidor DHCP en cada red física.

4.1. DHCP

4.1.1. Definición DHCP

DHCP (Protocolo de configuración de host dinámico) es un protocolo de administración de red que se usa para asignar dinámicamente una dirección de Protocolo de Internet (IP) a cualquier dispositivo o nodo en una red para que puedan comunicarse mediante IP.

DHCP automatiza y administra de forma centralizada estas configuraciones en lugar de requerir que los administradores de red asignen manualmente las direcciones IP a todos los dispositivos de red como se muestra en la figura 4.1. DHCP se puede implementar en pequeñas redes locales y en grandes redes empresariales. (Rouse, 2017)

El protocolo de configuración dinámica de host (DHCP) es un protocolo cliente / servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.

Las RFC 2131 y 2132 definen DHCP como un estándar de Fuerza de trabajo de ingeniería de Internet (IETF) basado en el protocolo Bootstrap (BOOTP), un protocolo con el que DHCP comparte muchos detalles de implementación. DHCP permite a los hosts obtener la información de configuración de TCP / IP necesaria de un servidor DHCP (Windows, 2018)

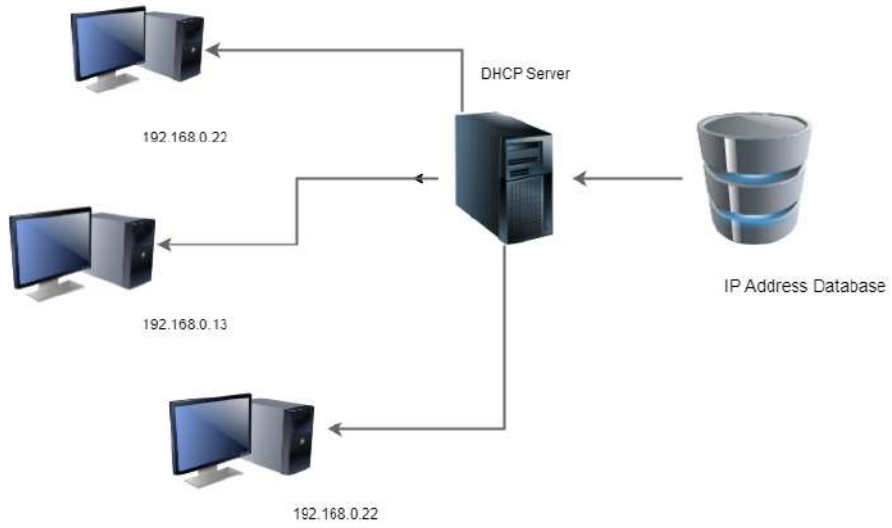


Figura 4. 1: DHCP

4.1.2. ¿Qué es un DHCP?

El servicio de DHCP es un servicio incluido en nuestro sistema Windows Server 2012 y cuya función principal es la de proveer direcciones IP a los dispositivos conectados en nuestro dominio de manera automática.

El funcionamiento del servicio DHCP consiste en que el servidor que tiene este servicio recibe la petición del cliente (servidor) de una dirección IP y éste se la suministra, una de las grandes ventajas es que el servidor DHCP administra de forma centralizada estas direcciones.

4.1.3. ¿Cómo funciona?

DHCP se ejecuta en la capa de aplicación del protocolo de control de transmisión / IP (TCP / IP) para asignar dinámicamente direcciones IP a clientes DHCP y asignar información de configuración de TCP/ IP a clientes DHCP. Esto incluye la información de la máscara de subred , las direcciones IP de la puerta de enlace predeterminada y las direcciones del sistema de nombres de dominio (DNS). (Rouse, 2017), como se muestra la figura 4.2.

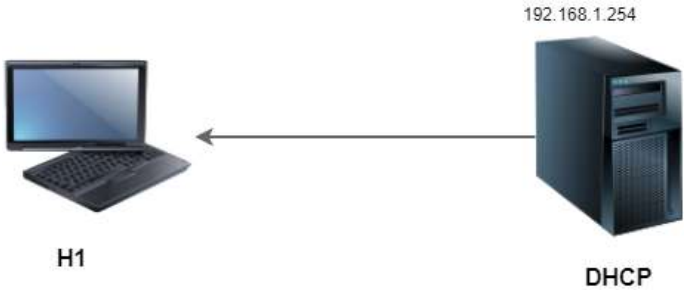


Figura 4. 2: Funcionamiento DHCP

En el lado izquierdo tenemos una computadora sin dirección IP. En el lado derecho hay un servidor DHCP configurado con la dirección IP estática 192.168.1.254. Este servidor DHCP proporcionará una dirección IP a nuestra computadora, así es como funciona ver figura 4.3:

Figura 4. 3: Enviando mensaje DHCP de descubrimiento

La computadora enviará un mensaje de descubrimiento de DHCP, Esta es una transmisión porque no tiene una dirección IP y no sabe si hay un servidor DHCP en la red. Por supuesto, en nuestro caso tenemos un servidor DHCP por lo que responderá a esta transmisión de la siguiente manera ver figura 4.4:

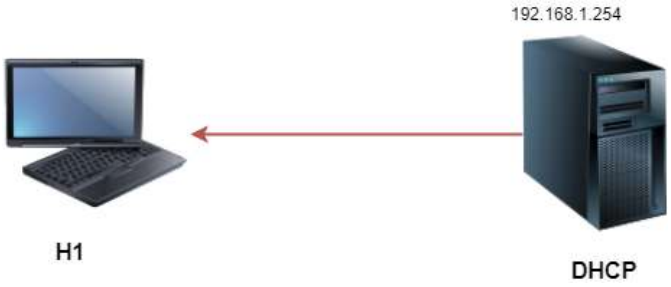


Figura 4. 4: Recibiendo el mensaje DHCP de oferta

El servidor DHCP responderá con un mensaje de oferta DHCP que contiene una dirección IP para la computadora (tenemos que configurar el servidor DHCP para definir qué direcciones IP queremos dar). Si lo deseamos, también podemos asignar una puerta de enlace predeterminada y servidor (es) DNS a la computadora. La computadora responderá a esta información ver figura 4.5:

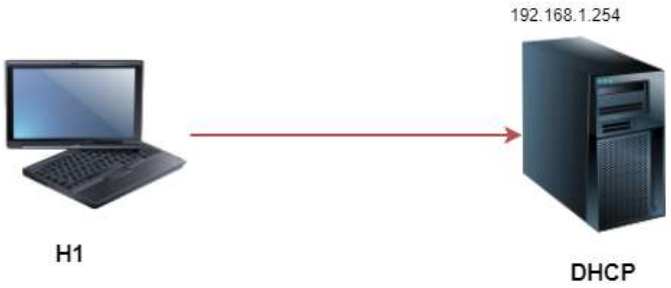


Figura 4. 5: Solicitud DHCP

La computadora enviará una Solicitud de DHCP en respuesta al mensaje de oferta de DHCP, preguntando amablemente si está bien utilizar la información que ha recibido. Nuestro servidor DHCP responderá a esto de la siguiente manera ver figura 4.6:

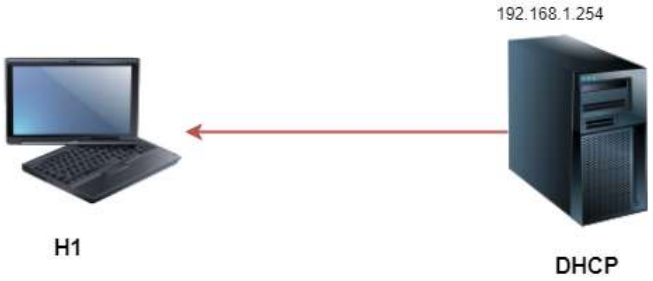


Figura 4. 6: Respuesta DHCP con un mensaje DHCP ACK

El servidor DHCP responderá con un mensaje DHCP ACK para decirle a la computadora que está bien usar esta información. (Molenar, 2016)

4.1.4. Configuración del Servicio DHCP

Esta propuesta pretende explicar brevemente la definición, aplicación, uso, e instrucciones del paso a paso de la configuración de un servicio DHCP para ambos servidores de la zona LAN.

El protocolo de configuración dinámica de host (DHCP) es un protocolo cliente / servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.

4.1.5. ¿Porque usar DHCP?

DHCP permite tener una única dirección IP de unidifusión para acceder a la red y sus recursos, en los servidores de la zona LAN se aplicó DHCP para automatizar el proceso de asignaciones de IP en cada PC.

El administrador de la red establece los servidores DHCP que mantienen la información de configuración de TCP / IP y proporcionan la configuración de la dirección a los clientes habilitados para DHCP en la forma de una oferta de arrendamiento.

Con un servidor DHCP que ejecute Windows Server 2012 o Windows Server 2012 R2, los administradores pueden definir una política de asignación de direcciones a nivel de servidor o nivel de alcance. Una política contiene un conjunto de condiciones para evaluar al procesar

¿Sabías Qué?

solicitudes de clientes.

4.2. Instalación DHCP

Para instalar DHCP en los servidores SrvDC-01 y SrvDC-02 en Windows Server 2012, seguiremos los siguientes pasos antes de comenzar debe recordar que el servidor DHCP es el que se encarga de asignar

> DHCP minimiza los errores de configuración causados por la configuración manual de la dirección IP, como errores tipográficos o conflictos de direcciones causados por la asignación de una dirección IP a más de una computadora al mismo tiempo.

direcciones IP a todas nuestras maquinas conectadas a una red.

1. Dirigirnos en administrador del servidor darle clic agregar roles y características presionamos siguiente, nuevamente siguiente vamos a fijarnos que este seleccionado el servidor en este caso es SrvDC-01 en la pantalla siguiente y seleccionamos el rol que vamos a usar en este caso servidor DHCP como se muestra la figura 4.7.

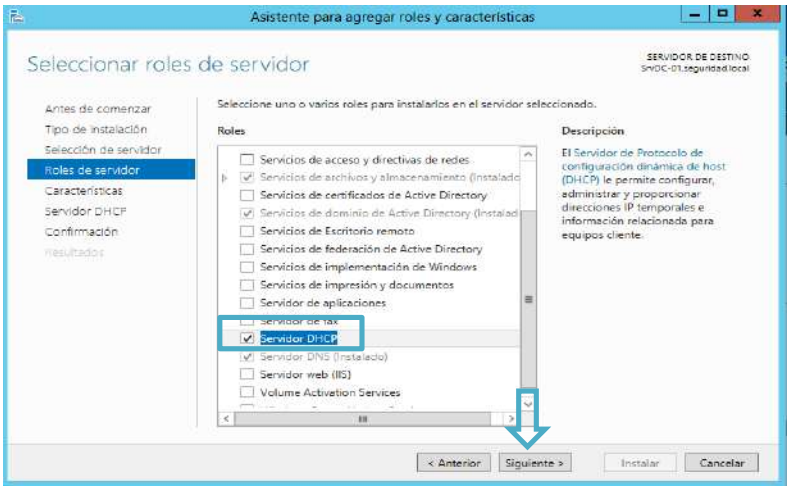


Figura 4. 7: Seleccionado Servidor DHCP para la instalación.

2. Marcamos el servidor DHCP le damos en siguiente nuevamente siguiente y al final dirá que confirmemos las instalaciones ver figura 4.8.

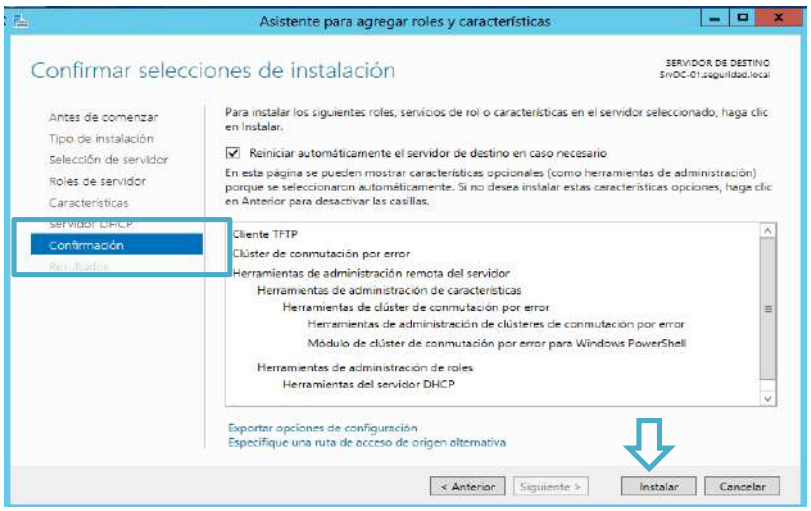


Figura 4. 8: Confirmación para instalar DHCP

3. Esperamos para que se instale el servidor DHCP, dirigirse en la opción completar configuración DHCP, ver la figura 4.9.

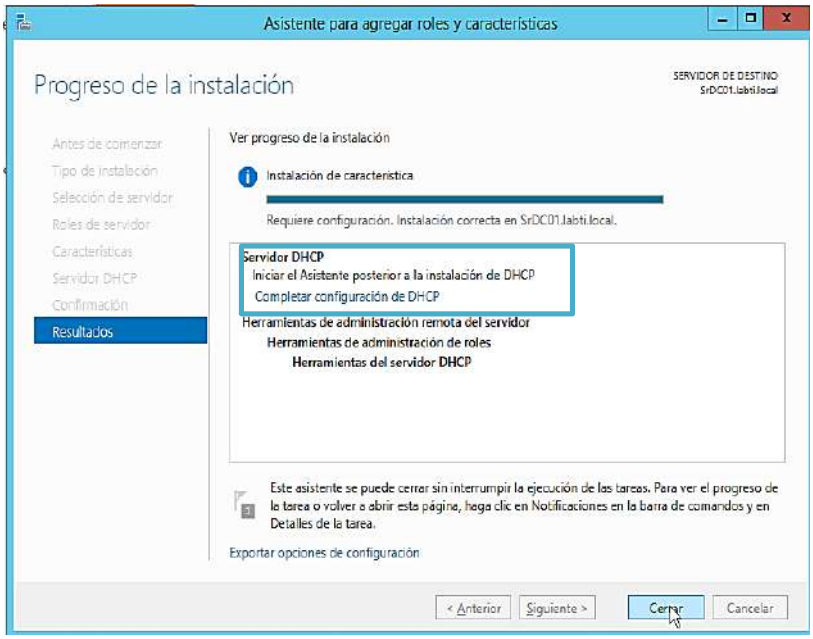


Figura 4. 9: Instalando DHCP

4. Finalizando la instalación aparece una notificación que debe confirmar la instalación en la cual describe lo que se va instalar, damos clic en siguiente como se muestra la figura 4.10.

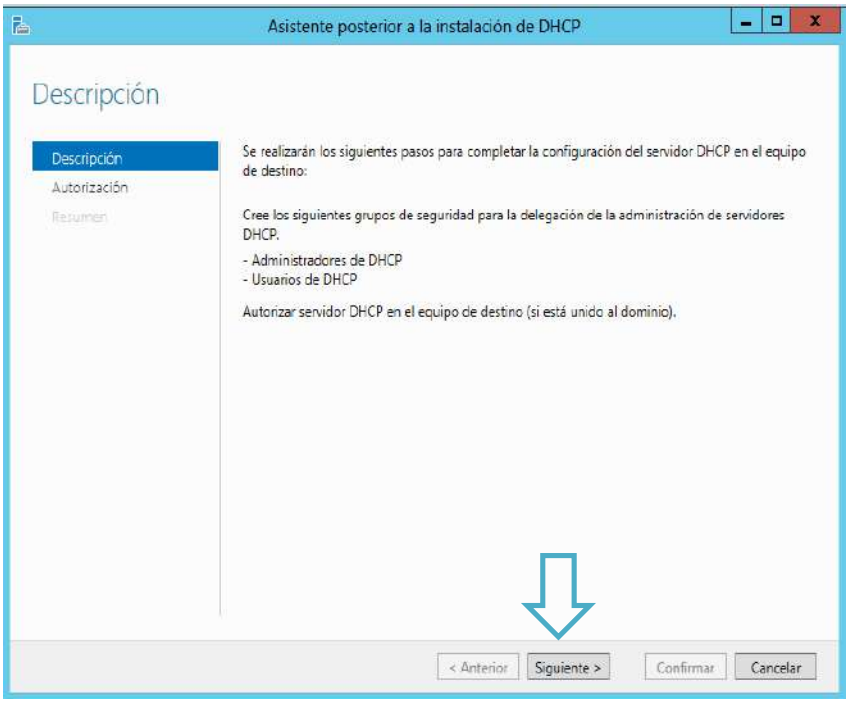


Figura 4. 10: Confirmación la instalación DHCP

5. Aparecerá una autorización en la cual debemos confirmar, como podemos observar en la figura 4.11 al momento de elegir la opción usar las credenciales del siguiente usuario, automáticamente muestra el nombre de usuario, en este caso sería SEGURIDAD\Administrador.

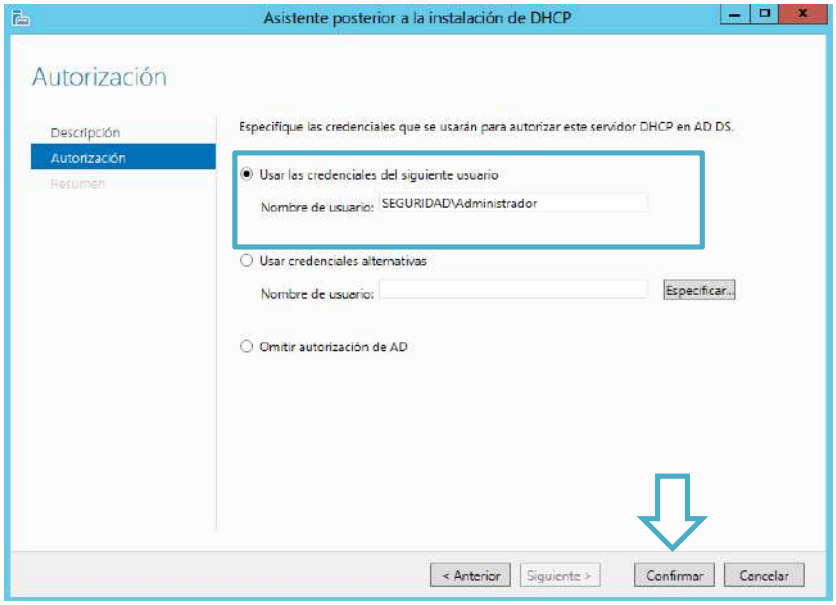


Figura 4. 11: Solicitando una autorización para la instalación DHCP

6. Al confirmar una breve descripción de los permisos que autorizados como se muestra la figura 4.12.

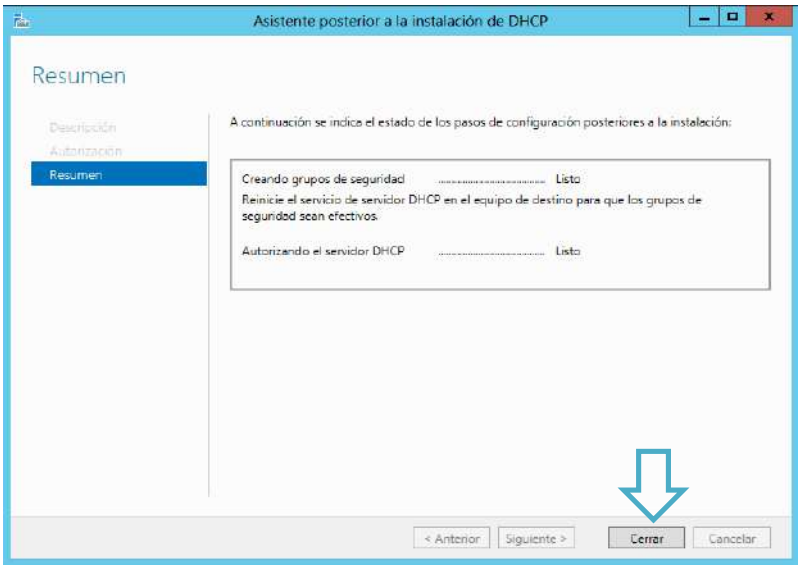


Figura 4. 12: Resumen de los permisos autorizados para la instalación DHCP

7. Finalmente, como podemos observar en la figura 4.13, ya está instalado el servidor DHCP (SrvDC-01) en Windows Server 2012.

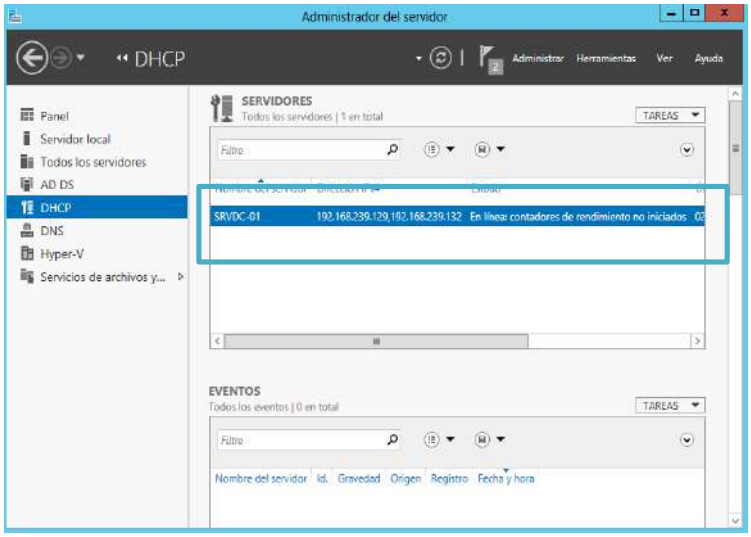


Figura 4. 13: DHCP instalado

Nota:

Para instalar el DHCP en el servidor SrvDC-02 seguimos los mismos pasos que usamos para instalar el servidor SrDC-01.

4.3. Configurando y Alta del servicio DHCP

Para configurar el DHCP en Windows Server 2012 seguimos los siguientes pasos a continuación (Delprato, 2013).

1. Nos dirigimos al servidor DHCP seleccionamos el servidor clic derecho y presionamos donde dice administrador de DHCP ver figura 4.14.

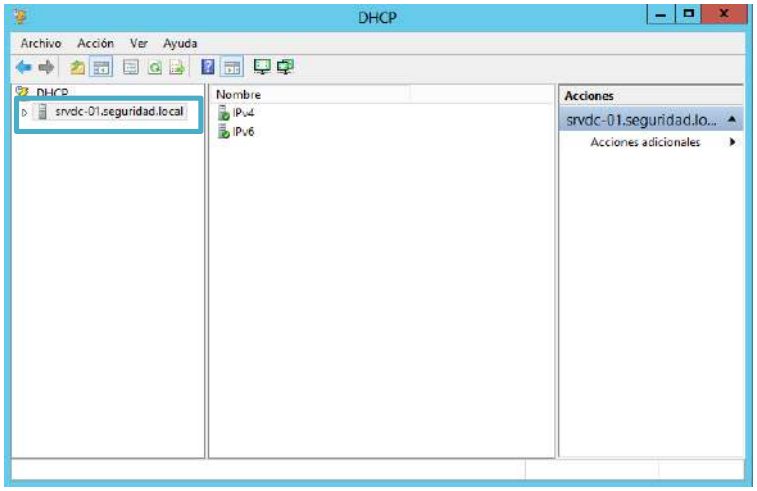


Figura 4. 14: Administrador DHCP

2. Le damos clic en el servidor SrvDC-01 muestra un listado IPV4 y IPV6, dar clic en el IPV4 clic derecho crear ámbito nuevo para a seguir al asistente como se muestra la figura 4.15.

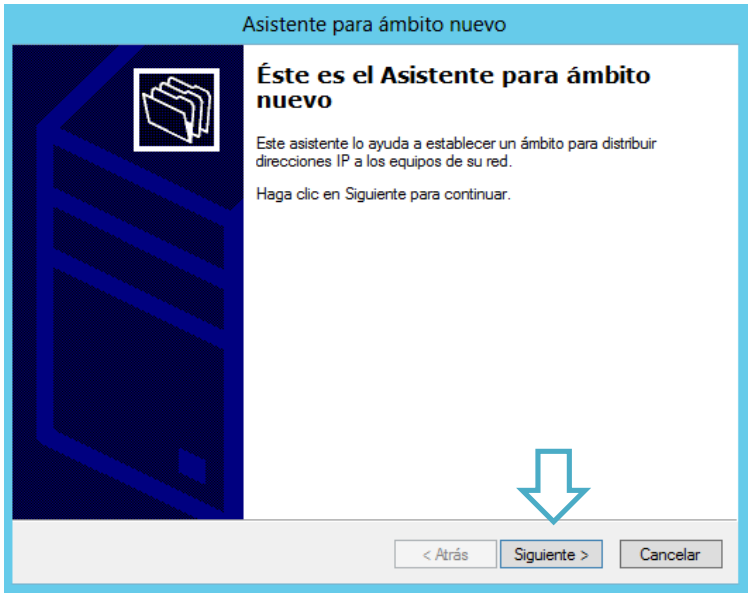


Figura 4. 15: Asistente para ámbito nuevo

3. Presionamos siguiente pedirá que ingrese un nombre del ámbito en este caso le asignare Red siguiente después pedirá que digite los intervalos de direcciones IP como se muestra la figura 4.16.

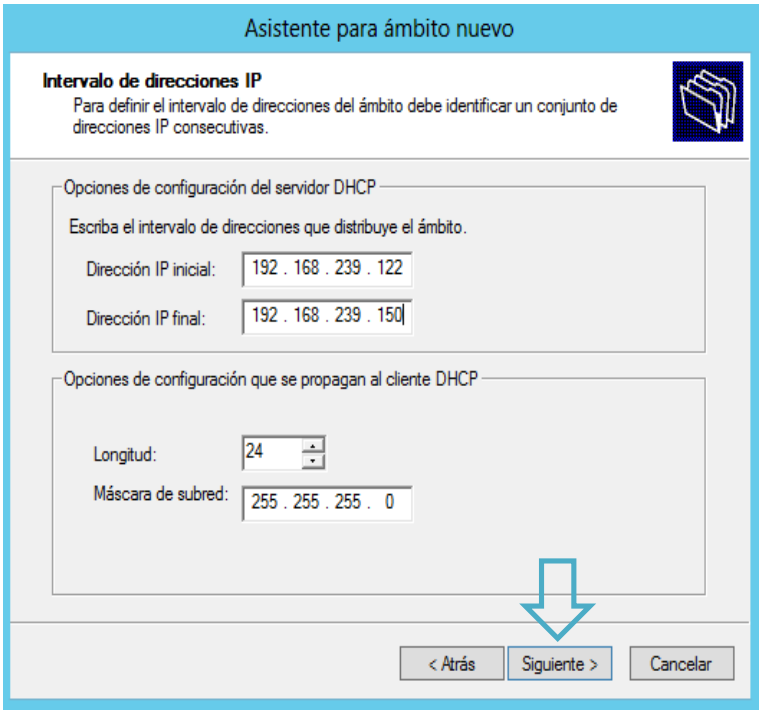


Figura 4. 16: Intervalo de direcciones IP

4. Agregar exclusiones y retraso en caso de que no queremos para este ejemplo los dejamos vacío le damos en siguiente ver figura 4.17.

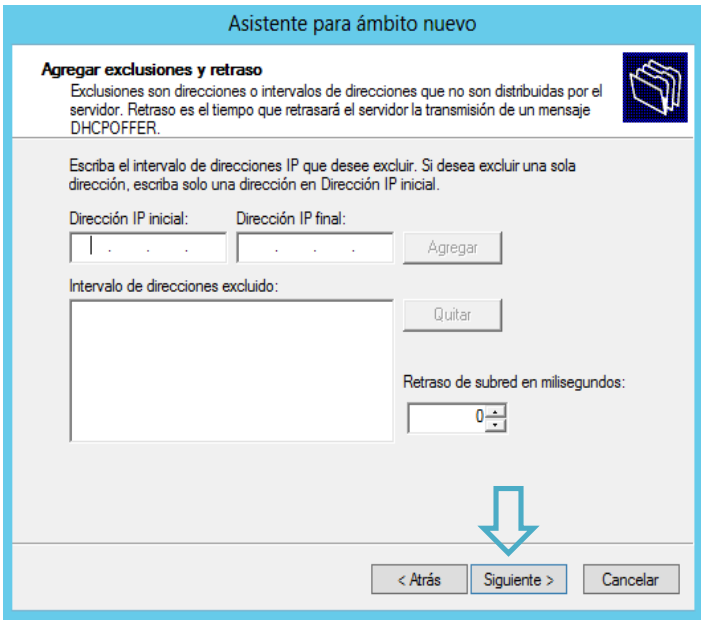


Figura 4. 17: Agregar exclusiones y retraso

5. Configurar la duración de la concesión, es decir el tiempo que va a durar esta IP a ciertos equipos por defecto nos pones en 8 días

como se muestra la figura 4.18, pero podemos asignarle menor tiempo para que nos consuma las direcciones IP y pueda ser liberadas más rápida para que otros equipos las utilice en este caso es para una red física lo dejaremos por defecto.

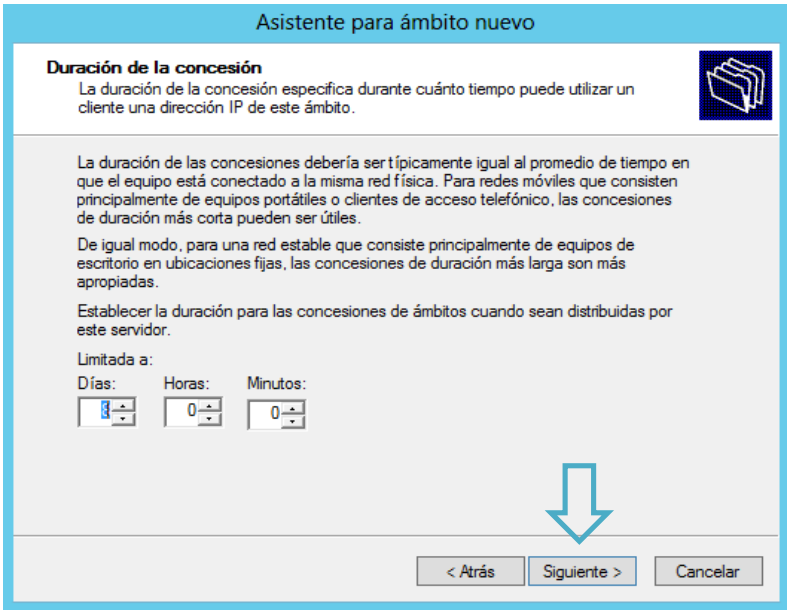


Figura 4. 18: Duración de la concesión

6. Marcamos donde dice configuraciones ahora le damos siguiente ver figura 4.19.

Figura 4. 19: Configuración DHCP

7. Configuramos los puertos enlaces predeterminadas les dar clic en siguiente como se observa la figura 4.20.

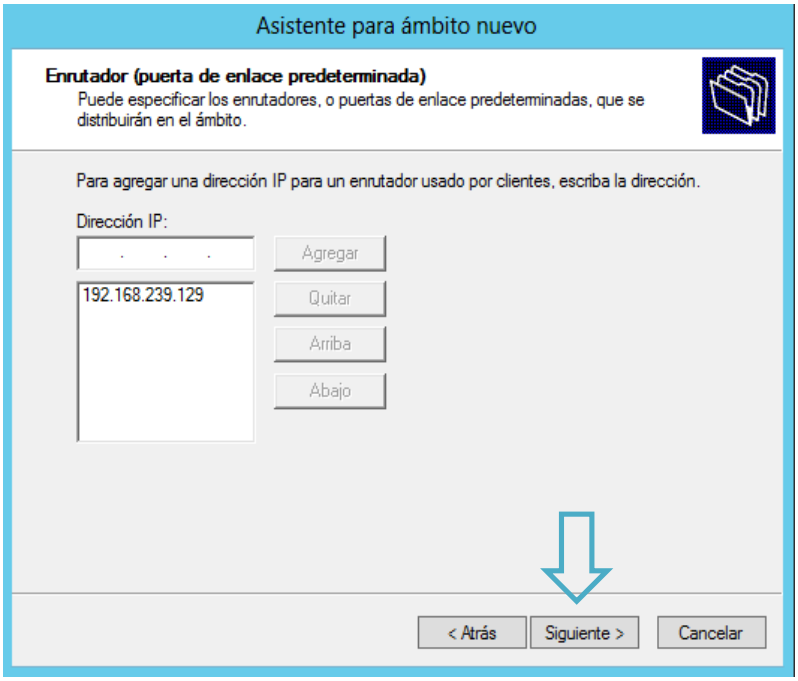


Figura 4. 20: Enrutador DHCP

8. Muestra las configuraciones y el nombre del dominio dar clic en siguiente ver figura 4.21.

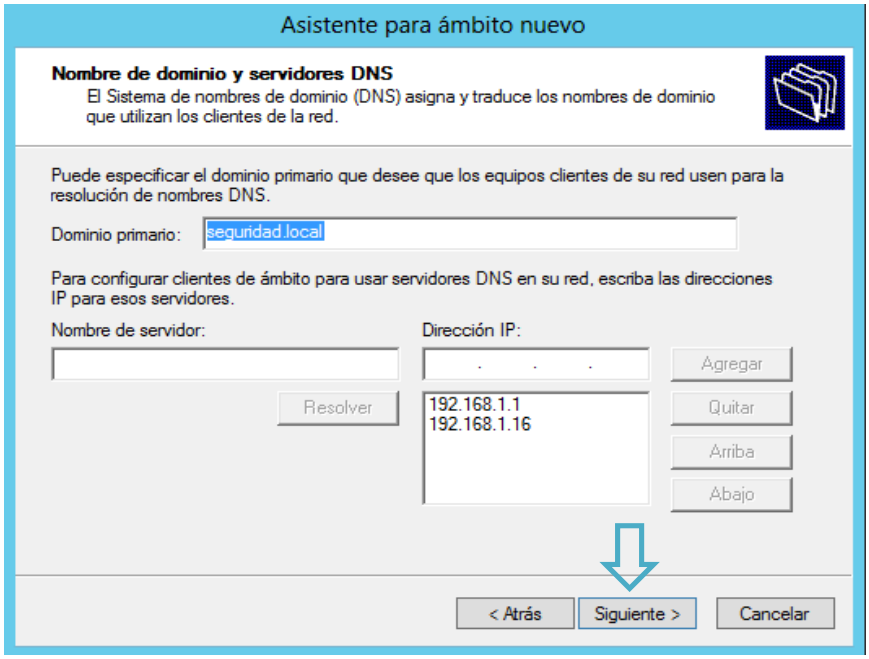


Figura 4. 21: Nombre de domino y servidores DNS

9. Para configurar servidores wifi pulsamos siguiente como se muestra la figura 4.22.

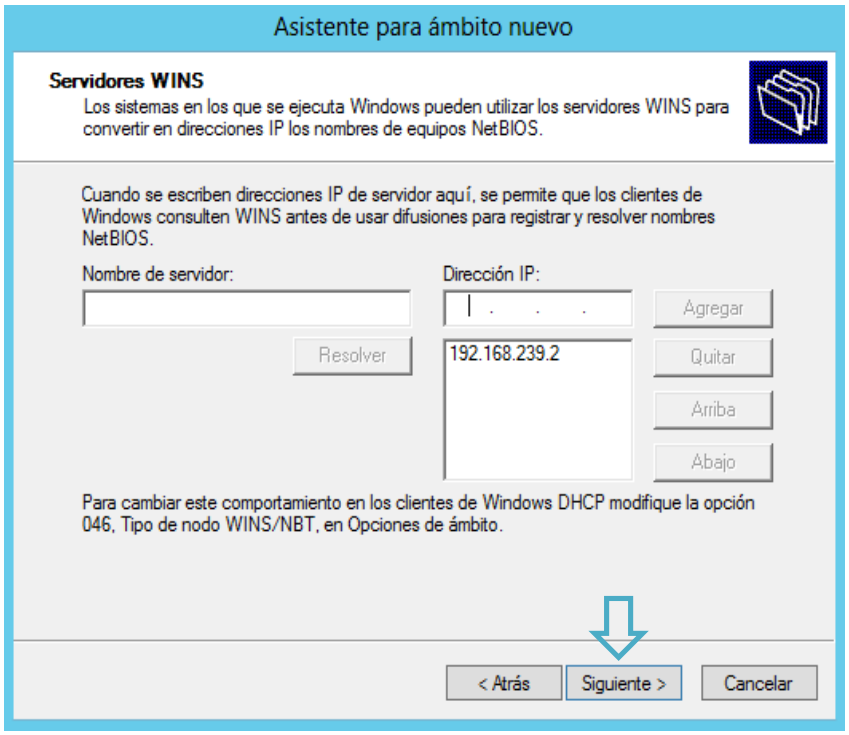


Figura 4. 22: Servidores WINS

10. Para finalizar activamos el ámbito le damos siguiente, ver figura 4.23.

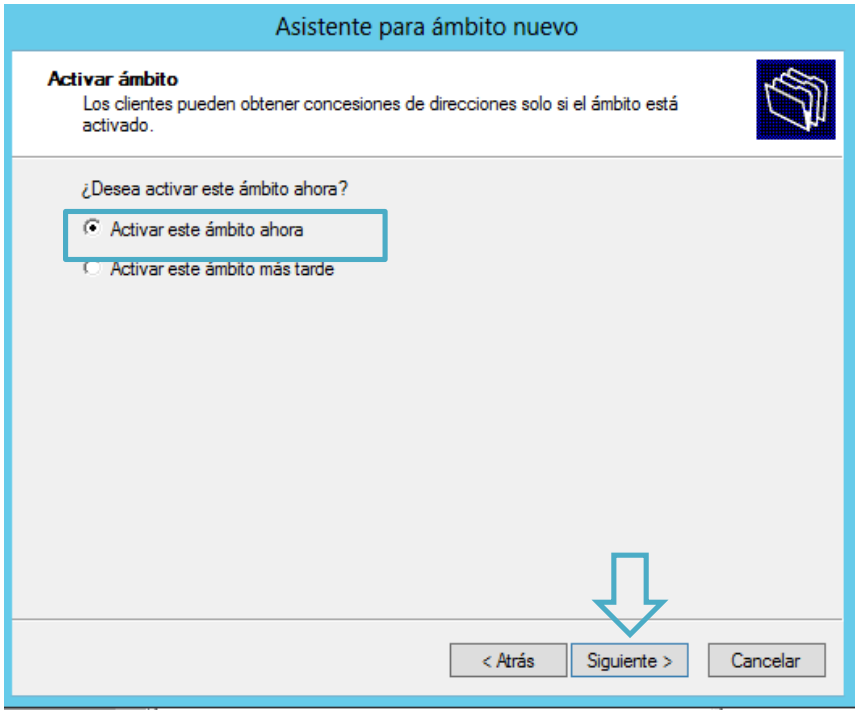


Figura 4. 23: Activar el ámbito

11. Finalizamos la para creación de ámbitos, ver figura 4.24.

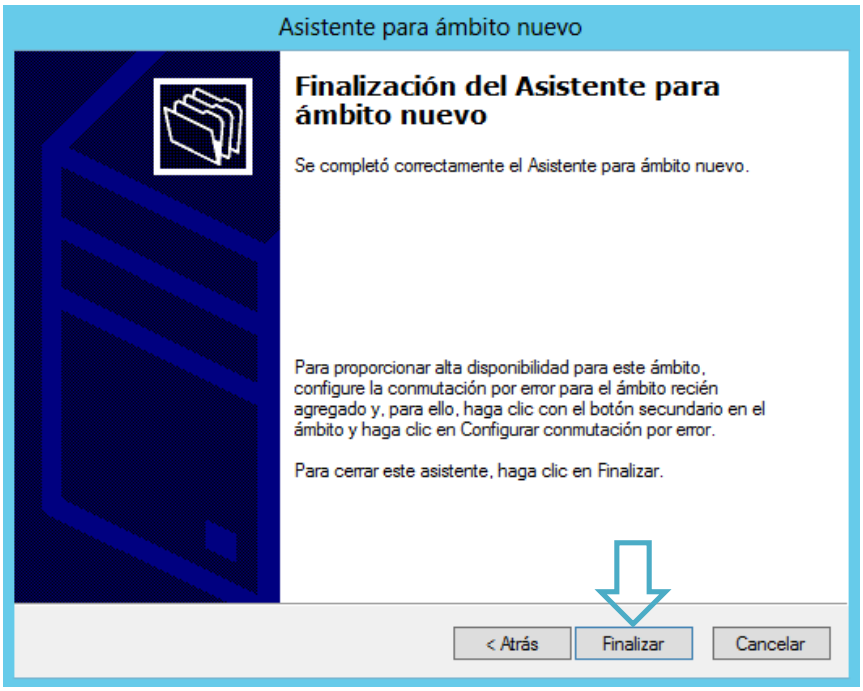


Figura 4. 24: Finalización del asistente para ámbito nuevo

12. Como observamos ya tenemos el ámbito creado que le pusimos Red, ver figura 4.25.

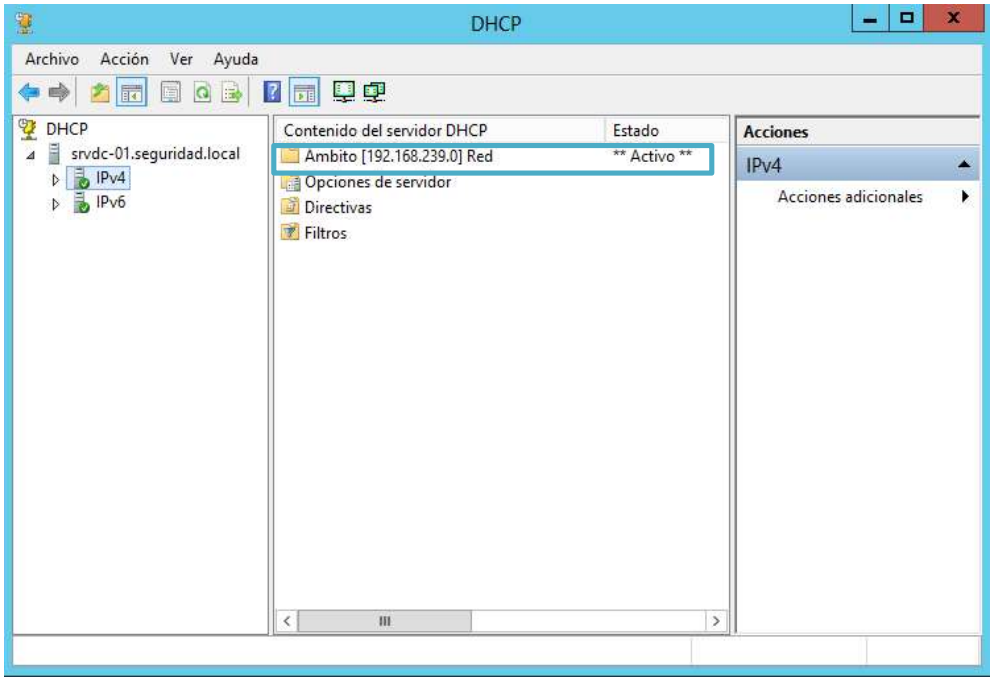


Figura 4. 25: Creación del ámbito DHCP

13. Como podemos observar hemos creado de manera correcta porque aparece las direcciones que hemos colocado en el DHCP, ver figura 4.26.

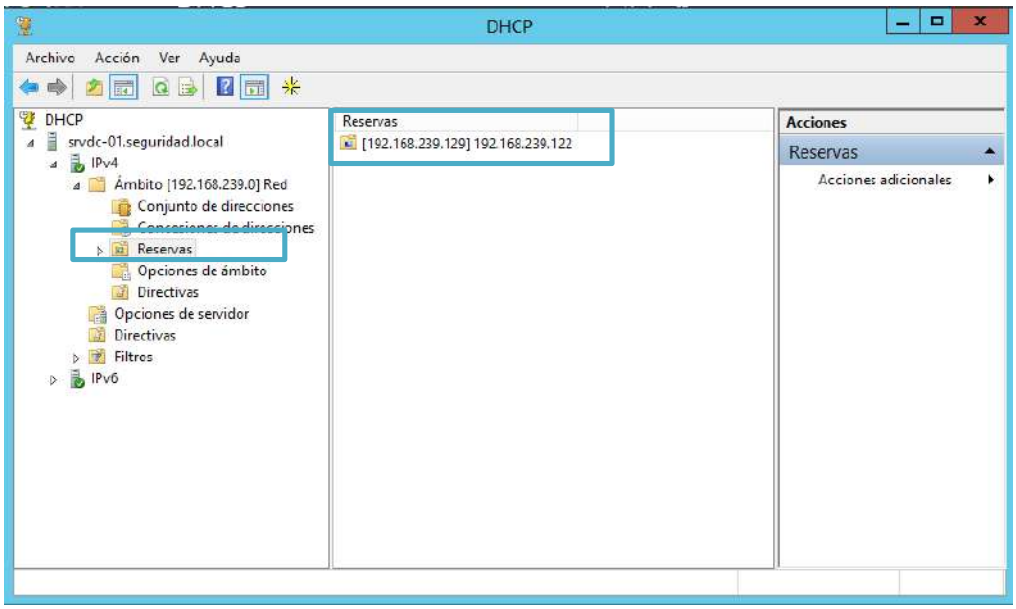


Figura 4. 26: Direcciones DHCP

14. Para comprobar nos vamos al cmd digitamos ipconfig /all, como se muestra la figura 4.27.

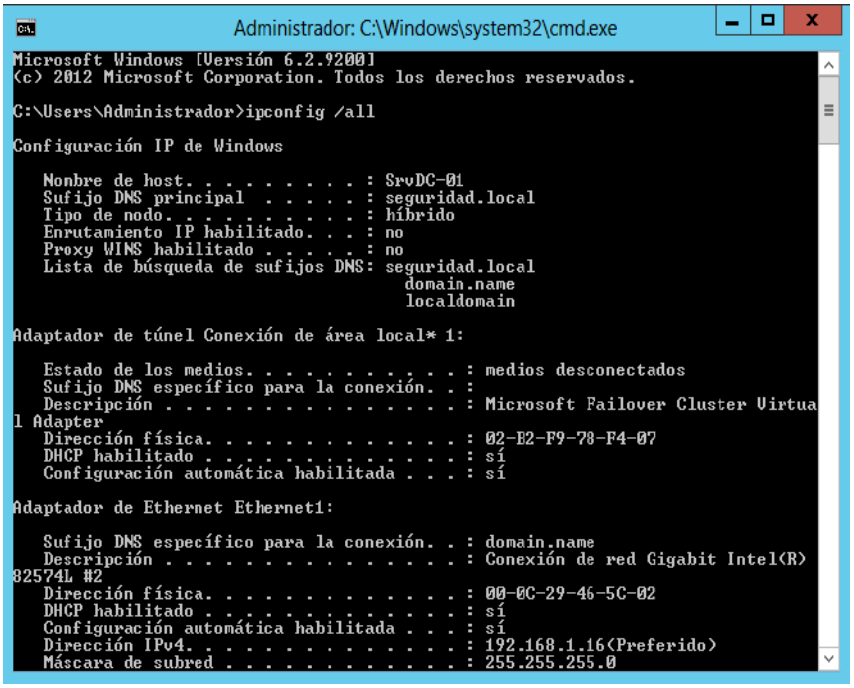


Figura 4. 27: Comprobando las direcciones DHCP para red LAN y WAN

4.4. IPAM

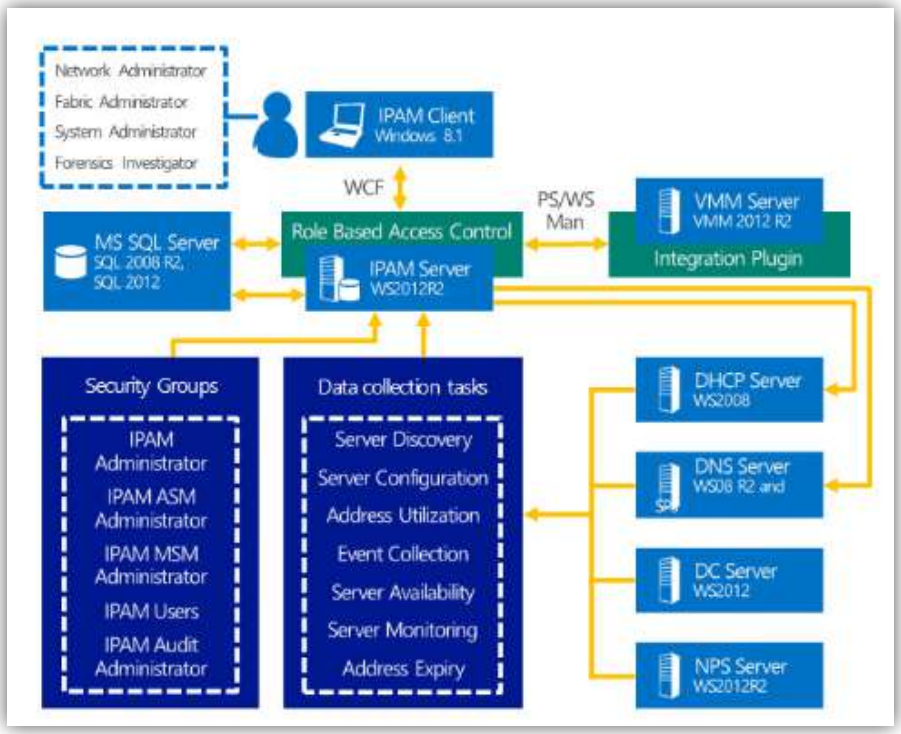
La gestión de direcciones IP es un componente crítico de la operativa de las redes; más ahora, cuando empiezan a generalizarse tecnologías como RFID, VoIP, ENUM o IPv6. Por ello, no basta con una solución interna basada en islas DNS/DHCP. Hoy es preciso contar con un modo eficiente de configurar, automatizar, integrar y administrar los servicios IP, como el que proporcionan los sistemas de gestión de direcciones IP (IPAM).

La gran disponibilidad de herramientas básicas para todo tipo de plataformas lleva a muchas empresas a desplegar servidores DNS y DHCP con poca o ninguna gestión central, y, con frecuencia, sin un esquema de direcciones y de nombres a escala corporativa. Existen paquetes de software de servidor DNS –principalmente BIND (Berkeley Internet Naming Domain), desarrollado en los últimos años 80, y Active Directory (AD) de Microsoft– que, pese a su gran eficiencia, sólo soportan los aspectos más básicos de la gestión de direcciones IP. Es decir, con estas herramientas, DNS y DHCP sólo resultan efectivos para pequeños dominios únicos. (networkworld, 2006)

Es decir IPAM (IP Address Management) es la administración de DNS y DHCP, que son los servicios de red que asignan y resuelven direcciones IP a máquinas en una red TCP / IP. En pocas palabras, IPAM es un medio para planificar, rastrear y administrar el espacio de direcciones de Protocolo de Internet utilizado en una red. Más comúnmente, herramientas como DNS y DHCP se utilizan en conjunto para realizar esta tarea, aunque el IPAM real pegará estos servicios para que cada uno tenga conocimiento de los cambios en el otro (por ejemplo, DNS conociendo la dirección IP tomada por un cliente a través de DHCP y actualizándose en consecuencia). (Peralta, 2012)

4.4.1. ¿Qué es significa exactamente el IPAM?

IPAM cubre todo el entorno DHCP y DNS de Microsoft y supervisa, gestiona y audita la implementación. Antes de Windows Server 2012 esto solo era posible con hojas de cálculo, hojas de papel o costosas aplicaciones de terceros. Con el lanzamiento de Windows Server 2012, esto se volvió mucho más fácil, pero faltaban áreas. Una parte importante de esto fueron las redes virtuales creadas y administradas



dentro de SCVMM.

Figura 4. 28: IPAM

System Center Virtual Machine Manager 2012 permite la virtualización de red totalmente aislada mediante un protocolo denominado NVGRE: encapsulación de enrutamiento genérico de virtualización de red. Cada VM tiene una dirección de proveedor y una dirección de cliente, lo que permite soluciones multitenant con la misma dirección IP de cliente en una red. (Microsoft, 2014)

Es fácil ver, por qué es una buena idea estar atentos a estos rangos de direcciones IP, subredes y direcciones IP individuales. Una vez que se haya instalado IPAM, el complemento de integración utilizará automáticamente la gestión de servicios web (WS Man) para actualizar el servidor IPAM con todos los datos de red virtual de SCVMM.

4.4.2. Especificaciones de IPAM

El alcance de los servidores IPAM está limitado únicamente a un único bosque Active Directory. Los servidores que se tienen en cuenta (NPS, DNS y DHCP) deben ejecutar Windows Server 2008 (o superior) y pertenecer al dominio. Algunos elementos de red (WINS - Windows Internet Naming Service, proxy…) no se tienen en cuenta en el servidor IPAM. Desde Windows Server 2012 R2 es posible utilizar una base de datos SQL (Bonnet, 2012).

Un servidor IPAM puede tener en cuenta 150 servidores DHCP y 500 servidores DNS (6.000 ámbitos y 150 zonas DNS).

Con la instalación de IPAM, se instalan también las siguientes funcionalidades:

- ✓ Herramientas de administración del servidor remoto: Instalación de las herramientas DHCP, DNS y del cliente IPAM que permiten realizar la administración remota de los servidores DHCP, DNS e IPAM.
- ✓ Base de datos interna Windows: Base de datos interna que puede instalarse mediante los roles y características internas.
- ✓ Servicio de activación de procesos Windows: Elimina la dependencia con el protocolo http generalizando el modelo del proceso IIS.
- ✓ Administración de las directivas de grupo: Instala la consola MMC que permite administrar las directivas de grupo.

- ✓ .NET Framework: Instalación de la funcionalidad .NET Framework 4.5.

Bibliografía

Azure, M. (19 de abril de 2018). Soporte técnico de Microsoft. Obtenido de https://support.microsoft.com/es-ec/help/323416/how-to-install-and-configure-a-dhcp-server-in-a-workgroup-in-windows-s

Bonnet, N. (2012). Windows Server 2012 R2 Administración. México: Ediciones ENI.

Delprato, G. (28 de Diciembre de 2013). Windows Server 2012: Instalando y Configurando DHCP. Obtenido de Windows Server: https://windowserver.com/2012/12/20/windows-server-2012-instalando-y-configurando-dhcp/

Microsoft. (22 de Mayo de 2014). IP Address Management (IPAM). Obtenido de https://blogs.technet.microsoft.com/uktechnet/2014/05/22/ipam-part-3/

Molenar, R. (Agosto de 2016). NetworkLessons. Obtenido de Introducción a DHCP: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dhcp/

networkworld. (01 de Diciembre de 2006). Obtenido de http://www.networkworld.es/archive/ipam-direcciones-ip-bajo-control

Peralta, M. (17 de Julio de 2012). Introducción a Windows Server 2012 IPAM. Obtenido de https://ramonmorillo.com/2012/07/17/introduccion-a-windows-server-2012-ipam/

Rouse, M. (Julio de 2017). DHCP (Protocolo de configuración de host dinámico). Obtenido de https://searchnetworking.techtarget.com/definition/DHCP

Windows. (Enero de 2018). DHCP. Obtenido de https://technet.microsoft.com/pt-pt/library/cc781008(v=ws.10).aspx

Unidad

V

Unidad V

Configuraciones de Red y Servidores DNS

5. Introducción IPv4 e IPv6

El protocolo TCP/IP es el protocolo utilizado para gestionar el tráfico de datos en la red. Este protocolo en realidad está formado por dos protocolos diferentes y que realizan acciones diferentes. Por un lado está el protocolo TCP, que es el encargado del control de transferencia de datos y por otro está el protocolo IP, que es el encargado de la identificación de la máquina en la red. (Ecured, 2017)

El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts, independientemente de si los hosts se encuentran en la misma red o en redes diferentes. Tanto el protocolo de Internet versión 4 (IPv4) como el protocolo de Internet versión 6 (IPv6) proporcionan direccionamiento jerárquico para los paquetes que transportan datos.

El diseño, la implementación y la administración de un plan de direccionamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente. En este capítulo, se examina detalladamente la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP. (Cisco Networking, 2014)

Ipv4 usa direcciones de 32 bits, limitándola a 232 = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales LAN. Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPv4. Esta limitación ayudó a estimular el impulso hacia Ipv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4.

IPv6 es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual del IPv4. En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

5.1. Configuración eta de red

1. Damos clic derecho sobre el icono de red y daremos clic en abrir centro de redes y recursos compartidos, como se muestra la figura 5.1.

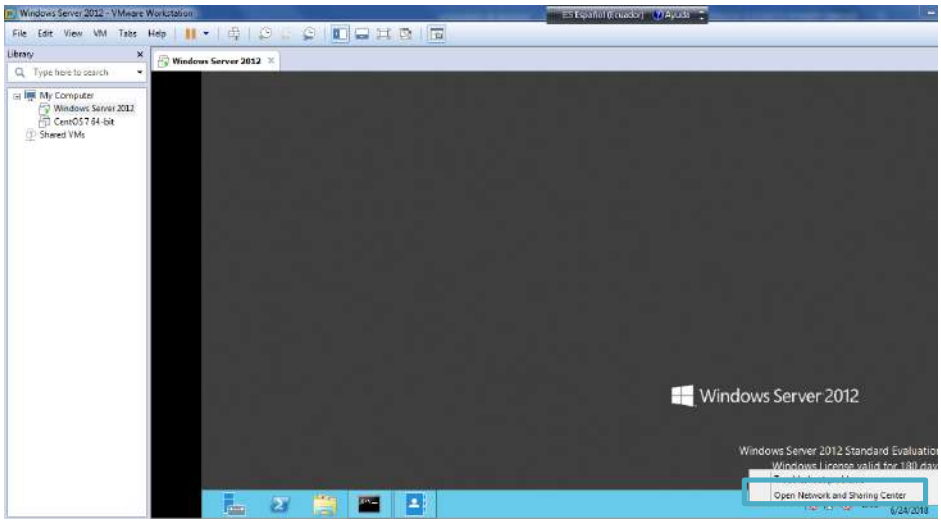


Figura 5. 1: Abriendo Centro de Recursos de Red

2. Luego damos clic en cambiar configuración del adaptador ver figura 5.2.

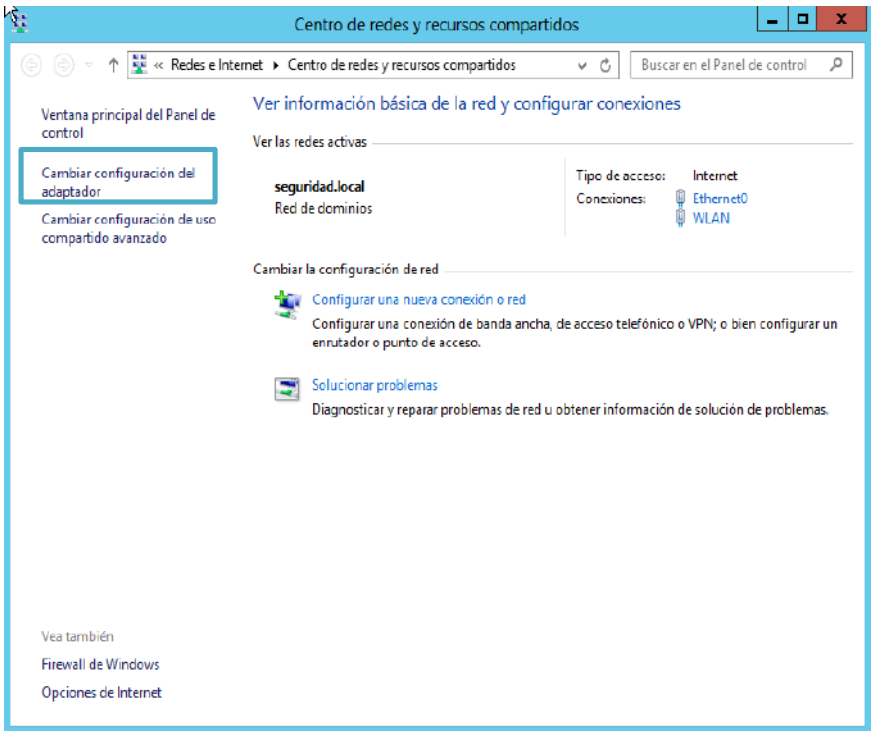


Figura 5. 2: Centro de redes y recursos compartidos

3. Luego sobre la red que se va a configurar se da clic izquierdo y luego propiedades, como se muestra la figura 5.3.

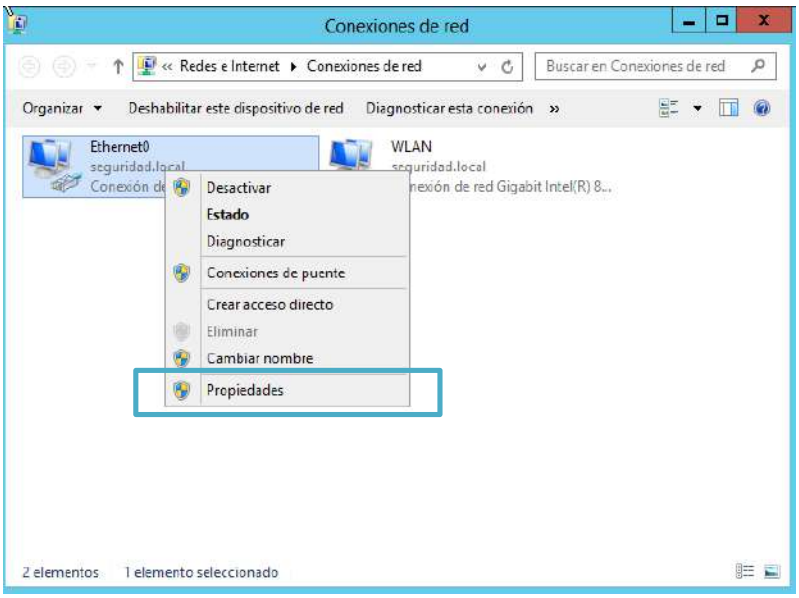


Figura 5. 3: Conexiones de Red

4. Dentro de "Propiedades de Ethernet" seleccionamos "Protocolo de Internet versión 4 (TCP/IPv4)" y hacemos clic en "Propiedades", ver figura 5.4.

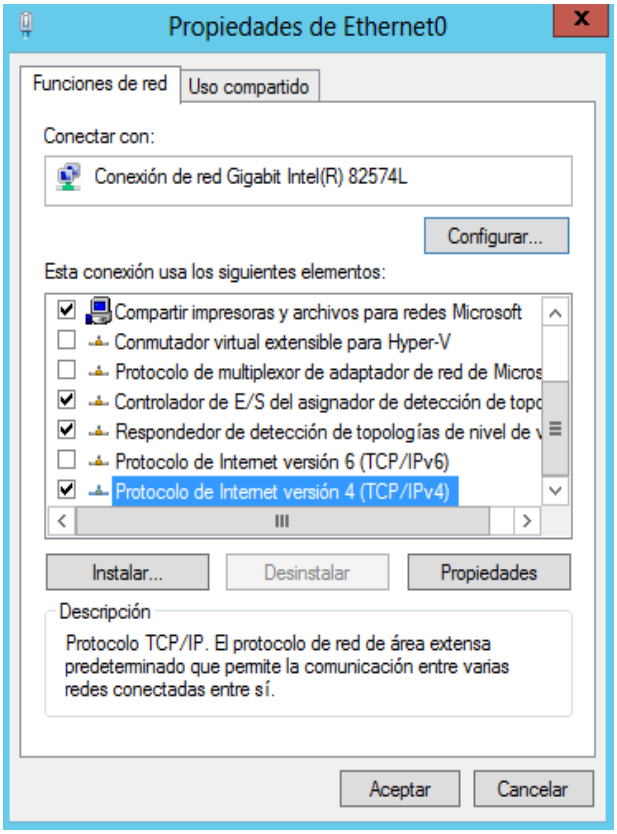


Figura 5. 4: Propiedades de Ethernet

5. En propiedades vamos a la pestaña "General" donde configuraremos los parámetros de red. Podemos seleccionar "Obtener una dirección IP automática" si tenemos un servidor DHCP alcanzable en nuestra red o "Usar la siguiente dirección IP". Si seleccionamos "Usar la siguiente dirección IP" debemos proporcionar tres datos:
   - Dirección IP: Dirección única y válida de la red.
   - Máscara de subred.
   - Puerta de enlace predeterminada: Puerta de acceso a la red. Es el siguiente salto para la salida a Internet, etc. (Ver figura 5.5)

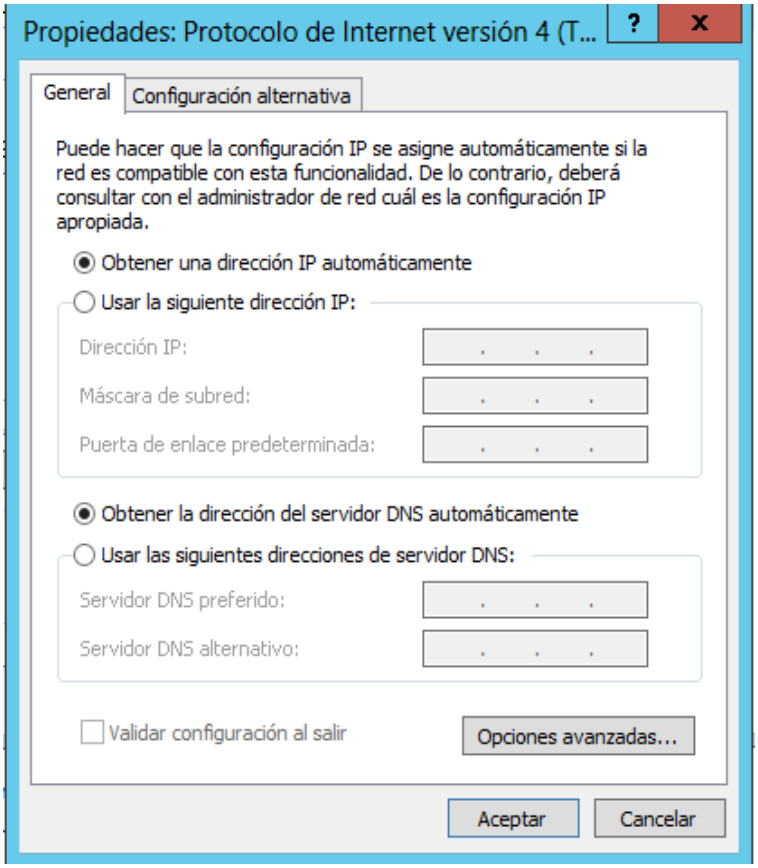


Figura 5. 5: Propiedades del protocolo IPv4

6. Y asignamos la dirección IP 192.168.239.125 dejamos por defecto la máscara y como servidor DNS dejamos la misma dirección IP, como se muestra la figura 5.6.

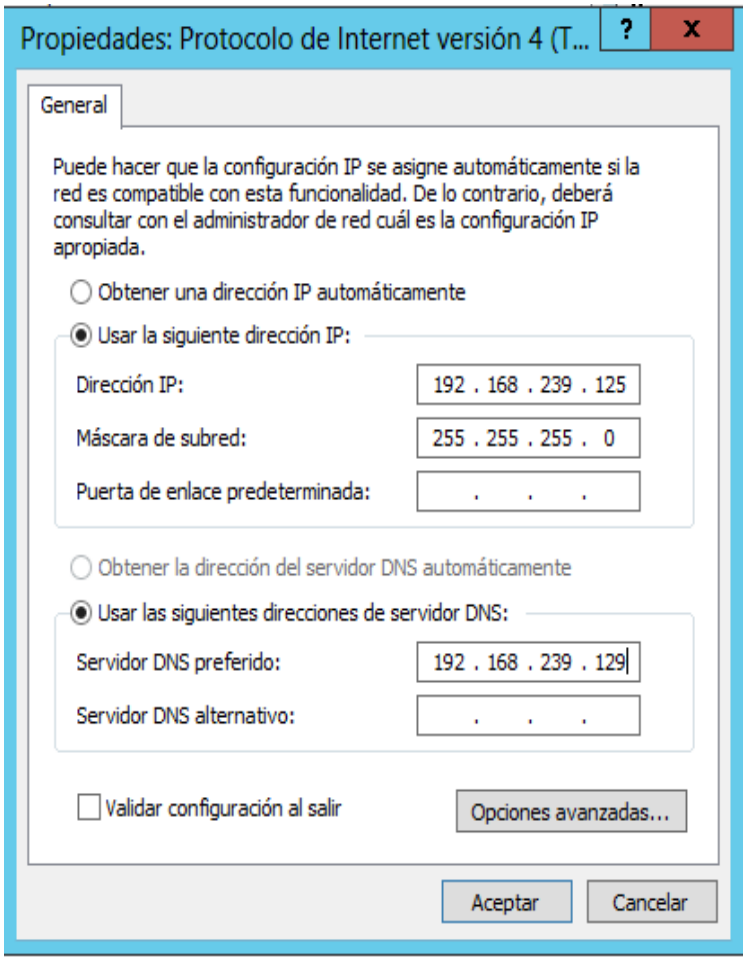


Figura 5. 6: Configurando direcciones IP

7. Pulsamos aceptar y ahora si reiniciamos el servidor.

5.2. Protocolo NAT y NAP

5.2.1. Protocolo NAT

NAT (Network Address Translation) es un proceso de cambio de las direcciones IP y los puertos de origen y destino. La traducción de direcciones reduce la necesidad de direcciones públicas IPv4 y oculta los rangos de direcciones de redes privadas. El proceso generalmente es realizado por enrutadores o firewalls.

Hay tres tipos de traducción de direcciones:

1. NAT estática: traduce una dirección IP privada a una dirección pública. La dirección IP pública siempre es la misma.
2. NAT dinámica: las direcciones IP privadas se asignan al grupo de direcciones IP públicas.
3. Traducción de dirección de puerto (PAT): una dirección IP pública se usa para todos los dispositivos internos, pero se asigna un puerto diferente a cada dirección IP privada. También conocido como sobrecarga NAT.

Un ejemplo te ayudará a entender el concepto ver figura 5.7:

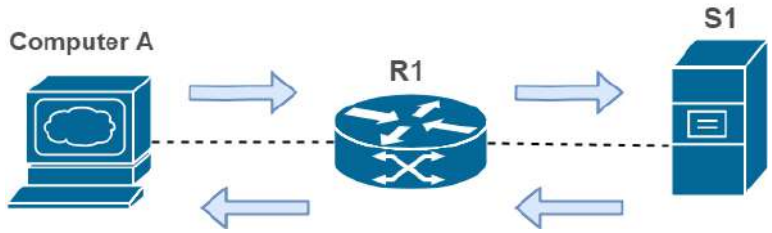


Figura 5. 7: Protocolo NAT

Computadora A solicita una página web desde un servidor de Internet. Debido a que el Equipo A usa direcciones IP privadas, el enrutador debe cambiar la dirección de origen de la solicitud porque las direcciones IP privadas no se pueden enrutar a través de Internet.

El enrutador R1 recibe la solicitud, cambia la dirección IP de origen a su dirección IP pública y envía el paquete al servidor S1. El servidor S1 recibe el paquete y responde al enrutador R1. El enrutador R1 recibe el

paquete, cambia las direcciones IP de destino a la dirección IP privada del equipo A y envía el paquete al equipo A. (CCNA, 2018)

5.2.2. Protocolo NAP

La Protección de acceso a la red (NAP) es una tecnología de Microsoft que impone el cumplimiento de los requisitos de salud de un sistema al garantizar que las computadoras de escritorio o portátiles recién conectadas no contengan ni permitan la creación de un virus o troyano. Antes de permitir que una computadora recién conectada acceda a la red, el software tanto del cliente como del servidor comprueba el sistema operativo de la computadora recién conectada, los navegadores de Internet, los programas antivirus, los firewalls, los programas y componentes de seguridad y todas las demás aplicaciones. Las computadoras cliente compatibles tienen acceso completo a la red, y los administradores del sistema de red pueden configurar el NAP para que las máquinas cliente no compatibles tengan acceso restringido.

Microsoft Network Access Protección utiliza puntos de cumplimiento NAP, computadoras o dispositivos de red que incluyen:

- ✓ Servidores de red privada virtual.
- ✓ Conductores con capacidad IEEE 802.1X.
- ✓ Control de acceso a la red.
- ✓ Servidores de protocolo de configuración dinámica de host.
- ✓ Autoridades de registro sanitario.

Sin embargo, estas computadoras o dispositivos de red deben usar Windows Server 2012 o la versión R2, que son capaces de almacenar las políticas de requisitos de salud de la computadora cliente y evaluar el cumplimiento utilizando el protocolo de Servicio de Usuario de Acceso Remoto de Autenticación (RADIUS) (para ser reemplazado por Diameter, un protocolo mejorado pero similar) que proporciona administración centralizada de autenticación, autorización y contabilidad para las computadoras cliente. Si no se cumple, los protocolos colocarán la computadora cliente en una red restringida. Este es un subconjunto de la Intranet (la red corporativa), que contiene recursos para ayudar a corregir la computadora del

cliente. Después de la corrección, la computadora del cliente puede volver a recibir una nueva evaluación. (Techopedia, 2014)

Es decir que el protocolo NAP es una tecnología que permite a los administradores definir determinadas condiciones en que se garantizará o no el acceso a la red interna de la empresa. Puede por ejemplo tratarse del caso de un ordenador portátil en que el antivirus, el antispyware o el cortafuegos tengan errores de configuración considerados peligrosos. El cliente NAP habiendo detectado defectos de configuración, podrá tomar la iniciativa permitiendo al ordenador conectar con un servicio de reparación para corregir los problemas detectados. (Francois, 2013)

5.3. Presentación del servicio DNS

DNS son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder. Cuando un ordenador está conectado a una red (ya sea Internet o una red casera) tiene asignada una dirección IP. Si estamos en una red con pocos ordenadores, es fácil tener memorizadas las direcciones IP de cada uno de los ordenadores y así acceder a ellos, pero ¿qué ocurre si hay miles de millones de dispositivos y cada uno tiene una IP diferente? Pues que se haría imposible, por eso existen los dominios y las DNS para traducirlos. (Sánchez, 2011)

Por lo tanto, el DNS es un sistema que sirve para traducir los nombres en la red, y está compuesto por tres partes con funciones bien diferenciadas.

- ✓ Cliente DNS: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.
- ✓ Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.
- ✓ Zonas de autoridad: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org).

5.3.1. ¿Qué es un DNS?

DNS significa Sistema de Nombres de Dominio (Domain Name System). DNS es un método usado en las redes informáticas principalmente para traducir los nombres de dominio, por ejemplo www.google.com, en su respectiva dirección IP, por ejemplo, a la dirección 2607: f8b0:4006:819::200e ver figura 5.8.

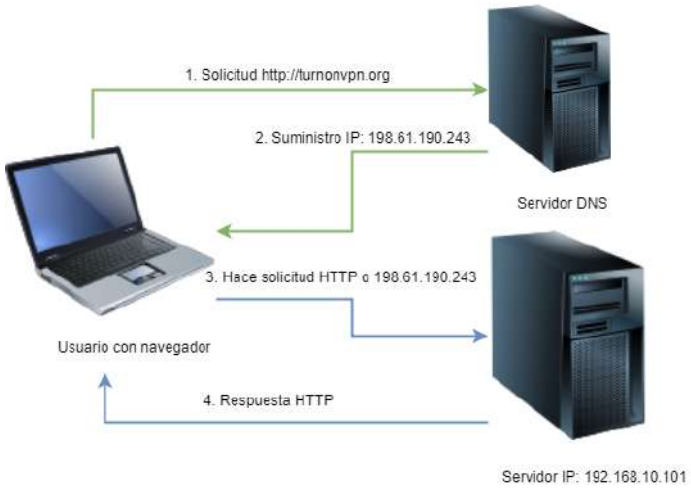


Figura 5. 8: DNS

Un DNS funciona como un directorio telefónico, donde los dominios funcionan como los nombres de una persona o empresa, mientras que la dirección IP como su número telefónico.

En internet, este sistema funciona de manera descentralizada, en un grupo de servidores DNS, los cuales poseen una base de datos de los nombres de dominio y sus respectivas direcciones IP. (Navia, 2018)

5.3.2. ¿Cómo funciona un DNS?

Las direcciones de los servidores DNS se pueden registrar manualmente o automáticamente mediante DHCP en la configuración de red de un equipo, como se muestra en la figura 5.9:

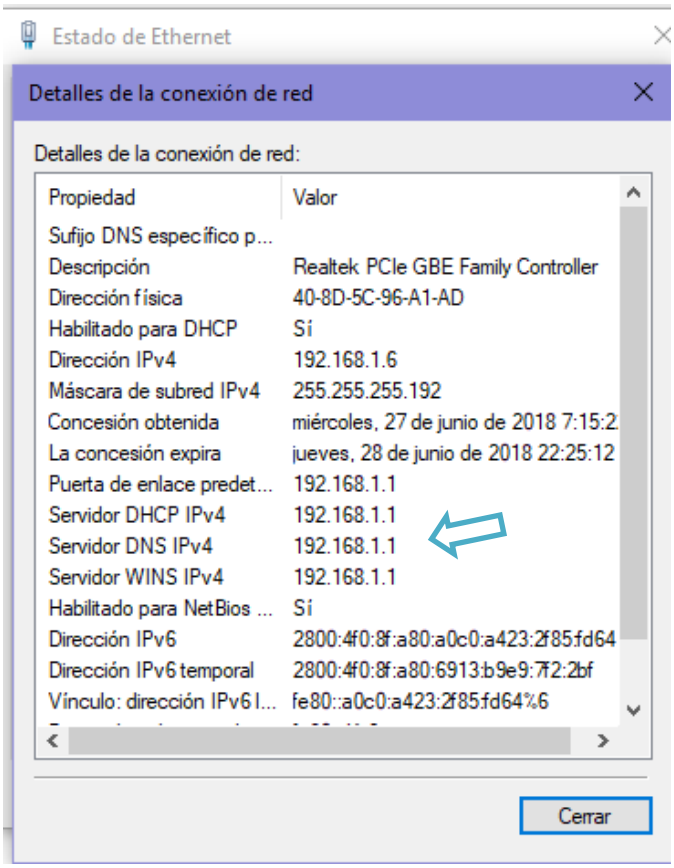


Figura 5. 9: Configuración Servidores DNS

Estas direcciones IP generalmente son los servidores DNS del proveedor de internet (ISP).

Así pues, cuando se pone una dirección IP en la barra de direcciones de un navegador como se muestra la figura 5.10:

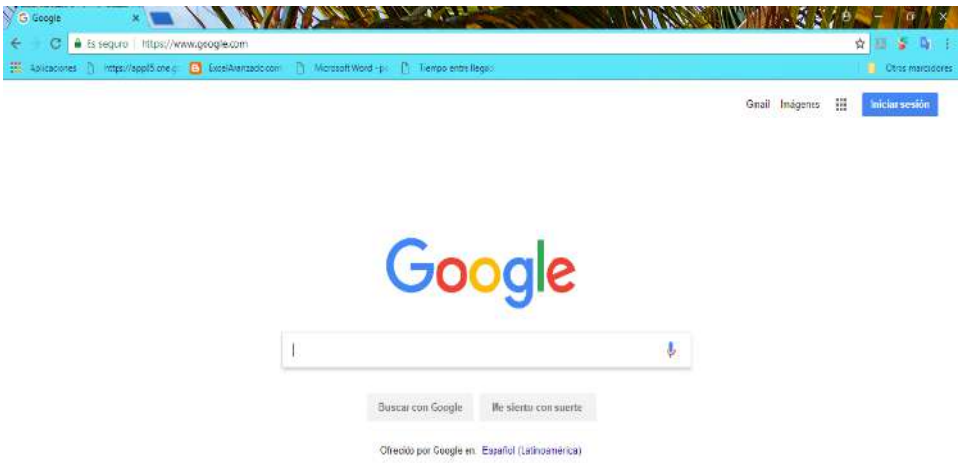


Figura 5. 10: Resolución nombre de dominio

Este realiza una petición al sistema operativo, para que solicite la resolución del dominio al servidor DNS. El DNS entonces entregará la dirección IP respectiva. Con esta dirección IP se establece la conexión entre el cliente (navegador) y el servidor donde se aloja el contenido de la página web. (Navia, 2018)

De esta forma también podemos conocer si el servidor está traduciendo el nombre de dominio o no (ver figura 5.11):

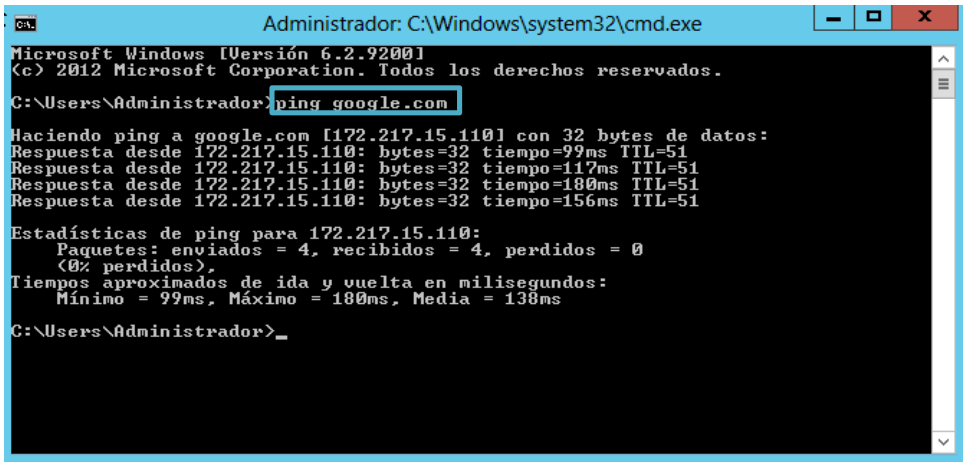


Figura 5. 11: Conocer la IP del dominio

Si la resolución no la puede hacer el servidor DNS inmediato, se pueden realizar peticiones de resolución a otros servidores DNS. Hasta que finalmente luego de varios intentos, se responde que el dominio no existe o no está registrado.

5.3.3. ¿Para qué sirve un servidor DNS?

El servidor DNS permite hacer más amigable la introducción de la dirección de un sitio, porque de otro modo tendríamos que aprendernos los 4 números, o más que podría componer una dirección IP.

Por otro lado, también permite que toda la red conozca cómo llegar desde cualquier lugar del mundo a nuestros servicios, porque la información de dominio se propaga en la red de manera redundante

en varios servidores DNS, actualizándose de manera periódica. (Navia, 2018)

5.3.4. Configuración del servicio DNS

En esta propuesta se pretende mostrar paso a paso la configuración del servicio de DNS el cual es aplicado para la comunicación entre servidores, este servicio es una base de datos distribuida y jerárquica que gestiona y mantiene información asociada a nombres de dominio en redes como Internet. Su uso más común es la asignación de nombres de dominio a direcciones IP de los nodos de Internet y la localización de los servidores de correo electrónico de cada dominio.

5.3.5. Instalación del servidor DNS

Para la instalación del rol servidor DNS debemos tener asignado una IP fija para ellos revisaremos la configuración de tarjeta de red explicado anteriormente.
Luego vamos al administrador del servidor y en la opción administrar damos clic en agregar roles y características, como se muestra la figura 5.12.

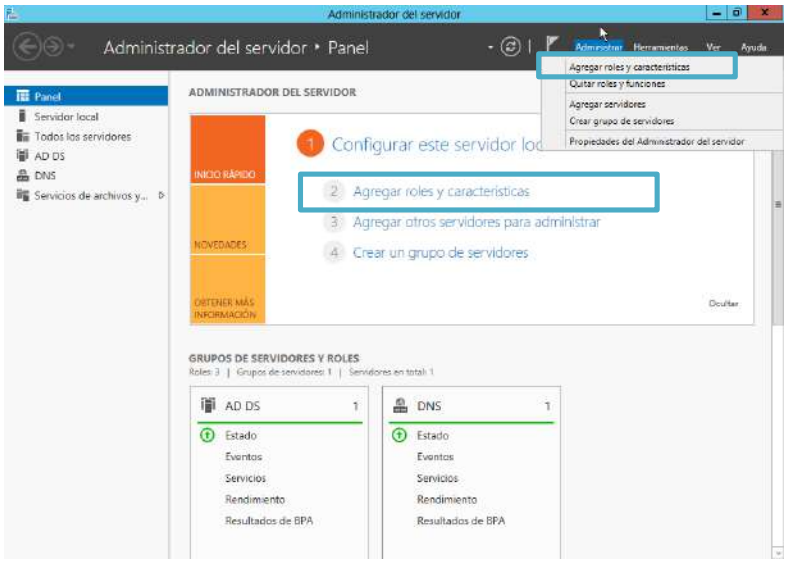


Figura 5. 12: Administrador de servidor

Nos mostrara la ventana de asistente de agregar roles y características en la cual damos clic en siguiente (ver figura 5.13).

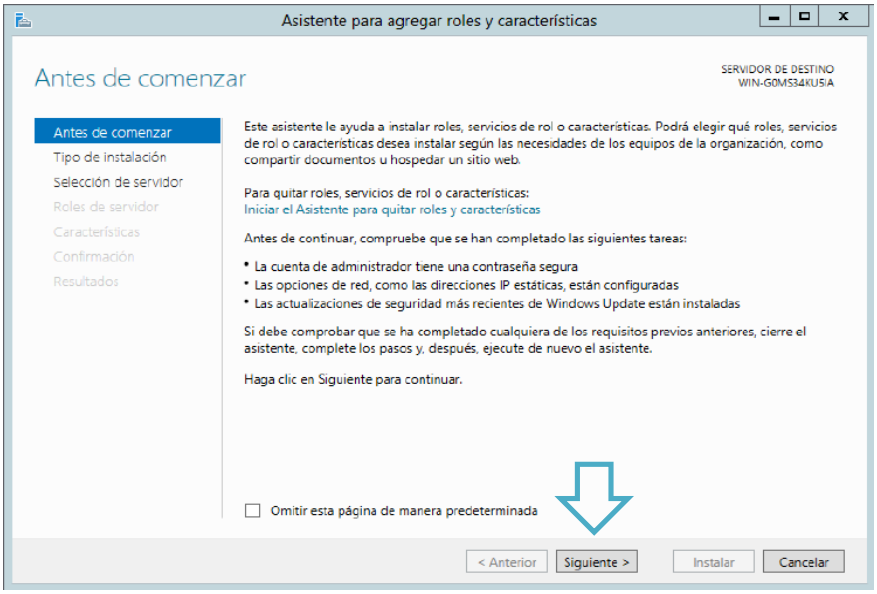


Figura 5. 13: Asistentes para agregar roles y características

Damos clic en instalación basada en características o roles y luego clic en siguiente, como se muestra figura 5.14.

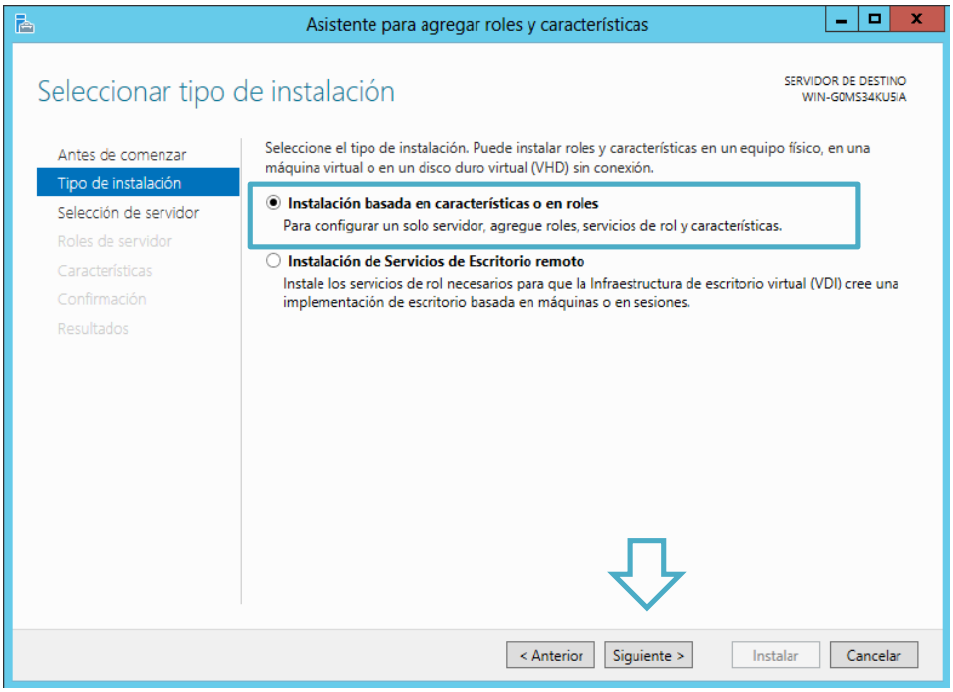


Figura 5. 14: Tipo de instalación

En la siguiente ventana escogemos el nombre del servidor en el cual se va a instalar el rol DNS y clic en continuar, como se muestra la figura 5.15.

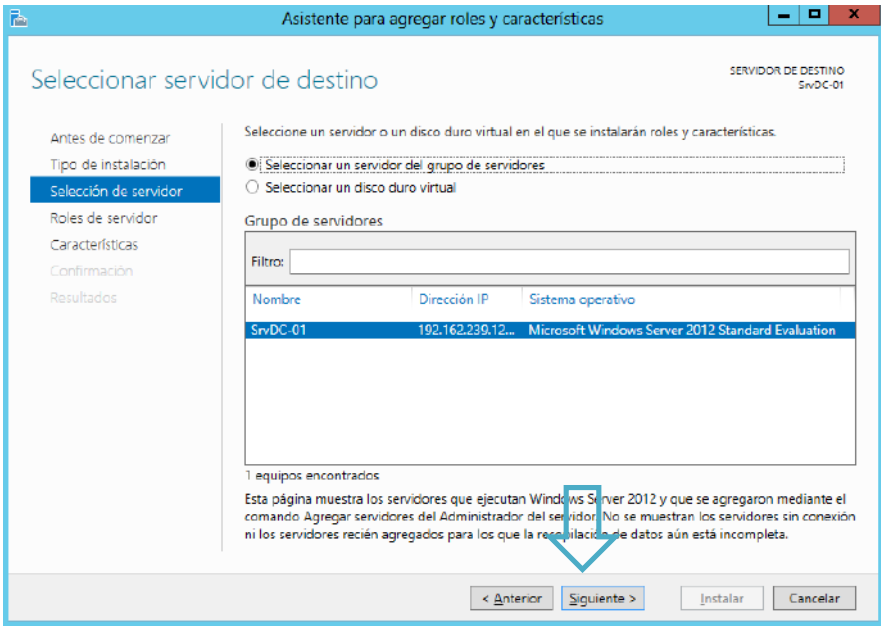


Figura 5. 15: Seleccionar el servidor

Marcaremos el rol "Servidor DNS", ver figura 5.16.

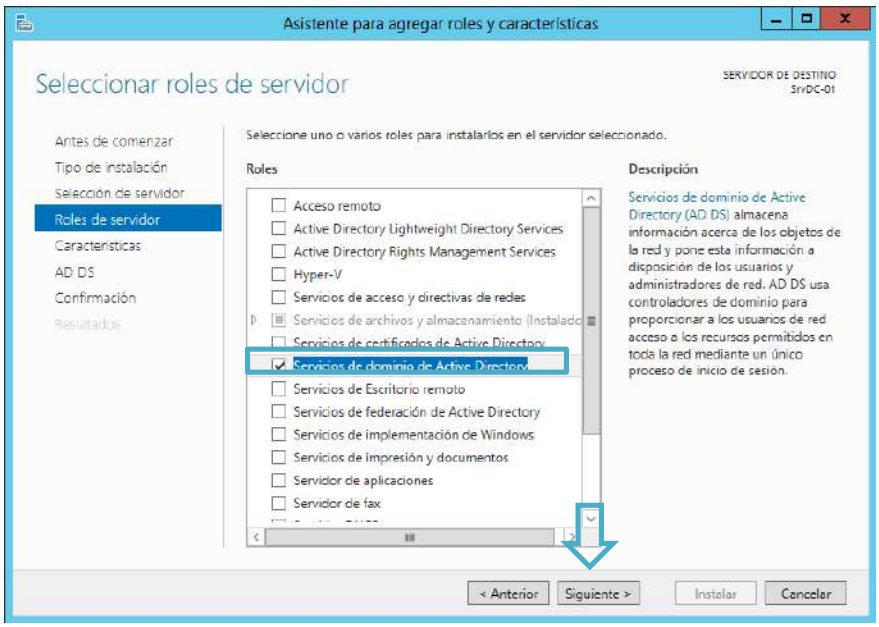


Figura 5. 16: Elegir opción DNS

El rol "Servidor DNS" requerirá de la característica "Herramientas de administración remota del servidor" - "Herramientas de administración de roles" - "Herramientas del servidor DNS". Nos lo indicará en la ventana de agregar características requeridas, marcaremos "Incluir herramientas de administración (si es aplicable)", como se muestra la figura 5.17:

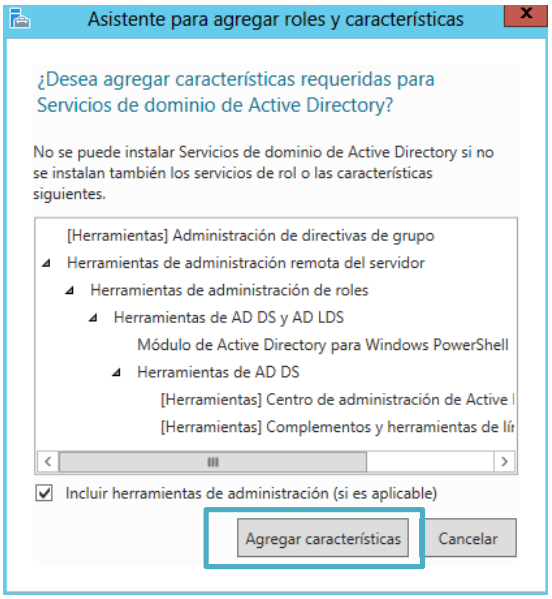


Figura 5. 17: Características Servidor DNS

El asistente para agregar roles y características nos indicará las características que se instalarán, pulsaremos "Siguiente", ver figura 5.18:

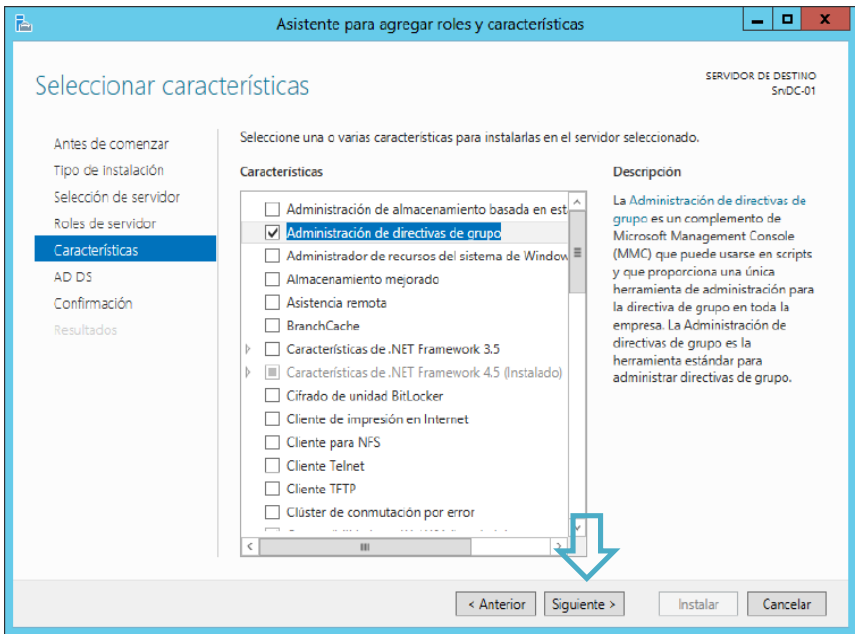


Figura 5. 18: Características DNS

El asistente para instalar el rol de Servidor DNS nos indicará algunas cuestiones a tener en cuenta, pulsaremos "Siguiente", ver figura 5.19:

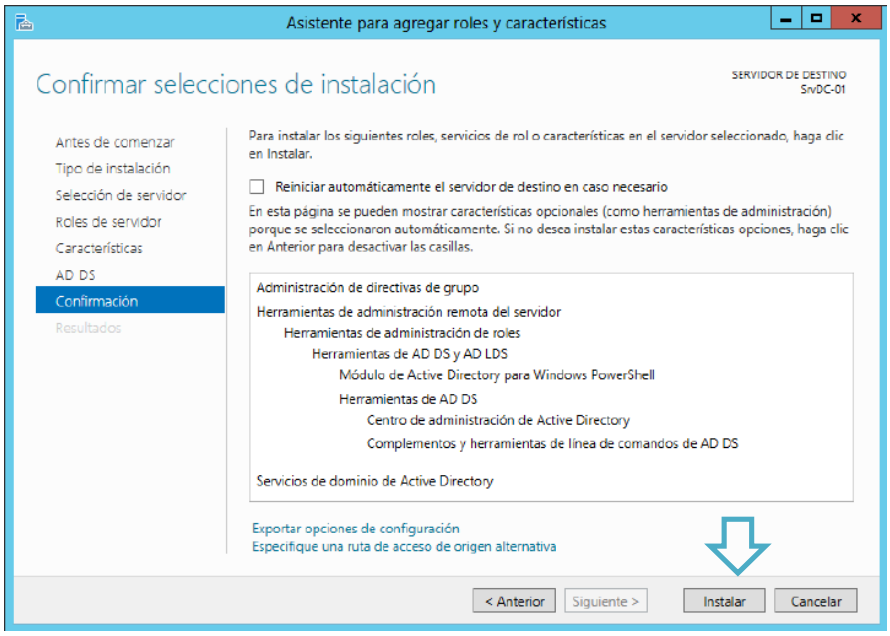


Figura 5. 19: Confirmación instalador DNS

Se iniciará la instalación del rol de Servidor DNS, el asistente nos indicará el progreso del proceso, ver figura 5.20:

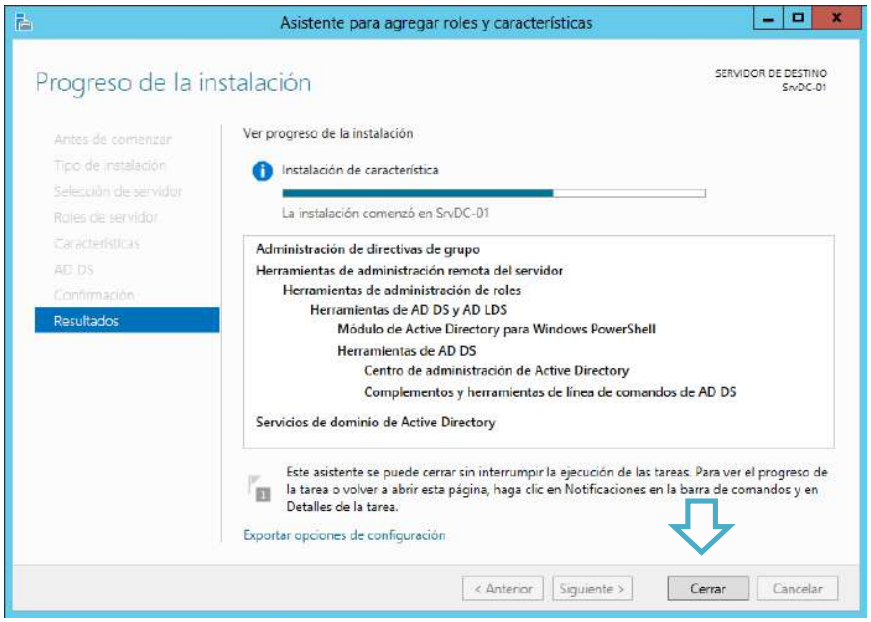


Figura 5. 20: Instalando DNS

El asistente para agregar roles y características nos indicará que el proceso ha finalizado con el texto "Instalación correcta". Pulsaremos "Cerrar".

5.4. Administración del servidor DNS

La administración de DNS es básica en la administración de dominios. En Openprovider la administración del servidor de nombre de dominios es gratuita para todos los clientes.

Utiliza nuestros DNS geográficamente dispersos para una seguridad óptima o utiliza Openprovider como copia de seguridad de tus propios DNS.

Los servidores de Nombres de Openprovider garantizan calidad y estabilidad en todo momento. Puedes escoger cómo utilizar nuestros servidores de nombres: puedes utilizar el DNS maestro, utilizar nuestros servidores como DNS esclavos, o bien utilizar tus propios servidores para todas las funciones. (Gónzales, 2016)

Para ello debemos realizar los siguientes pasos una vez reiniciado el equipo nos vamos al administrador de servidor y en la pestaña de herramientas damos clic en DNS (ver figura 5.21).

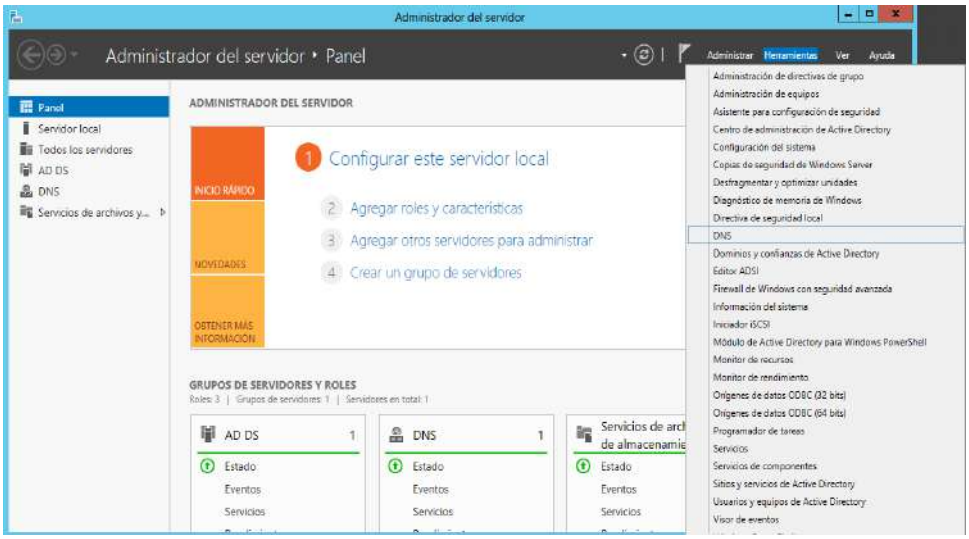


Figura 5. 21: Comprobando la instalación DNS

¿Sabías Qué?

No mostrará la ventana de administrador de DNS, ver figura 5.22.

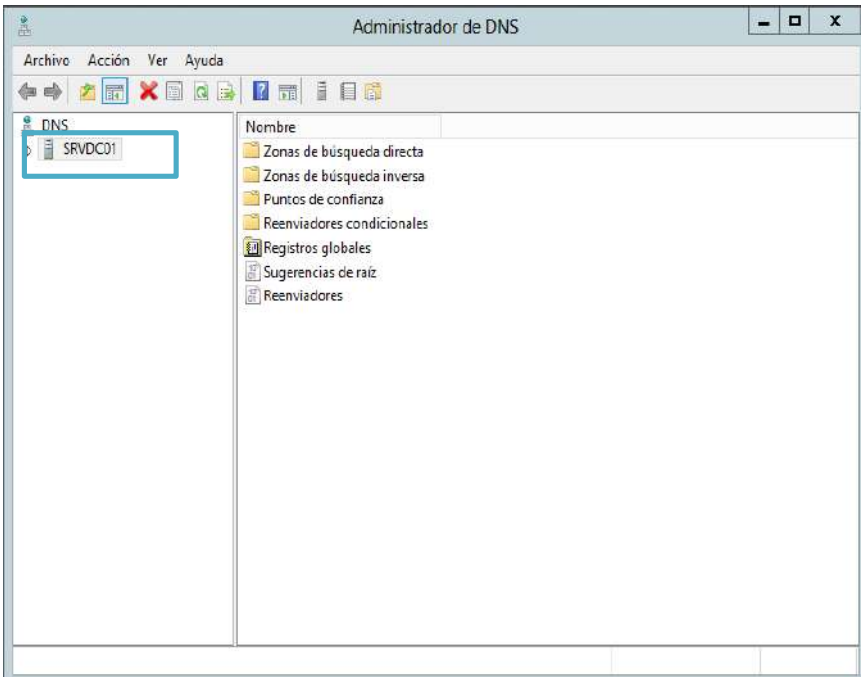


Figura 5. 22: Administrador DNS

Sobre el icono del servidor damos clic izquierdo y luego presionamos configurar servidor DNS, ver figura 5.23.

Esta herramienta llamada DNS nos permite conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder.

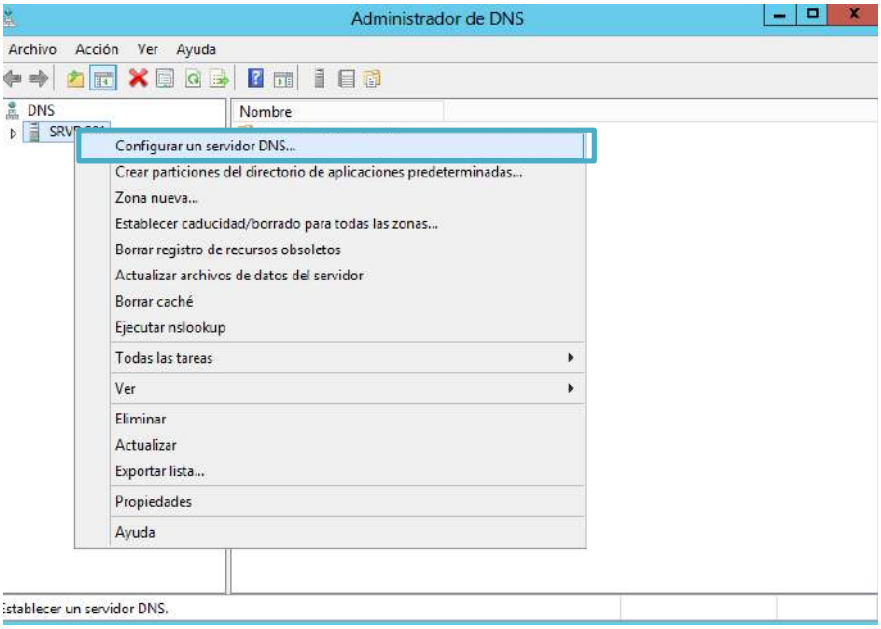


Figura 5. 23: Configurando un servidor administrador DNS

En la siguiente ventana damos clic en siguiente, ver figura 5.24.

Figura 5. 24: Asistente para configurar DNS

Dejamos marcada la opción por defecto y damos clic en siguiente, ver figura 5.25.

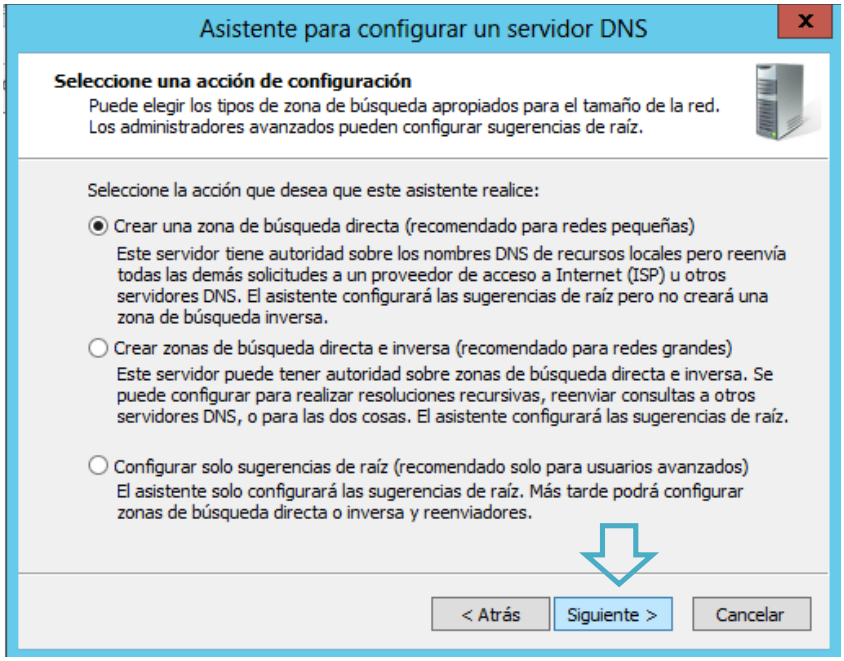


Figura 5. 25: Seleccionar una acción de configuración

Marcamos la opción que pertenecerá a la misma zona y clic en siguiente, ver figura 5.26.

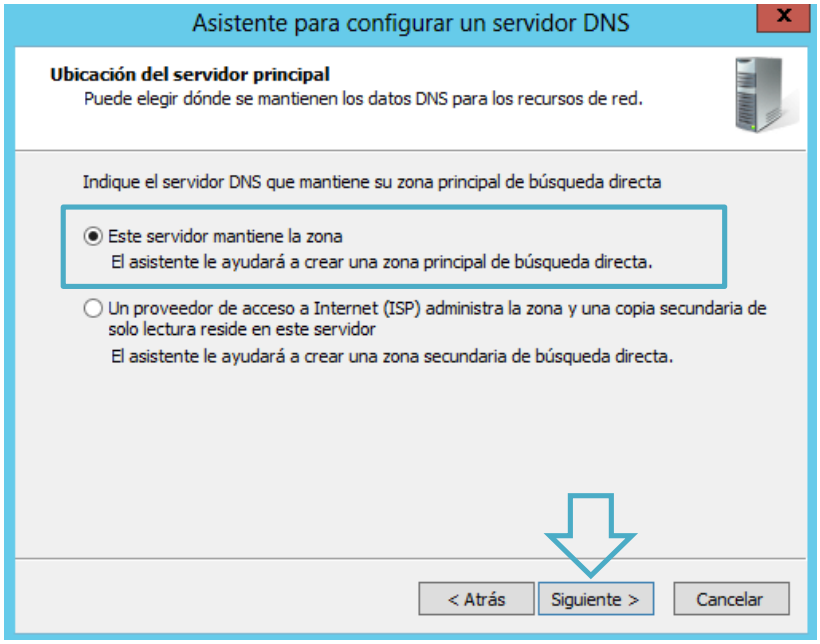


Figura 5. 26: Ubicación del servidor principal

Damos un nombre a la zona en este caso será techserv.local y dar clic en siguiente, ver figura 5.27.

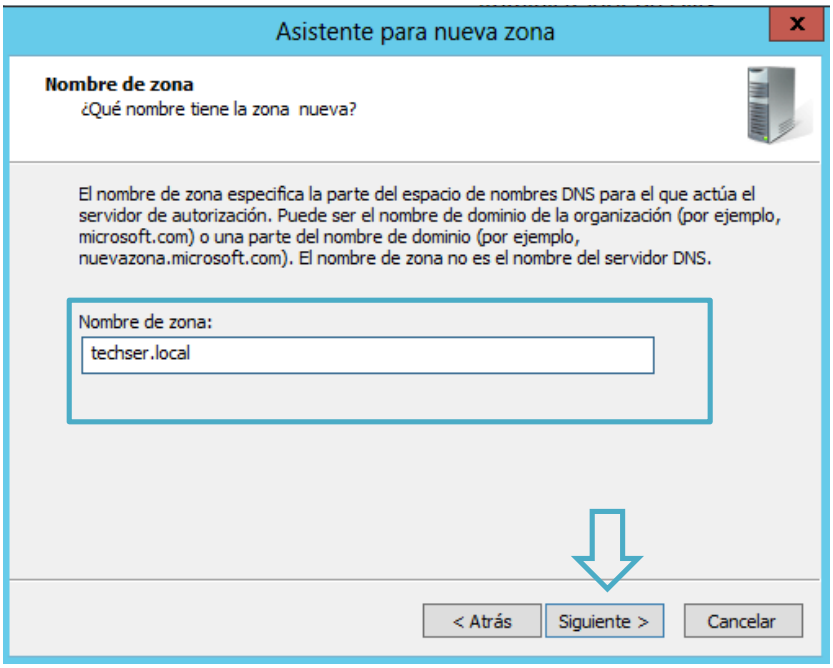


Figura 5. 27: Nombre de Zona

Dejamos la opción por defecto y damos clic en siguiente, ver figura 5.28.

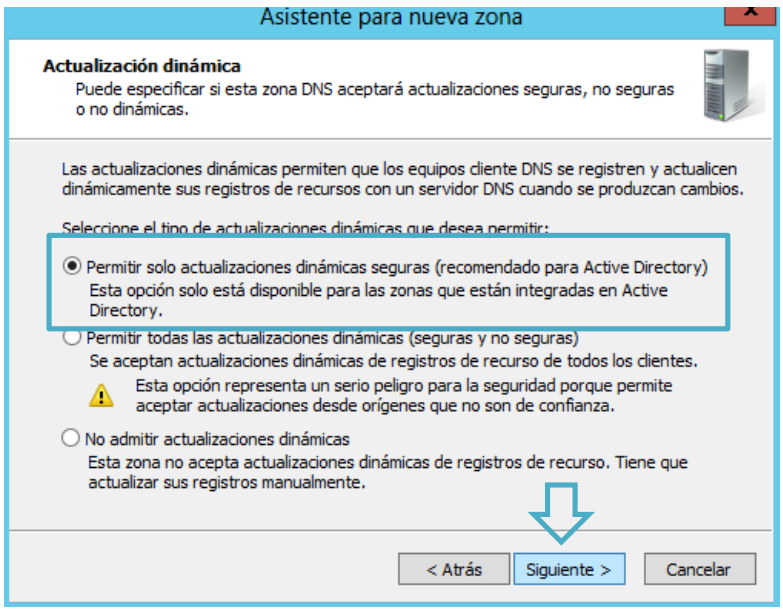


Figura 5. 28: Actualización dinámica

En la siguiente ventana podemos configurar las direcciones IP en este caso marcamos la opción no y dar clic en siguiente, ver figura 5.29.

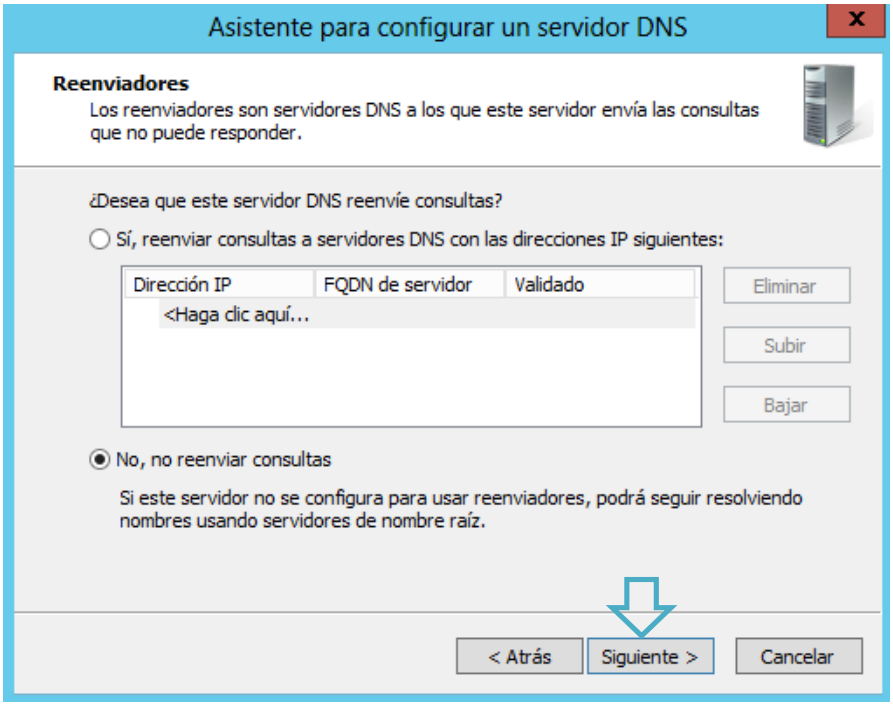


Figura 5. 29: Reenviadores

Procederá con la búsqueda de sugerencia de raíz y luego nos mostrará la ventana siguiente en donde daremos clic en finalizar, ver figura 5.30 y 5.31.

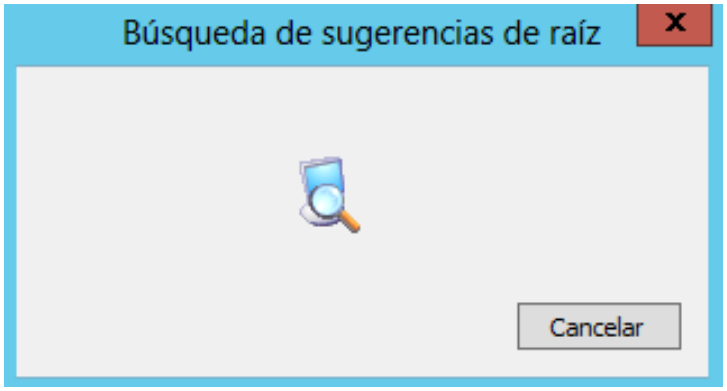


Figura 5. 30: Búsqueda de sugerencia de raíz

Figura 5. 31: Finalización del asistente servidor DNS

Luego en el administrador DNS damos clic en zona de búsqueda y podemos ver que está configurado el servidor DNS, ver figura 5.32.

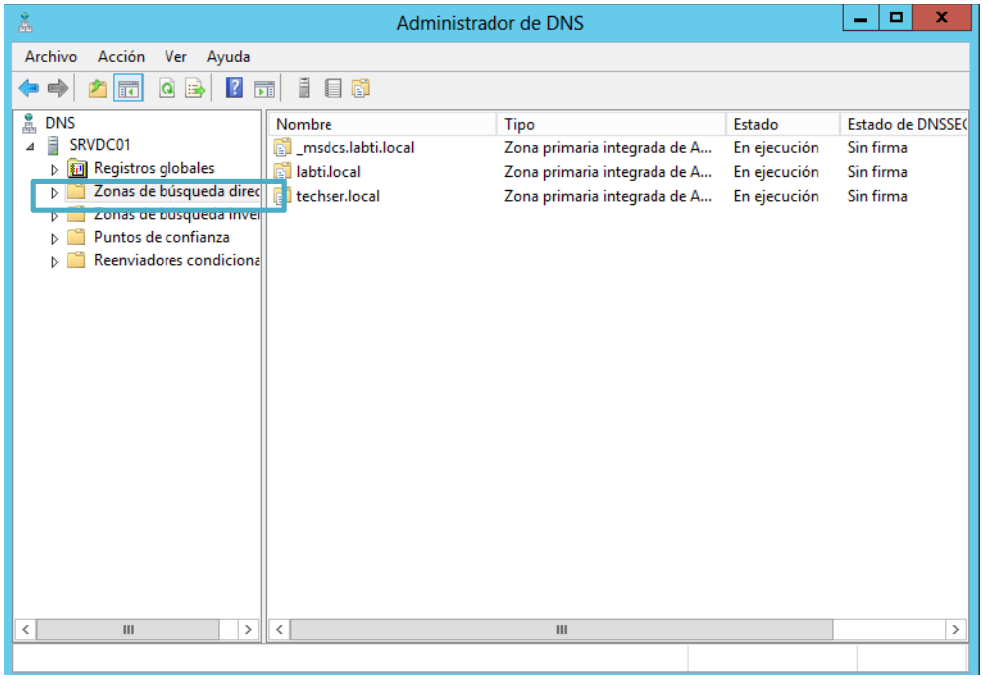


Figura 5. 32: Configurando Administrador DNS

5.5. Zonas del DNS

La Zona DNS del plan de alojamiento te permite apuntar distintas entradas de esta a servidores externos, de esta manera puedes utilizar servicios externos, por ejemplo:

- ✓ Utilizar un servicio de alojamiento con nosotros y el servicio de e-mail con Google Apps.
- ✓ Utilizar nuestros servidores DNS con un plan de Redirección y Parking (gratuito), pero apuntar a un blog alojado en Blogger.com bajo tu propio dominio.
- ✓ Apuntar tu dominio a tu propio ordenador y servir el contenido de la página web desde él, incluso si tienes una dirección IP dinámica, en ese caso puedes utilizar nuestra herramienta DNS. (Ponce, 2018)

5.5.1. Zonas DNS

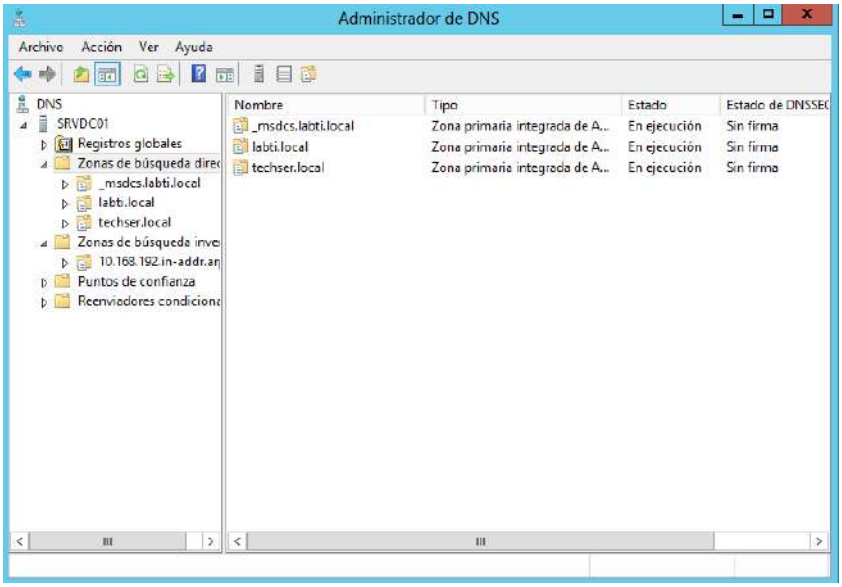


Figura 5. 33: Registro DNS

5.5.2. Registros DNS

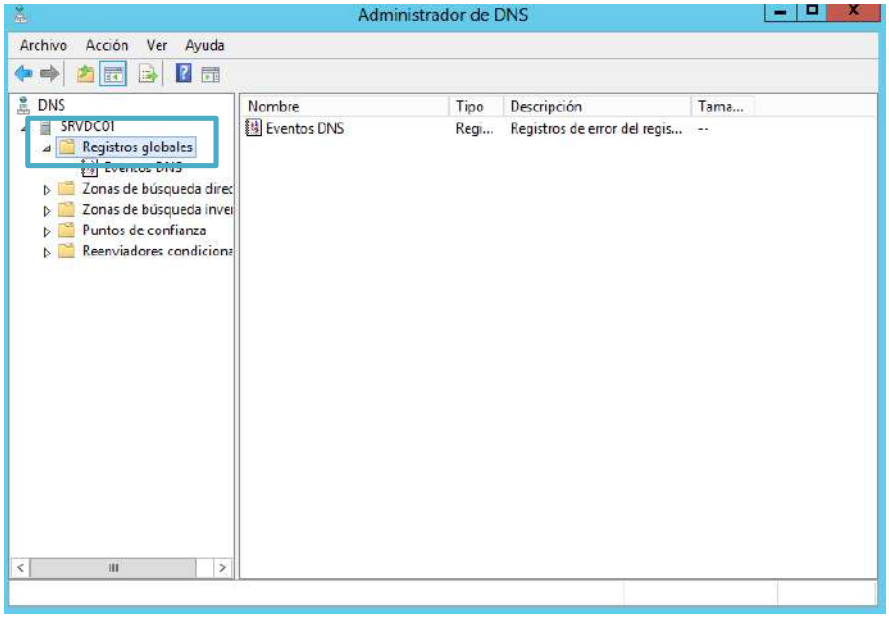


Figura 5. 34: Zona DNS

Los registros DNS son archivos de mapeo o sistemas que le indican a un servidor DNS a qué dirección IP está asociado un dominio particular. También les indican a los servidores DNS cómo manejar las solicitudes que se envían a cada nombre de dominio. Por ejemplo, cuando

escribe www.dominioejemplo.com en su navegador y pulsa Intro, el DNS lo traducirá a la dirección IP exacta donde se encuentra alojado el dominio. (Verdezoto, 2018)

Bibliografía

CCNA. (Abril de 2018). ¿Qué es NAT? Obtenido de http://study-ccna.com/what-is-nat/

Cisco Networking. (Abril de 2014). Asignación de direcciones IP. Obtenido de http://www.itesa.edu.mx/netacad/introduccion/course/module8/index.html#8.0.1.1

Ecured. (28 de Junio de 2017). Protcolo IPv4 y IPv6. Obtenido de http://www.ecured.cu/Ipv4

Francois, J. (2013). Windows Server Arquitectura y Gestión de los servicios de dominio. Barcelona: ENI. Obtenido de Arquitectura y Gestión de los servicios de dominio : https://books.google.com.ec/books?id=FqRjctcIsSEC&pg=PT306&lpg=PT306&dq=protocolo+nap&source=bl&ots=jjM6Yxbo9t&sig=hvCebRN2mu4MyOG_JHrc81AcQic&hl=es-419&sa=X&ved=0ahUKEwjkzdb4uvXbAhXks1kKHRfCALcQ6AEIVDAE#v=onepage&q=protocolo%20nap&f=false

Gonzáles, X. (Mayo de 2016). Administración de DNS. Obtenido de https://www.openprovider.es/servicios/administracion-de-dns/

Navia, F. (Enero de 2018). ¿Qué es un servidor DNS (Domain Name System) y para qué sirve? Obtenido de https://fireosoft.com.co/blogs/que-es-servidor-dns-sirve/

Ponce, R. (Febrero de 2018). Zona DNS. Obtenido de DonDominio: https://www.dondominio.com/help/es/209/zona-dns/

Sánchez, M. (29 de Enero de 2011). Cómo funciona Internet: ¿Qué son y para qué sirven las DNS? Obtenido de https://www.xatakamovil.com/conectividad/como-funciona-internet-dns

Techopedia. (Septiembre de 2014). Protección de acceso a redes de Microsoft (NAP). Obtenido de https://www.techopedia.com/definition/24148/microsoft-network-access-protection-nap

Verdezoto, J. (2018). ¿Qué son los registros DNS? Obtenido de Centro de ayuda de dominio: https://support.marcaria.com/hc/es/articles/215527983--Qu%C3%A9-son-los-registros-DNS-

Unidad

VI

Unidad VI

Servidores de Archivos

DFS y NTFS

6. Introducción

La función de un servidor de archivos es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por éste. En principio, cualquier ordenador conectado a una red con un software apropiado, puede funcionar como servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente, es decir normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina. (Mena, 2016)

NTFS es el sistema de archivos predeterminado en todas las versiones modernas de Windows; por lo tanto, al igual que FAT, tiene un amplio uso. A diferencia de FAT, está en uso como el sistema de archivos en el que se ejecutan la mayoría de las computadoras domésticas y comerciales.

Un concepto central en NTFS es simple: todo es (o está almacenado en) un archivo. Los archivos, directorios y estructuras regulares que controlan el diseño del sistema de archivos en el disco (como la FAT de FAT16) son archivos o están almacenados en archivos. No existe un plano de existencia separado para los metadatos del sistema de archivos (como los inodos en un sistema de archivos UNIX-y o las entradas de directorio FAT + en FAT16).

El siguiente concepto central en NTFS es que lo anterior es un poco engañoso. La mayoría (pero no todos) de lo que pensamos como metadatos del sistema de archivos se almacena en una estructura de datos particular: la Tabla Maestra de Archivos (MFT), que se almacena como un archivo, pero es muy similar a las FAT y Dirent, como 'Veré. Pasaremos mucho tiempo hoy y la próxima clase hablando sobre MFT y cómo se relaciona con los archivos almacenados en el disco.

La última cosa de alto nivel que necesita saber sobre NTFS es que divide un disco en unidades asignables llamadas clústeres, al igual que FAT. Al igual que FAT, los clústeres tienen el tamaño de una potencia de dos del tamaño del sector del disco subyacente. Sin embargo, a diferencia de FAT, el clúster 0 comienza al principio de la partición, por lo que no hay ninguna de las tonterías del "primer clúster es el número de clúster 2" con el que lidiar. (Levine, 2017)

6.1. NTFS

6.1.1. ¿Qué es NTFS?

Es un sistema de archivos diseñado específicamente para Windows NT, y utilizado por las versiones recientes del sistemas operativos Windows.

Ha reemplazado al sistema FAT utilizado en versiones antiguas de Windows y en DOS.

NTFS permite definir el tamaño del clúster de forma independiente al tamaño de la partición. El tamaño mínimo del bloque es de 512 bytes. Este sistema también admite compresión nativa de archivos y encriptación.

Es un sistema ideal para particiones de gran tamaño, pudiendo manejar discos de hasta 2 terabytes. (Alegsa, 2010)

6.1.2. Estructura NTFS

Este sistema como tal se basa en una estructura llamada MFT (Master File Table), la que contiene información detallada de los archivos.

NTFS permite el uso de nombres extensos, aunque, a diferencia de FAT32, distingue entre mayúsculas y minúsculas.

En cuanto a rendimiento, el acceso a los archivos en una partición NTFS es más rápido que en una partición de tipo FAT, ya que usa estructuras de datos avanzadas (B+Tree) para localizar los archivos. En teoría, el tamaño límite de una partición es de 16 exabytes exactamente 17 mil millones de TB. (EcurRed, 2017)

6.1.3. Archivos NTFS

Un servidor de archivos es un tipo de servidor que almacena y distribuye diferentes tipos de archivos entre los clientes de una red de ordenadores. Su función es permitir a otros nodos el acceso remoto a los archivos que almacena o sobre los que tiene acceso. (Mena, 2016)

Los formatos de archivos NTFS:

- Permite el acceso a archivos y carpetas por medio de permisos.
- Se basa en una estructura llamada "tabla maestra de archivos" o MFT, la cual puede contener información detallada en los archivos.

6.1.4. Gestión de archivos

Es la administración de los archivos esto se realiza a través del sistema operativo permitiendo que los usuarios tengan acceso directo con los archivos y tengan control de ellos, así como también se puede enviar y compartir archivos con otros usuarios, brindarles seguridad y protección a estos. (OrjaLes, 2012)

De modo que le permite al usuario realizar ciertas operaciones con ellos, las cuales son:

1. Puedes crear un archivo, identificándolo con un nombre y determinar el espacio de este.
2. Abrir el archivo, aquí se realiza distintas operaciones como su ejecución, leerlo, escribir en él.
3. Borrarlo de modo que puedes liberar el espacio que ocupa este archivo.
4. Cerrar el archivo, finaliza la ejecución de este.
5. Modificarlo permite hacer cambios al archivo como cambiar su nombre.

6.2. Rol de servidor de archivos

Los principales problemas en la gestión del almacenamiento son la demanda creciente de almacenamiento y una disponibilidad permanente de los datos. Para responder a estas necesidades en la gestión de la capacidad y del almacenamiento, es importante definir directivas de gestión de los recursos de almacenamiento.

El rol de servidor de archivos pone a disposición de los administradores herramientas para la administración del sistema de archivos.

Entonces, es posible gestionar la capacidad a partir de una administración de cuotas, así como a partir de un sistema de filtrado por extensión de archivo. Los informes permiten obtener, de forma muy rápida, información muy variada. (Guzman, 2012)

6.2.1. Instalación del rol de servidor de archivos

1. Entramos a consola de administrados de servidor hace clic en agregar roles y características, tal como muestra la figura 6.1.

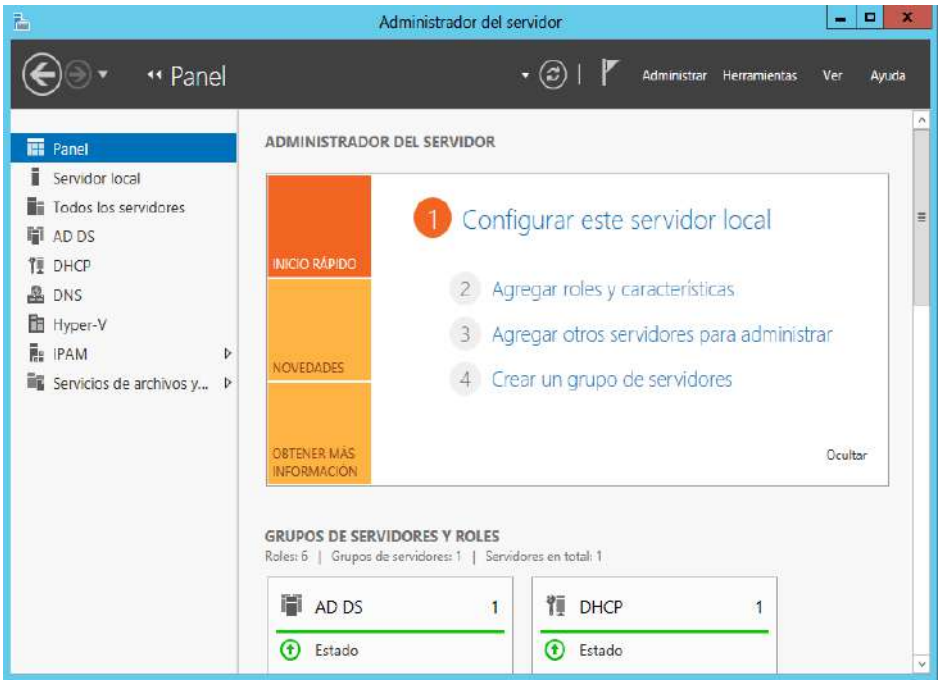


Figura 6. 1: Administrador del servidor

2. Seleccionamos el tipo de instalación le dar clic siguientes como se muestra la figura 6.2.

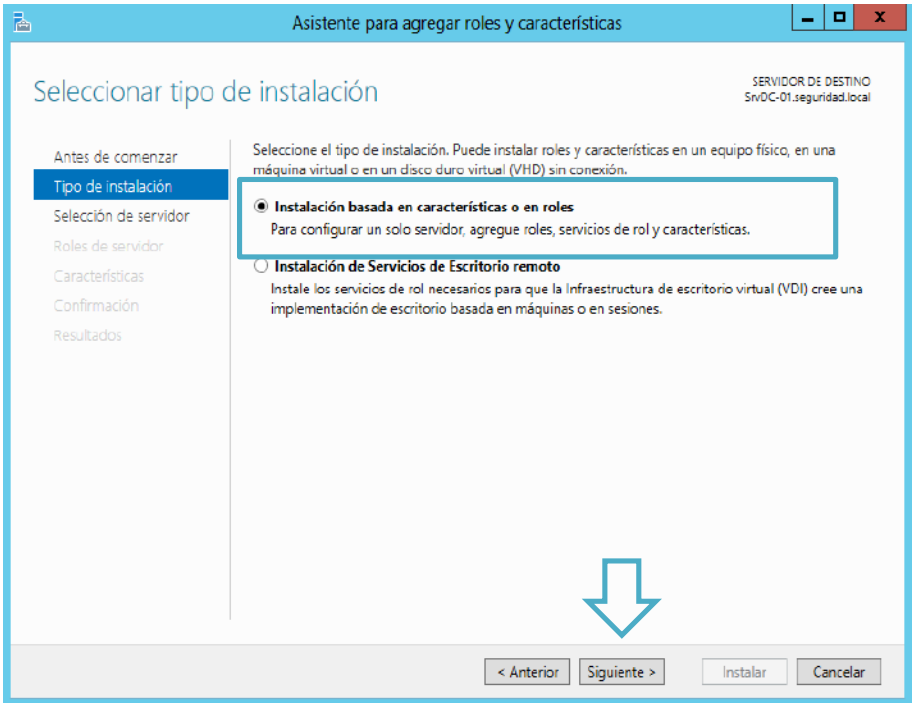


Figura 6. 2: Seleccionar el tipo de instalación

3. Después aparece la siguiente ventana la de selección de servidores por defecto saldrá SrvDC-01, pulsamos en siguiente desplegamos la opción servicios de archivos y almacenamientos, y a continuación servicios iSCSI y archivos, después confirmamos la instalación mostrará un resumen y al finalizar cerramos luego, luego de eso confirmamos si se instaló correctamente, como se muestra la figura 6.3.

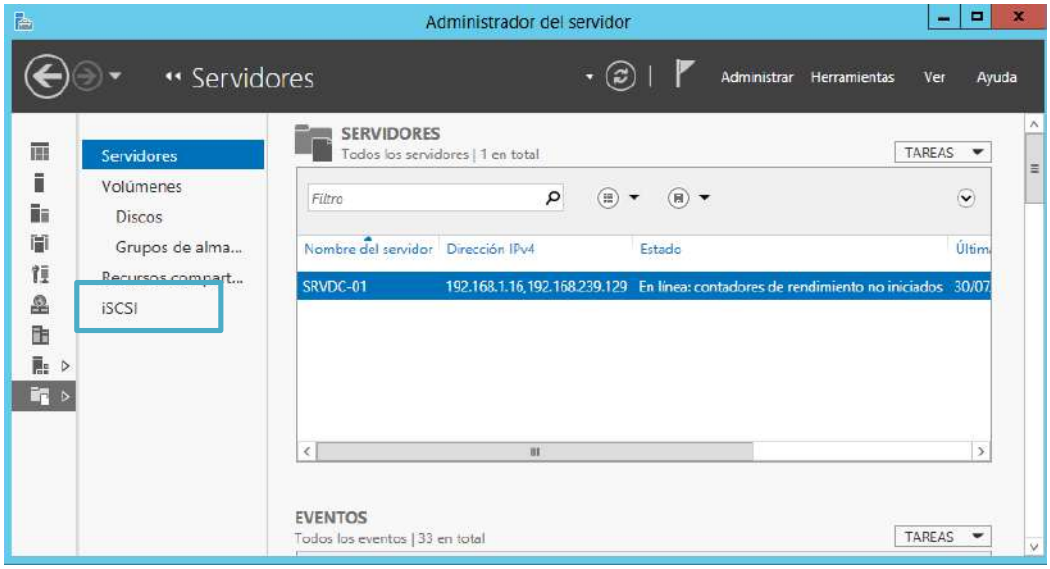


Figura 6. 3: Servicios de archivos y almacenamientos instalado

6.3. Seguridad de un sistema de archivos

Uno de los mayores problemas que se presentan al almacenar información en un computador es la seguridad de esta, teniéndose que idear mecanismos que protejan esta información tanto de daños físicos como de acceso inadecuado o mal intencionado. Los orígenes de los problemas de seguridad tienen diferentes causas: (Salazar, 2012)

- Pueden ser producidos por actos fortuitos debido a causas ajenas al sistema informático (como incendios, apagones de luz, etc.)
- Averías en el propio computador o error en los programas (mal funcionamiento del procesador, errores de comunicación, etc.)
- Errores humanos o actos mal intencionados (ejecución incorrecta de un programa)

Un sistema de archivos por definición, es una estructura jerárquica de carpetas que alojan archivos, y los aseguran mediante series de Listas de Control de Acceso (ACLs) y Entradas de Control de Acceso (ACEs) que definen el tipo de permisos que se permiten o niegan a aquellas carpetas y archivos. Así que el primer método para asegurar carpetas y sus archivos en un mundo Windows son los permisos. (Sánchez, 2012)

Para esos realizamos los siguientes pasos:

1. Pasos crear la carpeta en el disco local, como se muestra la figura 6.4.

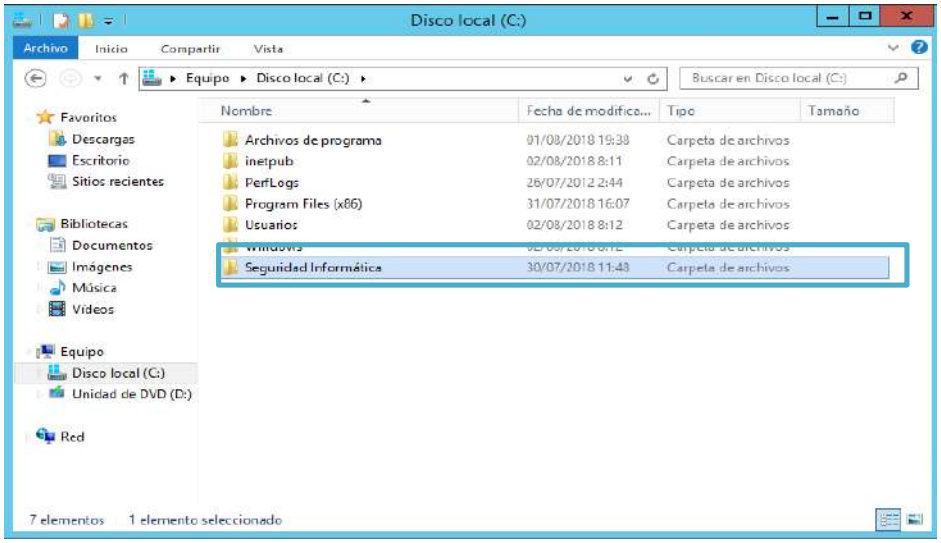


Figura 6. 4: Creación una carpeta disco local C

2. Lo que debemos hacer es establecer los permisos de acceso en las carpetas para eso damos clic derecho dentro de la carpeta seguridad informática propiedades opción compartir la carpeta y dar los respectivos permisos, ver figura 6.5.

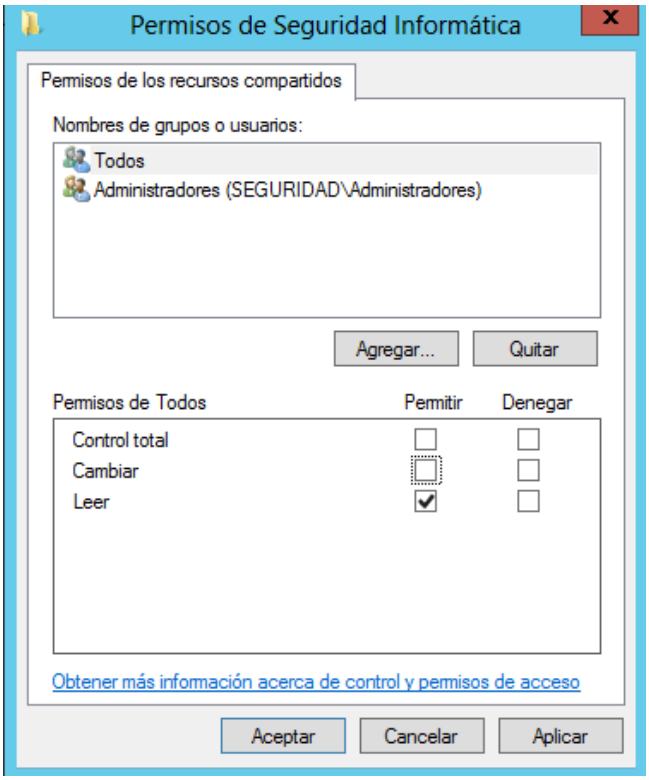


Figura 6. 5: Permisos de seguridad de la carpeta creada

3. Luego de terminar los permisos nos dirigimos en seguridad también accedemos a dar permiso, ver figura 6.6.

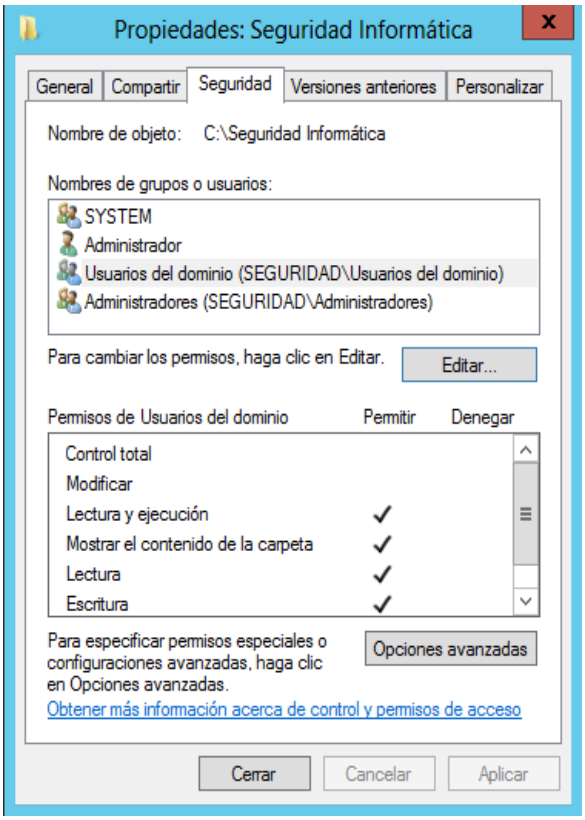


Figura 6. 6: Eligiendo el usuario que vamos a dar acceso

4. Damos clic opciones avanzadas y aparecerá configuraciones de seguridad para la carpeta que hemos creado, ver figura 6.7.

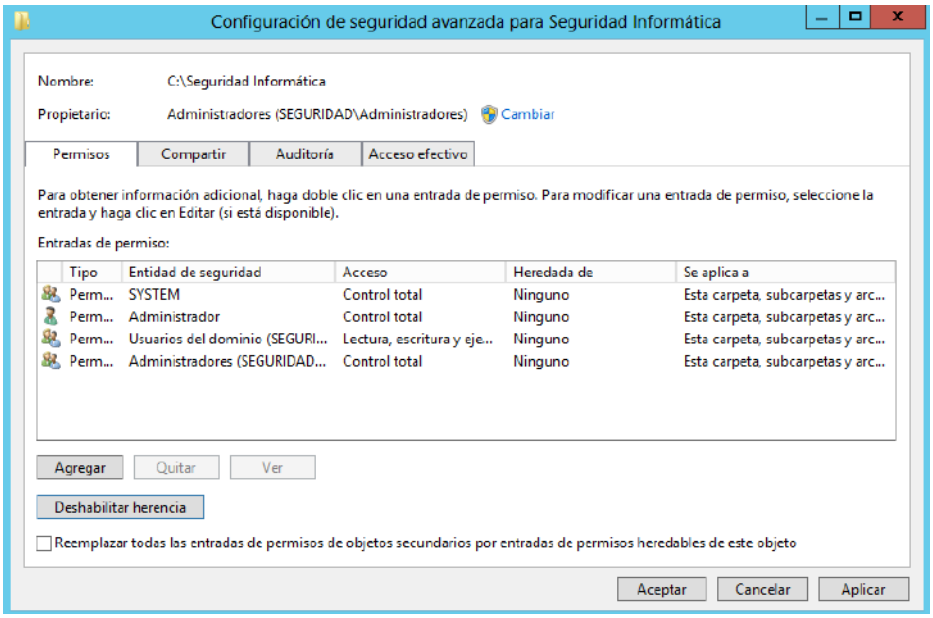


Figura 6. 7: Configuración de seguridad avanzada

5. Deshabilitamos la herencia seleccionamos convertir los permisos heredados en permisos explícitos en este objeto, ver figura 6.8.

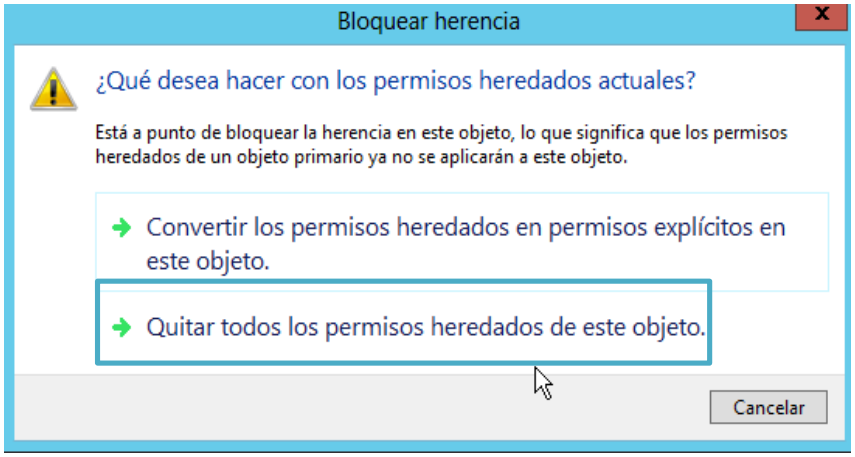


Figura 6. 8: Desactivar los permisos heredados

6. Después de eso nos vamos a la entrada de permisos y solo seleccionamos las opciones que como se muestra en la figura aceptamos y cerramos, ver figura 6.9.

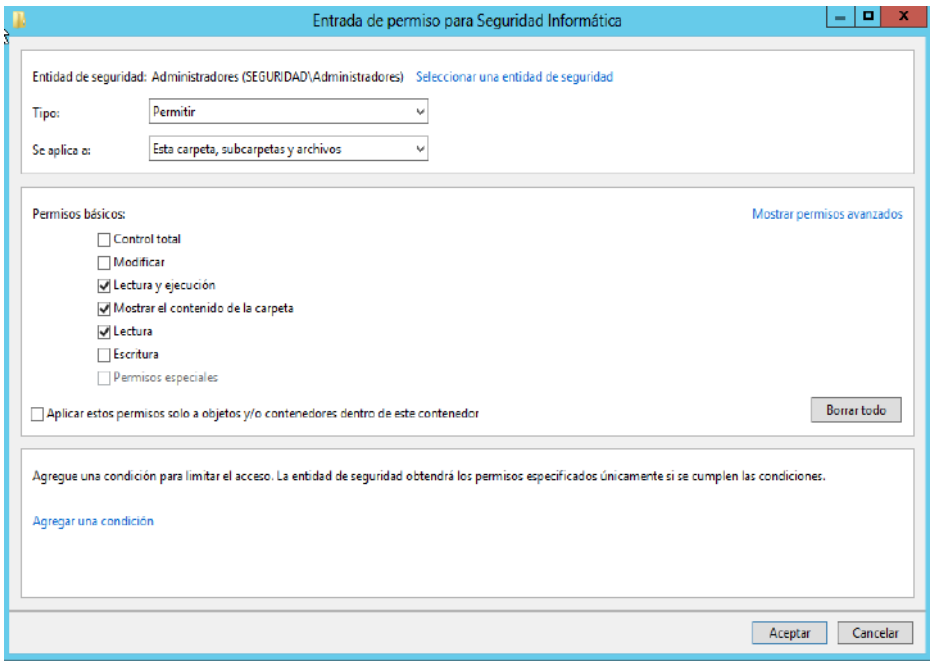


Figura 6. 9: Entrada de permiso

7. Abrirnos la carpeta Seguridad Informática, que se encuentra en el disco local C y creamos un documento que se llamará informática, ver figura 6.10.

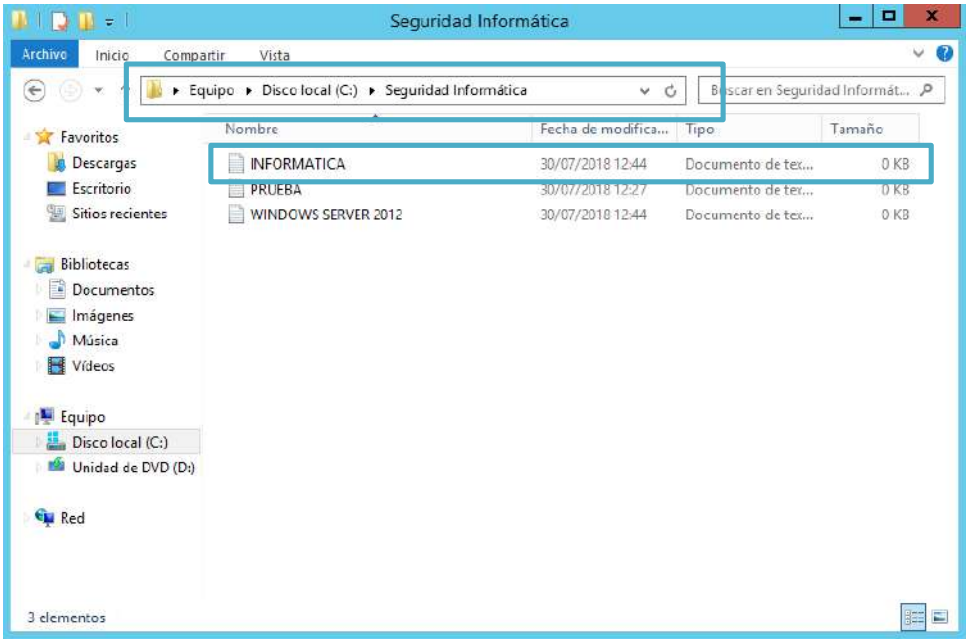


Figura 6. 10: Creación del archivo informática

8. Presionamos Windows + r y digitamos \\SRVDC-01 y nos dirige a la carpeta compartida, ver figura 6.11.

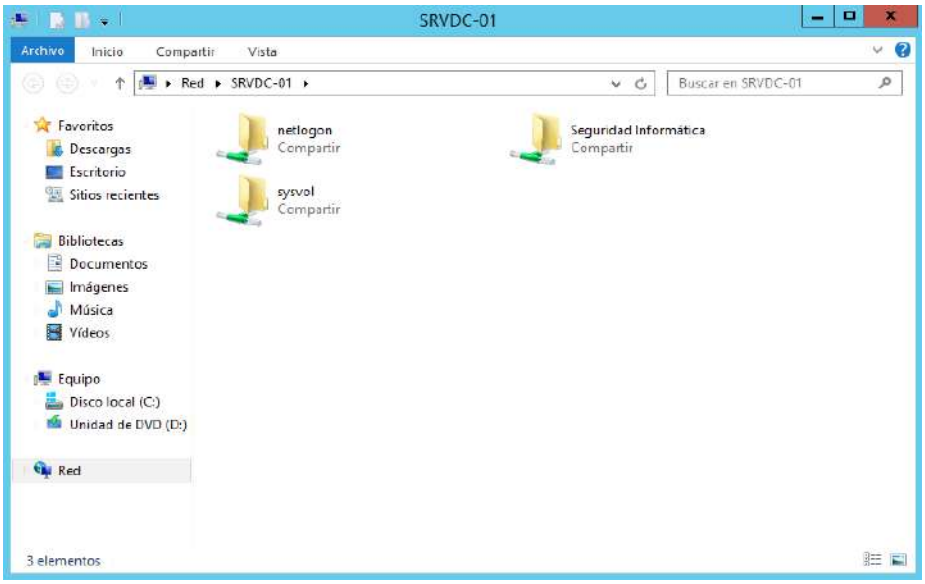


Figura 6. 11: Carpeta Compartida

9. Luego digitado el comando \\SRVDC-01 como se muestra la figura 6.11, abrimos y vemos los archivos que se creó, ver figura 6.12.

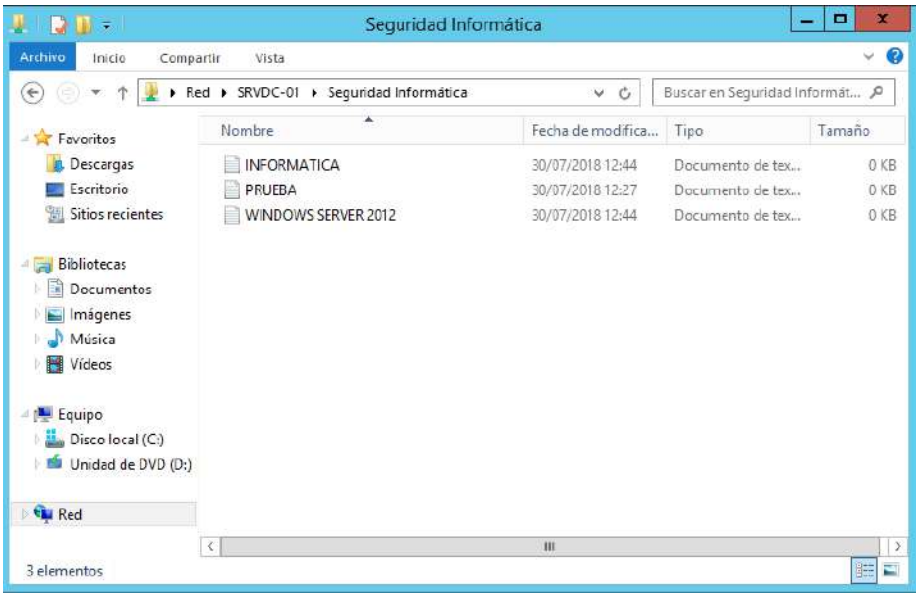


Figura 6. 12: Comprobando que se pueda acceder la carpeta

10. Para comprobar nos vamos al administrador de servidor, servidores de archivos y almacenamientos y dirigimos a recursos compartidos, ver figura 6.13.

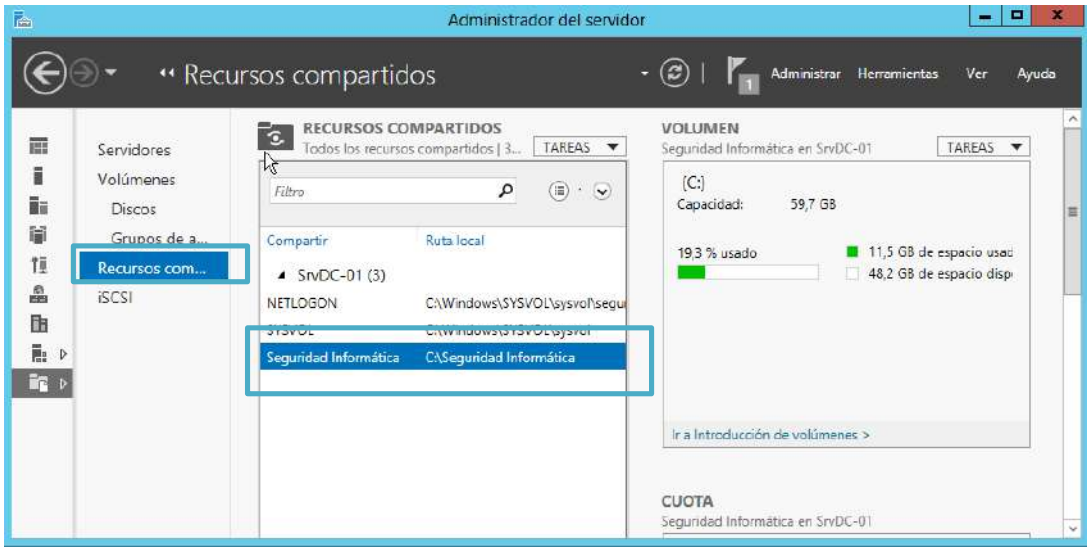


Figura 6. 13: Recursos Compartidos

6.4. Sistema de gestión de archivos DFS

Un sistema de archivos distribuido (de ahora en adelante DFS) es una forma de organización de archivos usando múltiples servidores de ficheros como destinos bajo un mismo alias o "Espacio de nombres" proporcionando además redundancia, mayor rendimiento y tolerancia a fallos.

El DFS permite especificar los horarios de sincronización/replicación y el ancho de banda máximo utilizable por la herramienta, de forma que se realice a las horas que menos incidencia tenga en el rendimiento general de la red (noches y/o fines de semana) o que realizándose en tiempo real se asigne una velocidad lo suficientemente controlada para no perjudicar a la navegación esperada por los usuarios. (Flores, 2015)

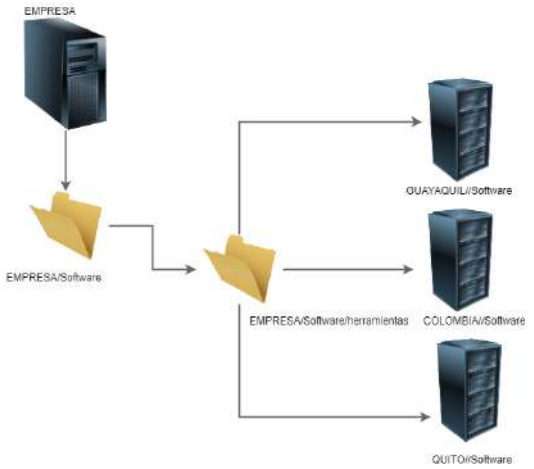


Figura 6. 14: DFS

Entonces podemos decir es un Sistema de Archivos Distribuidos (DFS - Distributed File System) es un servicio que permite a los usuarios el acceso transparente a sus datos sin necesidad de que conozcan el equipo exacto en el que se encuentran compartidos, y permitiendo tener esos datos replicados en diferentes equipos al mismo tiempo. Gracias a este servicio se consigue un sistema tolerante a fallos, gracias a la distribución de los servicios entre varios equipos. (Morales, 2013)

DFS es un servicio que se compone de dos tecnologías básicas:

- Espacio de Nombres (Name Spaces): Un Espacio de Nombres es un recurso de red que va a apuntar (o representar) de manera transparente a cualquiera de los equipos que pertenezcan a ese Espacio de Nombres, como si se tratara de un alias o acceso directo. De esta manera los usuarios accederán a ese recurso simbólico y no al nombre del equipo en sí. El sistema es el que elegirá realmente a qué equipo físicamente accede el usuario en ese momento.

- Replicación de Archivos: Mantiene el contenido de varias carpetas de manera idéntica entre diferentes equipos de la red.

Por tanto, uniendo ambas funcionalidades, el usuario accederá a su información de manera transparente, sin necesidad de saber a qué equipo realmente está accediendo. Del mismo modo, si cualquiera de los equipos implicados tuviera un problema y se encontrara inaccesible, los usuarios seguirían trabajando en cualquiera del resto de equipos incluidos en el Espacio de Nombres. (Morales, 2013)

6.4.1. El espacio de nombres

Espacios de nombres DFS es un servicio de rol de Windows Server que te permite agrupar las carpetas compartidas ubicadas en distintos servidores en uno o varios espacios de nombres estructurados lógicamente. Esto permite ofrecer a los usuarios una vista virtual de las carpetas compartidas, donde una única ruta de acceso conduce a los archivos ubicados en varios servidores, tal y como se muestra en la siguiente figura 6.15:

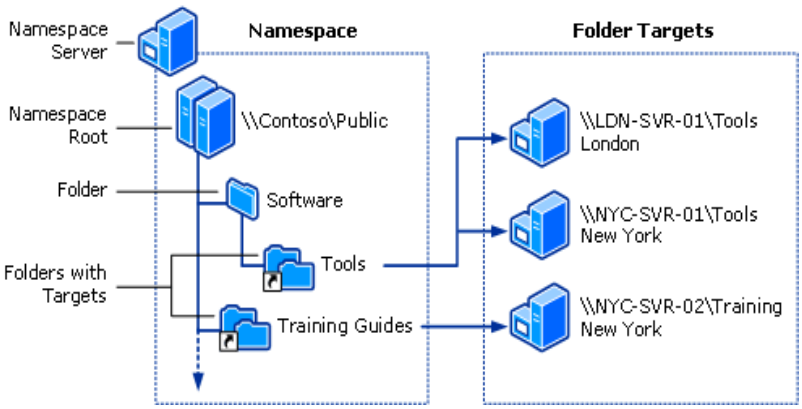


Figura 6. 15: Espacio de nombres DFS

Aquí se muestra una descripción de los elementos que componen un espacio de nombres DFS: (Microsoft, 2017)

- ✓ Servidor de espacio de nombres: Un servidor de espacio de nombres que aloja un espacio de nombre. El servidor de espacio de nombres puede ser un servidor miembro o un controlador de dominio.
- ✓ Raíz de espacio de nombres: La raíz de espacio de nombres es el punto inicial del espacio de nombres. En la figura anterior, el nombre de la raíz es público (Public) y la ruta de acceso del espacio de nombres es \\Contoso\Public. Este tipo de espacio de nombres es un espacio de nombres basado en dominio, ya que comienza con un nombre de dominio (por ejemplo, Contoso) y sus metadatos se almacenan en los Servicios de dominio de Active Directory (AD DS). Aunque en la figura anterior se muestra un único servidor de espacio de nombres, un espacio de nombres basado en dominio puede alojarse en varios servidores de espacio de nombres para aumentar la disponibilidad del espacio de nombres.
- ✓ Carpeta: Las carpetas sin destinos de carpeta agregan estructura y jerarquía al espacio de nombres y las carpetas con destinos de carpeta ofrecen a los usuarios contenido real. Cuando los usuarios exploran una carpeta que incluye los destinos de carpeta en el espacio de nombres, el equipo cliente recibe una referencia que redirige de forma transparente al equipo cliente a uno de los destinos de carpeta.
- ✓ Destinos de carpeta: Un destino de carpeta es la ruta de acceso de UNC de una carpeta compartida u otro espacio de nombres que está asociado a una carpeta de un espacio de nombres. El destino de carpeta es donde se almacenan los datos y el

contenido. En la figura anterior, la carpeta denominada Herramientas (Tools) tiene dos destinos de carpeta, uno en Londres (London) y otro en Nueva York (New York), y la carpeta denominada Guías de aprendizaje (Training Guides) tiene una sola carpeta de destino en Nueva York (New York). Un usuario que se desplaza a \\Contoso\Public\Software\Tools se redirige de forma transparente a la carpeta compartida \\LDN-SVR-01\Tools o \\NYC-SVR-01\Tools, en función del lugar en el que se encuentre actualmente el usuario.

6.4.2. Replicación de archivos

La Replicación asegura que el contenido de las carpetas DFS estará siempre disponible para los usuarios, puesto que son replicadas en otras carpetas compartidas de otro servidor del dominio. Replicar un espacio de nombres DFS garantiza la disponibilidad del sistema de archivos distribuido asociado con dicho espacio para los usuarios del dominio incluso si se cae el servidor de espacio de nombres del dominio.

Al replicar una carpeta DFS, se almacena una copia duplicada del contenido de la carpeta original en otra carpeta compartida. La replicación DFS utiliza un algoritmo de compresión denominado Compresión diferencial remota (RDC). RDC detecta los cambios en los datos de un archivo y permite que la replicación DFS replique solo los bloques de archivo modificados en lugar del archivo completo. (Massón, 2018)

Para utilizar la replicación DFS se deben crear grupos de replicación y agregar carpetas replicadas a dichos grupos. Un grupo de replicación es un conjunto de servidores, llamados miembros, que participan en la replicación de una o más carpetas replicadas. Las carpetas replicadas se mantienen sincronizadas entre los miembros. Cuando cambian los datos en una carpeta replicada, estos se replican a través de las conexiones entre los miembros del grupo de replicación. Las conexiones entre todos los miembros conforman la topología de la replicación.

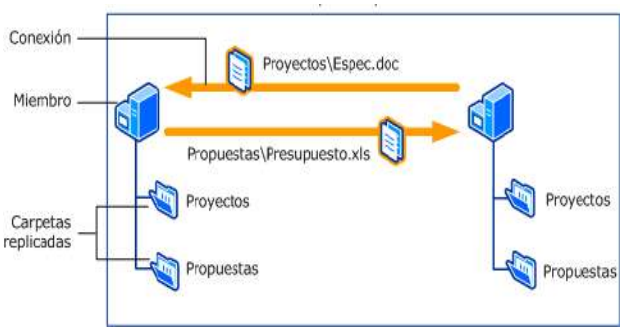


Figura 6. 16: Grupo de replicación DFS

Cuando agregamos varias carpetas replicadas a un grupo de replicación el proceso de implementación de las réplicas se simplifica ya que la topología, la programación y el límite del ancho de banda del grupo se aplican a cada una de las carpetas del grupo (ver figura 6.16).

Además cada carpeta replicada también tiene una configuración única de manera que se pueden filtrar distintos archivos y subcarpetas para cada carpeta. (Massón, 2018)

6.5. Uso de informes

En el nodo Administración de informes de almacenamiento del Complemento de la consola de administración de Microsoft® (MMC) del Administrador de recursos del servidor de archivos, puedes realizar las siguientes tareas: (Microsoft, 2017)

- ✓ Programar informes de almacenamiento periódicos que te permiten identificar tendencias de uso del disco.
- ✓ Supervisar intentos de guardar archivos no autorizados de todos los usuarios o un grupo seleccionado de usuarios.
- ✓ Generar informes de almacenamiento al instante.

Por ejemplo, puedes:

- ✓ Programar un informe para que se ejecute todos los domingos a medianoche y hacer que se genere una lista que incluya los archivos a los que se ha obtenido acceso más recientemente en los dos últimos días.
- ✓ Ejecutar un informe en cualquier momento para identificar todos los archivos duplicados en un volumen de un servidor para que el

espacio de disco pueda recuperarse rápidamente sin perder ningún dato.

- ✓ Ejecutar un informe Archivos por grupo de archivos para identificar cómo los recursos de almacenamiento se segmentan en distintos grupos de archivos.
- ✓ Ejecutar un informe Archivos por propietario para analizar cómo los usuarios individuales usan los recursos de almacenamiento compartidos. (Microsoft, 2017)

Bibliografía

Alegsa, L. (05 de Diciembre de 2010). Definición de NTFS. Obtenido de http://www.alegsa.com.ar/Dic/ntfs.php

EcurRed. (s.f.). NTFS. Recuperado el 20 de Junio de 2018, de https://www.ecured.cu/NTFS

Flores, J. (06 de Noviembre de 2015). DFS: sistema de archivos distribuido. Obtenido de http://www.irix.es/blog/dfs-sistema-de-archivos-distribuido/

Guzman, L. (Noviembre de 2012). Rol de servidor de archivos. Obtenido de Windows Server 2012 - Las bases imprescindibles para administrar y configurar su servidor: https://www.ediciones-eni.com/open/mediabook.aspx?idR=065a654496f1b39947d4c298321b4796

Levine, B. (Agosto de 2017). Introducción a NTFS. Obtenido de https://people.cs.umass.edu/~liberato/courses/2017-spring-compsci365/lecture-notes/13-introduction-to-ntfs/

Massón, J. A. (13 de Marzo de 2018). Sistema de Archivos Distribuido (DFS). Obtenido de http://www.asirlasgalletas.com/2018/03/xiii-sistema-de-archivos-distribuido-dfs.html

Mena, L. (07 de Octubre de 2016). Servidor de Archivos en Windows Server 2012. Obtenido de https://prezi.com/ex-c-jy16vnm/servidor-de-archivos-en-windows-server-2012/

Microsoft. (07 de Julio de 2017). Administración de informes de almacenamiento. Obtenido de https://docs.microsoft.com/es-es/windows-server/storage/fsrm/storage-reports-management

Microsoft. (10 de Julio de 2017). Información general de Espacios de nombres DFS. Obtenido de https://docs.microsoft.com/es-es/windows-server/storage/dfs-namespaces/dfs-overview

Morales, R. (30 de Abril de configurar el Espacio de Nombres y la Replic ivos (DFS). Obtenido de http://www.ticarte.com/contenido/como-configurar-el-espacio-de-nombres-y-la-replicacion-de-archivos-dfs

OrjaLes, T. (12 de Diciembre de 2012). Sistemas de gestion de archivos. Obtenido de http://sistemasoperativos03-unefa.blogspot.com/2011/12/normal-0-21-false-false-false-es-ve-x.html

Salazar, A. (03 de Noviembre de 2012). Seguridad en los sistemas de archivos. Obtenido de https://es.slideshare.net/asalazar29/seguridad-en-los-sistemas-de-archivos?from_action=save

Sánchez, J. (15 de Noviembre de 2012). Carpetas: seguridad, acceso y replicación. Obtenido de https://blogs.msmvps.com/juansa/blog/2011/09/15/carpetas-seguridad-acceso-y-replicacin/

Unidad

VII

Unidad VII

GPO Directivas de Grupo

7. Introducción

GPO, por sus siglas en inglés "Group Policy Object", que significa "Grupo de políticas para un objeto", es quien permite la edición de un grupo de políticas que se le aplicaran a un objeto u objetos en particular.

Una GPO se enlaza con un contenedor, es decir, que se debe crear dos GPO, una para el contenedor de los usuarios, donde solo se editará y se aplicará políticas específicas para los usuarios. Se creará una segunda GPO para el contenedor de las máquinas, donde se editará y se aplicará políticas exclusivas de máquina. (Calzaretta, 2013)

Un GPO permite implementar configuraciones específicas para uno o varios usuarios y/o equipos. Nos centraremos en cómo se debe hacer la gestión correcta de GPO en Active Directory de Microsoft Windows. Para la configuración de GPO que sólo afecten a un usuario o equipo local se puede utilizar el editor de directivas locales gpedit.msc. En nuestro caso accederemos en el entorno de Servicios de Dominio de Active Directory, con la consola de administración gpmc.msc.

Las GPO permiten administrar objetos de usuarios y equipos, aplicando la más restrictiva en caso de existir más de una política. Se puede usar una GPO para casi cualquier cosa, como indicar qué usuario o grupo tiene acceso a una unidad de disco, o limitar el tamaño máximo que puede tener un archivo.

Las GPO se pueden diferenciar dependiendo del objeto al que configuran y se pueden entender en distintos niveles:

- ✓ Equipo Local: tan solo se aplican en el equipo que las tiene asignadas independientemente del dominio al que pertenezca.
- ✓ Sitio: se aplican a los equipos y/o usuarios de un sitio, independientemente del dominio.
- ✓ Dominio: se aplican a todos los equipos y/o usuarios de un dominio.
- ✓ Unidad Organizativa (OU): se aplican únicamente a los equipos y/o usuarios que pertenecen a la OU.

7.2. Implementando directivas de grupo

Para la configuración debemos ir al administrador de servicios y damos clic en herramienta luego en administración de directivas de grupos, como se muestra la figura 7.1

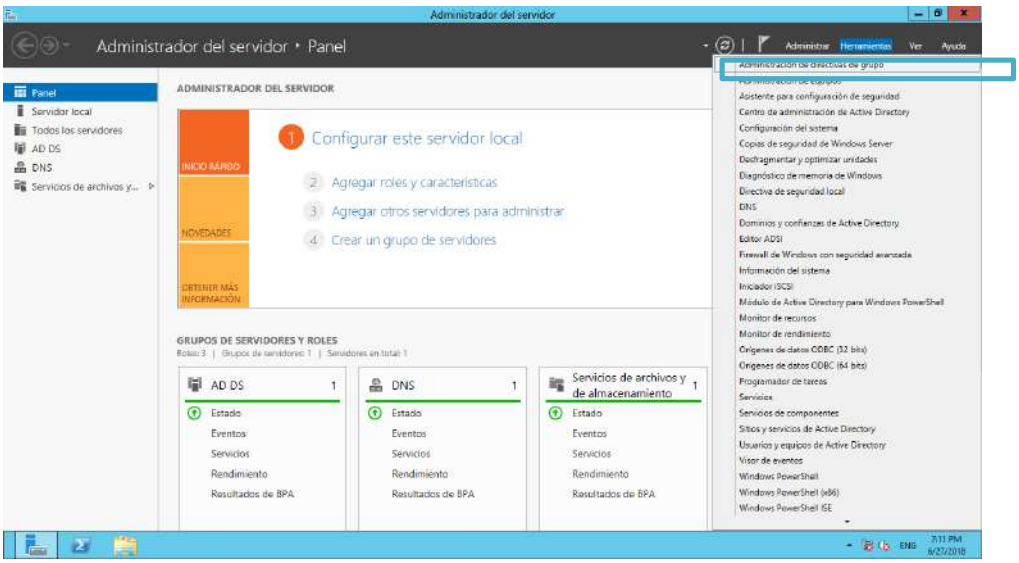


Figura 7. 1: Administrador del servidor

Nos abrirá la ventana de administración de directivas de grupo donde observaremos el árbol del controlador de dominio, ver figura 7.2.

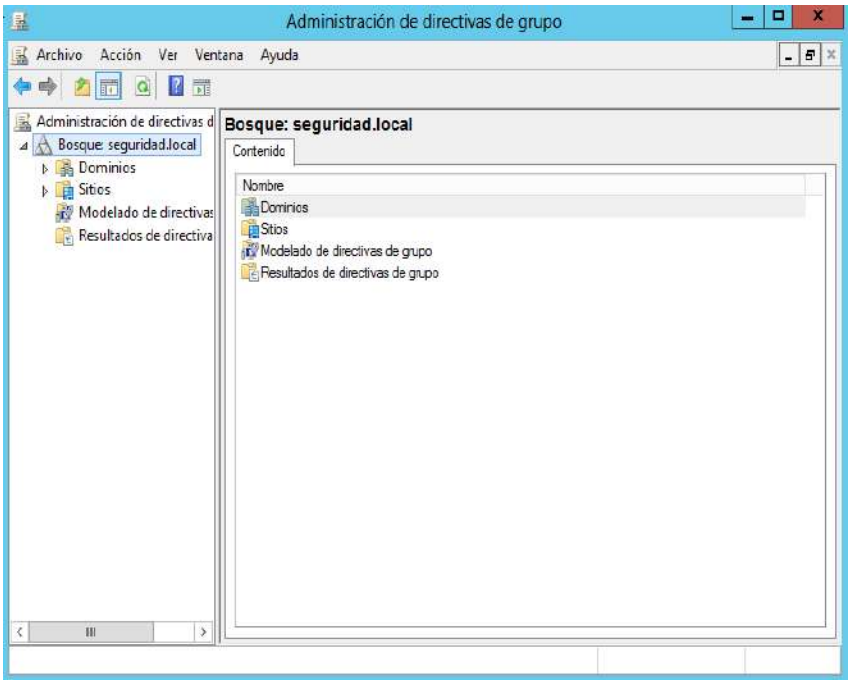


Figura 7. 2: Administración del directivo de grupo

Podemos ver que por defecto se crean dos directivas de grupo, ver figura 7.3.

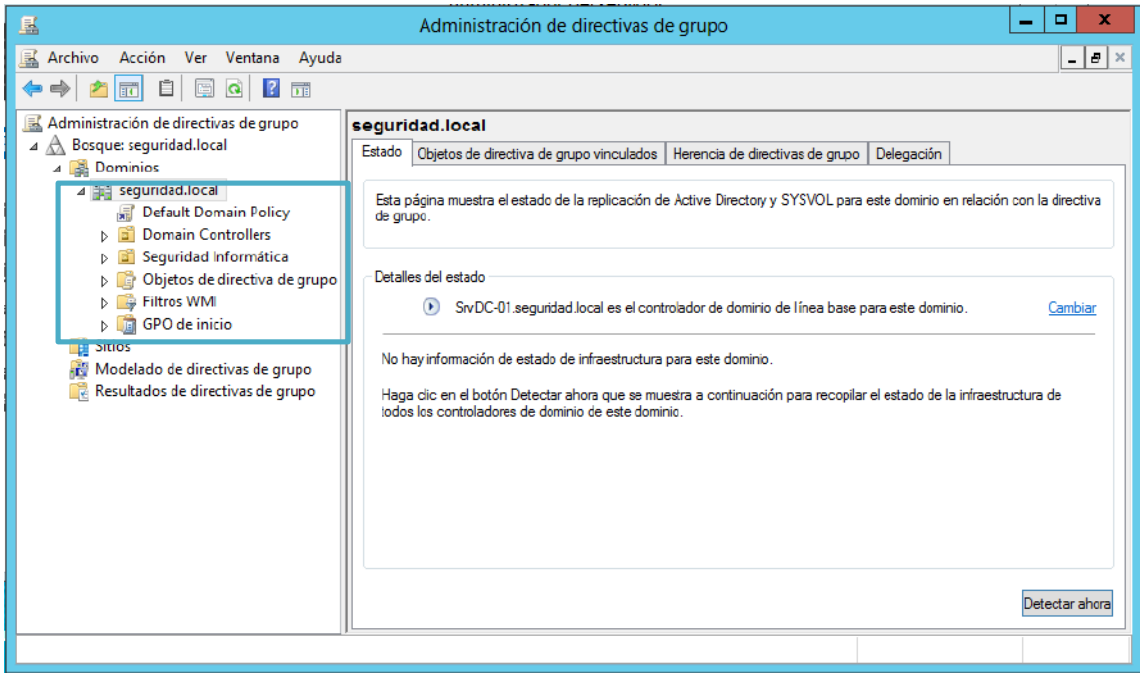


Figura 7. 3: Directivas del grupo

Para poder administrar las directivas damos clic en ella y nos abrirá otra ventana que nos pide autorización para abrir la consola de administración, tal como muestra la figura 7.4

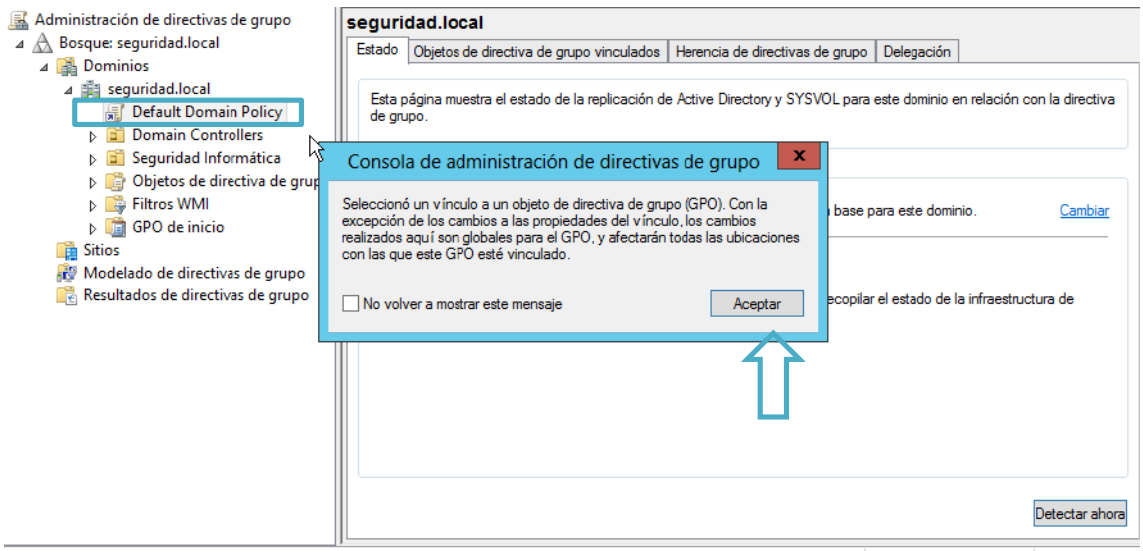


Figura 7. 4: Consola administrativa del grupo

Luego nos mostrara sus opciones de configuración ver figura 7.5 y 7.6.

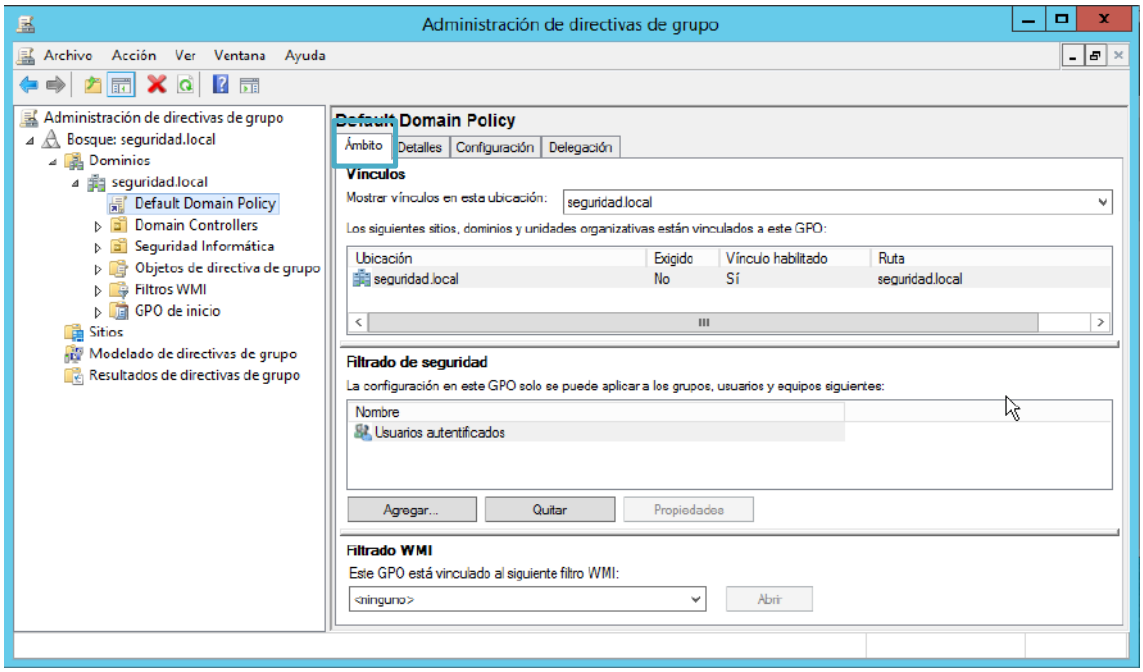


Figura 7. 5: Ámbito Política

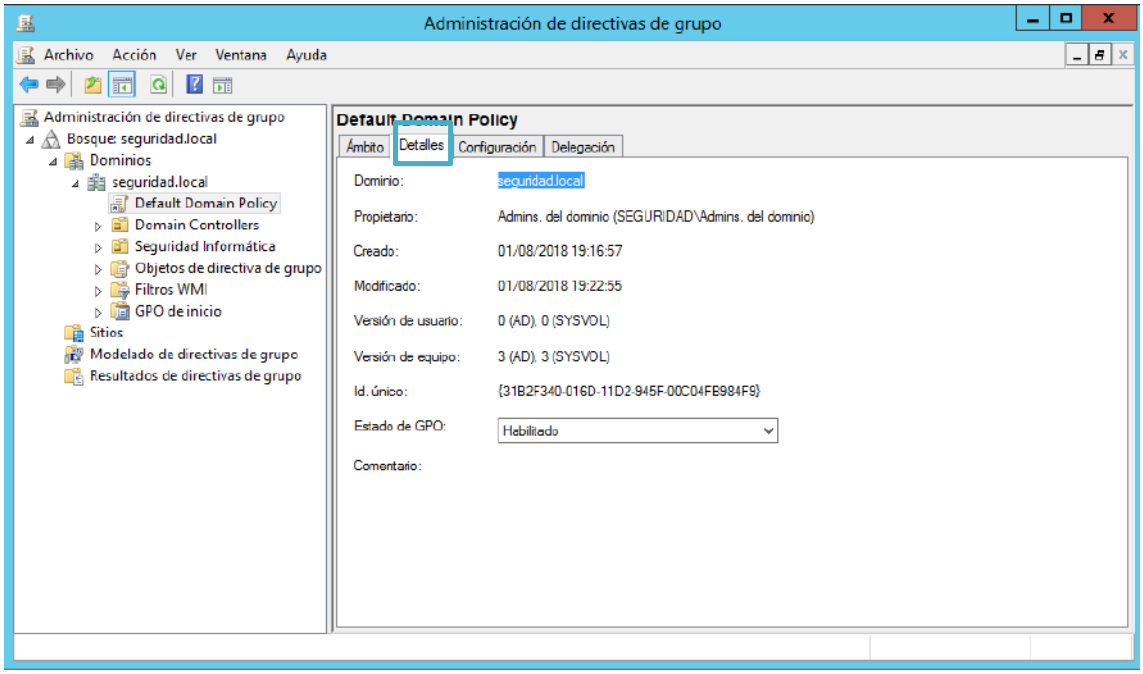


Figura 7. 6: Detalles de Política

En la opción de configuración en la que debemos agregar para poder obtener las configuraciones, ver figura 7.7.

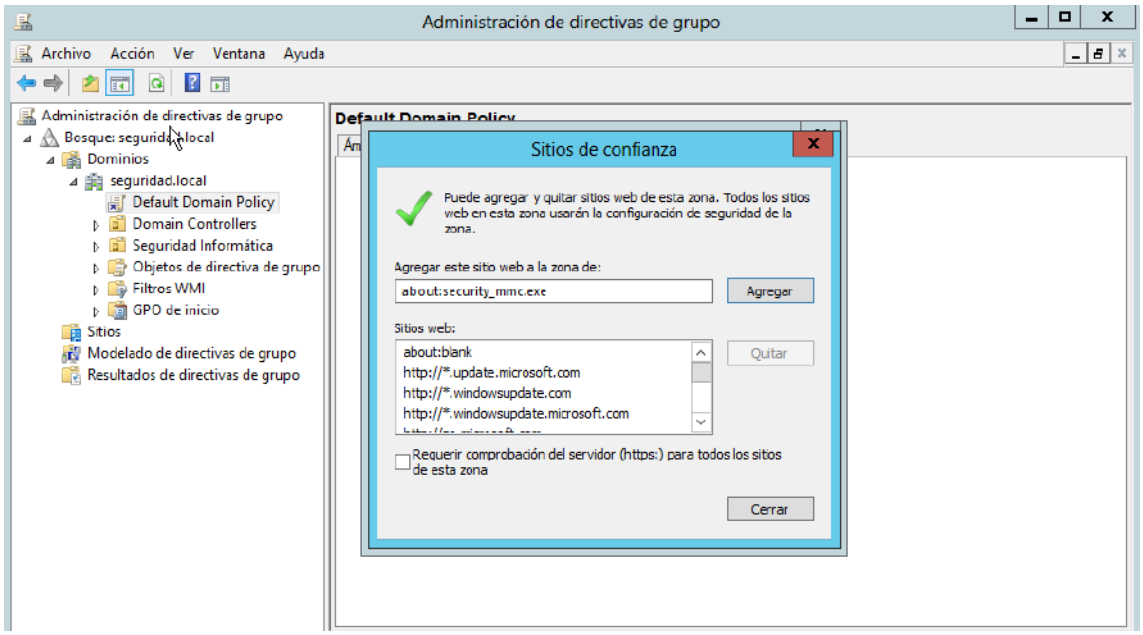


Figura 7. 7: Sitios de Confianza

En esta opción me muestra las configuraciones que hemos realizados, ver figura 7.8

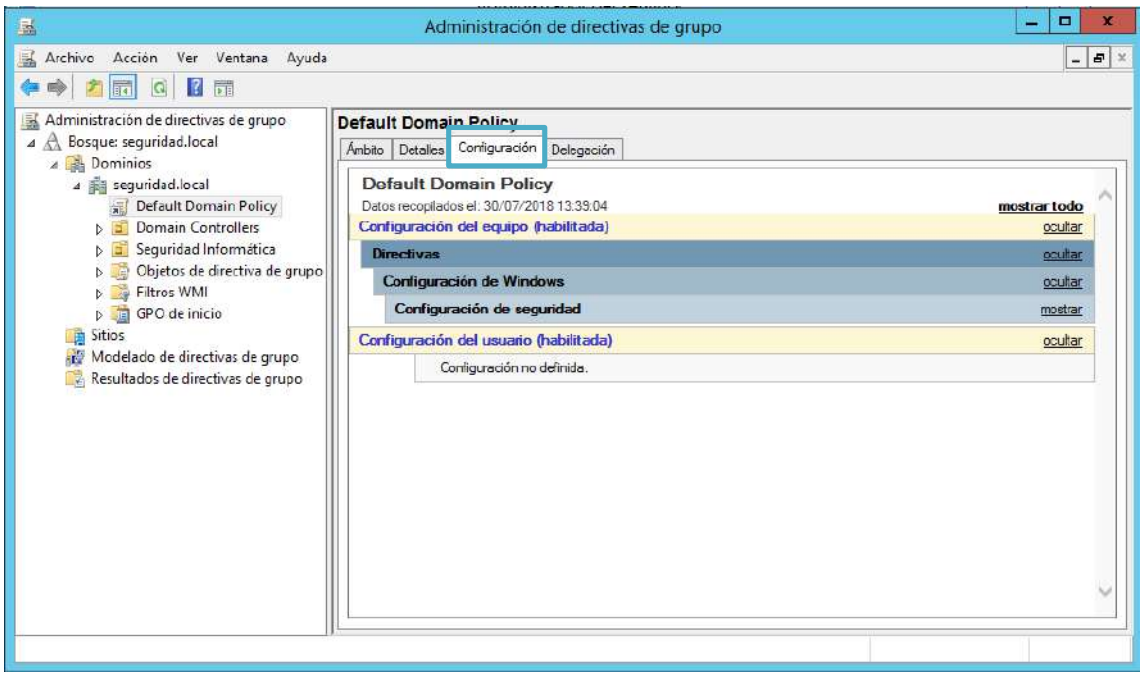


Figura 7. 8: Configuración de GPO

En esta opción me muestra las delegaciones de las directivas del grupo que vamos a realizar, ver figura 7.9.

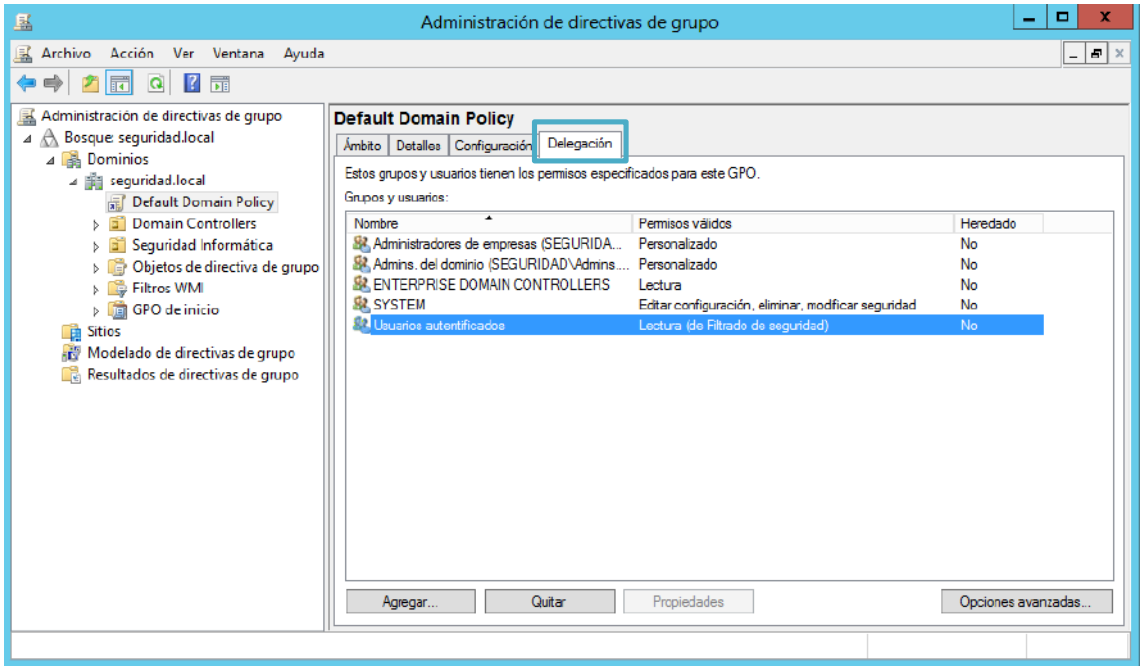


Figura 7. 9: Delegación GPO

7.3. Gestión de directivas de grupo

7.3.1. Creación de una GPO

1. Dentro de Administrador del servidor seleccionar Herramientas y Administración de directivas de grupo, ver figura 7.10: (Pajuelo, 2014)

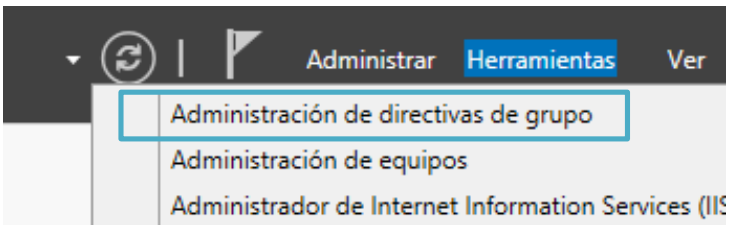


Figura 7. 10: Administración de directivas del grupo

2. Aparecen las GPO del dominio.

3. Para crear una nueva GPO desde cero, pulsar en Objetos de directiva de grupo con el botón derecho y seleccionar Nuevo, ver figura 7.11:

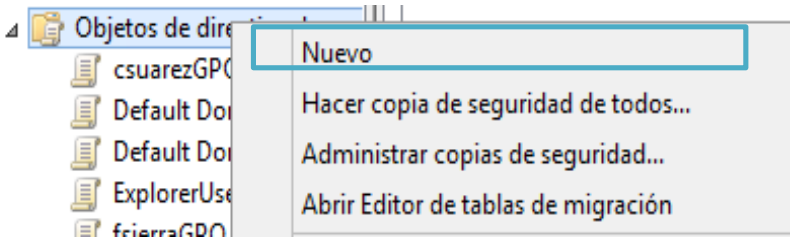


Figura 7. 11: Crear nuevo GPO

4. No seleccionar ninguna GPO de origen. Pulsar Aceptar, ver figura 7.12:

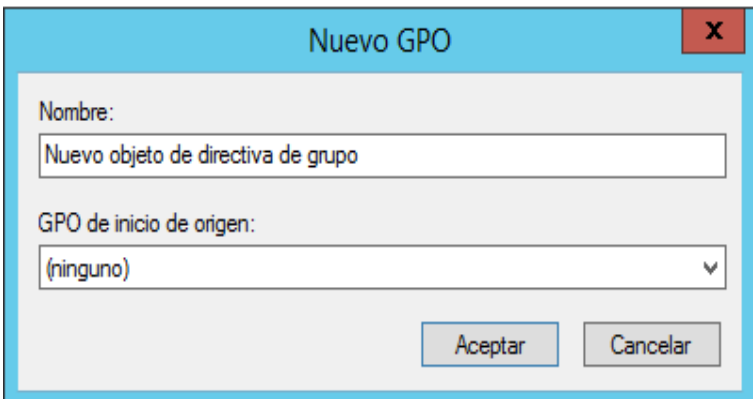


Figura 7. 12: Nuevo GPO

5. Pulsar sobre la nueva GPO con el botón derecho y seleccionar Editar, ver figura 7.13.

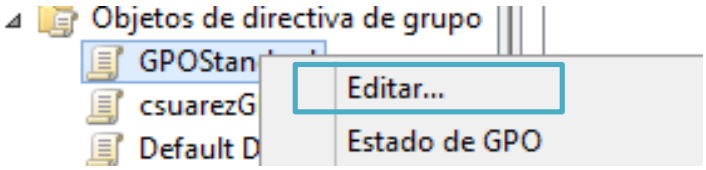


Figura 7. 13: Editar GPO

Una vez dentro de la edición de la GPO hay que asignar la unidad de red que los usuarios deben montar, siguiendo las políticas adecuadas. (Pajuelo, 2014)

1. Navegar a Configuración del usuario, Preferencias, Configuración de Windows, Asignaciones de Unidades y editar la unidad que viene asignada en la GPO pulsando sobre ella con el botón derecho y seleccionar Propiedades, como se muestra la figura 7.14:

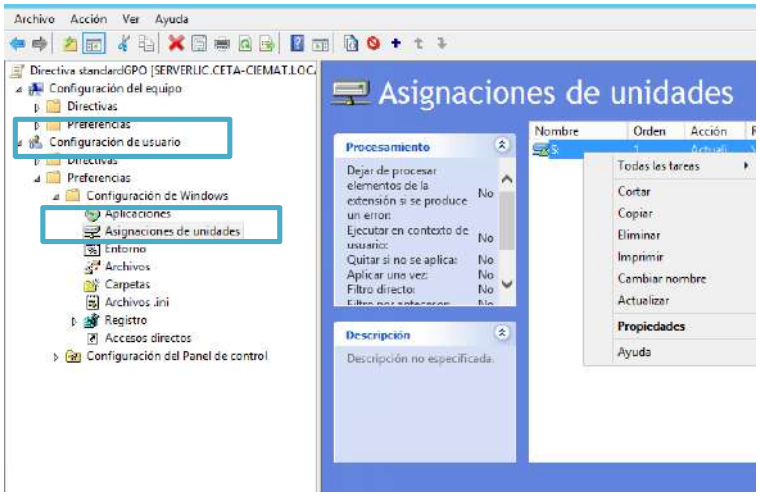


Figura 7. 14: Asignaciones de unidades

2. Seleccionar la ubicación, el nombre con el que se quiere mostrar la unidad, la letra que se le asignará y el usuario que se conectará (ver figura 7.15):

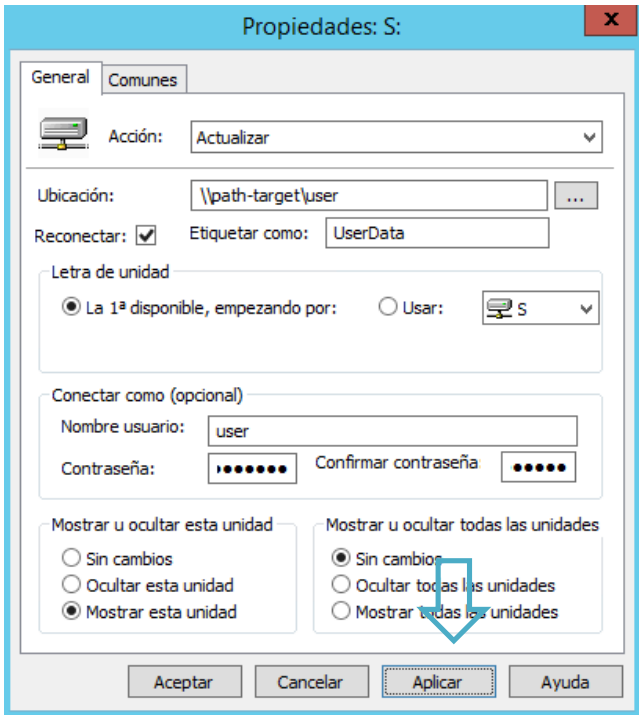


Figura 7. 15: Ubicación de la unidad

7.4. Plantillas administrativas

En esta ocasión vamos a ver la forma sencilla de cómo podemos agregar estas nuevas plantillas de office para las políticas de grupo y a su vez el link de enlace de la descripción de cada una de ellas.

1. Debemos hacer es descargar las plantillas.

2. Los archivos descargados van a alojar 2 carpetas la que nos interesa es la ADMX (ver figura 7.16)

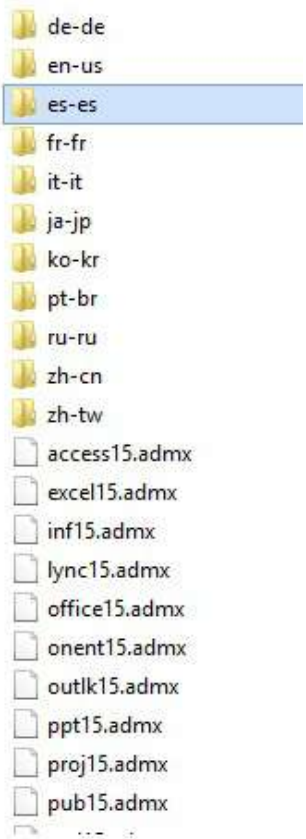


Figura 7. 16: Plantillas administrativas

3. Los archivos ADMX los vamos a copiar en la siguiente ruta C:\Windows\PolicyDefinitions y los archivos ADML se colocarán dentro de las carpetas correspondientes al lenguaje EN-US, ES-ES dependiendo el caso.

\ADMX: la carpeta ADMX contiene versiones basadas en XML (archivos .admx o. adml) de los archivos de plantilla administrativa para

Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2.

Los archivos de plantilla administrativa se dividen en archivos ADMX (independiente del idioma) y ADML (específicos del idioma). De manera predeterminada, la carpeta %systemroot%\PolicyDefinitions de un equipo local almacena todos los archivos ADMX, mientras que los archivos ADML lo hacen en carpetas específicas del idioma dentro de la carpeta %systemroot%\PolicyDefinitions. Cada subcarpeta de idioma contiene los archivos. adml para ese idioma. Así, por ejemplo, los archivos ADML del idioma inglés se almacenarían en la carpeta. (Santiago, 2014)

%systemroot%\PolicyDefinitions\en-us. Se incluyen los siguientes idiomas: chino simplificado (República Popular China), chino (Hong Kong RAE), inglés, francés, alemán, italiano, japonés, coreano, portugués (Brasil), ruso y español. Los archivos que se almacenan en la carpeta \ADMX son: (ver figura 7.17)

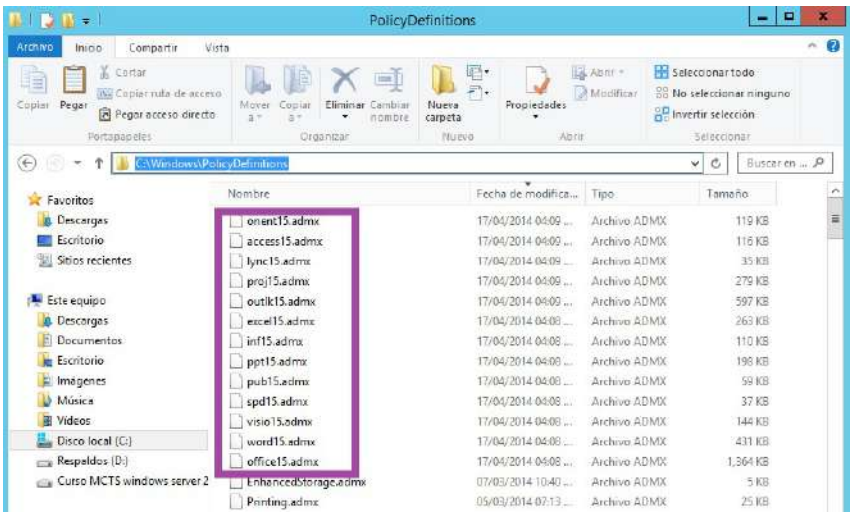


Figura 7. 17: Extensiones admx

Ahora en directivas de grupo vemos las nuevas características instaladas.(ver figura 7.18)

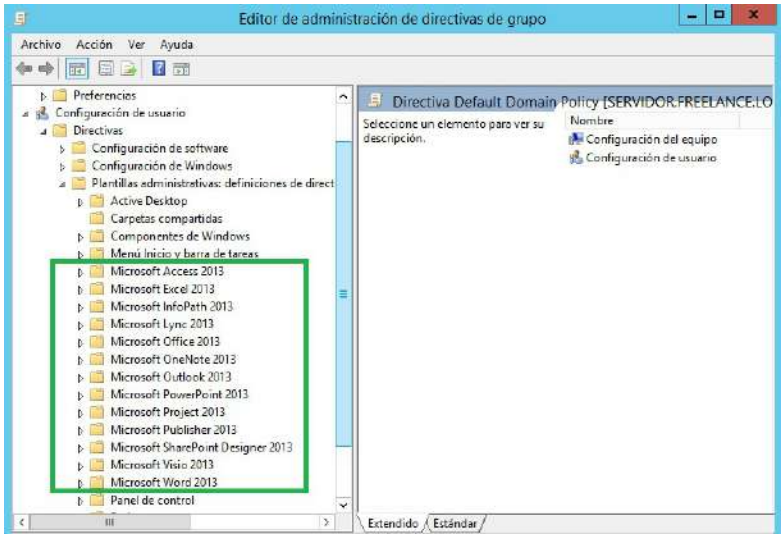


Figura 7. 18: Editor de administración de directivas de grupo

7.5. Uso de la herramienta GPOTool

GPOTool.exe es una herramienta con interfaz de usuario por la línea de comandos en Windows Server 2008 y 2008 R2. Esta aplicación está prevista para emplearse internamente en los entornos de dominio Windows que contengan más de un controlador de dominio, y en los que la replicación Active Directory esté activa. El papel de esta herramienta es el de determinar la validez de la sincronización entre los objetos GPC y GPT asociados a las directivas de grupo. Esta herramienta, que permite realizar la verificación de una directiva de grupo, está disponible desde Windows 2000. La coherencia de las GPO (entre los contenedores GPC y GPT) puede comprobarse, a su vez, mediante esta herramienta. Se trata de una herramienta gratuita que puede descargarse con las Resource Kit Tools para Windows Server 2003 en la URL: http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=17657. No obstante, si el sistema operativo ejecutado es Windows Server 2008/2012/2012 R2, es posible descargar el ejecutable por la línea de comandos visitando directamente el blog personal del autor (en francés): http://www.nibonnet.fr/?p=272 (Sánchez, 2013)

Se han incluido los nuevos archivos.
Descargue el ejecutable y cópielo en la raíz de la partición C.
Abra una ventana de comandos DOS y, a continuación, escriba cd \.
La instrucción permite seleccionar la raíz de la partición, escriba el comando gpotool ad1 /verbose.

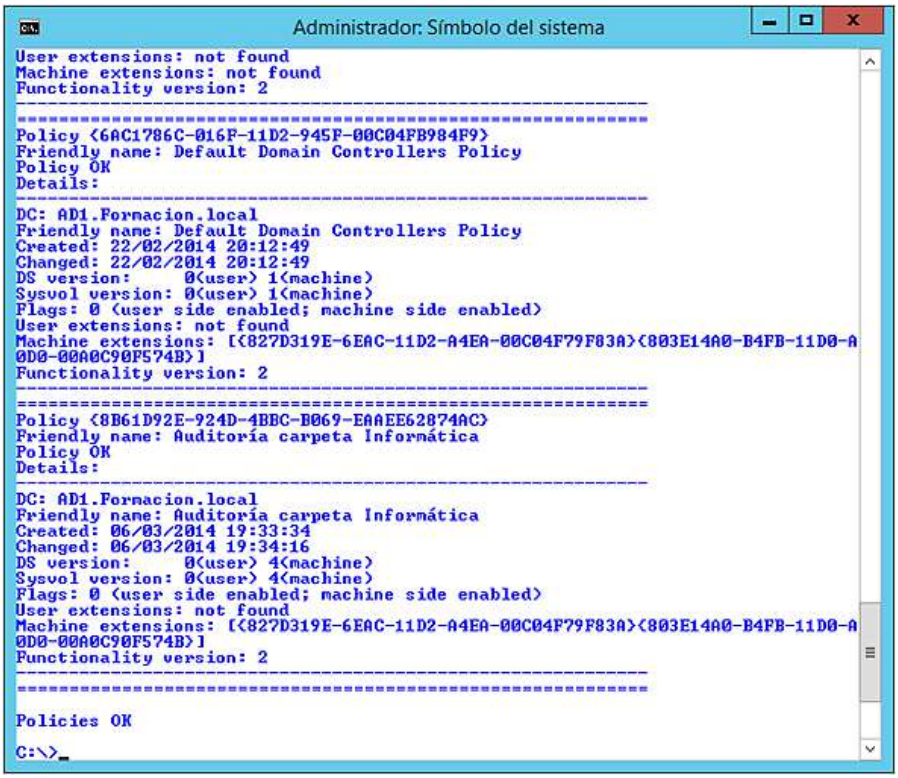


Figura 7. 19: Administrador símbolo del sistema

Es, por lo tanto, fácil comprobar un posible problema de replicación. Si este último presentara algún problema, sería preciso utilizar los registros de eventos. (Sánchez, 2013)

Bibliografía

Calzaretta, J. (Mayo de 2013). Plataformas de servidor de Windows: introducción a la política de grupo. Obtenido de http://kb.mit.edu/confluence/display/istcontrib/Windows+Server+Platforms+-+Introduction+to+Group+Policy

Pajuelo, F. (10 de Diciembre de 2014). Directivas de Grupo (GPO) en Windows Server 2012. Obtenido de https://cetatech.ceta-ciemat.es/2014/12/directivas-de-grupo-gpo-en-windows-server-2012/

Sánchez, J. (Febrero de 2013). Uso de la herramienta GPOTool. Obtenido de Windows Server 2012 R2 - Las bases imprescindibles, administrar, configurar su servidor: https://www.ediciones-

eni.com/open/mediabook.aspx?idR=7980efd7ca29b0596574698902c61681

Santiago, J. O. (11 de Mayo de 2014). Plantillas administrativas. Obtenido de INSTALACIÓN DE LAS PLANTILLAS ADMINISTRATIVAS (ADMX/ADML) DE OFFICE: https://blogseti.wordpress.com/2016/10/27/plantillas-administrativas-de-office-2016-y-gpos/

Unidad

VIII

Unidad VIII

Política de Seguridad Implementando GPO

8. Introducción

Las políticas de grupo son colecciones de configuraciones de usuario y configuración de computadora que pueden vincularse a computadoras, sitios, dominios y unidades organizativas (OU) para especificar el comportamiento de los escritorios de los usuarios. Por ejemplo, al usar políticas de grupo, puede especificar los programas que están disponibles para los usuarios, los programas que aparecen en el escritorio del usuario y las opciones del menú Inicio. (Calzaretta, 2013)

8.1. Pasos para configurar las GPO

1. Estando en el Administrador del Servidor se procede ir al menú Herramientas y se escoge la opción Administración de directivas de grupo. Una vez abierta la herramienta se ubica el bosque seguridad.local, luego el dominio seguridad.local y por último, la unidad organizativa Empresa de Seguridad. Como se observa en la Figura 8.1.

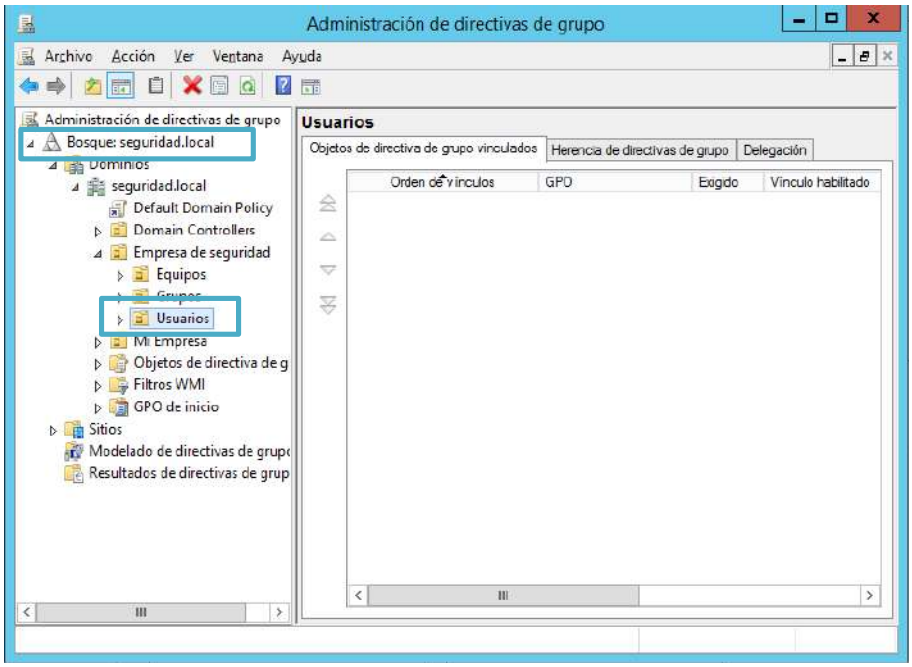


Figura 8. 1: Vista de la herramienta Administración de directivas de grupo

¿Sabías Qué?

2. Se creará dos GPO: Una para los equipos y una para los usuarios.

   a) Se creará la GPO para los usuarios. Estando dentro de la carpeta Empresa de seguridad, se procede ir a la subcarpeta Usuarios, se hace clic derecho y se escoge la opción Crear un GPO en este dominio y vincularlo aquí. Como se observa en la Figura 8.2.

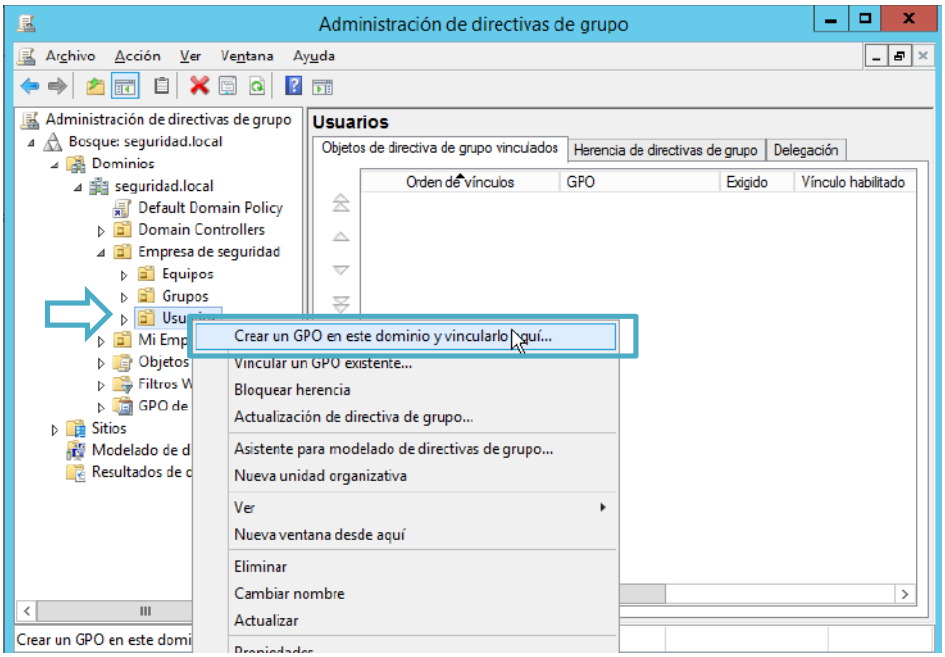


Figura 8. 2: Creación de la GPO para los usuarios Parte 1

Se le asigna un nombre a la nueva GPO. Se llamará Políticas de usuario. Observar Figura 8.3.

Una GPO puede contener una o más configuraciones; un contenedor puede tener enlazadas ninguna o varias GPO; y una GPO puede estar enlazada a más de un contenedor sin importar su clase. Lo anterior es la consecuencia de la existencia como objeto independiente que tienen las GPO.

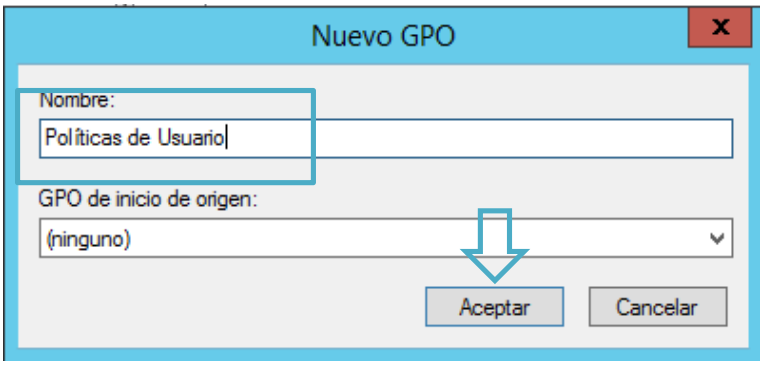


Figura 8. 3: Creación de la GPO para los usuarios Parte 2

b) Se creará la GPO para los equipos. Estando dentro de la carpeta Empresa de seguridad, se procede ir a la subcarpeta Equipos, se hace clic derecho y se escoge la opción Crear un GPO en este dominio y vincularlo aquí. Luego se le da el siguiente nombre: Políticas de Equipos. Como se observa en la Figura 8.4.

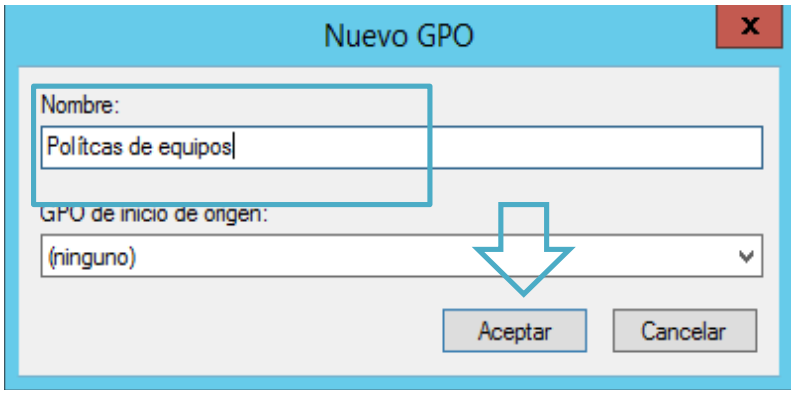


Figura 8. 4: Creación de la GPO para los usuarios

3. En este punto se crearán varias políticas para el usuario.

a) Los usuarios solo pueden iniciar sesión desde las 8 am hasta las 5 pm.
Esta política se la puede crear directamente desde las cuentas creadas. No necesitan del editor de administración de directivas de grupo. Para esto se debe ir a Herramientas y abrir Usuarios y equipos de Active Directory. Estando allí se procede a ubicar la unidad organizativa Empresa de Seguridad y la subcarpeta Usuarios. Luego se ubica el o los usuarios a los cuales se les aplicará esta política. Como se observa en la Figura 8.5.

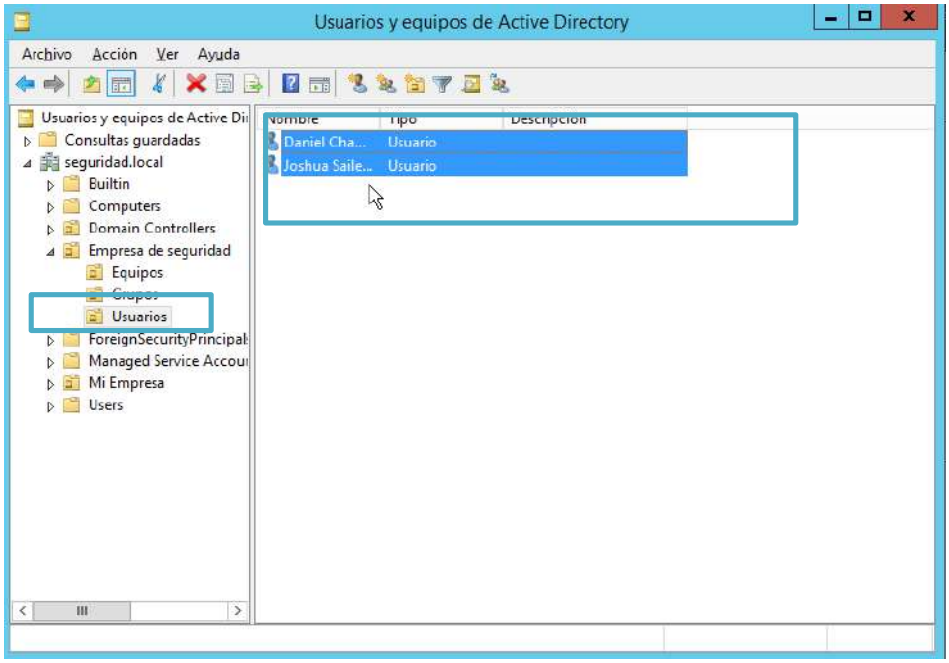


Figura 8. 5: Usuarios y equipos de Active Directory

Como se vio en la figura, se debe seleccionar los usuarios a los cuales se les configurará las horas que pueden iniciar sesión. Para esto se da clic derecho en la selección y se da clic en Propiedades. Luego se debe ubicar la pestaña Cuenta. Después se marcará el check de Horas de sesión y se hace clic en el botón Horas de sesión. Como se observa en la Figura 8.6.

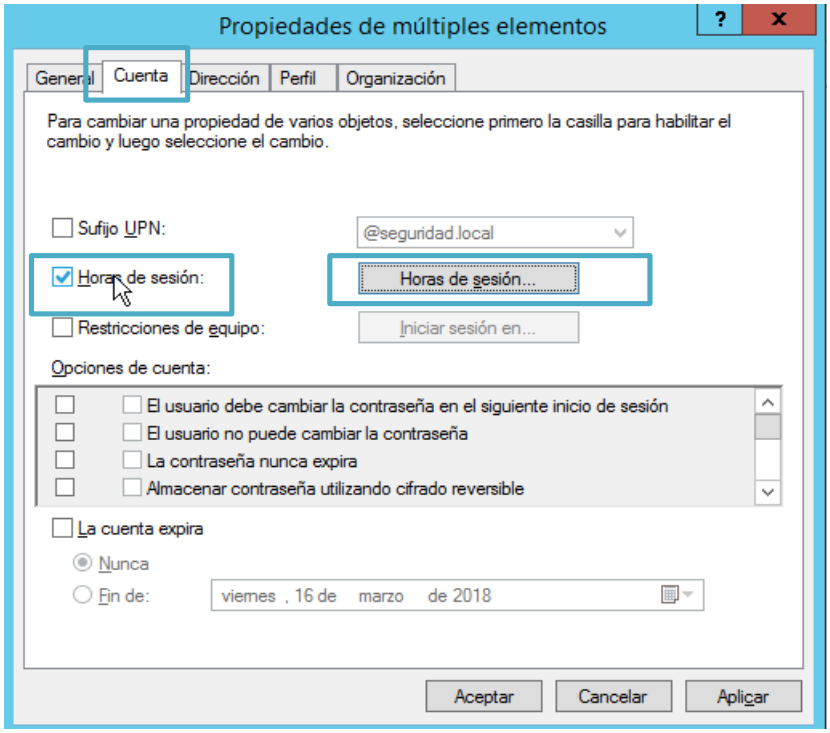


Figura 8. 6: Propiedades de múltiples elementos

En esta parte se debe seleccionar las horas que se le denegarán al usuario para que no pueda iniciar sesión. Es decir, solo se debe seleccionar las horas permitidas para que pueda iniciar sesión. (De 8 am a 5 pm), hacer clic en aceptar. Como se observa en la Figura 8.7.

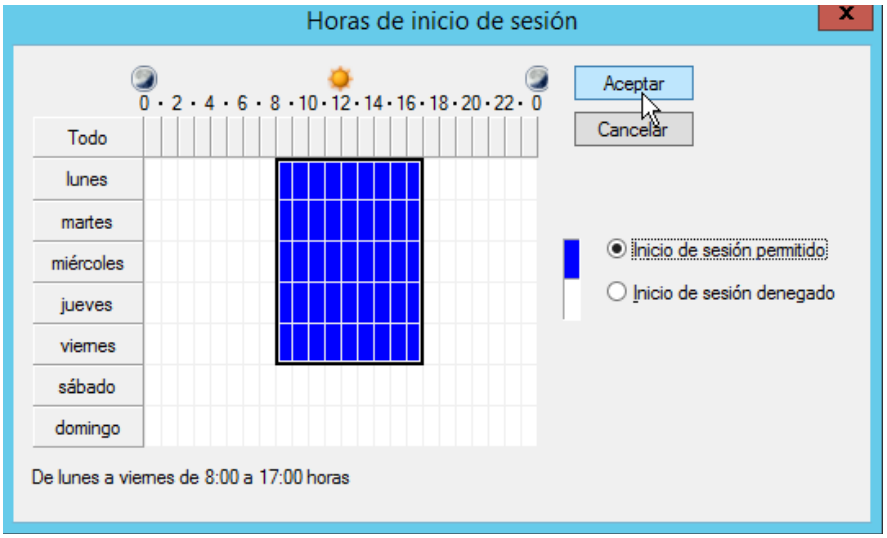


Figura 8. 7: Horario de inicio de sesión

Se puede comprobar si funciona la política. A las 2 am aproximadamente se intentó iniciar sesión y este fue el resultado. Como se observa en la Figura 8.8.

Figura 8. 8: Intento de inicio de sesión en una hora no permitida

b) Los usuarios no deben tener acceso al panel de control

Para esto se procede ir a la siguiente ruta: Administrador del servidor → Herramientas → Administración de directivas de grupo → Bosque: seguridad.local → Dominios → seguridad.local → Empresa de seguridad → Usuarios → Políticas de usuario. Se da clic derecho y se escoge la opción editar. Como se observa en la Figura 8.9.

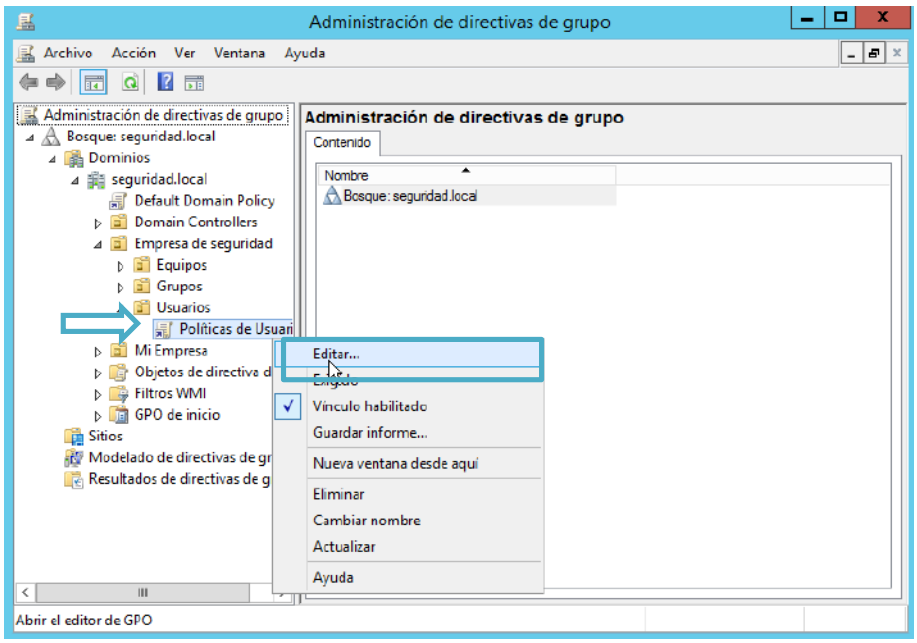


Figura 8. 9: Abrir el editor de administración de directivas del grupo

Se abre el editor de administración de directivas de grupo. Aquí se debe ir a la siguiente ruta: Configuración de usuario → Directivas → Plantillas administrativas → Panel de Control. De lado derecho se mostrará algunas políticas en cuanto al panel de control. Se selecciona la política

que dice: Prohibir el acceso a Configuración de PC y a Panel de Control. Clic derecho y clic en editar. Como se observa en la Figura 8.10.

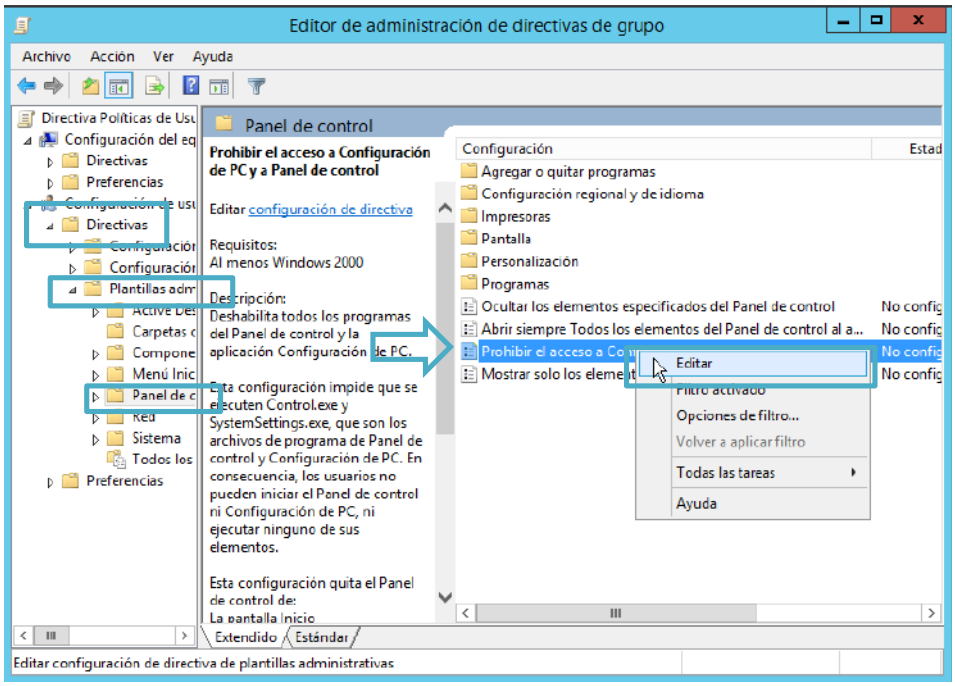


Figura 8. 10: Ubicación de la directiva a editar

Luego se debe habilitar dicha directiva y, por último, clic en aplicar y aceptar. Como se observa en la Figura 8.11.

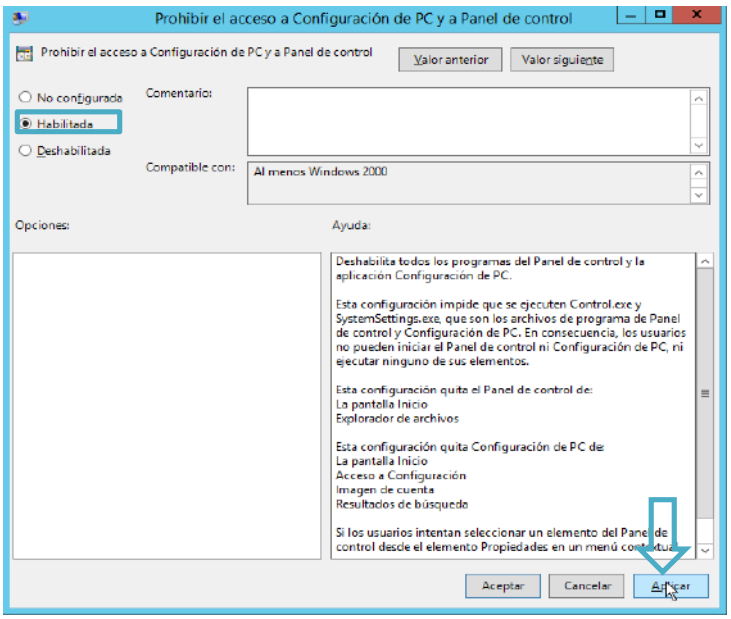


Figura 8. 11: Configuración de la directiva

c) Debe usarse el papel tapiz de la empresa. No puede cambiarse

Para esta política se tiene dos maneras de realizarla: guardando la imagen en el servidor o guardando la imagen en el cliente. En este caso se la guardará en el servidor.

Como primer paso se debe guardar la imagen logo.png en la carpeta Logo que está dentro del disco local C del servidor SrvDC-01. Como se observa en la Figura 8.12.

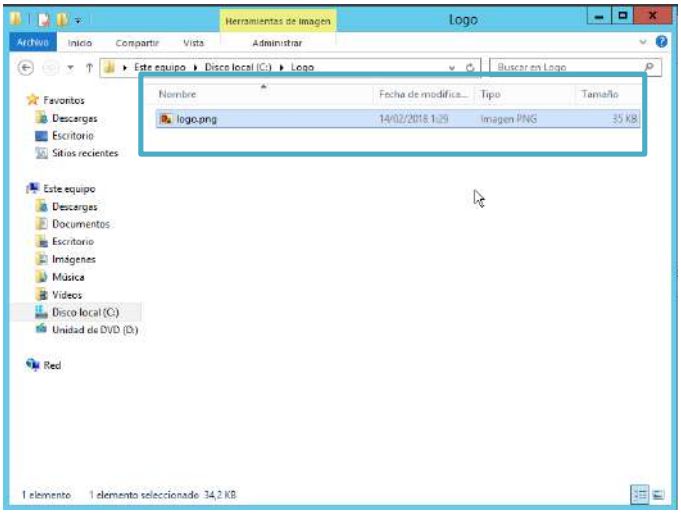


Figura 8. 12: Ubicación del logo para el papel tapiz

Luego de esto, se debe abrir el Editor de administración de directivas de grupo desde la herramienta de Administración de directivas de grupo. Después se debe ir a la siguiente ruta: Configuración de Usuario → Directivas → Plantillas administrativas → Active Desktop → Active Desktop → Habilitar Active desktop. Y se da clic en editar. Observar la Figura 8.13.

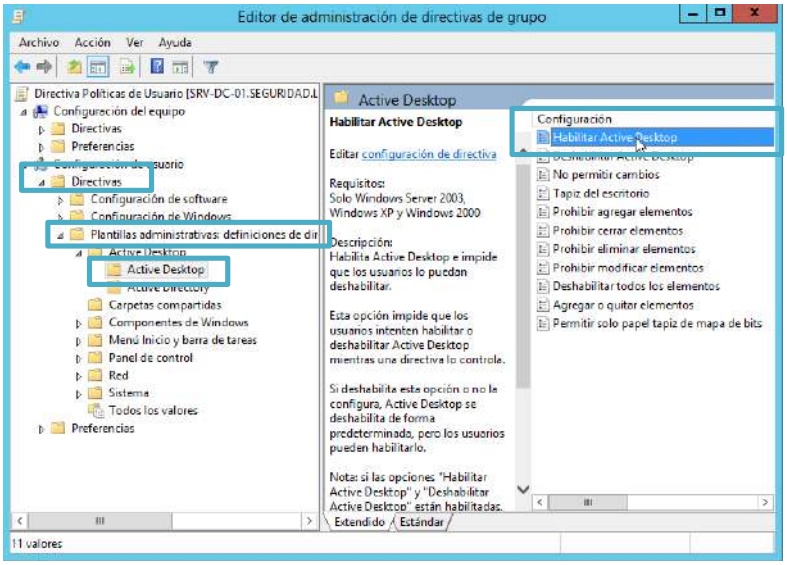


Figura 8. 13: Editor de administración de directivas de grupo

Se debe habilitar la política y se da clic en aplicar y clic en aceptar. Como se observa en la Figura 8.14.

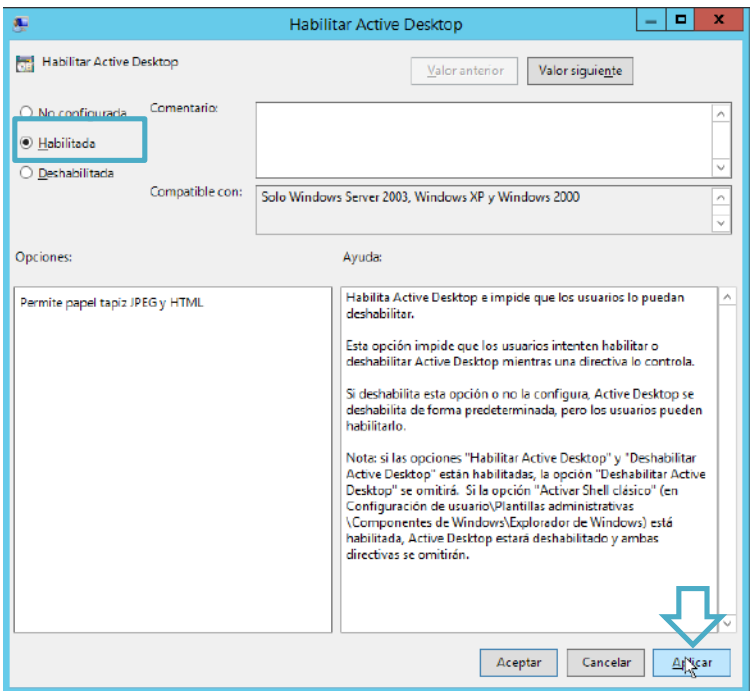


Figura 8. 14: Habilitar Active Desktop

Luego de esto se debe ubica la política Tapiz de escritorio y clic derecho y se selecciona editar. Como se observa en la Figura 8.15.

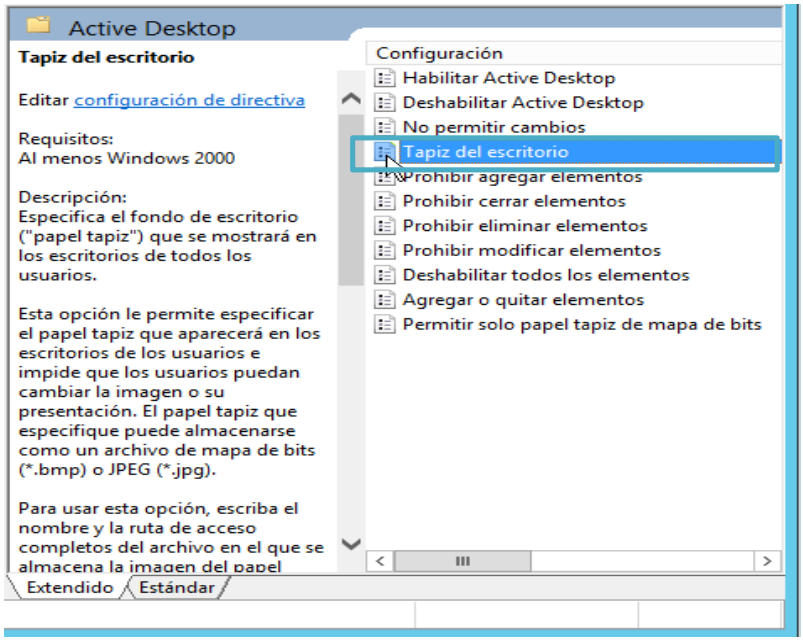


Figura 8. 15: Configurar papel tapiz

Se procede a marcar la opción Habilitar y a ingresar la ruta en donde se encuentra la imagen. En este caso, la imagen se encuentra guardad en una carpeta compartida que está en la red. Esta es su ruta: \\SRV-DC-01\Logo\logo.jpg.

Se da clic en aplicar y clic en aceptar. Como se observa en la Figura 8.16.

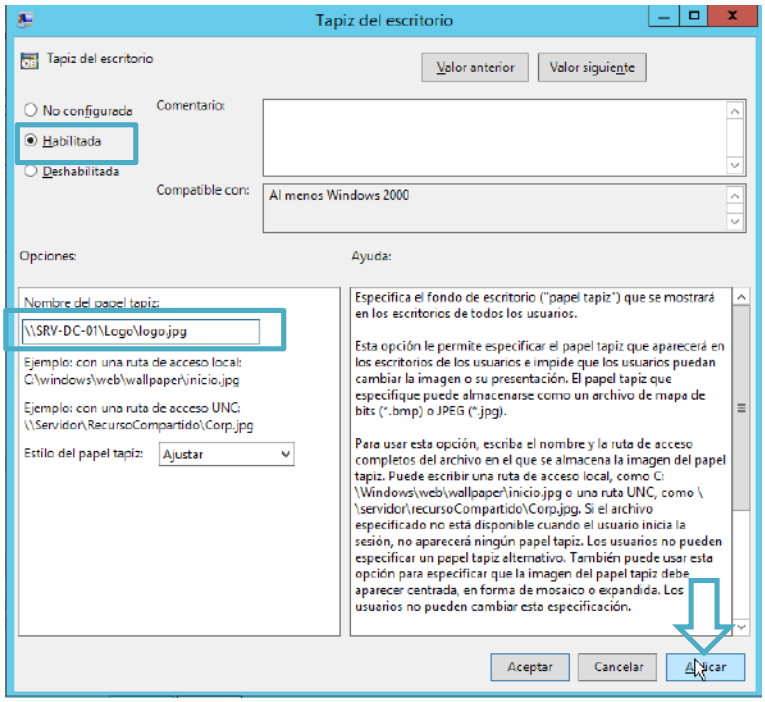


Figura 8. 16: Tapiz de escritorio

Por último, se procede a verificar si los cambios se guardaron con éxito. Se debe iniciar sesión en la PC-01 y comprobar el fondo de escritorio. Como se observa en la Figura 8.17.

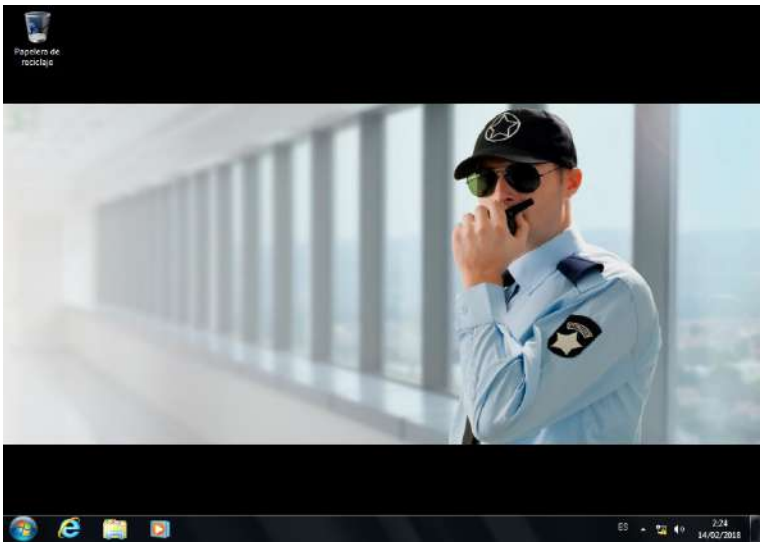


Figura 8. 17: Comprobación del correo funcionamiento del papel tapiz

4. Ahora se crearán políticas para los equipos.

   a) Los usuarios deben cambiar su contraseña cada 30 días

Para levantar esta política se debe ir a Administrador de servidor → Herramientas → Administración de directivas de grupo. Estando allí se sigue esta ruta: Bosque: seguridad.local → Dominios → seguridad.local → Empresa de seguridad → Equipos → Política de equipos. Se da clic derecho y se escoge la opción editar. Como se observa en la Figura 8.18.

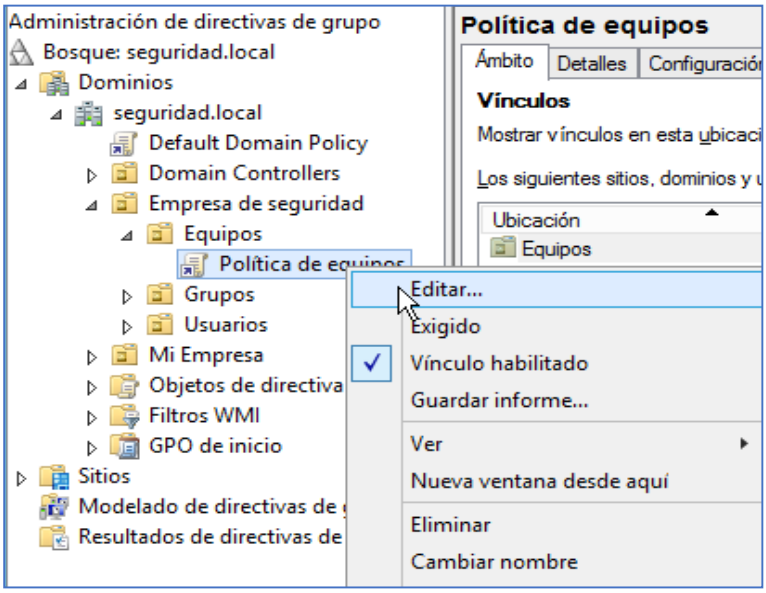


Figura 8. 18: Abrir el editor de Administración de directivas de grupo para la GPO de equipos

Una vez abierto el editor de administración de directivas de grupo, se sigue la siguiente ruta:

Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directivas de contraseñas y se selecciona la política Vigencia máxima de la contraseña, clic derecho y propiedades. Como se observa en la Figura 8.19.

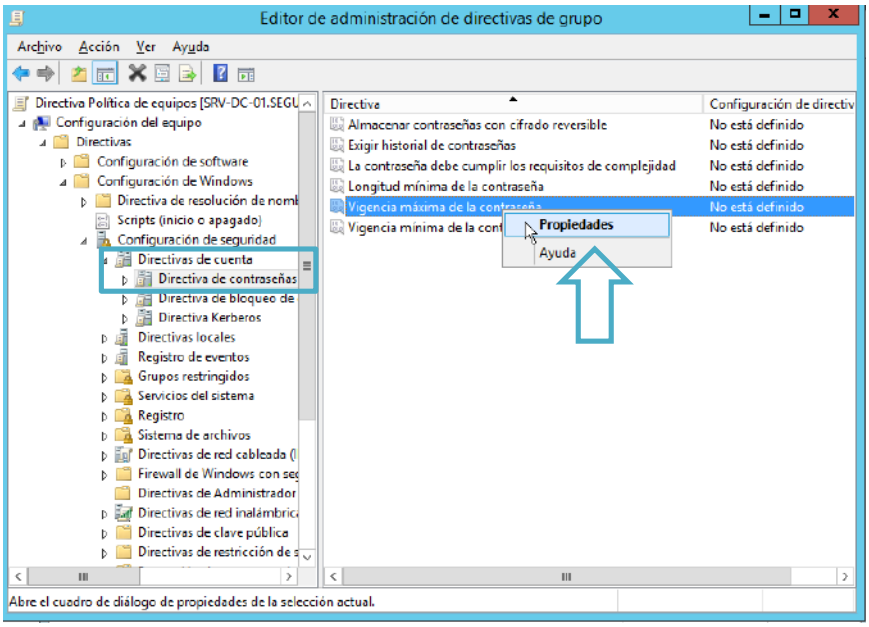


Figura 8. 19: Ubicar la directiva para la vigencia máxima de la contraseña

Después se configura los 30 días que pide la política. Se marca el check "Definir esta configuración de directiva" y en los días se coloca "30 días". Se da clic en Aplicar y clic en Aceptar. Como se observa en la Figura 8.20.

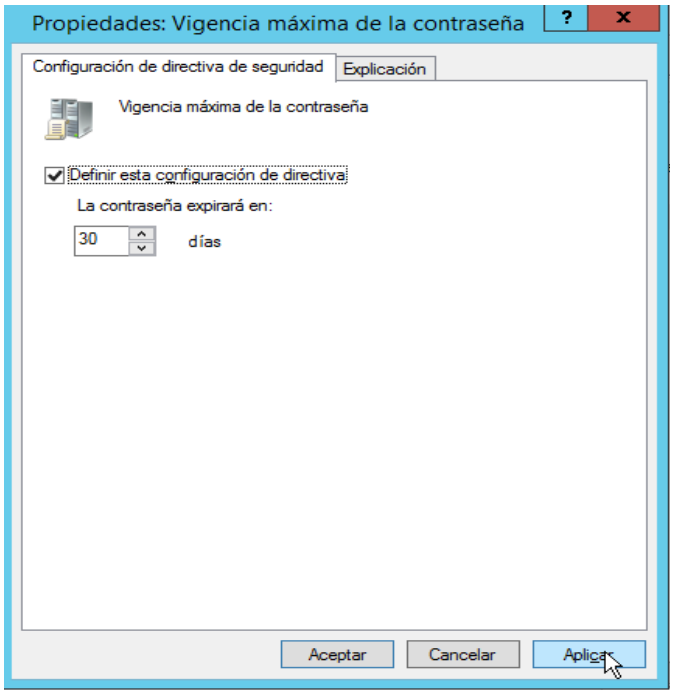


Figura 8. 20: Configurar los días de la vigencia máxima de la contraseña

b) Solo los administradores pueden apagar la máquina

Se debe seguir esta ruta: Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuarios → Apagar el sistema. Se hace clic derecho y propiedades. Como se observa en la Figura 8.21.

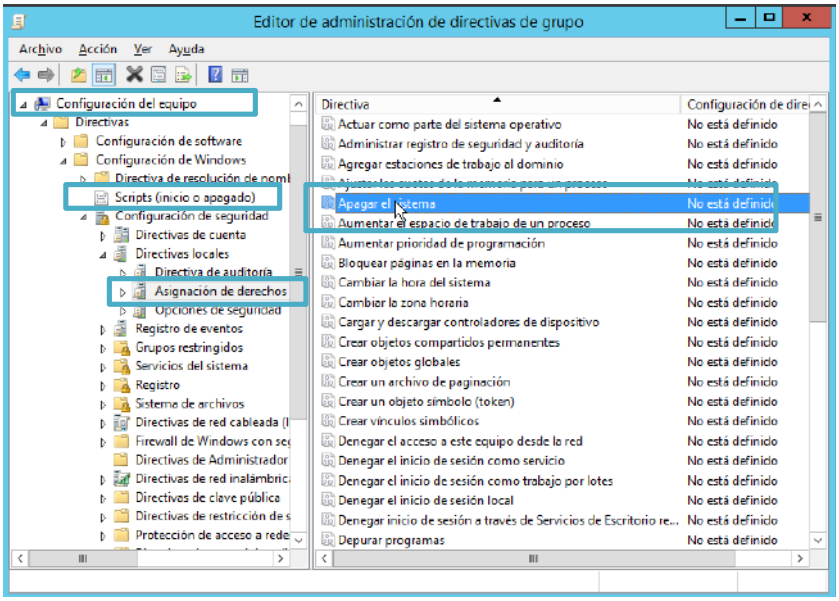


Figura 8. 21: Editar la política apagar el sistema

Luego se habilita el check "Definir esta configuración de directiva" y se procede a agregar el usuario administrador. Como se observa en la Figura 8.22.

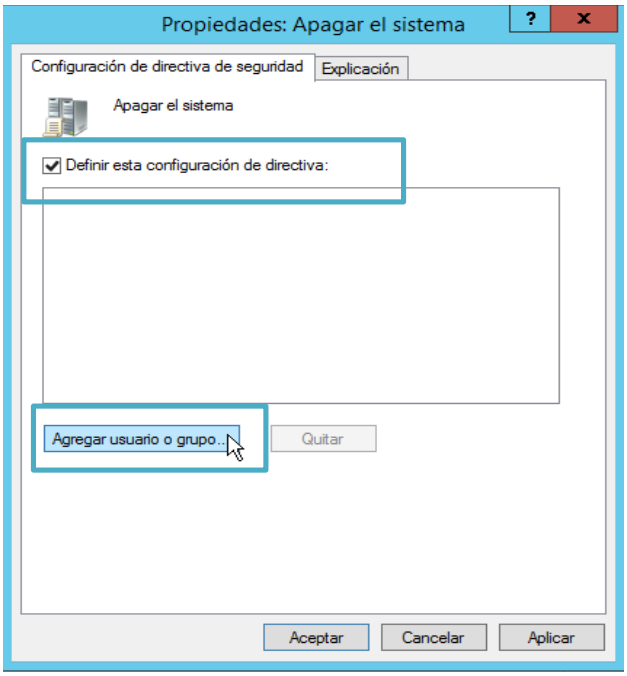


Figura 8. 22: Editar la política apagar el sistema

Se escribe el usuario Administrador, ejemplo: SEGURIDAD\Administrador. Clic en Aceptar. Luego Clic en aplicar y clic en aceptar. Como se observa en la Figura 8.23.

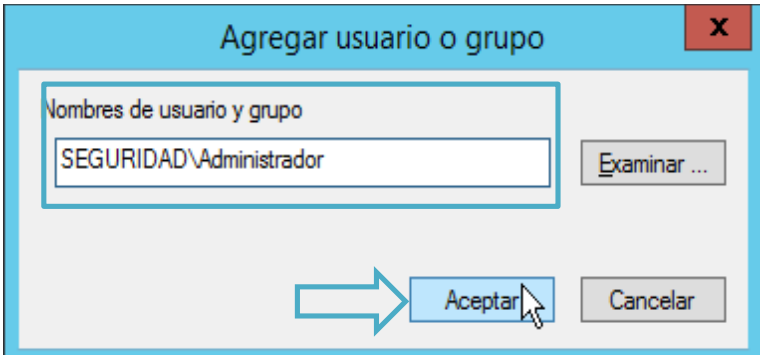


Figura 8. 23: Agregar usuario o grupo

Y listo, eso sería todo. Básicamente se pueden configurar muchas políticas que ya están predefinidas en el servicio de DA/GPO, otras se pueden crear dependiendo de la necesidad.

Unidad

IX

Unidad IX

Monitorización y Seguimiento del Servidor

9. Administrador de tareas

(Smith, 2012), da a referir que el Administrador de tareas en Windows Server 2012 es similar a las versiones anteriores (2003, 2008). Es una herramienta interesante que te permite:

- ✓ Verifique y monitoree el rendimiento y uso de los recursos tales como RAM y CPU, entre otras, para su servidor.
- ✓ Administrar procesos, aplicaciones y servicios.
- ✓ Administre a los usuarios conectados a su servidor (vea las aplicaciones y procesos que usan, desconecte a los usuarios, acceda al administrador de cuentas de los usuarios).

Para acceder al Administrador de tareas, haga clic con el botón derecho en la barra de tareas y seleccione Administrador de tareas en el menú.

9.1.1. Procesos

Esta pestaña muestra las aplicaciones en ejecución y los procesos en segundo plano. Cuando un proceso tiene varias ventanas abiertas, esto se muestra al usuario como un número que sigue el nombre del proceso y un control para expandir la vista y ver estos nombres de ventanas. Los procesos se enumeran en orden alfabético en grupos, de forma predeterminada, el orden se puede cambiar haciendo clic en cualquiera de los nombres de columna, como se muestra la figura 9.1. El estado de las aplicaciones modernas no se muestra de forma predeterminada, pero se puede habilitar seleccionando ver, valores de estado, Mostrar estado suspendido. (Morrison, 2012)

Algunos procesos de fondo y sistema también proporcionan una opción para expandir y ver objetos secundarios. Este es el caso de los procesos que alojan un servicio. Expanda el proceso para ver qué servicios se estén ejecutando en el proceso. Esto debería ayudar a que los problemas de rendimiento del servicio sean mucho más fáciles de diagnosticar, en comparación con las versiones anteriores del Administrador de tareas, entre las funciones tenemos:

- ✓ Puede visualizar el uso de la memoria en porcentaje o en cantidad (Mb).
- ✓ Puede ordenar el uso por orden ascendente o descendente haciendo clic en el título de la columna correspondiente.
- ✓ Puede visualizar más detalles para cada proceso (si está disponible), detener un proceso o mostrar la ventana del administrador de servicios haciendo clic con el botón derecho.
- ✓ Puede detener un proceso seleccionándolo y haciendo clic en el botón Finalizar tarea.
- ✓ Administrador de tarea, es útil cuando desea inspeccionar procesos sospechosos y abrir una ubicación de archivo.
- ✓ Puede crear un volcado de memoria completo para depurar una aplicación haciendo clic derecho en el proceso correspondiente.

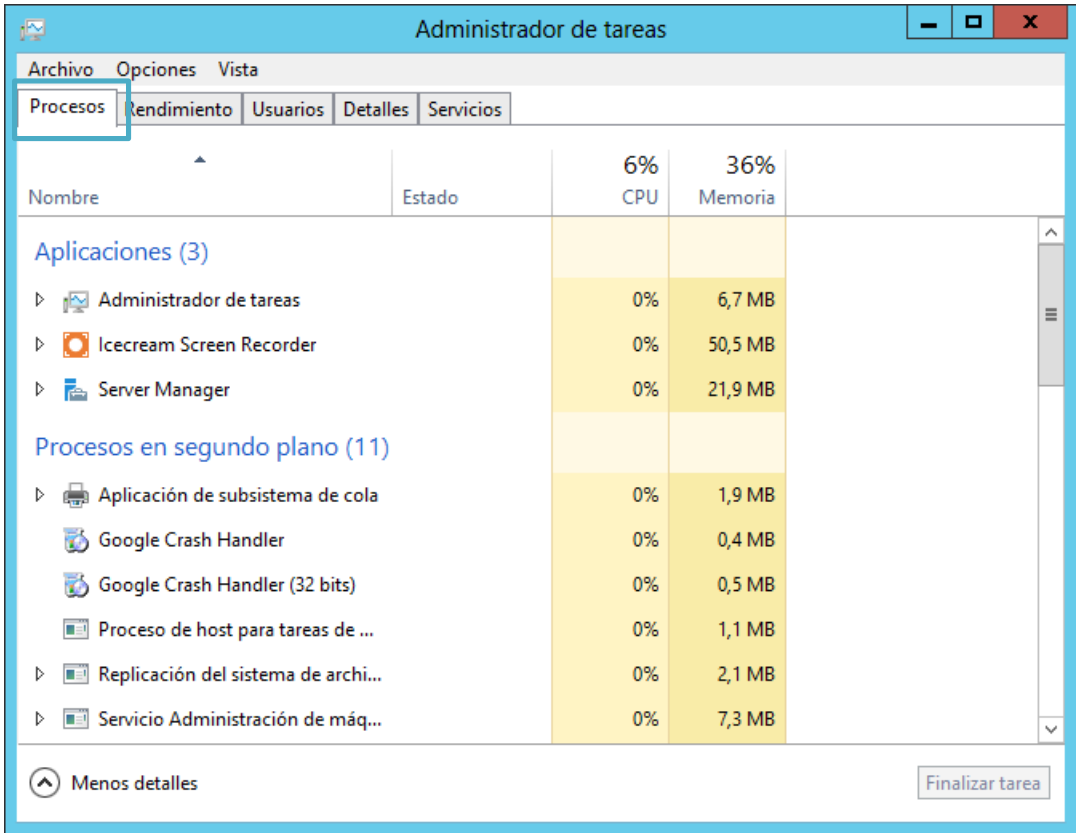


Figura 9. 1: Proceso Administrador de tareas

9.1.2. Rendimiento

La pestaña Rendimiento muestra gráficas y detalles de las 4 métricas de rendimiento de PC clave. También tenga en cuenta el enlace, abrir monitor de recursos en la parte inferior, proporcionando una ruta a esta

otra interfaz cuando necesite realizar una resolución de problemas adicional ver figura 9.2, entre las funciones tenemos:

- ✓ Puede supervisar el rendimiento de su servidor en tiempo real al mostrar gráficos en el procesador, la memoria y el uso de la red, y acceder al Monitor de recursos.
- ✓ Puede copiar la información de un componente específico (procesador, memoria, tarjeta de red) haciendo clic derecho en la pestaña correspondiente, copiando y pegando en su editor de texto favorito.
- ✓ Para abrir el Monitor de recursos desde la pestaña Rendimiento del Administrador de tareas, haga clic en Abrir monitor de recursos (en la parte inferior de la pantalla).
- ✓ El Monitor de recursos proporciona información útil sobre el uso de recursos, en tiempo real (procesador, memoria, disco, red).

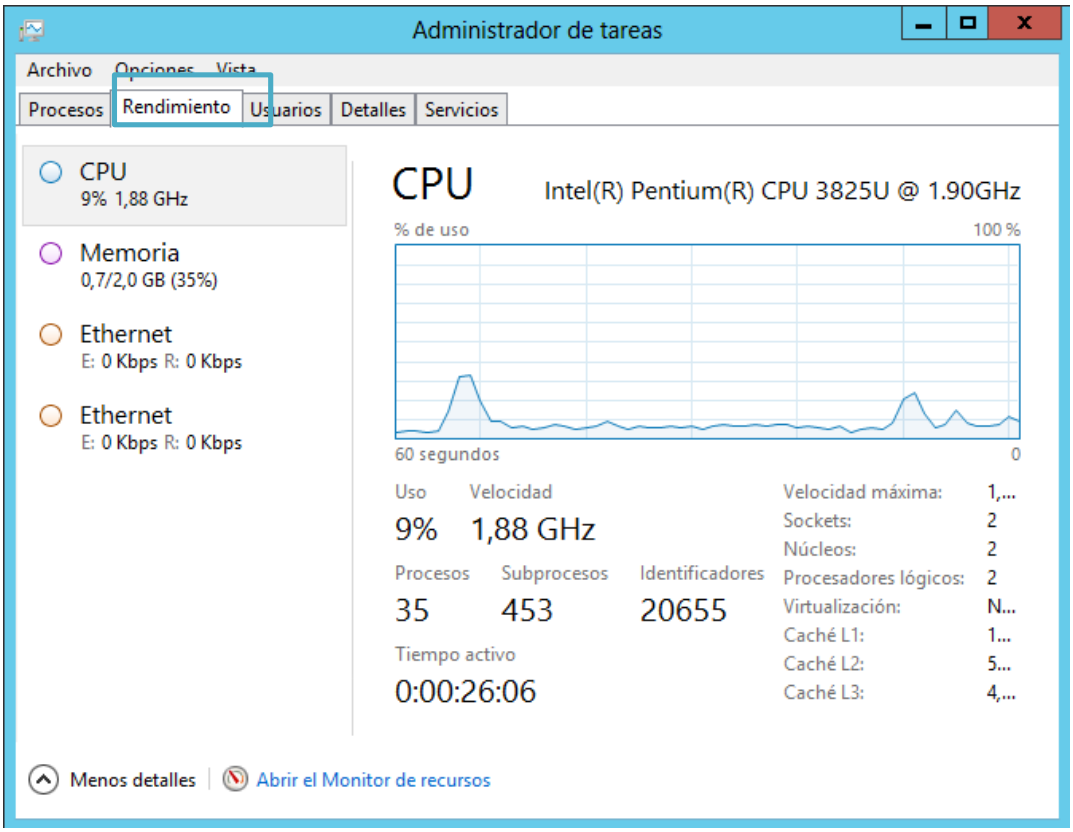


Figura 9. 2: Rendimiento Administrador de tareas

9.1.3. Usuarios

La pestaña Usuarios es donde puede ver los procesos que se ejecutan en la sesión de cada usuario. Esto difiere de la antigua interfaz del

Administrador de tareas donde todos los procesos de los usuarios se mostraban en la pestaña Proceso, ver figura 9.3, entre ellos tenemos las siguientes funciones.

- ✓ Esta pestaña se usa para administrar usuarios conectados a su servidor.
- ✓ Puede ver las aplicaciones y procesos que utiliza un usuario específico, su uso de recursos (procesador y memoria en porcentaje o cantidad).
- ✓ También puede desconectar a un usuario o abrir el administrador de cuentas de los usuarios para cambiar una contraseña o parámetros generales (certificados EFS).

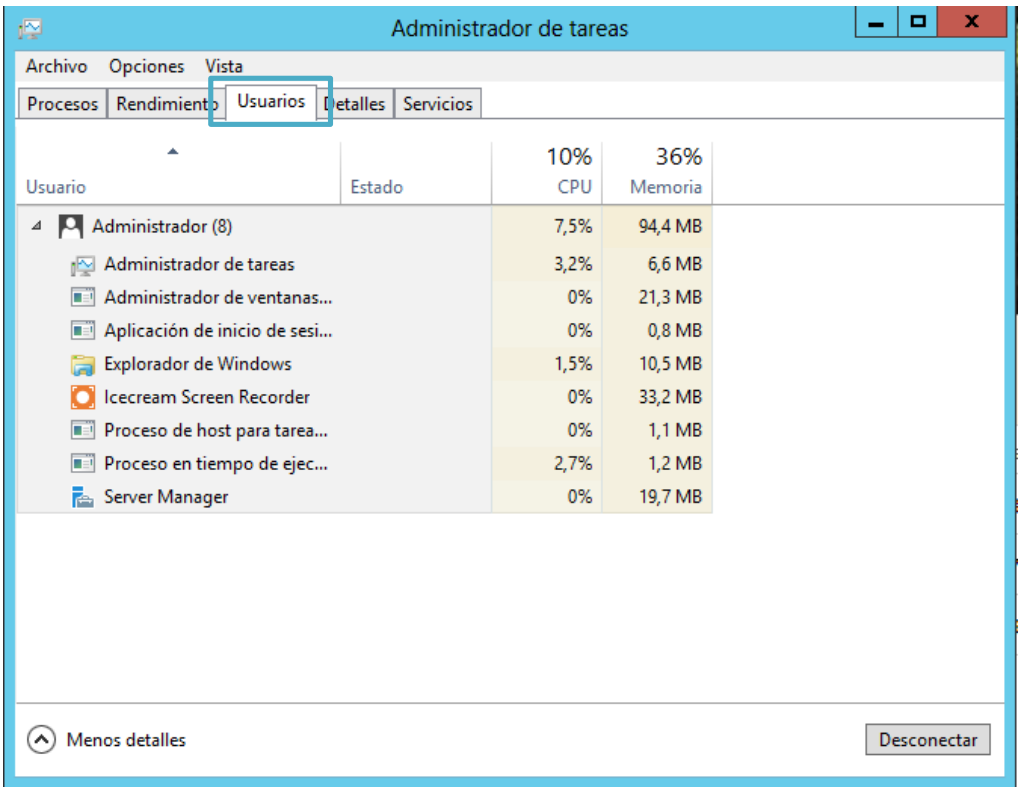


Figura 9. 3: Usuarios Administrador de tareas

9.1.4. Detalles

La pestaña Detalles es donde la nueva interfaz del Administrador de tareas proporciona las mismas opciones de selección de columnas y la misma lista de procesos que en el antiguo Administrador de tareas, ver figura 9.4. Esto es útil para visualizar todos los procesos juntos, o si se

necesita ordenar por una métrica de rendimiento acumulativa, en la cual cumple con las siguientes funciones:

- ✓ Desde esta pestaña, puede ver más detalles sobre los procesos.
- ✓ Puede finalizar un proceso, obtener una vista de estructura de árbol, definir su prioridad, analizar dependencias, crear un volcado de memoria completo y abrir una ubicación de archivo.
- ✓ El botón Finalizar tarea en la esquina inferior derecha de la pantalla le permite detener el proceso seleccionado.

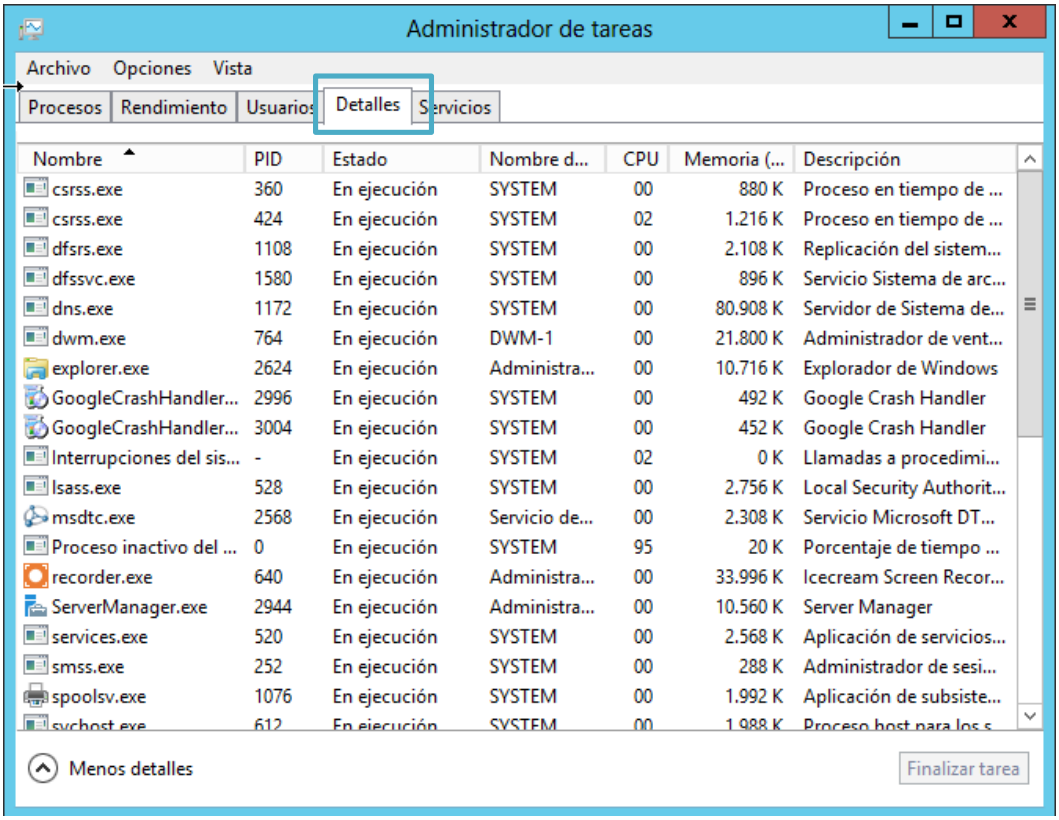


Figura 9. 4: Detalles Administrador de tareas

9.1.5. Servicios

La pestaña Servicios es la última pestaña en la interfaz de detalles. Como se muestra a continuación (ver figura 9.5), esto ofrece una vista muy similar al antiguo Administrador de tareas, cumple con las siguientes funciones:

- ✓ Desde esta pestaña, puede administrar los servicios deteniéndolos, comenzando y reiniciándolos.

- ✓ Puede abrir la utilidad del administrador de servicios haciendo clic en el botón Abrir servicios que se encuentra en la parte inferior de la pantalla.

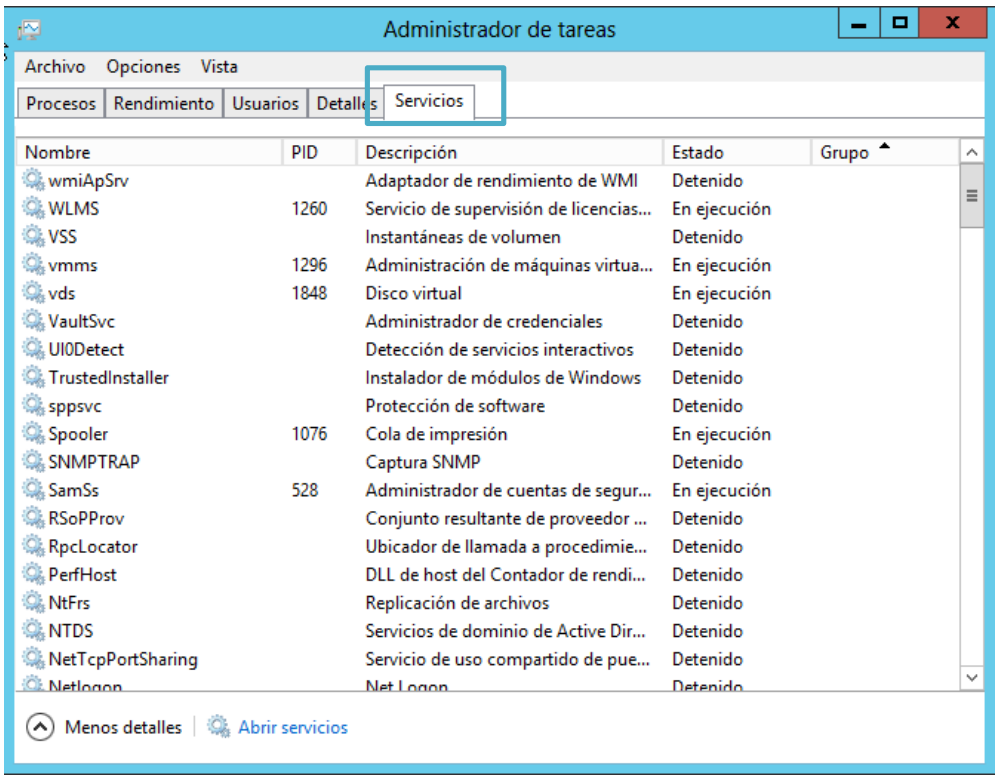


Figura 9. 5: Servicios Administrador de tareas

9.2. Monitor de rendimiento y recursos

9.2.1. Monitor de rendimiento

El monitor de rendimiento es una herramienta que nos permite analizar el rendimiento del sistema. Para ejecutar dicha herramienta realizaremos el siguiente proceso:

Abrimos el Panel del Administrador del servidor, en la parte lateral del lado derecho, dar clic en herramientas, luego se despliega un listado de herramientas, buscamos la herramienta monitor de rendimiento, dar clic en ello. Mostrará la siguiente ventana, como se muestra la figura 9.6:

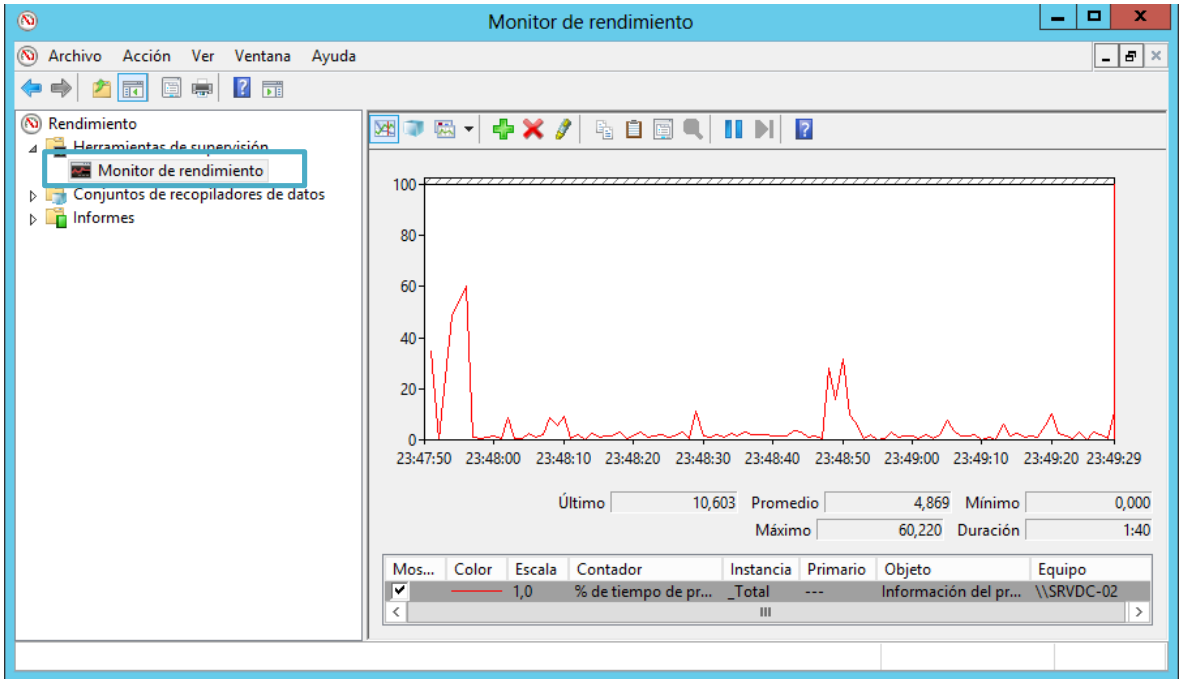


Figura 9. 6: Monitor de rendimiento

9.2.2. Monitor de recursos

(Zamora, 2016), dice que el monitor de recursos nos brinda información detallada acerca de los recursos del sistema, CPU, memoria, discos duros y red. Esta herramienta nos permite analizar que procesos o servicios están consumiendo de manera anormal alguno de los recursos de hardware del servidor, lo cual puede incidir en un bajo rendimiento en la máquina.

Para acceder al monitor de recursos nos dirigimos al administrador del servidor y elegimos la opción Monitor de recursos o bien a través de PowerShell con el comando resmon.exe, como se muestra la figura 9.7:

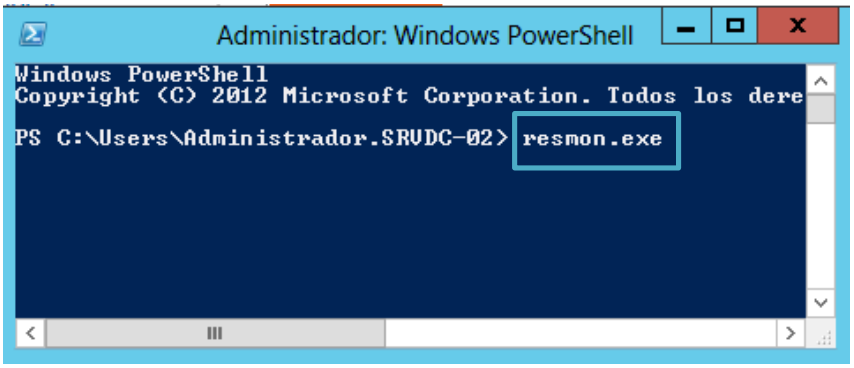


Figura 9. 7: PowerShell

Una vez ejecutada el comando muestra la ventana del monitor de recursos, esta opción se desplegará la siguiente ventana en la cual podremos visualizar y gestionar el rendimiento de nuestro servidor, veremos que tenemos disponibles las siguientes pestañas para administrar:
Información general.

- ✓ CPU
- ✓ Memoria
- ✓ Disco
- ✓ Red

Podemos desplegar cada pestaña para observar el comportamiento de nuestro recurso de hardware como se muestra la figura 9.8.

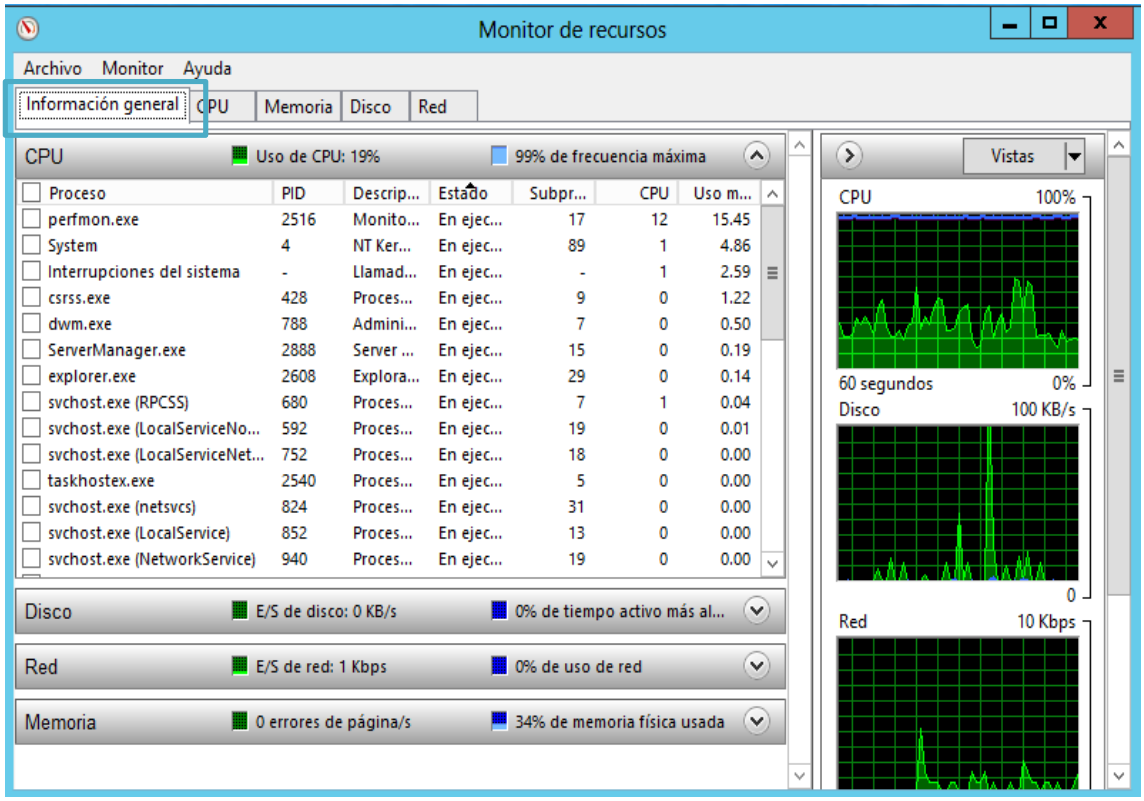


Figura 9. 8: Monitor de recursos Información General

Si se dirige opción memoria al darle clic muestra una ventana monitor de recursos de la memoria, donde nos indica la memoria disponible, en caché entre otras, como se muestra la figura 9.9.

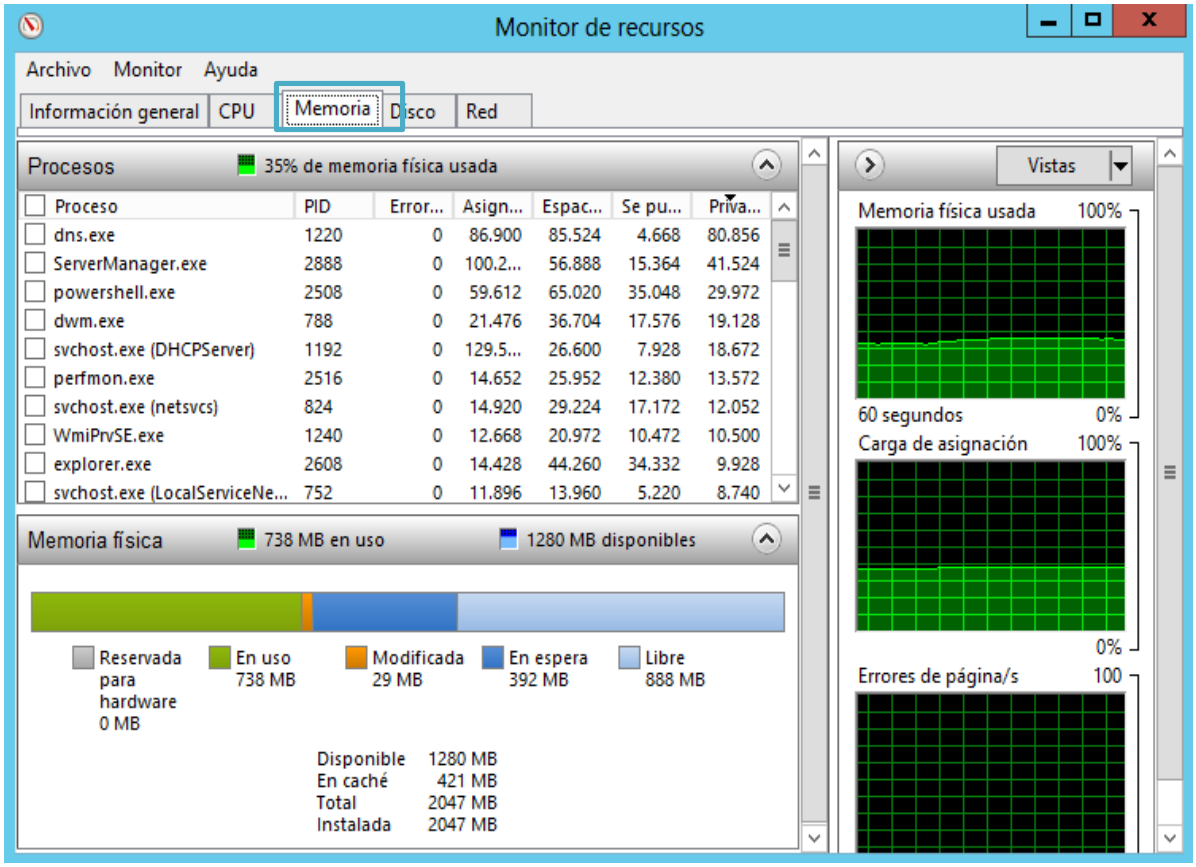


Figura 9. 9: Monitor de recursos de la Memoria

9.3. Visor de eventos

El Visor de eventos, que se muestra en la figura 9.10, le permite acceder a la información del evento grabado. El Visor de eventos de Windows Server 2012 y Windows Server 2012 R2 difiere del Visor de eventos en versiones anteriores del sistema operativo Windows Server, como Windows Server 2003, ya que no solo ofrece la aplicación, la seguridad, la configuración y los registros del sistema, sino que también contiene registros de aplicaciones y servicios separados. Estos registros están diseñados para proporcionar información por rol o por aplicación, en lugar de tener todos los eventos relacionados con el servicio de rol y la aplicación canalizados al registro de la aplicación. Cuando busque eventos relacionados con un servicio, función o aplicación específica, verifique si ese servicio, función o aplicación tiene su propio registro de aplicación. (Orin, 2014)

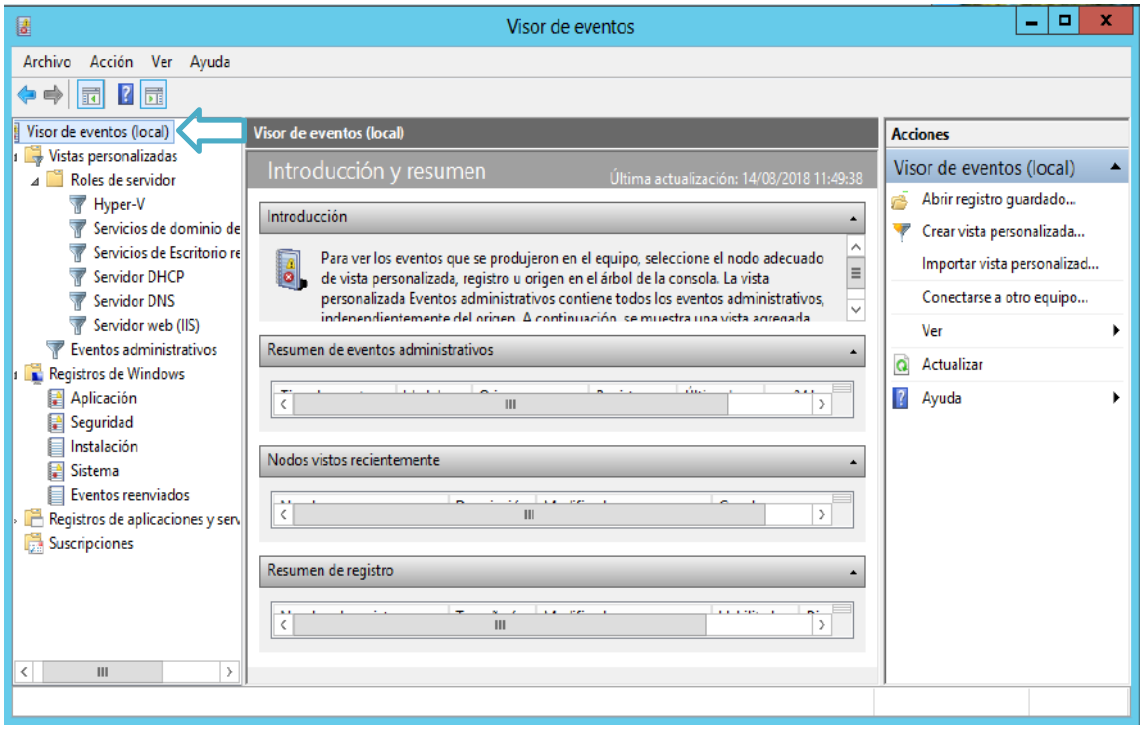


Figura 9. 10: Visor de eventos

9.3.1. Filtros de registro de eventos

(Orin, 2014), se da referir que los filtros y los registros de eventos le permiten ver solo aquellos eventos que tienen características específicas. Los filtros se aplican solo a la sesión actual del Visor de eventos. Si constantemente usa un filtro específico o un conjunto de filtros para administrar los registros de eventos, en su lugar debe crear una vista personalizada. Los filtros se aplican solo a un solo registro de eventos. Puede crear filtros en un registro basado en las siguientes propiedades:

- ✓ Registrado.- Le permite especificar el rango de tiempo para el filtro.
- ✓ Nivel de evento.- Le permite especificar niveles de eventos. Puede elegir las siguientes opciones: Crítico, Advertencia, Detallado, Error e Información.
- ✓ Orígenes de eventos.- Le permite elegir la fuente del evento.
- ✓ Id.- De evento Le permite filtrar en función de la identificación del evento. También puede excluir identificadores de eventos específicos.
- ✓ Palabras clave.- Le permite especificar palabras clave basadas en los contenidos de los eventos.
- ✓ Usuario.- Le permite limitar eventos según el usuario.

- ✓ Computadora.- Le permite limitar eventos basados en la computadora.

Para crear un filtro, realice los siguientes pasos:

1. Abra el Visor de eventos y seleccione el registro que desea filtrar.
2. Determine las propiedades del evento que desea filtrar.
3. En el panel Acciones, haga clic en Filtrar registro actual.
4. En el cuadro de diálogo Registro de registro actual, que se muestra en la figura 9.11, especifique las propiedades del filtro.

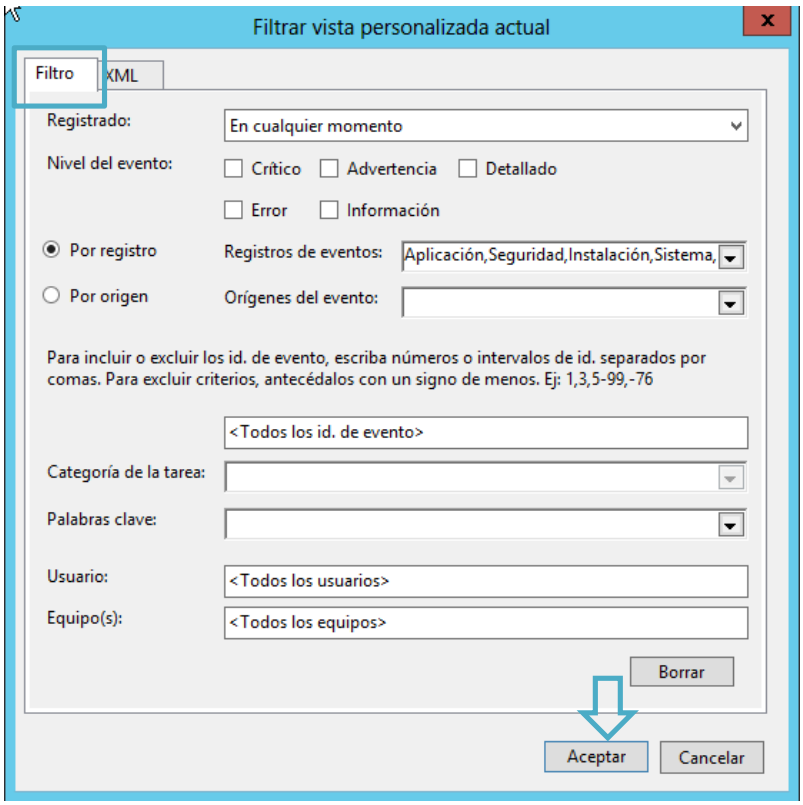


Figura 9. 11: Especificaciones de las propiedades del Filtro

9.3.2. Vistas de registro de eventos

Las vistas de registro de eventos le permiten crear vistas personalizadas de eventos en cualquier registro de eventos almacenados en un servidor, incluidos los eventos en el registro de eventos reenviados. En lugar de mirar a través de cada registro de eventos para ver elementos de interés específicos, puede crear vistas de registro de eventos que se dirijan solo a esos elementos específicos. El Visor de eventos incluye una vista personalizada llamada Eventos administrativos. Esta vista muestra eventos críticos, de advertencia y de error de una variedad de registros

de eventos importantes, como la aplicación, la seguridad y los registros del sistema.

Las vistas difieren de los filtros de las siguientes maneras:

- ✓ Persistente Puede usar una vista en múltiples sesiones de Visor de eventos. Si configura un filtro en un registro, no estará disponible la próxima vez que abra el Visor de eventos.
- ✓ Incluir registros múltiples Una vista personalizada puede mostrar eventos de registros separados. Los filtros están limitados a mostrar eventos de un registro.
- ✓ Exportable Puede importar y exportar vistas de registro de eventos entre computadoras.

(Orin, 2014), dice que al crear una vista de registro de eventos es un proceso similar a la creación de un filtro. La principal diferencia es que puede seleccionar eventos de varios registros y le da al registro de eventos un nombre y elige un lugar para guardarlo. Para crear una vista de registro de eventos, realice los siguientes pasos:

1. Abrir el Visor de eventos.
2. Haga clic en el nodo Vistas personalizadas y luego en Crear vista personalizada en el menú Acciones.
3. En el cuadro de diálogo Crear vista personalizada, que se muestra en la figura 9.12 , seleccione las propiedades de la vista, que incluyen:
    - ✓ Cuando se registran los eventos.
    - ✓ El nivel del evento.
    - ✓ Origen del evento.
    - ✓ Categoría de tarea.
    - ✓ Palabras clave.
    - ✓ Usuario.

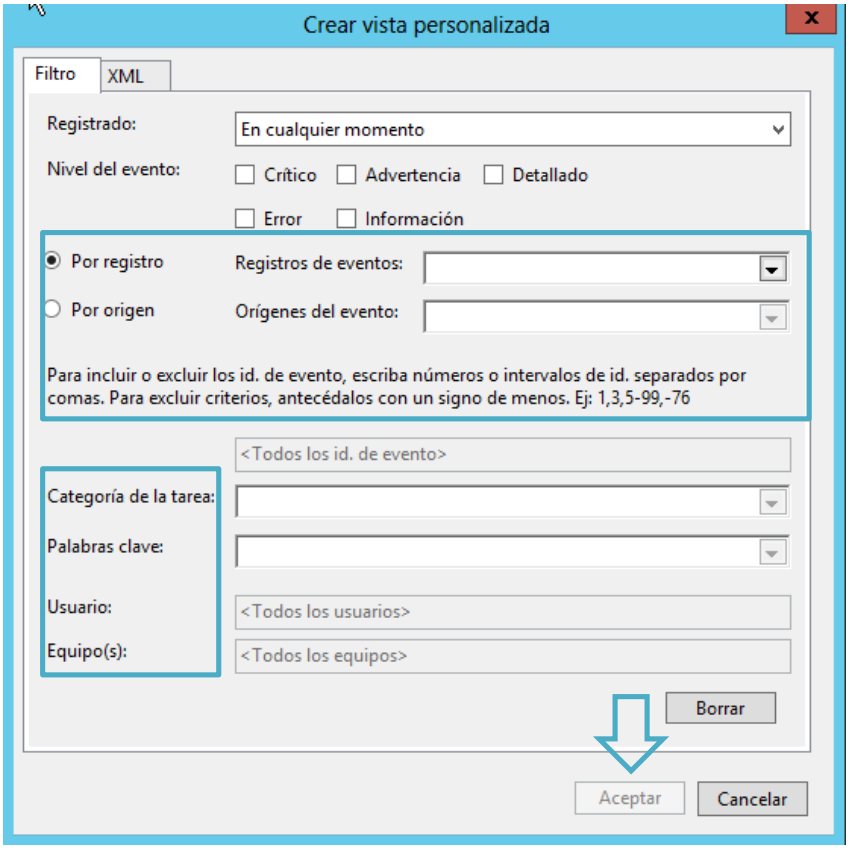


Figura 9. 12: Creación de una vista personalizada

4. En el cuadro de diálogo Guardar filtro en vista personalizada, ingrese un nombre para la vista personalizada y una ubicación donde guardar la vista, ver figura 9.13, clic en aceptar.

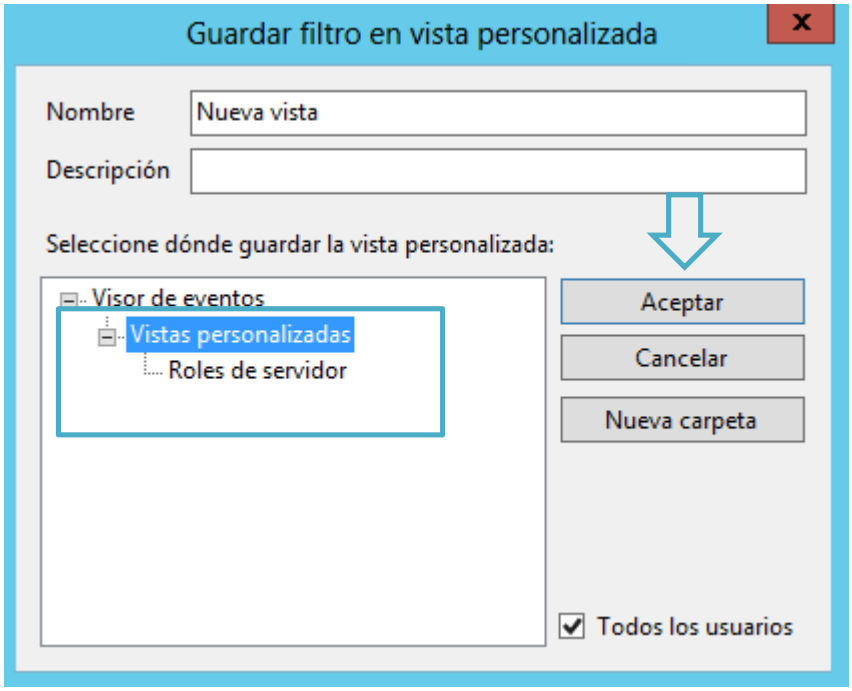


Figura 9. 13: Introducción del nombre de la vista personalizada

5. Verifique que la nueva vista aparezca como su propio nodo en el Visor de eventos.

Puede exportar una vista de registro de eventos personalizada seleccionando la vista de registro de eventos y haciendo clic en Exportar vista personalizada. Las vistas exportadas se pueden importar en otras computadoras con Windows Server 2012 y Windows Server 2012 R2.

9.4. El entorno WinRE

(Microsoft, 2017), dice que el Windows PE (WinPE) para Windows Server 2012, es un sistema operativo que sirve para instalar, implementar y reparar ediciones de escritorio de Windows Server 2012 y otros sistemas operativos Windows. En Windows PE, puedes:

- ✓ Configurar la unidad de disco duro antes de instalar Windows.
- ✓ Instalar Windows mediante aplicaciones o scripts desde una red o una unidad local.
- ✓ Capturar y aplicar imágenes de Windows.
- ✓ Modificar el sistema operativo Windows mientras no se está ejecutando.

- ✓ Configurar herramientas de recuperación automática.
- ✓ Recuperar datos de dispositivos que no pueden arrancar.
- ✓ Agregar tu propio shell personalizado o interfaz de usuario gráfica para automatizar este tipo de tareas.

Es decir, que el Windows PE es el entorno de preinstalación de Windows, se trata de un sistema Windows muy ligero que permite ejecutar un conjunto de herramientas para desplegar un sistema operativo Windows.

9.5. Firewall

El Firewall de Windows con seguridad avanzada es un firewall que se ejecuta en Windows Server 2012 y está activado de manera predeterminada. La configuración de Firewall dentro de Windows Server 2012 se administra desde la consola de administración de Microsoft Windows Firewall. (Rosario, 2014)

Para establecer la configuración del Firewall, realice los siguientes pasos:

1. Dirigirse al Administrador del servidor desde la barra de tareas, dar clic en el menú Herramientas y seleccione Windows Firewall con seguridad avanzada, ver figura 9.14.

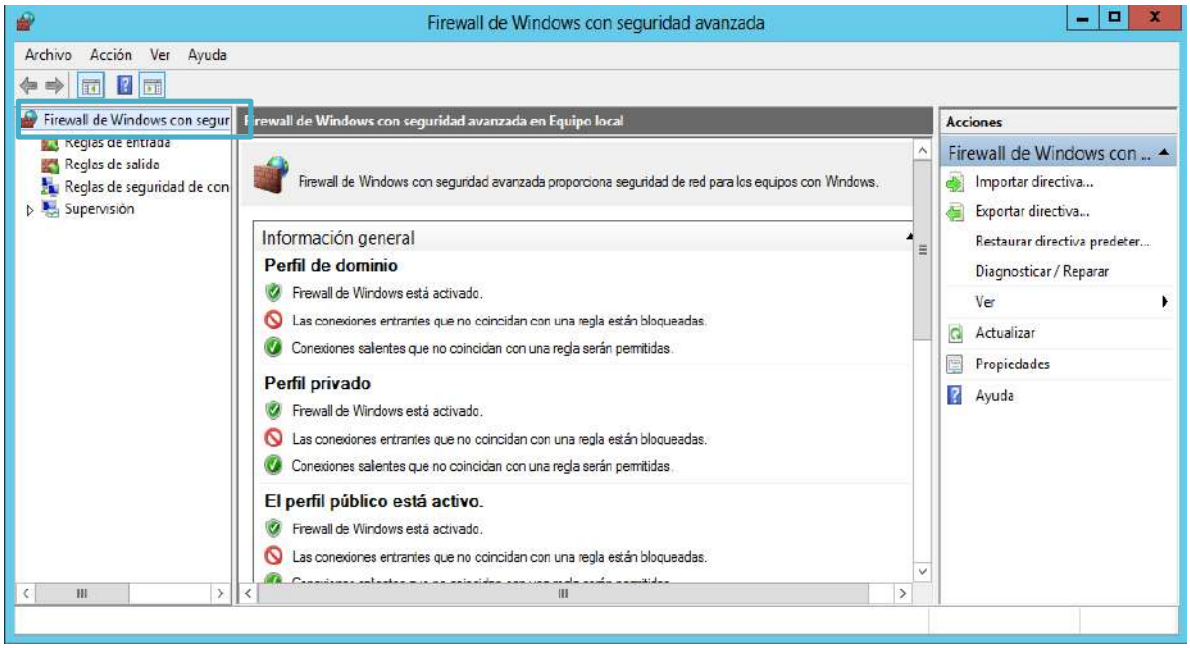


Figura 9. 14: Firewall de Windows

2. Para ver la configuración actual, seleccione Propiedades del Firewall de Windows desde la MMC. Esto permite el acceso para modificar la configuración de cada uno de los tres perfiles de firewall, que son: dominio, privado y público y la configuración de IPsec, ver figura 9.15.

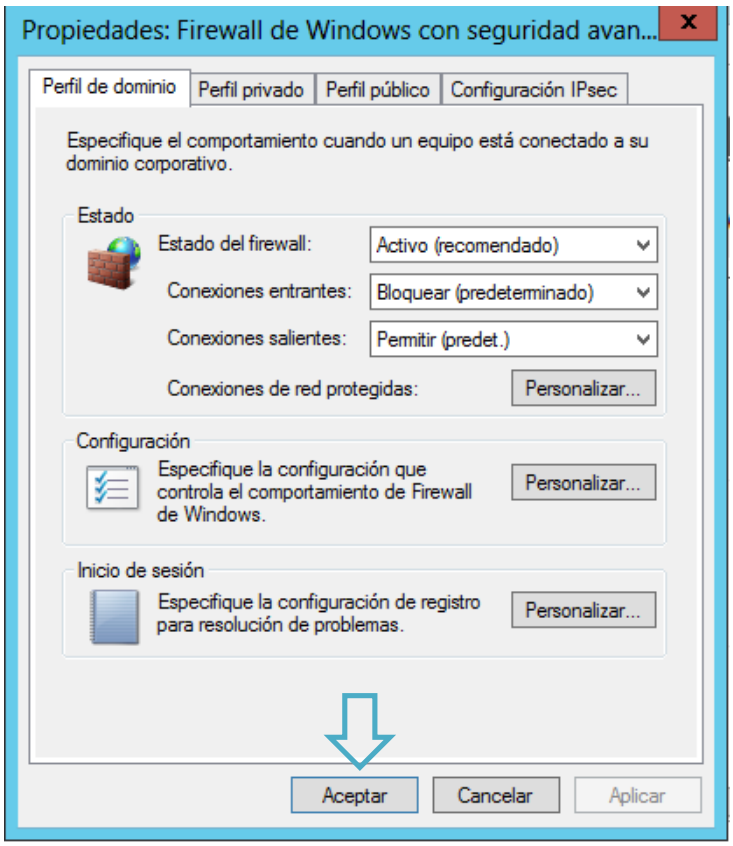


Figura 9. 15: Propiedades de Firewall de Windows

3. Aplicar reglas personalizadas, que incluirán los dos pasos siguientes:

   - ✓ Seleccione Reglas de entrada o Reglas de salida en Firewall de Windows con seguridad avanzada en el lado izquierdo de la consola de administración. (Como usted sabe, el tráfico saliente es el tráfico generado desde el servidor hacia Internet y el tráfico entrante es viceversa). Las reglas que están habilitadas actualmente se indican mediante el icono de casilla de verificación verde, mientras que las reglas desactivadas muestran un icono de casilla de verificación gris.
   - ✓ Al hacer clic con el botón derecho en una regla, podrá activar / desactivar, como se muestra la figura 9.16.

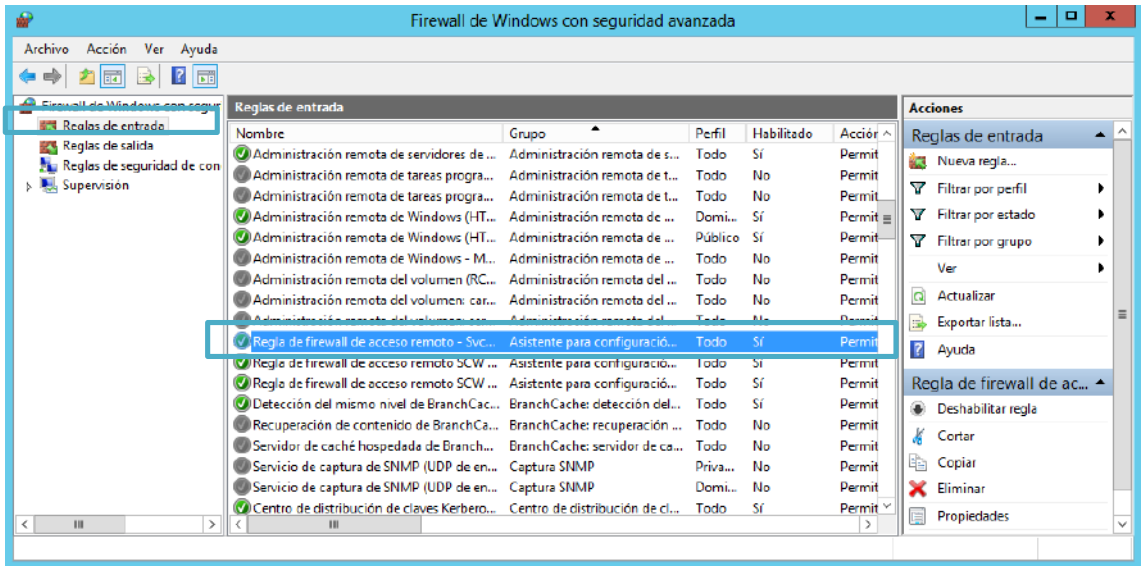


Figura 9. 16: Activar Regla del Firewall de Windows

9.5.1. ¿Cómo crear una nueva regla de firewall?

Para crear una nueva regla de firewall, debe seguir los siguientes pasos:

1. Desde el lado derecho de las Reglas de entrada o las Reglas de salida, haga clic en "Nueva regla", como se muestra la figura 9.17.

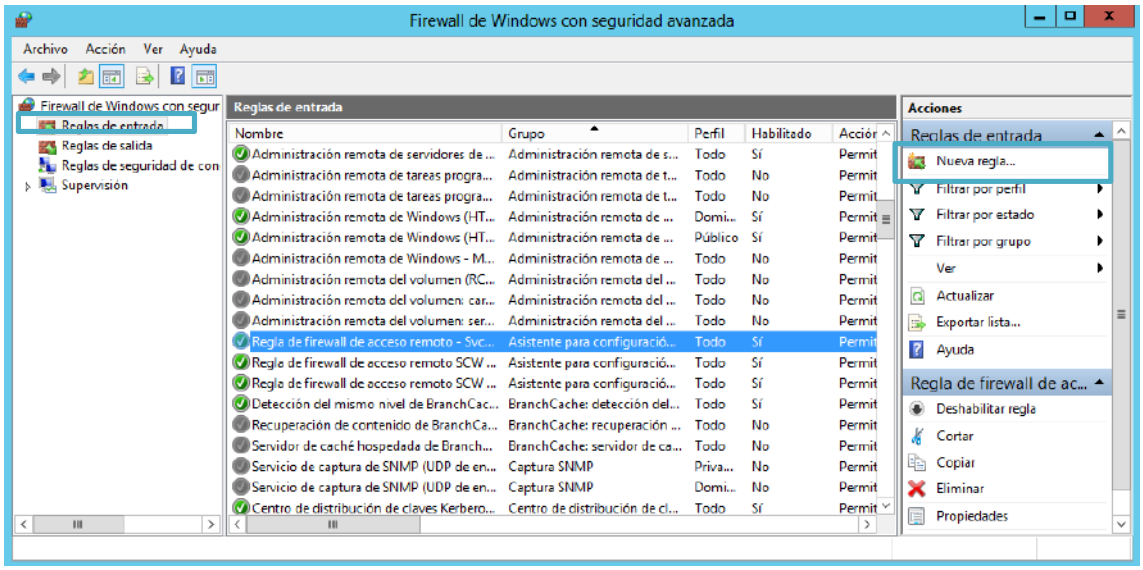


Figura 9. 17: Nueva Regla Firewall de Windows

2. Personalizado desde el botón radial Tipo de regla, clic en siguiente, como se muestra la figura 9.18.

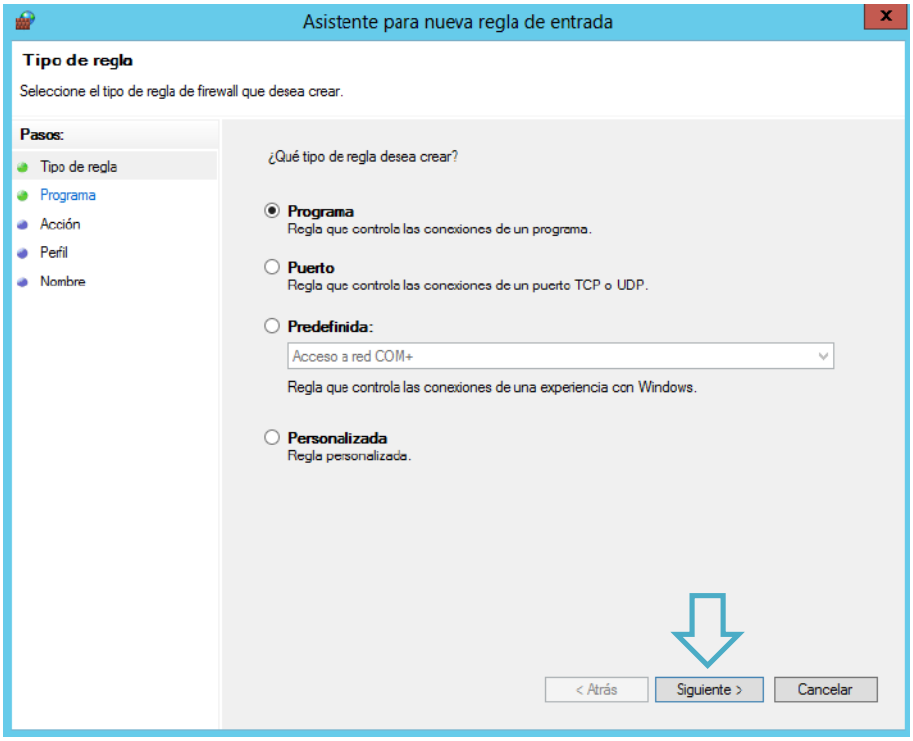


Figura 9. 18: Asistente para nueva regla de entrada

3. Seleccione la asociación de programa para la regla de firewall personalizada como todos los programas o la ruta a un programa, clic en siguiente, ver figura 9.19.

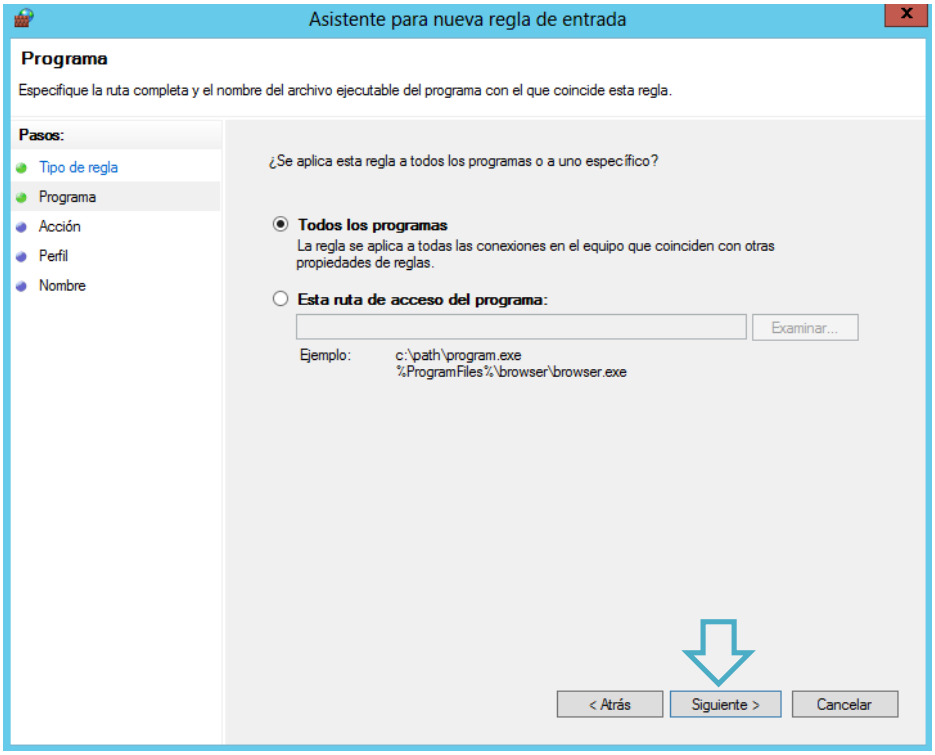


Figura 9. 19: Asistente para nueva regla, programa

4. Seleccione una acción para hacer coincidir el tráfico, dar clic en siguiente, ver figura 9.20.

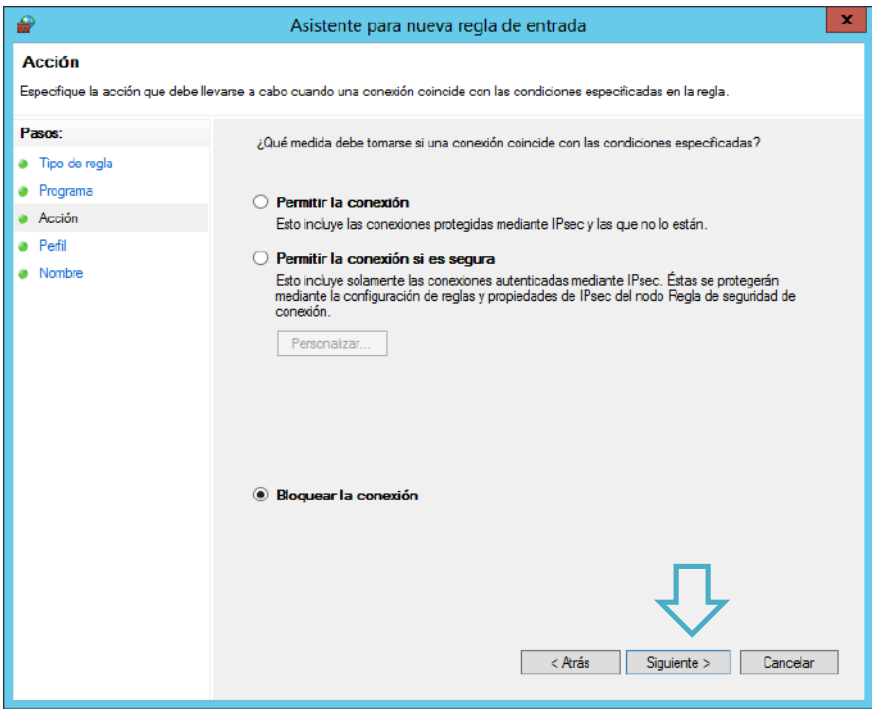


Figura 9. 20: Asistente para nueva regla, acción

5. Seleccione los perfiles asociados con la regla personalizada dar clic en siguiente, como se muestra la figura 9.21.

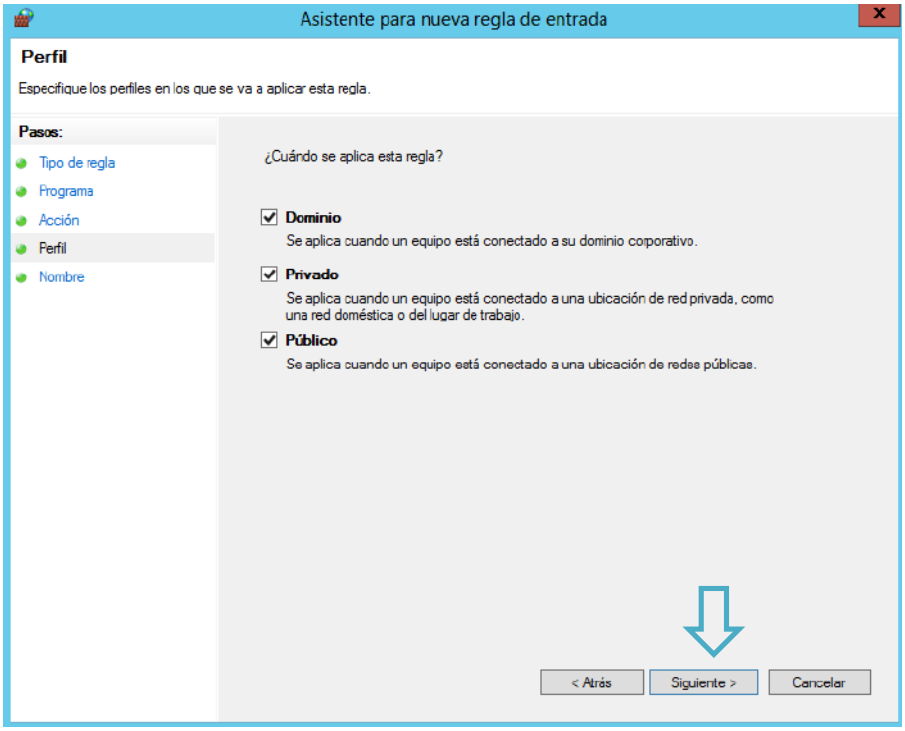


Figura 9. 21: Asistente para nueva regla, perfil

6. Escriba un nombre para su regla de Firewall y una descripción opcional, dar clic en finalizar como se muestra la figura 9.22.

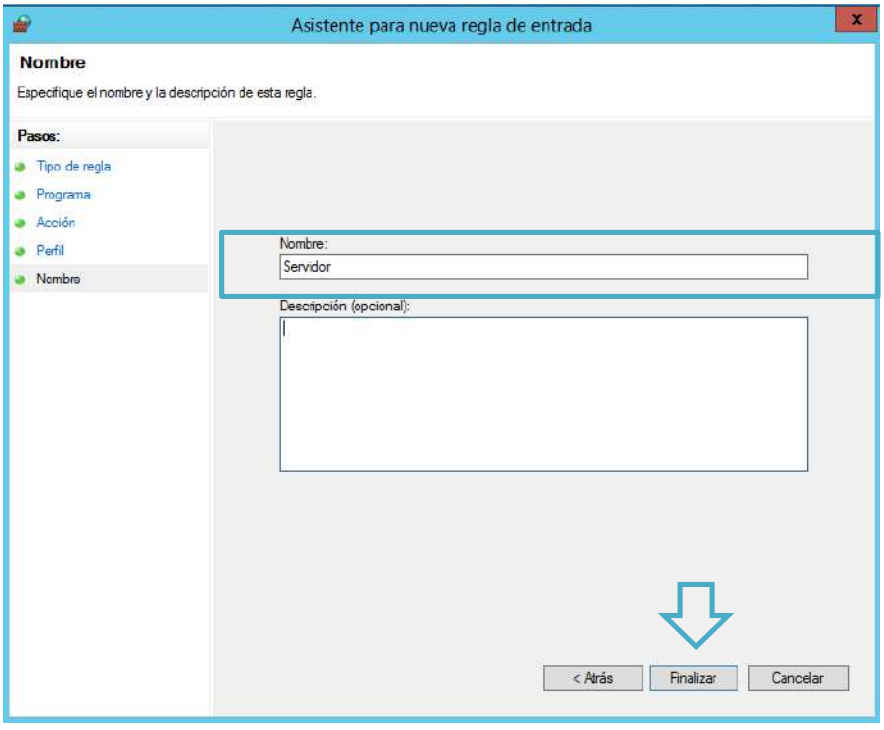


Figura 9. 22: Colocar nombre, asistente para nueva regla

7. La regla del firewall se puede encontrar en la pestaña Regla correspondiente, ya sea entrante o saliente, dependiendo del tipo

creado. Para deshabilitar o eliminar la regla, encuentre la regla en este caso servidor como lo implementamos en la figura 9.22, dar clic con el botón derecho y seleccione deshabilitar regla o eliminar, como se muestra la figura 9.23.

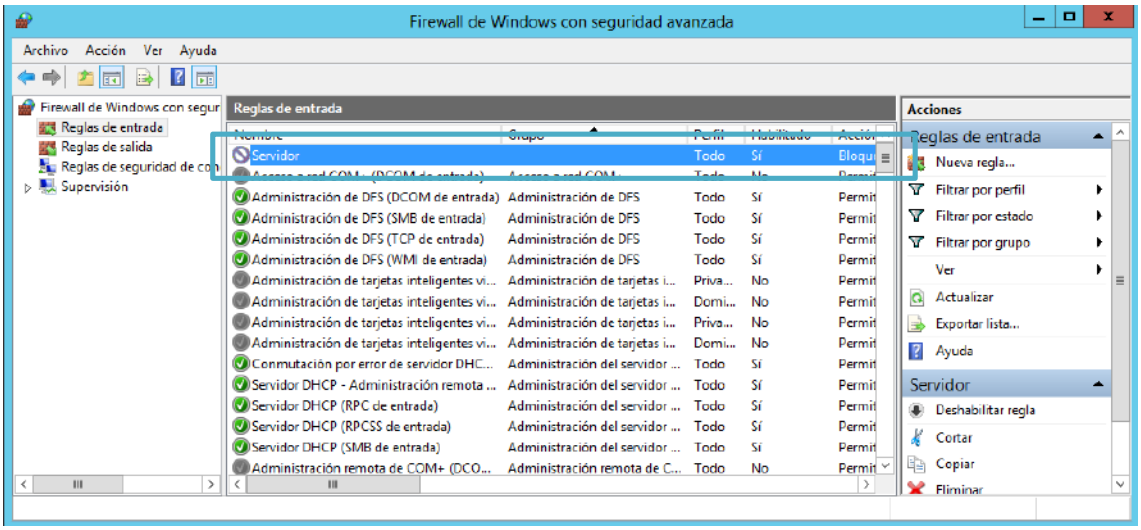


Figura 9. 23: Regla Servidor Firewall de Windows

9.6. Backup Windows Server

Windows Server Backup (WSB) es una función que proporciona opciones de copia de seguridad y recuperación para entornos de servidor Windows.

Los administradores pueden usar Windows Server Backup para hacer una copia de seguridad de un servidor completo, el estado del sistema, los volúmenes de almacenamientos seleccionados o archivos o carpetas específicos, siempre que el volumen de datos sea inferior a 2 terabytes . (Rouse, 2014)

Para instalar la copia de seguridad en Windows Server 2012 seguimos los siguientes pasos:

1. Dirigirse en administrador de servidor, clic en opción agregar roles y características, seleccionar el nombre del servidor dar clic en siguiente, aparecerá ventana de roles de servidores en esa opción no seleccionamos nada, pulsamos clic en siguiente, luego muestra otra ventana donde nos indica las características y elegir

la opción copia de seguridad de windows server como se muestra la figura 9.24.

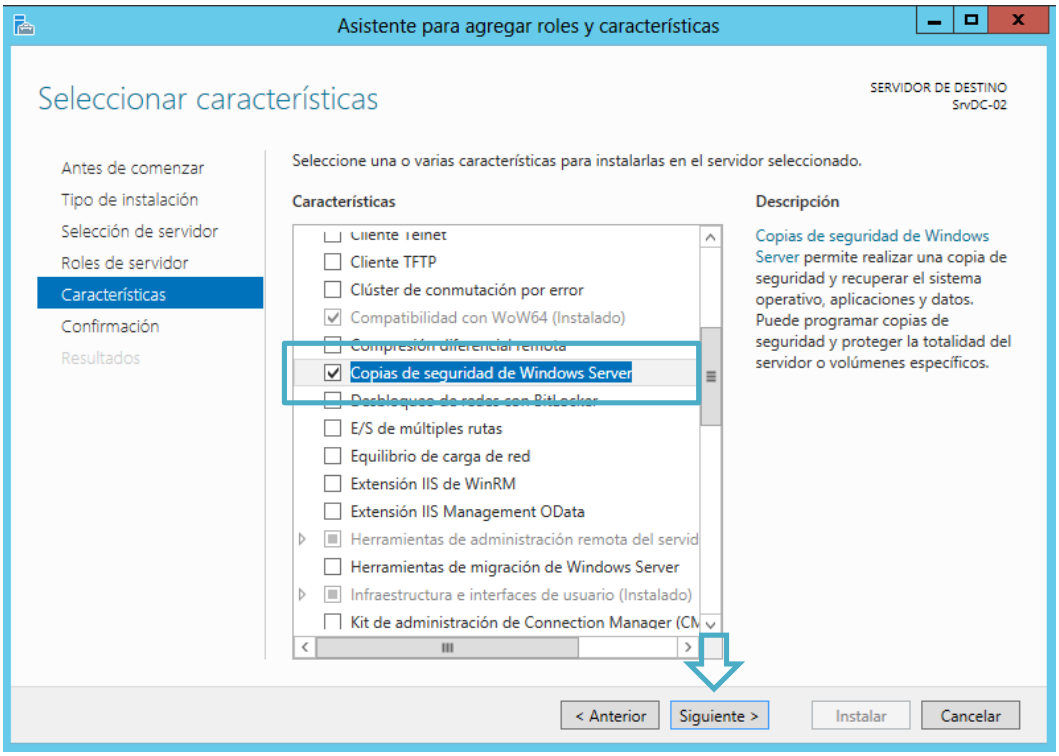


Figura 9. 24: Instalando características copia de seguridad

2. Al dar clic en siguiente aparece la ventana de confirmación como se muestra la figura 9.25, pulsamos en instalar.

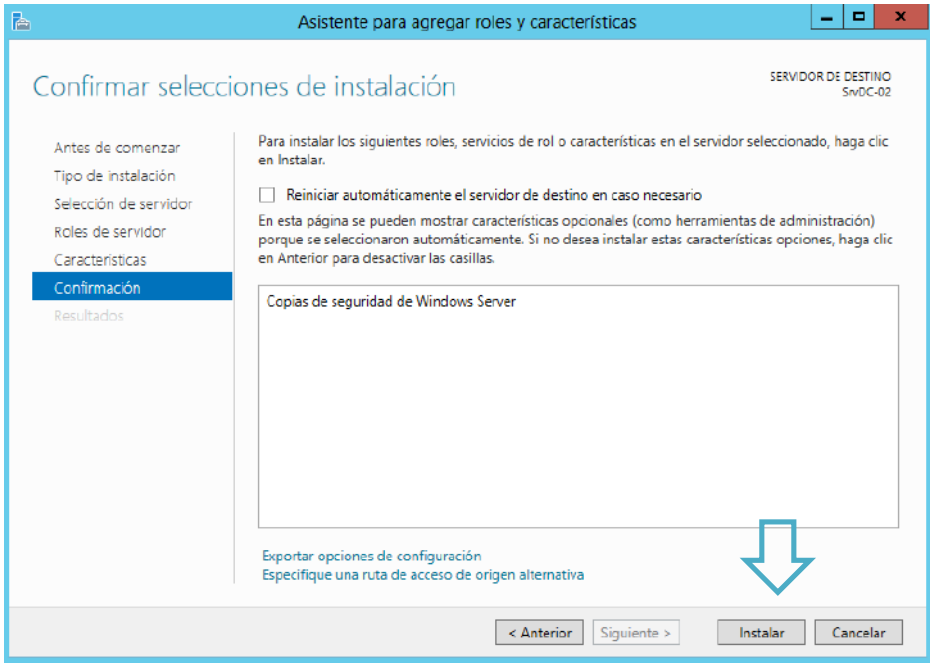


Figura 9. 25: Confirmación de la instalación

3. Al pulsar instalar, esperar hasta que instale y clic en cerrar, como se muestra la figura 9.26.

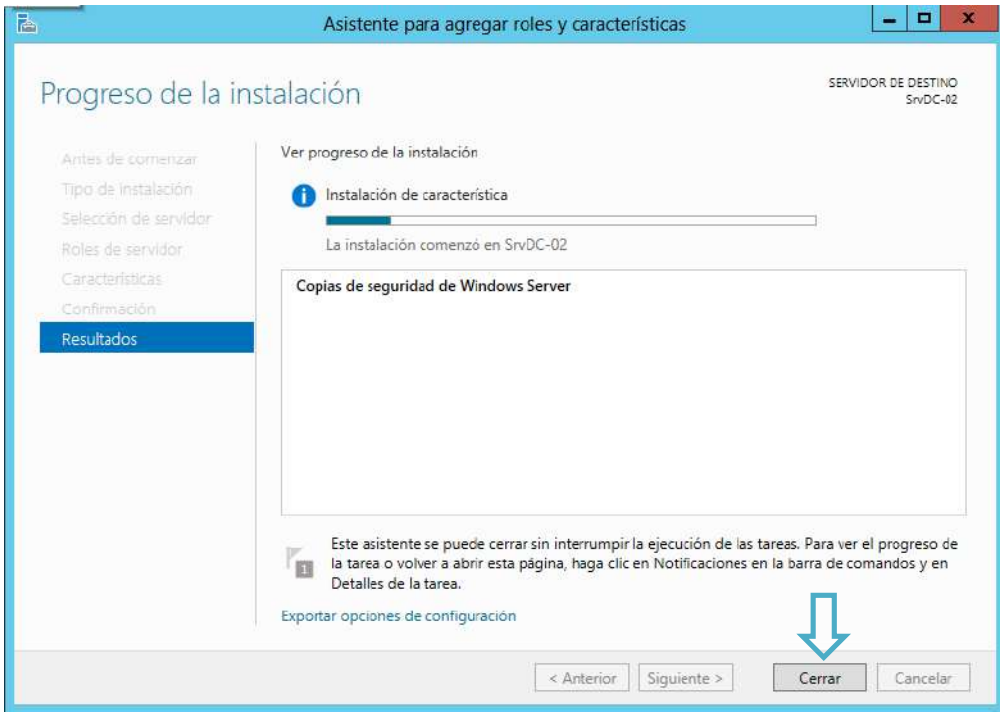


Figura 9. 26: Progreso de instalación de la copia de seguridad

4. Para abrir la copia de seguridad nos dirigirse en lado derecho del administrador de servidor, opción herramienta, mostrara un listado de opciones donde se escoge copia de seguridad de windows server como se muestra la figura 9.27.

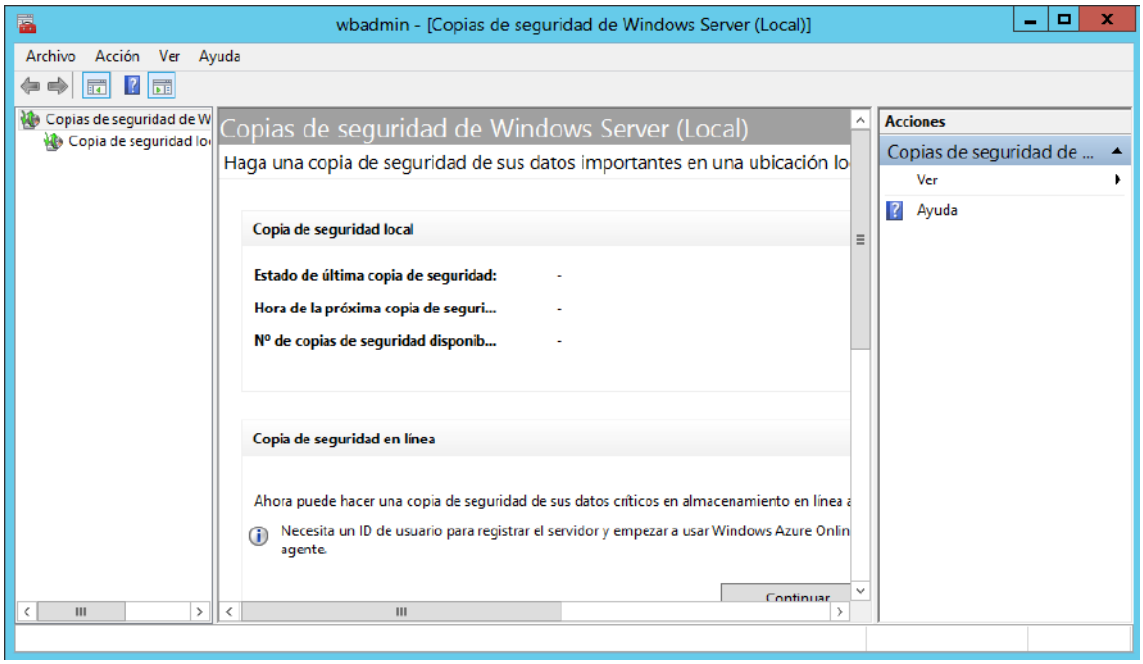


Figura 9. 27: Copia de seguridad de Windows Server

5. Para programar nuestras copias, dirigirse en el lado izquierdo, opción programar copia de seguridad como se muestra la figura 9.28.

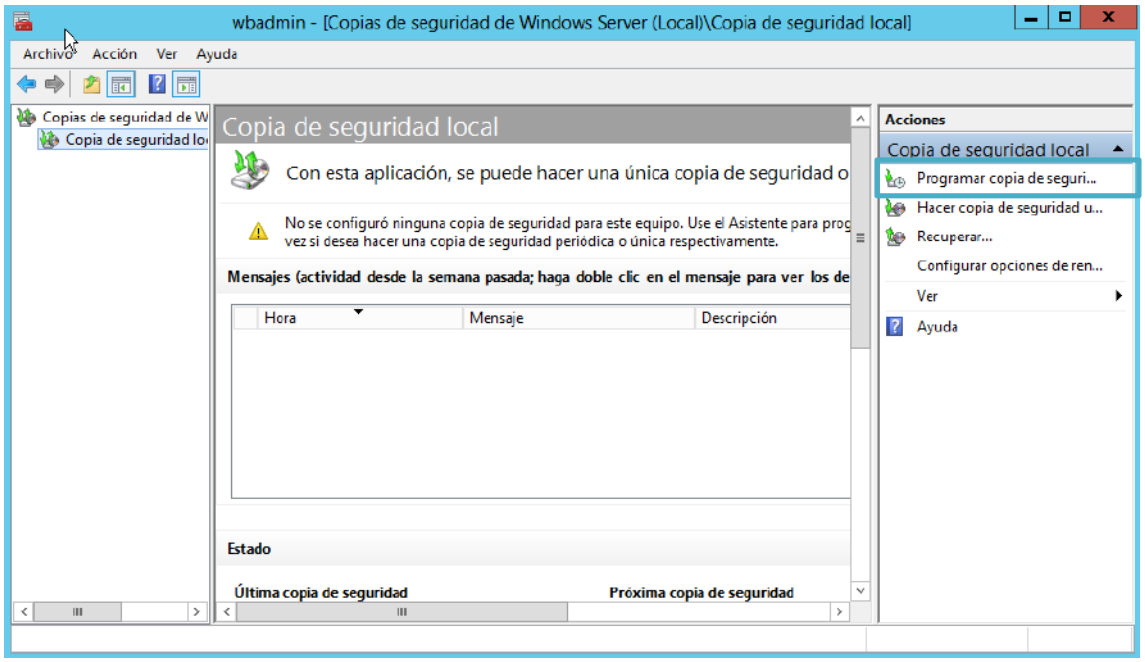


Figura 9. 28: Programar copia de seguridad

6. A continuación muestra el asistente para programar copia de seguridad, como se muestra la figura 9.29, dar clic en siguiente.

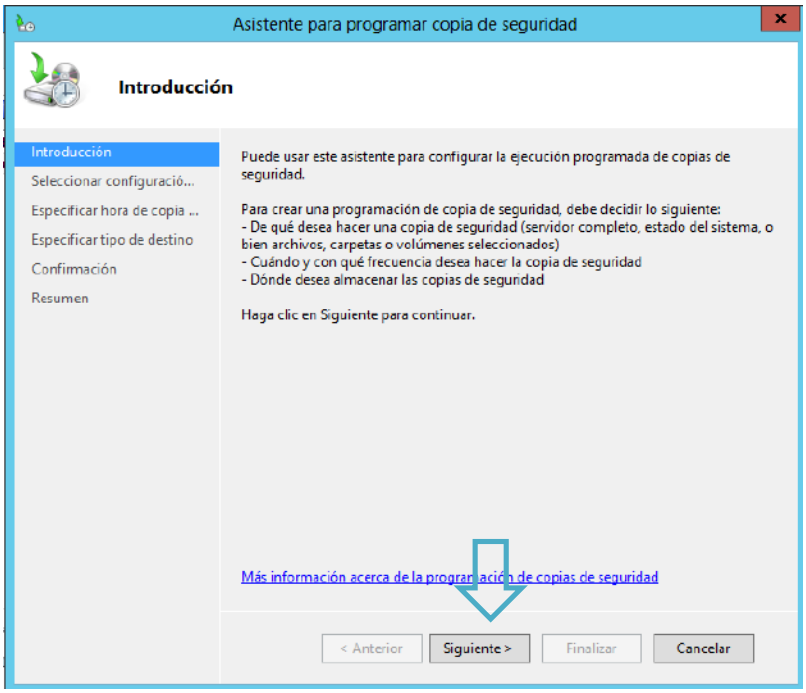


Figura 9. 29: Asistente para programar copia de seguridad

7. Elegir qué tipo de configuración desea programar, marcamos la opción personalizada como se muestra la figura 9.30, dar clic en siguiente.

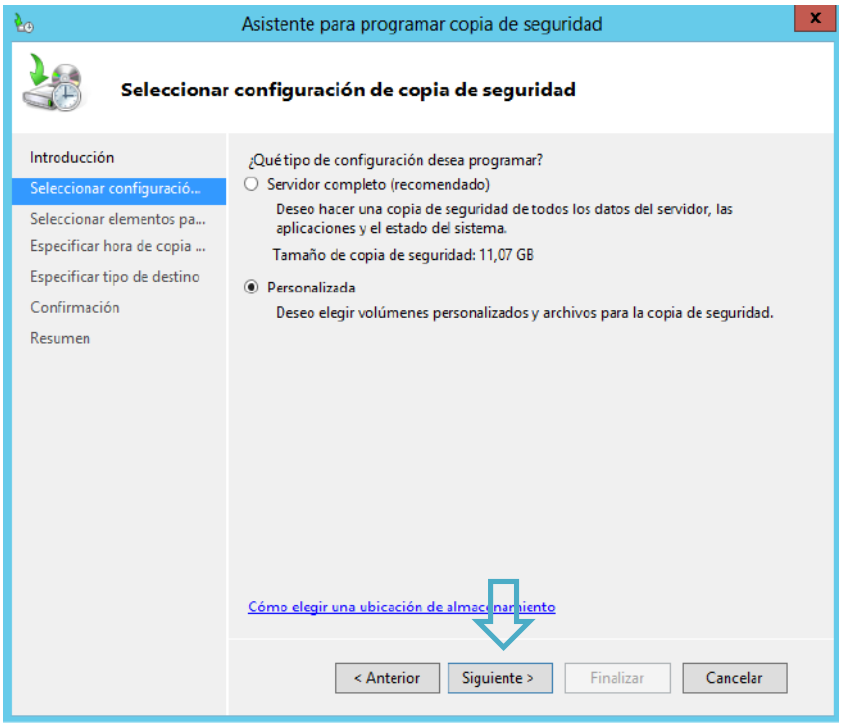


Figura 9. 30: Seleccionar tipo de configuración

8. Seleccionamos las opciones de recuperación (reconstrucción completa, estado del sistema y unidad C:\), que nos permitirán restaurar los archivos del sistema operativo en caso de una contingencia. Además, chequeamos el volumen de datos con los archivos que pretendemos respaldar (D:\), como se muestra la figura 9.31.

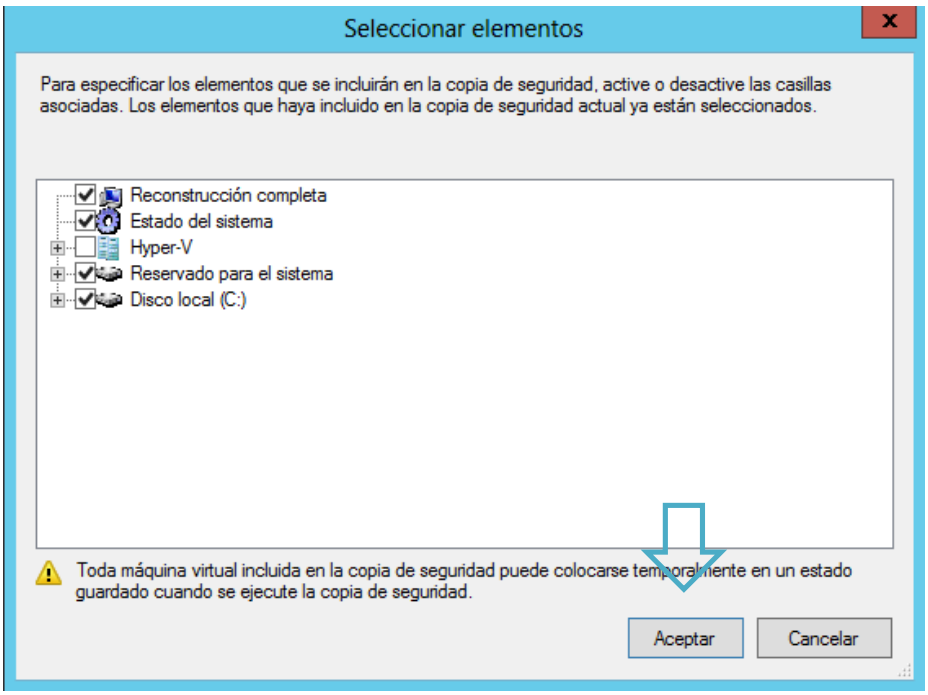


Figura 9. 31: Seleccionar elementos

9. Haciendo clic sobre el botón Configuración avanzada, en la pestaña Exclusiones es posible definir archivos y carpetas a evitar en el plan de copias. En este caso, hemos excluido del backup la carpeta $Recycle.bin, que almacena los archivos eliminados, luego dirigirse Configuración de VSS es posible configurar el sistema para que guarde o no los archivos de registro para las instantáneas de volumen, que podrían utilizar aplicaciones de terceros. Como no es nuestro caso, utilizamos la primera opción, para que el sistema los elimine, ver figura 9.32. (Salas, 2013)

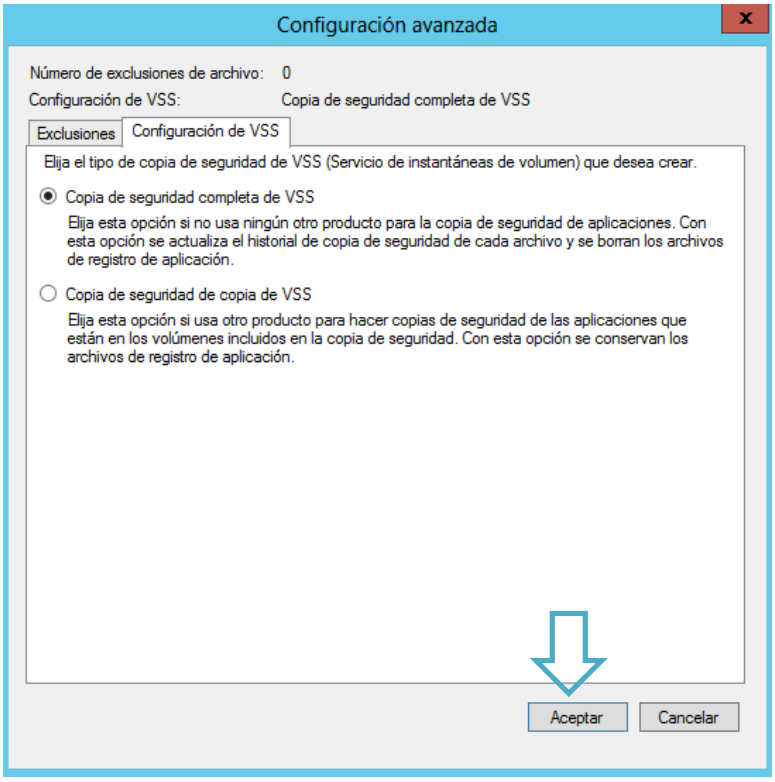


Figura 9. 32: Configuración avanzada

10. Tras pulsar el botón aceptar muestra una ventana donde debemos especificar la hora de copia de seguridad, en este caso elegí la opción una vez al día como se muestra la figura 9.33, dar clic en siguiente.

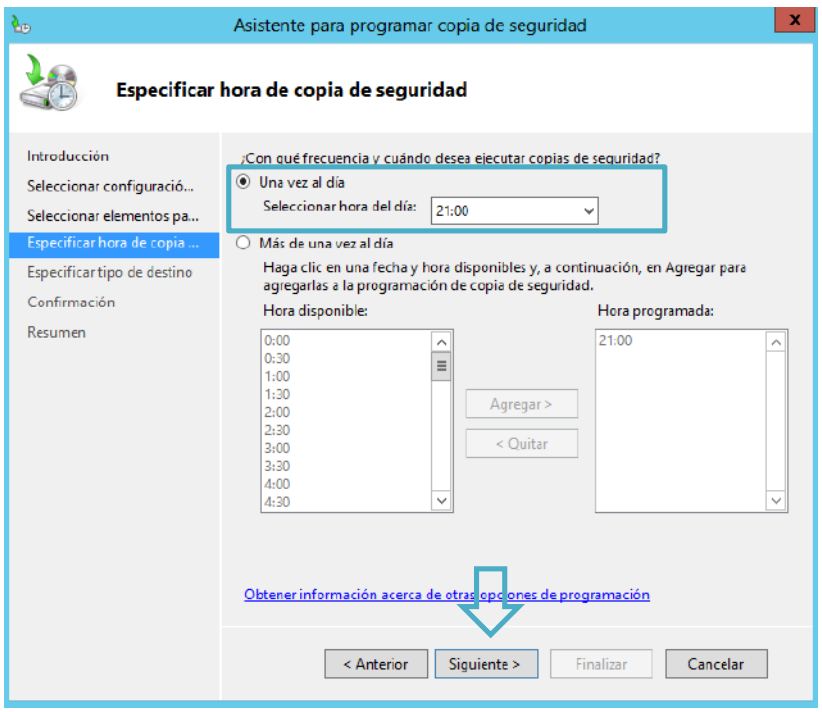


Figura 9. 33: Especificar hora de copia de seguridad

11. Finalmente se deberá seleccionar el destino de la copia. La opción más recomendada, por seguridad y rendimiento, es la realización de las copias de seguridad sobre un disco o conjunto de discos independientes. Así es como se muestra la figura 9.24.

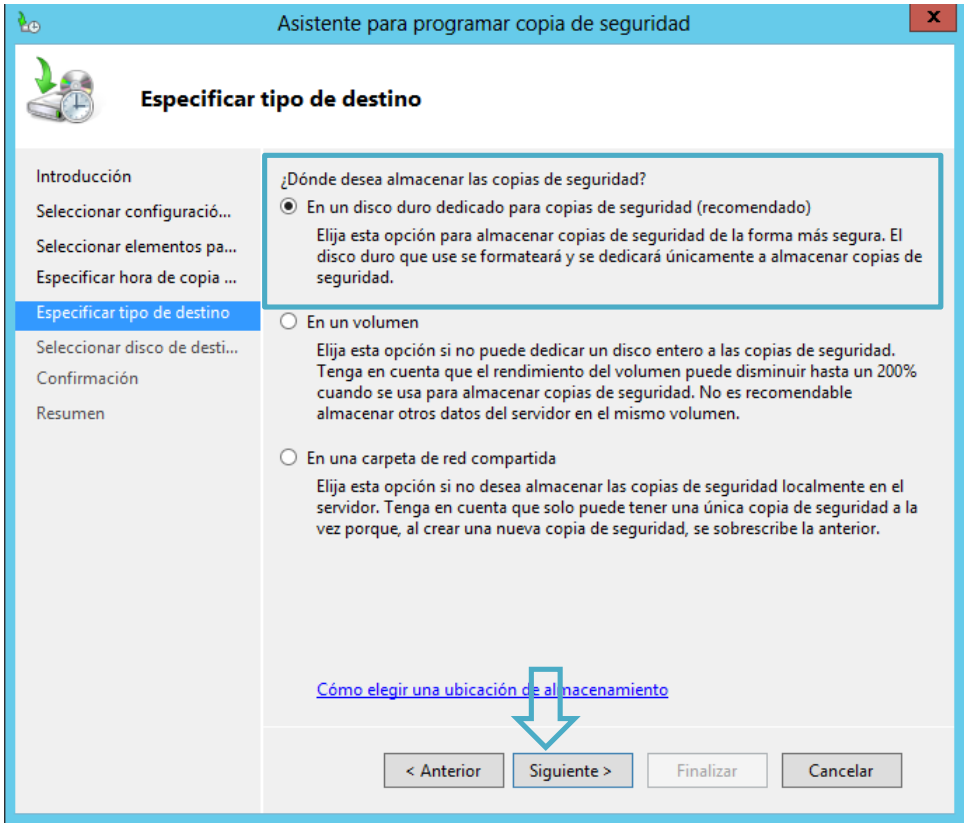


Figura 9. 34: Especificar tipo de destino

12. El asistente nos pedirá el disco de destino que queremos utilizar para las copias, pulsamos siguientes, luego mostrara los disco disponibles, confirmamos los datos y dar clic en finalizar, ya tenemos programado nuestra copia de seguridad.

Bibliografía

Microsoft. (24 de Marzo de 2017). Windows PE (WinPE). Obtenido de https://msdn.microsoft.com/es-es/library/windows/hardware/dn938389(v=vs.85).aspx

Morrison, B. (27 de Octubre de 2012). Windows 8 / Windows Server 2012: el nuevo administrador de tareas. Obtenido de https://technet.microsoft.com/askperf/2012/10/27/windows-8-windows-server-2012-the-new-task-manager/

Orin, T. (06 de Febrero de 2014). Administrar Windows Server 2012 R2: Monitor y auditoría. Obtenido de https://www.microsoftpressstore.com/articles/article.aspx?p=2217266&seqNum=2

Rosario, A. (11 de Septiembre de 2014). Windows Server 2012 - Firewall de Windows. Obtenido de https://www.point.com/windows_server_2012/windows_server_2012_firewall.htm

Rouse, M. (18 de Abril de 2014). Windows Server Backup. Obtenido de https://searchwindowsserver.techtarget.com/definition/Windows-Server-Backup

Salas, C. (30 de Octubre de 2013). Copia de seguridad en windows server 2012. Obtenido de http://www.expertosensistemas.com/copias-de-seguridad-en-windows-server-2012/

Smith, T. (25 de Octubre de 2012). Windows Server 2012 - Administrador de tareas. Obtenido de https://kb.iweb.com/hc/en-us/articles/230242348-Windows-Server-2012-Task-Manager

Zamora, D. (10 de Diciembre de 2016). Monitoreo de servidores en Windows Server 2012. Obtenido de www.solvetic.com/tutoriales/article/2514-monitoreo-de-servidores-en-windows-server-2012/

Unidad

V

Unidad X

WSUS distribución y administración de actualizaciones

10. Introducción a WSUS

Un servidor de actualizaciones es el encargado de coordinar las actualizaciones de Windows mediante el rol denominado WSUS. Su principal función es la de controlar que no halla sobrecarga en la red con las actualizaciones, descargándolas una vez y repartiéndolas por el resto de equipos en vez de que cada equipo descargue la suya.
"La función de WSUS (Windows Server Update Services) es recuperar los correctivos y actualizaciones del servidor de Microsoft con el objetivo de ponerlas a disposición de los distintos equipos de la red" (Bonnet, 2016).

Un servidor WSUS puede considerarse también como origen de actualización para otros servidores WSUS de una organización. En una implementación de WSUS, se debe tener por lo menos un servidor WSUS en una red debe estar conectado a Microsoft Update donde se podrá obtener información referente a actualizaciones disponibles, como se muestra la figura 10.1.

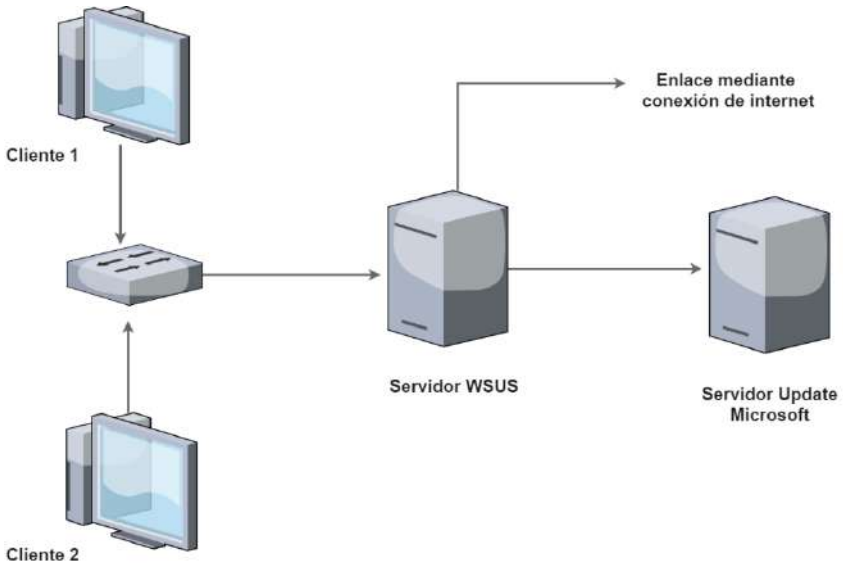


Figura 10. 1: Servidor WSUS

Windows Server Update Services (WSUS) permite a aquellos administradores de tecnologías de la información llevar acabo la implementación de las actualizaciones de los productos de Microsoft más recientes. Con WSUS, los administradores pueden administrar completamente la distribución de actualizaciones que publican en Microsoft Update para todos los equipos dentro de la red (Microsoft, 2018).

Para llevar a cabo WSUS se debe cumplir 3 etapas, que obligatoriamente se deben respetar.

10.1. Fase de identificación de actualizaciones a instalar.

Dentro de esta fase el obje car cuáles son las nuevas actualizaciones que se e ponibles. Al finalizar la configuración del servidor se necesita configurar cuáles serán los productos a actualizarse.

10.1.1. Fase de pruebas e instalación

Una vez finalizada la etapa de identificación de actualizaciones disponibles, se necesita aprobarlas. Es recomendable realizarlo en un grupo de máquinas de prueba que contienen instaladas varias aplicaciones utilizadas para la producción. La fase prueba y autenticación es indispensable, ya que nos permite asegurarnos de que no exista ningún problema en el sistema o en las aplicaciones después de instalar las correcciones.

10.1.2. Fase de despliegue

Una vez realizadas las pruebas y validadas las correcciones, se puede llevar acabo la instalación en los equipos de producción donde se requería la actualización. Es conveniente realizar la aprobación para el grupo o grupos disponibles.

10.2. Requisitos de instalación de WSUS

Entre los requisitos de instalación mínimos de hardware WSUS son:

Tabla 10. 1: Requisitos de instalación de WSUS

HARDWARE	REQUISITO
Procesador	Procesador x64 de 1,4 (GHZ)(Para mayor velocidad se recomienda 2GHZ o más)

Memoria	2 GB RAM más de lo que requiere el servidor
Espacio en disco	Mínimo 10 GB (Puede funcionar mejor con 40 GB O más)
Adaptador de red	Gabits 100 por segundo (MBPS) o superior

10.3. Instalación del rol del servidor WSUS

Primero debemos abrir el administrador de servidor y nos dirigimos a la opción Administrar dando clic Agregar roles y características, ver figura 10.2.

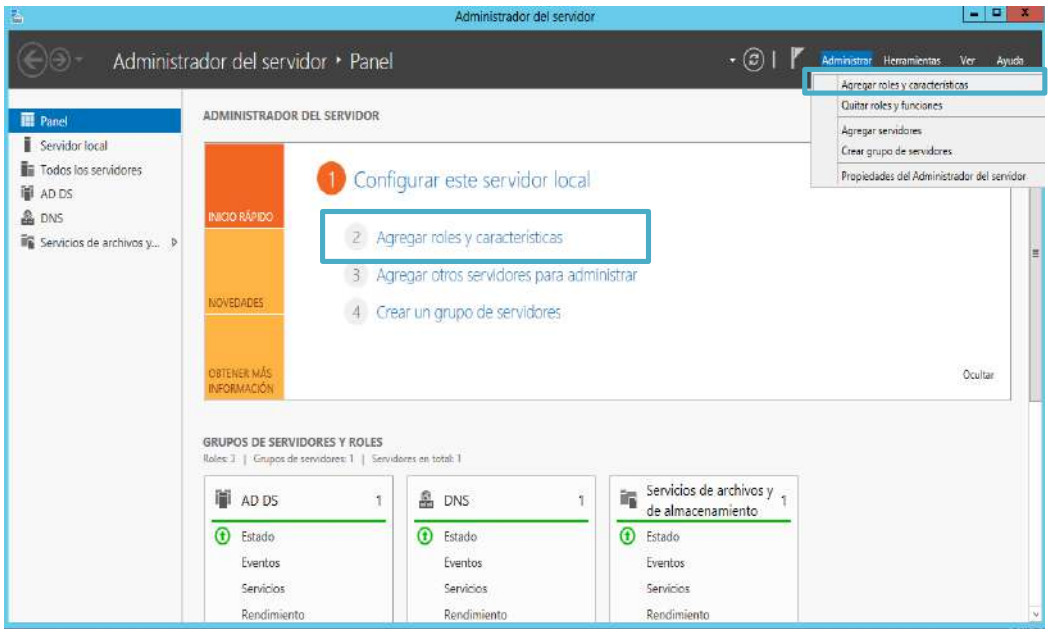


Figura 10. 2: Administrador del servidor

Nos mostrara la ventana de asistente para agregar roles y características y dar clic en siguiente, ver figura 10.3.

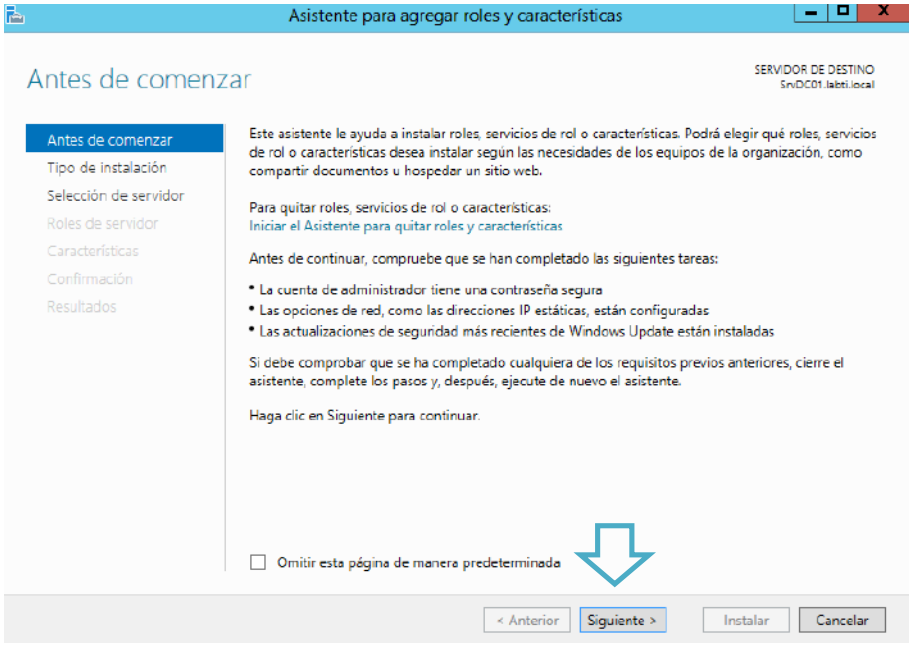


Figura 10. 3: Asistente para agregar roles y características

En la siguiente ventana debemos escoger el tipo de instalación y dejamos marcada la opción por defecto y dar clic en siguiente, ver figura 10.4.

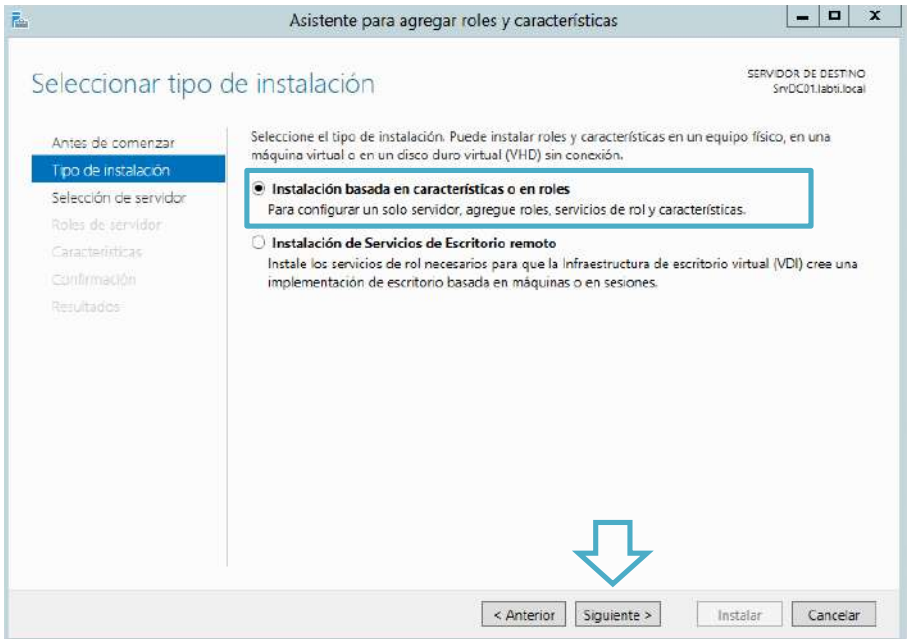


Figura 10. 4: Seleccionar tipo de instalación

A continuación, debemos escoger el servidor de destino en el que se va a instalar el rol de WSUS en nuestro caso será SrvDC01.labti.local y dar clic en siguiente, ver figura 10.5.

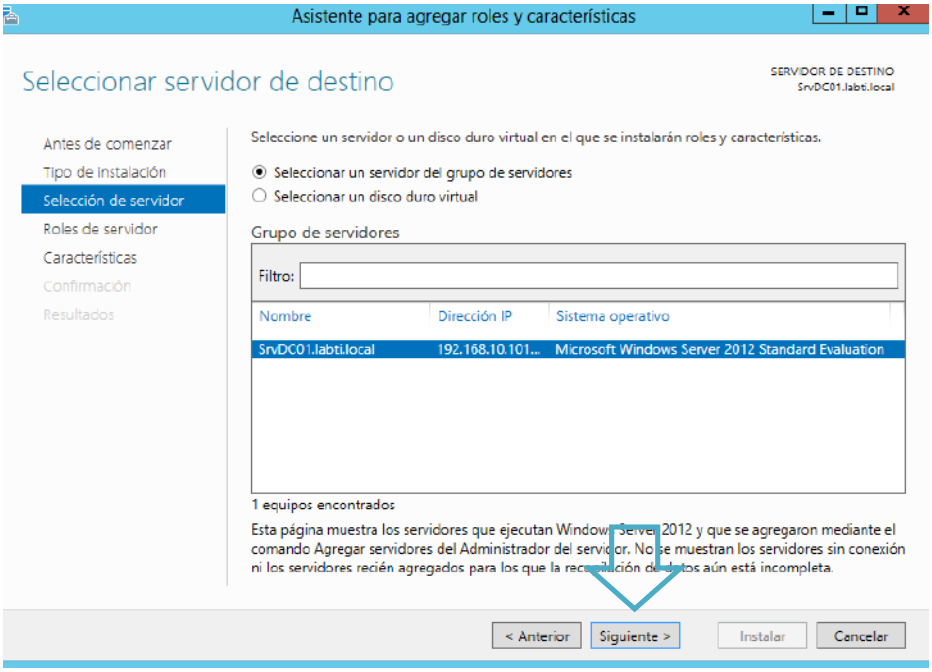


Figura 10. 5: Selección del servidor

En la siguiente ventana nos mostrara la lista de roles en el cual vamos hasta la última opción que es la Windows Server Update Services, ver figura 10.6.

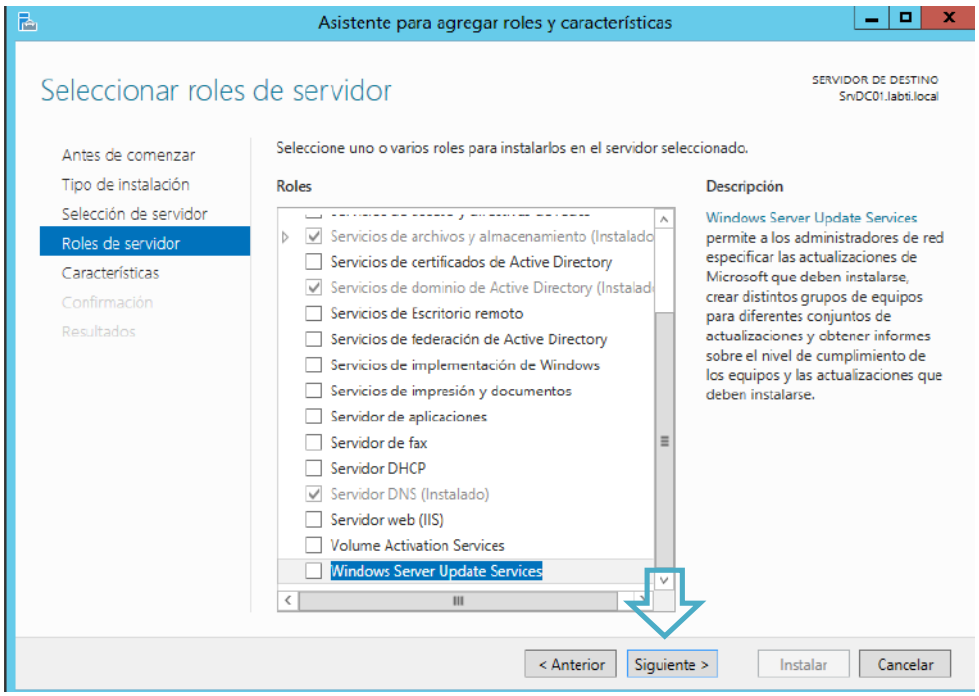


Figura 10. 6: Roles de servidor

Al dar clic en el rol nos mostrara otra ventana que nos indica las características que se deben agregar para el rol damos clic en agregar características y luego clic en siguiente, ver figura 10.7.

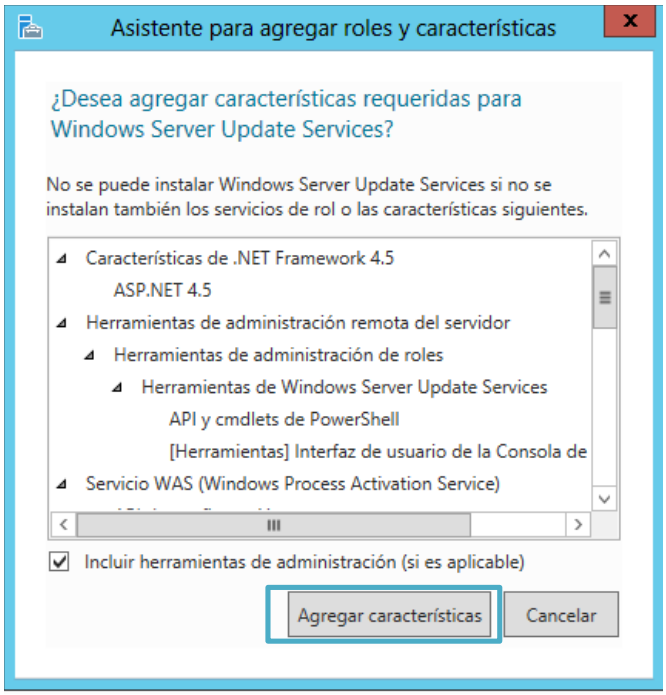


Figura 10. 7: Asistente para agregar roles y características

Luego nos permite seleccionar nuevas características en este caso dejamos marcadas las que están por defecto y dar clic en continuar, ver figura 10.8.

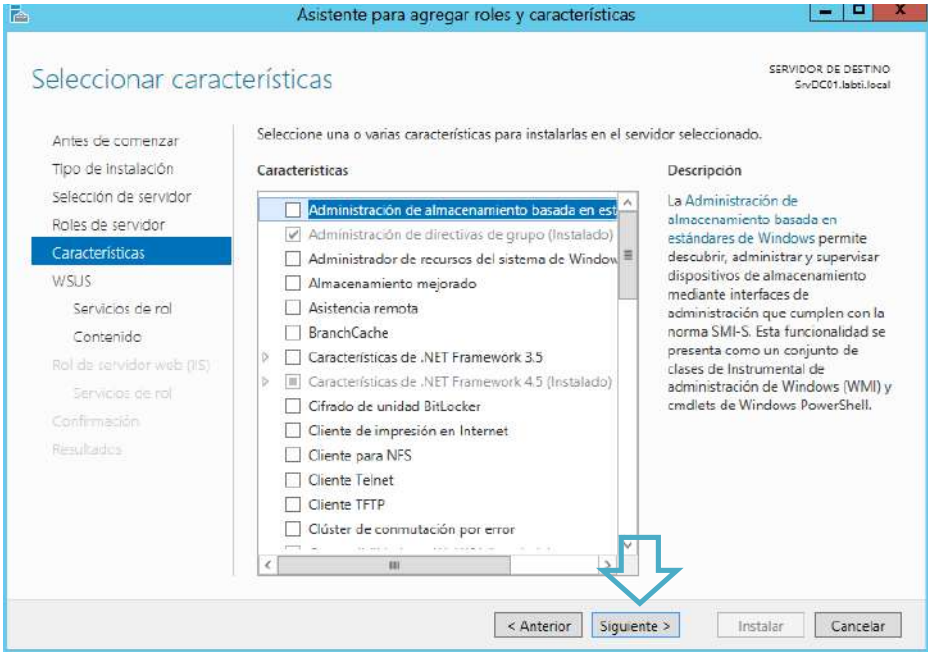


Figura 10. 8: Características de roles

En la siguiente ventana nos muestra que se inicia a configurar el rol WSUS y nos muestra las observaciones que debemos tener en cuenta y luego dar clic en siguiente, ver figura 10.9.

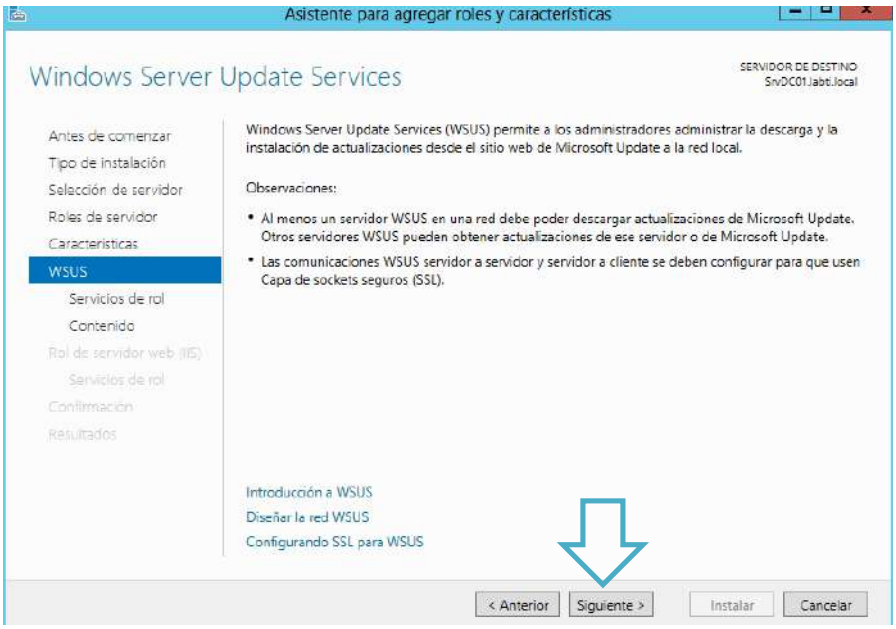


Figura 10. 9: Windows Server Update Services

En la siguiente ventana, debemos dejar las opciones que vienen ya por defecto, ya que la última opción, sería para instalar la base de datos sobre un servidor de base de datos ya integrado en nuestra red como este no es el caso se deja solo las por defecto y dar clic en siguiente, ver figura 10.10.

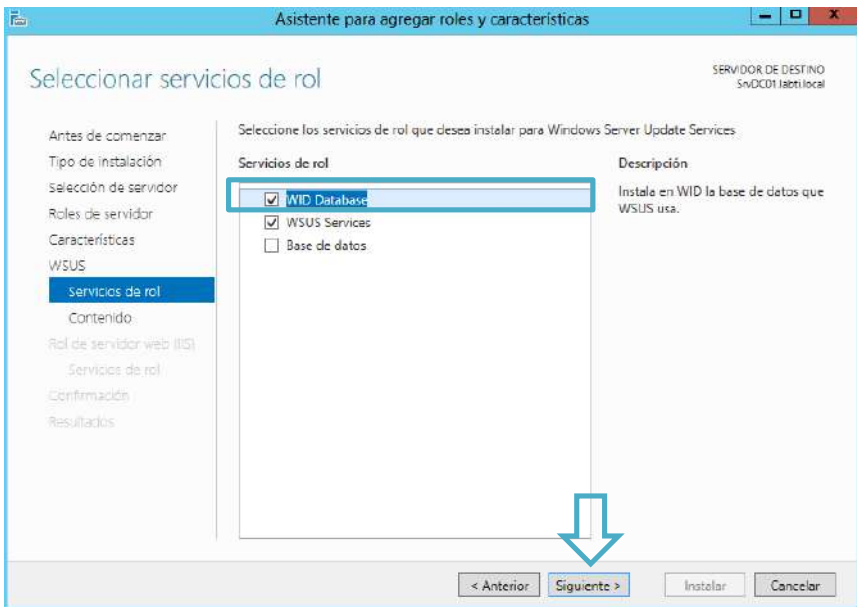


Figura 10. 10: Seleccionar servicios de rol

La siguiente ventana será la de selección de ubicación de contenido en el cual debemos dejar seleccionada la opción y en el siguiente cuadro debemos escribir la ruta en donde se almacenarán en cache las actualizaciones y dar clic en siguiente, ver figura 10.11 y 10.12.

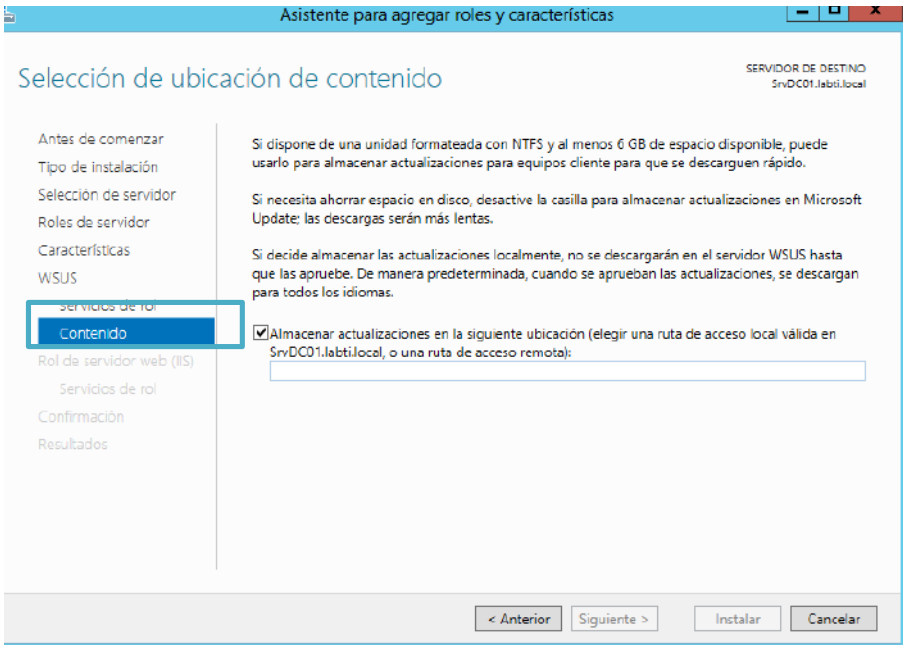


Figura 10. 11: Selección de ubicación de contenido

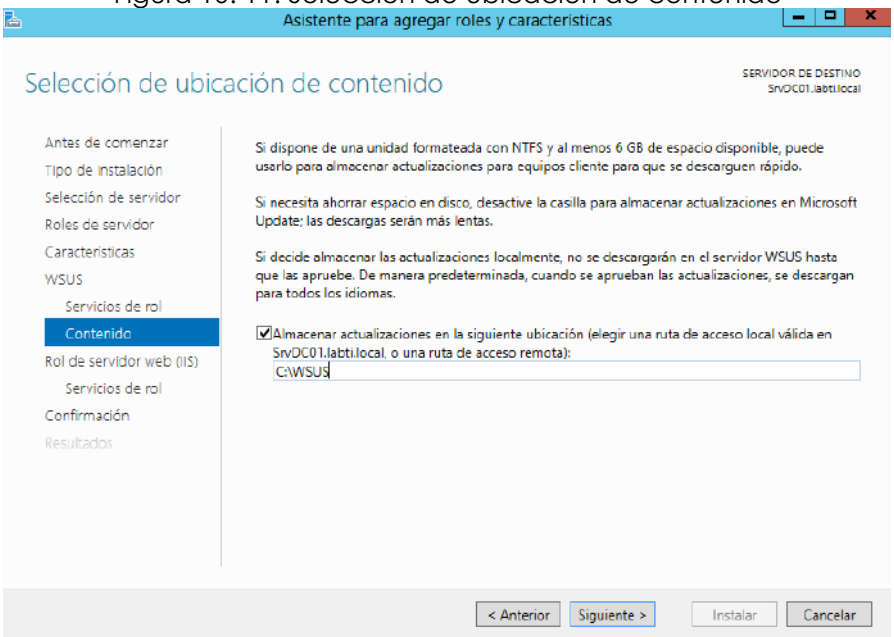


Figura 10. 12: Ubicación de contenido

Una vez indicada la ruta en la siguiente ventana nos pedirá la configuración del servidor web ya que es fundamental para el WSUS, para guardar la configuración dar clic en siguiente, ver figura 10.13.

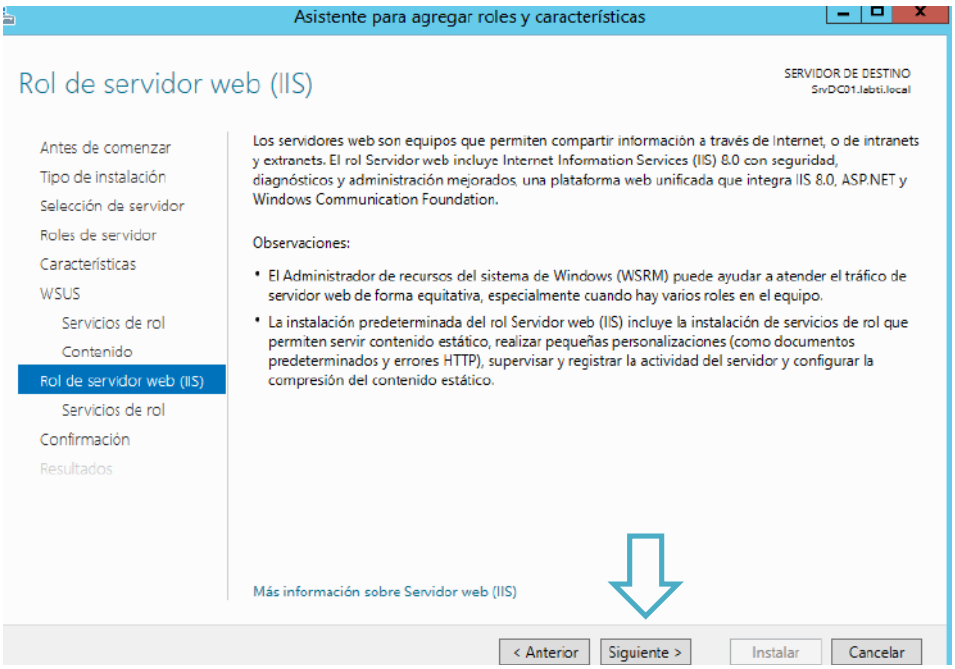


Figura 10. 13: Rol de servidor web IIS

Nos pedirá que confirmemos la instalación del rol para ello dejamos por defecto como esta y dar clic en siguiente, ver figura 10.14.

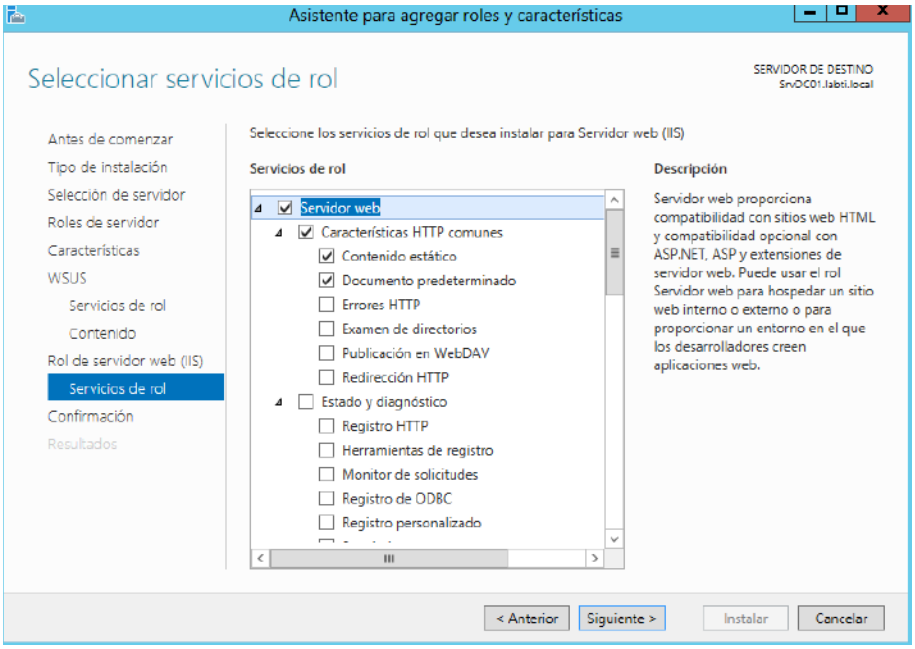


Figura 10. 14: Servicios de rol

En la siguiente ventana tenemos los servicios de rol a instalar, pero en este caso debemos dejar por defecto las opciones marcadas y dar clic en instalar, ver figura 10.15.

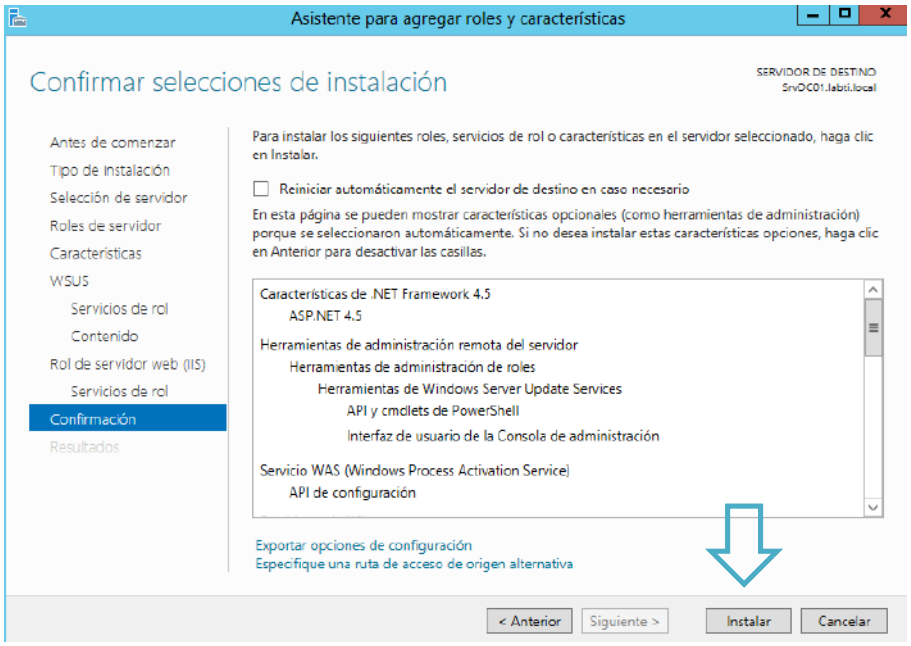


Figura 10. 15: Confirmar selecciones de instalación

Luego de la configuración del rol, iniciara la instalación y en esta ventana nos mostrara el progreso de instalación, ver figura 10.16.

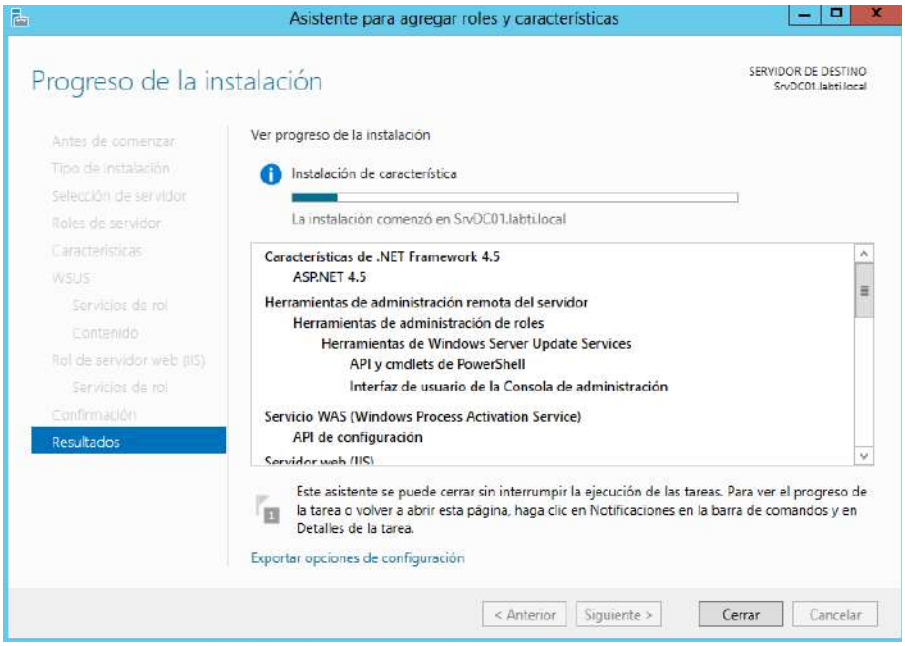


Figura 10. 16: Progreso de la instalación

Una vez finalizada la instalación del servicio, debemos realizar la configuración de WSUS para ello dar clic en iniciar tareas posteriores a la instalación, ver figura 10.17.

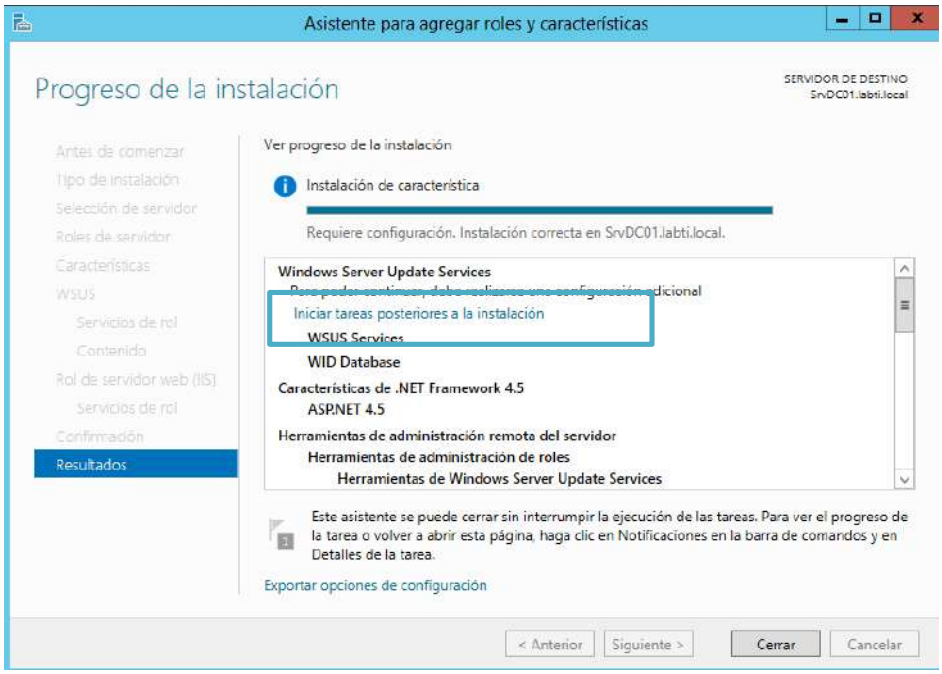


Figura 10. 17: Iniciar tareas posteriores a la instalación

Una vez que demos clic para iniciar las tareas de instalación nos mostrara un mensaje que nos indica que se está configurando el servidor, una vez finalizado la configuración nos dirá que esta correcta la instalación y daremos clic en cerrar como se muestra la figura 10.18.

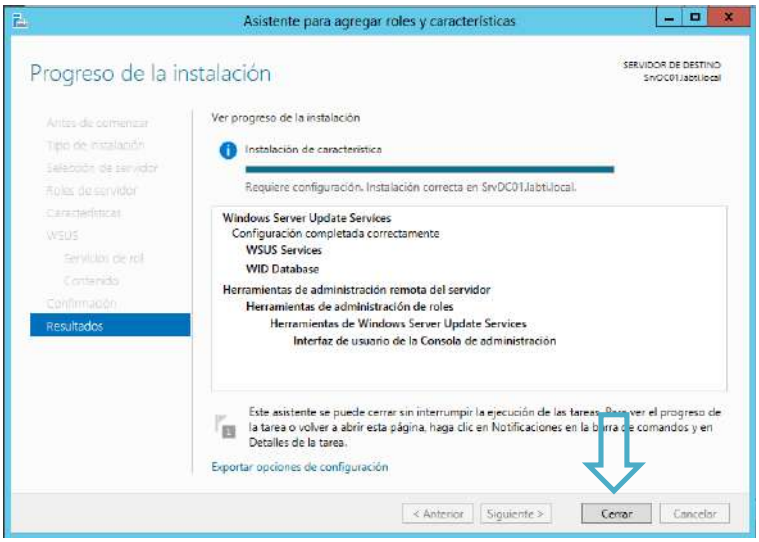


Figura 10. 18: Resultado de la instalación

10.4. Configurando el servidor WSUS

Para realizar la configuración del servidor nos vamos al administrador de servicios en la opción herramienta y buscamos la opción Windows server Update Services figura 10.19.

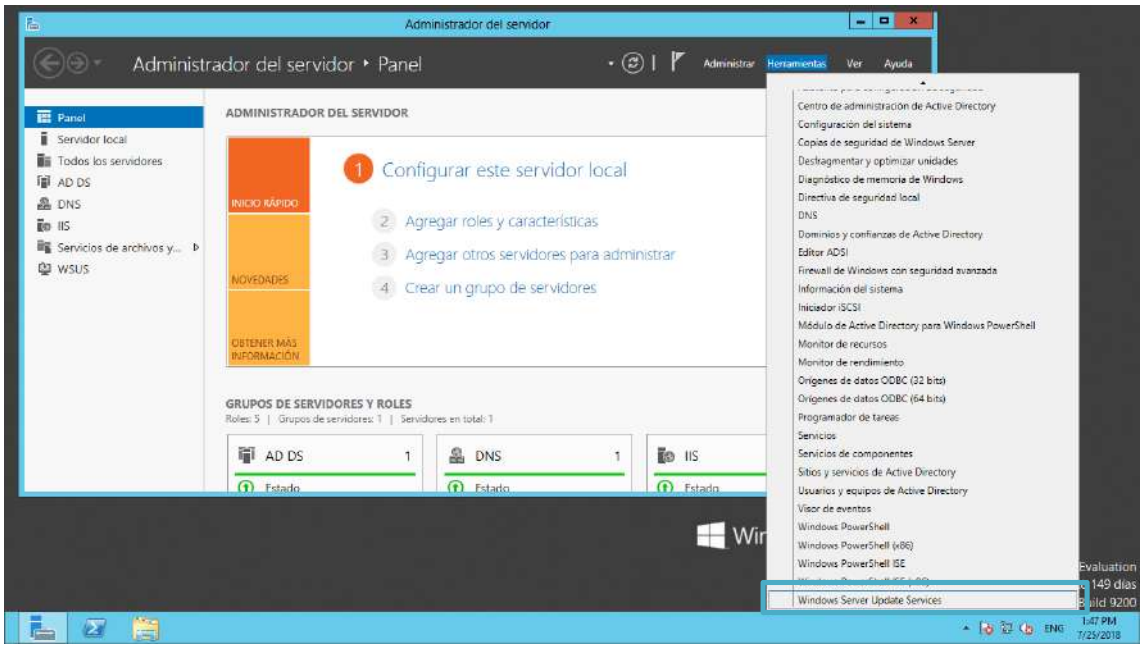


Figura 10. 19: Herramientas

Al dar clic se nos abrirá la ventana de asistente para la configuración de WSUS donde se dará clic en siguiente, ver figura 10.20.

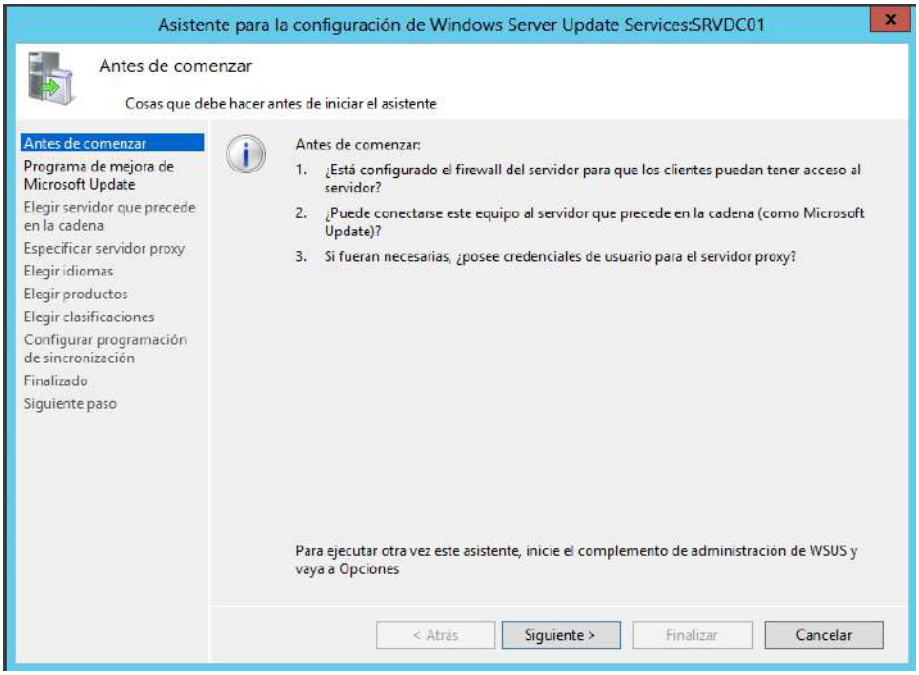


Figura 10. 20: Asistente para la configuración de Windows Server Update

En la siguiente ventana nos preguntara si deseamos participar en el programa de mejora de Windows Update, marcaremos la casilla y dar clic en siguiente, ver figura 10.21.

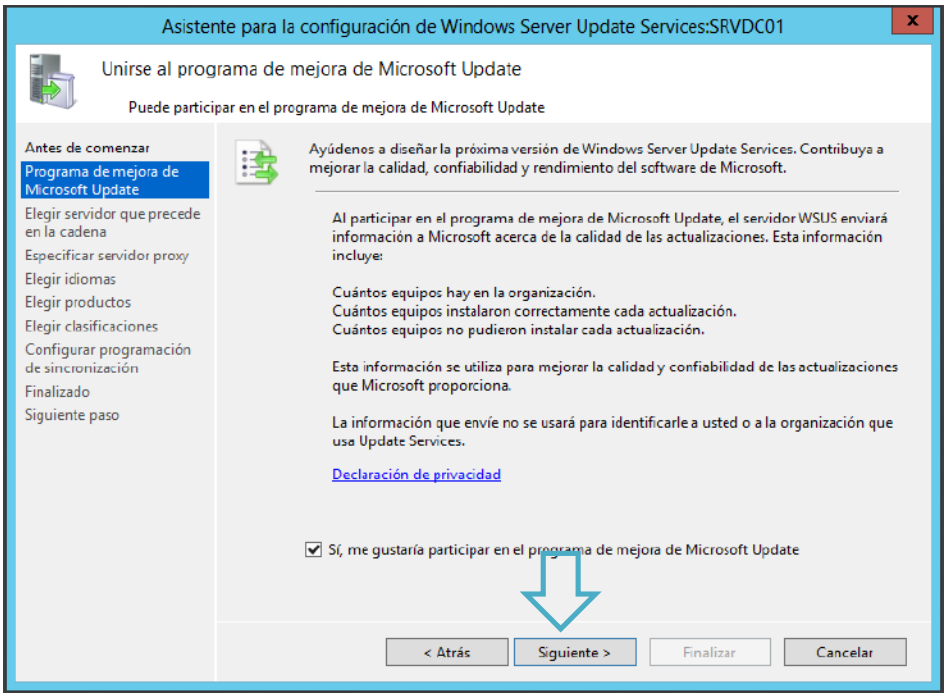


Figura 10. 21: Programa de mejora de Microsoft Update

En la siguiente ventana nos pedirá elegir el servidor que procede en la cadena, en este caso dejamos marcada la opción por defecto y dar clic en siguiente, ver figura 10.22.

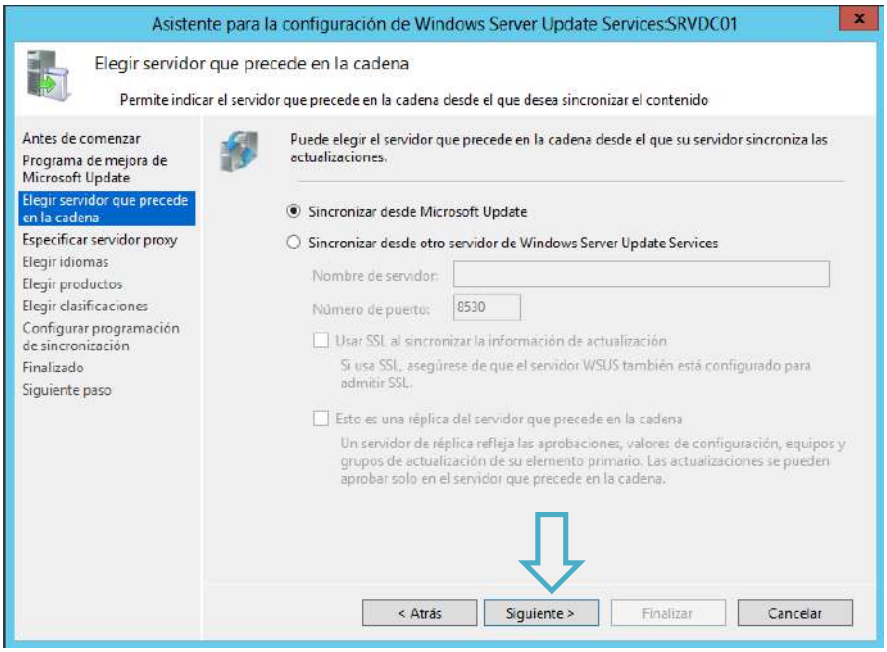


Figura 10. 22: Elegir servidor que precede en la cadena

En la siguiente ventana nos pedirá especificar a qué servidor desea conectarse. Si el servidor requiere de un servidor proxy para poder acceder a Microsoft Update o depende de otro servidor de forma ascendente, se podría realizar las configuraciones del servidor proxy dentro de esta ventana; de lo contrario, se dará clic en siguiente, ver figura 10.23.

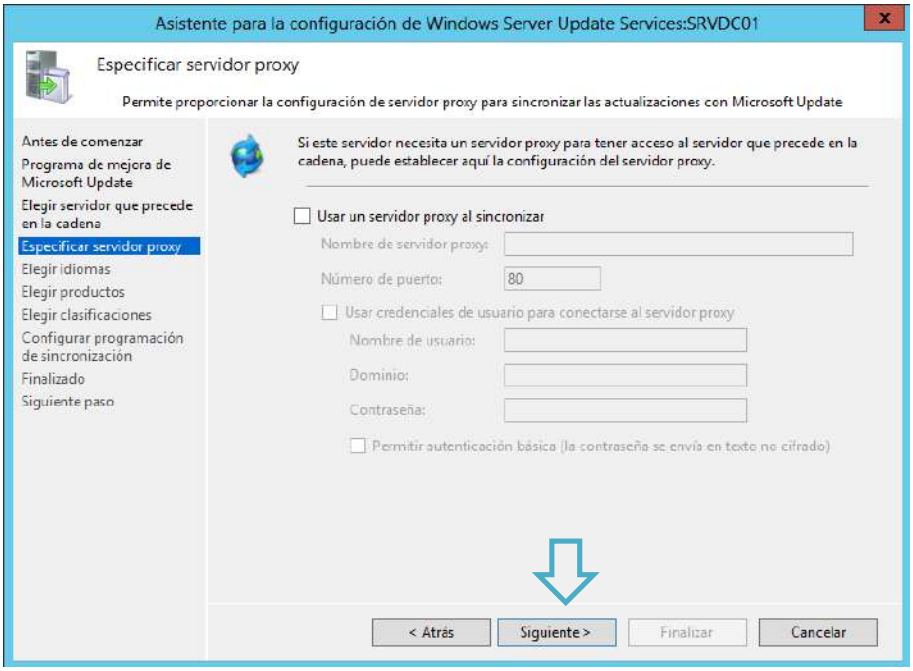


Figura 10. 23: Especificar servidor proxy configuración

En esta siguiente ventana deberemos dar clic en iniciar conexión para poder conectarse al servidor que procede la cadena, ver figura 10.24 y 10.25.

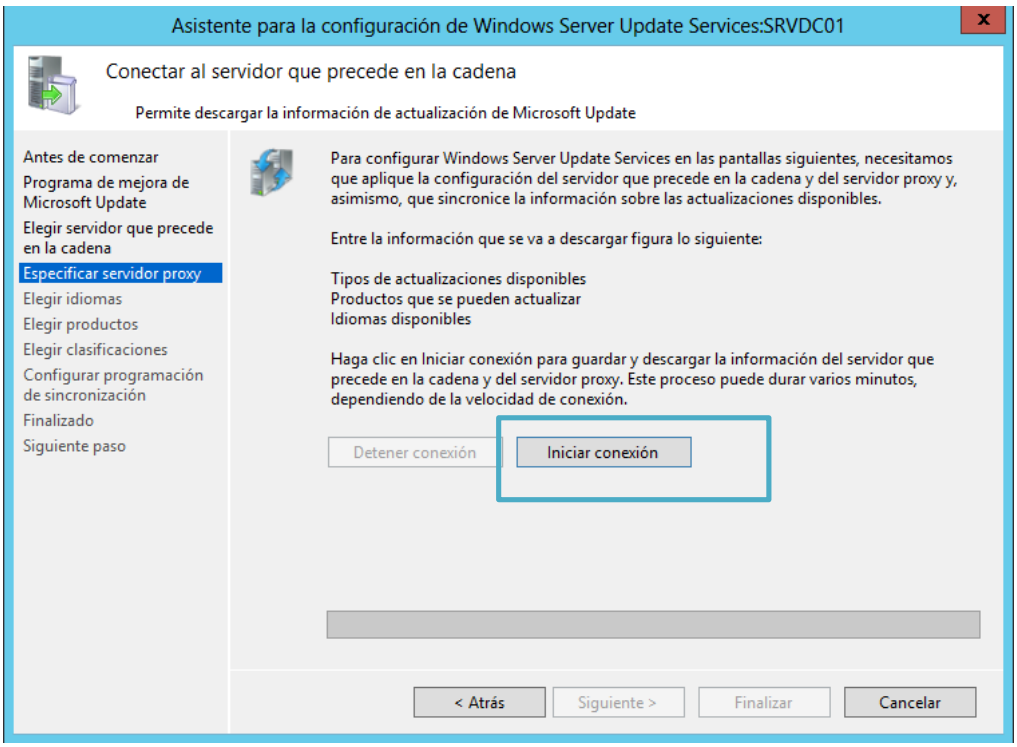


Figura 10. 24: Permite descargar la información en el servidor proxy

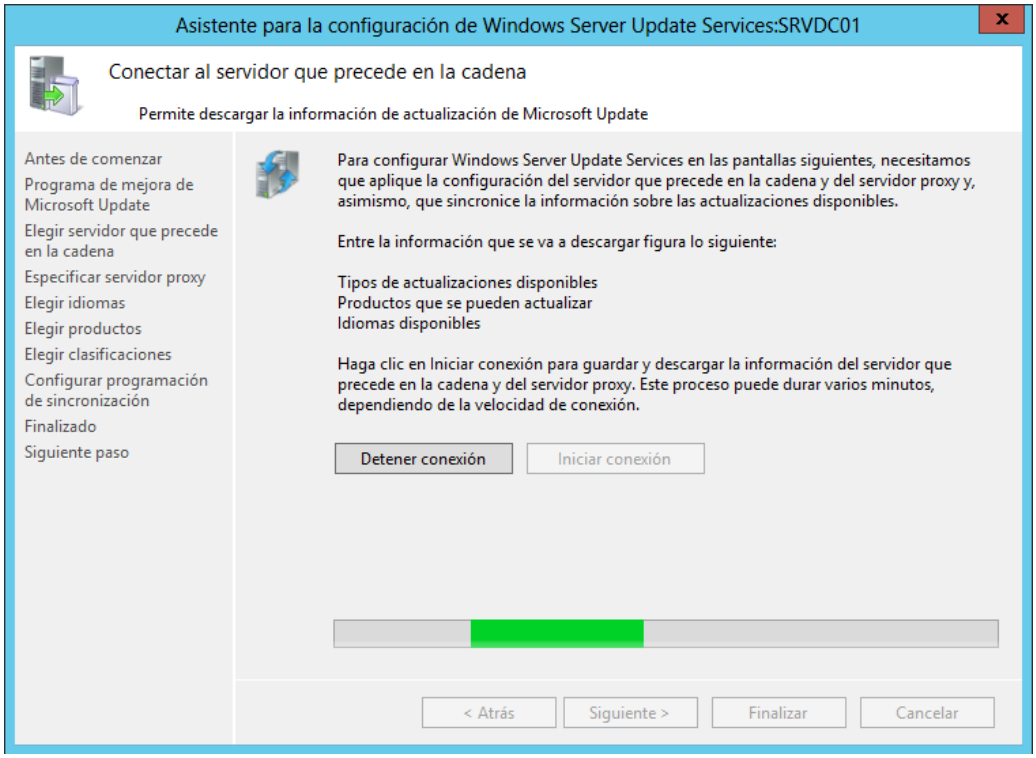


Figura 10. 25: Cargando las conexiones del servidor proxy

Una vez realizada la conexión y está tenga éxito dar clic en siguiente, ver figura 10.26.

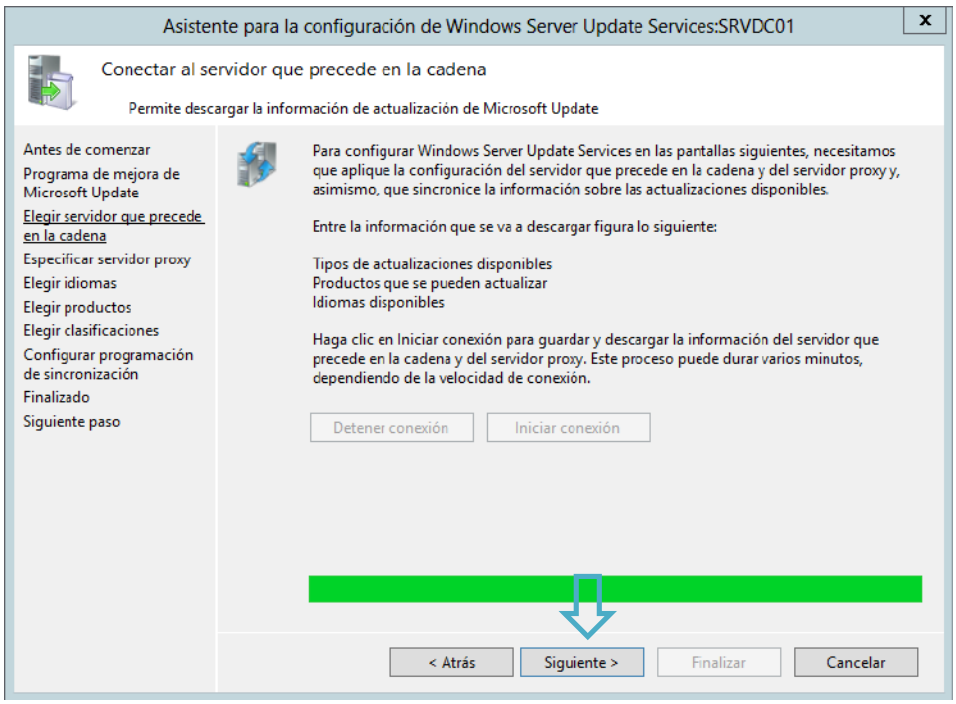


Figura 10. 26: Completando la conexión

En esta ventana debemos escoger el idioma en que se desean descargar las actualizaciones en este caso escogeremos español y dar clic en siguiente, como se muestra la figura 10.27.

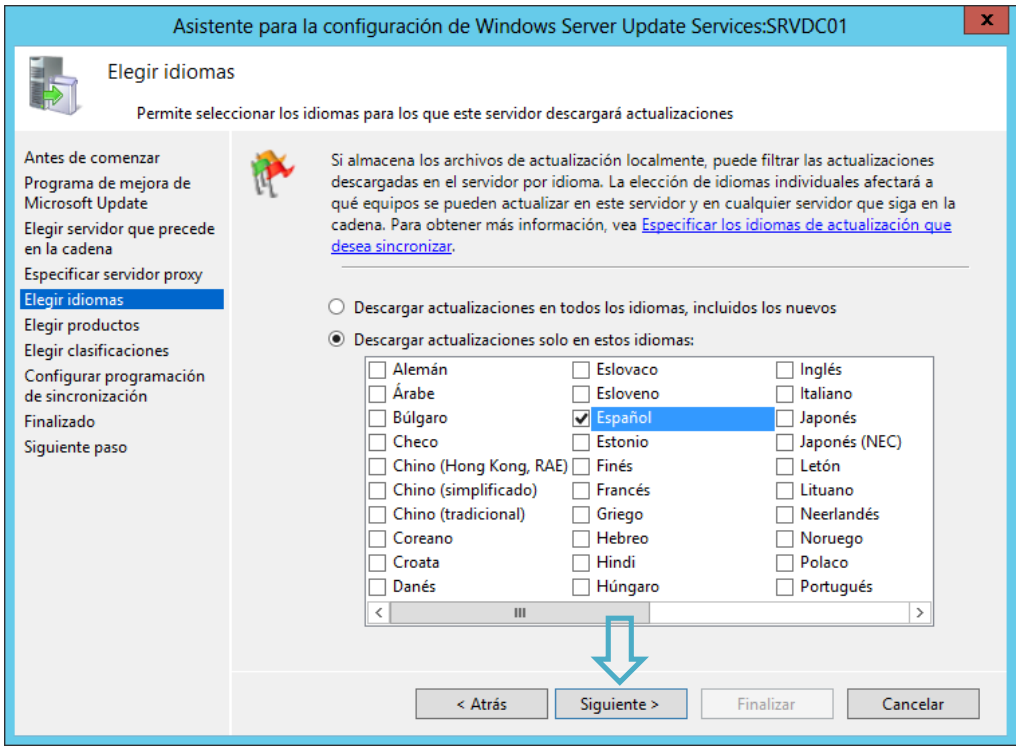


Figura 10. 27: Elegir idioma

En este paso se procederá a elegir los productos a actualizar, una vez marcados dar clic en siguiente, ver figura 10.28.

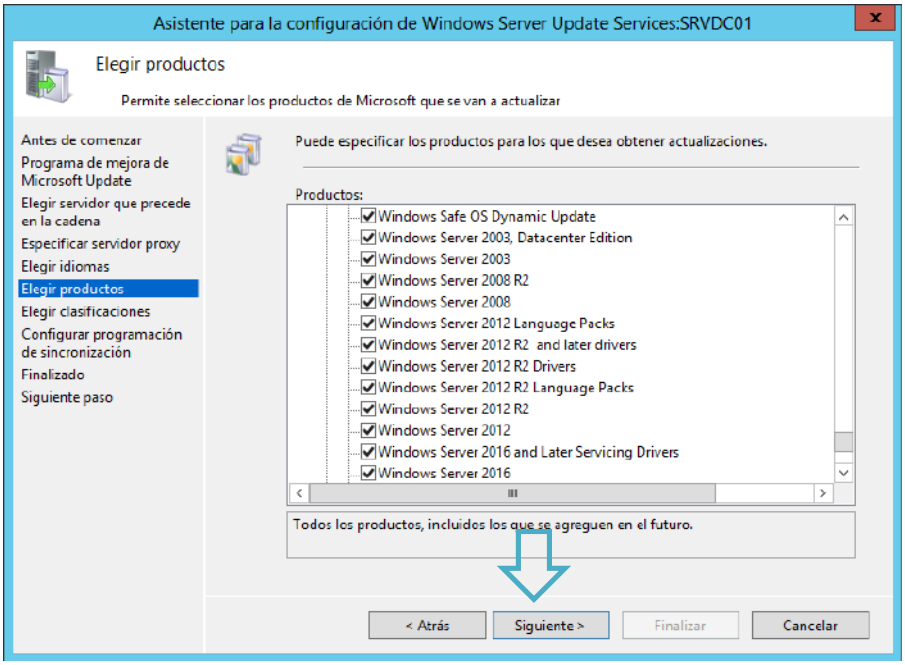


Figura 10. 28: Elegir productos

Marcamos la clasificación de actualizaciones que deseamos que se sincronicen y dar clic en siguiente, ver figura 10.29.

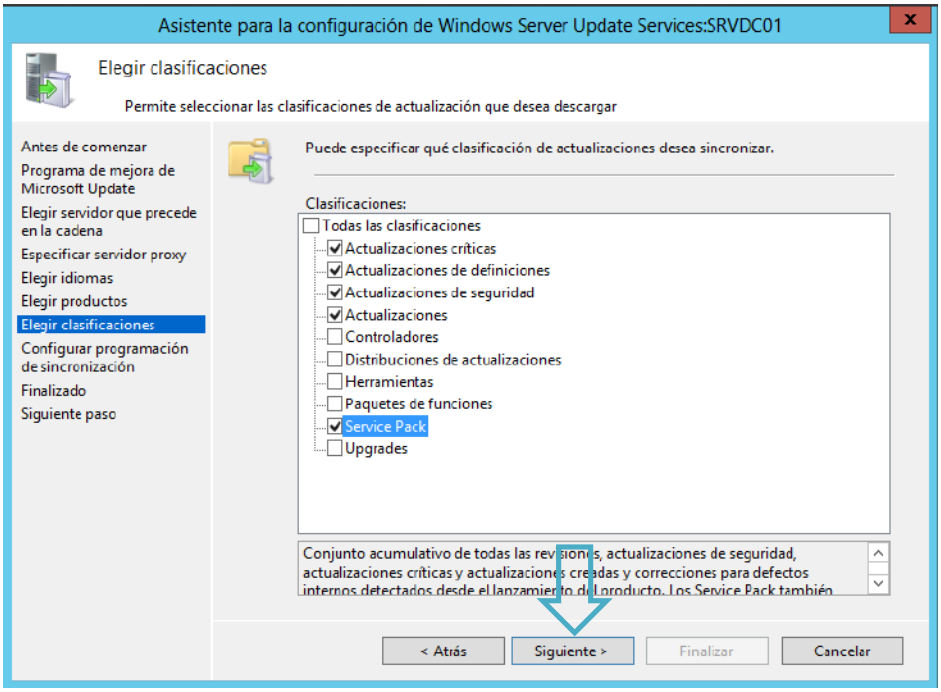


Figura 10. 29: Elegir clasificaciones

En la siguiente ventana dejamos marcada la opción de sincronizar manualmente y dar clic en siguiente, ver figura 10.30.

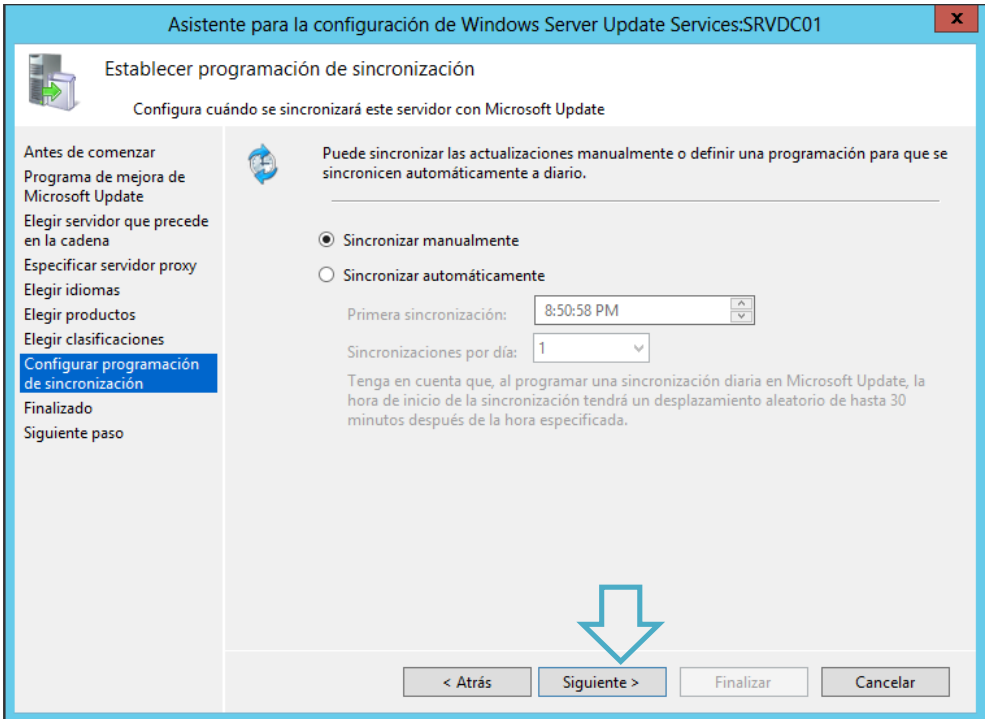


Figura 10. 30: Configurar programación de sincronización

En la siguiente ventana daremos clic en iniciar sincronización inicial, ver figura 10.31.

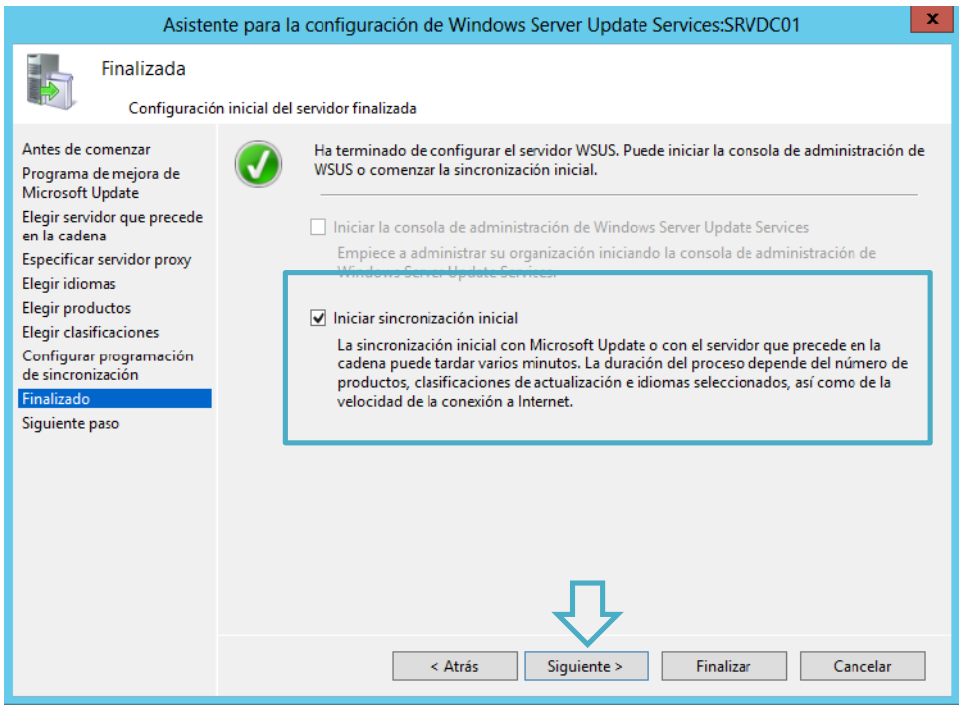


Figura 10. 31: Finalizando

Para finalizar la configuración dar clic en finalizar, ver figura 10.32.

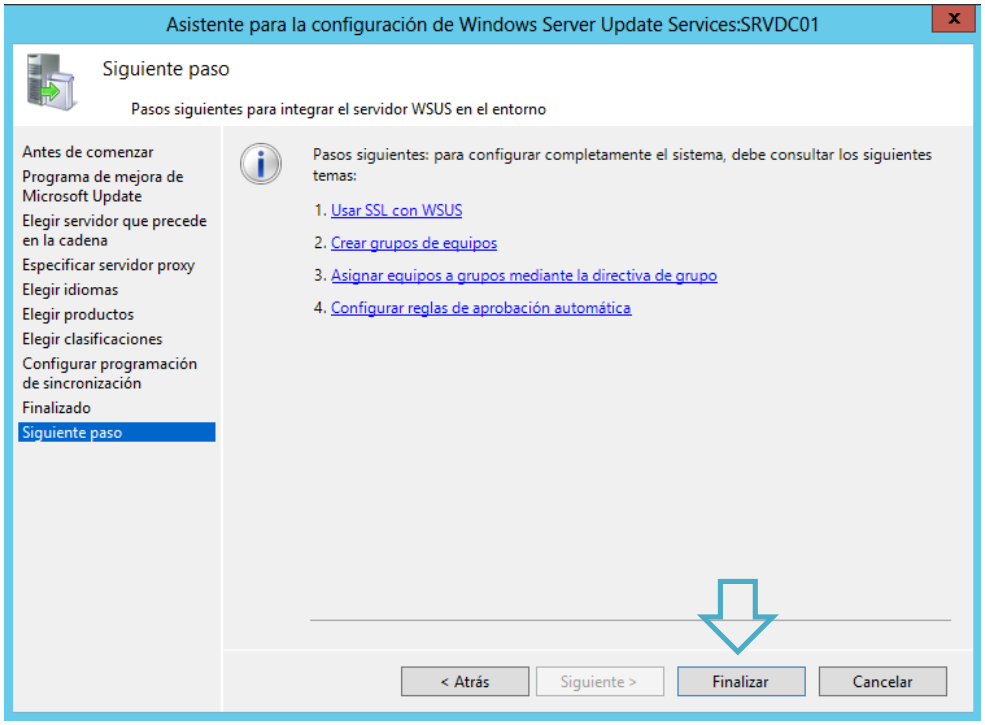


Figura 10. 32: Ingresar el servidor WSUS en el entorno

Al finalizar se nos abrirá la ventana de sincronización, esperamos a que termine la configuración que realizamos en el asistente, ver figura 10.33.

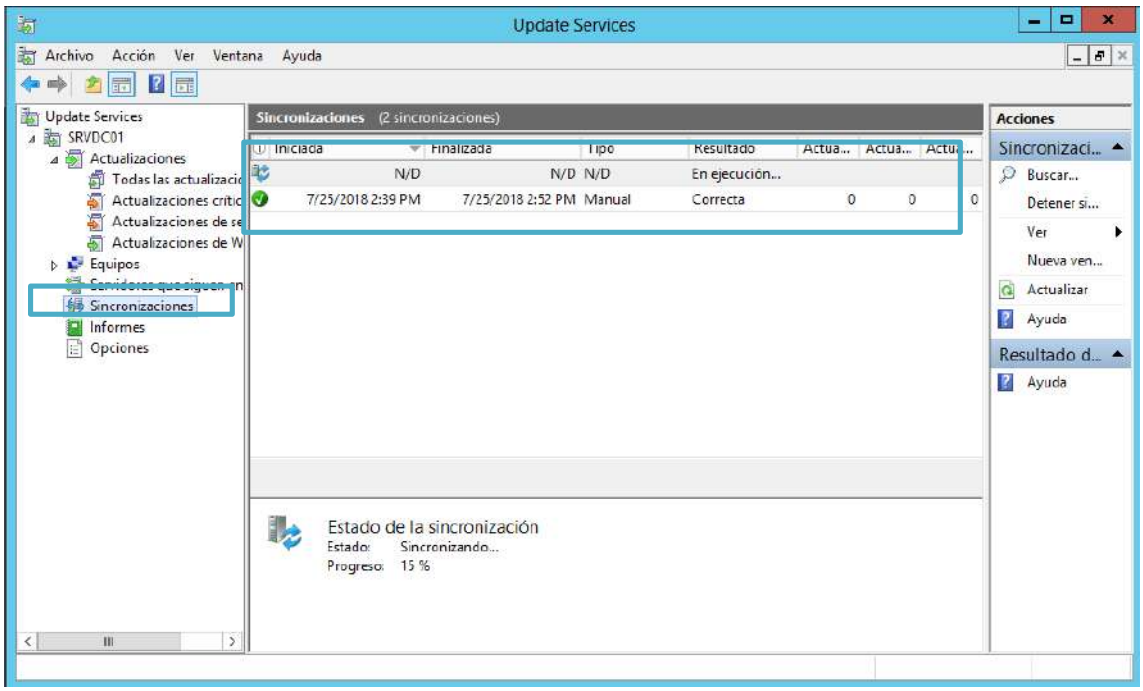


Figura 10. 33: Servicios de actualizaciones

Bibliografía

Bonnet, N. (2016). Windows Server 2012 R2. (N. Bonnet, Ed.). Ediciones ENI.

Microsoft. (2018). Introducción a Windows Server Update Services. Retrieved July 10, 2018, from https://msdn.microsoft.com/es-es/library/hh852345(v=ws.11).aspx

Unidad VI

Unidad XI

Zona Desmilitarizada

11. Instalación y configuración de servidor web en Windows 2012

Un servidor de base de Datos se utiliza para almacenar, recuperar y administrar los datos de una base de datos. El servidor gestiona las actualizaciones de datos, puede permitir el acceso simultáneo de muchos servidores o usuarios web y garantiza la seguridad y la integridad de los datos. En donde MySQL es la base de datos más famosa de alojamiento web la cual está diseñada para funcionar con lenguaje de programación PHP y sus servicios.

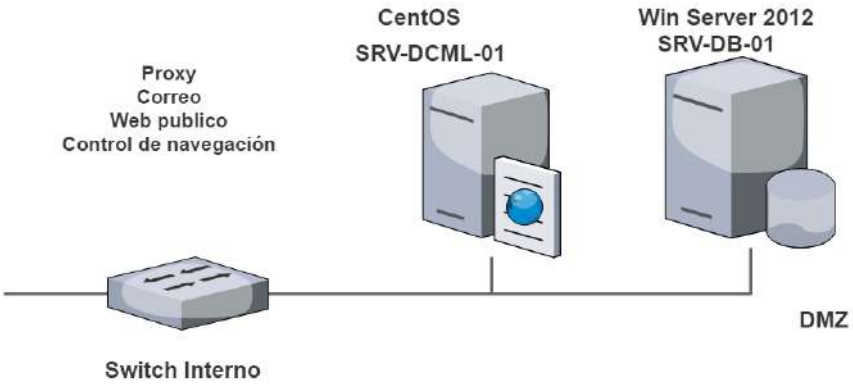


Figura 11. 1: Esquema zona desmilitarizada

¿Sabías Qué?

las webs personales. Obteniendo sitios más dinámicos y llenos de funcionalidades. Así pues, para instalar una plataforma de CMS es necesario un servidor web, base de datos y lenguaje programación. Los más comunes utilizan servidores con base de Datos MySQL y lenguaje de programación PHP.

Para la instalación de un servidor web es necesario realizar una serie de pasos:

- ✓ Paso 01-Instalar My SQL
- ✓ Paso 02- Instalar PHP
- ✓ Paso 03-Instalar servicios del Servidor Web (IIS)

11.1. Paso 01-Instalar My SQL

Para instalar My SQL en la computadora se debe ingresar a la página mysql.com y descargar MySQL para Windows. Lo más recomendable al momento de descargar es utilizar la opción "comunity". Como se observa en la Figura 11.2.

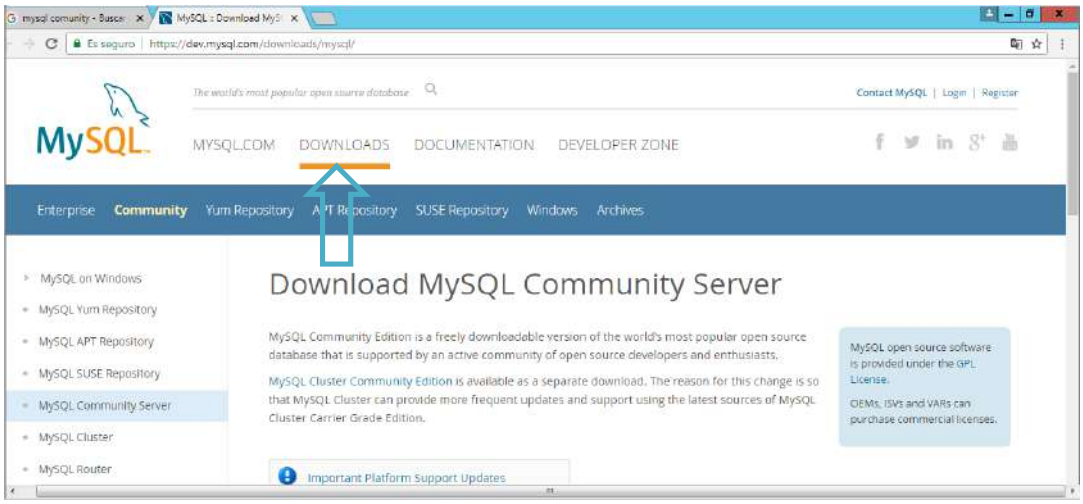


Figura 11. 2: Descarga de MySQL Comunity

Una vez descargado MySQL en la Pc debe ser instalada como se muestra:

1. Se deben aceptar los términos y condiciones de licencia .Como se observa en la Figura 11.3.

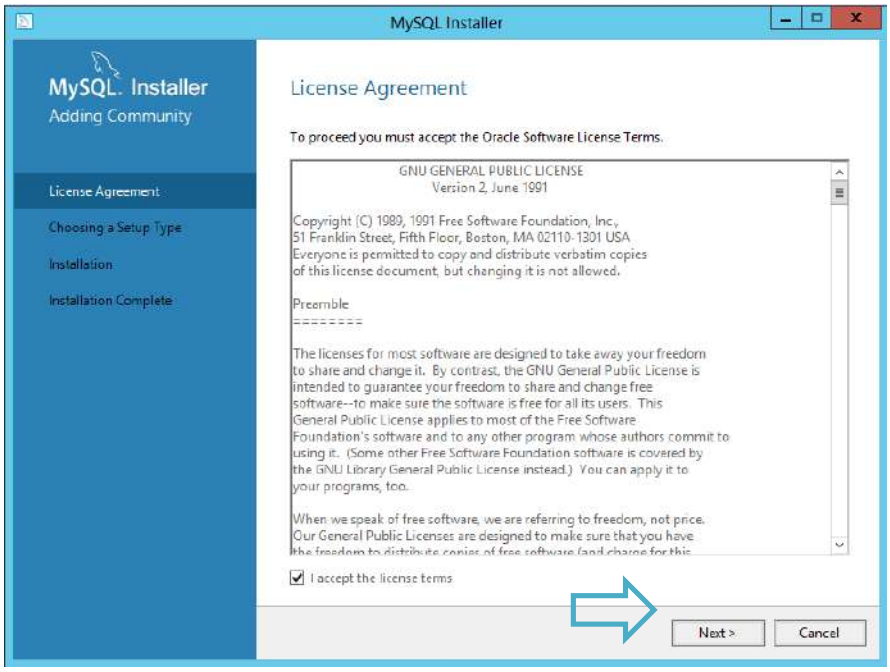


Figura 11. 3: Aceptar términos y condiciones de licencia

2. Existen varias configuraciones de tipos de servidores, en este caso debe escoger la opción "Server only". Como se observa en la Figura 11.4.

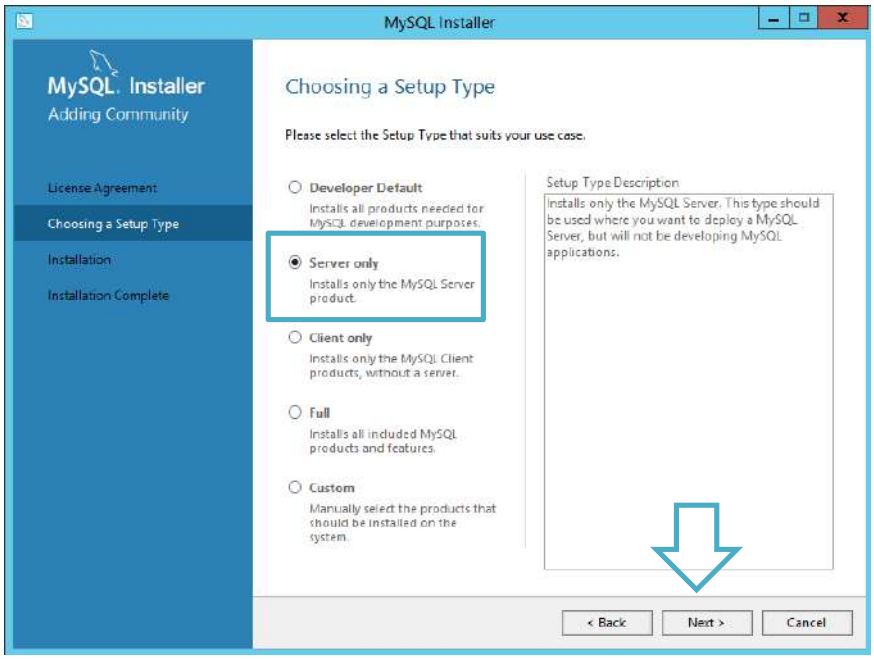


Figura 11. 4: Configuraciòn de tipo de servidor

3. Una vez configurado el tipo de servidor, aparecerá la instalación de actualizaciones, dar click en execute. Se debe esperar unos

segundos hasta que se realicen todas las actualizaciones. Como se observa en la Figura 11.5.

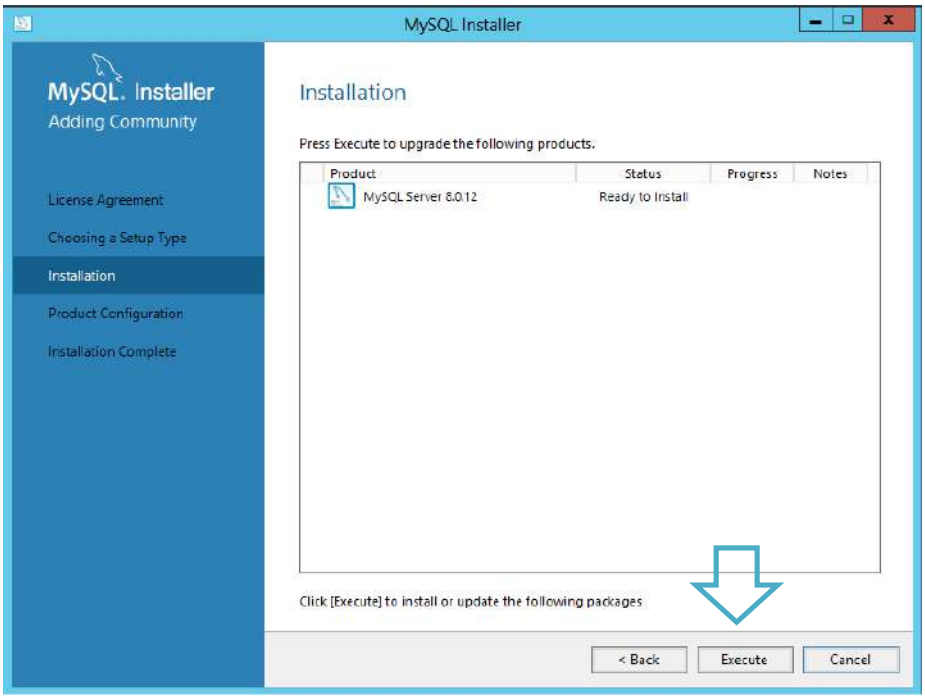


Figura 11. 5: Instalación de actualizaciones

4. A continuación, en TIPOS Y REDES, seleccionar el tipo de configuración "Server Machine", dar clic en siguiente. Como se observa Figura 11.6.

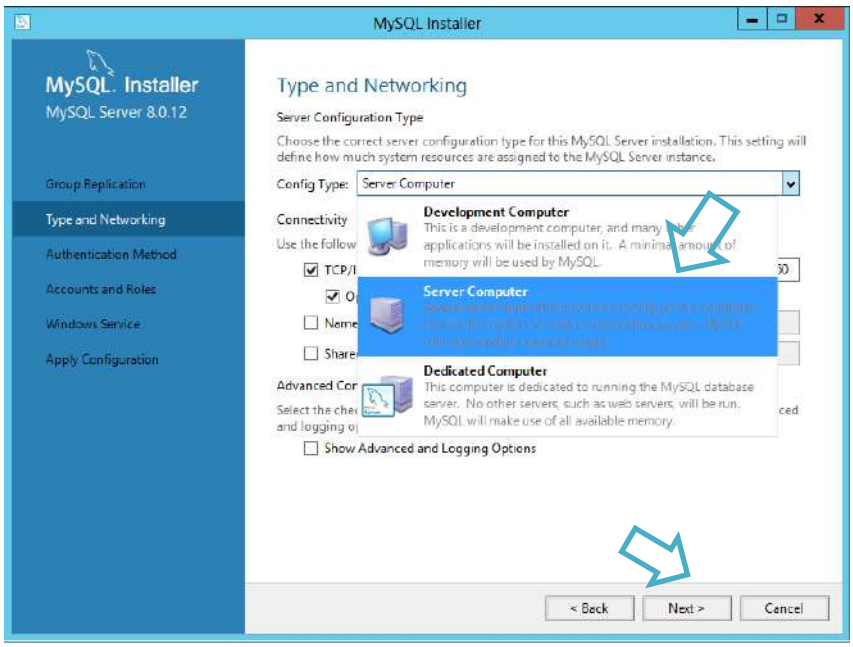


Figura 11. 6: Tipos de redes

5. En Cuentas y Roles, debe asignar una contraseña a la cuenta root, luego de esto dar clic en siguiente. Como se observa Figura 11.7.

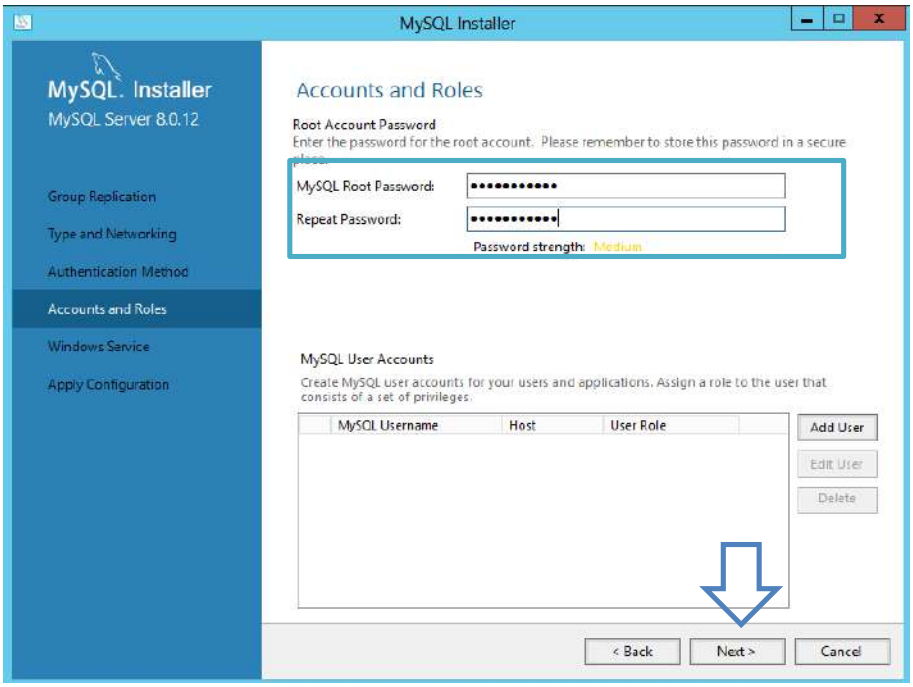


Figura 11. 7: Asignación de contraseña al root

6. En la Aplicación de la Configuración de Servidor, dar clic en ejecutar se procederá a la ejecución de los respectivos pasos, dar clic en finalizar. Como se aprecia en la Figura 11.8.

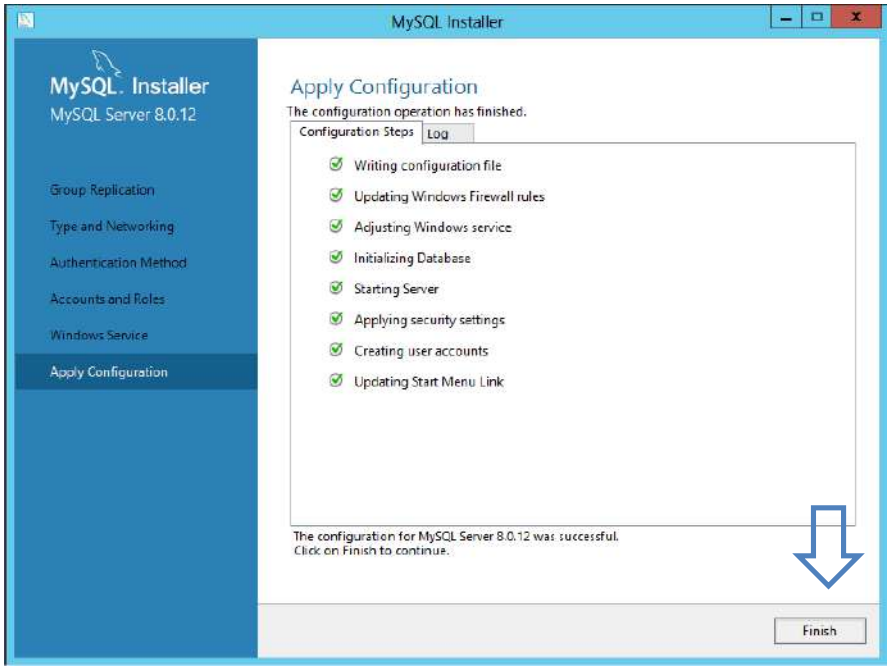


Figura 11. 8: Ejecución de instalación

7. ¡Fin de la Instalación!

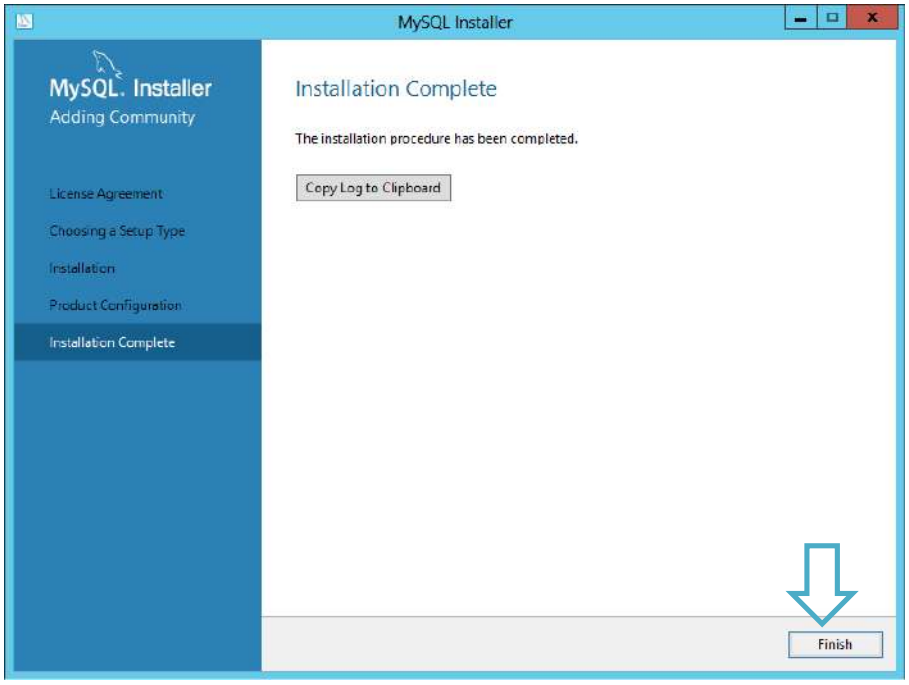


Figura 11. 9: Instalación completa

11.2. Paso 02- Instalar PHP

Es necesario constar con librerías de C++ que puedan ser mostradas.

1. Ingresar a windows.php.net para instalar las librerías de Visual C++. Como se observa en la Figura 11.10.

Las construcciones de VC11 requieren tener Visual c ++ redistribuido de Visual Studio 2012 para su instalación.

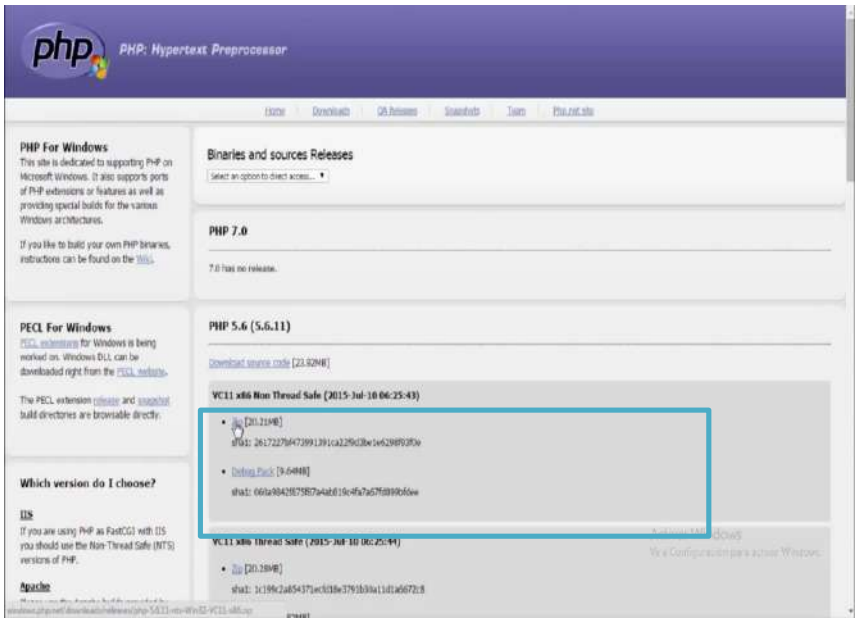


Figura 11. 10: Descargar librerías

2. Es necesario asignar el tamaño del archivo a descargar, en este caso sería: VSU_4/vcredit_x86.exe. Como se observa en la Figura 11.11.

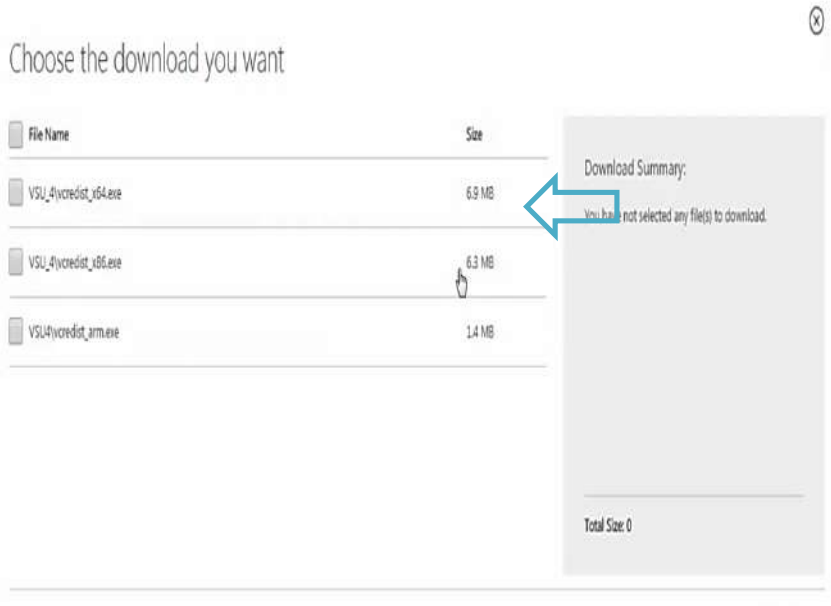


Figura 11. 11: Asignar tamaño al archivo

¿Sabías Qué?

Ejecutar la descarga de librerías como Administrador. Aparecerá el paquete PHP comprimido. Se debe descomprimir el paquete de PHP en una carpeta llamada **php** que se encuentre dentro del disco local (C:). Como se observa en la Figura 11.12.

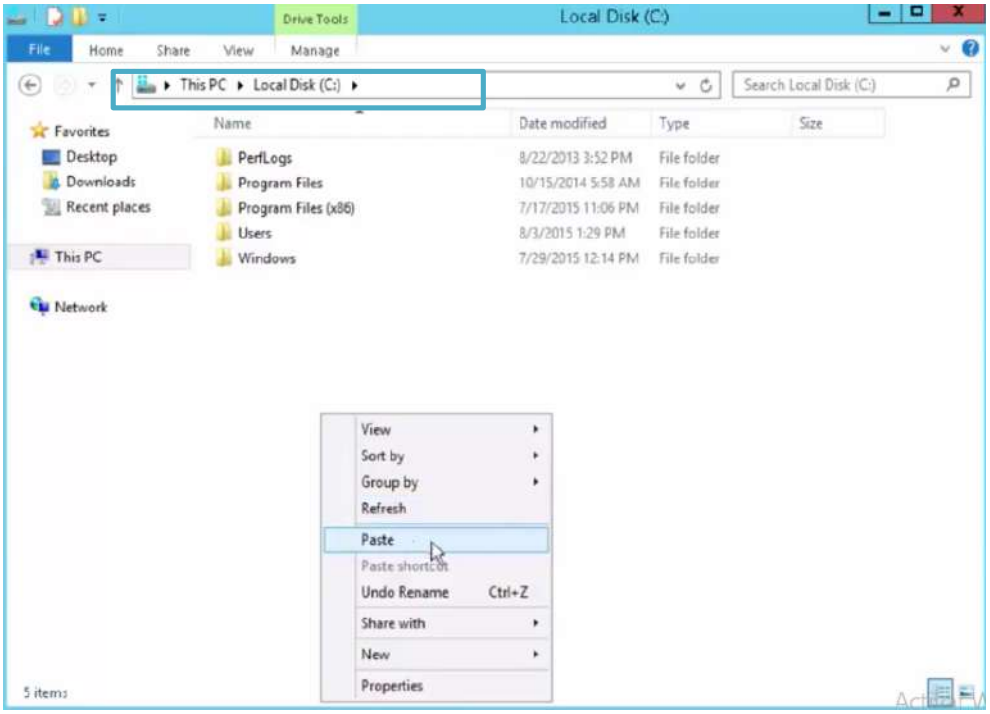


Figura 11. 12: Mover la carpeta php al disco local(c:)

3. Agregar c:/php a la variable de entorno de ruta, ingresar a las propiedades de la Pc. Dar clic en Configuración avanzada del sistema. Aparecerá un panel de configuración del sistema, dar clic en variable de entorno, luego de eso renombrar el archivo php.ini-production localizado in c:/php a PHP.ini. Como se observa en la Figura 11.13.

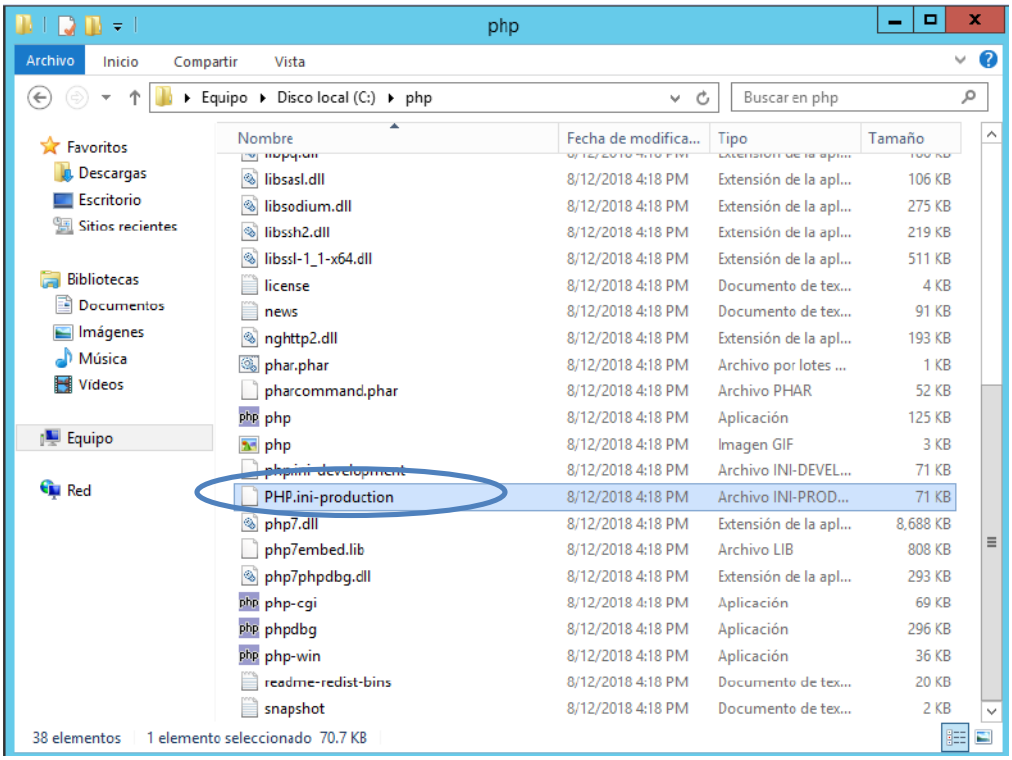


Figura 11. 13: Renombrar el archivo del disco local

4. Editar el archivo PHP.ini, habilitar y cambiar los siguientes elementos. Como se observa en la Figura 11.14.

ITEN	VALUE
date.timezone	America/Sao_Paulo
fastcgi.impersonate	1
Cgi.fix_pathinfo	1
Cgi.force_redirect	0
Extensión_dir	./ext

Figura 11. 14: Elementos de archivo php (A)

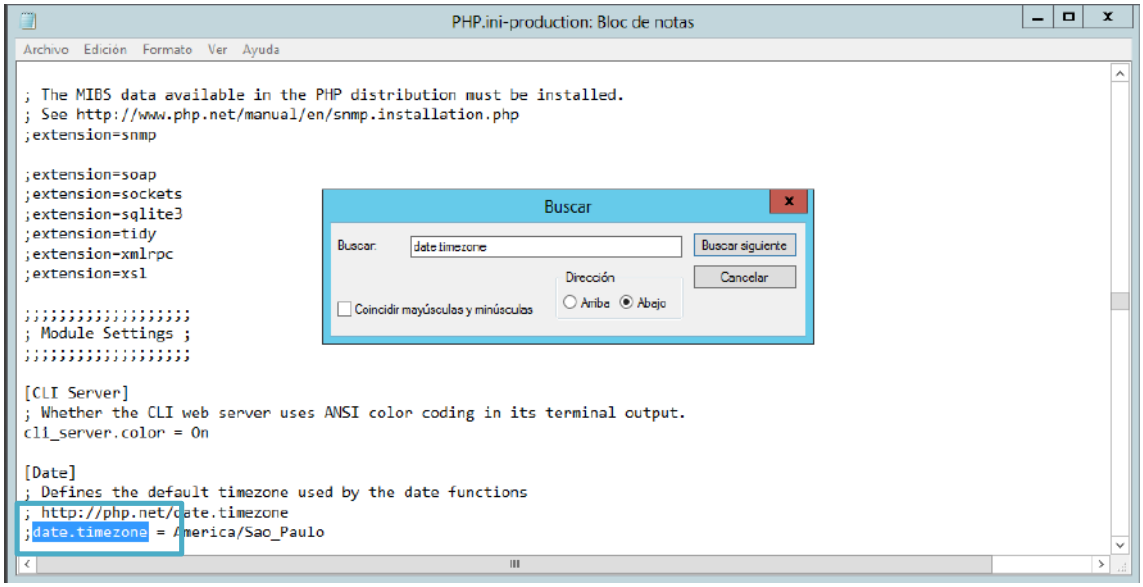


Figura 11. 15: Elementos de archivo php (B)

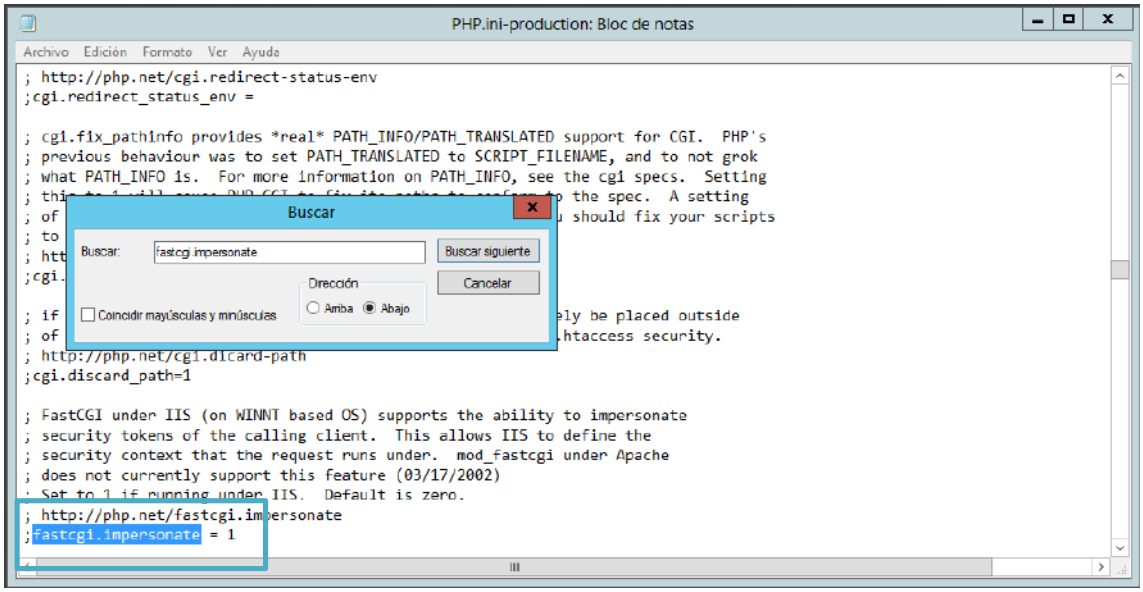


Figura 11. 16: Elementos de archivo php (C)

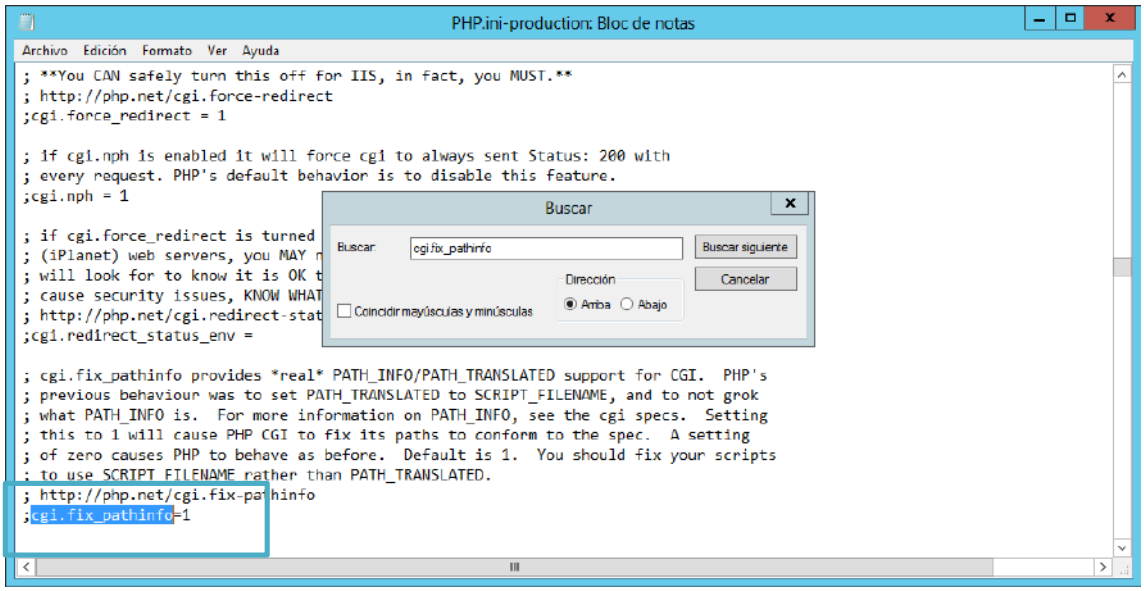


Figura 11. 17: Elementos de archivo php (C)

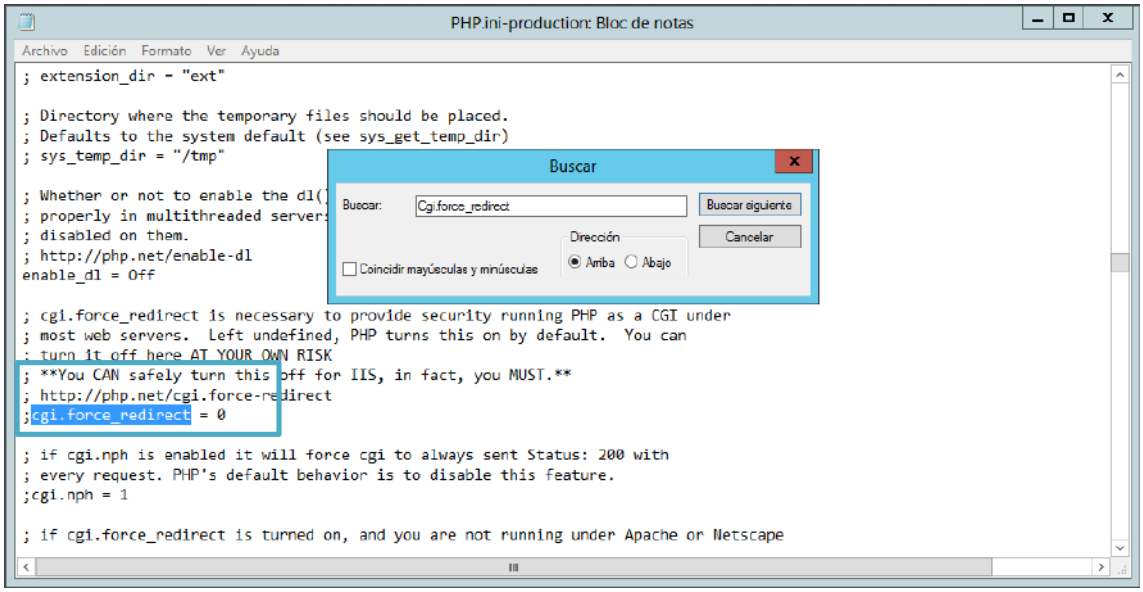


Figura 11. 18: Elementos de archivo php (D)

5. Se debe guardar el archivo con las configuraciones realizadas.

6. Abrir el cmd del sistema y ejecute el comando (-info) para probar la instalación en PHP, luego editar el archivo PHP.ini, habilitar y cambiar los siguientes elementos: Como se observa en la Figura 11.19.

MODULE	DESCRIPTION
extension=php_mysqli.dll	Módulo PHP MySQL
extension=php_mysqli.dll	Módulo PHP MySQL
extension=php_gd2.dll	Módulo PHP GD
extension=php_intl.dll	Módulo PHP INT
extension=php_curl.dll	Módulo PHP CURL
extension=php_ldap.dll	Módulo PHP LDAP

Figura 11. 19: Editar elementos de php.ini

7. Se configurarán todos los elementos asignados en la tabla. Como se observa en la Figura 11.20.

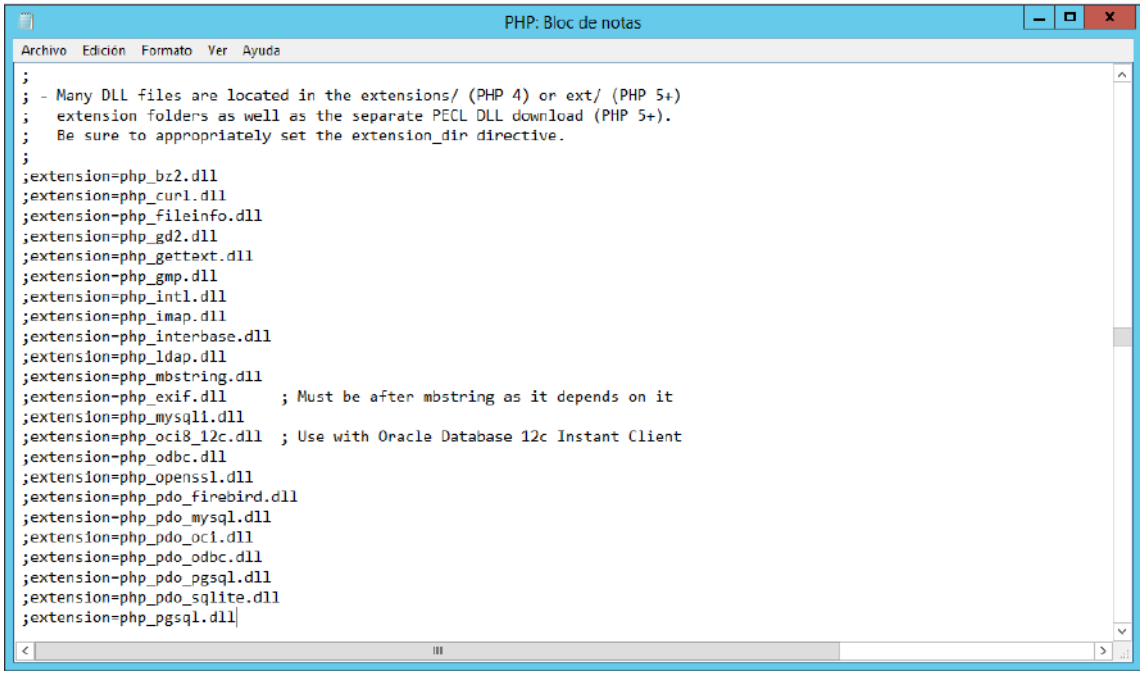


Figura 11. 20: Configuración de elementos en php.ini

8. Abra un panel de comando y ejecute el comando (-m) para probar la instalación en PHP. A continuación, se muestran todos los comandos accesibles. observar Figura 11.21.

Figura 11. 21: Ejecución de comando -m

11.2. Paso 03-Instalar servicios del Servidor Web (IIS)

1. Al agregar las características y roles del servidor, debe declarar que desea un Servidor Web. Como se observa en la Figura 11.22.

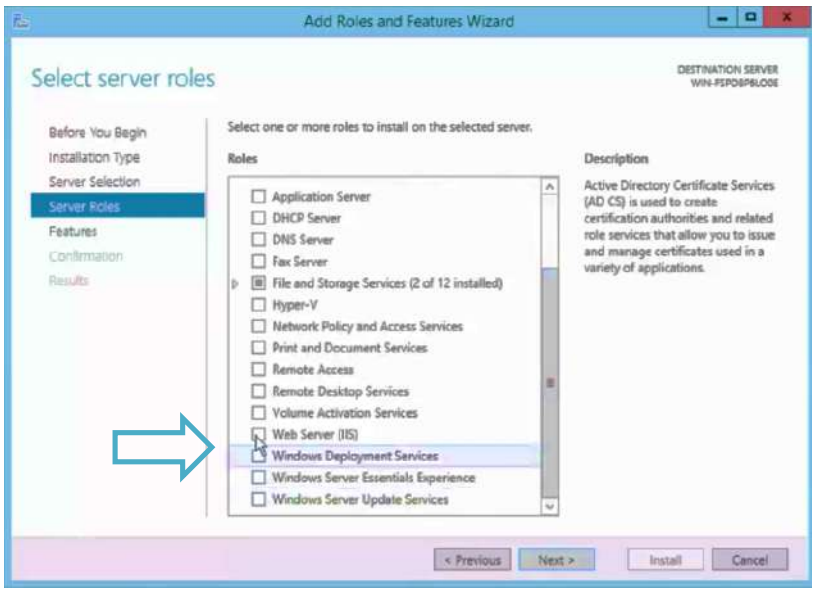


Figura 11. 22: Declaración de servidor web

2. En las asignaciones de roles de servicios, es necesario agregar CGI, ya que esta tecnología de red permite al cliente solicitar datos de un programa ejecutado en un servidor web. Como se observa en la Figura 11.23.

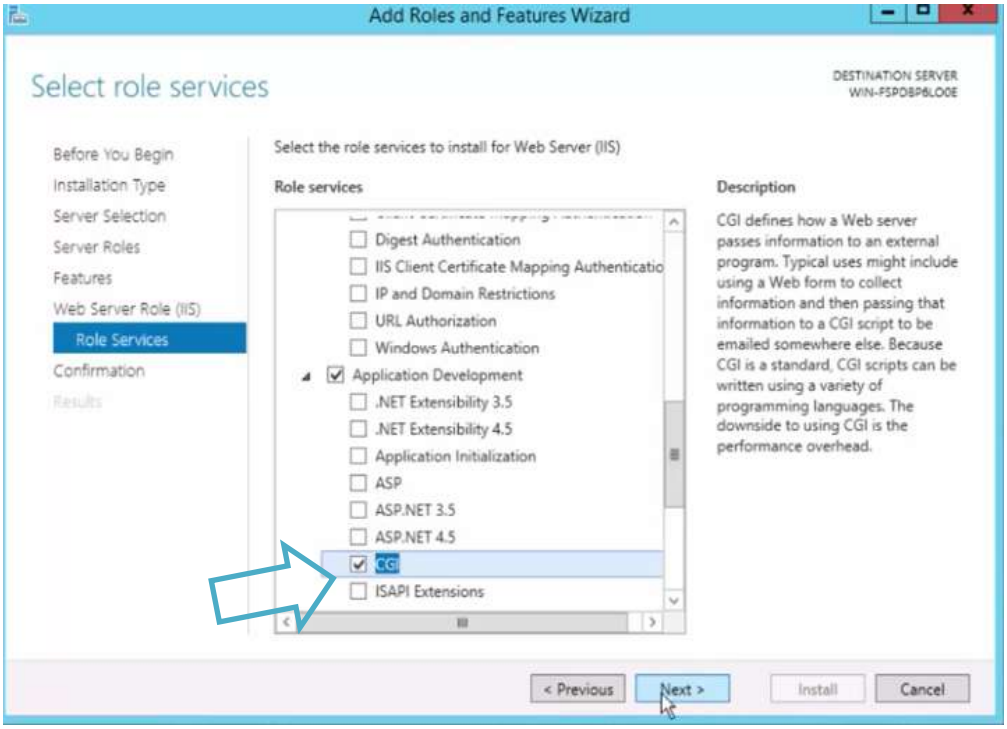


Figura 11. 23: Agregar CGI a los roles de servicios

3. Comprobar qué dirección IP corresponde al servidor IIS Web que se ejecuta con el comando: netstat-na find ":80". De forma predeterminada, el servidor IIS se ejecutará en todas las direcciones. (0.0.0.0) Como se observa en la Figura 11.24.

Figura 11. 24: Comprobar la direcciones IP

4. Después de la instalación, abra el administrador IIS de la herramienta administrativa y agregue el módulo PHP a IIS Root folder: C:/INETPUB/WWWROOT.
5. Agregar un módulo de mapeo con restricciones de archivos y ficheros.
6. Agregar index.php como una página por defecto. En la Win creada, existe una opción llamada "Default Document" donde se agrega el nombre del nuevo documento por defecto.
7. Reiniciar el servicio IIS el cual se encuentra en la ruta de la carpeta: C:/INETPUB/WWWROOT. El cual se hará dando clic derecho para apagar y encender.
8. Abrir el bloc de notas, crear un archivo de prueba php y guardarlo en C:/INETPUB/WWWROOT. Como se aprecia en la Figura 11.25.

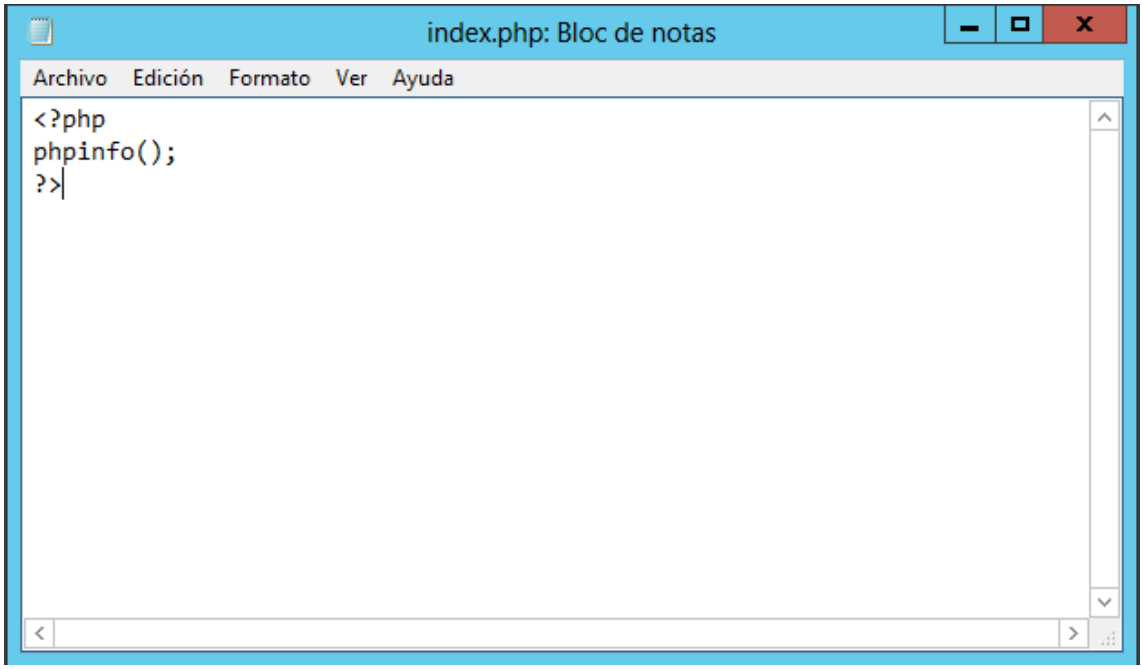


Figura 11. 25: Agregar Index PHP

9. Para probar su configuración de IIS, abra su navegador e intente acceder al archivo (NOMBRE ADQUIRIDO).Como se aprecia en la Figura 11.26.

Figura 11. 26: Prueba de la configuración

¡De manera exitosa es realizada la instalación de servicios!

Unidad

XII

Unidad XII

Zona WAN

Firewall Endian

12. Configuración de la zona WAN Firewall

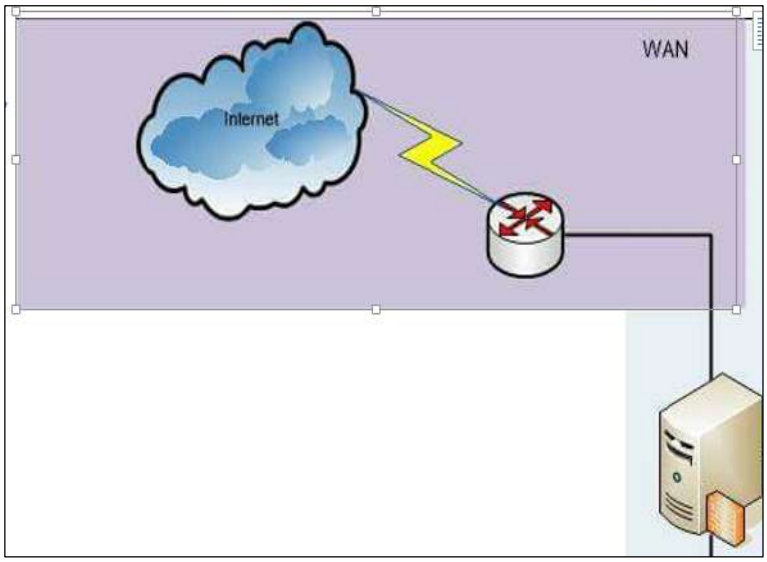


Figura 12. 1: Esquemas de las WAN

El firewall a utilizar es el ENDIAN para su configuración vamos a descargar el firewall

Una vez instalado nuestro firewall procedemos a su configuración como se demuestra en las siguientes figuras.

1. El primer paso es escoger el idioma en el que vamos a trabajar en este caso escogeremos el idioma English como se observa en la Figura 12.2.

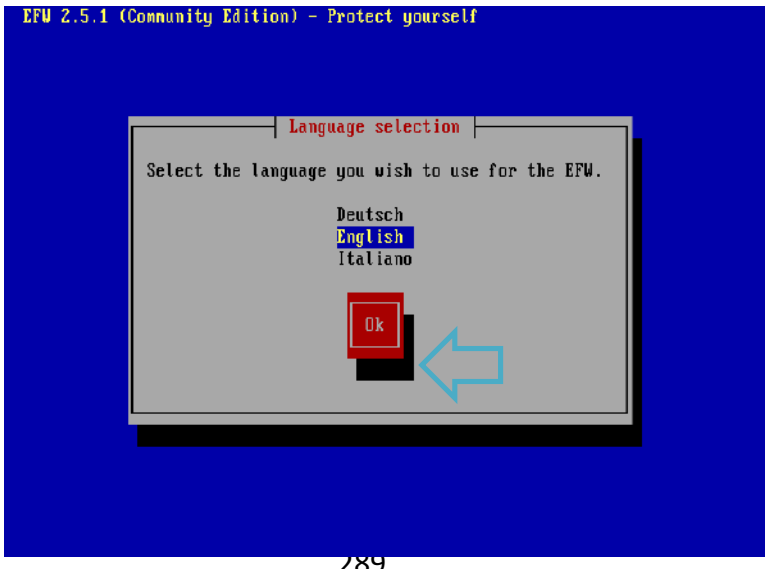


Figura 12. 2: Tipos de idioma

2. Una vez escogido nuestro idioma de trabajo se procede a instalar el firewall el ENDIAN escogeremos la opción de "YES" Y luego a ok como se observa en la Figura 12.3.

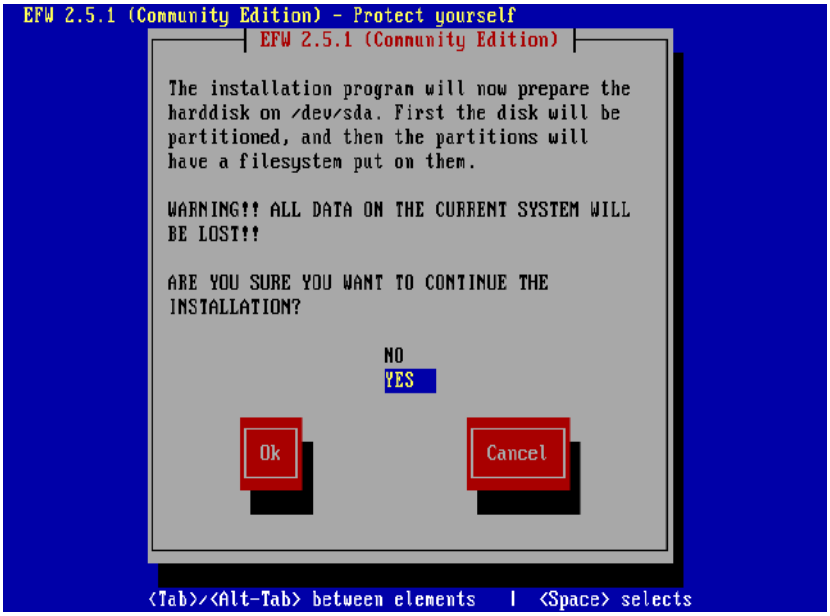


Figura 12. 3: Permisos para instalar el firewall

3. Luego nos preguntara si queremos que el programa instale puertos seriales en este caso escogeremos la opción "NO" y luego la opción OK como se muestra en la figura 12.4.

Figura 12. 4: Elección para cambiar de puertos

4. El siguiente paso es la configuración de la ip que va tener el firewall en este caso va a tener la siguiente dirección 192.168.10.15 y su máscara de red va hacer 255.255.255.0 y damos al OK como se demuestra en la figura Figura 12.5.

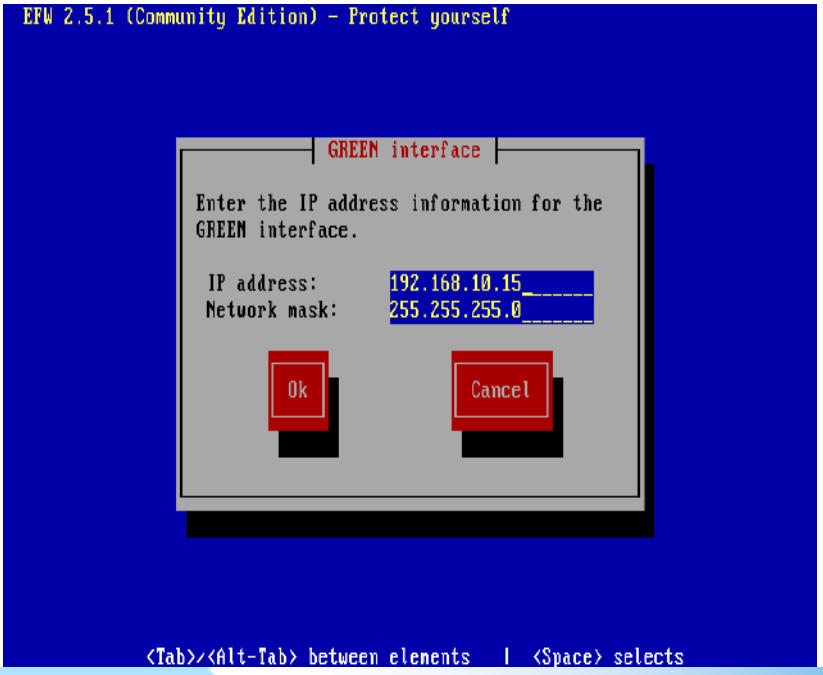


Figura 12. 5: Configuración de la IP de mascara de red

¿Sabías Qué?

La IP del firewall va hacer la puerta de enlace hacia las demás redes.

Luego de la instalación de firewall se procede a la configuración de las deferentes área del caso puesto en práctica para eso necesitamos ciertos requerimientos

Requerimientos:

- ✓ Red LAN: servicios privados solo accesibles desde la LAN, debe comunicarse con la DMZ y con la WAN.
- ✓ Red DMZ: servicios públicos accesibles desde la DMZ, LAN y WAN, no debe ver la LAN.
- ✓ Red WAN: Debe acceder a los servicios públicos de la DMZ por el firewall (re direccionamiento de IP) y no debe ver la LAN.
- ✓ Todas las redes deben salir a internet.

Configuración:

Al igual que en la entrada del firewall, en esta agregaremos tres adaptadores de red a nuestra máquina de endian, uno para nuestra LAN otro para DMZ y otro para la WAN, una vez tengamos estos adaptadores. Y tal como se ve en las siguientes figuras Figura 12.6 y Figura 12.7.

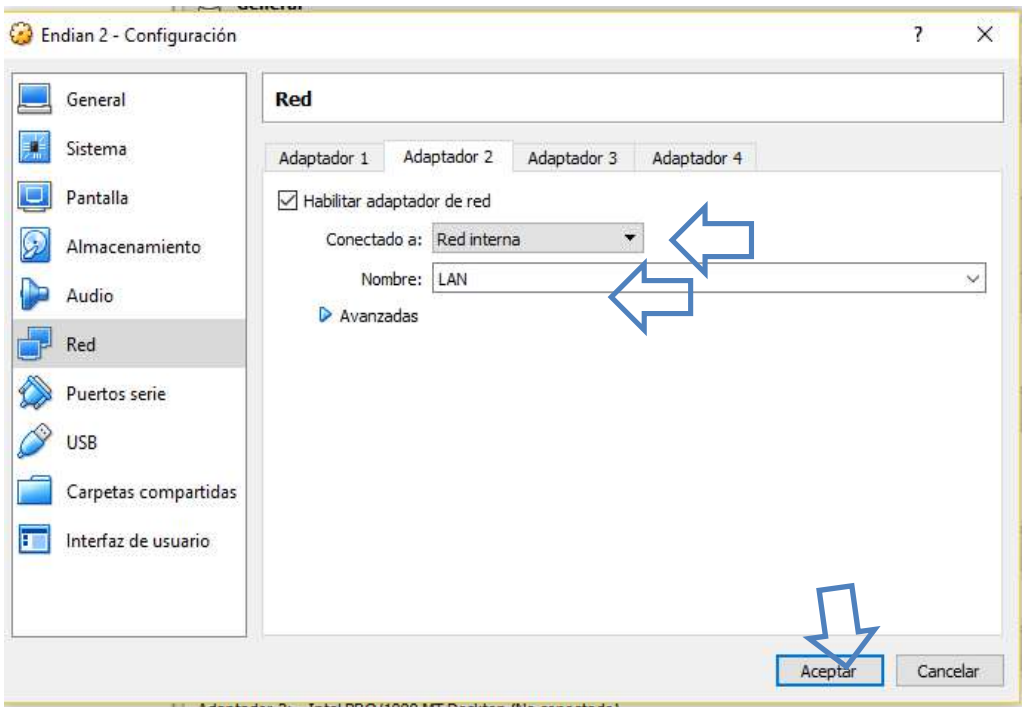


Figura 12. 6: Adaptador de LAN

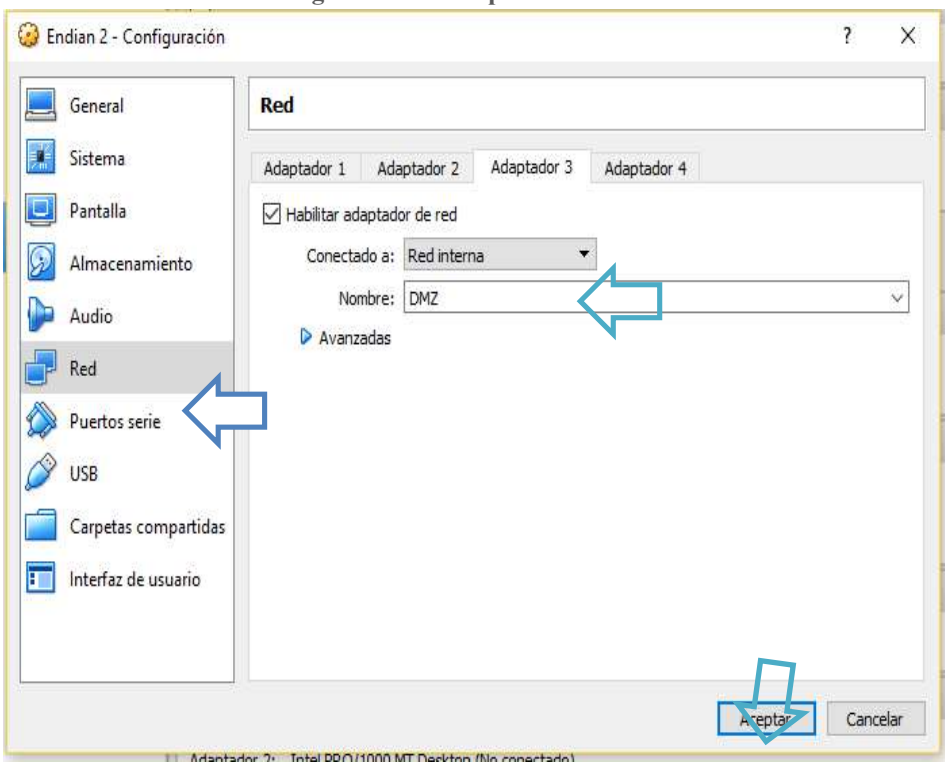


Figura 12. 7: Adaptador de la DMZ

Una vez configurados los adaptadores en las máquinas virtuales, procedemos a iniciar el Endian, tal como se muestra en la figura 12.8.

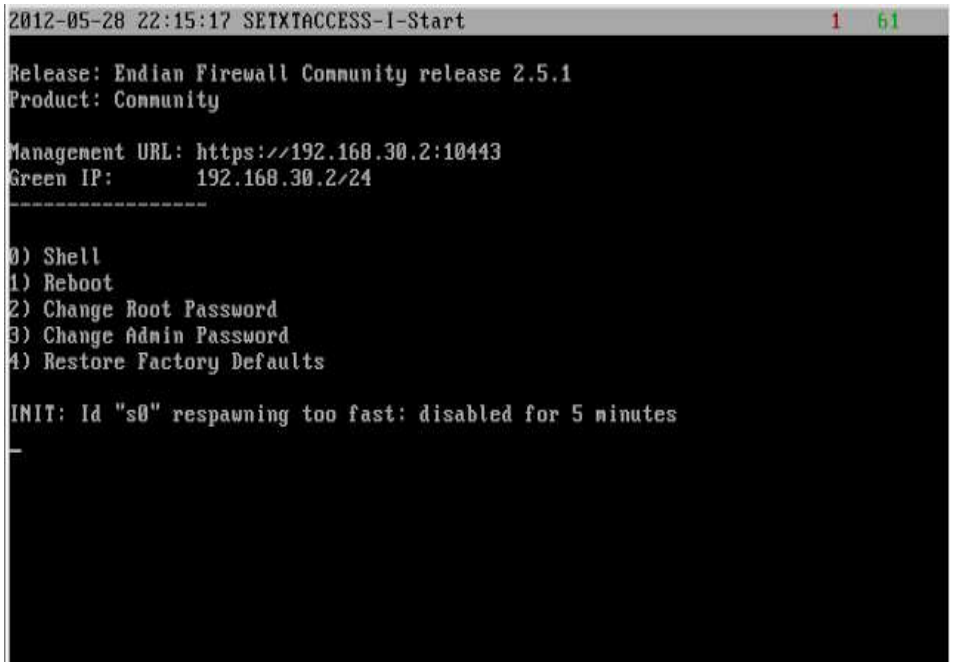


Figura 12. 8: Instalación de Endian

Cuando nos aparezca este pantallazo escogeremos la opción 0 para ingresar a la shell. Tal como se muestra en la figura Figura 12.9.

Figura 12. 9: Ingreso a la Shell

Una vez allí le diremos login y pondremos la contraseña del root que por defecto es endian. Tal como se muestra en la figura Figura 12.10.

Figura 12. 10: Contraseña de root

Aquí podremos administrar desde la shell de endian con algunos de los comandos que usualmente usamos en nuestras maquina con SO en Linux.

Desde la maquina Windows, pondremos la dirección IP que le dimos en la instalación, la pondremos en la barra de direcciones y entraremos a la interfaz web de endian tal como se muestra en la figura Figura 12.11.

Figura 12. 11: Ingreso a la interfaz web de endian

Una vez allí le daremos en el botón con las flechas (siguiente).

Si queremos hacer un respaldo de nuestro firewall escogemos la opción si en el siguiente paso, en este caso le diremos que no, y continuamos tal como se muestra en la figura Figura 12.12.

Figura 12. 12: Cambiar contraseña por defecto

Escogemos la contraseña para nuestro usuario y para el servicio SSH del root y continuamos. En endian, las Zonas se definen por colores, por eso es importante leer bien lo que hacemos ya que allí está todo muy bien definido. Tal como se muestra en la figura Figura 12.13.

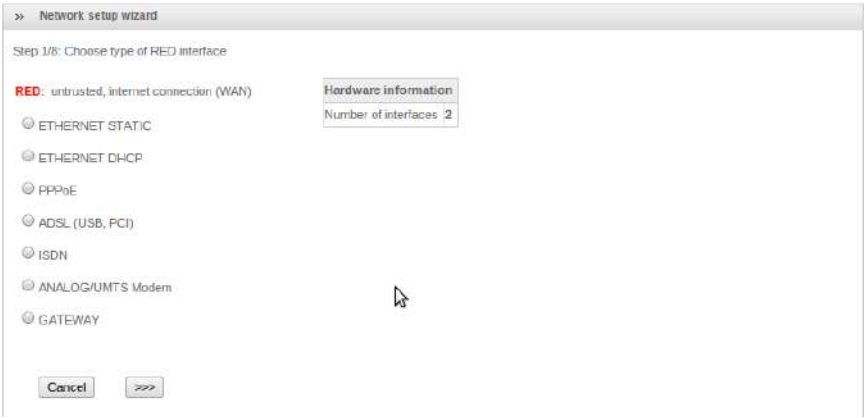


Figura 12. 13: Configurando el tipo interfaz zona roja

En este paso configuraremos el tipo de interfaz para la zona roja que es la WAN, seleccionaremos ethernet estático para que nuestra dirección sea estática y le damos siguiente, donde escogeremos el color para nuestra zona DMZ que como allí dice naranja para DMZ o azul para wifi. Aquí configuraremos la zona roja que será la LAN, le pondremos una dirección IP, la que nosotros destinemos a la LAN, la máscara y chuleamos la opción verde en la tabla de abajo para confirmar la MAC el vínculo y la interfaz en este caso eth0 como se muestra en la figura 12.14.

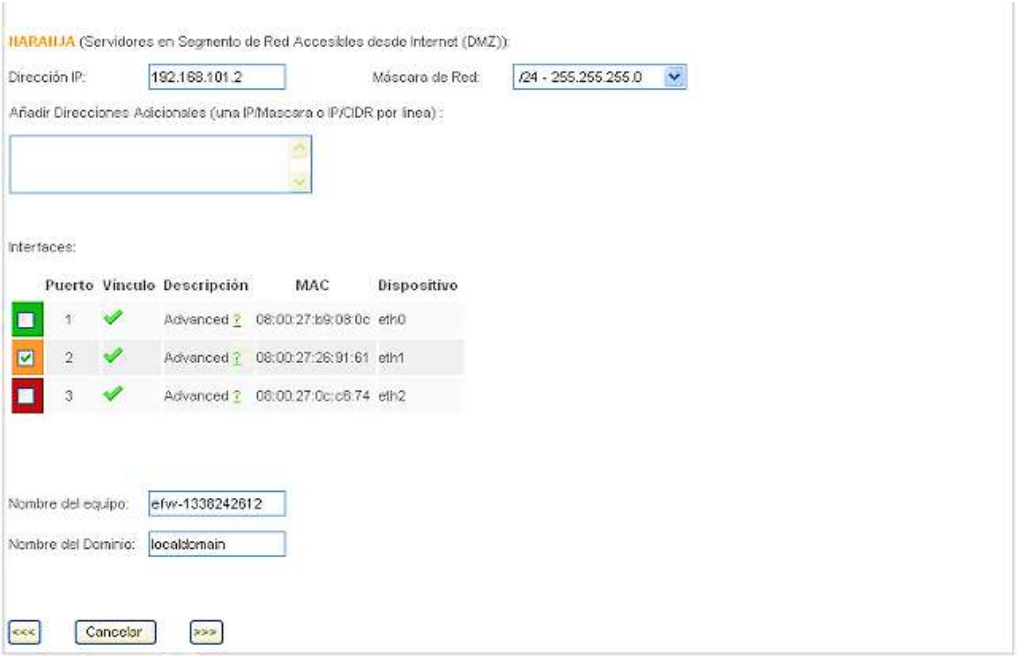


Figura 12. 14: Configuración zona naranja

En la misma página configuraremos la zona VERDE que será la DMZ, le pondremos una dirección IP estática y su respectiva mascará que asignamos en una previa planeación para la DMZ y chuleamos la opción naranja en la tabla, si queremos cambiamos el nombre del equipo y del dominio y continuamos.

¿En el siguiente paso configuraremos la dirección estática para nuestra WAN, como sabremos que ip ponerle? En la shell de endian haremos un dhclient a la interfaz por la que este nuestra WAN en nuestro caso la eth2 y vemos que IP nos entrega. Tal como se muestra en la figura Figura 12.15.

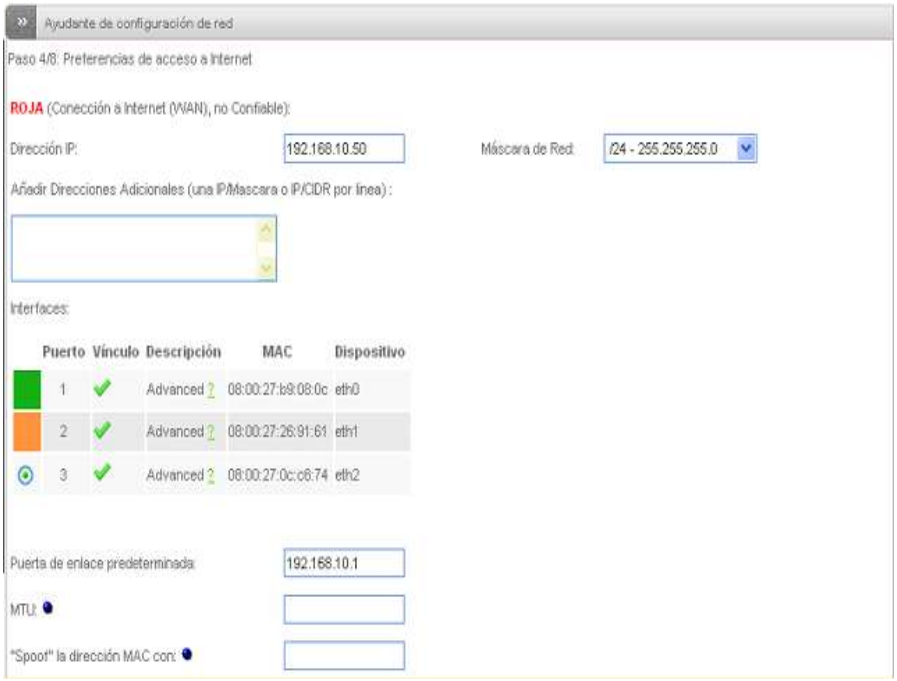


Figura 12. 15: Configuraciòn estàtico para la WAN

Agregaremos la ip que obtuvimos con la máscara, seleccionamos la opción roja o la última de la tabla, y agregamos el gateway. Tal como se muestra en la figura 12.16.

Figura 12. 16: Agregar IP de las puertas de enlace

Aquí pondremos los servidores DNS que normalmente usamos para salir a internet y continuamos, donde nos pedirá una dirección de correo electrónico, pero esto es opcional y se puede omitir. Tal como se muestra en la figura 12.17.

Figura 12. 17: Servidores DNS

Una vez estemos en el último paso le damos Aceptar, aplicar configuración, esperamos 20 segundos y nos aparecerá el login. Tal como se muestra en la figura 12.18.

Figura 12. 18: Aplicar configuración

Entramos con el usuario admin y la contraseña endian (en la imagen dice conectar a 192.168.30.2, pido disculpas esto es un error de imagen, nuestra dirección es la 192.168.10.15).

¿Sabías Qué?

Debemos tener en cuenta que la regla que aplica firewall por defecto es aceptar, por lo tanto todos los paquetes que salen y entran hacia la LAN serán.

Alfonso Aníbal Guijarro Rodríguez, Profesor Titular de la Universidad de Guayaquil, Ecuatoriano, Ingeniero en Computación por la Escuela Superior Politécnica del Litoral, Posgrados: Master en Gerencia Educativa a nivel Superior por la Universidad de Guayaquil, Master Universitario en Modelado Computacional de Ingeniería por la Universidad de Cadíz – España. Formación adicional: Certificado MTCNA, Cableado Estructurado, Microsoft Technology Associate in: Security Fundamentals, Windows Server Administration Fundamentals, Networking Fundamentals, Windows Operating System Fundamentals, Certificación Plus Panduit Latinoamerica, IT-essential, CCNA, CCNA Security, Ubiquiti Airmax Certified Admin, ha participado en eventos científicos y posee múltiples publicaciones de alto impacto.

Fausto Raúl Orozco Lara, Ingeniero en Sistemas Computacionales, por la Universidad de Guayaquil, con estudios de Posgrado, Magister en Telecomunicaciones, por la Universidad Católica Santiago de Guayaquil; Docente Titular Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Sistemas Computacionales e Ingeniería en Networking y Telecomunicaciones. Especialista en Servidores de plataforma Unix, Virtualización, Redes y Telecomunicaciones. Diplomado de Seguridad Informática Ofensiva.

Miguel Alfonso Molina Calderón, Ingeniero en Sistemas Computacionales y Magister en Sistemas de Información con experiencia en el desarrollo e implementación de sistemas informáticos y en el área de soporte de usuarios. Magister en Docencia y Gerencia en Educación Superior y docente contratado de la Facultad de Ciencias Matemáticas de la Universidad de Guayaquil desde el año 2003. Coautor de varios artículos publicados en revistas internacionales. Padre de familia amante de sus hijos, aficionado por el fútbol y voleibol.

Johana Elisabeth Trejo Alarcón, Ingeniero en Computación especialidad Sistemas Tecnológicos, por la Escuela Superior Politécnica del Litoral (ESPOL), Magister en Seguridad Informática Aplicada (ESPOL), Realiza estudios Doctorales en la ESPOL “Doctorado en Ciencias Computacionales Aplicada” , Investigador de proyectos FCI – Universidad de Guayaquil, Docente Universitario en la Carrera de Ingeniería en Sistemas Computacionales y la Carrera de Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

ISBN: 978-9942-33-083-3

compAs