1. Administración de Sistemas Windows

1.1. Introducción y objetivos

En este tema vamos a estudiar los conceptos asociados a Windows Server que es un sistema operativo de tipo servidor, preparado para gestionar una red de ordenadores mediante un sistema de dominios y un directorio activo que permite una administración centralizada.

Existen varios roles principales dentro de Windows Server que cualquier empresa necesita instalar y configurar. Entre los más importantes tenemos los roles de ficheros, impresión, DNS, DHCP y servidor web y comentaremos su configuración en un entorno empresarial.

Finalizaremos el tema con una aproximación a la integración de Windows Server con las nubes públicas. Hoy en día, ya casi no existen instalaciones únicas de Windows Server, sino que se poseen las denominadas redes hibridas con conexiones a las nubes públicas.

Con el estudio de este tema pretendemos alcanzar los siguientes objetivos:

* Diferenciar las versiones existentes del producto, así como las diferentes instalaciones.
* Aprender a instalar un directorio activo y manejaremos las diferentes consolas de gestión.
* Aplicar políticas de grupo para configurar entornos empresariales y como afectan a los clientes basados en Windows conectados a la red.
* Instalar servidores de ficheros y servidores web.
* Conocer los servicios de red principales en un entorno Windows Server.
* Aplicar las configuraciones de seguridad más habituales en entornos corporativos con infraestructura Windows
* Introducirnos en el mundo híbrido, empresa-nube pública.

En los vídeos de este tema podremos aprender los siguientes conceptos:

Vídeo 1. Instalación Windows Server. Después de la instalación limpia de un Windows Server crearemos un directorio activo.

Vídeo 2. Gestionaremos usuarios y máquinas en el directorio activo creado en el vídeo anterior. Así mismo instalaremos nuevos roles como el role DHCP.

1.2. Ediciones e instalación de Windows

Tal y como pide Microsoft (2022), al instalar Windows Server, debe elegir entre instalar el servidor con o sin la Experiencia de escritorio.

Importante

Esta es una decisión fundamental porque no puede agregar ni quitar la Experiencia de escritorio después de instalar el servidor.

Server Core es una instalación de Windows Server sin la Experiencia de escritorio. Server Core está disponible para las ediciones Standard y Datacenter, pero no está disponible para Windows Server Essentials, y la versión gratuita de Hyper-V Server solo está disponible como una instalación de Server Core.

Puede administrar y configurar Server Core en el propio servidor a través de PowerShell, la línea de comandos o a través de la herramienta basada en texto denominada Sconfig.

A screenshot of a computer

Description automatically generated

Figura 1. Configuración Windows Server Core con Sconfig. Fuente: elaboración propia.

La administración remota es el método normal de administración del servidor mediante el uso de varias herramientas, como la comunicación remota de PowerShell, la herramienta de administración remota del servidor (RSAT) y Windows Admin Center. En la siguiente tabla se describen las herramientas disponibles localmente.

A table of information

Description automatically generated with medium confidence

Tabla 1. Herramientas Windows server. Fuente: elaboración propia.

Server Core tiene ventajas sobre Windows Server con Experiencia de escritorio y es la instalación recomendada para la mayoría de los escenarios, pero puede que no sea adecuado en todos los casos. En la tabla siguiente se enumeran las principales ventajas y desventajas.

A table with text on it

Description automatically generated

Tabla 2. Ventajas e inconvenientes del Server Core. Fuente: elaboración propia.

Roles de servidor disponibles

Aunque algunos roles de servidor no están disponibles, en las implementaciones de Server Core están disponibles los siguientes:

* Servicios de certificados de Active Directory.
* AD DS.
* Servidor DHCP.
* Servidor DNS.
* Servicios de archivo (incluido Administrador de recursos del servidor de archivos).
* Active Directory Lightweight Directory Services (AD LDS).
* Hyper-V.
* Servicios de impresión y documentos.
* Servicios de multimedia de transmisión por secuencias.
* Servidor web (incluido un subconjunto de ASP.NET).
* Servidor Windows Server Update.
* Servidor de Active Directory Rights Management.
* Servidor de acceso remoto.

Configuración posterior a la instalación

Después de instalar Windows Server, normalmente debe completar las siguientes acciones:

* Configurar la dirección IP.
* Establecer el nombre de equipo.
* Unirse a un dominio de Active Directory.
* Configure la zona horaria.
* Habilitar las actualizaciones automáticas.
* Agregar roles y características.
* Habilitar la característica Escritorio remoto.
* Configurar Firewall de Windows Defender.

Puede realizar esta configuración posterior a la instalación mediante Sconfig. También puede usar herramientas como Windows Admin Center y la comunicación remota de PowerShell para completar estas tareas en Server Core.

Nota

Aunque puede habilitar Escritorio remoto en Server Core, solo habilita la conectividad RDP con la interfaz de la línea de comandos.

1.3. Servicios de dominio de Active Directory

Tal y como afirma Microsoft (2022), un AD DS y sus servicios relacionados forman la base de las redes empresariales que ejecutan los sistemas operativos Windows. La base de datos de AD DS es el almacén central de todos los objetos del dominio, como cuentas de usuario, cuentas de equipo y grupos. AD DS proporciona un directorio jerárquico en el que se pueden realizar búsquedas y un método para aplicar ajustes de configuración y seguridad a los objetos de una empresa.

¿Qué son los componentes lógicos?

AD DS incluye componentes lógicos y físicos. Debe comprender cómo funcionan conjuntamente los componentes de AD DS a fin de administrar la infraestructura de forma eficaz. Además, puede usar las opciones de AD DS para realizar acciones como las siguientes:

* Instalación, configuración y actualización de aplicaciones.
* Administración de la infraestructura de seguridad.
* Habilitación del servicio de acceso remoto y DirectAccess.
* Emisión y administración de certificados digitales.
* Los componentes lógicos de AD DS son estructuras que se usan para implementar un diseño de AD DS adecuado para una organización.

En la tabla siguiente se describen los tipos de componentes lógicos que contiene una base de datos de AD DS.

A list of information on a computer

Description automatically generated with medium confidence

Tabla 3. Componentes lógicos. Fuente: elaboración propia.

¿Qué son los componentes físicos?

AD DS incluye componentes lógicos y físicos. Debe comprender cómo funcionan conjuntamente.

A table with text on it

Description automatically generated

Tabla 4. Componentes físicos. Fuente: elaboración propia.

Definición de usuarios, grupos y equipos

Además de los componentes y objetos de alto nivel, AD DS contiene otros objetos como usuarios, grupos y equipos.

En AD DS, debe proporcionar una cuenta de usuario a todos los usuarios que requieran acceso a los recursos de red. Con esta cuenta de usuario, los usuarios pueden autenticarse en el dominio de AD DS y acceder a los recursos de red.

En Windows Server, una cuenta de usuario es un objeto que contiene toda la información que define a un usuario. Una cuenta de usuario incluye:

* El nombre de usuario.
* Una contraseña de usuario.
* Pertenencias a grupos.

Una cuenta de usuario también contiene parámetros que se pueden configurar en función de los requisitos de la organización.

El nombre de usuario y la contraseña de una cuenta de usuario sirven como credenciales de inicio de sesión del usuario. Un objeto de usuario también incluye otros atributos que describen y administran el usuario. Puede usar lo siguiente para crear y administrar objetos de usuario en AD DS:

* Centro de administración de Active Directory.
* Usuarios y equipos de Active Directory.
* Windows Admin Center.
* Windows PowerShell.
* La herramienta de línea de comandos dsadd.

Aunque podría ser práctico asignar permisos y derechos a cuentas de usuario individuales en redes pequeñas, esto se vuelve poco práctico e ineficiente en redes empresariales grandes.

Por ejemplo, si varios usuarios necesitan el mismo nivel de acceso a una carpeta, resulta más eficaz crear un grupo que contenga las cuentas de usuario necesarias y, a continuación, asignar los permisos necesarios al grupo.

Sugerencia

Como ventaja adicional, puede cambiar los permisos de archivo de los usuarios si los agrega o los quita de los grupos en lugar de editar los permisos de archivo directamente.

Tal y como afirma Panek W. (2019), antes de implementar grupos en su organización, debe comprender el ámbito de varios tipos de grupos de AD DS. Además, debe entender cómo usar los tipos de grupo para administrar el acceso a los recursos o para asignar derechos y responsabilidades de administración.

Los equipos, al igual que los usuarios, son entidades de seguridad, en este sentido:

Tienen una cuenta con un nombre de inicio de sesión y una contraseña que Windows cambia automáticamente de forma periódica.

Se autentican con el dominio.

Pueden pertenecer a grupos y tener acceso a los recursos, y puede configurarlos mediante una directiva de grupo.

Una cuenta de equipo comienza su ciclo de vida cuando crea el objeto de equipo y lo une a su dominio. Después de unir la cuenta de equipo a su dominio, las tareas administrativas cotidianas incluyen:

* Configuración de las propiedades del equipo.
* Traslado del equipo entre unidades organizativas.
* Administración del propio equipo.
* Cambio de nombre del objeto de equipo, así como su restablecimiento, deshabilitación, habilitación y finalmente eliminación.

Definición de usuarios, grupos y equipos

Un bosque de AD DS es una colección de uno o varios árboles de AD DS que contienen uno o varios dominios de AD DS. Dominios en un recurso compartido de bosque:

* Una raíz común.
* Un esquema común.
* Un catálogo global.

Un dominio de AD DS es un contenedor administrativo lógico para objetos como:

* Usuarios.
* Grupos.
* *Computers.*

Un bosque es un contenedor de nivel superior en AD DS. Cada bosque es una colección de uno o varios árboles de dominios que comparten un esquema de directorio común y un catálogo global. Un árbol de dominios es una colección de uno o varios dominios que comparten un espacio de nombres contiguo. El dominio raíz del bosque es el primer dominio que se crea en el bosque.

El dominio raíz del bosque contiene objetos que no existen en otros dominios del bosque. Dado que siempre se crean estos objetos en el primer controlador de dominio, un bosque puede estar formado por un solo dominio con un único controlador de dominio, o puede estar formado por varios dominios en varios árboles de dominio.

En el gráfico siguiente se muestra Contoso.com como dominio raíz del bosque. Debajo hay dos dominios, Adatum.com en un árbol independiente y Seattle.Contoso.com como un elemento secundario de Contoso.com.

A diagram of a company

Description automatically generated

Figura 2. Definición de bosques y dominios. Fuente: Microsoft, 2022.

Los siguientes objetos existen en el dominio raíz del bosque:

* El rol de maestro de esquema.
* El rol de maestro de nombres de dominio.
* El grupo de administradores de empresa.
* El grupo de administradores de esquema.

¿Qué es un dominio de AD DS?

Un dominio de AD DS es un contenedor lógico para administrar usuarios, equipos, grupos y otros objetos. La base de datos de AD DS almacena todos los objetos de dominio y cada controlador de dominio almacena una copia de la base de datos.

En el gráfico siguiente se muestra un dominio de AD DS. Contiene usuarios, equipos y grupos.

A diagram of a company's company

Description automatically generated

Figura 3. Dominios. Fuente: Microsoft, 2022.

Los objetos que se usan con más frecuencia se describen en la tabla siguiente:

A blue and white table with text

Description automatically generated

Tabla 5. Objetos directorio activo. Fuente: elaboración propia.

Nota

AD DS permite que un único dominio contenga casi 2000 millones de objetos. Esto significa que la mayoría de las organizaciones solo necesitan implementar un único dominio.

Un dominio de AD DS suele describirse como:

* Un límite de replicación. Al realizar cambios en cualquier objeto del dominio, el controlador de dominio en el que se produjo el cambio lo replica en todos los demás controladores de dominio del dominio. Si existen varios dominios en el bosque, solo se replican los subconjuntos de los cambios en otros dominios. AD DS usa un modelo de replicación de arquitectura multimaestro que permite a todos los controladores de dominio realizar cambios en los objetos del dominio.
* Una unidad administrativa. El dominio de AD DS contiene una cuenta de administrador y una cuenta de administradores de grupo. De forma predeterminada, la cuenta de administrador forma parte del grupo de administradores de dominio y el grupo de administradores de dominio forma parte de todos los grupos de administradores locales de los equipos unidos a un dominio. Además, de forma predeterminada, los miembros del grupo de administradores de dominio tienen control total sobre todos los objetos del dominio.

Nota

La cuenta de administrador del dominio raíz del bosque tiene derechos adicionales.

Un dominio de AD DS proporciona:

* Autenticación. Cada vez que se inicia un equipo unido a un dominio o un usuario inicia sesión en un equipo unido a un dominio AD DS lo autentica. La autenticación comprueba que el equipo o el usuario tiene la identidad adecuada en AD DS comprobando sus credenciales.
* Autorización. Windows usa tecnologías de autorización y control de acceso para determinar si los usuarios autenticados pueden tener acceso a los recursos.

Sugerencia

Las organizaciones con estructuras administrativas descentralizadas o con múltiples ubicaciones podrían considerar la implementación de múltiples dominios en el mismo bosque para acomodar sus necesidades administrativas.

A continuación, en la lección magistral *Instalación de un directorio activo* se profundiza y se muestra el proceso de configuración de un entorno de red corporativo con un directorio activo configurado y sus herramientas de trabajo habituales.

En el siguiente vídeo *Instalación y configuración de un Windows Server* vamos a realizar una instalación de un sistema operativo Windows Server. También realizaremos la instalación y configuración de un directorio activo y veremos los pasos iniciales de gestión.

1.4. Implementación objetos de directiva de grupo

Tal y como afirma Microsoft (2022), las primeras versiones de Windows Server, la característica directiva de grupo de los sistemas operativos Windows ha proporcionado una infraestructura con la que los administradores pueden definir la configuración de forma centralizada y, después, implementarla en los equipos de las organizaciones.

Por lo tanto, el personal de TI de las empresas puede definir, aplicar y actualizar toda su configuración mediante la configuración de los GPO. Al usar la configuración de los GPO, puede modificarse todo el sitio o un dominio de la organización, o bien limitar su enfoque a una sola unidad organizativa.

Sugerencia

El filtrado basado en los atributos de los equipos físicos y en la pertenencia a grupos de seguridad también permite a la empresa definir con más detalle el destino de su configuración de GPO.

¿Qué es una directiva de grupo?

Directiva de grupo es un marco de los sistemas operativos Windows con componentes que residen en AD DS, en controladores de dominio y en cada una de las instancias de servidor y cliente de Windows. Con estos componentes, puede administrar la configuración en un dominio de AD DS. Define la configuración de la directiva de grupo en un objeto de directiva de grupo (GPO).

Un GPO es un objeto que contiene una o más configuraciones de directiva que se aplican a una o varias opciones de configuración para un usuario o un equipo.

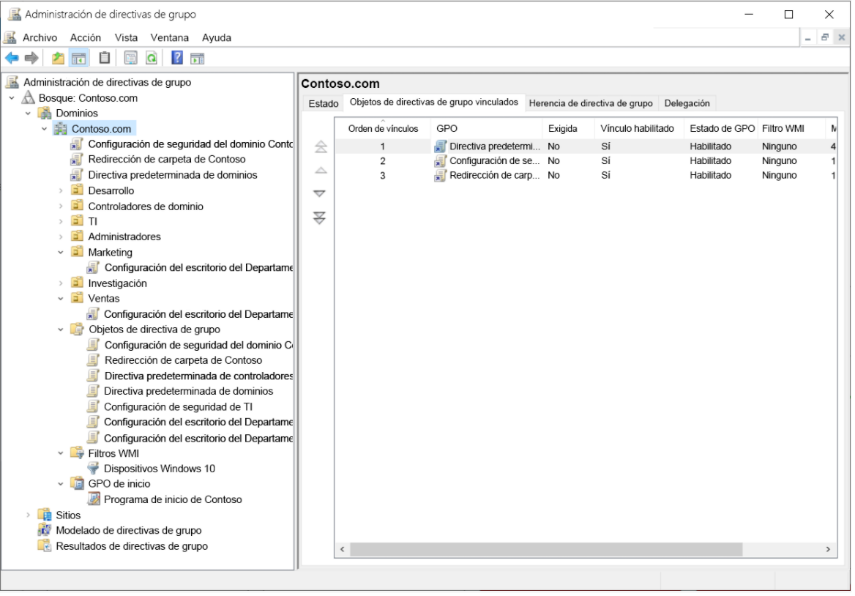


Figura 4. Directivas de grupo. Fuente: Microsoft, 2022.

Una directiva de grupo es una herramienta administrativa de gran eficacia. Los GPO se pueden usar para insertar diversas configuraciones en un gran número de usuarios y equipos. Dado que pueden aplicarse a distintos niveles, desde el equipo local a un dominio, las configuraciones también pueden enfocarse de forma precisa.

Una directiva de grupo se usa principalmente para configurar los valores que no quiere que configuren los usuarios. Además, puede usarla para estandarizar los entornos de escritorio en todos los equipos de una unidad organizativa (UO) o de toda una organización. También puede usar las directivas de grupo para proporcionar seguridad adicional, establecer algunas configuraciones avanzadas del sistema y para otros fines que se describen en una unidad de demostración posterior.

El componente más pormenorizado de una directiva de grupo es una configuración de directiva individual. Una configuración de directiva individual define una configuración específica, por ejemplo, una configuración de directiva que impide que un usuario acceda a las herramientas de edición del registro. Si define esa configuración de directiva y, a continuación, la aplica a un usuario, este no podrá ejecutar herramientas como Regedit.exe.

Algunas configuraciones afectan a un usuario, lo que se conoce como parámetros de configuración de usuario o directivas de usuario y otras afectan al equipo, lo que se conoce como parámetros de configuración del equipo o directivas de equipo.

Importante

La configuración no afecta a los grupos directamente y solo se aplica a los objetos de usuario y de equipo.

Una directiva de grupo administra varias configuraciones de directiva y su marco es extensible. Con las directivas de grupo puede administrar prácticamente todos los valores configurables.

Para definir una configuración de directiva:

* En el Editor de administración de directivas de grupo, busque la configuración de la directiva y, a continuación, seleccione Entrar. Se abre el cuadro de diálogo Propiedades de la configuración de directiva.
* Cambie el estado de la directiva a Habilitada o Deshabilitada. La mayoría de las configuraciones de directiva pueden tener tres estados: No configurada, Habilitada y Deshabilitada.
* Si es necesario, configure los valores adicionales y, cuando haya finalizado, seleccione Aceptar.

Los GPO almacenan la configuración de la directiva de grupo. En un GPO nuevo, el valor predeterminado de una configuración de directiva es No configurada. Al habilitar o deshabilitar una configuración de directiva, Windows Server modifica la configuración de los usuarios y los equipos a los que se aplica el GPO.

Nota

Al devolver una configuración al valor No configurada, esta se devuelve a su valor predeterminado.

Para crear un GPO en un dominio:

1. En Administración de directivas de grupo, haga clic con el botón derecho o acceda al menú contextual del contenedor Objetos de directiva de grupo y, a continuación, seleccione Nuevo.
2. Para modificar los valores de configuración de un GPO, haga clic con el botón derecho o acceda al menú contextual del GPO y, a continuación, seleccione Editar. Al hacerlo, se abre el complemento Editor de administración de directivas de grupo.

El Editor de administración de directivas de grupo muestra todas las configuraciones de directiva disponibles en un GPO en una jerarquía organizada, que comienza con la división entre la configuración del equipo y la configuración de usuario: el nodo Configuración del equipo y el nodo Configuración de usuario.

Los GPO se muestran en un contenedor denominado Objetos de directiva de grupo. Los dos niveles siguientes de la jerarquía son los nodos denominados Directivas y Preferencias. Al avanzar por la jerarquía, vemos que el Editor de administración de directivas de grupo muestra distintas carpetas, llamadas nodos o grupos de configuración de directivas. Las configuraciones de directiva se encuentran en las carpetas.

1.5. Servidor web, servidor de archivos y monitorización

¿Qué es un servidor web IIS?

Afirma Microsoft (2022) que las iniciales de Internet Information Services, aunque es más conocido como servidor web, en realidad son conjuntos de servicios que transforman un sistema Microsoft Windows en un servidor capaz de ofrecer servicios Web, FTP.

Por muchos años IIS fue un CD-ROM separado del Sistema Operativo denominado Option Pack, recién con Windows 2000 se incorporó al instalador del sistema como un paquete más instalable variando las limitaciones dependiendo de la versión de Windows.

Desde 2016 es un servidor que ha venido en crecimiento. Las estadísticas de Netcraft lo ubican como el servidor más utilizado como servidor web con cerca de 688 millones de instalaciones seguidos por Nginx con 358 millones y Apache con 313 millones.

Sin embargo, a la hora de ver la cuota total de sitios web activos en internet los números cambian y tanto Apache como Nginx superan a IIS como servidor en sitios web más activos donde cae al 10% de los sitios.

Es apto tanto como servidor web en Internet y en Intranet, siendo en Intranet o en servidores privados donde tiene mayor cuota debido al mercado empresarial que lo utilizan para aplicaciones internas en empresas de mediana y gran escala, ya que va de la mano de Visual Studio.NET muy arraigado en el sector privado empresarial.

¿Cómo maneja las peticiones el servidor IIS?

A diferencia de Apache y Nginx que dividen la carga de trabajo en diversos subprocesos, dependiendo de la configuración incluso un subproceso por cada petición, IIS opta por el modelo de proceso único, es decir que un solo proceso maneja todas las peticiones.

También, cabe decir que para determinadas operaciones especiales se delegan a subprocesos, es decir que el proceso principal hace uso de subproceso sin embargo solo delega una parte de la responsabilidad porque es siempre el proceso principal quien recibe y responde la petición.

Una de las ventajas más importantes de IIS es el manejo de las peticiones y como estas pueden ser atendidas de manera concurrente, sobre todo por la alta necesidad que tienen las aplicaciones de realizar peticiones al servidor para enviar y recibir datos, así mismo como importantes mejoras en la entrada y salida asíncrona de datos que permiten aumentar la performance de la aplicación.

Requisitos mínimos de IIS

Los requisitos de hardware mínimos son relativamente bajos, sin embargo, hay que entender que estos requisitos son para instalar e iniciar los servicios únicamente. A la hora de utilizarlo en un servidor en producción la potencia del procesador y la cantidad de memoria depende de la cantidad de tráfico, de la cantidad de usuarios y la carga de trabajo que se espera.

Para la versión de Windows Server en cuestión del procesador el requisito mínimo es un CPU de 1,4 Ghz, algo que cumple la mayoría de los CPU modernos, luego el rendimiento aumenta al aumentar la cantidad de MHz y núcleos de CPU.

Mínimo:

* Procesador de 64 bits a 1,4 GHz.
* Compatible con el conjunto de instrucciones x64.
* Admite DEP y NX.
* Admite CMPXCHG16b, LAHF/SAHF y PrefetchW.
* Admite la traducción de direcciones de segundo nivel (EPT o NPT).

En lo referido a memoria si el servidor es instalado sin escritorio, es decir solo consola, la cantidad de memoria mínima requerida son 512MB mientras que con el escritorio el mínimo sube a 2GB mínimo. Obviamente, para un servidor que soporte clientes la cantidad de memoria debe ser incrementada de acuerdo con el tráfico, peticiones, usuarios y carga de trabajo esperadas.

Mínimo:

* 512 MB (2 GB para la opción de instalación Servidor con Experiencia de escritorio)
* Tipo ECC (código de corrección de errores) o tecnología similar.

Características del Servidor Internet Information Services

La arquitectura de IIS es modular para permitir una gestión ordenada y la posibilidad de agregar funciones adicionales, brinda soporte para los varios protocolos: HTTP/HTTPS, FTP/FTPS, SMTP y NNTP, provee soporte SSL para Socket Layer y, adicionalmente, provee múltiples alternativas de autentificación como Kerberos entre otros.

Nativamente, el lenguaje dinámico soportado es ASP.NET, sin embargo, también es posible configurar para utilizar PHP, VBScript, Perl e incluso Java (Java Server Pages y Servlets) y prácticamente cualquier lenguaje como módulo adicional o a través de la interface CGI.

Además de los módulos para soportar lenguajes de programación y scripting IIS, está formado por otros módulos como pueden ser:

* Módulos de seguridad: se utilizan para agregar capas de seguridad a las peticiones y proteger los datos. Un ejemplo claro son los métodos de autentificación que luego pueden ser implementados en las aplicaciones para la validación de usuarios y sesiones.
* Módulos de contenido: se utilizan para la generación y envío de contenido al usuario, como pueden ser archivos estáticos o dinámico generados por aplicaciones .NET, PHP, PERL o CGI.
* Módulos de compresión: son módulos que permiten la compresión de contenido. Existen dos módulos, uno para contenido dinámico y otro para contenido estático.
* Módulos de almacenamiento caché: brinda soporte para caché de datos en memoria con el fin de mejorar el rendimiento de las aplicaciones reduciendo el tiempo y la latencia en tiempo de respuesta sobre todo en aplicaciones de alto tráfico.
* Módulos de registro y diagnóstico: es un módulo que provee diferentes herramientas como por ejemplo de registro, que permite registro de actividad web como las peticiones. A su vez, también provee un monitor de solicitudes para supervisar el funcionamiento del servidor web y de las aplicaciones.

Instalación de Servidor IIS

Para instalar Internet Information Server en Windows Server se debe primero abrir el panel de Administración del Servidor y hacer clic en Agregar roles y características, tal como aparece en la imagen:

A screenshot of a computer

Description automatically generated

Figura 5. Instalación Internet Information Services. Fuente: elaboración propia.

¿Qué es un sistema de archivos?

Antes de que pueda almacenar datos en un volumen, primero debe formatearlo. Para ello, debe seleccionar el sistema de archivos que el volumen deberá usar. Hay varios sistemas de archivos disponibles, cada uno con ventajas y desventajas.

Un sistema de archivos ofrece una variedad de características que implementan el almacenamiento y recuperación de archivos en los dispositivos de almacenamiento. Permite organizar los archivos en una estructura jerárquica y controla tanto el formato como la convención de nomenclatura de estos. Los sistemas de archivos admiten una amplia gama de dispositivos de almacenamiento, incluidos los discos duros y los medios extraíbles.

Todos los sistemas de archivos disponibles en el sistema operativo Windows constan de los siguientes componentes de almacenamiento:

* Archivos. Son una agrupación lógica de datos relacionados.
* Directorios. Son una colección jerárquica de directorios y archivos.
* Volúmenes. Son una colección de directorios y archivos.

¿Cuáles son las características distintivas de los tipos de sistemas de archivos de Windows Server?

Algunos de los tipos de sistema de archivos de Windows Server son:

* Tabla de asignación de archivos (FAT), FAT32 y tabla de asignación de archivos extendida (exFAT).
* Sistema de archivos NT (NTFS).
* Sistema de archivos resistente (ReFS).

El sistema de archivos FAT es el más sencillo disponible en la compatibilidad con sistemas operativos Windows. Realiza un seguimiento de los objetos del sistema de archivos mediante una tabla de nivel del volumen. FAT conserva dos copias de la tabla para ofrecer resistencia. Tanto las dos tablas como el directorio raíz deben residir en una ubicación fija del disco con formato.

Debido a la limitación de tamaño de la tabla de asignación de archivos, no puede usar FAT para crear volúmenes mayores de 4 gigabytes (GB). Para alojar discos de mayor tamaño, Microsoft desarrolló FAT32,que admite particiones de hasta 64 GB.

exFAT es el sistema de archivos diseñado para las unidades flash USB, que incluye compatibilidad para volúmenes de tamaños mayores que los disponibles con FAT32. Funciona con los dispositivos multimedia, como TV de pantalla plana modernos, centros y reproductores multimedia portátiles.

Ni FAT, ni FAT32 ofrecen seguridad en el nivel de sistema de archivos. No debe crear volúmenes FAT o FAT32 en los discos conectados a los servidores que ejecuten cualquiera de los sistemas operativos Windows Server. Sin embargo, puede plantearse el uso de FAT, FAT32 o exFAT para dar formato a los medios externos, como las unidades flash USB.

Sugerencia

A partir de Windows Server 2016, FAT y FAT32 admiten el cifrado a través del Sistema de cifrado de archivos (EFS).

NTFS

Tradicionalmente, NTFS ha sido la opción de sistema de archivos más común para los sistemas operativos Windows Server. NTFS ofrece muchas mejoras con respecto a FAT, que aprovechan las estructuras de datos avanzadas para mejorar el rendimiento, la confiabilidad y el uso del espacio en disco. NTFS también ofrece seguridad integrada, con funciones de control de acceso como las listas de control de acceso (ACL), la auditoría, el registro en diario del sistema de archivos y el cifrado. NTFS también admite la compresión y el cifrado del sistema de archivos, aunque son mutuamente excluyentes. Por ello, no se pueden aplicar en el mismo archivo o carpeta.

Nota

NTFS es necesario cuando se implementan volúmenes en servidores que hospedan varios roles y características de Windows Server, como Active Directory Domain Services (AD DS), VSS y el Sistema de archivos distribuido (DFS).

ReFS

Microsoft lanzó ReFS en Windows Server 2012 para mejorar las capacidades de NTFS. Uno de los principales puntos fuertes de ReFS, como se indica en su nombre, es su resistencia mejorada a los datos dañados gracias a un mecanismo de detección más preciso y a una funcionalidad para corregir los problemas de integridad en línea. ReFS también ofrece compatibilidad con tamaños mayores de archivos y volúmenes individuales, incluida la de duplicación.

En la mayoría de los casos, ReFS es la opción de sistema de archivos óptima para los volúmenes de datos en Windows Server 2022. Sin embargo, debe tener en cuenta que ReFS no ofrece una paridad de características completa con NTFS. Por ejemplo, ReFS no admite la compresión y el cifrado en el nivel de archivo. Tampoco es la opción adecuada para los volúmenes de arranque y los medios extraíbles.

La instalación del servidor de ficheros la realizaremos como el resto de los roles desde el administrador de servidor, agregando el rol de archivos que podemos ver en la figura siguiente:

A screenshot of a computer

Description automatically generated

Figura 6. Instalación del rol servidor de archivos. Fuente: elaboración propia.

Monitorización

En el pasado, la administración del entorno de TI suponía la utilización de distintas herramientas en varias consolas. Windows Admin Center combina esas herramientas en una única consola que se puede implementar fácilmente y con acceso sencillo a través de una interfaz web.

Desde esta consola de administración es ahora mucho más fácil la monitorización de toda la plataforma Windows de los entornos corporativos.

Windows Admin Center es una aplicación web modular formada por los cuatro módulos siguientes:

* Administrador del servidor.
* Clústeres de conmutación por error.
* Clústeres hiperconvergidos.
* Clientes de Windows 10.

A screenshot of a computer

Description automatically generated

Figura 7. Consola de administración y monitorización: Windows Admin Center. Fuente: elaboración propia.

1.6. Infraestructura de red de Windows server

DHCP

Microsoft (2022) nos enseña que este servicio configura automáticamente los dispositivos de red con la información de configuración de dirección IP. Esto puede ayudar al personal de soporte técnico de TI de la empresa al simplificar y centralizar la asignación de las configuraciones de dirección IP. Si la empresa decide no usar DHCP, cada vez que agregue un cliente a su red deberá configurar su interfaz de red con información sobre la red a la que se va a conectar.

Sugerencia

La información que debe configurar incluye la dirección IP, la máscara de subred de la red, la configuración de DNS de cliente para la resolución de nombres y la puerta de enlace predeterminada para el acceso a otras redes.

Ventajas de DHCP

La principal ventaja de utilizar DHCP es reducir el mantenimiento necesario para configurar la información de dirección IP en los dispositivos de red. Muchas organizaciones administran miles de dispositivos informáticos, como impresoras, escáneres, *smartphones,* equipos de escritorio y portátiles. Por este motivo, no es práctico administrar manualmente las configuraciones de dirección IP de red para organizaciones de este tamaño.

Como DHCP es un proceso automatizado, es más preciso que configurar manualmente la información de dirección IP. Esto resulta especialmente importante para los usuarios que no conocen ni entienden el proceso de configuración.

DHCP facilita la actualización de la información de configuración de la dirección IP. Como administrador, cuando hace un cambio en el servicio de red, como proporcionar un servidor nuevo de sistema de nombres de dominio (DNS), solo realiza una actualización única en los servidores DHCP y ese cambio lo reciben todos los clientes de DHCP. Por ejemplo, un usuario móvil con un equipo portátil que usa DHCP obtiene automáticamente la información nueva de configuración de la dirección IP cuando se conecta a una red nueva.

Nota

De manera predeterminada, todos los sistemas operativos Windows recuperan automáticamente una dirección IP después de la instalación inicial del sistema operativo (SO).

Funcionamiento de DHCP

El servicio cliente DHCP se ejecuta en todos los equipos con Windows que tienen propiedades TCP/IPconfiguradas para obtener una dirección IP automáticamente. El cliente DHCP se comunica con un servidor DHCP para obtener la información de configuración de dirección IP. Los clientes pueden usar la dirección DHCP asignada durante un período determinado, lo que se conoce como tiempo de la concesión. El servidor DHCP está configurado con un grupo de direcciones y opciones de configuración. Esta información determina qué información de configuración de dirección IP se entrega a los clientes. En el gráfico siguiente se presenta el proceso de comunicación de cuatro pasos.

A diagram of a diagram

Description automatically generated

Figura 8. Proceso de comunicación DHCP. Fuente: Microsoft, 2022.

La comunicación para la generación de concesiones DHCP usa difusiones de dirección IP. Como las difusiones de dirección IP no se enrutan, debe configurar un servidor DHCP en cada subred o configurar una retransmisión DHCP. Muchos enrutadores incluyen la funcionalidad de retransmisión DHCP.

Los cuatro pasos de la generación de concesiones son los siguientes:

1. El cliente DHCP difunde un paquete DHCPDISCOVER. Los únicos equipos que responden son los que tienen el rol del servidor DHCP o los equipos o enrutadores que ejecutan un agente de retransmisión DHCP. En el último caso, el agente de retransmisión DHCP reenvía el mensaje al servidor DHCP que configuró para retransmitir las solicitudes.
2. Un servidor DHCP responde con un paquete DHCPOFFER, que contiene una dirección potencial para el cliente. Si varios servidores DHCP reciben el paquete DHCPDISCOVER, pueden responder varios servidores DHCP.
3. El cliente recibe el paquete DHCPOFFER. Si el cliente recibe varios paquetes DHCPOFFER, selecciona la primera respuesta. Después, el cliente envía un paquete DHCPREQUEST que contiene un identificador de servidor. Esto informa a los servidores DHCP que reciben la difusión del paquete DHCPOFFER del servidor que el cliente eligió aceptar.
4. Los servidores DHCP reciben el paquete DHCPREQUEST. Los servidores que el cliente no aceptó usan este mensaje como notificación de que el cliente rechazó la oferta del servidor. El servidor elegido almacena la información del cliente de la dirección IP en la base de datos DHCP y responde con un mensaje DHCPACK. Si el servidor DHCP no puede proporcionar la dirección ofrecida en el DHCPOFFER inicial, el servidor DHCP envía un mensaje DHCPNAK.

Renovación de la concesión de DHCP

Cuando la concesión de DHCP alcanza el cincuenta por ciento del tiempo de la concesión, el cliente intenta renovar la concesión automáticamente. Este proceso se realiza en segundo plano. Es posible que un equipo tenga la misma dirección IP asignada por DHCP durante mucho tiempo. Esto se debe a que el equipo renueva la concesión varias veces.

Para intentar renovar la concesión de la dirección IP, el cliente envía un mensaje DHCPREQUEST de unidifusión. El servidor que concedió originalmente la dirección IP envía un mensaje DHCPACK de vuelta al cliente. Este mensaje contiene los parámetros nuevos que cambiaron desde que se creó la concesión original. Tenga en cuenta que estos paquetes no se difundirán porque, en este momento, el cliente tiene una dirección IP que puede usar para las comunicaciones de unidifusión.

Nota

Al actualizar las opciones de configuración de DHCP, es posible que los clientes no obtengan las opciones actualizadas hasta que se complete el cincuenta por ciento del tiempo de la concesión. Por ejemplo, si configura un tiempo de la concesión de seis días, es posible que los clientes no obtengan las opciones actualizadas durante tres días.

Si el cliente DHCP no puede ponerse en contacto con el servidor DHCP, el cliente espera hasta que expire el 87,5 por ciento del tiempo de la concesión. En este momento, el cliente envía una difusión DHCPREQUEST (en lugar de una unidifusión) para obtener una renovación y la solicitud va a todos los servidores DHCP, y no solo al servidor que proporcionó la concesión original. Sin embargo, esta solicitud de difusión es para una renovación, no para una concesión nueva.

Como los equipos cliente pueden moverse mientras están apagados (por ejemplo, un equipo portátil conectado a una subred nueva), también intentan realizar la renovación durante el proceso de inicio o cuando el equipo detecta un cambio de la red. Si la renovación se realiza correctamente, se restablece el período de la concesión.

Versión 6 de DHCP

La versión 6 de DHCP (DHCPv6) admite configuraciones con estado y sin estado para configurar clientes en un entorno IPv6. La configuración con estado ocurre cuando el servidor DHCPv6 asigna la dirección IPv6 al cliente, junto con datos DHCP adicionales. La configuración sin estado ocurre cuando el enrutador asigna la dirección IPv6 automáticamente y el servidor DHCPv6 solo asigna otras opciones de configuración de IPv6.

¿Qué es DNS?

DNS es un servicio de resolución de nombres estándar del sector. Los servidores que ejecutan el rol de servidor DNS responden a las solicitudes de los hosts y otros dispositivos de red para resolver nombres de equipo y nombres de host en direcciones IP. Los servidores DNS también pueden resolver direcciones IP en nombres. Los servidores DNS usan registros de recursos DNS almacenados en zonas DNS. Si un servidor DNS no puede resolver una consulta para un dispositivo de red, podría hacer referencia a otros servidores DNS mediante sugerencias de raíz o reenvíos.

Nota

El formato exacto de la zona depende del tipo de la zona.

Puede crear registros de recursos DNS manualmente, o bien los hosts IP y los dispositivos de red pueden realizar registros DNS automáticamente con un servidor DNS.

El uso más común de DNS consiste en resolver nombres de dominio completos (FQDN), como sea-dc1.contoso.com, en direcciones IP. Los usuarios requieren esta funcionalidad para acceder a recursos de red y sitios web.

Los administradores usan la resolución de nombres en DNS cuando configuran y administran aplicaciones, en parte porque los usuarios pueden recordar los nombres con mayor facilidad que las direcciones IP. Los servidores y clientes Windows unidos a un dominio también usan DNS para buscar controladores de dominio en un dominio de AD DS.

Nombres de dominio DNS

La estructura de nomenclatura que usa DNS es el espacio de nombres DNS. Es jerárquico; es decir que se inicia con un dominio raíz. Ese dominio raíz puede tener cualquier número de subdominios. A su vez, cada subdominio puede tener cualquier número de subdominios propios.

Los nombres de dominio pueden ser públicos (accesibles desde Internet) o privados. Si son privados, decida cómo definirá el espacio de nombres de su organización. Si son públicos, debe trabajar con la Corporación de Internet para la Asignación de Nombres y Números (ICANN) u otras autoridades de registro de nombres de Internet que puedan delegar (vender) nombres únicos. A partir de estos nombres, podrá crear los nombres de subdominio correspondientes.

Sugerencia

Para facilitar la obtención de certificados de confianza para las aplicaciones y la autenticación, se suele usar un nombre de dominio público que esté registrado en Internet.

Servidores DNS

Un servidor DNS responde a las solicitudes de registros DNS que realizan los solucionadores de DNS. Por ejemplo, un cliente de Windows 10 puede enviar una solicitud DNS para resolver sea-dc1.contoso.com a un servidor DNS, y la respuesta del servidor DNS incluye la dirección IP de sea-dc1.contoso.com.

Un servidor DNS recupera esta información desde una base de datos local que contiene registros de recursos. Si el servidor DNS no tiene la información solicitada, también puede reenviar las solicitudes DNS a otro servidor DNS. Un servidor DNS también almacena en caché la información solicitada previamente de otros servidores DNS.

Aunque puede configurar cualquier servidor de Windows como un servidor DNS, también es habitual instalar el rol del servidor DNS en cualquier equipo de Windows Server que se haya promovido a un controlador de dominio de AD DS.

Nota

Windows Server está configurado para ser un servidor DNS cuando se instala el rol del servidor DNS.

Registros de recursos y zonas DNS

Cuando un servidor DNS es responsable de resolver las solicitudes de un espacio de nombres específico, se crea una zona en el servidor DNS que corresponde a dicho espacio de nombres. Por ejemplo, si un servidor DNS es responsable de contoso.com, se crearía una zona contoso.com. Dentro de la zona, se crean registros de recursos que contienen la información que usará para responder a las consultas.

Solucionadores de DNS

Un solucionador de DNS es un cliente, como un cliente de Windows, que necesita resolver registros DNS. En Windows, el servicio de cliente DNS envía las solicitudes DNS al servidor DNS que está configurado en las propiedades de IP. Después de recibir respuesta a una solicitud de DNS, Windows almacena en caché la respuesta para uso futuro. Esta es la memoria caché del solucionador de DNS.

Nota

El equipo con Windows 10 comprueba la memoria caché de DNS antes de enviar solicitudes al servidor DNS en caso de que haya resuelto recientemente el registro necesario.

A diagram of a server

Description automatically generated

Figura 9. Cliente DNS. Fuente: Microsoft, 2022.

Sugerencia

Puede acceder al contenido de la memoria caché del solucionador de DNS mediante el cmdlet Get-DnsClientCache o la ejecución del comando ipconfig /displaydns. Puede borrar al contenido de la memoria caché del solucionador de DNS mediante el cmdlet Clear-DnsClientCache o el comando ipconfig /flushdns.

Es importante mencionar que el DNS no es la única manera en que los equipos host que ejecutan Windows pueden resolver nombres. Un equipo con Windows 10 puede usar los métodos siguientes según la configuración:

* Comprobar la memoria caché del solucionador de DNS.
* Comprobar el archivo Hosts que se encuentra en C:\Windows\System32\Drivers\etc.
* Enviar una solicitud al servidor DNS configurado.
* Transmitir una consulta de nombre NETBIOS.
* Comprobar el archivo LMHOSTS que se encuentra en C:\Windows\System32\Drivers\etc.
* Usar un servicio de resolución de nombres NETBIOS configurado, como el Servicio de nombres de Internet de Windows (WINS).

Sugerencia

Puede instalar la característica de servidor WINS en Windows Server si su organización requiere la resolución de nombres NETBIOS para admitir una aplicación específica.

Nombres de equipo y nombres de host

Un nombre de host es un nombre descriptivo que está asociado a la dirección IP de un host y lo identifica como un host TCP/IP. Un nombre de host no puede superar los 255 caracteres y solo debe contener caracteres alfanuméricos, puntos y guiones. Un nombre de host es un alias o un nombre de dominio completo. Los elementos del nombre usan puntos como separadores. Las aplicaciones usan el nombre de dominio completo estructurado en Internet. payroll.contoso.com es un ejemplo de nombre de dominio completo.

Un nombre NETBIOS es un nombre no jerárquico que usan algunas aplicaciones antiguas. Un nombre NETBIOS de dieciséis caracteres identifica al recurso NETBIOS de una red. Dicho nombre representa un único equipo o un grupo de equipos. NETBIOS usa los quince primeros caracteres para el nombre de un equipo específico y el decimosexto y último carácter para identificar un recurso o servicio de ese equipo. Un ejemplo de nombre NETBIOS es SEA-SVR2.

1.7. Seguridad en redes Windows

Tal y como afirma Panek W. (2019), hay que instalar parches de seguridad y realizar actualizaciones cada cierto tiempo.

Normalmente, las vulnerabilidades o agujeros en la seguridad conocidos se vuelven a cerrar en un corto período de tiempo gracias a las actualizaciones. Sin embargo, para garantizar la efectividad de estas, es importante que esté al corriente de los parches de seguridad y las actualizaciones necesarias y las instale lo antes posible. Asegúrese de que se instalan también parches de seguridad y actualizaciones para sus complementos o plug-in. Puede establecer que las actualizaciones se instalen automáticamente en la configuración de Windows Update.

Nota

Si quiere, puede probar (previamente a la instalación en el servidor) los parches de seguridad y las actualizaciones de seguridad para sus aplicaciones y complementos y, así, ver los posibles efectos en su entorno. Tenga en cuenta que para dicha comprobación necesita un segundo servidor.

Utilice siempre contraseñas seguras

Las contraseñas débiles facilitan a los posibles atacantes el acceso a su servidor. En caso de ataque, el atacante podría usar su servidor para actividades maliciosas, usar los recursos de su servidor o, posiblemente, tomar el control del servidor y bloquearlo. Por eso le recomendamos utilizar siempre contraseñas seguras y complejas y cambiarlas regularmente.

* Tenga en cuenta los siguientes criterios para crear una contraseña sólida y segura:
* Utilice una contraseña distinta para cada servidor y para cada base de datos que se ejecute en el servidor.
* Utilice una contraseña que no esté en los diccionarios.
* Utilice siempre una contraseña que difiera significativamente de las contraseñas anteriores.
* No utilice ningún dato de su entorno personal, como cumpleaños, nombres, etc.
* No utilice una contraseña que contenga el nombre de usuario o el nombre de la empresa.
* No comparta su contraseña con terceros.
* Combine diferentes tipos de caracteres, como letras, números y caracteres especiales.

Una contraseña segura contiene:

* Al menos ocho caracteres.
* Letras mayúsculas y minúsculas: a-z, A-Z.
* Números: 0-9.
* Caracteres especiales.

Restrinja el acceso al servidor

El acceso al sistema solo debería concederse a los usuarios que trabajen activamente en él.

Establezca una rutina para las copias de seguridad

La pérdida de datos puede provocar daños graves y costosos. Por esta razón, le recomendamos establecer lo antes posible una rutina adecuada para realizar copias de seguridad.

Algunos de los factores que debe tener en cuenta son, por ejemplo:

* Determinar la situación de riesgo: depende de la finalidad del servidor y de su dependencia con respecto a la base de datos.
* Clasificar los datos: ¿qué tipo de datos se quieren almacenar? ¿Quiere realizar una copia de seguridad de los datos relevantes para el sistema o de los datos personales?
* Disponer de datos: ¿qué aplicaciones dependen de los datos y en qué forma? ¿Pueden funcionar las aplicaciones también sin los datos que quiere almacenar?

Además, debe considerar las siguientes cuestiones antes de establecer una rutina:

* ¿Qué pérdida de datos es aceptable?
* ¿Cuánto tiempo se tardaría en restaurar los datos?
* ¿Qué importancia tiene el volumen de datos y cómo evolucionará el volumen de datos?
* ¿Cómo se debe hacer una copia de seguridad de los datos?
* ¿Existen plazos para la eliminación y el almacenamiento de datos?
* ¿Son confidenciales los datos? ¿Es necesaria una protección especial para acceder a estos? ¿Existen requisitos legales?
* ¿Cuándo se puede crear la copia de seguridad sin perjudicar a otros procesos?
* ¿Cuánto tiempo debe almacenar las copias de seguridad?

Otro punto importante que debe considerar al establecer su rutina es el tipo de copia de seguridad que quiere realizar. Se hace una distinción básica entre los siguientes tipos de copias de seguridad:

* Copia de seguridad completa: una copia de seguridad completa contiene todos los datos seleccionados para la copia de seguridad.
* Copia de seguridad diferencial: una copia de seguridad diferencial realiza una copia de seguridad de todos los archivos que han sido modificados o añadidos desde la última copia de seguridad completa. Los cambios se realizan siempre en relación con la copia de seguridad completa. Las copias de seguridad diferenciales aumentan día a día hasta que se vuelve a realizar una copia de seguridad completa. Sin embargo, requieren menos espacio en disco que una copia de seguridad completa y pueden realizarse más rápido.

Para recuperar datos de una copia de seguridad diferencial, también debe tener acceso a la última copia de seguridad completa. Cada copia de seguridad diferencial se puede modificar independientemente del resto.

Copia de seguridad incremental: las copias de seguridad incrementales ahorran mucho espacio y se pueden realizar rápidamente.

Con una copia de seguridad incremental, solo se realiza una copia de seguridad de los datos que se han creado o modificado desde la última copia de seguridad. No importa si se trata de una copia de seguridad completa o incremental.

Por lo tanto, para restaurar una copia de seguridad incremental, usted también debe tener acceso a otras copias de seguridad realizadas previamente, ya que las copias de seguridad son interdependientes. Si elimina una de las copias de seguridad incrementales anteriores o una copia de seguridad completa, no podrá restaurar todo el paquete.

Además de desarrollar una rutina adecuada para las copias de seguridad y de crear copias de seguridad con regularidad, también debe asegurarse de comprobar con regularidad si las copias de seguridad se pueden recuperar.

Refuerce sus aplicaciones

Dependiendo de la aplicación instalada, existen diferentes riesgos y amenazas. Para protegerse contra estos riesgos, debe reforzar sus aplicaciones. A continuación, hemos recopilado algunos consejos:

* Consulte la documentación pertinente o visite el sitio web del fabricante si necesita obtener más información sobre cómo instalar e implementar una aplicación de forma segura.
* Lea y siga las mejores prácticas para instalar cada aplicación.
* Realice una búsqueda de vulnerabilidades conocidas en su aplicación. Puede consultar la lista de información registrada sobre vulnerabilidades de seguridad conocidas, también conocida como Vulnerabilidades y exposiciones comunes (CVE®), para obtener más información. Aquí le dejamos el enlace a la página principal de CVE®.
* Compruebe las vulnerabilidades de su servidor utilizando un programa como Nmap.
* Realice una prueba de penetración para identificar otras vulnerabilidades.
* Instale solo aplicaciones necesarias.
* Instale solo las aplicaciones que realmente necesite. Cuantas más aplicaciones instale en el servidor, mayor será el riesgo de vulnerabilidades.

Nota

Intente instalar aplicaciones solo de fuentes oficiales. Las aplicaciones de fuentes no oficiales pueden contener malware o virus.

Deshabilite o desinstale los servicios que no necesite

Dependiendo del sistema operativo utilizado y del tipo de instalación, también se descargan e instalan diferentes programas y servicios adicionales que, a menudo, no son necesarios. Por eso es importante que los identifique y los deshabilite desactivando las directrices del sistema correspondientes.

Abra solo los puertos que realmente necesite

Los puertos abiertos rara vez suponen un riesgo para la seguridad. Si reduce el número de aplicaciones de terceros, el número de puertos necesarios disminuirá y será más manejable. Estos puertos abiertos solo se convierten en un riesgo si los programas conectados o de terceros tienen vulnerabilidades de seguridad y los atacantes se aprovechan de ello. Este riesgo aumenta cuando el número de aplicaciones que instala en el servidor es mayor.

Monitoree su servidor

La monitorización es una herramienta importante para aumentar la seguridad de su servidor. Solo así se puede detectar a tiempo un fallo en el servidor o un fallo en los componentes o aplicaciones individuales. Esto también se aplica a ciertos tipos de ataques informáticos. Cuando le atacan, una respuesta rápida es esencial para detener el ataque y minimizar el daño causado.

Además, le recomendamos que compruebe regularmente las entradas del registro de seguridad de su servidor.

Compruebe regularmente si hay malware en su servidor

El malware, el ransomware o programa de software malicioso y los virus pueden causar daños considerables en su equipo. Asegúrese de tener instalados y activos un software antivirus y antispyware. Actualice regularmente sus firmas de antivirus y antimalware. Asegúrese también de que el software antivirus esté siempre activo y supervisando el tráfico de datos. Igualmente, le recomendamos realizar regularmente un análisis completo de los discos duros o unidades SSD.

Configure la política para bloquear las cuentas en uso durante los ataques

Esta configuración le permite defenderse contra ataques de fuerza bruta. En los ataques de fuerza bruta, los ciberdelincuentes intentan adivinar las contraseñas de una o más cuentas de usuario probando automáticamente diferentes combinaciones de letras y números. Cuantas más combinaciones se prueben, mayores serán las posibilidades de éxito del ataque.

Después del bloqueo, no se podrá acceder a las cuentas afectadas durante un cierto período de tiempo.

A screenshot of a computer

Description automatically generated

Figura 10. Opciones de seguridad en directiva de seguridad. Fuente: elaboración propia.

Use la herramienta Attack Surface Analyzer

Microsoft ha desarrollado una herramienta de software gratuita (Attack Surface Analyzer) que le permite analizar la superficie de ataque en busca de vulnerabilidades de seguridad. Este software muestra los cambios que se han producido en el sistema operativo después de instalar un nuevo software.

Puedes utilizar esta o cualquier otra herramienta de seguridad disponible para Windows. Revisar la sección «A fondo» para más información.

En este segundo vídeo, *Gestión de un directorio activo,* vamos a gestionar usuarios y máquinas de una red Windows Server y aprenderemos también a instalar roles y características nuevas dentro de nuestra red como pueda ser el servicio DHCP.

1.8. Entornos híbridos

Hoy en día la instalación de Windows server en los centros de datos no corresponden a una instalación aislada. La demanda de integración con las nubes públicas provoca que la mayoría de las redes actuales se denominen redes hibridas, con una parte en los centros de datos locales y una conexión con la nube pública.

Por ello Windows server se integra de una forma nativa con la nube pública de Microsoft denominada Azure.

Azure Arc es un servicio que proporciona un conjunto de tecnologías para organizaciones que quieren simplificar sus entornos complejos y distribuidos. Proporciona un enfoque centralizado, unificado y de autoservicio para administrar lo siguiente:

* Windows Server.
* Servidores Linux.
* Clústeres de Kubernetes.
* Servicios de datos de Azure.

Azure Arc también amplía la adopción de procedimientos en la nube como DevOps y Azure Security en entornos locales, de varias nubes y perimetrales. Además de extender el plano de control para la administración, Azure Arc permite a las empresas ejecutar servicios de datos de Azure en cualquier lugar.

Se han realizado mejoras continuas en el controlador de tejido de Azure (el plano de control de Azure). Este plano de control es responsable de administrar el ciclo de vida de los recursos, como las VM, las instancias de bases de datos, los clústeres de Apache Hadoop y los clústeres de Kubernetes.

Por ejemplo, cada vez que la empresa aprovisiona, escala, detiene o finaliza un recurso, como una VM de Azure, el controlador de tejido de Azure procesa esta operación. Entre el controlador de tejido y los recursos hay otra capa denominada Azure Resource Manager, que automatiza el ciclo de vida de los recursos. Azure tiene proveedores de recursos para cada uno de estos tipos de recursos hospedados en Azure.

Nota

Azure Resource Manager ofrece una capa de administración que le permite crear, actualizar y eliminar recursos de su suscripción a Azure.

Funcionalidades de Azure Arc

Aunque Azure Arc tiene la posibilidad de modificar drásticamente la estrategia de administración en escenarios híbridos, actualmente está limitado a dos características disponibles para los sistemas registrados, como se describe en la tabla siguiente.

A blue and white text on a white background

Description automatically generated

Tabla 6. Funcionalidades Azure Arc. Fuente: elaboración propia.