Sistemas Operativos en Red

UD 07. Administración avanzada de Windows Server

Autor: Sergi García

Actualizado Enero 2024

Licencia

Nomenclatura

A lo largo de este tema se utilizarán diferentes símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

📖 **Importante**

❗ **Atención**

💬 **Interesante**

ÍNDICE

Unidad 07. Administración avanzada de Windows Server

1. Introducción

En el desarrollo de esta unidad trataremos la administración de un entorno de Windows Server va más allá de la configuración básica y la gestión de usuarios y recursos. En este contexto, nos sumergiremos en las técnicas y herramientas avanzadas que te permitirán optimizar la administración de tus sistemas, así como ofrecer soluciones efectivas para el despliegue de sistemas operativos, la gestión de aplicaciones y la conectividad remota.

2. Escritorio móvil (Perfiles móviles)

El escritorio móvil (también llamado perfiles móviles) es una técnica que permite a los usuarios almacenar sus archivos y configuraciones de escritorio en una ubicación centralizada accesible desde diferentes dispositivos. Esto se puede lograr utilizando las carpetas de red y la redirección de carpetas en Windows Server.

> ! **Atención**: es interesante que esta ubicación donde guardemos los datos de escritorio, se le haga backup periódico y si es posible tenga algún sistema de redundancia debajo, como un RAID 1 (Espejo).

Para poner en marcha esta técnica, debes seguir estos pasos:

- **Crear una carpeta compartida:** en Windows Server, crea una carpeta compartida en la ubicación deseada donde los usuarios almacenarán sus datos de escritorio. Asegúrate de configurar los permisos adecuados para que los usuarios tengan acceso a esta carpeta compartida. También es importante, si procede, arroparla de medidas de seguridad como backup, RAID 1 (Espejo), etc.
- **Configurar la redirección de carpetas:** utiliza la política de grupo (Group Policy) para configurar la redirección de carpetas de los usuarios. Esto redirigirá automáticamente las carpetas de usuario, como Documentos y Escritorio, a la carpeta compartida que has creado. Para configurarlas:
    - Desde “Herramientas administrativas” y ahí “Administración de directivas de grupo”, busca la GPO que se aplica a tus usuarios del dominio (o crea una nueva, aplicada a todos los usuarios del dominio).
    - Navega hasta "Configuración de usuario" > "Configuración de Windows" > "Redirección de carpetas".
    - Haz clic con el botón derecho en la carpeta que deseas redirigir (por ejemplo, "Escritorio") y selecciona "Propiedades".
    - Elige la opción "Básica: Redirigir todo el contenido de Escritorio a la ubicación siguiente".
    - Especifica la ubicación de la carpeta compartida que creaste en el primer paso.
        - **La ubicación puede ser un recurso compartido en red, recomendando el uso de una carpeta compartida como la propuesta anteriormente.**
- **Aplicar la política de grupo:** asigna la política de grupo que configuraste a las unidades organizativas (OUs), grupos de usuarios específicos que desees o a todos los usuarios. Esto garantizará que la redirección de carpetas se aplique a los usuarios adecuados.
- **Reiniciar los Dispositivos:** los usuarios deben reiniciar sus dispositivos para que los cambios surtan efecto. Después del reinicio, los archivos y configuraciones del escritorio se guardarán automáticamente en la carpeta compartida en lugar de en el perfil local del usuario.

Al implementar esta configuración, centralizarás los datos de escritorio en una carpeta compartida en el servidor, lo que facilita el acceso a los mismos desde múltiples dispositivos y garantiza la disponibilidad y la copia de seguridad de los datos del usuario. Esto puede ser especialmente útil en entornos empresariales donde se necesita un enfoque centralizado de la gestión de datos.

3. REMOTE DESKTOP

Remote Desktop (Escritorio Remoto) es una característica fundamental en Windows Server que permite a los administradores y usuarios acceder y controlar de forma remota:

- **Administración de servidores:** los administradores pueden gestionar servidores Windows Server de forma eficiente sin necesidad de estar físicamente en el centro de datos, lo que ahorra tiempo y recursos.
- **Soporte técnico:** el soporte técnico puede resolver problemas en las estaciones de trabajo de los usuarios finales a través de conexiones remotas, lo que reduce los tiempos de resolución y minimiza la interrupción del trabajo.
- **Entornos virtuales:** en entornos de virtualización, Remote Desktop facilita el acceso a máquinas virtuales (VM) y escritorios virtuales, lo que permite una gestión centralizada y un uso eficiente de los recursos.

Esto es posible hacerse desde cualquier dispositivo compatible con RDP (Remote Desktop Protocol). Algunas de las principales ventajas de Remote Desktop son:

- **Gestión Centralizada:** los administradores pueden acceder de forma remota a servidores y estaciones de trabajo para realizar tareas de administración, actualizaciones, solución de problemas y mantenimiento sin necesidad de estar físicamente en el lugar.
- **Seguridad:** Remote Desktop incorpora mecanismos de seguridad robustos, incluyendo autenticación de dos factores y cifrado de datos, para proteger las conexiones remotas y los datos transmitidos.
- **Escalabilidad:** Windows Server permite habilitar múltiples sesiones de Remote Desktop, lo que facilita el acceso de varios usuarios o administradores a un servidor al mismo tiempo.

Para habilitar Remote Desktop en un servidor Windows Server:

1. Ir a las propiedades del sistema y configurar la opción "Permitir conexiones remotas a este equipo".
2. Configurar las reglas de firewall y las políticas de seguridad de manera adecuada para permitir el acceso remoto.
3. **Los usuarios deben tener permisos para iniciar sesión de forma remota**, lo que se puede configurar en el panel de control de Directivas de Seguridad Local.

> ! **Atención**: aseguraos de tener permiso de inicio de sesión remota, ya que es el error más típico.

4. INSTALAR PAQUETES MSI REMOTAMENTE DE TRABAJO

Para instalar paquetes MSI en estaciones remotas desde un servidor Windows, puedes utilizar varias herramientas y métodos, dependiendo de tus necesidades y preferencias. A continuación, te describimos dos métodos comunes para realizar instalaciones remotas de paquetes MSI en estaciones de trabajo desde un servidor Windows.

4.1 Instalar paquetes MSI mediante Group Policy (Directiva de Grupo)

Este método es adecuado para implementar de instalación de software en múltiples estaciones de trabajo a través de Active Directory. Aquí comentamos como hacerlo:

- **Preparación del paquete MSI**: Asegúrate de tener el archivo MSI del software que deseas instalar disponible en una ubicación accesible desde tu servidor Windows.
    - **Esta ubicación puede ser, por ejemplo, una carpeta compartida en el servidor.**
- **Creación de una política de grupo:** Desde "Herramientas administrativas" y ahí "Administración de directivas de grupo", busca la GPO que se aplica a tus usuarios del dominio o Crea una nueva GPO (Objeto de Política de Grupo) aplicada a quien corresponda.
- **Configuración de la política de Instalación:** en la GPO, navega hasta "Configuración del equipo" > "Directivas" > "Software" > "Instalación de software". Haz clic con el botón derecho y selecciona "Nuevo" > "Paquete" para agregar el paquete MSI.
- **Especificar la ubicación del paquete MSI**: selecciona el archivo MSI que deseas instalar desde la ubicación donde se encuentra almacenado **(por ejemplo, en una carpeta compartida en red en el servidor)**.
- **Configurar opciones de instalación:** puedes configurar opciones como "Asignar" o "Publicar" el software y seleccionar el método de instalación (por ejemplo, "Instalar este programa en modo silencioso").
- **Aplicar la política de grupo:** asigna la GPO a las unidades organizativas (OUs) que contengan las estaciones de trabajo en las que deseas realizar la instalación remota. Las estaciones de trabajo afectadas por la GPO recibirán automáticamente el paquete MSI y lo instalarán.

4.2 Instalar paquetes MSI mediante PowerShell remoto

Otro enfoque más flexible para realizar la instalación de paquetes MSI (e incluso de otro tipo de instalaciones de software más complejas) donde quieres que las instalaciones remotas de manera más específica o en un número reducido de estaciones de trabajo, puedes utilizar PowerShell remoto. Aquí está como hacerlo:

- **Configuración de PowerShell remoto:** Asegúrate de que PowerShell Remoto esté habilitado en las estaciones de trabajo que deseas administrar. Puedes habilitarlo utilizando el cmdlet "*Enable-PSRemoting*" en PowerShell en cada estación de trabajo.
- **Creación de un script de PowerShell:** Crea un script de PowerShell que utilice el cmdlet "*Start-Process*" para ejecutar el archivo MSI (o cualquier otro conjunto de instrucciones necesarias para hacer la instalación) en las estaciones de trabajo remotas. El script debe contener la lógica necesaria para identificar y conectar las estaciones de trabajo.
- **Ejecución del script**: ejecuta el script de PowerShell en el servidor Windows para iniciar la instalación remota en las estaciones de trabajo específicas.

5. WDS (WINDOWS DEPLOYMENT SYSTEM)

Windows Deployment Services (WDS) es una característica de Windows Server que facilita la implementación de sistemas operativos Windows en múltiples computadoras a través de la red. WDS permite la implementación automatizada de sistemas operativos Windows en computadoras cliente sin la necesidad de intervención manual. Esto ahorra tiempo y reduce la posibilidad de errores humanos durante el proceso de instalación.

WDS se integra estrechamente con Active Directory, lo que permite una autenticación segura y un control de acceso granular para garantizar que solo las computadoras autorizadas puedan recibir imágenes de implementación.

Pasos Generales para Configurar WDS:

- **Instalar el Rol WDS**: en tu servidor Windows, instala el rol de Windows Deployment Services a través del Administrador del Servidor o PowerShell.
- **Configurar las carpetas de implementación:** define las carpetas donde se almacenarán las

imágenes de sistema operativo y los archivos de implementación.

- **Agregar imágenes del sistema operativo:** importa o crea imágenes de sistema operativo que deseas implementar en las computadoras cliente.
- **Configurar opciones de implementación:** define las opciones de implementación, como el tipo de implementación (sin intervención, imágenes de arranque, etc.), las reglas de selección de imágenes y las configuraciones de red.
- **Iniciar implementaciones:** desde la consola de WDS, puedes iniciar implementaciones en las computadoras cliente seleccionadas.

6. SERVA, SERVIDOR PXE GRATUITO (ALTERNATIVA A WDS)

Serva es una herramienta de implementación de código abierto que se utiliza en lugar de Windows Deployment Services (WDS) en algunos escenarios específicos. Esta herramienta se puede obtener en https://www.vercot.com/~serva/

Algunas ventajas de Serva respecto a WDS son:

- **Facilidad de configuración:** Serva es conocido por su configuración relativamente sencilla en comparación con WDS. No requiere una infraestructura de servidor Windows completa y es más rápido de configurar, lo que puede ser una ventaja para pequeñas empresas o entornos de laboratorio.
- **Sin necesidad de Active Directory:** A diferencia de WDS, que a menudo se integra estrechamente con Active Directory para la autenticación y el control de acceso, Serva no tiene esta dependencia. Esto significa que puede ser una solución más simple si no estás utilizando Active Directory en tu entorno.
- **Compatibilidad con sistemas no Windows:** Serva puede ser utilizado para implementar sistemas operativos Linux y otras imágenes ISO además de Windows. Esto lo hace atractivo para entornos que utilizan una variedad de sistemas operativos.
- **No se requieren licencias adicionales:** Mientras que WDS forma parte del ecosistema de servidores Windows y puede requerir licencias adicionales de Windows Server, Serva es de código abierto y, por lo tanto, no conlleva costos de licencia directos.
- **Flexibilidad en la estructura de carpetas:** Serva permite una estructura de carpetas más flexible para almacenar imágenes y archivos de implementación, lo que puede facilitar la organización y el mantenimiento.
- **Soporte comunitario:** al ser de código abierto, Serva tiene una comunidad activa de usuarios y desarrolladores que pueden proporcionar soporte y soluciones a problemas comunes.

A pesar de estas ventajas, es importante destacar que WDS sigue siendo la solución preferida para muchas organizaciones, especialmente aquellas que ya tienen una infraestructura de servidor Windows y requieren una administración de implementaciones a gran escala, alta disponibilidad y características de seguridad avanzadas.

7. ENRUTAMIENTO

En un entorno de red, el enrutamiento se refiere al proceso de dirigir el tráfico de red desde una fuente hasta su destino a través de una serie de nodos intermedios, como routers o servidores. Cuando hablamos de **compartir Internet en Windows Server 2022**, generalmente estamos hablando de configurar el servidor para actuar como un router y permitir que otros dispositivos en la red accedan a Internet a través de él. A continuación, te proporcionaré una guía básica para configurar el enrutamiento en Windows Server 2022.

Pasos para configurar enrutamiento en Windows Server 2022:

- **Instala el Rol de Enrutamiento:**

    - Abre el "Administrador del servidor".
    - Haz clic en "Agregar roles y características".
    - Selecciona "Acceso remoto" en la lista de roles y completa el proceso de instalación. En algún momento te pedirá marcará para instalar tanto “Acceso remoto” como “Enrutamiento”. Debes marcar e instalar los roles.
- **Configura el Rol de Enrutamiento y Acceso Remoto:**
    - Después de instalar el rol, busca y abre la herramienta "Enrutamiento y acceso remoto" desde el "Administrador del servidor".
    - En la consola de enrutamiento y acceso remoto, expande el nombre del servidor y haz clic con el botón derecho en "Enrutamiento IPv4".
    - Selecciona "NAT" (Network Address Translation) y sigue el asistente para configurar la traducción de direcciones de red.
- **Configura la interfaz de red:** asegúrate de que las interfaces de red estén configuradas correctamente. La interfaz que conecta el servidor a Internet debe tener una dirección IP válida y configurada para obtener la dirección IP de manera automática (DHCP) o manualmente.
- **Configura las reglas de firewall:** ajusta las reglas de firewall para permitir el tráfico a través de la interfaz de red que proporciona acceso a Internet. Puedes hacer esto utilizando el "Firewall de Windows con seguridad avanzada".
- Prueba la Conexión: conecta un dispositivo en la red interna al servidor y verifica que tenga acceso a Internet.

Esta propuesta es un escenario básico utilizado para compartir Internet con los clientes. En otros casos puede haber consideraciones adicionales según la topología de tu red y los requisitos de seguridad.

8. DHCP EN WINDOWS SERVER

Configurar DHCP (Protocolo de Configuración Dinámica de Host) y VPN (Red Privada Virtual) en un servidor Windows Server 2022 puede ser esencial para gestionar las direcciones IP de los dispositivos en tu red.

Configuración del servicio DHCP:

- **Instala el rol de DHCP:**
    - Abre el "Administrador del servidor".
    - Haz clic en "Agregar roles y características".
    - Selecciona "Servicios de dominio de Active Directory" (si no estaban ya) y "Protocolo de configuración dinámica de host (DHCP)".
    - Completa el asistente de instalación.
- **Configura el servicio DHCP:**
    - Después de instalar el rol, abre la herramienta "DHCP" desde el "Administrador del servidor".
    - Expande el nombre del servidor y selecciona "Ámbitos".
    - Crea un nuevo ámbito DHCP para definir el rango de direcciones IP que se asignarán automáticamente a los dispositivos en la red.
    - Configura las opciones de ámbito, como la puerta de enlace predeterminada y los servidores DNS.
- **Autoriza el servidor DHCP:**
    - Asegúrate de que el servidor DHCP esté autorizado en la red. Esto es crucial para evitar conflictos con otros servidores DHCP.
- **Prueba el servicio DHCP:**
    - Conecta un dispositivo a la red y verifica si obtiene una dirección IP

automáticamente.

9. VPN EN WINDOWS SERVER

Una VPN (Red Privada Virtual) https://es.wikipedia.org/wiki/Red_privada_virtual permite expandir una red local a través de una red externa y no segura como por ejemplo Internet. Para conseguir esto, un servicio de VPN proporciona un túnel cifrado para el tráfico de datos, lo que garantiza que la información confidencial se mantenga segura durante la transmisión a través de Internet.

A efectos prácticos, con una VPN, los usuarios remotos pueden conectarse a través de Internet a la red interna de la organización como si estuvieran físicamente en la ubicación de la oficina, lo que facilita el acceso a recursos internos, aplicaciones y servicios.

Los pasos Generales para Configurar una VPN en Windows Server son:

- **Instalar el rol de "Acceso Remoto":** utiliza la herramienta "Administrador del servidor" para instalar el rol de "Acceso remoto". Ahí, elige como sub-rol, el de VPN. Esto habilitará la funcionalidad de VPN en tu servidor.
- **Configurar el servicio de VPN**: abre en “Herramientas administrativas” la herramienta "Enrutamiento y acceso remoto" y configura el servicio VPN. Esto incluye definir la autenticación, las direcciones IP que se asignarán a los clientes y las políticas de acceso.
- **Configurar el Firewall:** asegúrate de que el firewall en el servidor y cualquier dispositivo de red intermedio permita el tráfico VPN (generalmente utilizando los protocolos PPTP, L2TP/IPsec o SSTP).
- **Asignar permisos de acceso:** define quiénes pueden conectarse a la VPN configurando permisos de acceso en el servidor VPN. Esto generalmente se hace mediante la creación de grupos de usuarios o usuarios específicos autorizados para conectarse.
- **Configurar clientes VPN:** en los dispositivos cliente, configura una conexión VPN utilizando las credenciales proporcionadas y la dirección IP o el nombre de dominio del servidor VPN.
- **Pruebas y mantenimiento**: realiza pruebas para asegurarte de que la VPN esté funcionando correctamente. Además, realiza un mantenimiento periódico para asegurarte de que el servicio siga siendo seguro y eficiente.

La configuración de una VPN en Windows Server es una estrategia efectiva para ampliar la conectividad de red y garantizar la seguridad de las comunicaciones remotas (es decir, desde fuera de la red interna donde tengamos el servidor de Windows Server).

Una vez configurada una VPN, para probarla, deberéis utilizar un cliente VPN. Windows 10 incorpora el suyo propio de forma nativa (más información en https://support.microsoft.com/es-es/windows/conectarse-a-una-vpn-en-windows-3d29aeb1-f497-f6b7-7633-115722c1009c) pero existen multitud de clientes y servidores VPN libres para Windows, Linux, etc. como OpenVPN https://openvpn.net/community-downloads/ que dispone tanto de servidor como de cliente VPN.

10. PLANTILLAS DE CREACIÓN DE USUARIOS

En Windows Server 2022, puedes usar plantillas de creación de usuario para facilitar la creación de usuarios con configuraciones predefinidas.

Estrategia para creación y uso de plantillas de usuario:

- **Crear el usuario original:**
    - Inicia sesión en el servidor con privilegios administrativos.
    - Abre el "Administrador de usuarios y equipos de Active Directory" (dsa.msc).
    - Navega a la unidad organizativa (OU) donde deseas crear el usuario.

    - Haz clic derecho y selecciona "Nuevo" > "Usuario".
    - Completa el asistente para crear un nuevo usuario con la configuración inicial deseada.
- **Copiar a un nuevo usuario:**
    - Después de haber creado el usuario original, busca el usuario en el "Administrador de usuarios y equipos de Active Directory".
    - Haz clic derecho en el usuario original y selecciona "Propiedades".
    - Ve a la pestaña "Perfil".
    - En la sección "Perfil de usuario", haz clic en "Copia a".
    - Especifica la ruta del nuevo usuario al que deseas copiar la configuración.
- **Configuración adicional del nuevo Usuario:**
    - Después de copiar la configuración, puedes modificar el nuevo usuario según sea necesario. Esto puede incluir cambiar el nombre de usuario, la contraseña y cualquier otra configuración específica.
- **Verificación:**
    - Verifica que el nuevo usuario tenga la configuración copiada correctamente. Puedes hacer esto revisando las propiedades del nuevo usuario en la pestaña "Perfil".

Este enfoque es útil cuando deseas crear múltiples usuarios con configuraciones similares, ya que puedes evitar tener que configurar manualmente cada usuario. **Sin embargo, ten en cuenta que esta técnica no aborda todos los aspectos de la configuración del usuario, como permisos de carpeta y grupos de seguridad, que requieren configuración adicional.**

11. UNIR UN EQUIPO LINUX A UN DOMINIO WINDOWS SERVER

Dado que la autentificación en Active Directory de Windows Server utiliza Kerberos y LDAP para establecer la autenticación y la comunicación con el dominio, es posible agregar clientes GNU/Linux a dominios Windows. Para ello, además de una configuración de red adecuada y una resolución de DNS correcta, existen herramientasque facilitan la unión de clientes Linux a un dominio Windows. Una de las fórmulas más populares es la de utilizar las herramientas **SSSD (System Security Services Daemon) y "realmd"**. Estas herramientas proporciona un conjunto de servicios para integrar sistemas Linux con servicios de directorio, como Active Directory. En los siguientes enlaces explica su uso:

- https://blog.netwrix.com/2022/11/01/join-linux-hosts-to-active-directory-domain/
- https://somebooks.es/unir-un-cliente-ubuntu-20-04-a-un-dominio-de-active-directory-sobre-windows-server-2019-parte-1/
- https://somebooks.es/unir-un-cliente-ubuntu-20-04-a-un-dominio-de-active-directory-sobre-windows-server-2019-parte-2/

Como la configuración es algo tediosa, existen scripts que permiten automatizar esta tarea. Aquí algunos de los más populares:

- https://github.com/PierreGode/Linux-Active-Directory-join-script
- https://github.com/rfinotti/join_domain

12. BIBLIOGRAFÍA

[1] “Sistemas Operativos en Red, 2ª edición” de SomeBooks. El libro está disponible en la siguiente dirección http://somebooks.es/sistemas-operativos-red-2a-edicion/

[2] Mastering Windows Server 2022 - Fourth Edition, Jordan Krause

[3] Introducción a Windows Server 2022
https://learn.microsoft.com/es-es/windows-server/get-started/get-started-with-windows-server

[4] Grupos en Windows Server 2022
https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-groups