UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

UNAN – MANAGUA

RECINTO UNIVERSITARIO RUBÉN DARÍO

FACULTAD DE CIENCIAS E INGENIERÍA

DEPARTAMENTO DE TECNOLOGÍA

Seminario de Graduación para Optar al Título de Ingeniero en Electrónica.

TEMA:

Seguridad en el acceso a las redes de datos en la UNAN-MANAGUA, durante el periodo de Agosto a Noviembre del 2016.

Autores:

- Br. Manolo de Jesús Cuadra Pautter.
- Br. Josué Adiel Castillo González.

Tutor:

- Msc. Milciades Delgadillo.

Asesor Tecnológico:

- Msc. Edison Cuevas Videa.

Managua, 09 de Enero 2016.

Dedicatoria

Queremos dedicar este seminario en primer lugar a Dios Todopoderoso, por ser él quien nos ha impulsado a seguir a lo largo de nuestra vida afrontando los retos que cada día se nos han presentado, ha sido nuestra fortaleza en los momentos de dificultades y sobre todo en lo distintos acontecimientos que a nivel personal y familiar acontecieron en el transcurso de esta carrera.

A nuestros amadísimos padres quienes nos han apoyado incondicionalmente desde niños y que han sido nuestro ejemplo. A ellos que nos enseñaron a salir adelante, afrontando los retos y a vencer las dificultades que se nos presentan en cada etapa de nuestras vidas. .

A nuestros maestros de la carrera de Ingeniería en electrónica de la Universidad Nacional Autónoma de Nicaragua (UNAN-MANAGUA), quienes nos han sabido comprender en todo este tiempo. El buen maestro es el que sabe y maneja bien un tema como lo han demostrado todos los profesores que nos han impartido las diferentes materias que hemos visto a lo largo de la carrera, es por eso que dedicamos todo el esfuerzo de este trabajo a esos hombres y mujeres que hicieron todo lo posible por guiarnos en el buen camino.

Agradecimientos

Damos gracias a Dios por estar con nosotros, en cada paso que dábamos, por fortalecer nuestros cuerpos y gozar de salud durante este trabajo; por iluminar nuestras mentes y por haber puesto en el camino a aquellas personas que han sido apoyo durante este período de estudio.

Agradecemos a nuestra familia por el esfuerzo realizado por parte de ellos. A nuestros padres y demás familiares; ya que nos brindaron el apoyo, la alegría y la fortaleza necesaria para seguir adelante.

Un agradecimiento especial a las personas del Departamento de Tecnología SIUDT de la UNAN MANAGUA, en especial al MSc. Edison Cueva Videa que brindo el tiempo, espacio y apoyo para realizar lo abordado en este trabajo, por dedicarle tiempo a la revisión de ciertos aspectos e ideas en este documento.

Índice de Contenido

I. Resumen 1

II. Introducción 3

III. Antecedentes 5

IV. Justificación 6

V. Objetivos 7

5.1. Objetivo General: 7

5.2. Objetivos Específicos: 7

VI. Desarrollo 8

6.1. Mecanismos y tecnología existente en la UNAN-MANAGUA. 8

6.1.1. Instalación y Configuración básica de (*Microsoft Assessment and Planning Toolkit 9.4*) 9

6.1.2. Los recursos disponibles encontrados en el diagnóstico del TIC UNAN-MANAGUA. 16

6.2. Aportes de la tecnología NAP de Microsoft en el control de Acceso a las Redes de datos. 22

6.2.1. Protección de Acceso a la Red (NAP) 23

6.2.2. El servidor de directivas de red Network Policy Server (NPS) 23

6.2.3. Métodos de cumplimiento NAP 25

6.2.4. Servidor de saneamiento. 27

6.2.5. Arquitectura del cliente NAP 28

6.2.6. Arquitectura del servidor NAP 29

6.2.7. Las distintas directivas en NAP 30

6.2.8. Requisitos para la Infraestructura del NAP 31

6.3. Implementación de la tecnología NAP, utilizando Windows Server 2012 R2. 33

6.3.1. Introducción a Windows Server 2012 R2 33

6.3.2. Existen cuatro ediciones de Microsoft Windows Server 2012 R2: 33

6.3.3. Instalación mínima (Server Core) 36

6.3.4. Instalación Grafica con una GUI 38

6.3.5. Instalación de Windows Server 2012 R2 en el dominio unan.edu.ni: 39

6.4. Pasos para implementar de NAP: Instalación de la Entidad emisora de certificados "Active Directory Domain Services (AD DS)". 43

6.4.1. Jerarquías de Entidades de Certificación 43

6.4.2. Entidades de Certificación Raíz (Root Certification Authority) 43

6.4.3. Entidades de Certificación Subordinadas (Subordinate Certification Authority) 44

6.4.4. Tipos de Entidades de Certificación 44

6.4.5. Componentes de Active Directory Certificate Services 46

6.4.6. Instalación y configuración de la Entidad emisora de certificados (Active Directory Certificate Services). 47

6.5. Instalar y configurar el Servicio NPS (Network Policy Service) en Windows Server R2 2012. 57

6.6. Instalación y configuración del Rol DHCP en Windows Server 2012 R2 10.1.120.120/24. 64

6.7. Prueba de campo replicando en un escenario seguro (Red de prueva) de la red de la Unan-Managua, la configuración realizada de NAP con DHCP 69

VII. Conclusiones 72

VIII. Recomendaciones 74

IX. Bibliografía 75

X. Anexos 76

XI. Glosario 79

I. Resumen

El presente trabajo se realizó para el área de redes del Departamento SIUDT de la UNAN-MANAGUA, el cual presenta un estudio a fondo de las tecnologías de acceso a la red de datos brindadas por Windows Server 2012 R2, a continuación se hace una propuesta para la implementación de la tecnología protección de Acceso a la red (NAP, Network Access Protection), como método de protección de cualquier usuario de la intranet de la universidad vía protocolo de configuración host (DHCP), de esta manera brindar este servicio con vista al futuro, dejando un precedente al expandir esta tecnología en toda la red LAN de la UNAN-MANAGUA.

Actualmente la UNAN-MANAGUA, utiliza Windows Server 2012 R2 DATACENTER para mantener servicio de Active Directory, Servicio de Outlook, Exchange Server 2012; Servicios que corren en un arquitectura llamada virtualización. Sumado los servicios antes descritos también se cuenta con otros servicios de red que corren bajo sistema Linux, por lo que se puede decir que estamos bajo la presencia de una red Hibrida Linux/Windows, tanto en el lado servidor como en el lado cliente.

Ante este escenario no existe una solución de seguridad única, hasta el momento los métodos de protección de acceso ha sido el filtrado por autentificación de mensaje (MAC) y la implementación de redes de área local virtualizadas (VLANs), estas soluciones preventivas resuelven en parte el problema de seguridad; sin embargo la solución debe ir dirigida en cómo actualizar proactivamente ante el riesgos inminentes, como los son los virus, software desactualizados, programas espías o cualquier tipo de malware.

Con la implementación de esta nueva tecnología se lograra una mejora considerable en la seguridad de los sistemas, no solo de los recursos de red sino también de los clientes que acceden a los mismos. Al implementar esta nueva tecnología que nos presenta Microsoft podremos establecer una serie de condiciones que ayudaran a determinar que equipos de los que se conecten a la red desde cualquier medio (VPN, Internet, Wireless junto a otros), cumplan con una política de salud aceptable, acorde a las directrices de seguridad de la Universidad.

La tecnología Network Access Protection (NAP) también incluye una interface de programación de aplicación (API, Aplication Programmin Interface) para desarrolladores. A través de ella es posible la generación de componentes de seguridad realizados a medida de las necesidades de la red de la UNAN Managua. Una infraestructura NAP requiere de un servidor Windows server 2012 R2 para su despliegue, y los clientes soportados son Windows Server 2012 R2, Windows 10, Windows 8.1, Windows 7.

Cabe destacar que la solución NAP propuesta no está diseñada para asegurar la red de los usuarios maliciosos y mal intencionados, sino que está pensada para ayudar a mantener la higiene de los dispositivos con sistemas operativos Microsoft, NAP tiene como objetivo mantener la integridad general de la red.

II. Introducción

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

En este sentido el presente seminario de graduación aborda el estudio de las tecnologías de acceso a la red de datos brindadas por Windows Server 2012 R2, a partir del cual realizamos una propuesta para la implementación de la tecnología protección de Acceso a la red (NAP, Network Access Protección), como método de protección de cualquier usuario de la intranet de la universidad vía protocolo de configuración host (DHCP), de esta manera brindar este servicio con vista al futuro, dejando un precedente al expandir esta tecnología en toda la red LAN de la UNA-MANAGUA.

En un primer momento nos propusimos diagnosticar los mecanismos y tecnología existente en la UNAN-MANAGUA en la protección del acceso a las redes datos, a fin de poder tener una visión más clara de los mecanismo que esta importante universidad viene implementando. Seguidamente nos dimos a la tarea de identificar la tecnología de control de acceso a las redes de datos en el cual se enfoca el estudio del sistema de seguridad Network Access Protection, con el fin de visualizar la viabilidad de la implantación tomando en cuenta las bondades de la misma.

Finalmente estamos proponiendo la implementación del sistema de seguridad de acceso a la red de datos de la UNAN-MANAGUA utilizando tecnología de protección de acceso a la red (NAP) de Microsoft Windows Server R2 2012, en la subred del Sistema de Información Universitario de Desarrollo Tecnológico (SIUDT), así mismo presentamos como las conclusiones y las respectivas recomendaciones derivadas del desarrollo, fundamentalmente se recomienda que el actual servidor de asignación de direcciones dinámicas, DHCP, Server, el cual corre bajo entorno Linux, siendo este incompatible con el sistema NAP, por lo que se sugiere emigrarlo a Windows server 2012, para obtener un sistema NAP, DCHP, integrado.

III. Antecedentes

La red inalámbrica de UNAN-MANAGUA comenzó a configurarse entre los años 2009–2010, estaba distribuida en unas pocas zonas comprendidas entre los pabellones 4, 6, rectoría, pabellón 14 (TIC), laboratorio de computación en el pabellón 16, esta red contaba con un ancho de banda de 256 Kb, los equipos eran wr54g Linksys, ap100 DLink.

En la administración de la red se configuró un servidor con las siguientes características: Servidor Dell PowerEdge 400sc, con procesador Intel Pentium 4 corriendo a 3.2 GHz, memoria RAM de 512 Mb, disco duro de 8 Gb, con dos interfaces de red fastethernet 10/100, en el que se le instaló el sistema operativo Linux Ubuntu y se le configuraron los servicios de DNS (Domain Name System, Sistema de nombres de dominio) y DHCP (Dynamic Host Configuration Protocol, protocolo de configuración dinámico de host) para administrar la red inalámbrica y la red LAN.

IV. Justificación

La seguridad de redes de datos consiste en las políticas adoptadas para prevenir y monitorear el acceso no autorizado, el mal uso, la modificación o la denegación de un host a la red de datos. La seguridad de redes involucra también la autorización del acceso a datos en la red, que es controlado por el administrador.

La presente investigación, se propone diseñar un sistema confiable que permita desarrollar un sistema de seguridad en el acceso a las redes de datos para mejorar la administración de la red cableada de la UNAN-MANAGUA. Este sistema vendrá a facilitar una de las tareas más demandantes para los administradores de sistemas, como es asegurar que cualquier dispositivo que se conecte a la red corporativa cumplan con el modelo de seguridad definido por políticas administrativas (firewall activado, Sistemas Operativo con últimas actualizaciones, Software de Antivirus/Antimalware activo y actualizado).

Este tema es de gran importancia debido a un sin números de vulnerabilidades que enfrenta la red corporativa de la UNAN-MANAGUA, como lo son los virus, el correo spam, en vista de que son los únicos sistemas de seguridad de acceso que actualmente se encuentran en uso como lo es el filtrado por autentificación por mensaje (MAC) y la implementación de redes de área local virtualizadas (VLANs), se pretende sufragar con la tecnología NAP un sistema novedoso de saneamiento y que es parte integral de Windows Server 2012 R2 de Microsoft aprovechando que los servidores de la UNAN-MANAGUA ya cuenta con este sistema operativo lo cual facilita la implementación.

V. Objetivos

5.1. Objetivo General:

- Proponer un Sistema de Seguridad en el acceso a las redes de datos en la UNAN-MANAGUA durante el periodo de Agosto a Noviembre del 2016.

5.2. Objetivos Específicos:

- Diagnosticar los mecanismos y tecnología existente en la UNAN-MANAGUA en la protección del acceso a las redes datos.

- Determinar la tecnología de control de acceso a las redes de datos en el cual se enfoca el estudio del sistema de seguridad Network Access Protection (NAP).

- Proponer la implementación del sistema de seguridad de acceso a la red de datos de la UNAN-MANAGUA utilizando tecnología de protección de acceso a la red (NAP) de Microsoft Windows Server R2 2012, en la subred del Sistema de Información Universitario de Desarrollo Tecnológico (SIUDT).

VI. Desarrollo

6.1. Mecanismos y tecnología existente en la UNAN-MANAGUA.

Para hacer el diagnóstico de la red de datos de la UNAN-MANAGUA y los mecanismos que actualmente se encuentran en funcionamiento, se utilizó el método de observación a todos aquellos elementos que juegan un rol importante en el tema, también se utilizó la entrevista a las personas claves que se verán beneficiadas con el sistema.

"Además se hará uso del software (*Microsoft Assessment and Planning Toolkit*): se utiliza para la evaluación y planificación de varios productos al evaluar un entorno de red utilizando las tecnologías de recolección de datos sin agente para recopilar información de inventario y el rendimiento". (https://technet.microsoft.com/es-ni/windows/dd627342, 2016)

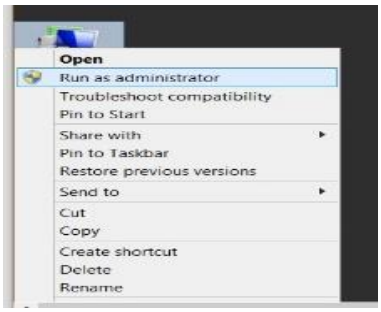
El kit de herramientas MAP utiliza Windows ® Management Instrumentation (WMI), Active Directory ® (Servicios de dominio de AD DS), proveedor de SMS, y otras tecnologías para recopilar datos en el entorno de hardware y los inventarios de equipo, software y sistemas que operan en pequeñas o grandes entornos de TI sin necesidad de instalar ningún software agente en los equipos de destino. Los datos y análisis proporcionados por el MAP agilizar el proceso de planificación para la migración de software, ayudar a evaluar la disponibilidad de controladores de dispositivo.

6.1.1. Instalación y Configuración básica de (*Microsoft Assessment and Planning Toolkit 9.4*)

- **Pasos a seguir para la instalación de Microsoft Assessment and Planning Toolkit 9.4.**

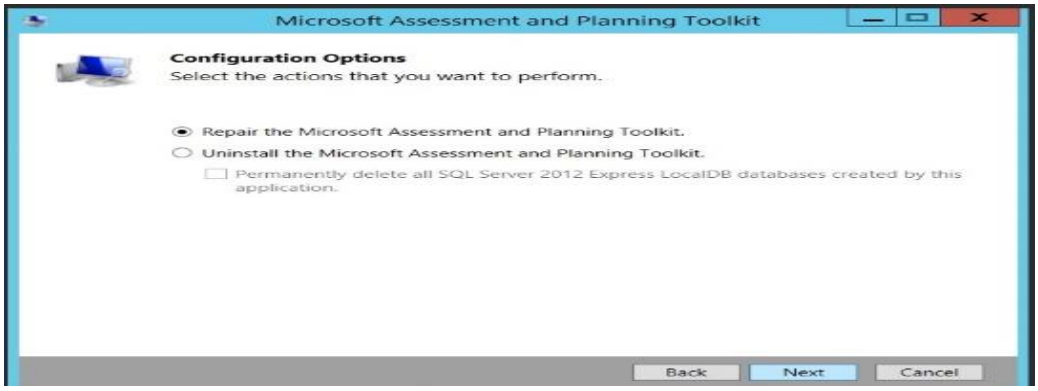
1. Descargar la aplicación desde el link oficial de Microsoft http://download.microsoft.com/download/4/6/F/46F45C42-D679-404E-9812-6053DD59A0D2/Microsoft_Assessment_and_Planning_Toolkit_Setup.exe

2. Una vez teniendo setup del programa Map toolkit, lo ejecutamos como administrador.

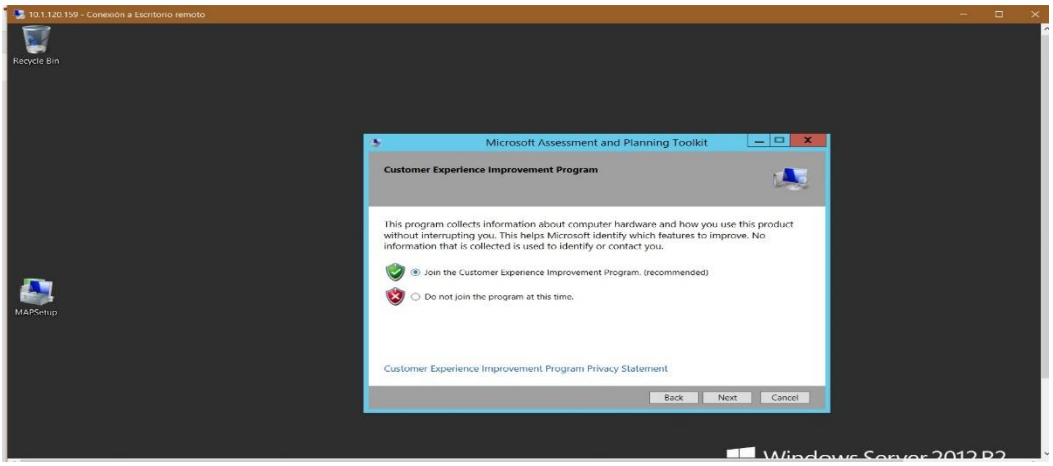


3. Nos aparecerá el mensaje de bienvenida al programa y le damos clic en next.

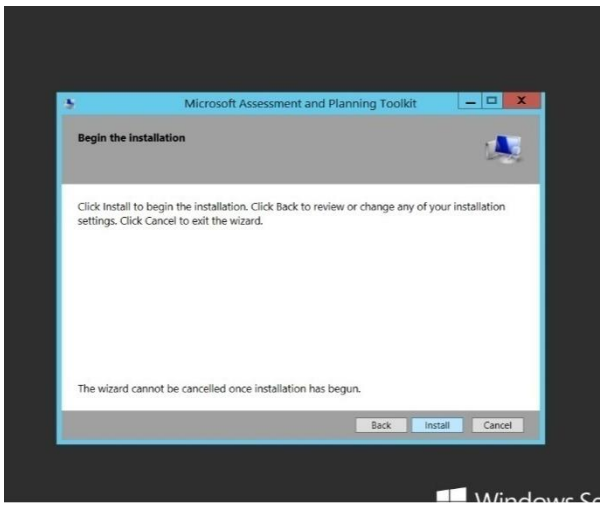
4. Luego abrirá una pestaña de **configuration options**, donde seleccionaremos la opción "Repair the Microsoft Assessment and Planning toolkit" y damos clic en "Next".

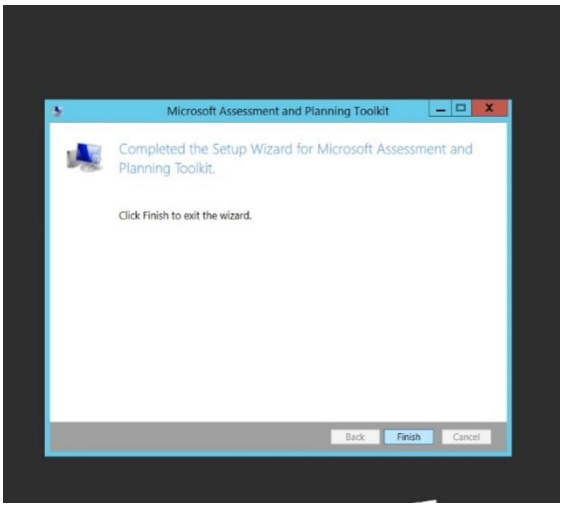


5. Se abrirá la opción de **Customer Experience Improvement Program** que es la experiencia recomendada, elegimos la opción de "Join the Customer Experience Improvement Program (Recommended)" y damos clic en "Next".



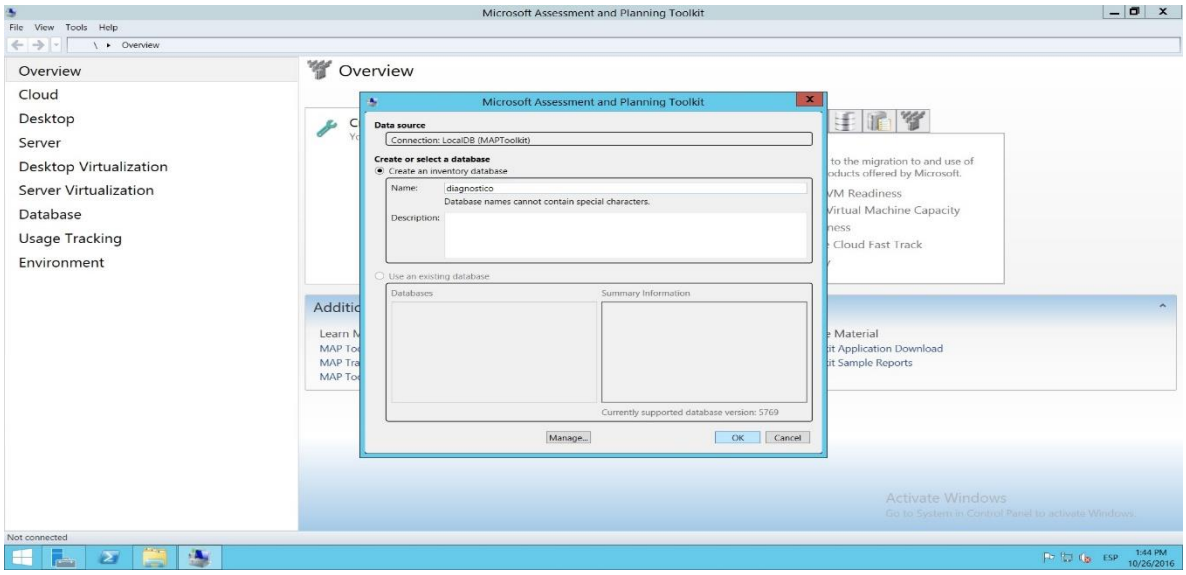
6. Por último se abrirá la pestaña de **Begin the Installation** donde elegimos la opción "Install" y en este paso el programa se procederá a instalar el programa "MapSetup" una vez que termine el proceso elegimos la opción "Finish".



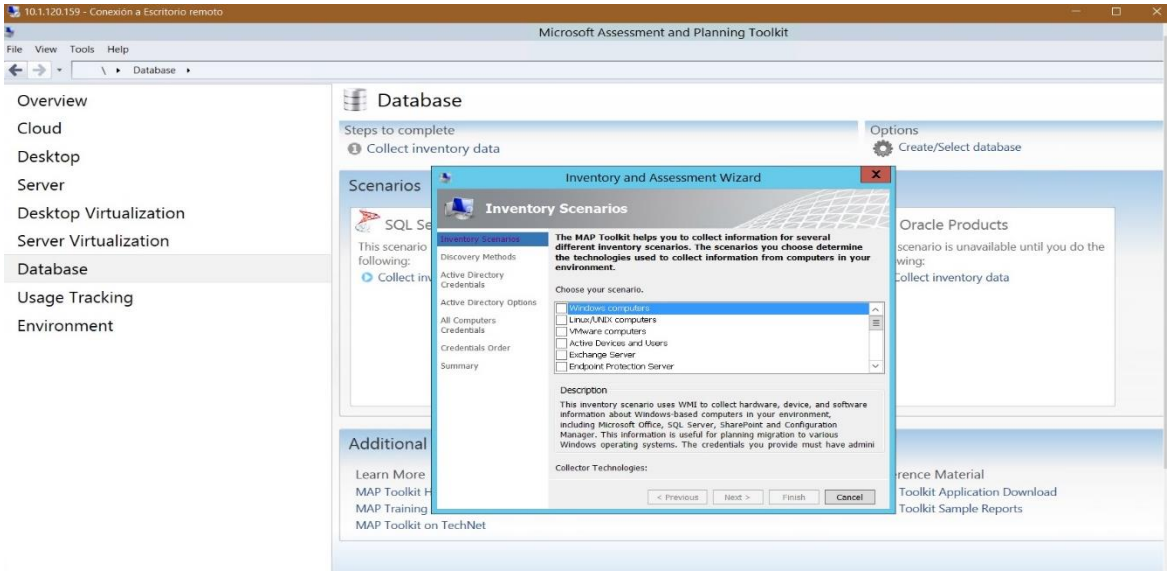


- **Configurar Microsoft Assessment and Planning Toolkit 9.4 una vez instalado.**

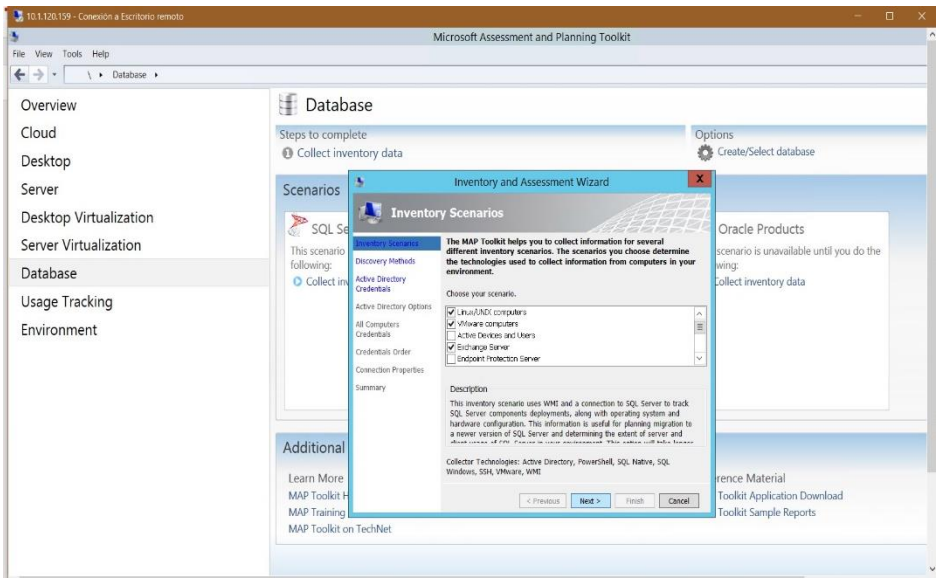
1. Una vez descargada nos pedirá asignar el nombre de la base de datos a la cual vamos a escanear y procedemos a darle clic en "OK". En la Instalación real se utilizó como nombre de base **Diagnostico.**



2. Procedemos abrir la pestaña **Database** y opción **Collect Inventory data** le damos un clic donde nos aparece el recuadro de **Inventory and Assessment wizard**

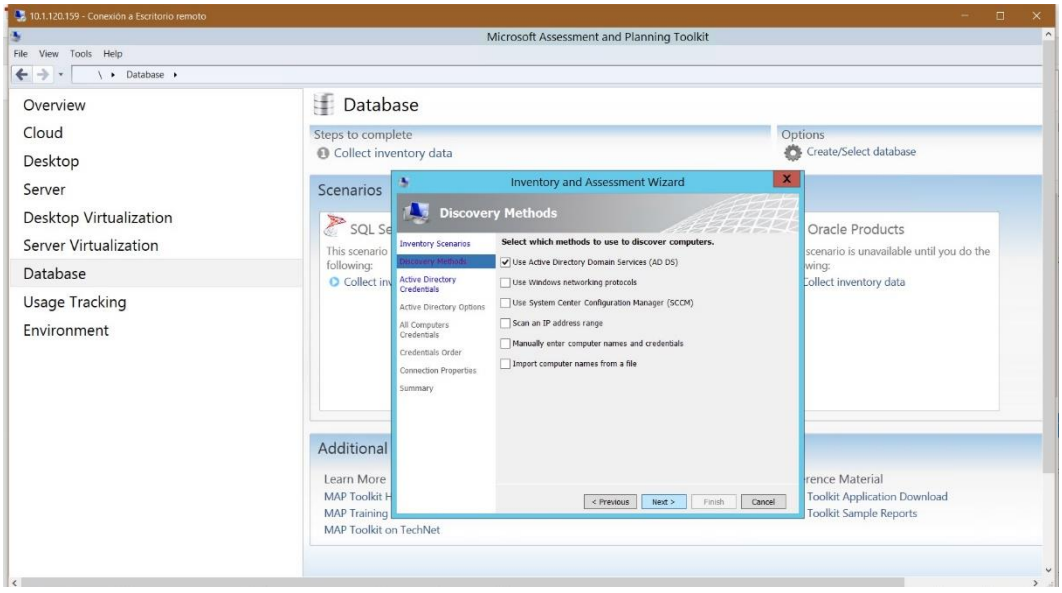


3. Nos mostrara los distintos escenarios para la determinación de los inventarios y las plataformas de los mismos. En este caso se tildaron las opciones “Windows Computers, Linux/Unix computer, VMware Computers, Exchange Server”

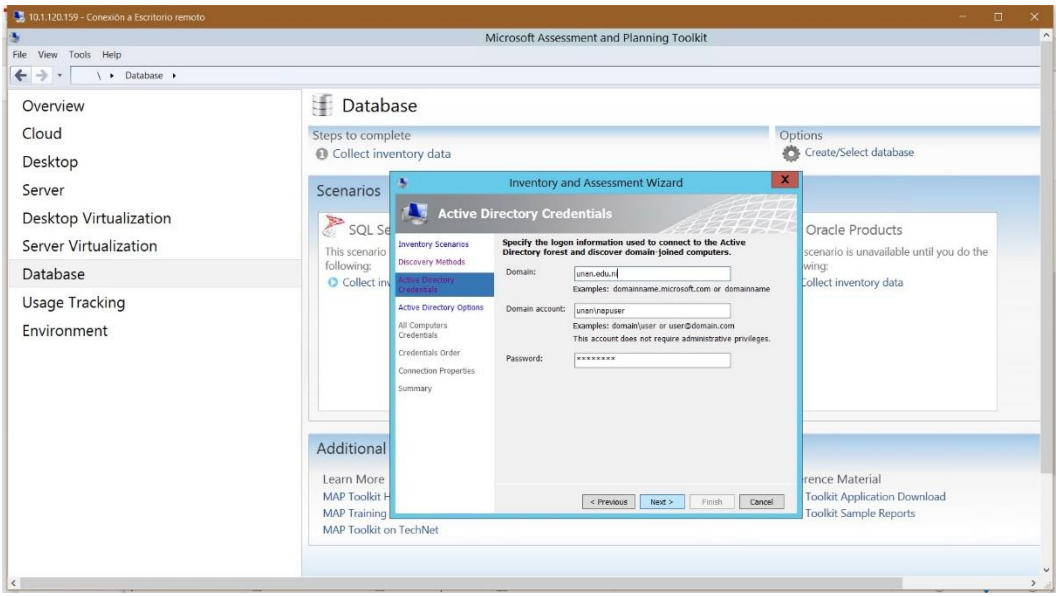


Damos clic en siguiente.

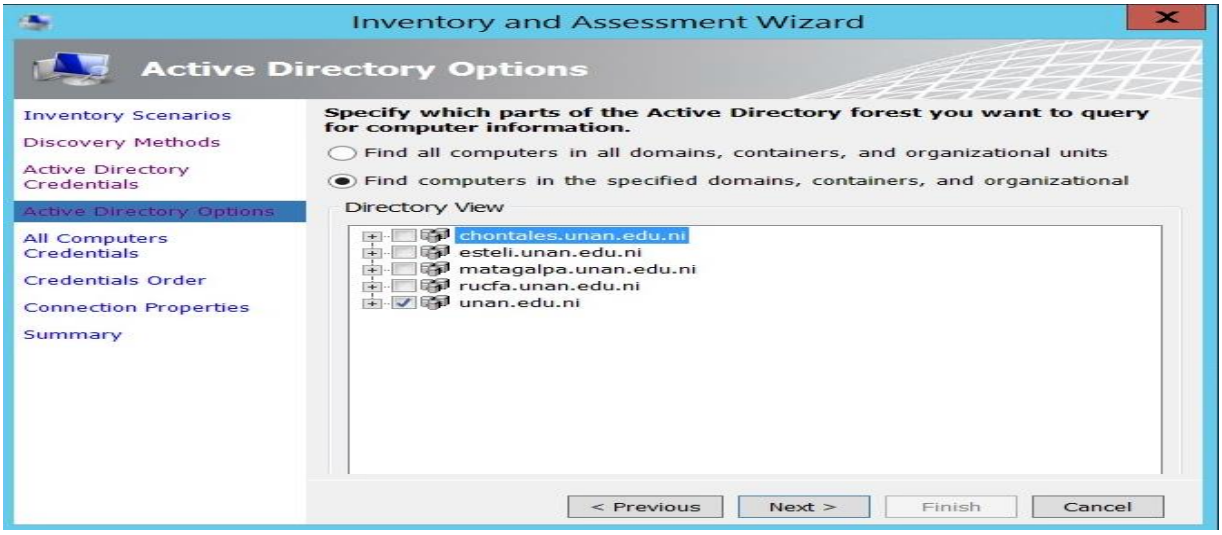
4. Seleccionamos el tipo de método del cual queremos hacer la recolección, en este caso tildamos en “por medio de **Active Directory Domain Services**” dado que trabajamos con el dominio **unan.edu.ni**.



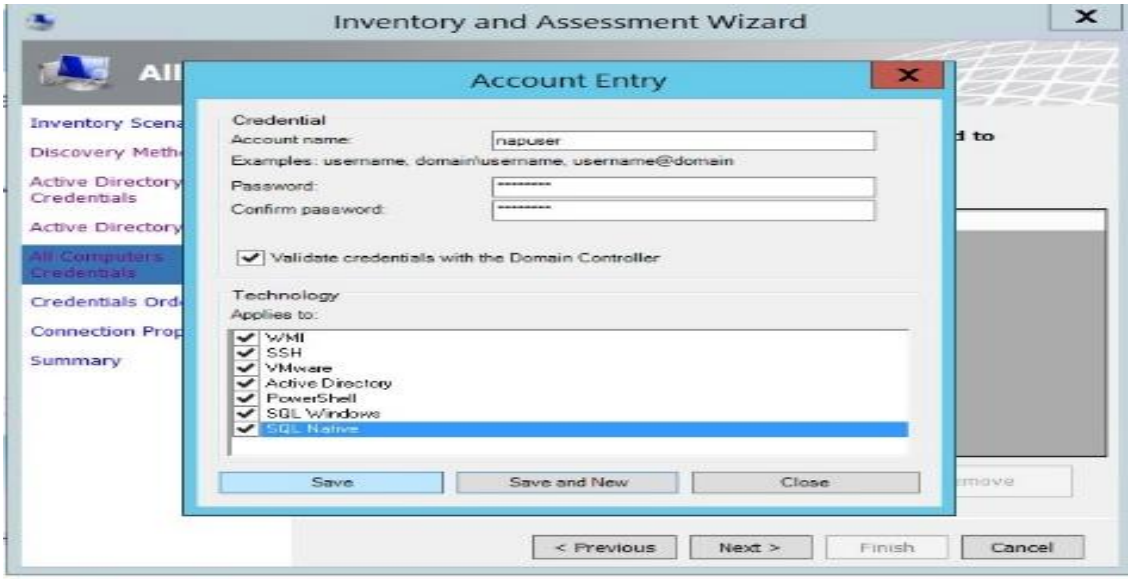
5. Ingresamos los datos de credenciales de administrador y damos clic en siguiente.



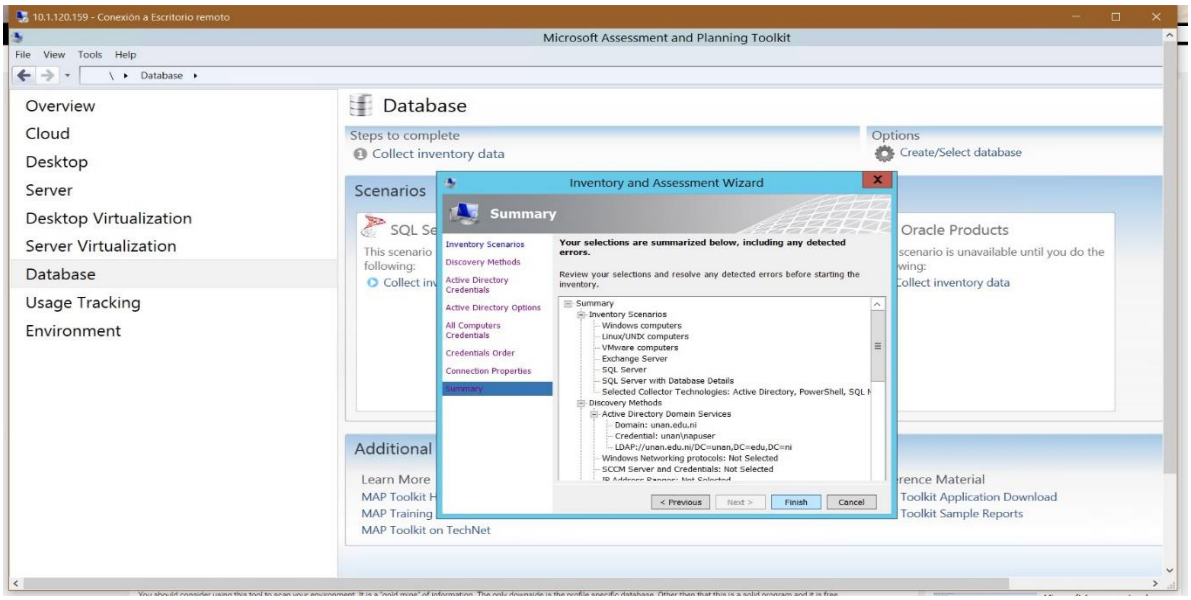
6. Especificamos cuales computadoras dentro de nuestro Árbol, queremos chequear y damos clic en siguiente. En nuestra configuración se especificó solo trabajar con la computadoras del Recinto Universitario Rubén Darío



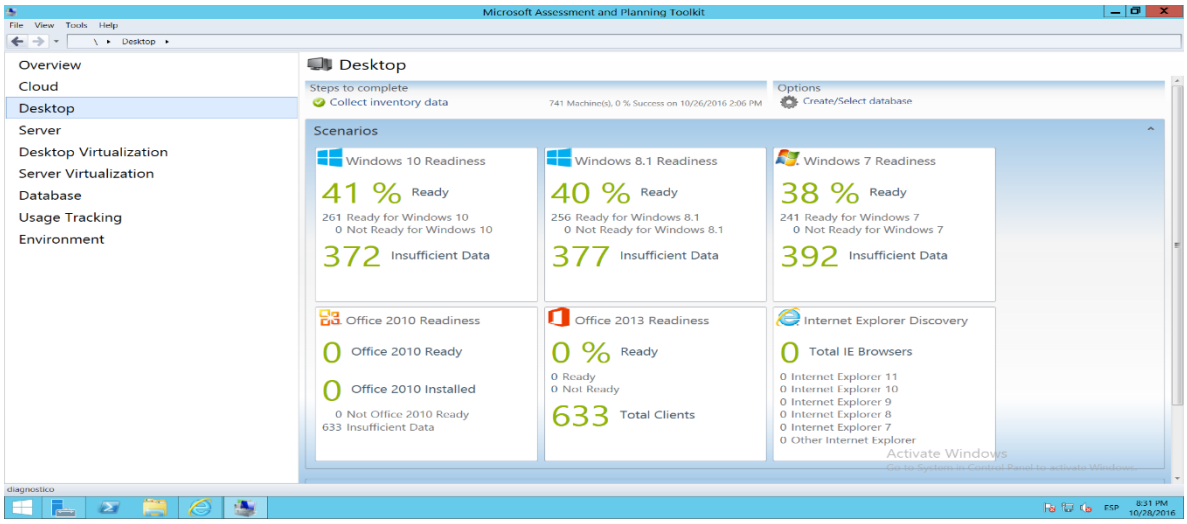
7. Clic en **Next** y especificamos la cuenta que utilizaremos



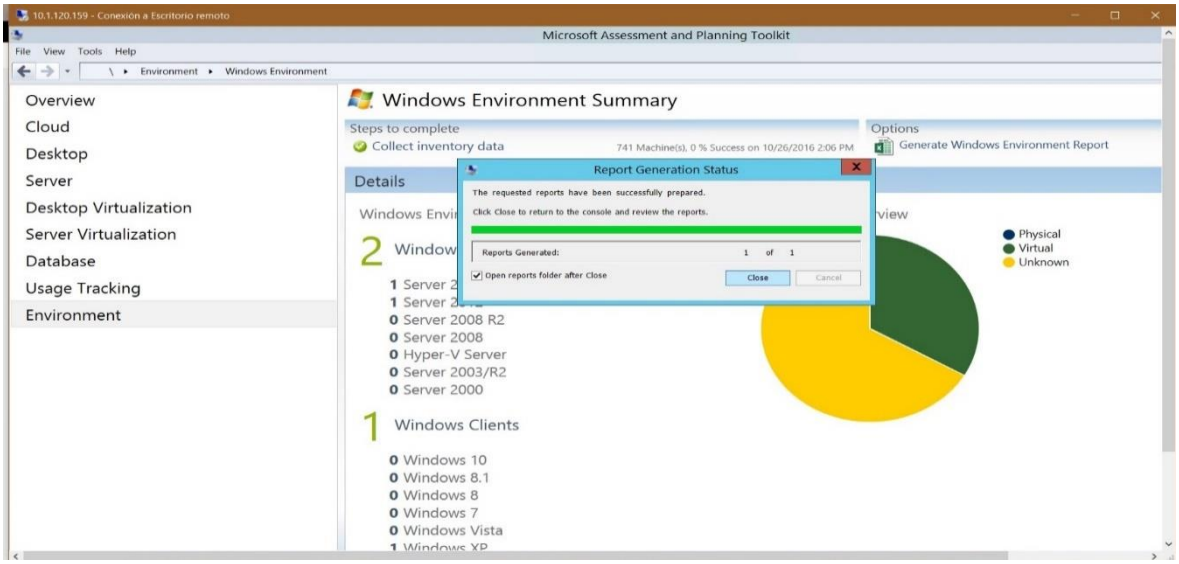
8. Nos muestra un resumen y damos en **Finish**



9. Nos muestra un resumen de los Upgrade que podríamos encontrar dependiendo de los sistemas operativo que nosotros deseamos consultar para saber con el estándar o lo requisitos mínimos con los cuales procedemos a trabajar.



Podemos además generar reporte de los equipos cliente como se muestra a continuación y descargarlos en un archivo Excel al darle clic a la opción **Generate Windows Environment Report** y con eso finalización la función del programa **Microsoft Assessment andPlanning Toolkit 9.4**.



6.1.2. Los recursos disponibles encontrados en el diagnóstico del TIC UNAN-MANAGUA.

- ✓ **Inventario de Hardware (Servidores)**

Marca y modelo	Systema Operativo	Procesador	Memoria	Rol
HP / ProLiant DL380 G5	Microsoft Windows Server 2012 R2 Enterprise	Intel® Xeon® CPU E5430 @ 2.66GHz, 64 bit / 2 cores / 4 p. lógicos	8 GB	Hypervisor
DELL / PowerEdge R710	Microsoft Windows Server 2012 R2 Enterprise	Intel® Xeon® CPU E5520 @ 2.27GHz, 64 bit / 8 cores / 16 p. lógicos.	48 GB	Hypervisor
DELL / PowerEdge 2950	Microsoft Windows Server 2012 R2 Enterprise	Intel® Xeon™ CPU 3.20GHz, 64 bit / 4 cores / 8 p. lógicos	32 GB	Hypervisor
DELL / PowerEdge 2950	Microsoft Windows Server 2012 R2 Enterprise	Intel® Xeon™ CPU 3.20GHz, 64 bit / 4 cores / 8 p. lógicos	32 GB	Hypervisor
DELL / PowerEdge R710	Open SUSE 11.3	Intel® Xeon® CPU E5520 @ 2.27GHz, 64 bit / 8 cores / 16 p. lógicos.	48 GB	Servidor dedicado Moodle
DELL/PowerEdge 1850	Microsoft Windows Server 2012 R2 Enterprise	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor de Backups
DELL/PowerEdge 1850	OpenSuSE 11.3	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor DNS
DELL/PowerEdge 1850	OpenSuSE 11.3	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor de VLANs
DELL/PowerEdge 1850	OpenSuSE 11.3	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor Proxy
DELL/PowerEdge 1850	OpenSuSE 11.3	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor Web
DELL/PowerEdge 1850	OpenSuSE 11.3	Intel Xeon 3,6 GHz, 64 bits	8GB	Servidor VMWare (Registro Académico)
DELL/PowerEdge 1850	Microsoft Windows Server 2012 R2 Enterprise	Intel Xeon 3,6 GHz, 64 bits	8GB	Sistema Financiero

Tabla 1. Inventario de Servidores

- ✓ **Inventario de Software. (Sistema operativo)**

Sistema Operativo	Cantidad	Porcentaje
Microsoft Windows Server 2012 R2	6	50.00%
OpenSUSE 11.3	6	50.00%
Total	**12**	**100%**

Tabla 1: Inventario de Sistemas Operativos

- ✓ **Inventario de servicios**

Máquina Virtual	Memoria	Procesadores	Descripción
APS1	4096	4	Servidor de aplicaciones FrontEnd con ISS, matrícula en línea.
ASG9	4096	2	UTM para Web application Firewall, publicación de sitios online.
AVS	8192	4	Servidor de consola y actualizaciones NOD32
Bugzilla	4096	1	Seguimiento y detección de fallos
CAS	2048	1	Autenticación de aplicaciones Single Sign.
DB1	6288	12	Web server
EXHubTransport	4096	2	Paso de tráfico correo interno y externo.
EXSMailbox	12288	2	Buzón de correo electrónico
OWA	8192	4	Front-e-End, servicio web outlook.
RDCB	1024	1	Servidor para controlar las sesiones remotas a las aplicaciones Windows publicadas por la Web.
RDG	4096	2	Remote Destock
RDSH	4096	2	Servidor de acceso remotovía terminal server.
RRH	2048	2	Servidor de recursos humanos, reloj.
RS	8192	2	
SIU	4096	2	Servidor de sistema de información universitaria
SSP	2048	1	Servidor de gestión de cuentas de usuarios.
VM-VirtualDesktop1	4096	2	Máquina virtual con Windows 7 con VSpace de Ncomputing para ThinCliens.
WEB-DB	4096	2	Aplicación Web FrontEnd DB.
WEB-UNAN	8192	2	Web server
WEB-UNAN2	4096	2	Web server

Tabla 2: Inventario de Servicios

- ✓ **Caracterización de la infraestructura de red, fundamentalmente encontramos cinco características las que a continuación se detalla.**

1. **Redundancia del tráfico de red:** La redundancia es una parte fundamental en una red para implementar HA (Alta disponibilidad o sus siglas en ingles "*High Availability***"**, es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional), pues permite que la misma sea tolerantes a fallas y que tengan una protección contra el tiempo de inactividad y la pérdida de conectividad, en consecuencia aumenta la disponibilidad, productividad y satisfacción del cliente.

2. **Mejores prácticas de red implementadas:** Es la aplicación de estándares internacionales en cuanto estructura, protocolos y organización de la infraestructura de red. Por ejemplo estándares ISO, ANSI, EIA.

3. **Escalabilidad de la red**: Es la capacidad de aumentar la capacidad de trabajo o de tamaño sin comprometer su funcionamiento y calidad normales. Cuando un sistema tiene esta propiedad, se le refiere comúnmente como "sistema escalable". Un ejemplo seria la implementación de dispositivos que permiten el manejo de redes virtuales (VLAN).

4. **Tecnología de almacenamiento en red:** Implementación de dispositivos tales como NAS o SAN que permiten almacenamiento en red para compartir recursos o servicios. Un aspecto muy importante si se desea poseer alternativas de respaldo (backup), clustering de HA y recuperación ante desastres.

5. **Medios de transmisión:** Forma de transmisión de los datos, existen dos tipos, por medio de cableado o de forma inalámbrica. Existen diferentes tecnologías implementadas en los dos casos tales como el uso de cable UTP, fibra óptica, microondas, etc.

✓ **Red Energética**

Aunque en apariencia convencional se da a la red eléctrica un papel sutil en un centro de datos, la realidad es que se vuelve extremadamente importante cuando se habla de alta disponibilidad, ya que al igual que la red de datos debe ser tolerante a fallas o cortes de energía. Se logró identificar que la red eléctrica del proyecto TIC puede perfectamente soportar cortes prolongados de energía con capacidad suficiente para suplir todos los servicios, esto se confirmó por el equipamiento instalado:

1. Generador eléctrico estacionario marca Perkins de 120 KVA, instalado contiguo al centro de datos con cerca perimetral (malla) y transmisión por medio de líneas empotradas.

2. Tres paneles de distribución, un principal (main) y dos paneles auxiliares para distribuir las líneas, estas esta empotradas y siguen buenas prácticas de instalación tal como el uso de códigos de color e implementación de polo a tierra.

3. Una fuente de alimentación continua Tripp Lite SmartOnline trifásico con capacidad de 20KVA para estabilizar y proporcionar energía libre de picos de voltaje.

4. Un Rack de 4 baterías de ciclo profundo con capacidad de almacenamiento de hasta 48V cada una.

- ✓ **Diagnóstico de la situación actual en el Acceso a las redes de datos de la UNAN-MANAGUA**

Actualmente la infraestructura de red cableada de la UNAN-MANAGUA, tiene dos métodos de seguridad en el acceso de las redes de datos uno de ellos es el filtrado de MAC por DHCP que es controlado por un servidor con software libre, este proporciona control de acceso a la red para la emisión o denegación de concesiones DHCP de direcciones IP en función de una dirección de Media Access Control (MAC). Esta característica solo está disponible actualmente para redes IPv4. Actualmente en la UNAN-MANAGUA se registran 2,200 códigos MAC en EL filtrado MAC-ADDRESS por DHCP.

El segundo método seguridad que utiliza es la implementación de redes de área local virtualizadas (VLANs), es un método para crear redes lógicas independientes dentro de una misma red física, varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo). Actualmente se conocen un total de 60 (VLANs), en toda la infraestructura de la red de la UNAN-MANAGUA.

Otro aspecto importante es que el 70% de las aplicaciones correspondían a tecnología Microsoft y como requisito de sistema operativo de escritorio Windows 7 Profesional asignando como un estándar el uso de este sistema operativo o de otros superiores y el resto en su mayoría servicios de red implementados en software libre, claramente existe una inclinación hacia el uso de aplicaciones para servicios y desarrollo en software propietario de Microsoft implicando desde este momento un rumbo de selección de la tecnología NAP que es un servicio de Windows Server 2012 R2 para sufragar la administración en el acceso a las redes de datos.

La red de datos presentaba condiciones muy básicas de transmisión, a pesar que se siguieron estándares y normas de cableado estructurado, no era una infraestructura capaz de permitir escalabilidad de la red y los servicios de transmisión. Por lo que fue necesario adquirir nuevos equipos tales como swicht administrables de capa dos y dispositivos para almacenamiento en la red (NAS o SAN) para permitir redundancia, tolerancia a fallas, respaldo de datos y la implementación de un clúster de alta disponibilidad. Pero también se encontraron algunos aspectos positivos, un ancho de banda de 32 MB para un posible respaldo en la nube, acceso a fibra óptica, dos swicht administrables y dos VLAN configuradas como una primera organización y optimización de la red por medio de la segmentación.

Sin duda la red eléctrica es la que presento los mejores elementos con características satisfactorias para implementar una infraestructura de servidores con alta disponibilidad y mantener accesible los servicios. La capacidad de tolerancia a cortes de energía prolongados cumple con todas las expectativas necesarias.

6.1.3. Diagrama de la red de acceso a datos de la UNAN-MANAGUA

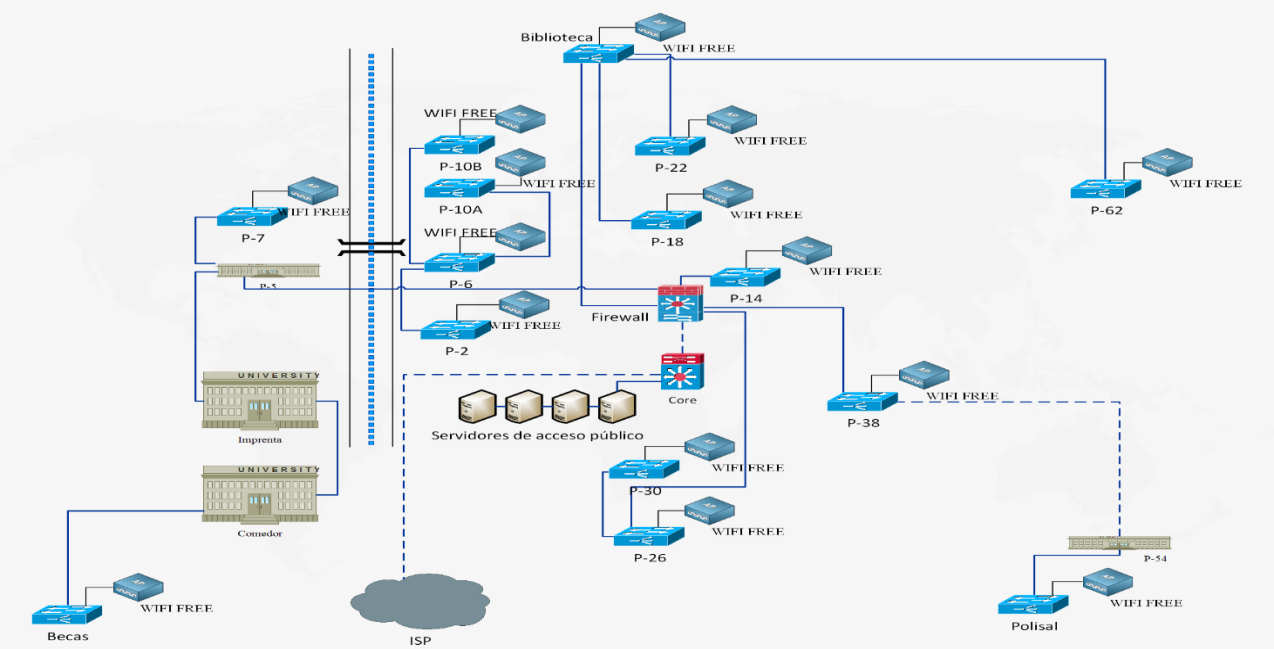


Ilustración 1 Diseño de red actual de la UNAN-MANAGUA (Parodi, 2016)

6.2. Aportes de la tecnología NAP de Microsoft en el control de Acceso a las Redes de datos.

La tecnología de protección de acceso a la red (NAP por sus siglas en ingles), se pensó en un principio para Microsoft Windows server 2003 R2; pero finalmente en su lugar apareció el control de cuarentena de acceso a la red (NAQS, Network Access Quarantine Control), integrándose con el servicio de autentificación de internet (IAS, internet Authentication Service), como solución de control de acceso para clientes de acceso remoto, y fue hasta que salió Windows server Longhorn (2008), que NAP fue difundido ampliamente. Esta nueva tecnología permite especificar cuál es la política de salud de una red.

Si para nosotros una buena política de salud pasa por defendernos de las enfermedades, hacer ejercicio de forma constante, una buena alimentación, etc.; para un equipo una buena política de salud pasaría por disponer de un antivirus a pleno funcionamiento y con las firmas actualizadas, tener instaladas todas las actualizaciones de seguridad, junto a otras medidas de que pueden considerarse como imprescindibles. Para los equipos que no cumpliesen con la política de seguridad establecida, podrían ser dos las circunstancias: en primer lugar que no fuese posible la conexión a la red o como alternativa que esta fuese limitada. En este segundo caso la conexión se realizaría pero en una red aislada, con acceso solo a algunos recursos y a la espera de poder cumplir con los mínimos requisitos de salud.

6.2.1. Protección de Acceso a la Red (NAP)

Se puede decir que NAP es un rol que está presente desde Windows Server 2008 y Windows Vista. El propósito de este rol es permitir la implantación de directivas de integridad sobre los puestos cliente. Es, por tanto, posible restringir el acceso a la red de aquellos equipos que no respetan ciertas condiciones exigidas por el administrador. El Rol asegura, no obstante, la actualización de los equipos que no responden a las condiciones integridad.“La funcionalidad NAP no puede, sin embargo, impedir que un usuario autorizado realice operaciones maliciosas en la red”. (Bonnet, 2012)

6.2.2. El servidor de directivas de red Network Policy Server (NPS)

Servidor de directivas de redes (NPS) permite crear y aplicar directivas de acceso a la red en toda la organización con fines de mantenimiento de clientes, autenticación de solicitudes de conexión y autorización de solicitudes de conexión. Además, puede usar NPS como un proxy RADIUS (Servicio de autenticación remota telefónica de usuario) para reenviar solicitudes de conexión a un servidor que ejecute NPS u otros servidores RADIUS que configure en grupos de servidores RADIUS remotos.

El servidor de directivas de redes NPS permite configurar y administrar de forma centralizada directivas de autenticación de acceso a la red, autorización y mantenimiento de clientes con las tres características siguientes:

- ✓ **RADIUS server**. NPS realiza la autenticación, autorización y administración de conexiones de forma centralizada para los conmutadores de autenticación inalámbricos, conexiones de acceso remoto telefónico y red privada virtual (VPN). Cuando se usa NPS como un servidor RADIUS, se configuran los servidores de acceso a la red, como los puntos de acceso inalámbrico y los servidores VPN, como clientes RADIUS en NPS. Además, se configuran las directivas de redes que usa NPS para autorizar las solicitudes de conexión.

- ✓ **RADIUS proxy**. Cuando se usa NPS como un proxy RADIUS, puede configurar las directivas de solicitud de conexión que indican al servidor NPS qué solicitudes de conexión debe reenviar a otros servidores RADIUS y a qué servidores RADIUS desea reenviar las solicitudes de conexión.

- ✓ **Network Access Protection (NAP) policy server**. Cuando se configura NPS como un servidor de directivas de NAP, NPS evalúa los informes de mantenimiento (SoH) enviados por equipos clientes compatibles con NAP que desean conectarse a la red. NPS también actúa como un servidor RADIUS cuando está configurado con NAP, realizando tareas de autenticación y autorización para las solicitudes de conexión. Puede configurar directivas y opciones de NAP en NPS, lo que incluye validadores de mantenimiento del sistema (SHV), directivas de mantenimiento y grupos de servidores de actualizaciones que permiten a los equipos cliente actualizar su configuración para ser compatibles con la directiva de red de la organización.

6.2.3. Métodos de cumplimiento NAP

El servicio NAP posee métodos de cumplimiento. Estos métodos de cumplimiento permiten gestionar los distintos accesos a la red local (VPN, Red Local, Wi-fi).

- **Cumplimiento NAP para 802.1x**

El cumplimiento de NAP para el control de acceso a la red mediante el puerto 802.1x se implementa usando un servidor que ejecuta el servidor de directivas de redes (NPS) y un componente del cliente de cumplimiento del host Protocolo Autenticación Extensible (EAP). En el cumplimiento basado en el puerto 802.1x el servidor NPS indica aun conmutador de autenticación 802.1x o un punto de acceso inalámbrico compatible con 802.1x que coloque cliente 802.1x en una red de actualizaciones mediante la aplicación de filtros IP o un identificador de LAN virtual a la conexión. El cumplimiento 802.1x ofrece una restricción de red segura para todos los equipos que obtienen acceso a la red usando servidores de acceso a la red compatibles con 802.1x.

- **Cumplimiento NAP para DHCP**

El cumplimiento DHCP se implementa mediante un componente de servidor de cumplimiento NAP para DHCP, los servidores DHCP y NPS pueden aplicar directivas de mantenimiento cuando un equipo intente conceder o renovar una dirección IP versión 4 (IPv4)..

- **Cumplimiento NAP para comunicaciones IPsec**

El cumplimiento NAP para las directivas del protocolo de seguridad de internet (IPsec) para Firewall de Windows se implementa usando un servidor de certificados de mantenimiento, un servidor de autoridad de registro de mantenimiento (HRA), un servidor que ejecute el servidor NPS y un cliente de cumplimiento IPsec.

El servidor de certificados de mantenimientos emite certificados x.509 para clientes NAP cuando estos van a ser compatibles. Estos certificados se usan a continuación para autentificar clientes NAP cuando inician comunicaciones IPsec con otros clientes NAP en una intranet.

El cumplimiento IPsec limita la comunicación la conmutación en la red a los clientes compatibles y ofrece la implementación más segura de NAP. Debido a que este método de cumplimiento usa IPsec, puede definir requisitos para proteger las comunicaciones por direcciones IP o por números de puerto TCP-UDP.

- **Cumplimiento NAP para la puerta de enlace de escritorio remoto**

La puerta de enlace de escritorio remoto es un servicio del rol de escritorio remoto disponibles en Windows server 2012 R2. Mediante la puerta de enlace de escritorio remoto, los usuarios autorizados pueden conectarse desde cualquier dispositivo conectado a internet a servidores de terminal Server y escritorios remotos de la red de la organización. Además, es posible aplicar y supervisar el estado de mantenimiento de los equipos cliente que son clientes de escritorio remoto con protección de acceso a redes.

El cumplimiento NAP para la puerta de enlace de escritorio remoto se implementa con un servidor que ejecuta servidor de directivas de redes y un servidor de puerta de enlace de escritorio remoto**.**

- **Cumplimiento NAP para VPN**

El cumplimiento NAP para redes móviles virtuales (VPN) se implementa usando un componente de servidor de cumplimiento de VPN y un componente de cliente de cumplimiento de VPN. Al usar este método de cumplimiento, los servidor VPN pueden aplicar directivas de mantenimiento cuando los equipos clientes intentan conectarse a la red atreves de una conexión VPN. La aplicación de VPN proporciona acceso de red limitado seguro a todos los equipos que obtienen acceso a la red promedio de una conexión VPN.

6.2.4. Servidor de saneamiento.

El servicio NAP va contener un servidor de directivas de cumplimientos presente en el área local. Este servidor se encargara de decidir si el puesto cliente que solicita el servicio se encuentra en el área local o en la red restringida, también llamada red de cuarentena. En la red de cuarentena existe un servidor de actualizaciones (WSUS…) a disposición de los clientes con el objetivo de poder actualizar sus equipos. Una vez realizada la operación, es posible que vuelva a integrarse en la red de producción.

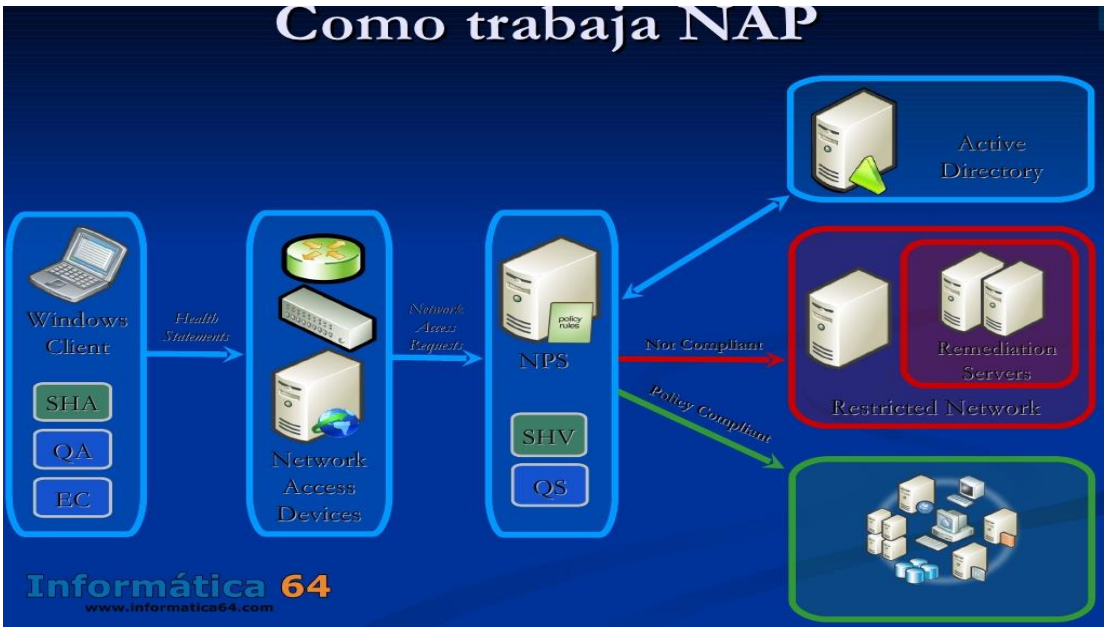


Ilustración 2 Muestra el servicio NAP por un arquitectura servidor y una arquitectura cliente distintas una de la otra". (Bonnet, 2012)

6.2.5. Arquitectura del cliente NAP

El cliente posee una capa de componentes Clientes de Cumplimiento. Cada Cliente se define mediante un tipo de acceso a la red específico (VPN, Wi-Fi…). Están concebidos para funcionar como un tipo de cliente de cumplimiento (El cliente de cumplimiento NAP para DHCP se ha concebido para funcionar con un cumplimiento NAP basado en DHCP). Algunos fabricantes de aplicaciones pueden proveer sus propios agentes.

Existe una capa de aplicaciones de Agente de Mantenimiento del sistema (en inglés SHA, de *System Health Agent*) que incluyen los componentes que gestionan y definen uno o varios elementos de mantenimiento del sistema. Por ejemplo, es posible utilizar un agente de mantenimiento del sistema para las firmas de antivirus, y otro agente de mantenimiento del sistema para las actualizaciones del sistema operativo. El Agente de mantenimiento del sistema se corresponde con un servidor de actualizaciones. Como con los propios clientes de cumplimiento, los fabricantes de aplicaciones pueden proveer sus propios agentes.

El Agente NAP gestiona la información de cumplimiento actual del cliente NAP y facilita la comunicación entre las capas del cliente de cumplimiento de actualización y el agente de mantenimiento del sistema.

La API (interfaz de programación de aplicaciones) del agente de mantenimiento del sistema permite a los agente de mantenimiento del sistema inscribirse en el agente NAP para indicar el estado del sistema. Se solicita también, responder a las consultas del agente NAP.

Funcionamiento del Agente de Mantenimiento del sistema SHA

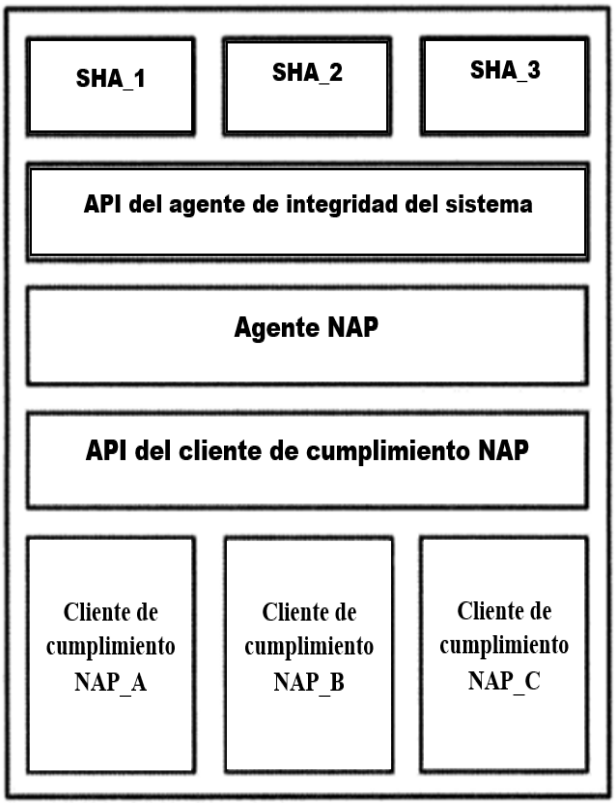


Ilustración 3 Comunicación entre el SHA y el API (Bonnet, 2012)

6.2.6. Arquitectura del servidor NAP

El servidor NPS recibe el mensaje de solicitud de acceso RADIUS (remove Access Dialin User service) y extrae la declaración de mantenimiento del sistema. A continuación, la transmite al componente servidor de administración NAP.

El servidor de administración NAP facilita la comunicación entre el servidor NPS y programas de validación de mantenimiento del sistema (SHV). Cada programa de validación de mantenimiento del sistema se define mediante uno o varios tipos de elementos y puede establecer una correspondencia con un agente.

La API del programa de validación de mantenimiento del sistema provee un juego de llamadas de función que permite a los programas de validación inscribirse desde el componente Servidor de administración NAP, recibe declaraciones de mantenimiento y enviar las respuestas.

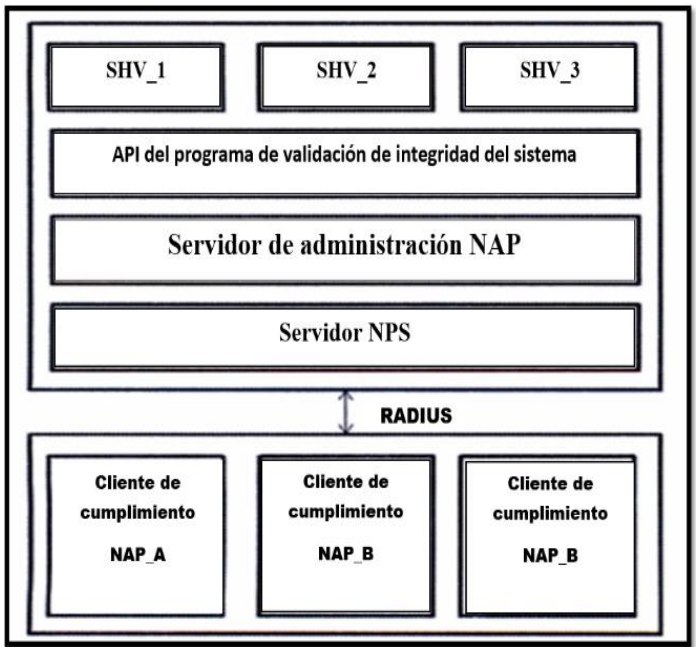


Ilustración 4 Servidor NPS como puente de comunicación con el servidor de NAP (Bonnet, 2012)

6.2.7. Las distintas directivas en NAP

NAP contiene tres tipos de directivas de red, directivas de control de integridad y directivas de solicitud de conexión.

La directiva de red posee varios elementos:

- Activación o no de la directiva.
- Autorización o bloqueo de acceso, así como el método el método de conexión de red
- Condición de activación (horario, sistema operativo)
- Método de autenticación.
- Tipo de medio utilizado (Wi-Fi, cable Ethernet).

Con el objetivo de explotar el programa de validación de administración de la seguridad Windows, es necesario configurar una directiva de control de inteligencia y aplicarla al programa de validación de administración del sistema.

Existen varios comportamientos posibles (superación de todos los controles SHV, superación de uno o varios controles SHV). Esta directiva permite determinar el acceso que va a ofrecer al puesto que ha realizado la solicitud. Existen varios niveles de acceso dentro de los cuales se encuentran:

- Acceso completo
- Acceso limitado
- Acceso bloqueo

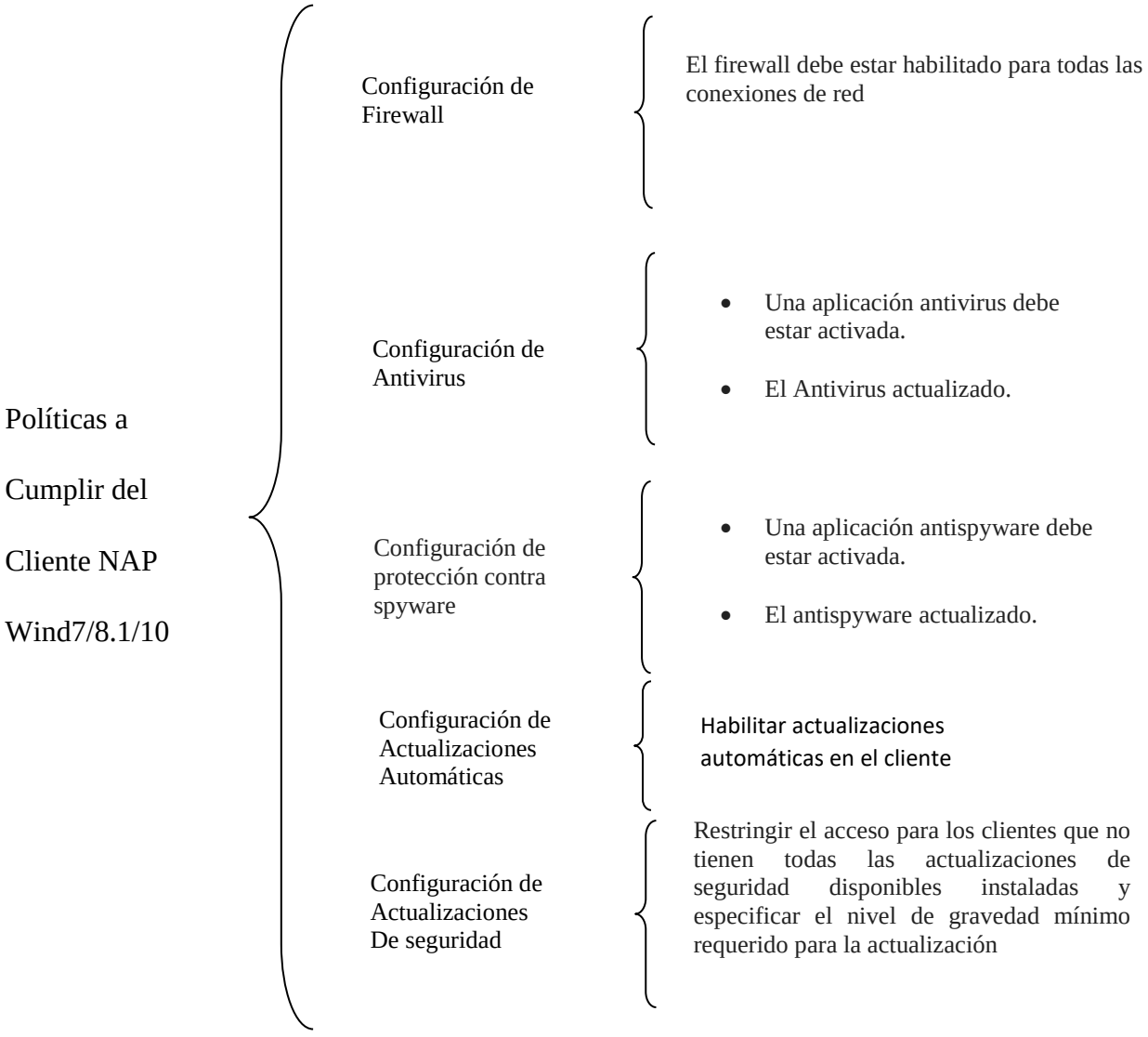
La directiva de solicitud de conexión permite indicar donde se realiza el procedimiento (de manera local o mediante un servidor RADIUS).

6.2.8. Requisitos para la Infraestructura del NAP

Para la implementación de NAP es necesario montar toda una infraestructura que cuente con:

- Active Directory
- Servidores de directivas de redes (NPS service)
- Servidores de protocolo de configuración dinámica de Host (DHCP servers)
- Dispositivos compatibles con IEEE 802.1x
- Servidores de certificados de mantenimiento (VHS servers)
- Servidores de red privada virtual (VPN servers)
- Agente de mantenimiento de sistemas (Windows 7SP1/8.1/10, Windows server 2012,Windows server longhorn+ agente NAP)

- Servidor de administración NAP (NPS)
- Validador de mantenimiento (NPS)
- Base de datos de cuentas de usuarios (directorio activo)
- Servidor de remediación (WSUS, SMS, Antivirus/Antimalware server, DNS server).



6.3. Implementación de la tecnología NAP, utilizando Windows Server 2012 R2.

6.3.1. Introducción a Windows Server 2012 R2

"Windows Server 2012 R2 es un sistema operativo (Orientado al Cloud) de la gama de servidores de Microsoft. Aparece en el mercado para reemplazar a Windows Server 2008 R2 con el fin de aportar novedades como:" (ASIMANE, 2014)

- ✓ Novedades en el **Servicio de Certificado de Active Directory (AD CS).**
- ✓ Novedades en **Active Directory Domain Services (AD DS).**
- ✓ Novedades en **Active Directory Rights Management Services (AD RMS).**
- ✓ Novedades de **Dynamic Host Configuration Protocol (DHCP).**
- ✓ Novedades en los **Servicios de Nombres (*Domain Name System – DNS).***
- ✓ Novedades en la **gestión de dirección IP (*IP Management – IPAM).***
- ✓ Novedades en **BranchCache.**
- ✓ Novedades en **PowerShell v4.**
- ✓ Novedades en la **Interfaz Gráfica.**
- ✓ Novedades en **Hyper – V.**
- ✓ Novedades en el **Cluster de Conmutación por error.**

https://www.microsoft.com/es-es/server-cloud/products/windows-server-2012-r2/overview.aspx

6.3.2. Existen cuatro ediciones de Microsoft Windows Server 2012 R2:

- ✓ **Windows Server 2012 R2 Foundation:** Esta edición con funcionalidad limitada del sistema operativo serviría para las pequeñas organizaciones que deseen adoptarse de una solución todo en uno, que esta edición solo está disponible en versión OEM (Preinstalado en equipos nuevos). En esta edición no es posible realizar virtualización con Hyper – V.

- ✓ **Windows Server 2012 R2 Essentials:** Esta edición con funcionalidad limitada del sistema operativo está más adaptada a las PYMES. Es esta edición tampoco es posible realizar virtualización con Hyper – V.

- ✓ **Windows Server 2012 R2 Standard:** Esta edición más completa del sistema operativo corresponderá a estructuras más importantes. Se encuentra disponible en todas las funcionabilidades excepción de la virtualización de Hyper-V, que está limitada a solo dos máquinas virtuales.

- ✓ **Windows Server 2012 R2 Datacenter:** Esta edición para el nuevo sistema operativo de Microsoft es la más completa corresponderá a estructuras más importantes. Ofrece todas las funcionalidades existentes sin ninguna limitación a nivel de creación de máquina virtual. Esta edición corresponderá perfectamente a entornos complejos como, por ejemplo estructuras Cloud.

En el marco de este trabajo, estaremos utilizando la versión Datacenter de Windows Server 2012 R2.

La configuración mínima para instalar Windows Server 2012 R2 es la siguiente:

- ✓ **Procesador:** Arquitectura de 64 bits exclusivamente, velocidad de 1,4 GHz como mínimo (es recomendable contar con un procesador multinúcleos).
- ✓ **Memoria RAM:** 512 MB Mínimo (recomendado contar por lo menos con 1024 MB).
- ✓ **Disco Duro:** 32 GB mínimo (la instalación real requiere en torno 10 GB, es necesario que el sistema operativo cuente con espacio para gestionar la memoria en el disco).
- ✓ **Un monitor:** Una resolución mínima de 800 x 600 (es recomendable contar con una resolución mínima de 1024 x 768).

En la figura 5: Se muestra los roles que se pueden instalar en cada edición de Windows Server 2012 R2

Rol de servidor	Datacenter y Standard	Essentials	Foundation
DHCP Server	●	●	●
DNS Server	●	■	●
Fax Server	●	●	●
Servicios de archivo	●	■[5]	◎[5]
Hyper-V	●	●	○
Políticas de Red y Accesos	●	■	○
Servicios de documento e impresora	●	●	●
Acceso remoto	●	■[6]	◎[6]
Servicios de Escritorio Remoto[7]	●	■[8]	◎[9]
Servicios UDDI	●	●	●
Web Server (IIS)	●	■	●
Windows Deploy Services	●	●	●
Windows Server Essentials Experience	●	■	○
Windows Server Update Services (WSUS)	●	●	○

● *Funcionalidad completa*
◎ *Parcial / limitada*
■ *Instalada/configurada automáticamente*
○ *No disponible*

Ilustración 5 Roles disponible en cada edición (https://msdn.microsoft.com/es-es/library/hh831786(v=ws.11).aspx, 2016)

6.3.3. Instalación mínima (Server Core)

La instalación mínima de Windows Server 2012 R2, también llamada instalación Server Core, corresponde a la instalación del sistema operativo desprovisto de su interfaz gráfica de usuario. La administración de un servidor instalado en modo Server Core se realiza por líneas de comandos un vez conectado en local al equipo. Sin embargo, será posible administrar un Server Core empleando las herramientas de administración grafica desde otro equipo de la red que tenga previamente instalados los componentes **RSAT** (*Remote Server Administration Tool*). Cuando se instala un servidor en modo Server Core, solamente se puede instalar los roles y características siguientes:

- ✓ Servicio Active Directory (AD DS).
- ✓ Servicio Active Directory Ligthweight Directory Services (AD LDS).
- ✓ Servicio Active Directory Certificate Services (AD CS).
- ✓ Servicio DHCP
- ✓ Servicio DNS
- ✓ Servicio de archivos y almacenamiento.
- ✓ Servicio de transferencia inteligente en segundo plano (BITS).
- ✓ BranchCache.
- ✓ Hyper-V.
- ✓ Internet Information Services (IIS).
- ✓ Servicio de Impresión.
- ✓ Streaming Media Services.
- ✓ ISCSI.
- ✓ Equilibrio de carga de red (Load Balancing).
- ✓ MPIO (Multipath I/O).
- ✓ Experiencia de calidad de audio y video de Windows (Wave).
- ✓ Servicio Telnet.
- ✓ Migración Unix.

Por defecto los roles y características de servidor no se instalan en el disco duro durante la instalación del sistema operativo en modo de instalación mínima. Para instalar un componente, se deberá de contar con acceso a una conexión a Internet en la máquina para que el sistema pueda descargar automáticamente los componentes restantes. Si no existe un acceso a internet disponible, es posible cargar las fuentes de instalación de Windows a partir de un DVD-ROM de instalación escribiendo el comando en la powershell siguiente.

Get-Windowsimage –imagepath <Unidad:> \ sources \install.wim

Es preciso memorizar el índice correspondiente a la versión de instalación del sistema operativo y, a continuación, a escribir el siguiente comando para instalar un rol o características de servidor:

Install-WindowsFeature <Nombre del rol /Características> -source

Win: <Unidad: \ sources \install.wim> :< index>

Para conocer un rol o características de servidor, bastara con escribir el comando en la powershell siguiente: ***Get-WindowsFeature***

Para convertir a una instalación Servidor con una GUI con Windows PowerShell: siga los pasos del siguiente procedimiento.

1. Determine el número de índice de una imagen de Servidor con una GUI (por ejemplo, SERVERDATACENTER, no SERVERDATACENTERCORE) con ***Get-WindowsImage -ImagePath <path to wim>\install.wim.***
2. Ejecute: ***Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell –Restart –Source c:\mountdir\windows\winsxs***
3. O bien, si desea usar Windows Update como el origen en lugar de un archivo WIM, use este cmdlet de Windows PowerShell:

   Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell –Restart

6.3.4. Instalación Grafica con una GUI

Con esta opción, se instalan todas las herramientas y la interfaz de usuario estándar. Los roles y características de servidor se instalan con Administrador del servidor o con otros métodos.

- **Interfaz de usuario:** interfaz gráfica de usuario estándar ("Shell gráfico de servidor"). El Shell gráfico de servidor incluye el nuevo Shell de Windows 8, pero no incluye la Tienda Windows ni compatibilidad con las aplicaciones de la Tienda Windows. Para habilitar la compatibilidad con las aplicaciones de la Tienda Windows, instale la característica Experiencia de escritorio.

- **Instalar, configurar, desinstalar roles de servidor localmente:** con el Administrador del servidor o con Windows PowerShell.

  Instalar, configurar, desinstalar roles de servidor remotamente: con el Administrador del servidor, RSAT o Windows PowerShell.

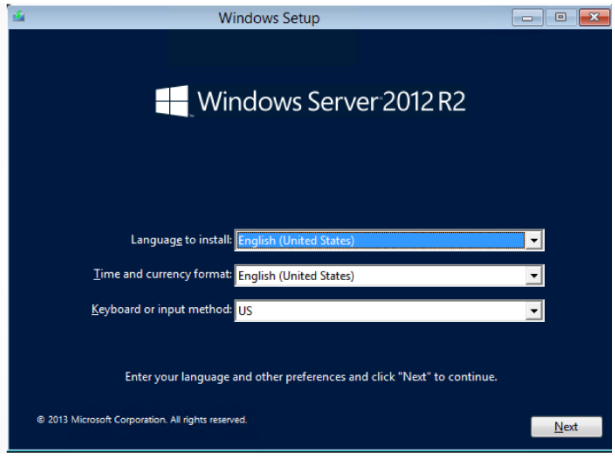
- **Microsoft Management Consolé:** instalada

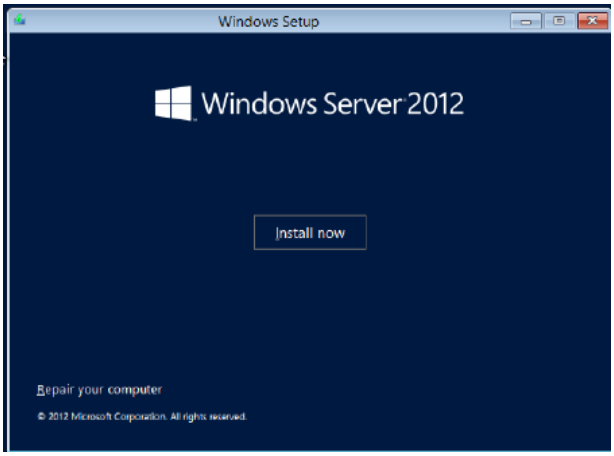
- **Experiencia de escritorio:** instalable con el Administrador del servidor o con Windows PowerShell.

- **Para convertir a una instalación Server Core con Windows PowerShell:** ejecute el siguiente cmdlet:
  Uninstall-WindowsFeature Server-Gui-Mgmt-Infra –Restart

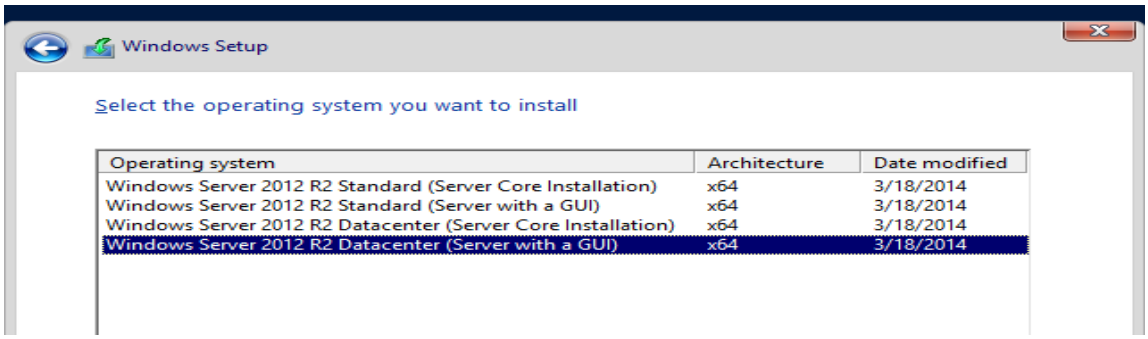
6.3.5. Instalación de Windows Server 2012 R2 en el dominio unan.edu.ni:

1. Conecte la unidad y arranque desde el DVD de instalación de Windows Server 2012 R2. Seleccionar idioma, el formato la hora, y el diseño del teclado damos clic en "**Next**". Aparecerá la pestaña de instalación donde daremos clic en el cuadro de "**Install now**"

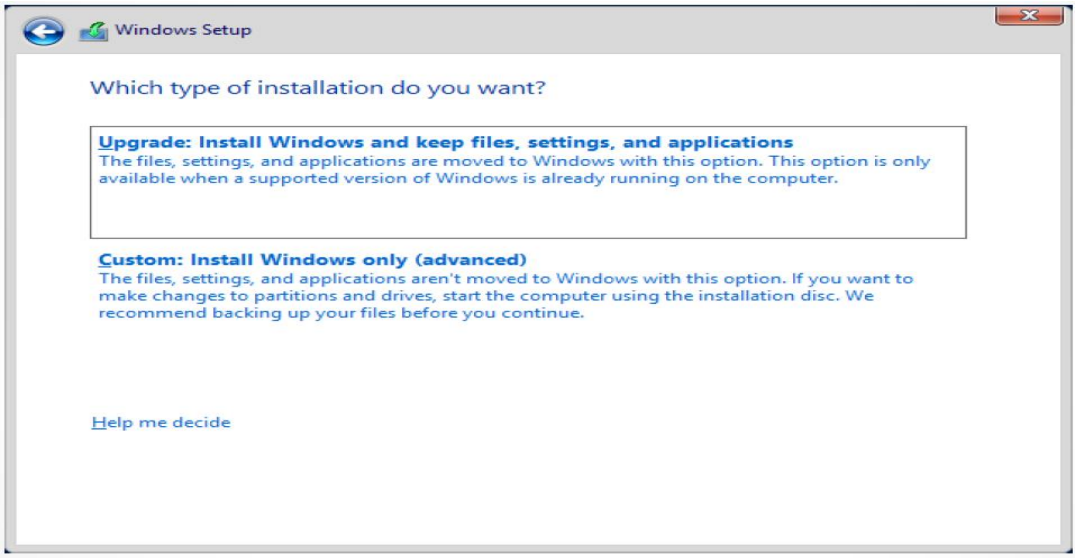




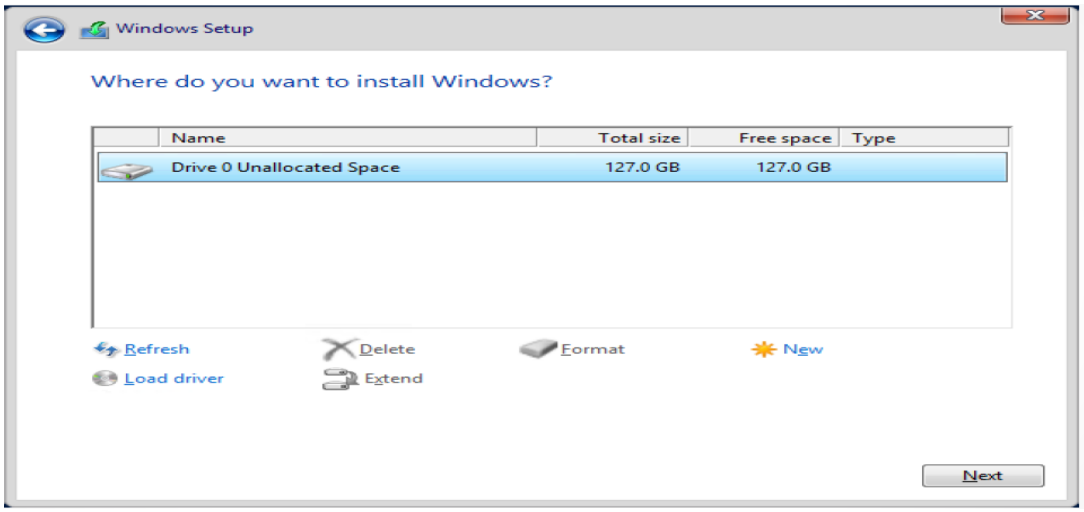
2. Seleccionamos la edición de Windows Server 2012 R2 a utilizar en este caso la edición más completa y para mejores prácticas es la **DatacenterGUI 64x** cuyas características ya hemos mencionamos.



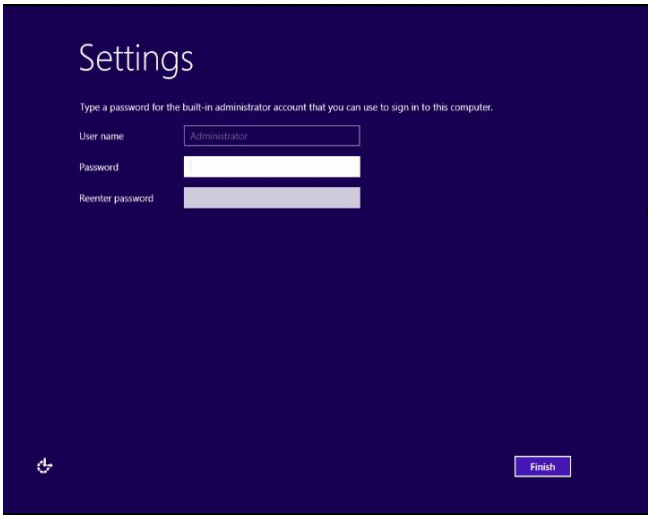
3. En la siguiente pestaña seleccionamos “Custom”: Instalar Windows solamente (avanzado).

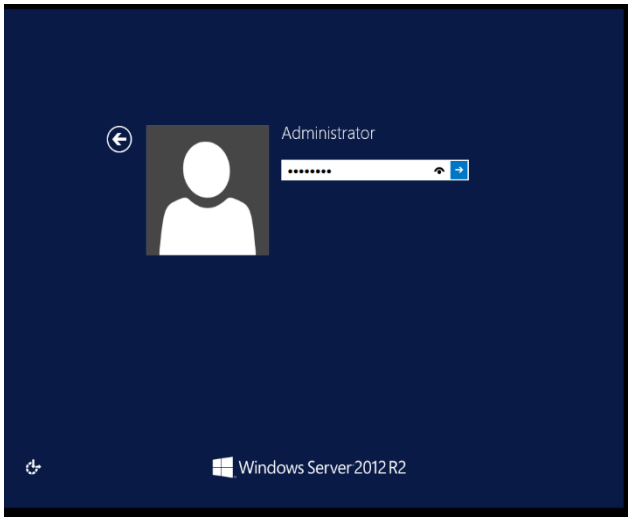


4. Procedemos a seleccionar la partición en la que se desea instalar Windows Server 2012 R2 y damos clic en **Next**.

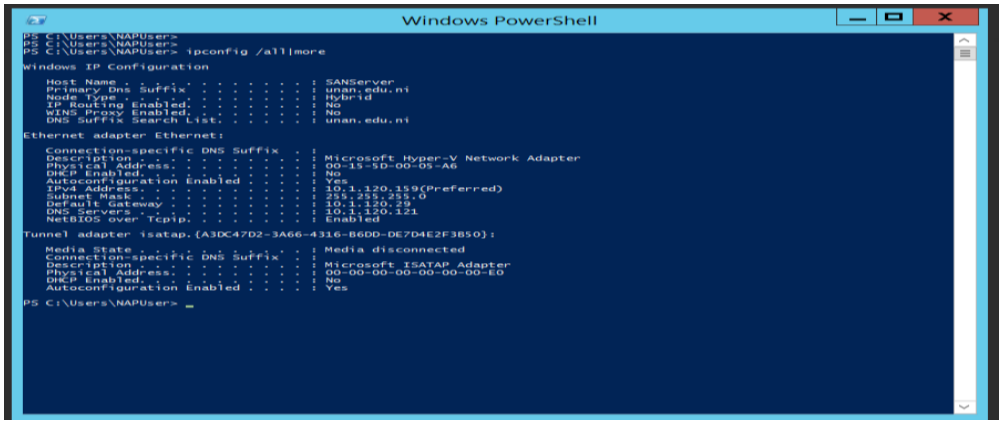


5. Cuando la instalación se haya completado, se deberá establecer las credenciales de administrador a utilizar y luego dar clic en "**Finish"** e iniciaremos sesión con la contraseña de administrador que anteriormente digitamos. En este punto la instalación ya terminaría y tendríamos un Windows Server listo para trabaja e utilizar.

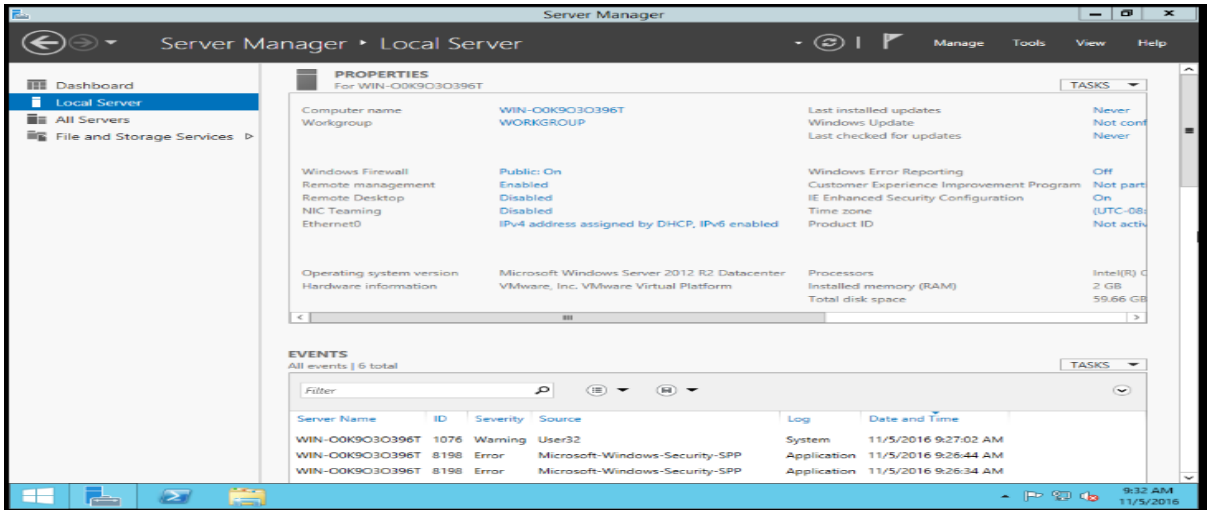




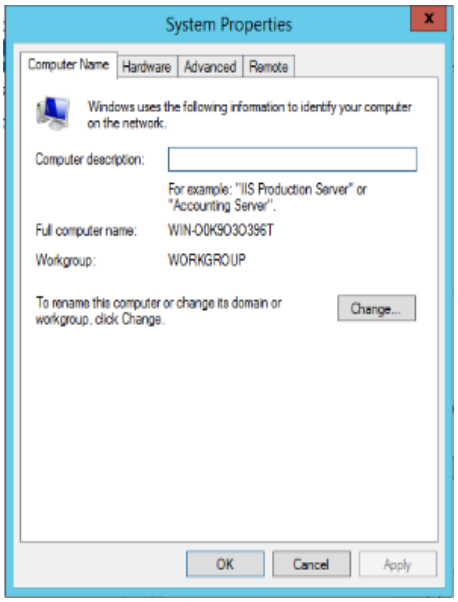
6. Para agregar un maquina al dominio unan.edu.ni del modo GUI, primero ejecutamos el comando ***ipconfig /all|more*** para verificar que en los parámetros de TCP/IP de la tarjeta se encuentre el DNS.

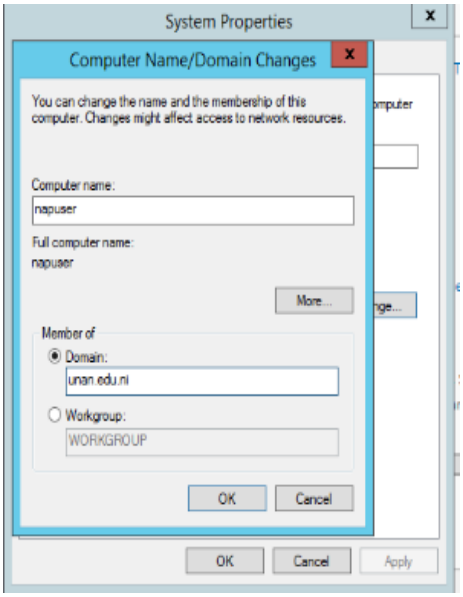


7. Ingresamos a *Server Manager – Local Server*



8. Clic en *Computer Name* o *Workgroup y luego* Clic en *Change* procedemos a registrar el nombre de la máquina y el dominio al cual se va agregar.





6.4. Pasos para implementar de NAP: Instalación de la Entidad emisora de certificados "Active Directory Domain Services (AD DS)".

"Microsoft implementa la Infraestructura de Clave Pública (PKI) a través de "Active Directory Certificate Services". Esta implementación es un modelo jerárquico de entidades de certificación (conocido como "Hierarchical CA Model" desde un punto de vista más técnico). Esto significa que puede existir una entidad raíz y entidades subordinadas que emitan certificados, y la confianza en la entidad raíz significa confiar en todas las entidades subordinadas que ésta tenga."(Di Loreto, 2016)**Jerarquías de Entidades de Certificación**

6.4.1. Jerarquías de Entidades de Certificación

La implementación más simple tendrá una sola CA (Certification Authority). Sin embargo, existe la posibilidad de implementar soluciones escalables que contengan múltiples CAs definidas en roles principales e hijas.

6.4.2. Entidades de Certificación Raíz (Root Certification Authority)

En lo alto de la jerarquía se encuentra la Entidad de Certificación Raíz, o Root CA. Es el mayor nivel de confianza dentro de una Infraestructura de Clave Pública dentro de la organización. Si ésta se encuentra comprometida en la seguridad, todas las Entidades "subordinadas" lo estarán.

Los certificados que emite una Entidad de Certificación Raíz pueden ser usadas para muchos fines. Sin embargo, en una infraestructura donde existen muchas otras CAs "subordinadas" (como veremos en breve), las Root CA se suelen utilizar casi exclusivamente para emitir certificados para las otras CAs.

6.4.3. Entidades de Certificación Subordinadas (Subordinate Certification Authority)

Realmente éstos son los "caballitos de batalla" de la infraestructura PKI. Las Entidades de Certificación Subordinadas son las que realizan la emisión de certificados para la gran mayoría de necesidades del usuario final. Por ejemplo: protección del correo electrónico, certificados para páginas web, certificados para servidores externos a la infraestructura PKI, etc.

6.4.4. Tipos de Entidades de Certificación

El rol de Active Directory Certificate Services permite la implementación de dos tipos de Entidades de Certificación: independientes y empresariales.

- **Entidades de certificación independientes (Stand-Alone Certification Authorities)**

Una Entidad de Certificación Independiente, para comenzar, no requiere de Active Directory Domain Services (ADDS). Se puede utilizar una CA independiente para los siguientes propósitos:

1. Firmas Digitales.
2. Correo Electrónico protegido mediante S/MIME (extensiones seguras multi-propósito).
3. Autenticación de Servidor Web Seguro mediante SSL o TLS.

- **Entidades de certificación empresarial (Enterprise Certification Authorities)**

Estas entidades están vinculadas y trabajan con Active Directory Domain Services (AD DS). Además de los propósitos que puede usarse una CA Independiente, una CA Empresarial puede utilizarse para:

1. Firmas Digitales.
2. Protección de Correo Electrónico mediante S/MIME.
3. Autenticación de Servidor Seguro mediante SSL y TLS.
4. Inicio de sesión en dominio utilizando tarjetas inteligentes (Smart Card).

Para instalar una CA Empresarial es necesario tener acceso a Active Directory Domain Services con un usuario que sea miembro del grupo "Administradores de Dominio" o con derechos de escritura en Active Directory.

Algunas de las características de una CA Empresarial son:

- Permite exigir la comprobación de credenciales de los usuarios durante el proceso de solicitud de certificado.
- Se pueden hacer uso de plantillas.
- Cada plantilla de certificados puede tener permisos establecidos en Active Directory para determinar si el solicitante tiene autorización para recibir dicho tipo de certificado que está intentando pedir.
- El nombre del sujeto del certificado se puede generar automáticamente a partir de la información de AD DS o puede ser suministrado explícitamente por el solicitante.
- Se minimiza la cantidad de información que el usuario debe proporcionar para recibir el certificado solicitado.

6.4.5. Componentes de Active Directory Certificate Services

El rol "Active Directory Certificate Services" tiene ciertos componentes o servicios, a través de los cuales se da vida a la Infraestructura de Clave Pública en Windows Server. Vamos a recorrer rápidamente cada uno de estos servicios que posteriormente veremos paso a paso con la instalación de este rol.

- **Certification Authorities**

Este servicio posee Entidades Raíz y Subordinadas. Es utilizado para generar certificados a usuarios, computadoras y servicios. Además, es utilizado para administrar la validez de los certificados.

- **Web Enrollment**

Este servicio permite a los usuarios conectarse a un Certification Authority mediante un navegador web para solicitar certificados y recibir las listas de revocación de certificados (CRL).

- **Network Device Enrollment Service**

Este servicio (conocido como "NDES") permite a routers u otros dispositivos de red que no tienen una cuenta de dominio, obtener un certificado válido.

- **Certificate Enrollment Policy Web Service**

Este servicio permite a usuarios y computadoras obtener información sobre políticas de inscripción de certificados.

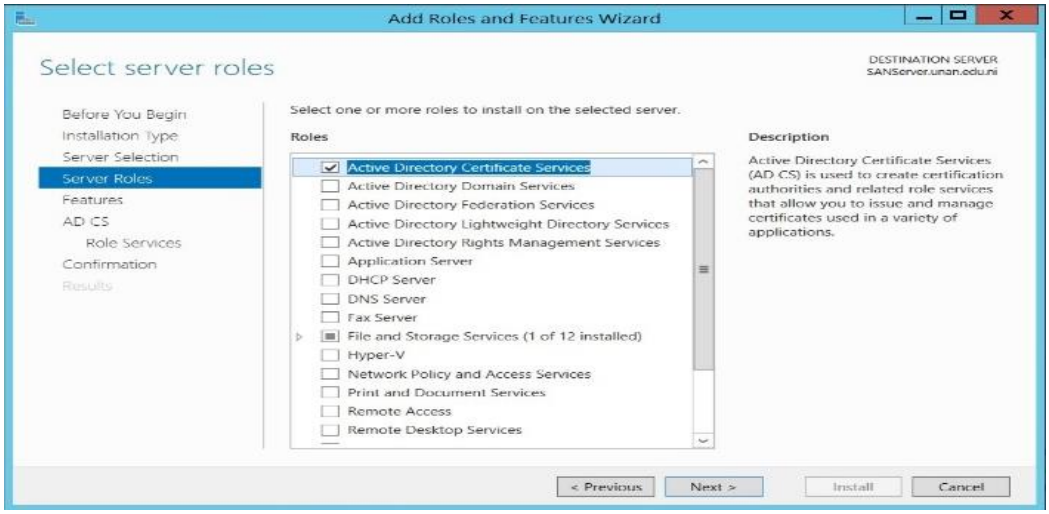
- **Certificate Enrollment Web Service**

Este servicio habilita a usuarios y computadoras a realizar un requerimiento e inscripción utilizando protocolo HTTPS. Cuando se utiliza en conjunto con el servicio "Certificate Enrollment Policy Web Service" se habilitan las inscripciones basadas en políticas para:

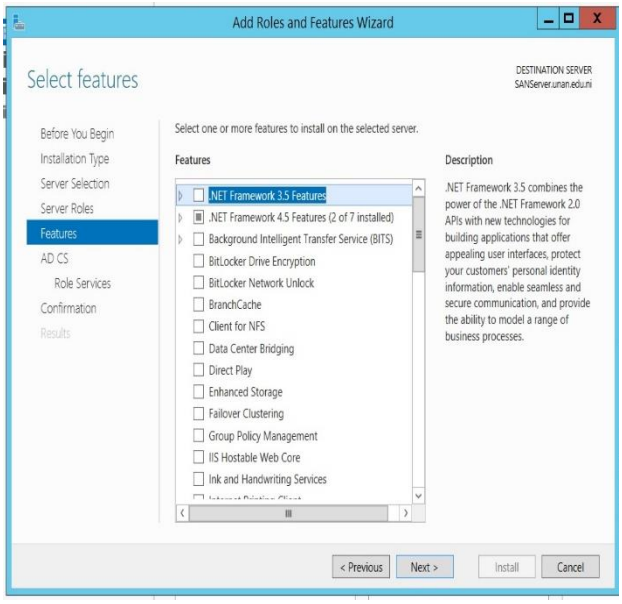
- Computadoras miembros del dominio no conectadas al dominio.
- Computadoras que no son miembros del dominio.

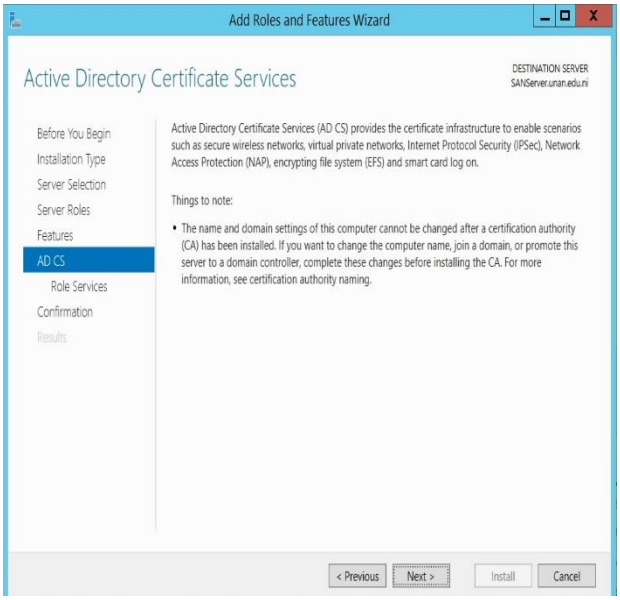
6.4.6. Instalación y configuración de la Entidad emisora de certificados (Active Directory Certificate Services).

1. En el dominio del servidor (unan.edu.ni), abrir **Server Manager** y pasar a la opción "**Select Server Roles"** y hacemos clic en "**Active Directory Certificado Services"** y luego hacemos clic en **"Next"**.

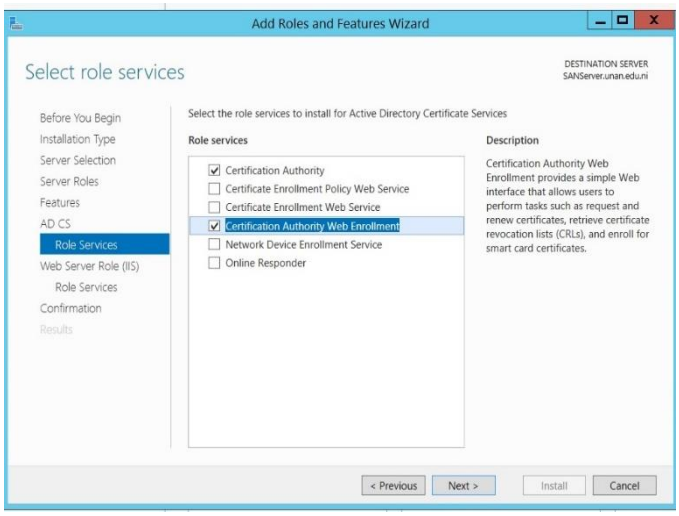


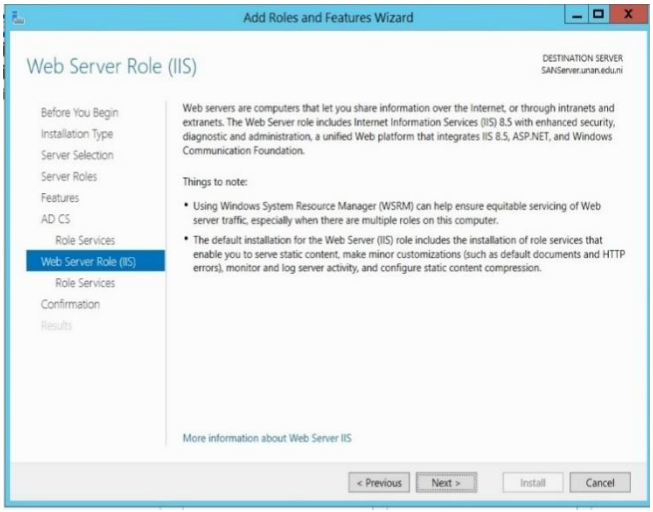
2. En la interfaz "**Select Features"**, continuamos con el próximo paso dando clic en "**Next"** e igualmente al llegar en la opción "**Active Directory Certificate Services"** simplemente hacemos clic en "**Next"** pasamos a la siguiente opción**.**



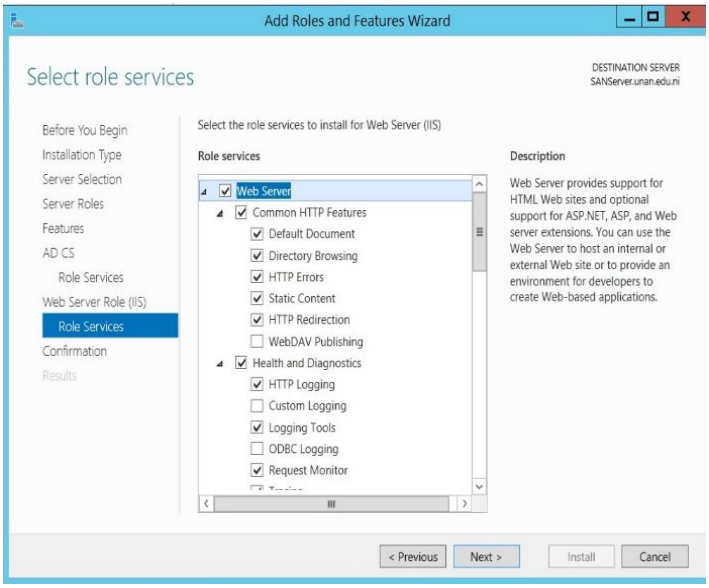


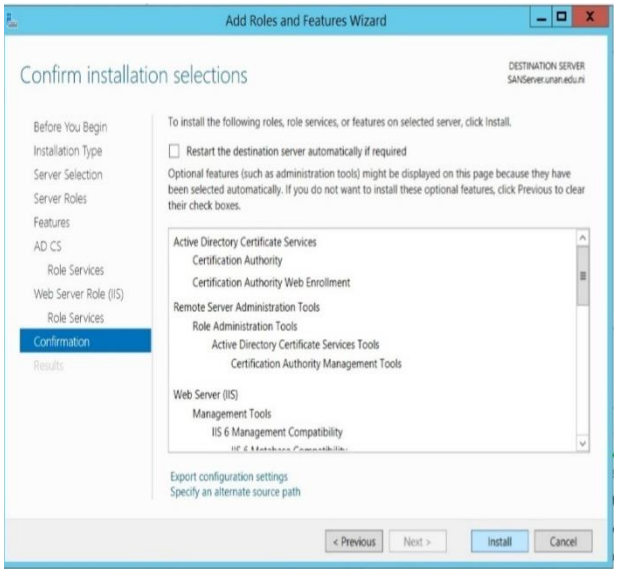
3. En la opción "**Select Role Services"**, marcar la casilla "**Certification Authority"** y la **"Certification Authority web Enrollment"** y hacemos clic en "**Next"** y al pasar a la pestaña **Web Server Role (IIS)** solamente volvemos a dar clic en "**Next".**



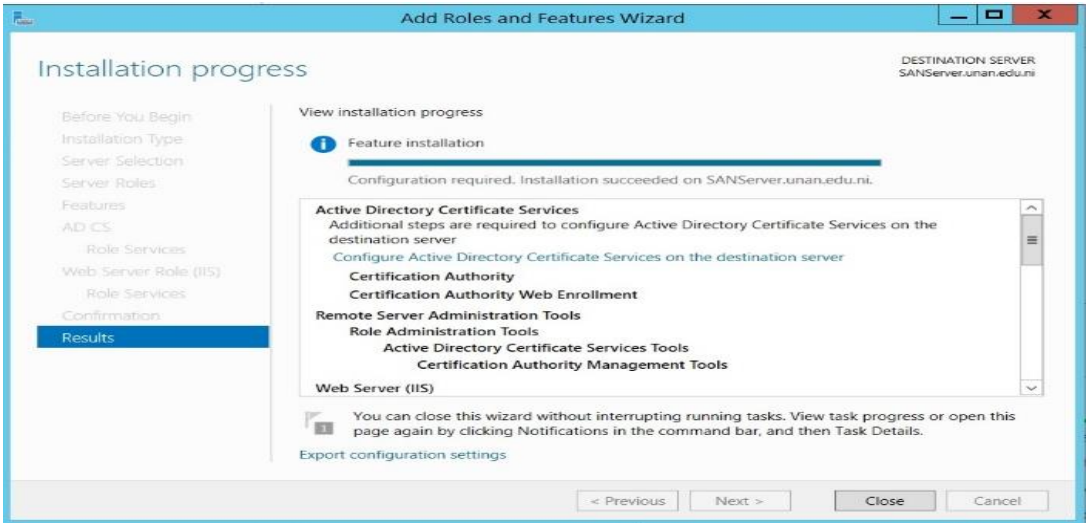


4. En la pestaña "**Selec Role Services"**, simplemente hacer clic en **"Next"** y al pasar en la interfaz de **Confirm installation selections**, aplicamos la opción **"Install"**.

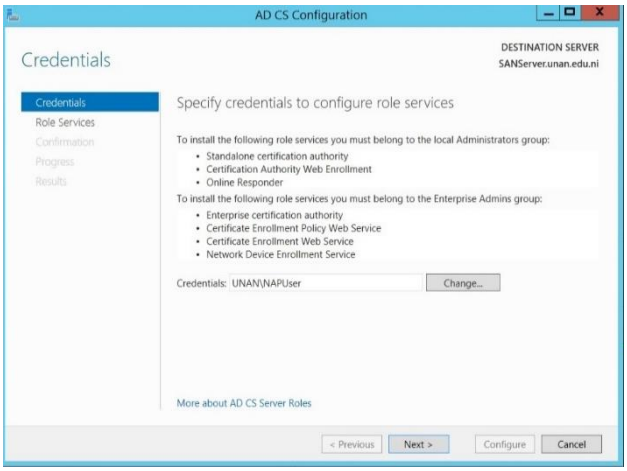


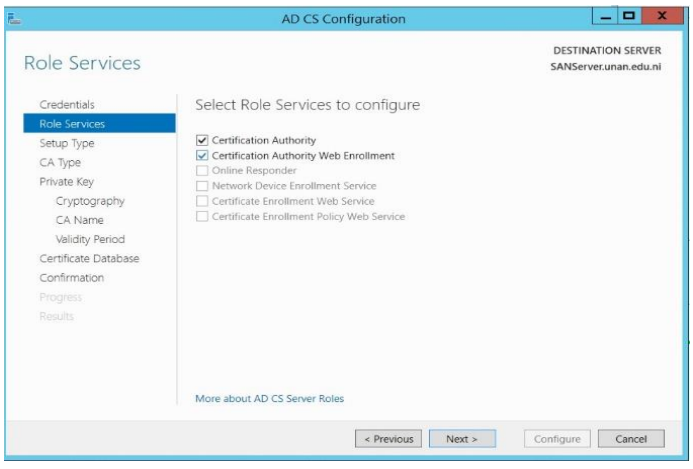


5. Después de completar la instalación, en la interfaz de Progreso hacemos clic en "**Configure Active Directory Certificate Services on the destination server"** para la configuración del rol de acuerdo a nuestras necesidades de uso**.**

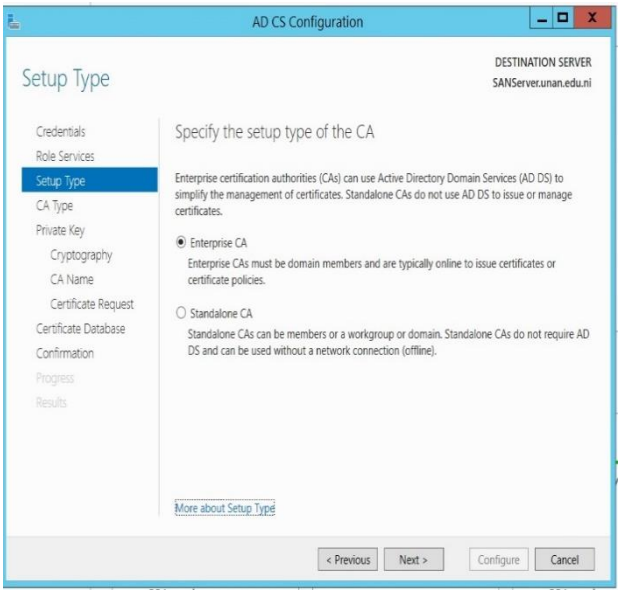


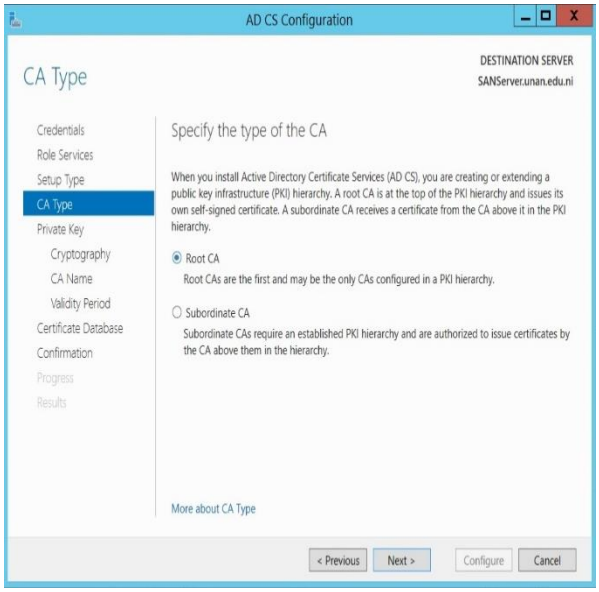
6. A continuación, en la interfaz de **Credenciales**, verificamos las credenciales de administrador sean **Napuser** y se luego hacemos clic en "**Next"**, para después pasar a la interfaz **"Role Services"**, seleccionamos las Casillas "**Certification Authority"** y "**Certification Authority Web Enrollment"** y hacemos clic en "**Next".**



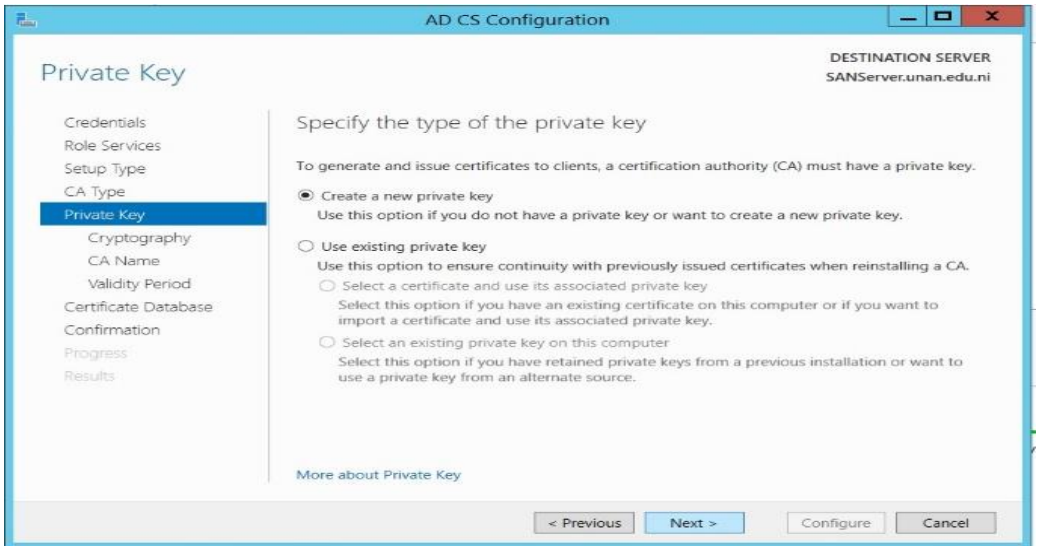


7. En el tipo de configuración en la interfaz **Setup type**, compruebe que la selección "**Enterprise CA"** este marcada al igual que en la pestaña **CA Type** compruebe que la entidad emisora de raíz este seleccionada **"Root CA"** y luego clic en **Next**

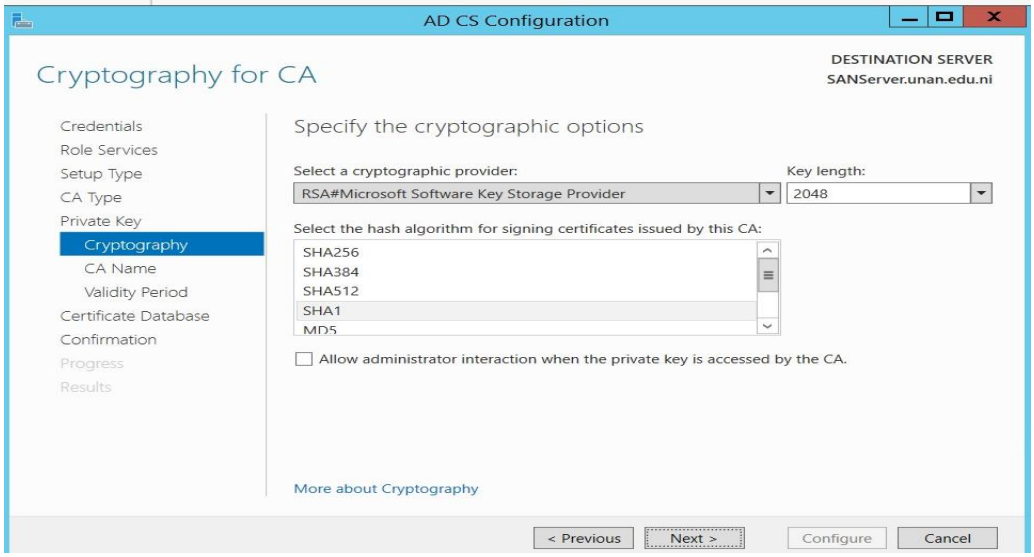




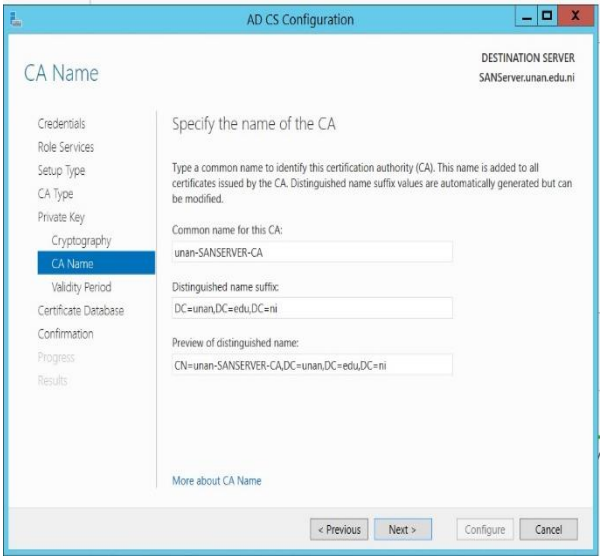
8. A continuación en la interfaz **Private key**, se hizo clic en "**Crear una nueva clave privada"** y damos clic en "**Next".**

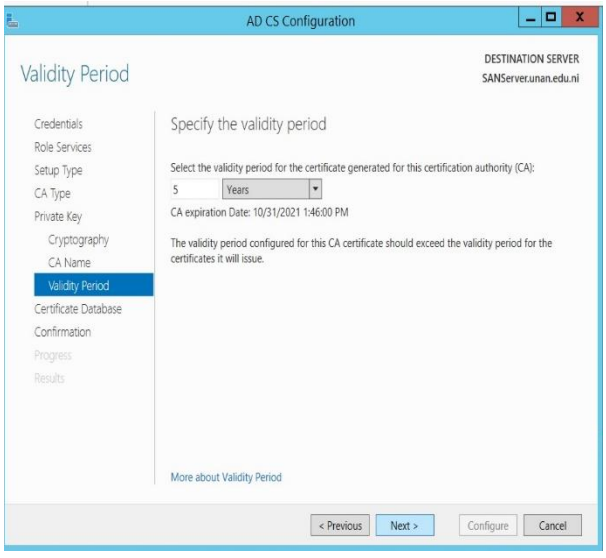


9. En la interfaz **criptografía para CA** , puede seguir siendo el valor predeterminado , que **RSA Criptografía** con **2.048 clave de** longitud y verificar que **SHA1** es seleccionado, y luego hacemos clic en "**Next".**

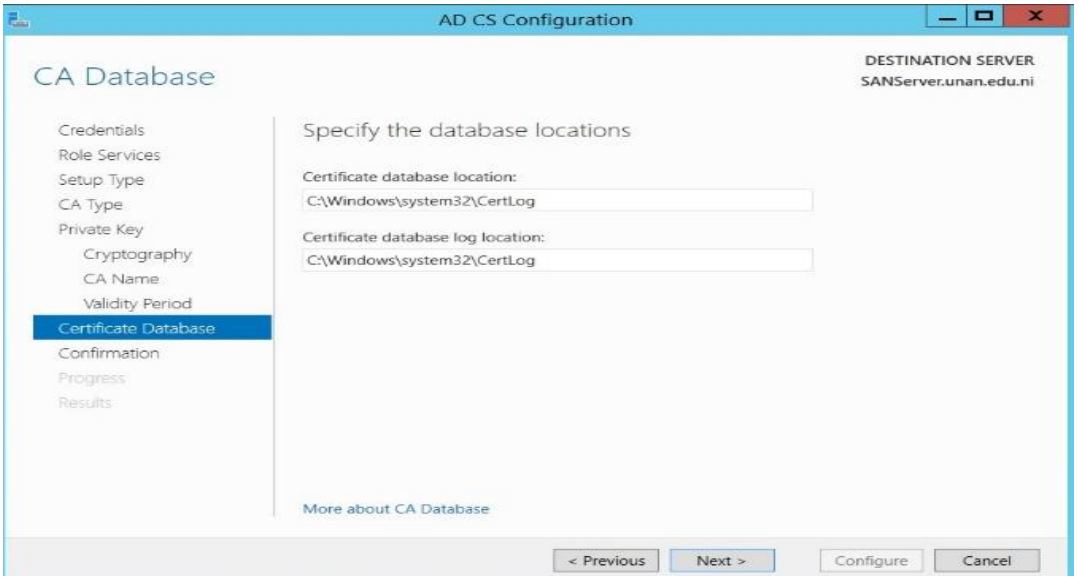


10. En la interface **CA Name**, únicamente damos clic a **Next**. En el período de validez, elijo **5 años para mi CA**, que es tiempo que por defecto da, y luego hacemos clic en **"Next"**.

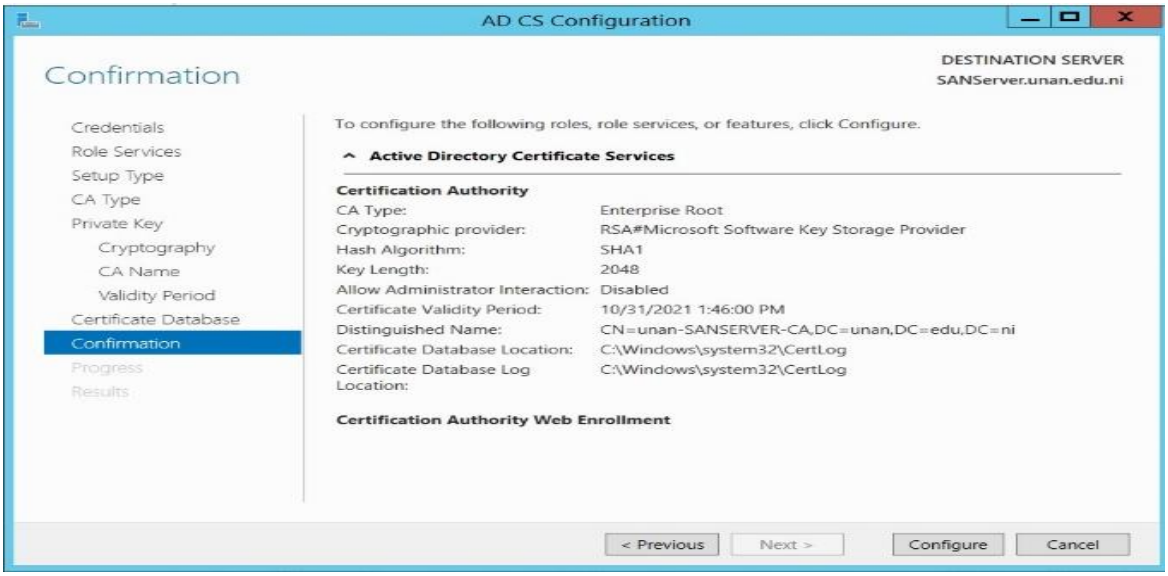




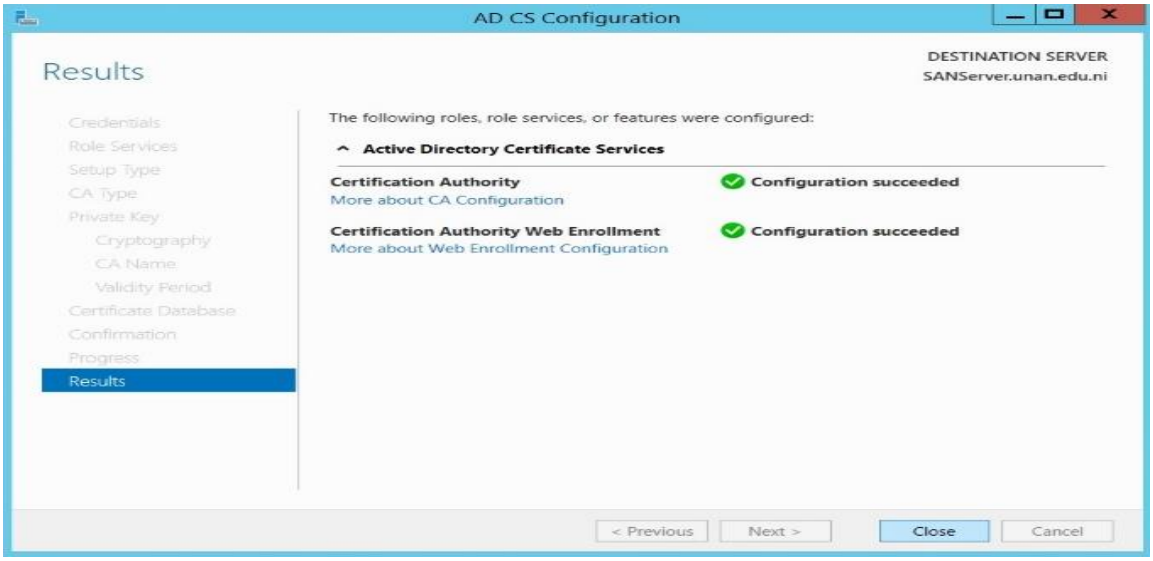
11. En la interface de **CA Database** solo damos clic en "**Next".**



12. A continuación en la interfaz **Confirmation** se comprueban todos los ajustes realizados y damos clic en "**Configure".**

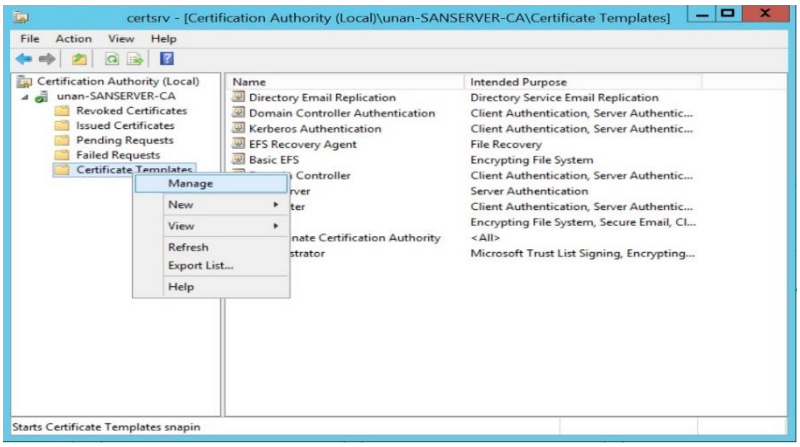


13. Por último si nuestro **CA** y el **CA Web Enrollment**están correctamente instalado se nos marcara en verde, más adelante mostraremos como el Network Access Protection necesita de que tengamos la entidad emisora de certificado CA



Configuración de la Entidad emisora de certificados:

- Una vez instalado y configurado el rol "Active Directory Certificate Services", nos dirigimos a la dirección **Server Manager/Tool/Certification Authority** y desplegamos la consola de administración **certsrv** y expandimos el apartado **Unan-SANSERVER-CA**



- Luego como parte del procedimiento hicimos clic en el apartado **Certificate Template** y a continuación seleccionamos en el menú contextual en la opción **manage** el cual nos abrirá otra consola llamada **Certificate Template Consola** hacemos clic en **Computer** y luego en **Propiedades.**

- Una vez estando en **Propiedades** nos dirigimos en la ficha **Security** y se selecciona el **Authenticated User** (usuario autenticado), y procedemos a asignarle los permisos para usuarios autenticados, lo cual aremos marcando la casilla **Enroll** y posteriormente acepta esta configuración.

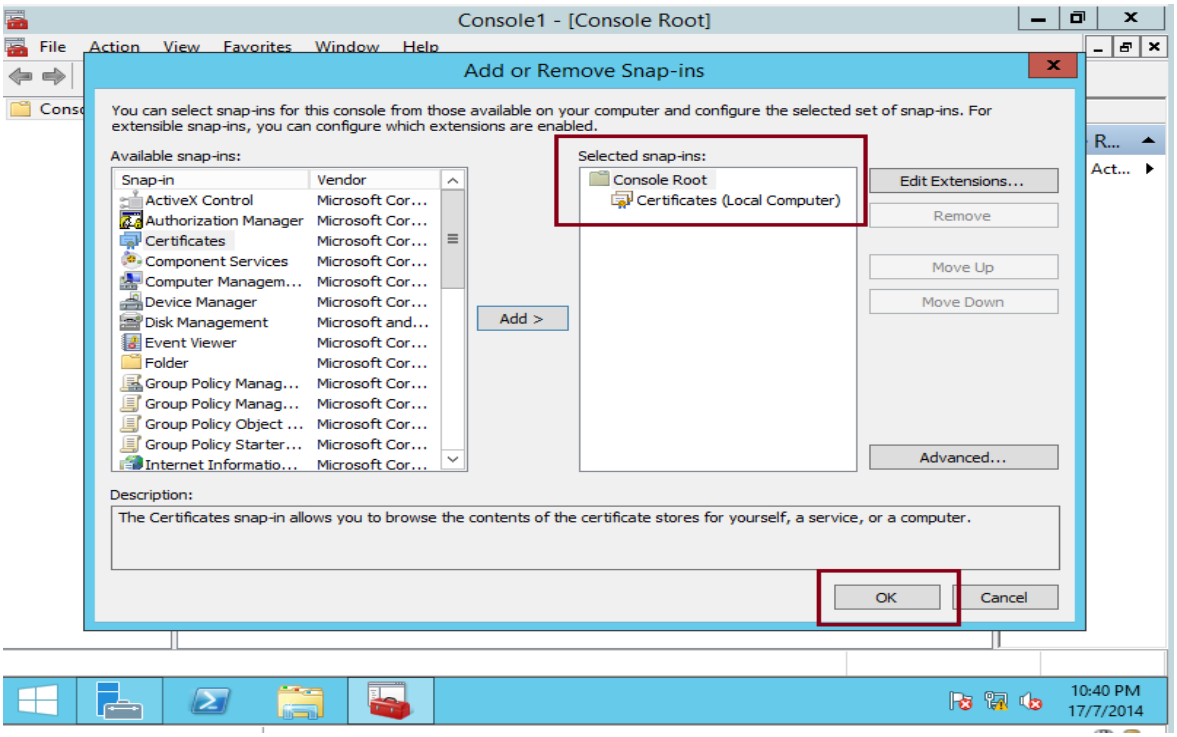
- En el mismo **certsv** en el apartado **Unan-SANSERVER-CA** hacemos clic y seleccionamos **All Task**y clic **Stop Service** con el fin de detener todos los servicios, luego hacemos los mismos procedimientos y esta vez hacemos el inverso damos clic en **Star Services** (con el fin de que todos los cambios de la configuración se apliquen).

- A continuación abrimos otro servidor (Unan-Nps), en este nuevo servidor vamos a inscribir un nuevo certificado de **AD.**

  Abrimos RUN (con el comando ctr + r) y escribimos **MMC** en la barra de open.

- En el Servidor haga clic en **File-Add/Remove Snap-in.** En la opción de agregar y quitar un complemento hacemos clic en **certifacates** y posteriormente hacemos clic en agregar, seleccionamos la opción **Computer account** hacemos clic **Next** y **Finish**

- En el cuadro de **File-Add/Remove Snap-in** (Agregar o quitar Complemento), hagamos clic en **ok.**

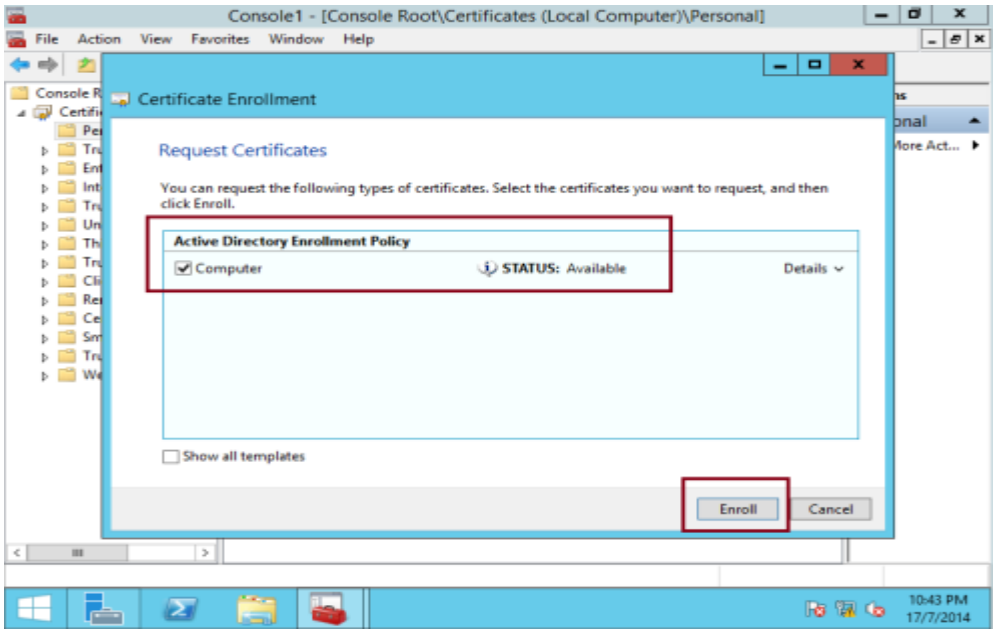


- En el árbol de Console1 expanda **certificate,** hacemos clic en **Personal/All tasks/Request New Certificate.**

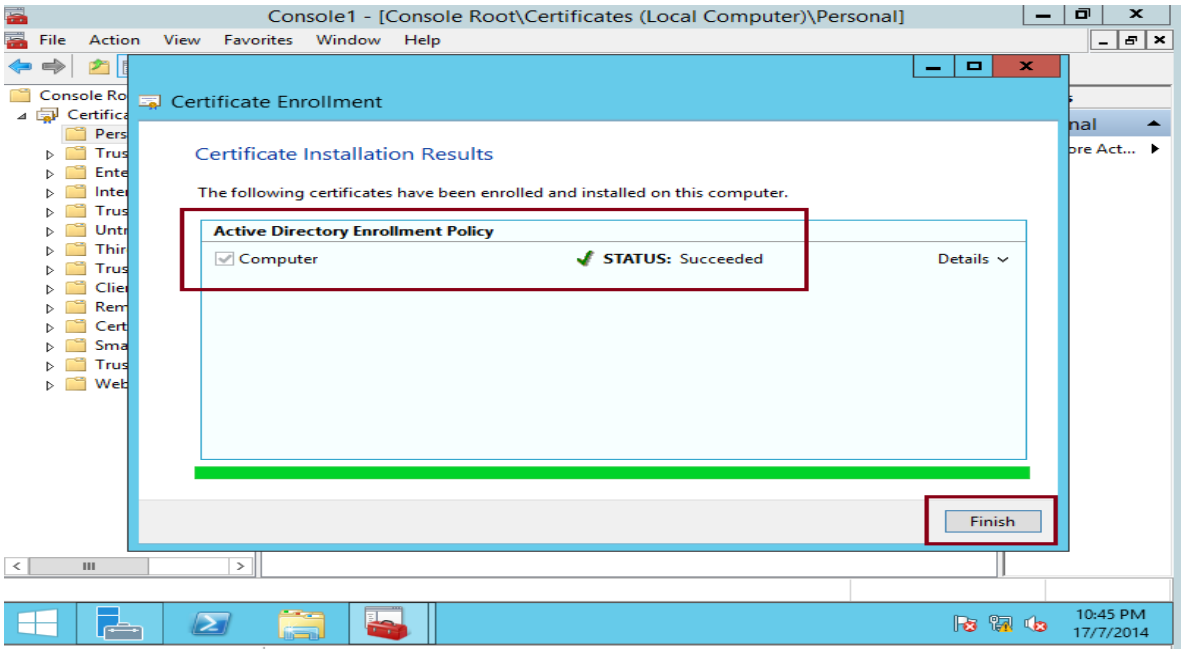
- En el recuadro de dialogo de inscripción del certificado solo basta con darle clic **NEXT.**

- A continuación en la interfaz **Select Certificate Enrollment Policy**, seleccionamos la directiva de inscripción de Active Directory.

- A continuación seleccionamos la casilla del **Computer** y damos en clic en inscribir.

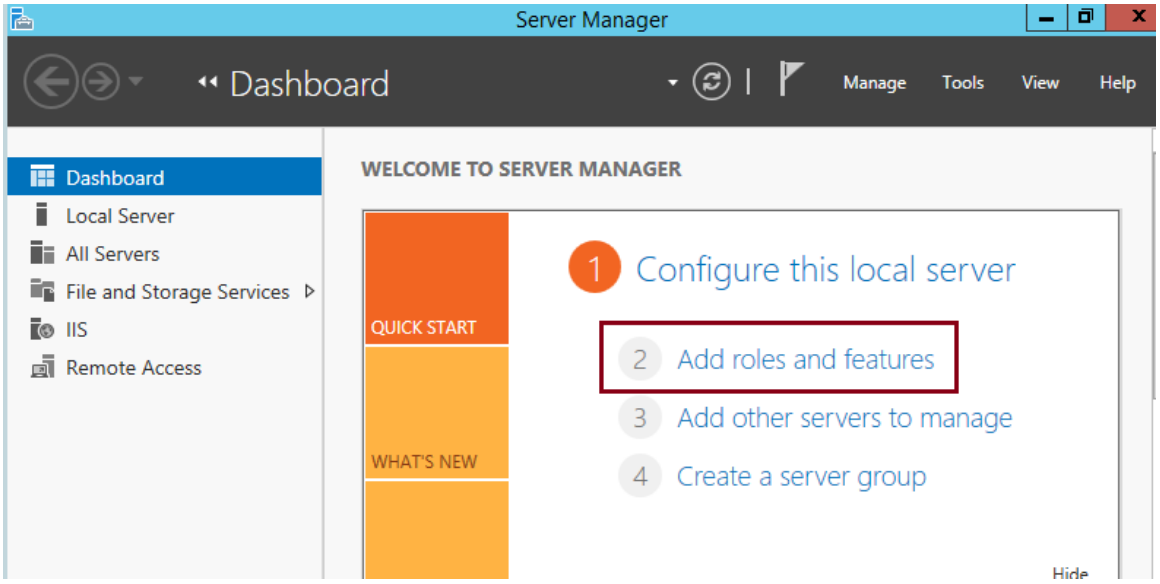


- Verificamos que la instalación del certificado tuvo éxito, y finalizamos dando clic en **Finish** así terminamos la instalación y configuración de la Entidad emisora de certificado con el único objetivo de que es un requisito NAP en el cual lo exponemos en el apartado **Nap con IPsec.**

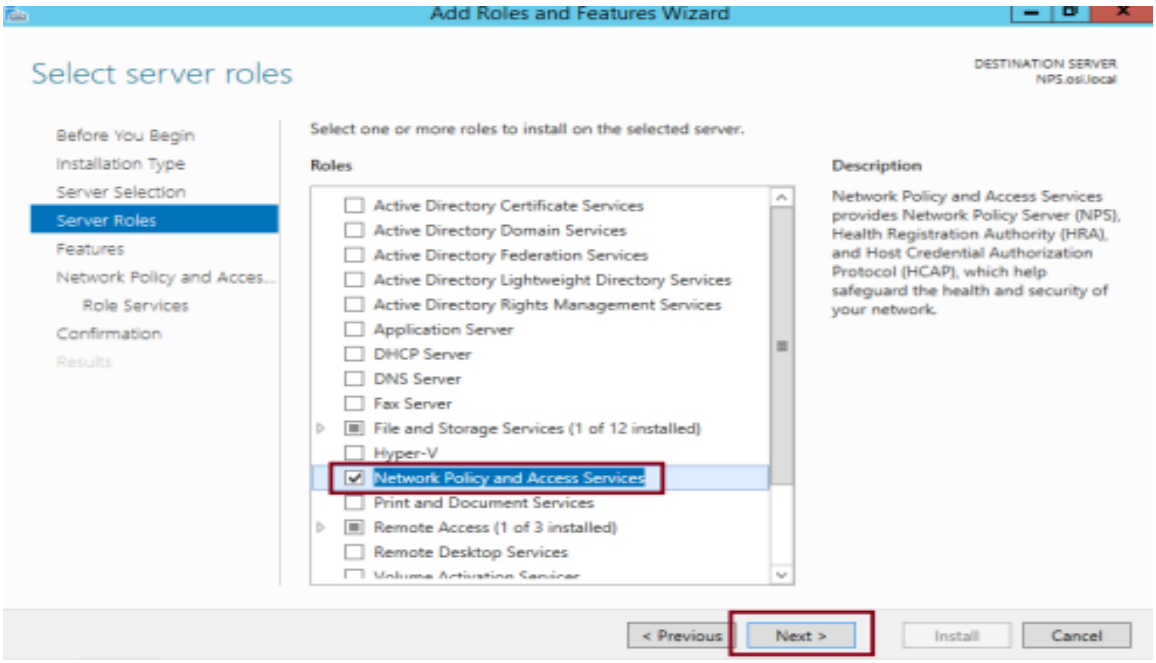


6.5. Instalar y configurar el Servicio NPS (Network Policy Service) en Windows Server R2 2012.

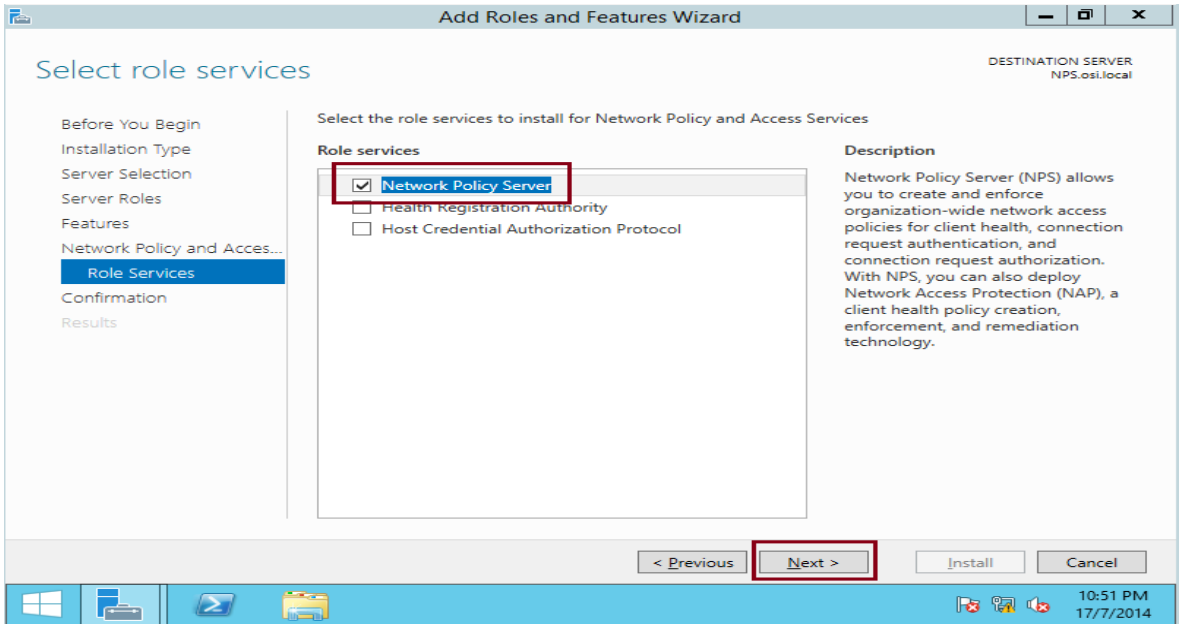
- Abrimos el Server Manager >>Add roles and features



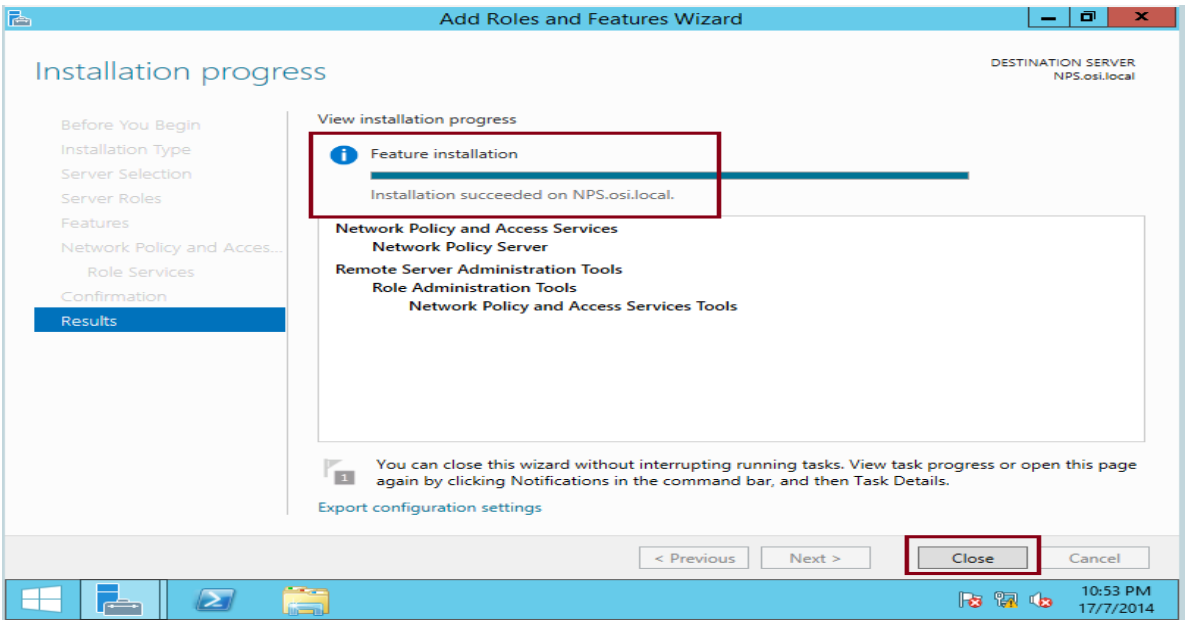
- En la interfaz Select Roles Roles, seleccionamos dándole clic a la casilla **Network Policy and Access Services** y avanzamos dando clic en **Next**.



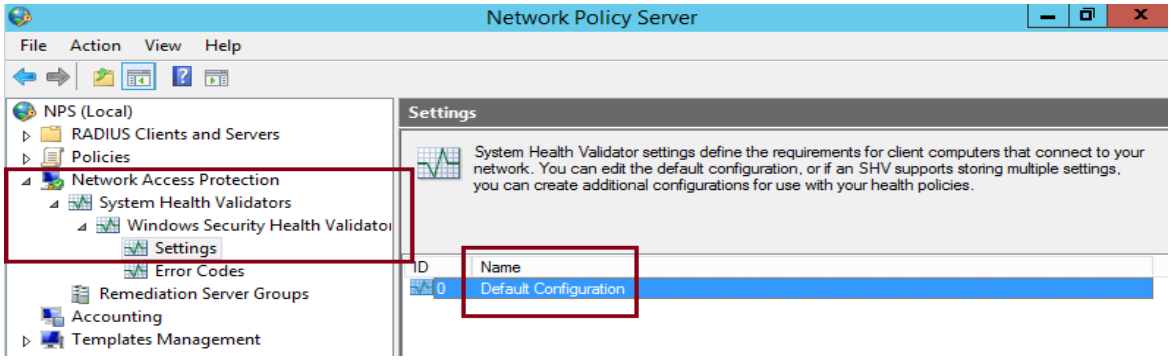
- Seleccionamos el rol **NPS** y damos clic en el botón **Next**



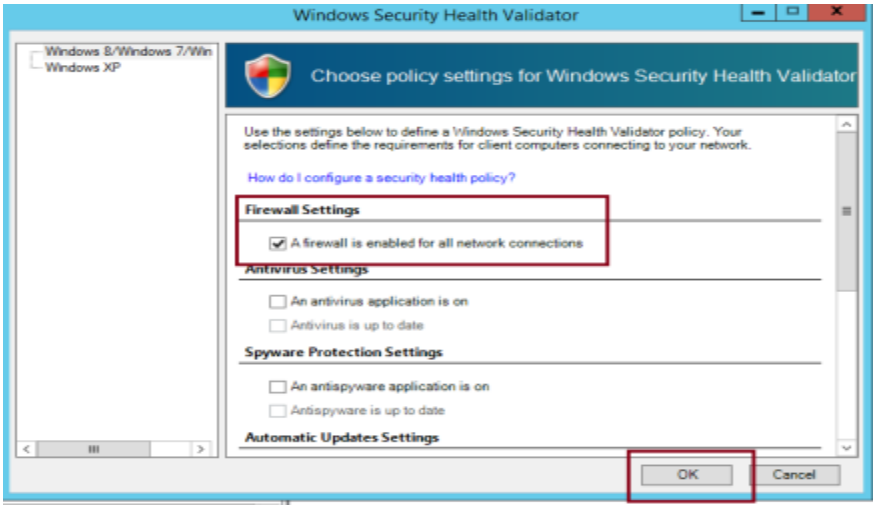
- Después de hecho clic en **install**, veremos finalizada la barra de instalación y cuando esté listo en botón **close** hacer clic para avanzar a la configuración del rol.



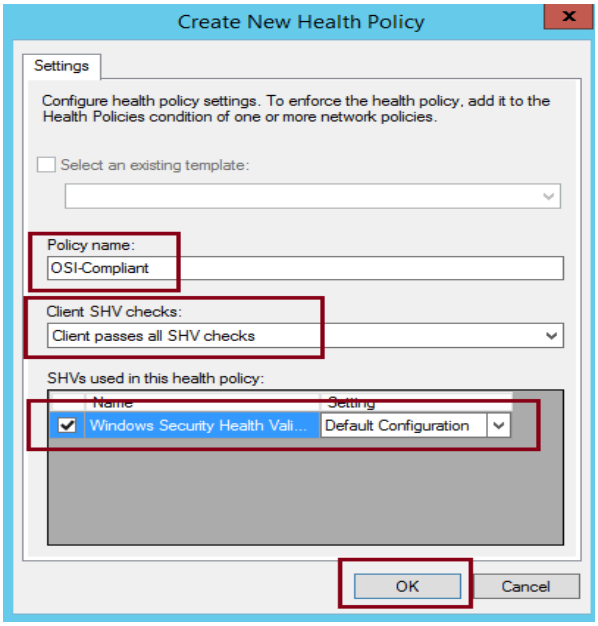
- Configurar SHV (System Health Validators)
    1. Inicio >> Ejecutar>>**nps.msc**
    2. En la consola del servidor de directivas de redes, se amplía la opción red de protección de acceso, posteriormente también se amplía el Sistema validadores de Salud, se expande la seguridad de Validador Windows, y luego hacemos clic en Configuración, en el panel derecho, hacemos doble clic configuración predeterminada.



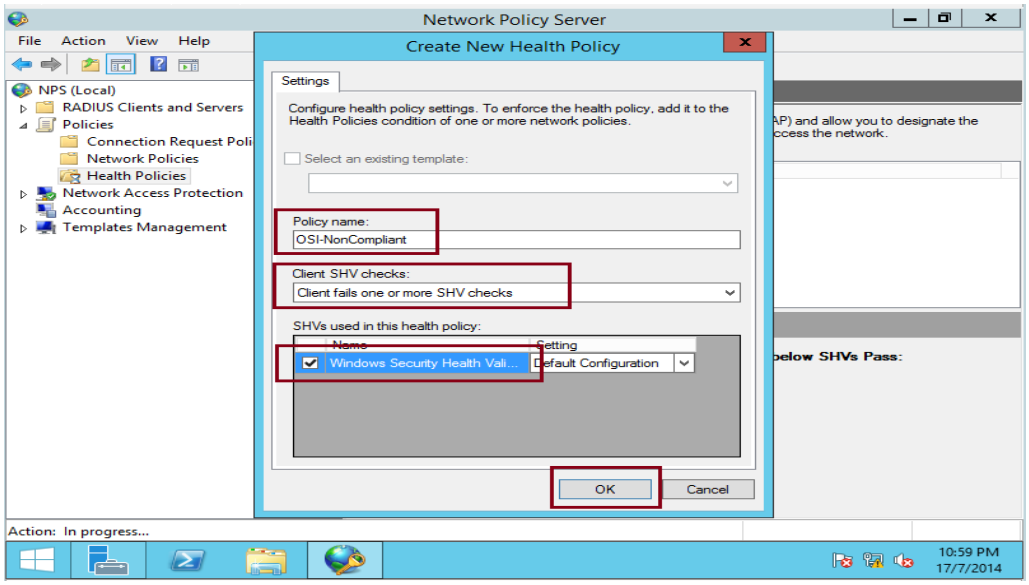
- Como es una configuración piloto en la interfaz de seguridad de Windows validador, experimentamos habilitando el firewall solamente y desactivamos las demás casilla en la opción de Windows 7/8.1/vista y presionamos la opción ok. Esto con el fin que cuando este sistema esté en marcha solo bastara con deshabilitar el firewall del computador cliente para negarle el acceso a la intranet de la Unan-Managua



- Configurar servidores que proporcionaran "sanción" a nuestro equipo, estos pueden ser Wsus. En esta demostración no utilizaremos Wsus.
- Configurar Directivas de Mantenimiento
    1. En la interfaz "Crear nueva directiva de la Salud", en **Policy name** se creó una directiva con el nombre "**Cumple"**, en el cuadro "**Client SHV Cheks"** seleccionamos la opción "Client passes all SHV checks" que significa que el cliente supera todas las comprobaciones del agente **SHV**y posteriormente habilitar el "**SHVs Used in this health policy**" el validador de mantenimiento de seguridad y presionamos en **ok**.

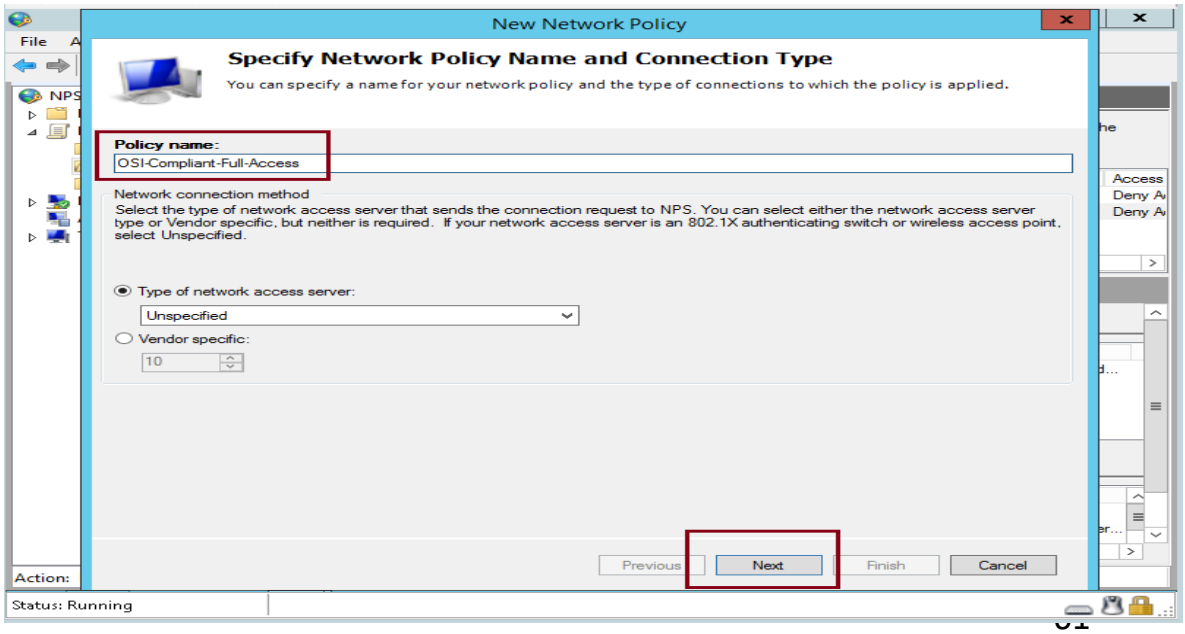


- Nuevamente repetimos el mismo paso anterior y creamos una directiva con el nombre "**NO CUMPLE"** y en el en el cuadro "**Client SHV Cheks"** seleccionaremos la opción, "*Client falis one or more SHV checks",* que significa que el cliente no supera todas las opciones del SHV y nos aseguramos del checkbox en el validador de seguridad.

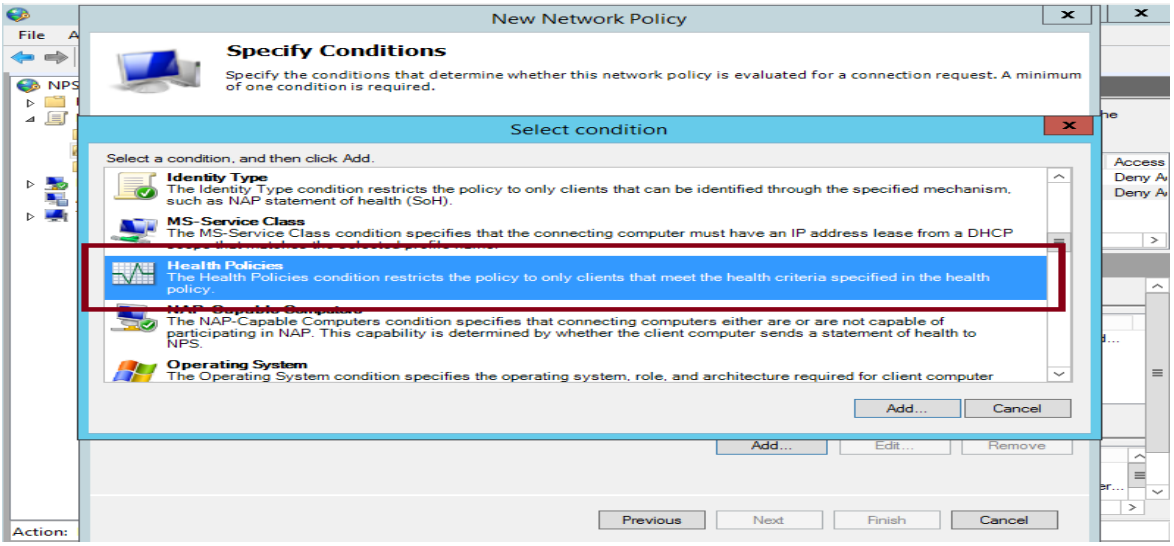


- Configurar Política de Red.

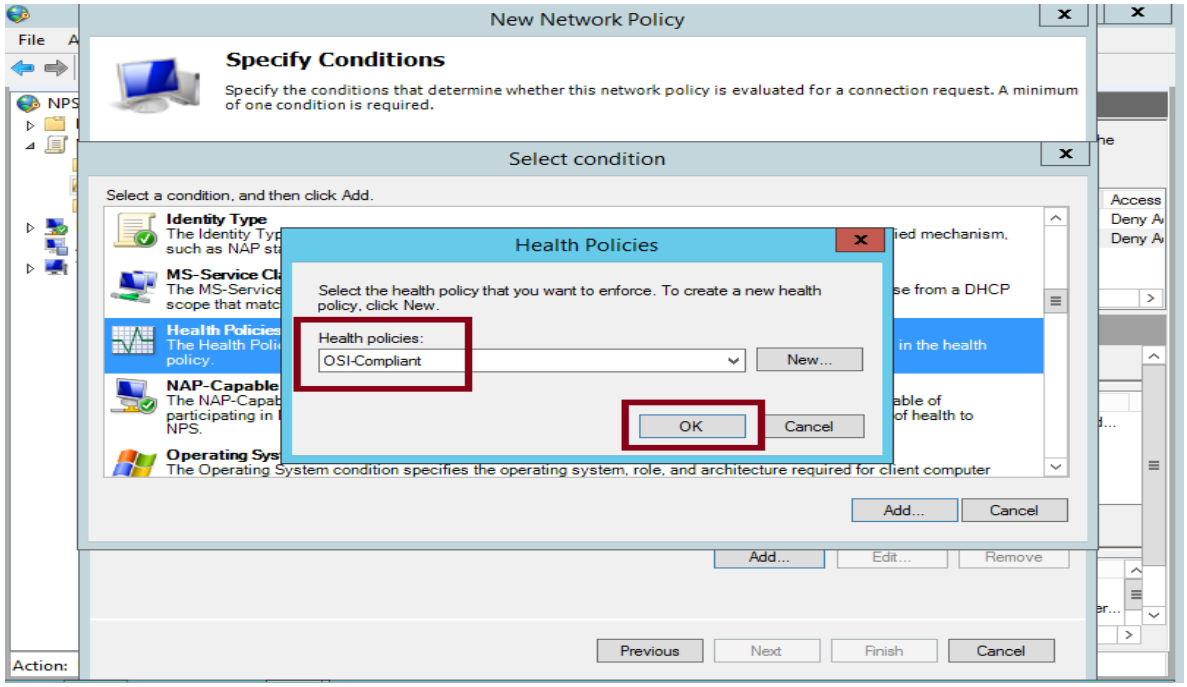
1. Deshabilitar todas las políticas por defecto.
2. Con el botón derecho del mouse sobre el nodo “Directivas de red”, presionar el menú nuevo
3. Especificar el nombre de la Política como “**Compliant-Full-Access,** y damos clic en **Next”.**



4. En la pantalla de especificar las condiciones, presionar el botón agregar y seleccionar **Health Policie** (Directivas de mantenimiento).



5. Cuando nos pregunte por la directiva de mantenimiento, seleccionamos "**Compliant**"



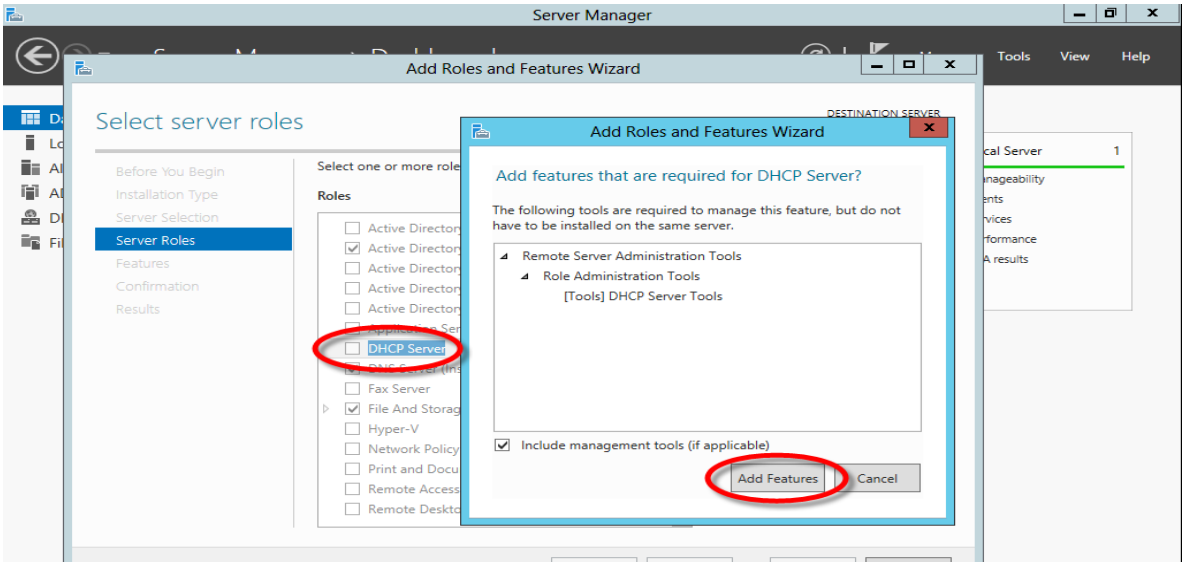
6. En la pantalla de especificar los permisos de acceso, seleccionar **Access Granted** (Acceso Concedido).

7. En la pantalla de configurar métodos de autentificación, solo dejamos **realizar solo comprobación de mantenimiento de equipos.**
8. En la pantalla de configurar opciones, debemos configurar el cumplimiento NAP, **para permitir Access Completo a la red**
9. **Luego damos clic en el botón finish**
10. **Ahora realizamos los mismo que el paso 2 al nueve, solo que en este caso**
    1. En el paso 1 le damos el nombre de la política como "**No Compliant"**
    2. En el paso 5 seleccionamos la directivas de mantenimiento (no cumple)
    3. En el paso 8 seleccionamos permitir Access Limitado.
    4. En la opción, **Configure Authentication Methods >> Configure Constraints >> NAP Enforcemen >> IP Filters >> Edit IP Filter** seleccionamos la subred restringida la cual es cuenta con la submascara **255.255.255.255** la cual son redes de conexión única para aislar equipos.

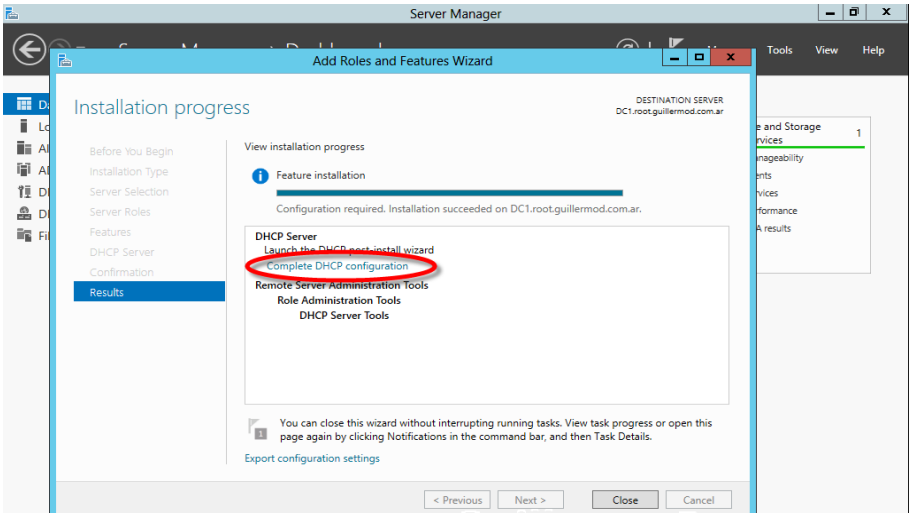
11. Luego damos clic en el botón Finish.

6.6. Instalación y configuración del Rol DHCP en Windows Server 2012 R2 10.1.120.120/24.

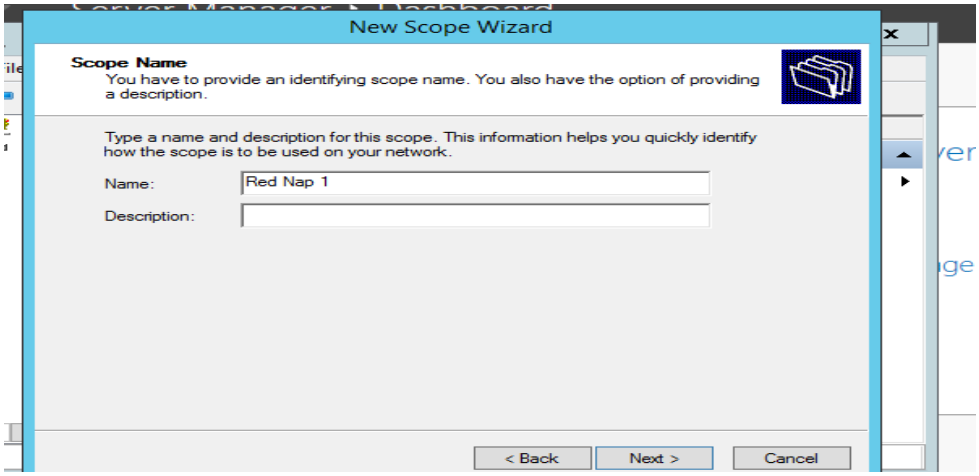
- En el **Server Manager**, hacemos clic en el menú de funciones y hacemos clic en Add **Roles and Feature** y agregamos el rol de DHCP.



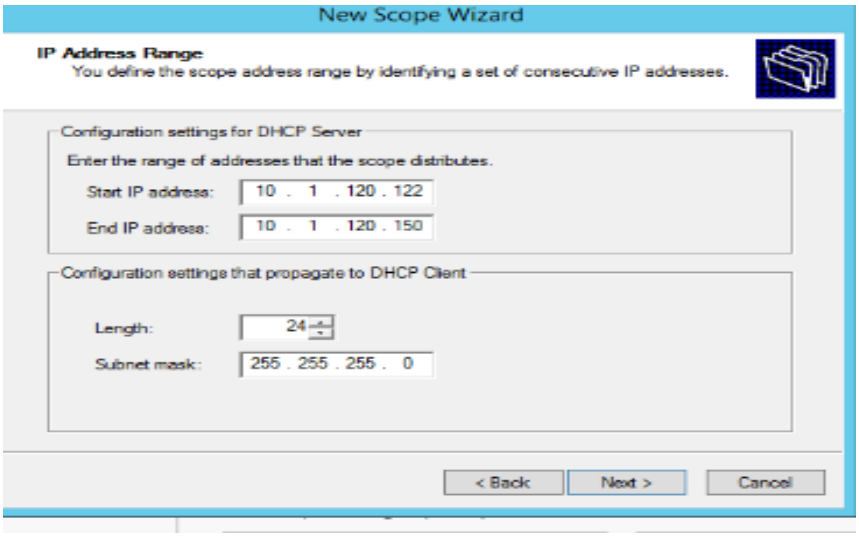
- Una vez seleccionado en la casilla de instalación el rol de DHCP, damos next a cada una de interfaces hasta dar con la opción **Install**, el cual procedemos a darle clic y al terminar dicha instalación hacemos clic en la pestaña de **Complete DHCP configuration.**



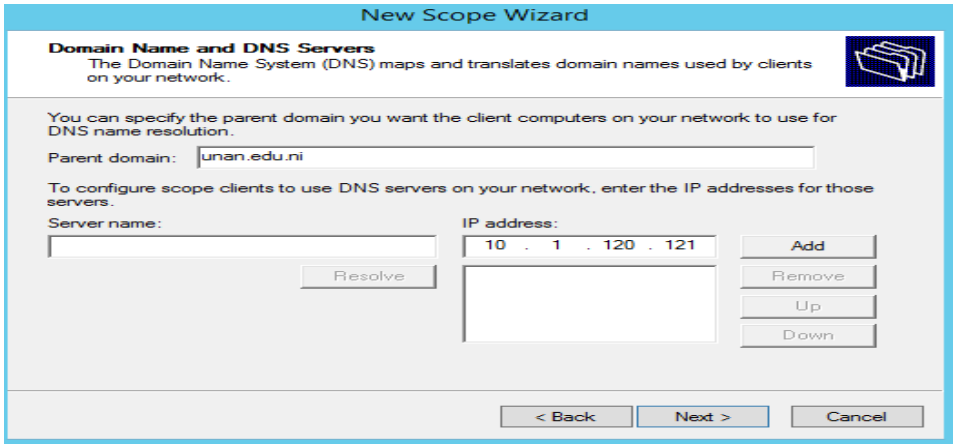
- Una vez finalizada la instalaciones nos regresamos al **Server Manager** en la opción **Tools** seleccionamos con un clic la opción **DHCP,** al abrir dicha interfaz seleccionamos la opción **ipv4**y haciendo clic derecho en el mouse nombramos un scope el cual lo nombraremos como **Red Nap 1.**



- Ingresamos las direcciones el rango IPs inicial y final que proveerá el DHCP a los Clientes, agregamos el rango desde la 10.1.120.122 hasta 10.1.120.150 y luego marcamos la casilla “Activate this scope”.

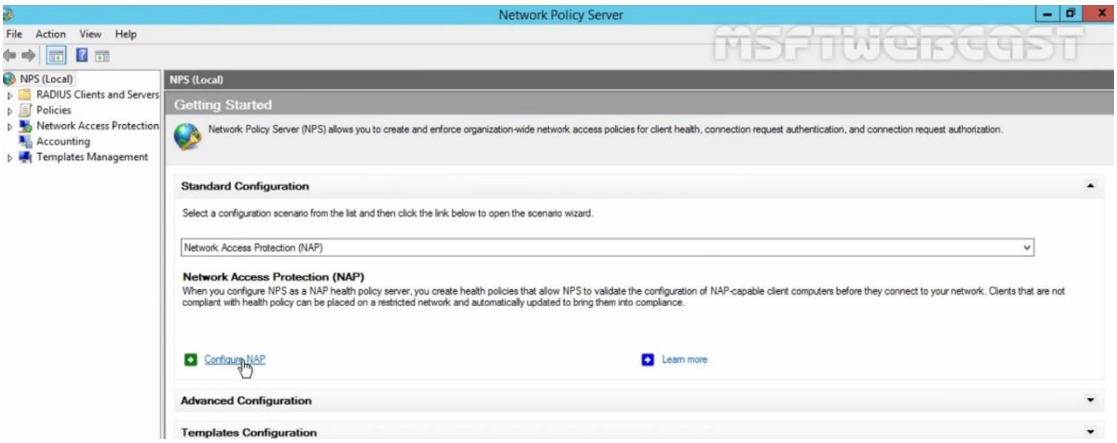


- En esta pestaña de configuración DNS del protocolo de internet versión 4 (IPv4). Agregamos el dominio unan.edu.ni la IP 10.1.120.121 y le damos clic en el botón next en todas las siguientes interfaz hasta llegar a la opción Finish.

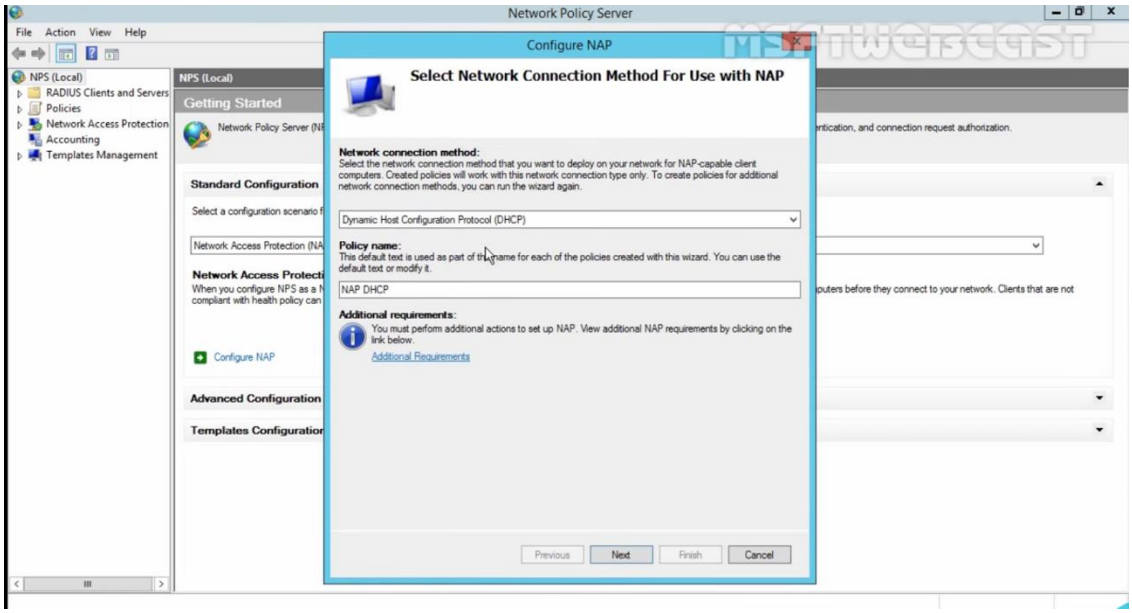


- **Configuración NAP con DHCP.**

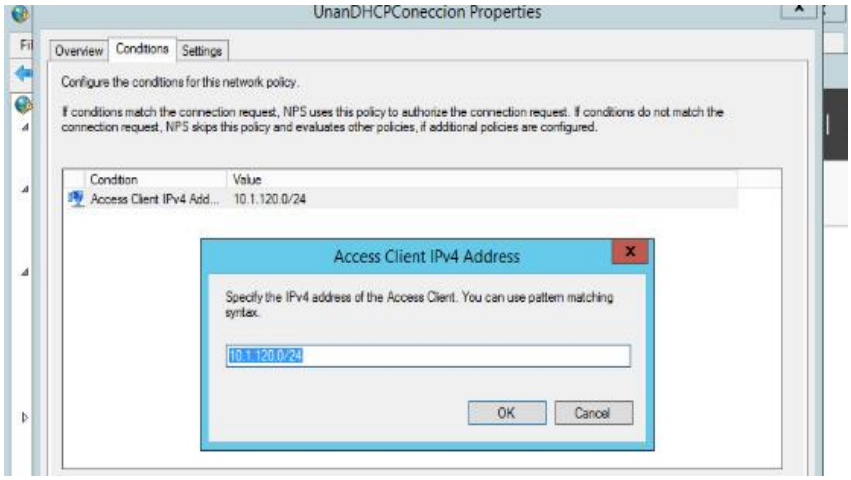
1. En la dirección Server Manager>>Tools>>Network Policy Server>>Configure NAP.



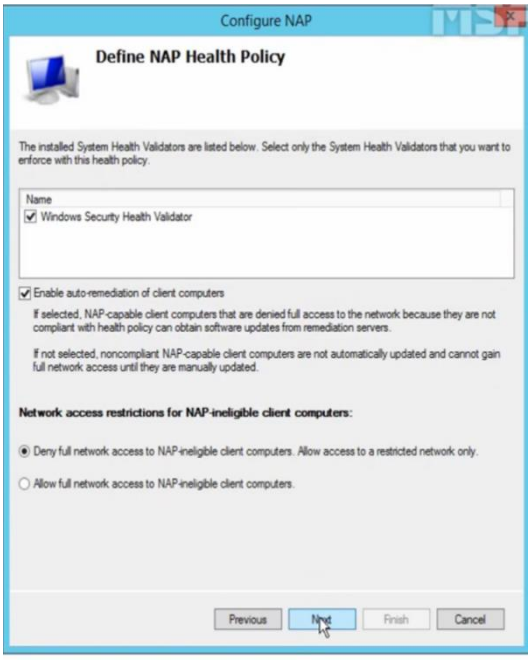
2. En la interfaz **Configure NAP**, Seleccionamos el método de conexión de red para el uso de NAP en este caso seleccionamos el protocolo DHCP.



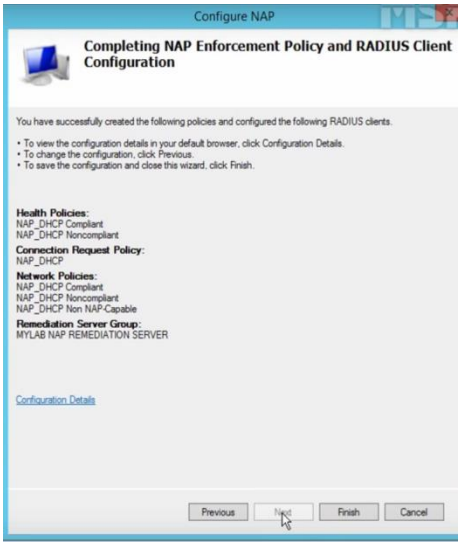
3. Agregamos el scope llamado "Red Nap 1" antes configurada en el rol DHCP



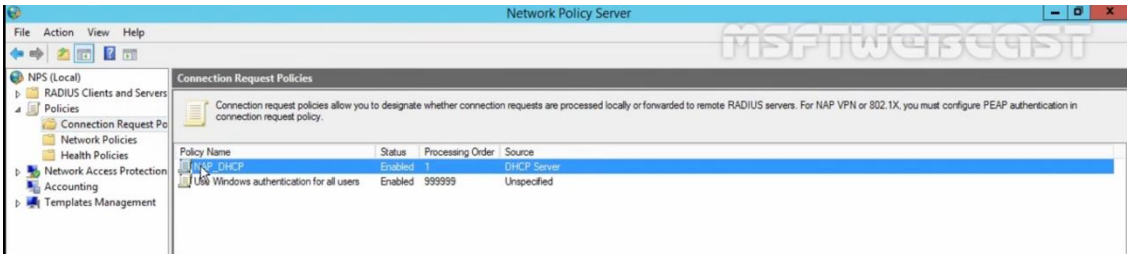
4. Al llegar a la interfaz "Definir las políticas de seguridad" comprobamos que las opciones "Windows Security Health Validator" este marcadas junto con auto-remediation del cliente, y el acceso total a la red.



5. Una vez completada estas opciones hacemos clic en **Next** hasta completar la configuración y por ultimo daremos clic en **Finish**.



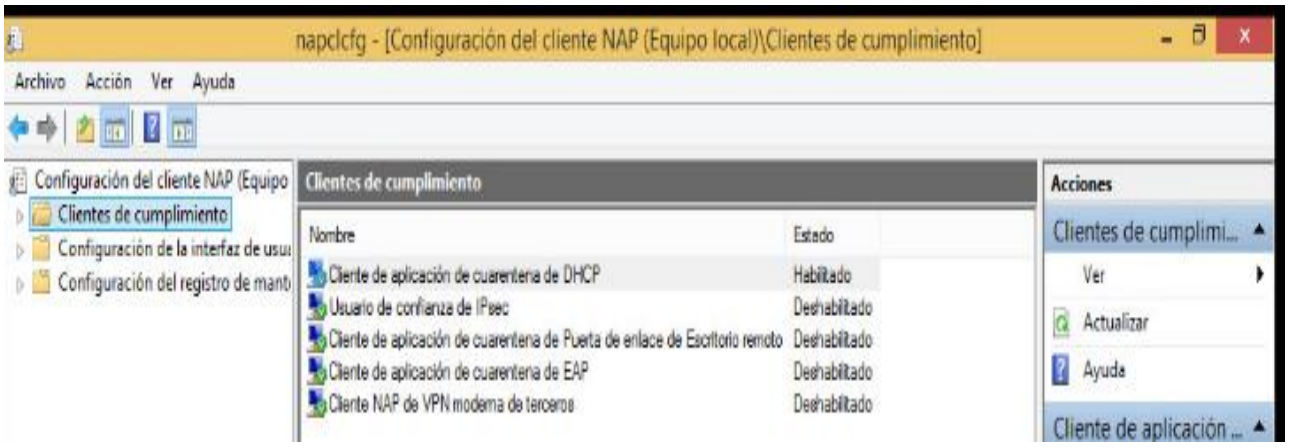
6. En la consola "Network Policy Service" expandimos la opción "Policies" y damos clic en "Conection Reques Policy" y verificamos que la política este activa.



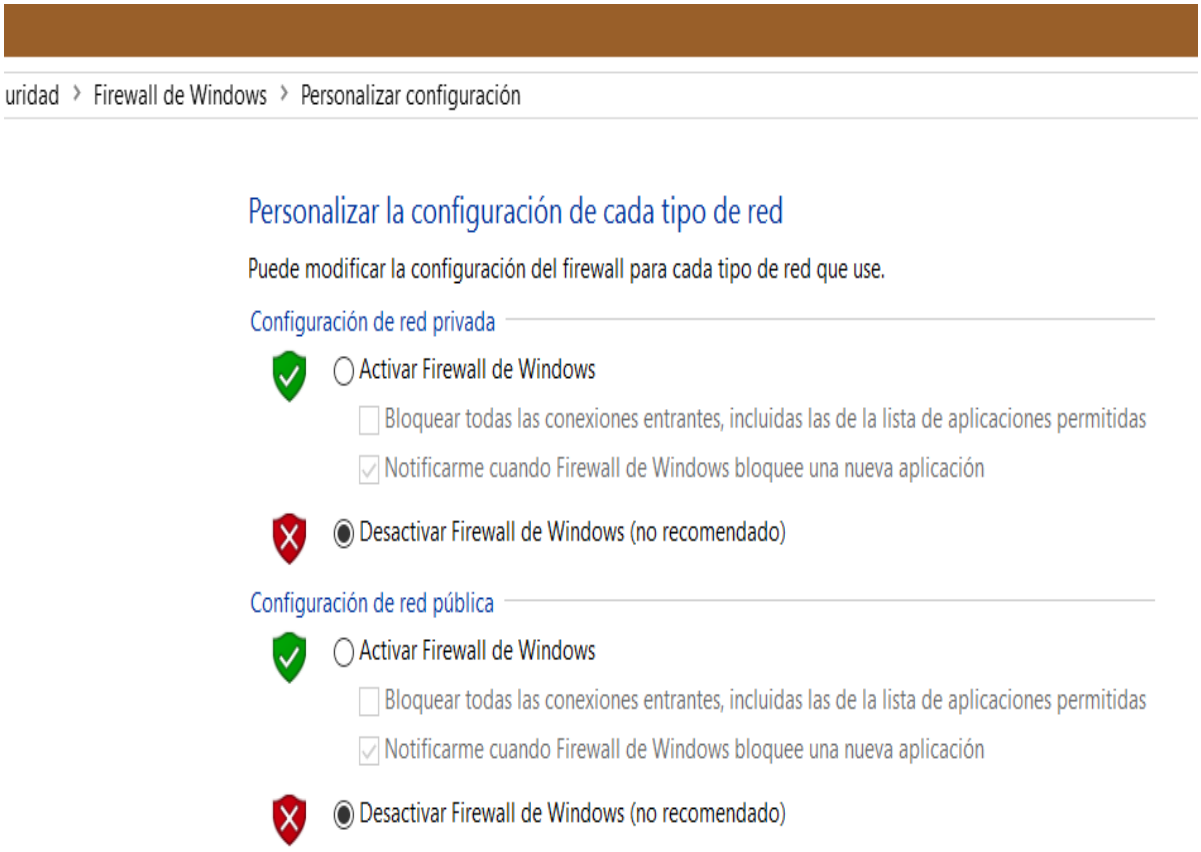
6.7. Prueba de campo replicando en un escenario seguro (Red de prueva) de la red de la Unan-Managua, la configuración realizada de NAP con DHCP

1. Iniciamos sesión en el cliente "**Napuser"**.

2. Sometemos el cliente a las políticas NAP abriendo la consola de cumplimiento, con la opción ejecutar con el comando (Win + R) en la barra open colocamos el comando **"napclcfg"** y en el directorio cliente de cumplimiento, habilitamos la opción (cliente de aplicación de cuarentena por DHCP) que por defecto estará deshabilitado.



3. Desactivamos el Firewall, en la misma barra de ejecutar colocamos el comando "**Firewall.cpl"** y hacemos clic en la opción **"Activar o desactivar firewall"** donde al dar en las casillas desactivar posteriormente haciendo clic en activar estaremos deshabilitando dicho servicio.



4. Abrimos la consola de símbolos donde comprobaremos la dirección ipv4 de nuestro computador de prueba con el comando "**ipconfig"** Renovamos nuestra IP con DHCP con el comando ipconfig /realease y después el comando ipconfig /renew y deberíamos de ver algo así.

5. En el uso de NAP con DHCP se puede resumir.
   - El cliente que no reconoce NAP queda restringida su comunicación en la red.
   - Cliente que reconoce NAP, y cumple los requisitos tiene conectividad completa.
   - Cliente que reconoce NAP y no cumple los requerimientos si se puede remediar, pasa a cumplir requerimientos. Si no se puede remediar, queda restringido.

VII. Conclusiones

Una vez desarrollado el presente seminario de graduación; Propuesta de Implementación de Seguridad de Acceso a Redes de datos en la UNAN Managua, hemos llegado a las siguientes conclusiones:

La red de datos de la Unan-Managua tiene un 70% de los equipos clientes ejecutando Sistemas Operativos Windows 7/8.1/10, el restante 30% corresponde a equipos bajo entorno Linux, lo cual es ventajoso para este sistema Network Access Protection (NAP) dado a lo compatibilidad de trabajar con equipos con mismo proveedor.

La tecnología NAPS, es una plataforma de Microsft Windows Server 2012, la que tuvo sus inicios en el año 2008, no obstante y a pesar de sus importancia en el área de la seguridad informática, esta no se ha venido utilizando ni sacando el mayor de los provechos, a pesar que la UNAN Managua, utiliza la tecnología más actualizada o de punta.

La propuesta para la implementación del sistema de seguridad en la UNAN Managua, podríamos afirmar que es de nivel intermedio producto de los múltiples conocimientos que se tienen que adquirir o dominar al trabajar con diversos servicios, en el caso de la presente propuesta no se estará implementando en una estructura nueva si no por el contrario se tendrán que realizar las respectivas adecuaciones sobre la estructura ya existente para lograr que esta puede implementarse para que los resultados esperados.

Debido a los a los convenios con Microsoft, la implementación del sistema de seguridad no le generara gastos económicos para la UNAN Managua, ni para sus administradores, por lo cual podemos concluir diciendo que esto representa uno de los aspecto positivo de mayor importancia para esta importante casa de estudio en cuanto a la implementación de esta sistema de seguridad por lo cual solo falta el interés de echarlo andar.

Cabe recalcar que esta propuesta de implementación del sistema de seguridad, es efectivo para evitar que computadores infectados de cualquier tipo de virus tenga acceso a los Servidores Centrales que proveen todos los servicios de red, este sistema no limita el acceso a ningún hacker con intenciones maliciosas siempre y cuando su ordenador cumpla con las políticas de red propuestas por el sistema NAP.

VIII. Recomendaciones

Con el ánimo de seguir incentivando el uso y el estudio de la protección de redes informática en la UNAN- MANAGUA se presenta a continuación una series de recomendaciones para futuros trabajos y aplicaciones prácticas.

El sistema de seguridad con tecnología NAP, se ha comprobado a través del presente trabajo, que es efectivo y cumple con las expectativas para brindar la seguridad de datos informáticos, por lo cual recomendamos viable su implementación.

Incentivamos a los administrados de la red de la UNAN-MANAGUA, aplicar este Sistema de seguridad NAP para sufragar los métodos de seguridad actuales.

Actualmente el servidor de asignación direcciones dinámica DHCP, corre bajo entorno Linux que es incompatible con el sistema NAP por lo que se recomienda migrarlo a Windows Server 2012 R2 para obtener un sistema NAP-DHCP integrado.

Para que NAP funcione y cubra el 100 % de la infraestructura de la UNAN-MANAGUA se requiere que muchos host actualice su computador con Windows 7 como mínimo ya que varios computadores aun usan Windows XP el cual actualmente no tiene soporte técnico por Microsoft.

Se estima por lo menos un tiempo de dos años para esta tecnología la cual aunque no es actual pero aun es poco usada, entre en vigencia ya que se tendría que capacitar al personal de soporte técnico y a los usuarios para evitar que se le deniegue el acceso completo a la intranet de la UNAN-MANAGUA.

IX. Bibliografía

ASIMANE, A. (2014). *Windows Server 2012 R2 configuracion de servicios avanzados.* Barcelona: ENI.

Bonnet, N. (2012). Bases Imprescindible para administras y configurar su servidor. En B. Nicolas, *Bases Imprescindible para administras y configurar su servidor* (pág. 287). NI.

Di Loreto, P. (05 de Noviembre de 2016). Obtenido de https://www.tectimes.net/articulo-active-directory-certificate-services-conceptos-y-fundamentos/

http://siu.unan.edu.ni/informacion.htm. (15 de Septiembre de 2016). Obtenido de http://siu.unan.edu.ni/informacion.htm

http://www.unan.edu.ni/index.php/presentacion. (10 de Septiembre de 2016). Obtenido de http://www.unan.edu.ni/index.php/presentacion

https://msdn.microsoft.com/es-es/library/hh831786(v=ws.11).aspx. (11 de Octubre de 2016). Obtenido de https://msdn.microsoft.com/es-es/library/hh831786(v=ws.11).aspx

https://technet.microsoft.com/es-ni/windows/dd627342. (15 de Septiembre de 2016). Obtenido de https://technet.microsoft.com/es-ni/windows/dd627342

Parodi, M. (2016). *Optimizacion de la re Wi-FI del Recinto Univercitario Ruben Dario, para mejorar el acceso y ancho de banda utilizando software libre.* Managua: UNAN-MANAGUA.

TIC-Nicaragua. (2000). *tic-nicaragua.* Recuperado el 16 de 09 de 2011, de http://www.tic-nicaragua.edu.ni/documgaes1.htm

unan.edu.ni. (10 de Septiembre de 2016). Obtenido de http://www.unan.edu.ni/index.php/presentacion

X. Anexos

Ilustración 6 Distribución de la Red de Datos de la Unan-Managua

Modelo de red con NAP en la infraestructura de la UNAN-MANAGUA

En la siguiente figura se ve un modelo de ejemplo de alto nivel de Network Access Protection (NAP) que tendría el prototipo implementado en la UNAN-MANAGUA.

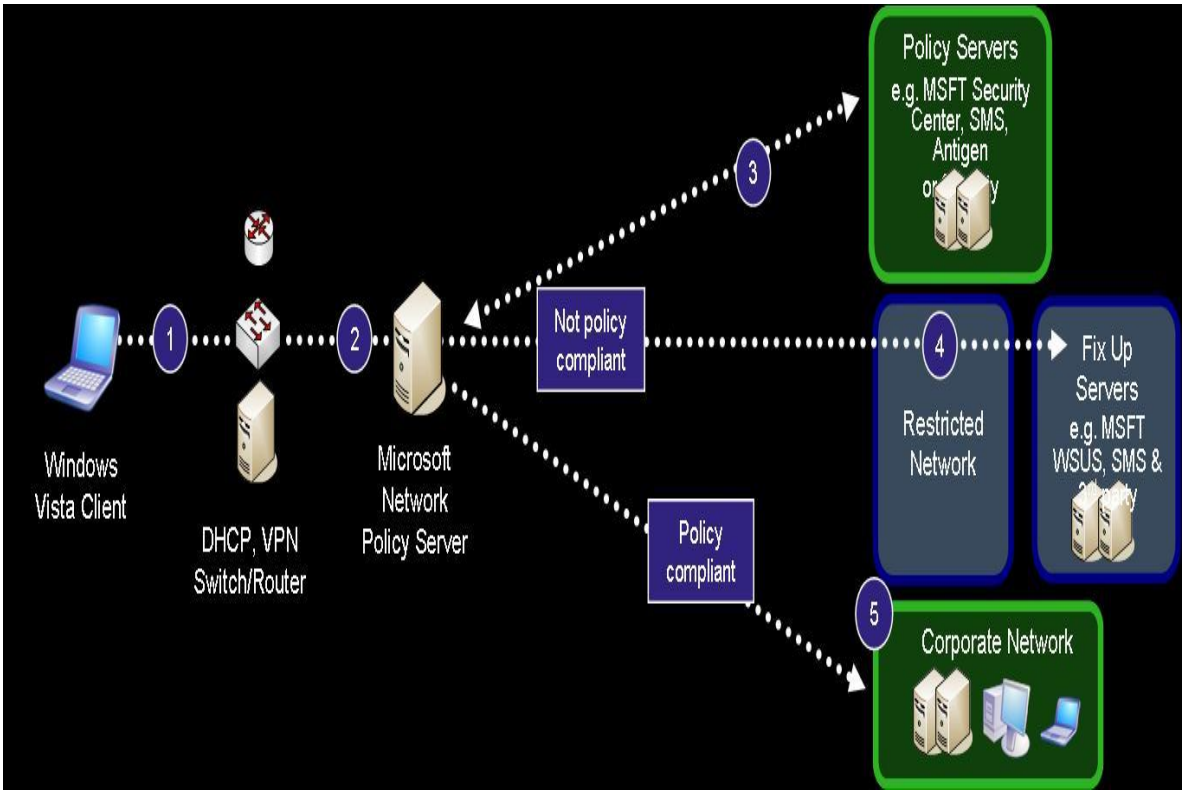


Ilustración 7 Cliente NAP con límite de acceso (https://technet.microsoft.com/es-ni/windows/dd627342, 2016)

"**En la Ilustración N° #8**; Apreciamos los servicios informáticos en Diagrama de bloque que provee el datacenter de la UNAN-MANAGUA" (SIUDT, 2016)

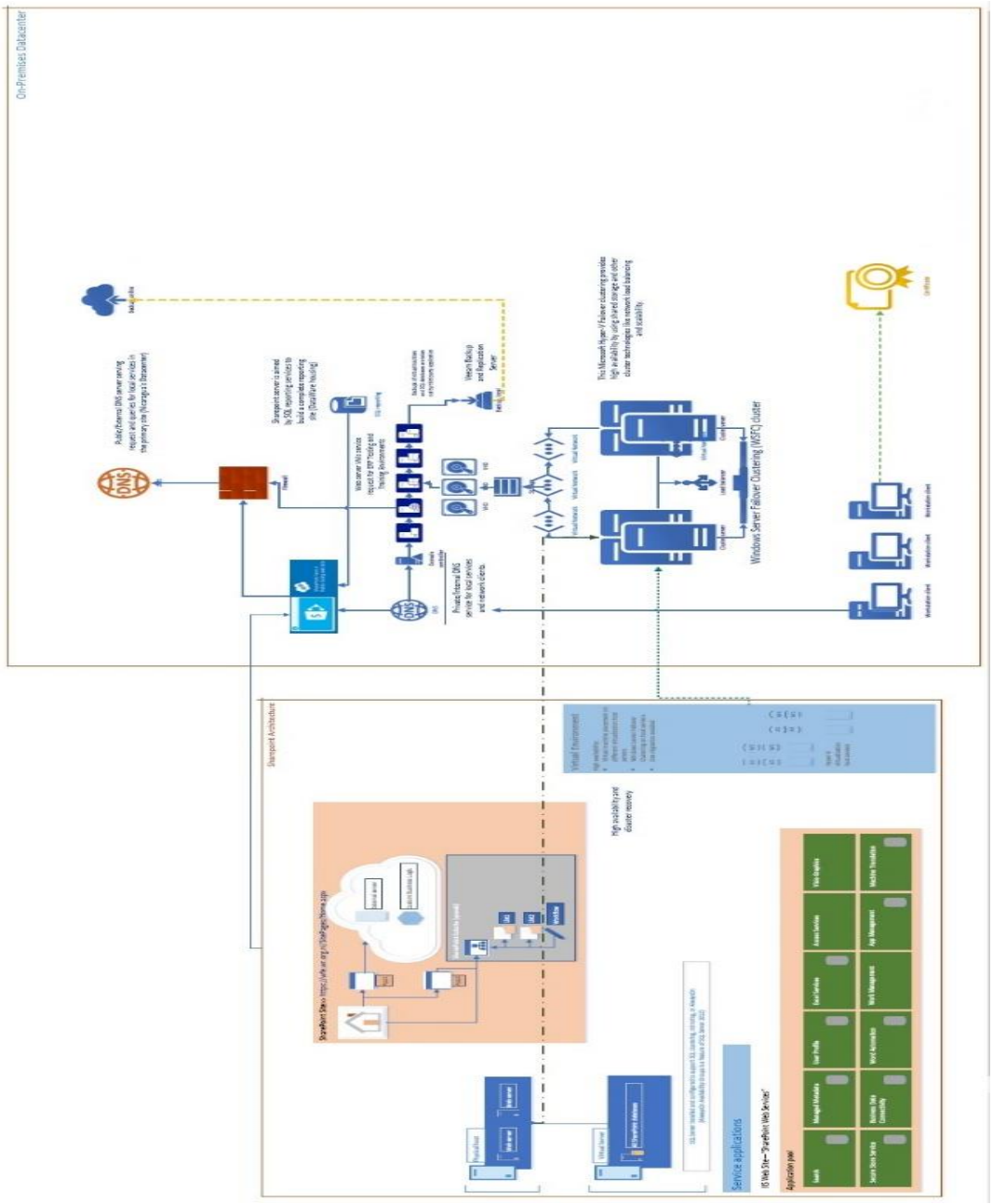


Ilustración 8 Diagrama en bloque de los Servicios informáticos que presenta la infraestructura de red de la Unan-Managua

XI. Glosario

Acceso: Con respecto a la privacidad, es la habilidad de un individuo para ver, modificar y refutar lo completo y precisa que puede ser la información personal identificable (PII) reunida sobre él o ella. Acceso es un elemento de las practicas honesta de información.

ANSI: (American National Standards Institute - Instituto Nacional Americano de Estándares) Es una organización encargada de estandarizar ciertas tecnologías en EEUU. Es miembro fundador de la ISO que es la organización internacional para la estandarización. Sistema de codificación de caracteres alfanuméricos diseñado en el American National Standards Institute, que permite hasta 256 caracteres distintos.

Antimalware server: Se llama **"Malware"** a todo archivo con contenido de carácter malicioso para un equipo informático. Esto no se limita a los virus, pues existen otros muchos archivos capaces de causar daños importantes en un ordenador o en una red informática. Del mismo modo se llama "Antimalware" a aquel software que evita la infiltración en el sistema y el daño.

Antivirus: Es el que detecta la presencia de un virus informático en un disquete o en una computadora y lo elimina.

API: (siglas de 'Application Programming Interface') Es un conjunto de reglas (código) y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas: sirviendo de interfaz entre programas diferentes de la misma manera en que la interfaz de usuario facilita la interacción humano-software.

DHCP: Protocolo de configuración dinámica de Host (**DHCP**) es un protocolo cliente-servidor que proporciona automáticamente un host de protocolo Internet (IP) con su dirección IP y otra información de configuración relacionados como, por ejemplo, la puerta de enlace predeterminada y la máscara de subred.

EAP: Extensible Authentication Protocol (**EAP**) es un framework de autenticación usado habitualmente en **redes** WLAN Point-to-Point Protocol.

EIA: (Electronics Industry Association). Alianza de Industrias Electrónicas: Es una organización comercial compuesta como una alianza de asociaciones de comercio para los fabricantes de electrónica en el de los Estados Unidos. Estas asociaciones, a su vez rigen los sectores de la actividad de las normas de la EIA. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.

Firewall: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

HA: (Alta disponibilidad o sus siglas en ingles "High Availability**"**, es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional), pues permite que la misma sea tolerantes a fallas, tengan una protección contra el tiempo de inactividad y la pérdida de conectividad, en consecuencia aumenta la disponibilidad, productividad y satisfacción del cliente.

HRA: Adaptador de bus de canal de fibra (tarjeta 64 bits PCI-X). Adaptador de bus SCSI (tarjeta 16 bits ISA). En hardware, un adaptador de host, controlador de host o adaptador de bus del host (**HBA**), conecta un sistema **servidor** (computadora) a una red de computadoras y dispositivos o unidades de almacenamiento.

Hyper – V: Es un programa de virtualización basado en un hipervisor para los sistemas de 64-bits con los procesadores basados en AMD-**V** o Tecnología de virtualización Intel (el instrumental de gestión también se puede instalar en sistemas x86).

IEEE 802.1x: La **IEEE 802.1X** es una norma del **IEEE** para el control de acceso a red basada en puertos. Es parte del grupo de protocolos **IEEE** 802 (**IEEE** 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.

IEEE: corresponde a las siglas de The Institute of Electrical and Electronics Engineers el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.

IPsec: (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. **IPsec** también incluye protocolos para el establecimiento de claves de cifrado.

IPv4: Es la versión actual del protocolo de Internet, el sistema de identificación que utiliza Internet para enviar información entre dispositivos. Este sistema asigna una serie de cuatro números (cada uno de los cuales está comprendido entre 0 y 255) a cada dispositivo.

ISO: (International Organization for Standardization) Organización Internacional de Estandarización', sistema de normalización internacional para productos de áreas diversas.

NAP: (Network Access Point) Punto de acceso a la red Un punto de acceso a la red (Network Access Point, **NAP**) era un centro público de intercambio de red donde los proveedores de servicios de internet (ISP) se interconectaban realizando acuerdos de intercambio o peering.

NAS: 'Network Attached Storage', aunque también es conocido por los términos 'almacenamiento conectado a la red'.

NPS: Servidor de directivas de redes. (**NPS**) permite crear y aplicar directivas de acceso a la red en toda la organización con fines de mantenimiento de clientes, autenticación de solicitudes de conexión y autorización de solicitudes de conexión.

Osi: (Open System Interconnection) Es un modelo de interconexión de sistemas abiertos también conocido como un modelo de referencia para los protocolos de la red de arquitectura en capas.

RADIUS: (Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

RSAT: Es una herramienta para los server admin, y permite administrar desde un equipo con Windows 7 el Directorio Activo, DNS, GPO, Hyper V.. etc esta es una notable herramienta. RSAT también permite a los administradores de TI administrar funciones y características que están instalados en los equipos remotos que ejecutan Windows Server 2008 R2 SP1 o Windows Server 2008 R2. Incluye soporte para la administración remota de equipos que ejecutan tanto el núcleo del servidor o las opciones de instalación completa de Windows Server 2008 R2 con SP1, Algunas funciones y características en Windows Server 2003 se pueden administrar en forma remota utilizando Remote Server

SAN: Storage Area Network Es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos: Una red de alta velocidad de canal de fibra.

SHA: (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

TCP: Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo **TCP**/IP.

TIC: Conjunto de técnicas y equipos informáticos que permiten comunicarse a distancia por vía electrónica.

UDP: son las siglas de Protocolo de Datagrama de Usuario (en inglés User Datagram Protocol) un protocolo sin conexión que, como TCP, funciona en redes IP. **UDP**/IP proporciona muy pocos servicios de recuperación de errores, ofreciendo en su lugar una manera directa de enviar y recibir datagramas a través una red IP

VLANs: (Red de área local virtual o LAN virtual) Es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

VPN: (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una **VPN** para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que de otro modo, no podrían.

WSUS: WSUS o Windows Server Update Services es una función más dentro del catálogo de roles disponible en Windows Server 2008 o superior. Este rol permite disponer de un sistema centralizado de actualizaciones para equipos de puesto de trabajo Windows a través de la **red** local de nuestra empresa.