Práctica No. 2

Código: DSUP11-GP-02

Nombre: Carlos Fabian Garces Torres
Título: Active Directory

Tiempo de duración: 120 minutos.

Fundamentos:

Active Directory (AD) es un servicio de directorio desarrollado por Microsoft para los sistemas operativos Windows Server. Este servicio permite a los administradores gestionar permisos y acceso a recursos de la red de manera centralizada. Según Tulloch y Team (2013), Active Directory es una pieza fundamental en la arquitectura de una red empresarial, proporcionando servicios de autenticación y autorización, así como una estructura de directorios jerárquica que facilita la administración de usuarios y recursos.

Historia y Evolución de Active Directory

Active Directory fue introducido por primera vez con Windows 2000 Server y ha evolucionado significativamente en las versiones subsiguientes de Windows Server. La evolución de AD ha incluido mejoras en la escalabilidad, seguridad y funcionalidad. Stanek (2013) destaca que una de las principales mejoras en versiones más recientes, como Windows Server 2016 y 2019, ha sido la incorporación de características como el reciclaje de objetos de Active Directory, la autenticación basada en privilegios y la integración con servicios en la nube.

Componentes Principales de Active Directory

Active Directory está compuesto por varios componentes esenciales que trabajan en conjunto para proporcionar sus servicios. Entre estos componentes se encuentran el

controlador de dominio, el almacén de datos (base de datos de AD), el servicio de replicación y los servicios de autenticación y autorización. Según Charte (2005), el controlador de dominio es el núcleo de Active Directory, respondiendo a las solicitudes de autenticación y gestionando las políticas de seguridad. El almacén de datos almacena información sobre los objetos del directorio, como usuarios, grupos y dispositivos, mientras que el servicio de replicación asegura que los datos se mantengan consistentes en todos los controladores de dominio de la red.

Funcionalidades y Beneficios de Active Directory

Active Directory ofrece una amplia gama de funcionalidades que benefician a las organizaciones de diversas maneras. Una de las funciones clave es el servicio de autenticación Kerberos, que proporciona un método seguro para que los usuarios inicien sesión en la red. Además, AD permite la implementación de políticas de grupo (Group Policy), que ayudan a los administradores a controlar la configuración de los sistemas y usuarios en toda la red desde un punto centralizado (Charte, 2005).

Otro beneficio significativo de Active Directory es su capacidad para manejar grandes cantidades de datos y usuarios de manera eficiente. Gracias a su estructura jerárquica, AD permite la delegación de autoridad administrativa, facilitando la gestión de grandes redes empresariales. Asimismo, la integración de Active Directory con otros servicios de Microsoft, como Exchange Server y SharePoint, proporciona una administración de recursos unificada y simplificada (Charte, 2005).

Seguridad en Active Directory

La seguridad es un aspecto crucial de Active Directory, y Microsoft ha incorporado diversas medidas para proteger los datos y la integridad de la red. Entre estas

medidas se encuentran el uso de autenticación multifactor, políticas de contraseñas robustas y el monitoreo continuo de actividades sospechosas. La función de Control de Acceso Basado en Roles (RBAC) permite a los administradores definir permisos específicos para diferentes roles dentro de la organización, reduciendo así el riesgo de acceso no autorizado (Charte, 2005).

Objetivos

- Instalar un sistema operativo Windows y configurar su tarjera de red para tener acceso a la red.
- Instalar el servicio de active Directory dentro del sistema operativo.
- Configurar un servidor DHCP en el controlador de directorio activo y comprobar su funcionamiento.

Materiales y Herramientas

- Windows Server 2019
- VirtualBox/Hiper-V
- Software de conexión remota
- Computador

Normas de Seguridad

Uso adecuado del equipamiento

Además, deben manipular los dispositivos con cuidado, evitando movimientos bruscos y asegurándose de seguir las instrucciones específicas para el uso de hardware y software.

Cumplimiento de las Políticas de la Institución

Respetar los horarios de uso del laboratorio y las normas de conducta establecidas por la institución.

Supervisión

Realizar todas las pruebas de funcionamiento del sistema bajo la supervisión del docente.

Inspección Previa

Inspeccionar visualmente todos los componentes antes de su uso para detectar posibles daños o defectos.

Preparación Previa del Estudiante

Fundamentos de Sistemas Operativos.

Es esencial que los estudiantes tengan una comprensión sólida de los sistemas operativos, especialmente Windows Server. Deben conocer cómo se administra un sistema operativo a nivel básico, incluyendo la instalación, configuración y gestión de servicios. Según Stanek (2003), estos conocimientos son fundamentales para comprender cómo se integra y funciona Active Directory dentro del entorno de Windows Server.

Conceptos Básicos de Redes

Los estudiantes deben estar familiarizados con los conceptos básicos de redes, como direcciones IP, subredes, máscaras de red, y protocolos de comunicación (TCP/IP). Este conocimiento es crucial para configurar y gestionar Active Directory, ya que AD depende de una infraestructura de red para su funcionamiento y replicación. Tulloch y Team (2013) señalan que la comprensión de estos conceptos ayuda a los estudiantes a diagnosticar y resolver problemas de conectividad que puedan surgir durante la configuración de AD.

Familiaridad con la Línea de Comandos y PowerShell

Aunque muchas configuraciones de Active Directory se pueden realizar a través de interfaces gráficas, la línea de comandos y PowerShell son herramientas poderosas para la administración de AD. Los estudiantes deben estar cómodos usando comandos básicos y cmdlets de PowerShell para realizar tareas de administración. La capacidad de escribir y ejecutar scripts de PowerShell puede facilitar la automatización de tareas repetitivas y mejorar la eficiencia (Stanek, 2013).

Conocimiento de Servicios de Red y Roles de Servidor

Es importante que los estudiantes comprendan los roles y servicios que se pueden instalar en Windows Server, como DHCP, DNS y el servicio de archivos. Active

Directory depende especialmente del servicio DNS para la localización de controladores de dominio y la replicación. Según Charte (2005), conocer cómo instalar y configurar estos servicios es esencial para asegurar que Active Directory funcione correctamente.

Gestión de Usuarios y Permisos

Una parte integral de la administración de Active Directory es la gestión de usuarios, grupos y permisos. Los estudiantes deben comprender cómo crear, modificar y eliminar cuentas de usuario y grupo, así como cómo asignar permisos y políticas de grupo. Este conocimiento es fundamental para garantizar que solo los usuarios autorizados tengan acceso a los recursos de la red y para mantener la seguridad del entorno de AD (Stanek, 2013).

Seguridad y Políticas de Grupo

Los estudiantes deben tener una comprensión básica de las políticas de grupo (Group Policy) y cómo se utilizan para aplicar configuraciones y restricciones en usuarios y equipos dentro de una red de Active Directory. Conocer cómo crear y aplicar políticas de seguridad robustas es esencial para proteger la red y los datos. Además, deben estar familiarizados con las mejores prácticas de seguridad para minimizar el riesgo de brechas de seguridad (Stanek, 2013).

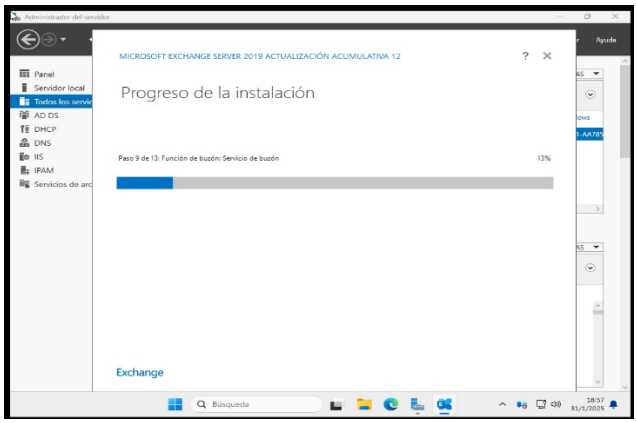
Familiaridad con la Estructura de Active Directory

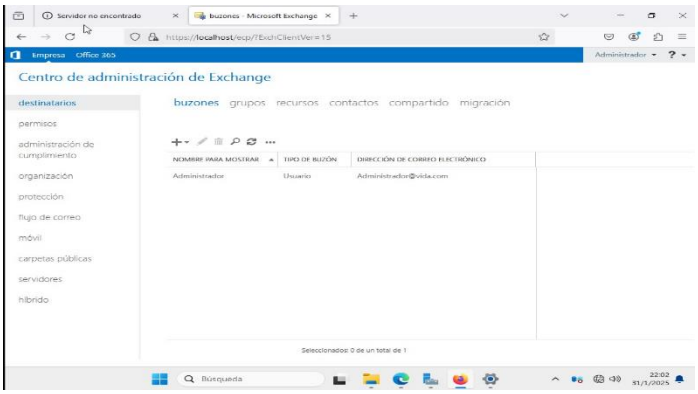
Es crucial que los estudiantes comprendan la estructura jerárquica de Active Directory, incluyendo los conceptos de dominios, árboles, bosques, unidades organizativas (OUs), y sitios. Este conocimiento les permitirá diseñar e implementar una estructura de AD que sea escalable y eficiente, y que refleje adecuadamente la organización y sus necesidades administrativas (Stanek, 2013).

Procedimiento

1. Prepare los medios de instalación y los recursos necesarios para la instalación de Windows Server.
2. Estructure el entorno virtual.
3. Realice la instalación del controlador de dominio en Windows Server.
4. Configure el controlador de dominio en Windows Server.
5. Defina la estructura del dominio y sus unidades organizativas y registre los componentes en la tabla 1.
6. Cree usuarios y dentro del controlador de dominio configurado.
7. Aplique una directiva de grupo para poder gestionar los recursos de la red según se detalla en la tabla 1.

Descripción de Resultados Obtenidos





Conclusiones

- Instalación de Windows y Configuración de la Tarjeta de Red Se logró instalar correctamente el sistema operativo Windows y configurar tarjeta de red, permitiendo el acceso a la red. Esto es esencial para la comunicación entre dispositivos y la integración con servicios de red como Active Directory.
- Directory en el servidor permite la gestión centralizada de usuarios, dispositivos y políticas dentro de la red. Esto facilita la administración de recursos y la seguridad mediante autenticación y control de acceso.

- Configuración y Verificación del Servidor DHCP El servidor DHCP se configuró en el controlador de dominio, permitiendo la asignación automática de direcciones IP a los dispositivos de la red. Su correcto funcionamiento garantiza una administración eficiente de la red y evita conflictos de direcciones IP.

Evaluación del Aprendizaje

¿Cuáles son los principales componentes de Active Directory y cómo se integran para proporcionar servicios de autenticación y autorización en una red?

Los principales componentes de active directory son dominios, controladores de dominio, bosques árboles, unidades organizativas, catalogo global, LDPA y políticas de seguridad de grupo, estos grupos trabajan juntos para para autenticar a los usuarios administrar permisos y aplicar configuraciones de una red, asegurando el acceso seguro y centralizado de recursos

Explique el proceso de configuración de un controlador de dominio en Windows Server 2019. ¿Cuáles son los pasos clave y las consideraciones importantes que se deben tener en cuenta?

Para configurar un controlador de dominio en Windows Server 2019 se asigna una ip estática, se instala ADDS se promociona el servidor, se configura el dominio y se reinicia es clave asegurar una red estable, aplicar actualizaciones establecer seguridad y elegir niveles funcionales compatibles con la estructura existente.

¿Qué es una Política de Grupo (Group Policy) en Active Directory y cómo se utiliza para gestionar configuraciones y restricciones en una red? Proporcione un ejemplo de una política comúnmente aplicada.

Una política de GPO en active Directory permite gestionar configuraciones y restricciones en usuarios y equipos de una red , Se aplica desde el controlador de dominio un ejemplo común es restringir el acceso al panel de control evitando cambios no autorizados en la configuración del sistema

Describa cómo se gestionan los usuarios y grupos en Active Directory. ¿Cuáles son las mejores prácticas para asegurar que solo los usuarios autorizados tengan acceso a los recursos de la red?

En ACTIVE DIRECTOY los usuarios y los grupos se gestionan mediante Unidadaes organizativas y políticas Las mejores prácticas incluyen usar grupos de seguridad,aplicar el principio de privilegio mínimo y habilitar autenticación de multifactor

Criterio	Excelente (5)	Bueno (4)	Satisfactorio (3)	Necesita Mejora (2)	Insuficiente (1)
Instalación y Configuración de Controlador de Dominio	Instalación y configuración del controlador de dominio realizada sin errores, con todos los servicios operativos.	Instalación mayormente correcta, con pequeños errores solucionables.	Instalación funcional, pero con varios errores menores o configuraciones subóptimas.	Instalación con errores significativos o incompleta, con varias funcionalidades no operativas.	Instalación incorrecta o fallida, con muchas funcionalidades no operativas.
Configuración de Usuarios y Grupos	Creación y gestión de usuarios y grupos realizada correctamente , con políticas	Creación y gestión de usuarios y grupos mayormente correcta, con pequeños	Gestión funcional de usuarios y grupos, pero con varios errores menores.	Gestión incorrecta o incompleta de usuarios y grupos, con problemas	Gestión de usuarios y grupos incorrecta o no realizada, con graves

	de seguridad bien definidas y documentadas.	errores menores.		significativos de seguridad.	problemas de seguridad.
Implementación de Políticas de Grupo	Configuración y aplicación de Políticas de Grupo realizada correctamente, con ejemplos prácticos aplicados correctamente.	Implementación de Políticas de Grupo mayormente correcta, con pequeños errores menores.	Implementación funcional de Políticas de Grupo, pero con varios errores menores o configuraciones subóptimas.	Implementación incorrecta o incompleta de Políticas de Grupo, con problemas significativos.	Políticas de Grupo no implementadas o implementadas incorrectamente, con graves problemas de configuración.
Configuración de DNS y Servicios de Red	Configuración de DNS y otros servicios de red realizada correctamente, asegurando la correcta resolución de nombres y replicación.	Configuración de DNS y servicios de red mayormente correcta, con pequeños errores menores.	Configuración funcional de DNS y servicios de red, pero con varios errores menores o ineficiencias.	Configuración incorrecta o incompleta de DNS y servicios de red, con problemas significativos de conectividad.	Configuración de DNS y servicios de red incorrecta o no realizada, con graves problemas de conectividad.
Seguridad y Administración de AD	Implementación completa de medidas de seguridad, incluyendo auditorías y controles de acceso avanzados, sin errores.	Implementación de medidas de seguridad mayormente correcta, con algunos errores menores.	Implementación funcional de medidas de seguridad, pero con varios errores menores o omisiones.	Implementación incorrecta o incompleta de medidas de seguridad, con problemas significativos.	Medidas de seguridad no implementadas o implementadas incorrectamente, con graves vulnerabilidades.

Bibliografía

Charte, F. (2005). *Windows Server 2003* (Manuales Avanzados).

Tulloch, M., Team, W. S. (2013*). Introducing Windows Server 2012 R2*. Microsoft press.

Stanek, W. (2013). *Windows Server 2012 inside out*. Pearson Education.

Anexos

Tabla 1

Pasos para levantar un controlador de dominio.

Numero	Pasos
Preparar el entorno	Asegúrate de tener Windows Server 2019 instalado y configurado con las actualizaciones más recientes.
	Asigna una dirección IP estática al servidor.

	Configura el nombre del servidor correctamente, ya que este nombre formará parte del dominio.
Instalar Active Directory Domain Services (AD DS)	Abre el Server Manager.
	Haz clic en Agregar roles y características.
	En la ventana del asistente, selecciona Instalación basada en roles o características.
	Selecciona tu servidor y haz clic en Siguiente.
	En la ventana de Roles de servidor, selecciona Servicios de dominio de Active Directory (AD DS) y confirma agregando las características necesarias.
	Haz clic en Siguiente y luego en Instalar.
Promover el servidor a controlador de dominio	Después de la instalación, aparecerá una notificación en el Server Manager indicando que se requiere promover este servidor a controlador de dominio. Haz clic en Promover este servidor a controlador de dominio.
	Selecciona la opción Agregar un nuevo bosque si es el primer dominio, e ingresa el nombre del dominio raíz (por ejemplo, example.local).
	Configura las opciones del nivel funcional del bosque y dominio. Por defecto, selecciona Windows Server 2016 o superior.
	Configura la contraseña del modo de restauración de directorios (DSRM).
	Revisa las opciones de DNS y deja la configuración por defecto, a menos que necesites hacer ajustes avanzados.
	Revisa las rutas de las bases de datos y archivos de registro de AD y haz clic en Siguiente.
	Haz clic en Instalar para completar la promoción del servidor a controlador de dominio. El servidor se reiniciará automáticamente.
Configuración posterior	Una vez que el servidor se reinicie, verifica que el dominio esté funcionando correctamente.
	Usa la herramienta Usuarios y Equipos de Active Directory para empezar a administrar tu dominio, crear usuarios, grupos, y organizar la estructura del AD.
Configurar DNS (Opcional)	Revisa la configuración de DNS para asegurarte de que esté funcionando correctamente, ya que Active Directory depende de DNS para la resolución de nombres dentro del dominio.

Nota. En la tabla se detallan los pasos para crear un controlador de dominio

MX y ADML en el contexto de las plantillas administrativas. ¿Por qué es importante entender estas diferencias al administrar políticas de grupo en un entorno multilingüe?