"INFORME DE LA ASMINISTRACIÓN DE SERVIDORES Y SERVICIOS EN TATA CONSULTANCY SERVICES"

Autor: Razmen Yektajo Sánchez

Tesina presentada para obtener el título de:

Ingeniero en Sistemas Computaciones

Nombre del asesor:

Mtro. Juan Jesús Ruiz Lagunas

UNIVERSIDAD VASCO DE QUIROGA

DIRECCIÓN DE INGENIERÍA EN SISTEMAS Y SEGURIDAD INFORMÁTICA

N° DE ACUERDO: LIC100846 CLAVE:16PSU0049F

Informe de la Administración de Servidores y Servicios en Tata Consultancy Services

TESINA

Para la obtención del título como

Ingeniero en Sistemas Computacionales

P R E S E N T A

Razmen Yektajo Sánchez

DIRECTOR DE TESINA

Mtro. Juan Jesús Ruiz Lagunas

Disclaimer

Este informe, titulado "Informe de la Administración de Servidores y Servicios en Tata Consultancy Services", es presentado como parte de un trabajo académico y tiene como objetivo proporcionar una visión detallada de la administración de servidores y servicios en Morgan Stanley.

Morgan Stanley es una de las principales firmas financieras y bancos de inversión en el mundo. Fundada en 1935, la empresa tiene su sede en Nueva York, Estados Unidos, y ofrece una amplia gama de servicios financieros a clientes institucionales, corporativos y particulares. Estos servicios incluyen banca de inversión, gestión de patrimonio, gestión de activos, investigación financiera, comercio de valores, préstamos y servicios de asesoramiento financiero.

Por motivos de confidencialidad el contenido de este informe se basa en investigaciones independientes, observaciones y datos disponibles de manera interna. Aunque se ha realizado un esfuerzo diligente para garantizar la precisión y relevancia de la información, no se garantiza que esté completa, actualizada o libre de errores.

Esta información no debe ser reproducida, distribuida, divulgada ni utilizada por terceros sin el permiso expreso de Morgan Stanley. Cualquier uso no autorizado está estrictamente prohibido y puede estar sujeto a medidas legales.

ÍNDICE

ÍNDICE DE IMÁGENES

1 Capítulo 1: Introducción

1.1 Contexto general sobre la administración de sistemas en entornos Windows

En Morgan Stanley la administración de sistemas en entornos Windows es una disciplina fundamental en el mundo de la tecnología de la información. Windows es uno de los sistemas operativos más ampliamente utilizados en el mundo empresarial e incluso hogares, lo que lo convierte en una plataforma crítica para el funcionamiento de una amplia gama de aplicaciones y servicios. (Stanley, 2023)

La administración de sistemas en entornos Windows implica una serie de tareas esenciales para garantizar que los sistemas basados en Windows funcionen de manera eficiente, segura y confiable. Estas tareas abarcan desde la instalación y configuración inicial del sistema operativo hasta la gestión continua de actualizaciones, seguridad, recursos y aplicaciones.

A lo largo de los años, Microsoft ha desarrollado diversas versiones de Windows, cada una con sus propias características y desafíos específicos. Algunas de las tareas clave y de manera resumida en la administración de sistemas Windows incluyen: Instalación y configuración, actualización y parches, gestión de usuarios y grupos, monitoreo del rendimiento, copia y recuperación seguridad, virtualización, gestión de políticas y directivas de automatización, escalabilidad y planificación de capacidad.

1.2 Declaración del problema y objetivos de la investigación.

La administración de sistemas en entornos Windows requiere un conocimiento profundo de las herramientas y tecnologías específicas de Microsoft, así como la capacidad de adaptarse a las cambiantes demandas tecnológicas. Con el aumento de la virtualización, la nube y la movilidad, los administradores de sistemas en entornos Windows también deben estar preparados para gestionar sistemas distribuidos y entornos híbridos que combinan recursos locales y en la nube. Esta disciplina es fundamental para mantener la integridad y la disponibilidad de los sistemas de información en el mundo actual.

El objetivo principal de este documento es explicar, con base en la propia experiencia como administrador de sistemas de Windows, cómo se debe mantener la infraestructura tecnológica de una organización funcionando sin problemas, de manera segura y eficiente. Esto se logra mediante la implementación de buenas prácticas de administración, la adopción de medidas de seguridad efectivas y la adaptación constante a los cambios en la tecnología y las necesidades de la organización.

El uso inadecuado de las prácticas mencionadas anteriormente, puede llevar a problemas de seguridad, ineficiencias operativas y riesgos financieros. Es fundamental investigar y comprenderlos para que, de esta manera, sea posible mejorar la administración de sistemas en entornos Windows.

En resumen, esta investigación tiene como objetivo comprender y abordar los desafíos actuales en la administración de sistemas en entornos Windows, con la finalidad de mejorar la eficiencia operativa, fortalecer la seguridad y cumplir con los requisitos normativos, lo que en última instancia contribuirá al éxito de las organizaciones.

2 Capítulo 2: Marco Teórico

2.1 Historia y evolución de los sistemas operativos Windows, Linux y Mac.

La historia y evolución de los sistemas operativos Windows es una narrativa que abarca varias décadas y ha dejado una marca indeleble en la industria de la computación y la tecnología. A continuación, se presenta un resumen de los hitos más significativos en esta trayectoria:

Windows 1.0 (1985):

Windows 1.0 fue el primer sistema operativo gráfico de Microsoft destinado a funcionar como un entorno de usuario para MS-DOS. Ofrecía una interfaz de usuario basada en ventanas y permitía ejecutar múltiples aplicaciones al mismo tiempo.

Windows 2.0 (1987):

Mejoras: Introdujo mejoras significativas en la interfaz de usuario, incluida la posibilidad de superponer ventanas y una mayor compatibilidad con aplicaciones. Introducción de los primeros programas de Microsoft Office.

Windows 3.0 (1990) y Windows 3.1 (1992):

Gran éxito: Estos sistemas operativos representaron un salto importante en la popularidad de Windows, gracias a su mejorado rendimiento y mayor compatibilidad con hardware y software de terceros.

Windows 95 (1995):

Cambio de paradigma: Windows 95 marcó un hito significativo al introducir el botón "Inicio", la barra de tareas y el menú de inicio. Fue el primer sistema operativo de Microsoft en prescindir completamente de MS-DOS como sistema base.

Windows 98 (1998):

Mejoras de estabilidad y rendimiento: Windows 98 trajo consigo mejoras en la estabilidad y el rendimiento, así como una mayor integración con Internet.

Windows 2000 (2000):

Orientado a empresas: Introducido como un sistema operativo empresarial, Windows 2000 ofrecía mejoras en la administración de red, seguridad y estabilidad.

Windows XP (2001):

Fundamentales cambios: Windows XP fue un hito importante, unificando la línea de productos entre la familia NT y la familia 9x. Introdujo una interfaz más pulida y características como la restauración del sistema y la administración de cuentas de usuario.

Windows Vista (2007):

Cambios importantes: Aunque presentó mejoras en la seguridad y la interfaz de usuario, Windows Vista fue criticado por su alto consumo de recursos y problemas de compatibilidad con hardware y software existentes.

Windows 7 (2009):

Regreso al éxito: Windows 7 fue bien recibido y se convirtió en uno de los sistemas operativos más populares. Introdujo una interfaz refinada y mejoras de rendimiento.

Windows 8 (2012):

Interfaz Modern UI: Windows 8 introdujo una interfaz de usuario radicalmente diferente, optimizada para pantallas táctiles, pero recibió críticas mixtas debido a la abrupta transición desde el tradicional escritorio de Windows.

Windows 10 (2015):

El último sistema operativo: En lugar de lanzar una nueva versión, Microsoft optó por un enfoque de servicio continuo con actualizaciones regulares. Windows 10 es el sistema operativo actual de Microsoft y ha visto varias actualizaciones importantes desde su lanzamiento.

(Mueller, 2004)

UNIX (1970s): La historia de Linux tiene sus raíces en el sistema operativo UNIX, que fue desarrollado en los laboratorios Bell de AT&T.

Minix (1987): Andrew Tanenbaum creó Minix, un sistema operativo tipo UNIX, como herramienta educativa.

Linux (1991): Linus Torvalds desarrolló el núcleo Linux como un proyecto de código abierto, y rápidamente se convirtió en una parte fundamental del sistema operativo.

Distribuciones Linux (varias fechas): A lo largo de los años, se han creado numerosas distribuciones de Linux, como Red Hat, Debian, Ubuntu y Fedora, cada una adaptada para diferentes usos.

Kernel Linux 2.6 (2003): Esta versión del kernel introdujo mejoras significativas en rendimiento y capacidad de administración de energía.

Linux en dispositivos móviles (2010s**):** Linux se convirtió en la base de sistemas operativos móviles, como Android.

Linux en servidores (continuo): Linux ha dominado el mercado de servidores debido a su estabilidad, seguridad y flexibilidad.

(Felber, 1995)

macOS:

Mac OS Classic (1984-2001): El sistema operativo original de Macintosh fue lanzado con la primera Macintosh. Pasó por varias versiones hasta Mac OS 9.

Mac OS X (2001): Apple introdujo Mac OS X, que estaba basado en el kernel UNIX. Esta fue una transformación significativa en la plataforma Mac.

macOS (2012): Apple cambió el nombre de su sistema operativo a macOS, siguiendo una convención de nombres similar a iOS.

macOS en Intel (2006): Apple hizo la transición de procesadores PowerPC a Intel, lo que permitió la ejecución de Windows en Mac mediante Boot Camp.

macOS en ARM (2020): Apple anunció la transición de sus Mac a procesadores ARM, lo que marcará un cambio importante en la plataforma.

(Halvorsen, Clarke, & Manning, 2011)

2.2 Virtualización

La virtualización es una tecnología que permite crear ambientes virtuales, conocidos como máquinas virtuales (VMs), en un único hardware físico. Esto es posible gracias a un componente central llamado hipervisor.

Hipervisor (Hypervisor): El hipervisor es un software o firmware que se instala directamente en el hardware físico del servidor. Su función es crear y gestionar las máquinas virtuales. Hay dos tipos principales de hipervisores:

- **Hipervisor de Tipo 1 (Nativo):** Se instala directamente en el hardware, sin necesidad de un sistema operativo anfitrión. Esto lo hace más eficiente y adecuado para entornos de servidores. Ejemplos de hipervisores de Tipo 1 incluyen VMware vSphere/ESXi, Microsoft Hyper-V y Xen.
- **Hipervisor de Tipo 2 (o "Hosted"):** Se instala sobre un sistema operativo anfitrión y es adecuado para entornos de desarrollo o pruebas. Ejemplos de hipervisores de Tipo 2 incluyen Oracle VirtualBox y VMware Workstation.

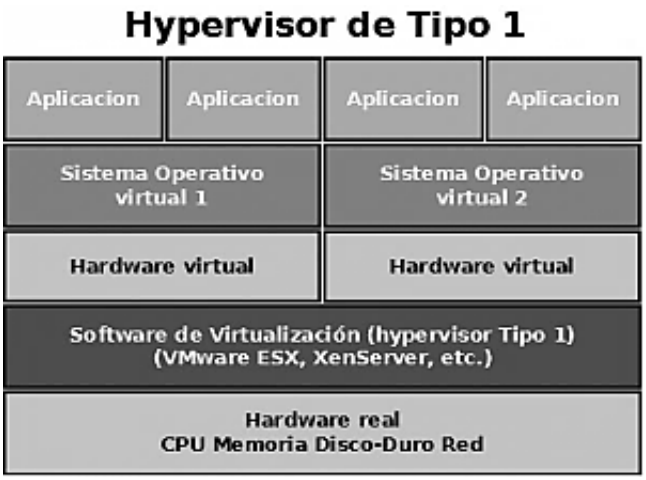
Máquinas Virtuales (VMs): Una vez que el hipervisor está instalado, se pueden crear múltiples máquinas virtuales. Cada una de estas máquinas actúa como una instancia independiente de un sistema operativo y sus aplicaciones asociadas. Las VMs comparten los recursos físicos del servidor, pero están completamente aisladas entre sí.

El proceso general de cómo funciona la virtualización es el siguiente:

1. Instalación del hipervisor: Se instala el hipervisor en el servidor físico. En el caso de un hipervisor de Tipo 1, esto se hace directamente en el hardware. En el caso de un hipervisor de Tipo 2, se instala sobre un sistema operativo existente.
2. Creación de máquinas virtuales: Una vez que el hipervisor está en funcionamiento, se pueden crear máquinas virtuales en el servidor. Cada máquina virtual tiene su propio sistema operativo, recursos asignados (como CPU, memoria, almacenamiento) y configuraciones de red.
3. Ejecución de máquinas virtuales: Las máquinas virtuales se ejecutan como procesos independientes y se comportan como si estuvieran en hardware físico separado. El hipervisor se encarga de la asignación de recursos y la gestión de acceso a los componentes físicos.
4. Gestión y monitorización: A través de una interfaz proporcionada por el hipervisor, los administradores pueden supervisar y gestionar las máquinas virtuales. Esto incluye tareas como iniciar, detener, mover o cambiar la configuración de las VMs según sea necesario.
5. Flexibilidad y aislamiento: La virtualización ofrece una gran flexibilidad en la asignación de recursos y en la gestión de cargas de trabajo. Además, las VMs están aisladas entre sí, lo que significa que un problema en una máquina virtual no afecta a las demás

A continuación, se explica el hipervisor de tipo 1, también conocido como hipervisor bare-metal o hipervisor nativo que se ejecuta directamente en el hardware de un sistema, sin necesidad de un sistema operativo host adicional. Su función principal es gestionar y asignar recursos de hardware a múltiples máquinas virtuales (VM) de manera eficiente.

Ilustración 1



Fuente:https://www.zeppelinux.es/conceptos-basicos-sobre-maquinas-virtuales/diagrama_virtualizacion_hypervisor_tipo_1/

2.3 Roles y responsabilidades del administrador de sistemas en Windows.

El administrador de sistemas en entornos Windows se desempeña un papel esencial en el mantenimiento y la gestión de la infraestructura tecnológica de una organización. Los roles y responsabilidades varían según el tamaño y la complejidad de la infraestructura, pero generalmente incluyen las siguientes funciones:

1. Instalación y configuración de sistemas operativos: El administrador de sistemas es responsable de instalar, configurar y mantener los sistemas operativos Windows en servidores y estaciones de trabajo. Esto incluye la selección de opciones de configuración, la partición de discos, la instalación de controladores de hardware y la personalización según las necesidades de la organización.

2. Gestión de usuarios y grupos: Administrar cuentas de usuario, grupos y permisos es una responsabilidad clave. Esto implica crear y eliminar cuentas de usuario, asignar permisos de acceso a recursos compartidos, configurar políticas de contraseñas y asegurarse de que los usuarios tengan el acceso adecuado a los recursos.

3. Actualizaciones y parches: Mantener el sistema con las últimas actualizaciones y parches de seguridad es crucial para proteger contra vulnerabilidades. El administrador debe planificar y aplicar parches de manera regular y minimizar el impacto en la operación diaria.

4. Seguridad y políticas: Configurar y mantener políticas de seguridad, cortafuegos y herramientas antivirus es esencial para proteger los sistemas Windows contra amenazas y ataques cibernéticos. Esto también incluye la monitorización de registros de seguridad y la respuesta a incidentes.

5. Copia de seguridad y recuperación: Implementar y administrar estrategias de copia de seguridad para proteger datos críticos y establecer planes de recuperación en caso de desastres. Esto garantiza la continuidad del negocio y la recuperación de datos en caso de fallos.

6. Monitoreo y rendimiento: Supervisar el rendimiento del sistema, identificar cuellos de botella y resolver problemas de rendimiento para garantizar un funcionamiento óptimo de la infraestructura tecnológica.

7. Automatización y scripting: Utilizar scripts y herramientas de automatización, como PowerShell, para simplificar tareas repetitivas y mejorar la eficiencia de la administración de sistemas.

8. Virtualización: En entornos empresariales, administrar tecnologías de virtualización como Hyper-V para crear y gestionar máquinas virtuales en servidores Windows.

9. Gestión de servidores: Configurar y mantener servidores de aplicaciones, servidores web, servidores de bases de datos y otros servidores especializados según sea necesario para las operaciones de la organización.

10. Documentación y políticas: Mantener documentación detallada de la configuración del sistema, procedimientos operativos y políticas de seguridad. Esto es esencial para garantizar la coherencia y la continuidad de las operaciones.

11. Soporte técnico: Proporcionar soporte técnico a usuarios finales y resolver problemas técnicos en tiempo real para minimizar el tiempo de inactividad.

12. Planificación y escalabilidad: Planificar y ejecutar la expansión y escalabilidad de la infraestructura tecnológica para satisfacer las necesidades actuales y futuras de la organización.

Estas responsabilidades del administrador de sistemas en entornos Windows pueden variar según el entorno específico de la organización, pero en general, se espera que uno sea experto en la administración y optimización de sistemas basados en Windows y en mantener la seguridad y la integridad de los datos y recursos de la empresa. (Stanley, 2023)

2.4 Herramientas y tecnologías esenciales.

En el día a día de un Windows System se necesita estar familiarizado con una amplia variedad de herramientas y tecnologías para llevar a cabo sus responsabilidades de manera eficiente y efectiva (Stanley, 2023). A continuación, se presentan algunas de las herramientas y tecnologías esenciales que son fundamentales para este rol:

Microsoft Management Console (MMC): MMC es una interfaz que proporciona una forma común de acceder y administrar una variedad de herramientas y complementos, como el Administrador de dispositivos, el Administrador de discos, la Administración de directivas de seguridad local (Local Security Policy), entre otros.

Active Directory: Active Directory es una tecnología de Microsoft que permite la gestión centralizada de usuarios, grupos, políticas de seguridad y recursos compartidos en una red empresarial basada en Windows.

PowerShell: PowerShell es una poderosa herramienta de línea de comandos y scripting que permite la automatización de tareas de administración en Windows. Los administradores de sistemas deben estar familiarizados con su uso para realizar tareas repetitivas y complejas.

Remote Desktop Services (RDS): RDS permite la administración remota de servidores y estaciones de trabajo Windows, lo que es esencial para la gestión eficiente de una infraestructura distribuida.

Hyper-V: Hyper-V es la plataforma de virtualización de Microsoft que permite crear y gestionar máquinas virtuales en servidores Windows. Es esencial para la consolidación de servidores y la administración de recursos en entornos virtualizados.

Windows Update Services (WSUS): WSUS permite administrar las actualizaciones de seguridad y parches para sistemas Windows de manera centralizada, lo que es crucial para mantener la seguridad y la integridad del sistema.

System Center Configuration Manager (SCCM): SCCM es una herramienta de gestión de sistemas que facilita la implementación de software, la administración de configuraciones y la supervisión del estado de los sistemas Windows en toda la red.

Group Policy: Las Directivas de grupo permiten configurar y administrar la configuración y la seguridad de las estaciones de trabajo y servidores Windows en un entorno de dominio de Active Directory.

Herramientas de diagnóstico de red: Herramientas como ipconfig, ping, tracert y netstat son esenciales para la solución de problemas de red y la monitorización del tráfico en sistemas Windows.

Herramientas de seguridad: Esto incluye software antivirus, cortafuegos de software, soluciones de detección de intrusiones y herramientas de auditoría de seguridad para proteger los sistemas Windows contra amenazas.

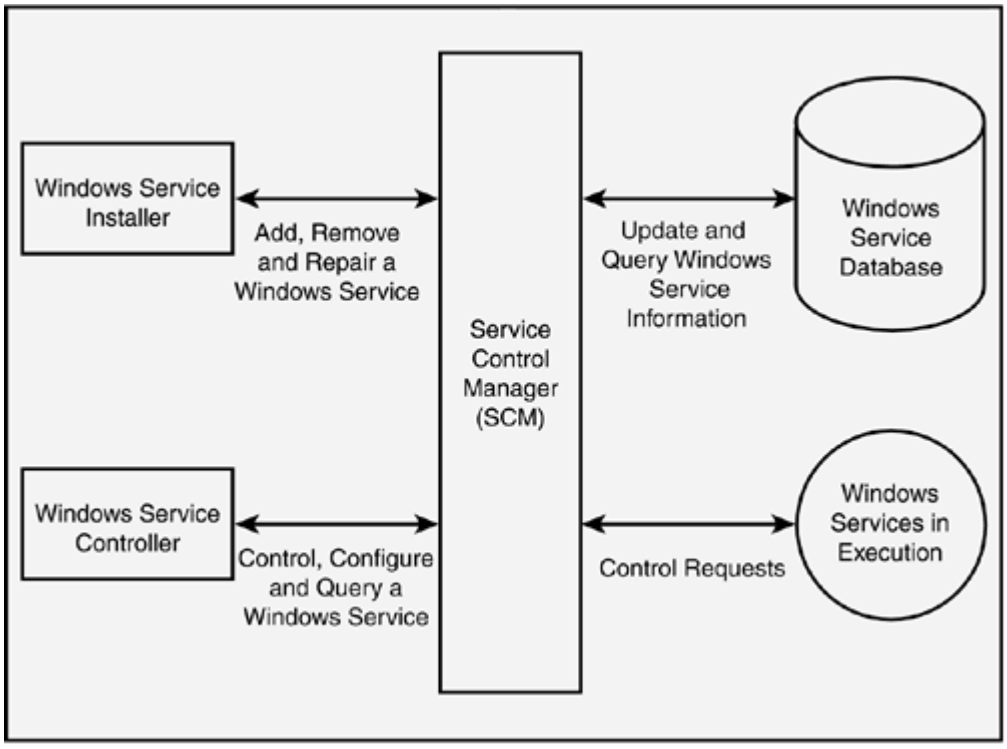
Herramientas de copia de seguridad: Soluciones de copia de seguridad y recuperación de datos que pueden integrarse con sistemas Windows para garantizar la disponibilidad y la protección de los datos críticos.

Monitoreo y administración de recursos: Herramientas como el Administrador de tareas, el Monitor de rendimiento de Windows y herramientas de terceros como Nagios o Zabbix para supervisar el rendimiento y la utilización de recursos en sistemas Windows.

Herramientas de administración remota: Soluciones de administración remota, como Remote Desktop Protocol (RDP), SSH (cuando sea aplicable) y software de administración remota de terceros para acceder y administrar sistemas de manera remota.

Estas son solo algunas de las herramientas y tecnologías esenciales que un administrador de sistemas en entornos Windows debe conocer y dominar para desempeñar con éxito sus funciones en la gestión y administración de sistemas basados en Windows. La selección específica de herramientas dependerá de las necesidades y la complejidad del entorno de TI de la organización. (Stanley, 2023) . En la siguiente imagen un diagrama que lo explica:

Ilustración 2



Fuente: https://www.oreilly.com/library/view/mcadmcsd-training-guide/078972824.html

3 Capítulo 3: Gestión de Sistemas Windows

La implementación y administración de servidores Windows es una parte crítica de la gestión de la infraestructura de TI de una organización. Llevamos a cabo las siguientes tareas:

3.1 Implementación de servidores Windows:

Para esto, Morgan Stanley tiene una manera estricta de implementación en los servidores Windows la cual es la siguiente:

1. Planificación: Antes de implementar un servidor Windows, es crucial realizar una planificación cuidadosa. Definir los objetivos, requisitos de hardware, necesidades de software y considera la virtualización si es apropiado.
2. Selección de hardware: Seleccionar el hardware que cumpla con los requisitos de rendimiento y capacidad de la aplicación. Esto puede incluir servidores físicos o máquinas virtuales si estás utilizando una plataforma de virtualización como Hyper-V.
3. Instalación del sistema operativo: Instala el sistema operativo Windows Server en el hardware seleccionado. Durante la instalación, configura las opciones de red, establece contraseñas seguras y selecciona las características y roles que necesitas, como Active Directory, Servidor web, Servidor de archivos, etc.
4. Configuración inicial: Después de la instalación, realiza la configuración inicial del servidor, incluida la asignación de direcciones IP, la configuración de nombres de host, la activación del firewall de Windows y la instalación de actualizaciones de seguridad. (Stanley, 2023)

3.2 Gestión de usuarios, grupos y permisos.

La gestión de usuarios, grupos y permisos en un entorno Windows es una parte fundamental de las responsabilidades de un administrador de sistemas. Esto garantiza la seguridad y el acceso adecuado a los recursos dentro de la red. La forma en que se realiza es la siguiente:

Gestión de usuarios y grupos:

1. Creación de usuarios: Utiliza el Administrador de usuarios de Windows o Active Directory (según el entorno) para crear nuevas cuentas de usuario. Define nombres de usuario, contraseñas seguras y otra información necesaria.
2. Modificación de usuarios: Actualiza la información de usuarios cuando sea necesario, como cambios en el nombre, el cargo o la ubicación. También puedes modificar los permisos de usuario y las pertenencias a grupos según las necesidades.
3. Eliminación de usuarios: Cuando un usuario ya no necesita acceso, deshabilita o elimina su cuenta de usuario para evitar el acceso no autorizado.
4. Creación de grupos: Crea grupos para simplificar la administración de permisos. Puedes crear grupos basados en departamentos, funciones o proyectos.
5. Asignación a grupos: Asigna usuarios a los grupos correspondientes según sus roles y necesidades de acceso. Esto facilita la gestión de permisos, ya que los permisos se pueden otorgar a nivel de grupo en lugar de a usuarios individuales.

Las siguientes imágenes muestran cómo se puede gestionar permisos y accesos a usuarios en diferentes grupos de seguridad:

Ilustración 3

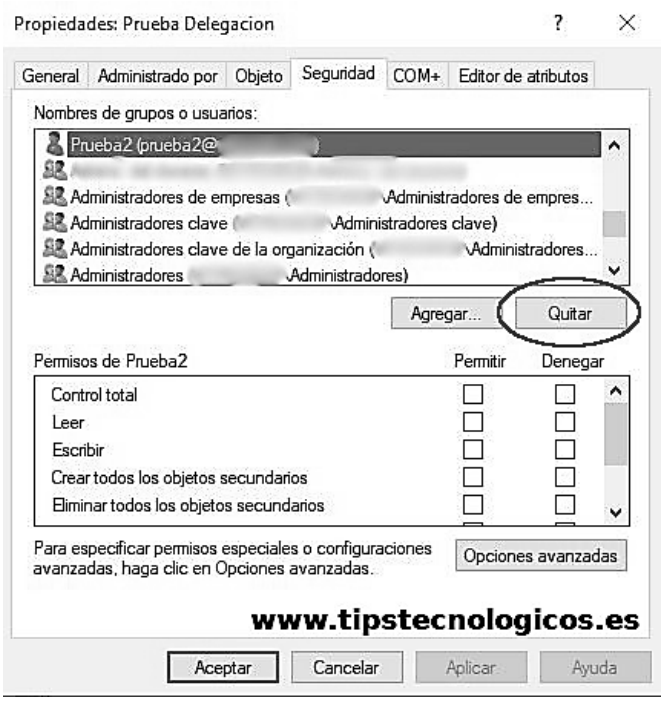
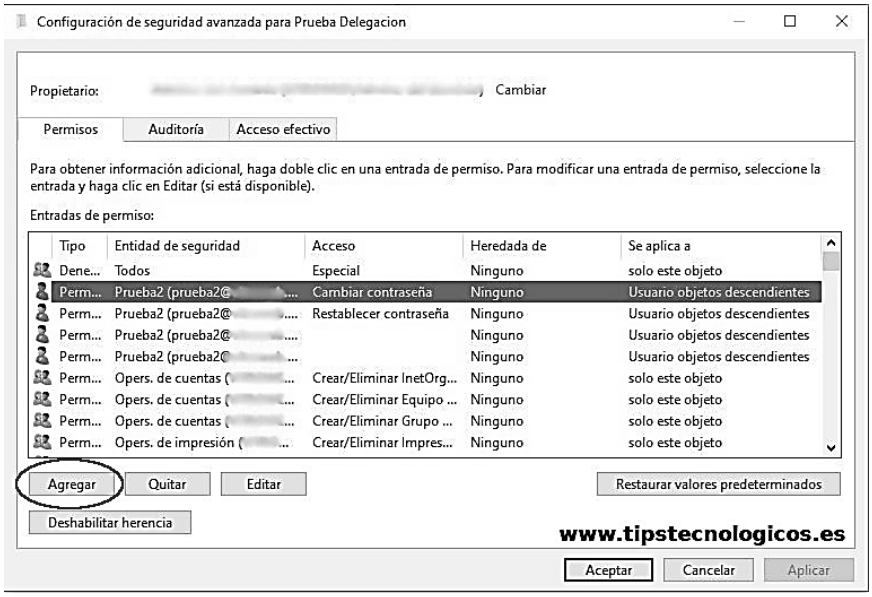


Ilustración 4



Fuente:https://tutorialesit.com/windows-server-delegacion-permisos-administracion-active-directory/

Gestión de permisos:

1. Permisos de carpetas y archivos: Utiliza las propiedades de seguridad de carpetas y archivos para asignar permisos. Define quién puede leer, escribir, modificar o eliminar archivos y carpetas específicos.
2. Permisos de recursos compartidos: Configura los permisos de recursos compartidos para controlar el acceso a carpetas y archivos compartidos a través de la red. Define qué usuarios o grupos pueden acceder y qué nivel de acceso tienen.
3. Directivas de grupo: Utiliza Directivas de grupo (Group Policy) para aplicar configuraciones de seguridad y permisos de manera consistente en múltiples sistemas. Esto es especialmente útil en entornos empresariales con Active Directory.
4. Auditoría de seguridad: Habilita la auditoría de seguridad para registrar eventos relacionados con la seguridad, como intentos de inicio de sesión fallidos o cambios en los permisos. Esto te permite realizar un seguimiento de actividades sospechosas.

3.3 Monitorización de recursos y rendimiento.

La monitorización de recursos y rendimiento es estrictamente necesario para garantizar que los servidores y estaciones de trabajo funcionen de manera eficiente, identificar problemas antes de que afecten a los usuarios y tomar decisiones informadas sobre la capacidad y el rendimiento de la infraestructura. Para esto se debe de llevar a cabo la monitorización de recursos y rendimiento en un entorno de administración de sistemas Windows:

Herramientas de monitorización de recursos y rendimiento:

Monitor de rendimiento de Windows: Esta herramienta incorporada proporciona una vista detallada de los recursos del sistema, como la CPU, la memoria, el almacenamiento y el rendimiento de red. Puedes acceder al

Monitor de rendimiento a través de la Consola de administración de sistemas (perfmon.msc).

Herramientas de línea de comandos: Windows ofrece varias herramientas de línea de comandos para la monitorización, como el comando "Tasklist" para ver procesos en ejecución o "Netstat" para mostrar conexiones de red.

Herramientas ade terceros: Hay numerosas herramientas de terceros disponibles para la monitorización de sistemas Windows, como SolarWinds, PRTG Network Monitor, Nagios, Zabbix y más. Estas herramientas suelen ofrecer características avanzadas y una interfaz centralizada para la monitorización

¿Qué monitorizamos?

a. Uso de CPU: Supervisa la carga de CPU para detectar picos de utilización que puedan indicar procesos que consumen muchos recursos.
b. Uso de memoria: Controla el uso de memoria RAM y la paginación al disco para asegurarte de que el sistema no sufra de falta de memoria.
c. Uso de almacenamiento: Se observa el espacio en disco disponible y el rendimiento del almacenamiento para evitar problemas de capacidad y cuellos de botella de E/S.
d. Procesos y servicios: Haz un seguimiento de los procesos y servicios en ejecución para identificar posibles cuellos de botella o aplicaciones problemáticas.
e. Eventos y registros: Consulta los registros de eventos de Windows para buscar errores y advertencias que puedan indicar problemas en el sistema.

3.4 Mejores prácticas de monitorización

1. Establece umbrales: Define umbrales para los recursos clave, como la CPU y la memoria, y configura alertas para que te notifiquen cuando se superen estos umbrales.

2. Programación de tareas: Automatiza la recopilación de datos de monitorización programando tareas para ejecutar herramientas de monitorización en momentos específicos o a intervalos regulares.

3. Tendencias a largo plazo: Realiza un seguimiento de las tendencias a lo largo del tiempo para identificar patrones de uso de recursos y planificar mejoras o ajustes.

4. Registro y documentación: Lleva un registro de las lecturas de monitorización y documenta los cambios y las acciones tomadas en respuesta a problemas o alertas.

5. Colaboración: Comparte información de monitorización con otros miembros del equipo de TI para una resolución más rápida de problemas y la toma de decisiones informadas. (Stanley, 2023)

4 Capítulo 4: Seguridad en Sistemas Windows

La seguridad de los sistemas Windows Servers es crucial para proteger los datos, los recursos y la infraestructura de una empresa. Para mejorar la seguridad de los servidores Windows es un proceso continuo y multidimensional que requiere atención constante y la adaptación a las amenazas cambiantes. Implementar estas prácticas de seguridad contribuirá significativamente a proteger cualquier entorno de servidores. (Stanley, 2023)

4.1 Amenazas y desafíos de seguridad en entorno Windows.

Los entornos Windows, debido a su amplia adopción en empresas y organizaciones, son un objetivo atractivo para una variedad de amenazas y desafíos de seguridad. A continuación, se describen algunas de las amenazas y desafíos de seguridad más comunes en entornos Windows:

Malware y virus: Los sistemas Windows son vulnerables a una amplia gama de malware, incluidos virus, gusanos, troyanos y ransomware. Estos programas maliciosos pueden robar datos, dañar sistemas y bloquear el acceso a archivos hasta que se pague un rescate.

Ataques de ingeniería social: Los atacantes a menudo utilizan la ingeniería social para engañar a los usuarios para que revelen información confidencial, como contraseñas o credenciales de inicio de sesión, o para hacer clic en enlaces maliciosos o abrir archivos adjuntos dañinos.

Ataques de fuerza bruta: Los atacantes intentan adivinar contraseñas mediante la prueba de múltiples combinaciones. En entornos Windows, esto puede dar lugar a intentos de inicio de sesión no autorizados en cuentas de usuario o servicios.

Vulnerabilidades y exploits: Los sistemas Windows a menudo se ven afectados por vulnerabilidades de seguridad que pueden ser explotadas por atacantes. Estas vulnerabilidades pueden surgir en el sistema operativo, aplicaciones o servicios de terceros.

Acceso no autorizado: Los intentos de acceso no autorizado pueden provenir de intrusos externos o usuarios internos malintencionados. Los administradores de sistemas deben implementar políticas de control de acceso para prevenir este tipo de amenazas.

Phishing: Los correos electrónicos de phishing intentan engañar a los usuarios para que proporcionen información confidencial, como nombres de usuario, contraseñas o detalles de tarjetas de crédito. Los enlaces y archivos adjuntos maliciosos también son comunes en los ataques de phishing.

Ataques de día cero: Estos son ataques que aprovechan vulnerabilidades desconocidas o no parcheadas antes de que los desarrolladores tengan la oportunidad de emitir correcciones. Los atacantes pueden utilizarlos para comprometer sistemas antes de que se descubra la vulnerabilidad.

Ransomware: Los ataques de ransomware cifran archivos y sistemas, exigiendo un rescate a cambio de la clave de descifrado. Esto puede causar graves interrupciones en las operaciones de una organización.

Ataques a la nube: Con la adopción de servicios en la nube basados en Windows, también existen amenazas relacionadas con la seguridad en la nube, como la exposición accidental de datos y la mala configuración de la seguridad en servicios como Azure o Microsoft 365.

4.2 Estrategias de seguridad: firewalls y políticas de seguridad.

Las estrategias de seguridad que involucran firewalls y políticas de seguridad son fundamentales para proteger una red o sistema de posibles amenazas y ataques cibernéticos. Los componentes más importantes son los siguientes:

Firewalls:

Un firewall es una barrera de seguridad que se utiliza para controlar el tráfico de red entre una red privada y una red pública, como Internet. Su principal función es permitir o bloquear el tráfico en función de un conjunto de reglas predefinidas. Hay dos tipos principales de firewalls:

Firewall de hardware: Estos son dispositivos físicos dedicados a la seguridad, como los enrutadores de seguridad. Se colocan entre la red interna y la red externa y filtran el tráfico según las reglas configuradas.

Firewall de software: Estos son programas o aplicaciones que se ejecutan en un servidor o dispositivo y realizan la misma función de filtrado de tráfico. Los firewalls de software son comunes en servidores y sistemas operativos de escritorio.

Las políticas de seguridad están estrechamente relacionadas con los firewalls. Establecer una política de seguridad adecuada implica definir las reglas y directrices que el firewall debe seguir al filtrar el tráfico de red. Algunos aspectos clave de las políticas de seguridad incluyen:

Reglas de acceso: Definir qué tráfico se permite y qué tráfico se bloquea. Esto se hace especificando puertos, direcciones IP, protocolos, etc.

Control de aplicaciones: Determinar qué aplicaciones o servicios pueden utilizarse a través de la red. Por ejemplo, se pueden permitir servicios web y bloquear aplicaciones de intercambio de archivos.

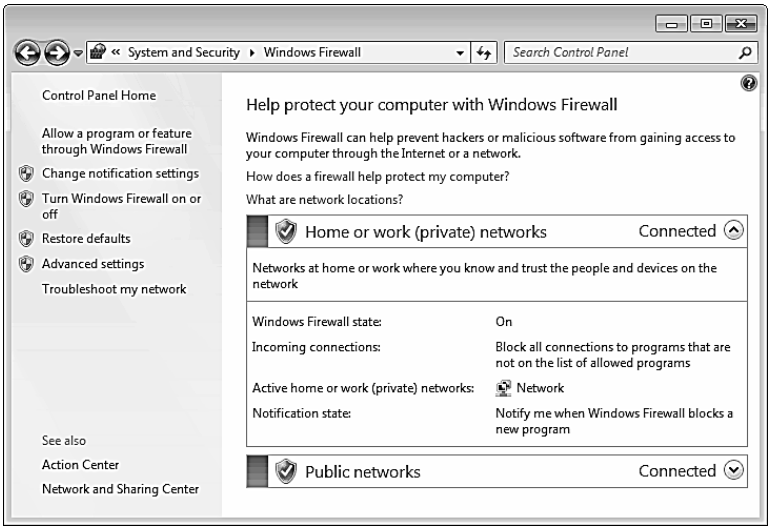
Gestión de amenazas: Configurar el firewall para detectar y prevenir intrusiones, malware y otros tipos de amenazas. Esto puede implicar el uso de firmas de amenazas, análisis de comportamiento y prevención de intrusiones.

Reglas de NAT (Network Address Translation): Si es necesario, el firewall puede realizar traducción de direcciones IP para ocultar las direcciones internas de la red y proteger la privacidad.

Es importante y fundamental capacitar al personal para comprender y cumplir con estas políticas de seguridad y garantizar que el firewall esté configurado y mantenido adecuadamente para mantener la red segura. (Stanley, 2023)

En todo ambiente Windows es necesario estar familiarizado con la interfaz del firewall, estas son algunas de las opciones que el usuario puede visualizar y manipular para la correcta gestión de su equipo.

Ilustración 5

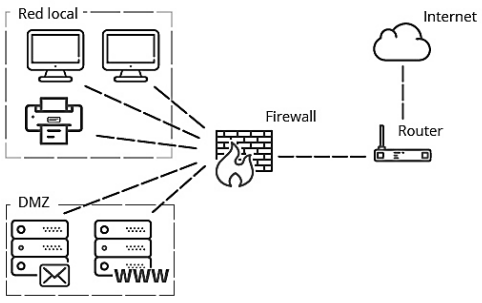


Fuente:https://www.elevate.in/?w=best-practices-for-configuring-windows-defender-firewall-windows-security-cc-xb9JDkc6

Distintas Zonas en la Arquitectura de Seguridad:

1. **Zona de Internet o No Confiable:** Esta es la zona de mayor riesgo, ya que está expuesta a Internet y a una amplia variedad de amenazas. El firewall se ubica entre esta zona y el resto de la red de la organización para filtrar y bloquear amenazas entrantes.
2. **Zona de Perímetro o DMZ (Demilitarized Zone):** La DMZ es una zona intermedia que contiene servicios públicos, como servidores web y correo electrónico. El firewall en esta zona permite el acceso limitado desde Internet a estos servicios sin exponer la red interna.
3. **Zona de Red Interna o Confiable:** Esta es la red interna de la organización, donde se almacenan los datos y se ejecutan las aplicaciones críticas. El firewall dentro de esta zona controla el tráfico interno y protege los activos de la organización contra amenazas internas y externas.
4. **Zonas Específicas:** Dependiendo de la arquitectura y las necesidades de la organización, se pueden crear zonas adicionales, como una zona de servidores, una zona de invitados o una zona de pruebas. Cada una de estas zonas puede tener diferentes niveles de seguridad y políticas de firewall específicas. La ilustración 9 muestra la forma en que repartimos el firewall para la asignación de dispositivos y dmz.

Ilustración 6



Fuente:https://www.incibe.es/empresas/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

4.3 Recuperación de datos y copias de seguridad.

Cuando hablamos de la recuperación de datos y las copias de seguridad estamos hablando de ciertas prácticas que ayudan a garantizar la disponibilidad y la integridad de los datos, así como a minimizar la pérdida de información en caso de incidentes, como fallas en el hardware, errores humanos, malware o ataques cibernéticos. Existen ciertas pautas para llevar a cabo una efectiva recuperación de datos y estrategias de copias de seguridad como administrador de sistemas de Windows:

1. Planificación de copias de seguridad:

- Identifica los datos críticos: Identifica los datos y sistemas más importantes que deben incluirse en las copias de seguridad. Esto puede incluir archivos de usuario, configuraciones del sistema, bases de datos y aplicaciones clave.
- Frecuencia de las copias de seguridad: Define con qué frecuencia se realizarán las copias de seguridad. La frecuencia puede variar según la criticidad de los datos. Por ejemplo, los datos críticos pueden respaldarse diariamente, mientras que otros pueden hacerlo semanal o mensualmente.
- Políticas de retención: Establece políticas de retención que determinen cuánto tiempo se conservarán las copias de seguridad. Asegúrate de cumplir con las regulaciones de retención de datos aplicables.

2. Selección de herramientas de copia de seguridad:

- Usa herramientas de copia de seguridad confiables: Selecciona software de copia de seguridad de calidad que sea compatible con sistemas Windows. Microsoft ofrece la herramienta "Windows Server Backup" para servidores Windows y "Backup and Restore" para sistemas Windows de escritorio.
- Considera soluciones de terceros: Si necesitas funcionalidades avanzadas, como copias de seguridad fuera del sitio o programación personalizada, considera soluciones de copia de seguridad de terceros.

3. Estrategias de copia de seguridad:

- Copias de seguridad completas: Realiza copias de seguridad completas de forma regular para garantizar que todos los datos estén respaldados.
- Copias de seguridad incrementales o diferenciales: Utiliza copias de seguridad incrementales o diferenciales para reducir el tiempo y el espacio de almacenamiento requerido para las copias de seguridad. Estas técnicas solo respaldan los datos que han cambiado desde la última copia de seguridad completa.
- Almacenamiento seguro: Almacena las copias de seguridad en ubicaciones seguras y separadas de la red principal para proteger contra pérdidas debido a desastres naturales o ataques cibernéticos.

4. Procedimientos de recuperación:

- Documentación: Documenta procedimientos claros para la recuperación de datos, incluyendo cómo restaurar sistemas y datos desde las copias de seguridad.
- Pruebas de recuperación: Realiza pruebas periódicas de recuperación para asegurarte de que las copias de seguridad sean efectivas y que puedas restaurar datos y sistemas según sea necesario.
- Capacitación del personal: Capacita a tu equipo en los procedimientos de recuperación para que sepan cómo responder ante incidentes y restaurar los sistemas rápidamente.

5. Monitoreo y mantenimiento:

- Supervisar el estado de las copias de seguridad de forma regular para asegurarte de que se estén realizando correctamente.
- Mantener el software de copia de seguridad actualizado y aplique parches de seguridad según sea necesario para proteger los datos de posibles amenazas.

5 Capítulo 5: Optimización y Rendimiento

5.1 Optimización de sistemas Windows para un rendimiento optimo.

La optimización del rendimiento en un entorno empresarial requiere una planificación cuidadosa, una monitorización constante y un enfoque proactivo en la administración de sistemas. Al seguir estas pautas, podemos asegurarnos de que los sistemas Windows funcionen de manera óptima en cualquier organización y que cumplan con las necesidades empresariales.

Planificación y Gestión:

- Realizar una evaluación inicial de los sistemas para identificar cuellos de botella y áreas que requieren optimización.
- Establecer un proceso de gestión de cambios para realizar actualizaciones y cambios en los sistemas de manera organizada y controlada.

Actualizaciones y Parches:

- Mantener todos los sistemas Windows y las aplicaciones empresariales actualizados con los últimos parches de seguridad y actualizaciones.
- Implementar un calendario de mantenimiento regular para aplicar parches y actualizaciones de manera sistemática.

Hardware y Virtualización:

- Asegurarse de que el hardware utilizado sea adecuado para las necesidades empresariales. Esto incluye la CPU, la RAM, el almacenamiento y la red.
- Considerar la virtualización para optimizar la administración de recursos y reducir el consumo de energía.

Políticas de Grupo (Group Policies):

- Utilizar políticas de grupo para configurar y controlar las configuraciones de seguridad y rendimiento en todas las máquinas Windows de la red empresarial.
- Establecer políticas de grupo específicas para limitar el acceso a recursos sensibles y mejorar la seguridad.

Monitorización y Gestión del Rendimiento:

- Implementar herramientas de monitorización de rendimiento para supervisar el uso de recursos en tiempo real.
- Establecer umbrales de alerta para detectar problemas de rendimiento antes de que afecten a los usuarios.

Automatización de Tareas:

- Utilizar herramientas de automatización, como scripts y tareas programadas, para realizar tareas de mantenimiento y administración de manera eficiente.
- Automatizar la implementación de parches y actualizaciones en horarios fuera de las horas laborables para evitar interrupciones.

Gestión de Almacenamiento:

- Implementar una gestión de almacenamiento eficiente para evitar que los discos se llenen y afecten al rendimiento.
- Utilizar tecnologías de almacenamiento en red (NAS y SAN) para centralizar el almacenamiento y facilitar la administración.

Capacitación y Soporte:

- Capacitar a los usuarios y al personal de TI en las mejores prácticas de uso y solución de problemas.

- Proporcionar un sistema de soporte técnico eficiente y procesos de escalada para abordar problemas de rendimiento de manera oportuna.

5.2 Herramientas de diagnóstico y solución de problemas.

Hoy en la actualidad disponemos de varias herramientas de diagnóstico y solución de problemas para optimizar el rendimiento y resolver problemas en los sistemas Windows. Estas herramientas son esenciales para identificar y abordar problemas que puedan afectar la eficiencia y el funcionamiento de los sistemas. Las utilizadas generalmente por empresas de IT son:

Administrador de tareas (Task Manager):

El Administrador de tareas es una herramienta incorporada en Windows que permite supervisar el rendimiento del sistema y administrar procesos en ejecución. Podemos utilizarlo para identificar aplicaciones o procesos que consumen demasiados recursos de CPU, memoria RAM o disco.

Monitor de recursos (Resource Monitor):

Esta herramienta proporciona una vista más detallada del rendimiento del sistema, incluyendo información sobre el uso de CPU, memoria, disco y red. Nos permite identificar procesos específicos que pueden estar causando cuellos de botella en el rendimiento.

Herramienta de comprobación de disco (Check Disk - chkdsk):

Utiliza esta herramienta para verificar y reparar errores en el sistema de archivos y sectores defectuosos en el disco duro. Puede mejorar el rendimiento y la estabilidad del sistema.

Herramienta de información del sistema (System Information):

Proporciona una vista detallada de la configuración y los componentes del sistema. Útil para obtener información sobre hardware y software que puede estar afectando el rendimiento.

Herramienta de diagnóstico de red (Network Diagnostics):

Ayuda a identificar y solucionar problemas de red, como problemas de conectividad o configuraciones incorrectas de adaptadores de red.

Herramienta de rendimiento (Performance Monitor):

Permite crear conjuntos de datos de rendimiento personalizados para supervisar métricas específicas del sistema a lo largo del tiempo. De gran ayuda para identificar patrones y problemas de rendimiento a largo plazo.

Herramienta de gestión de dispositivos (Device Manager):

Utiliza el Administrador de dispositivos para verificar y actualizar controladores de hardware, lo que puede mejorar el rendimiento y la compatibilidad del sistema.

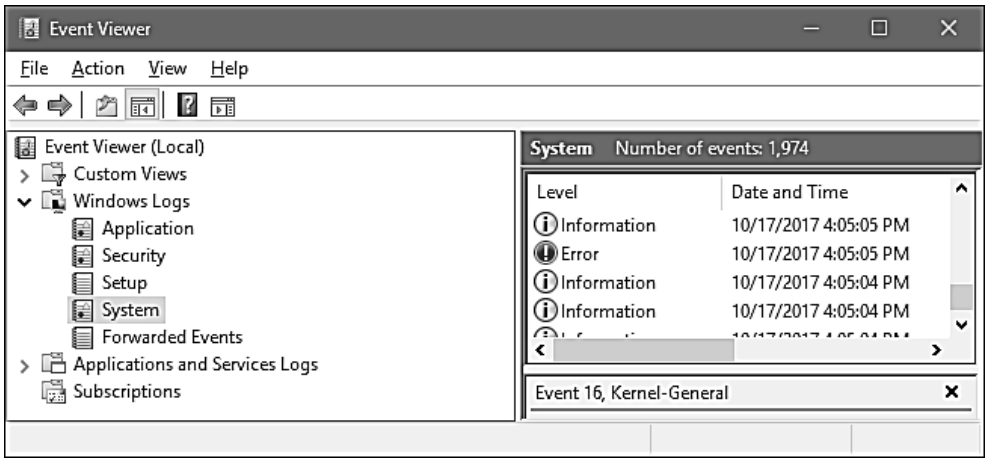
Herramienta de rendimiento de disco (Disk Cleanup):

Esta herramienta permite eliminar archivos temporales, cachés y otros elementos innecesarios que pueden ocupar espacio en disco y afectar el rendimiento. Acceso rápido: Busca "Liberador de espacio en disco" en el menú Inicio.

Herramienta de seguimiento de eventos (Event Viewer):

Permite examinar registros de eventos para identificar problemas, errores y eventos importantes que puedan afectar al rendimiento. Como en la siguiente imagen:

Ilustración 7



Fuente:https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/

5.3 Mejores prácticas para mantener el sistema de Windows eficiente.

Mantener el sistema operativo actualizado: Asegurarnos de que Windows esté configurado para descargar e instalar automáticamente las actualizaciones. Las actualizaciones suelen incluir correcciones de seguridad y mejoras de rendimiento.

Desinstalar software innecesario: Eliminar programas y aplicaciones que ya no se requieran. Cuanto menos software innecesario haya en el sistema, más rápido funcionará.

Mantener un firewall activado: El firewall de Windows ayuda a proteger tu sistema contra amenazas en línea y puede ayudar a prevenir ataques no deseados.

Actualizar los controladores: Mantén tus controladores de hardware (como los controladores de la tarjeta gráfica y del chipset) actualizados para garantizar un rendimiento óptimo. Puedes hacerlo a través del Administrador de dispositivos o descargando los controladores directamente desde el sitio web del fabricante.

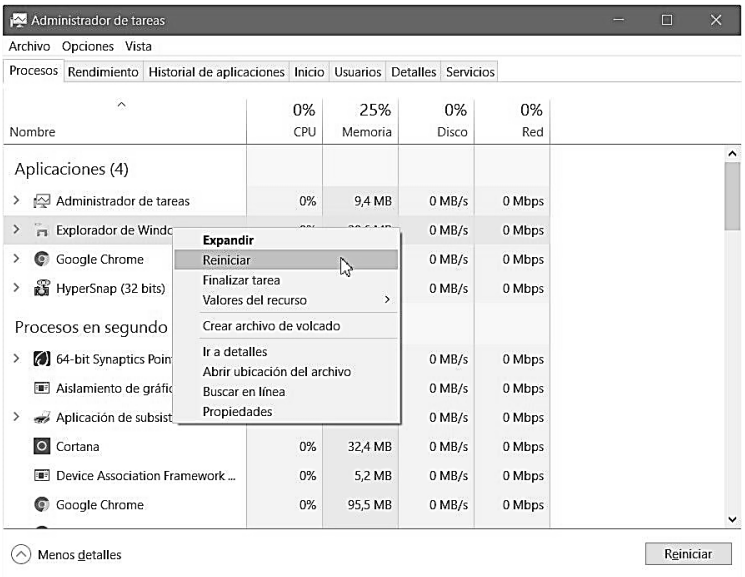
Realizar copias de seguridad regulares: Realizar copias de seguridad de los archivos importantes en caso de problemas. Puedes utilizar la herramienta de copia de seguridad de Windows o soluciones de terceros.

Monitorizar el rendimiento: Utiliza el Administrador de tareas de Windows o herramientas de terceros para supervisar el uso de recursos (CPU, memoria, disco, red) y detectar posibles cuellos de botella.

Considerar una actualización de hardware: Si el sistema es antiguo y no puede ejecutar las aplicaciones que se necesitan de manera eficiente, se considera la posibilidad de actualizar el hardware, como agregar más RAM o cambiar a un disco SSD.

En la siguiente imagen lo que se hace es reiniciar el servicio ya que esto puede ayudar a liberar un procedimiento que pudo haber estado atorado.

Ilustración 8



Fuente:https://www.muycomputerpro.com/2017/03/28/administrador-de-tareas-de-windows

6 Capítulo 6: Administrador de Sistemas en TCS (Tata Consultancy Services)

6.1 Responsabilidades como un System Administrator en Morgan Stanley

Como se ha mencionado anteriormente, las responsabilidades de un administrador de sistemas (system admin) en Morgan Stanley o en cualquier otra institución financiera de alto nivel pueden variar según el nivel de experiencia, el equipo al que estén asignados y las necesidades específicas de la empresa. Sin embargo, a continuación, se describen algunas responsabilidades generales que un administrador de sistemas podría tener en Morgan Stanley u organizaciones similares:

Gestión de infraestructura: Configurar, mantener y supervisar servidores, almacenamiento y redes para garantizar que estén funcionando de manera eficiente y segura.

Seguridad de la información: Implementar y mantener políticas y procedimientos de seguridad, así como aplicar parches y actualizaciones de seguridad para proteger los datos confidenciales de la empresa.

Administración de cuentas de usuario: Crear, gestionar y eliminar cuentas de usuario, controlando los accesos y las autorizaciones para garantizar la seguridad de la información.

Resolución de problemas técnicos: Diagnosticar y solucionar problemas de hardware y software, así como brindar soporte técnico a los usuarios finales.

Backup y recuperación de datos: Configurar y gestionar sistemas de respaldo y recuperación para garantizar la disponibilidad de datos críticos en caso de fallos o desastres.

Automatización de tareas: Desarrollar scripts y herramientas de automatización para agilizar procesos y tareas repetitivas.

Cumplimiento normativo: Asegurarse de que los sistemas y la infraestructura cumplan con los estándares y regulaciones de la industria financiera, como las normativas de seguridad y privacidad.

Monitoreo y rendimiento: Supervisar el rendimiento de sistemas y redes, identificar cuellos de botella y tomar medidas para optimizar el rendimiento.

Planificación de capacidad: Evaluar las necesidades futuras de hardware y software y planificar la expansión de la infraestructura según sea necesario.

Gestión de parches y actualizaciones: Aplicar parches de seguridad y actualizaciones de software de manera regular para mantener los sistemas protegidos y actualizados.

Documentación y seguimiento: Mantener registros detallados de la configuración del sistema, procedimientos y cambios realizados para facilitar la auditoría y la resolución de problemas.

Mantenerse actualizado: Mantenerse al día con las últimas tendencias y avances en tecnología de la información para garantizar que los sistemas estén alineados con las mejores prácticas y los estándares de la industria.

Es importante destacar que las responsabilidades específicas pueden variar según el rol y la ubicación dentro de una organización como Morgan Stanley, y es esencial seguir las políticas y procedimientos internos de la empresa, así como cumplir con las regulaciones financieras y de seguridad aplicables. (Stanley, 2023)

6.2 Manejo de servidores en producción

Diariamente en tcs (Morgan Stanley) manejamos distintos tipos de estados de servidores de Windows, pero los que principalmente gestionamos y que debemos dar mas importancia son los de producción, cuando se mencionan "servidores en estado de producción" en el contexto de la administración de sistemas, nos referimos a los servidores que están activos y funcionando en un entorno de producción en una organización, valga la redundancia. Estos servidores son esenciales para el funcionamiento continuo de las operaciones comerciales y proporcionan servicios y aplicaciones a los usuarios finales.

Como administrador de sistemas, mi principal responsabilidad es asegurarme de que estos servidores en producción estén en un estado óptimo para garantizar la disponibilidad y el rendimiento de los servicios que ofrecen. Los principales servidores. A continuación, se presentan ejemplos de servidores en estado de producción que podrían encontrarse en Morgan Stanley:

1. **Servidores de Trading**: Estos servidores son esenciales para ejecutar y gestionar las operaciones de trading de valores, derivados y otros instrumentos financieros en tiempo real. La velocidad y la fiabilidad son críticas en este entorno.
2. **Servidores de Datos Financieros**: Alojan bases de datos y sistemas que almacenan y gestionan datos financieros críticos, incluyendo cotizaciones de mercado, históricos de transacciones y datos de clientes.
3. **Servidores de Infraestructura de TI**: Proporcionan servicios de red, autenticación, directorio y otros servicios de infraestructura que respaldan las operaciones diarias y la conectividad en toda la organización.

4. **Servidores de Seguridad**: Incluyen firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y otros dispositivos de seguridad que protegen la red y los sistemas contra amenazas cibernéticas.
5. **Servidores de Almacenamiento**: Ofrecen almacenamiento centralizado y compartido para datos y aplicaciones críticas, asegurando la disponibilidad y la integridad de la información.
6. **Servidores de Aplicaciones Comerciales**: Alojan aplicaciones comerciales específicas utilizadas en la gestión de inversiones, banca de inversión y otros aspectos del negocio financiero.
7. **Servidores de Comunicaciones**: Respaldan sistemas de comunicación y colaboración, como correo electrónico y herramientas de mensajería instantánea utilizadas por los empleados de la empresa.
8. **Servidores de Continuidad del Negocio**: Configurados para garantizar la disponibilidad continua de los servicios críticos en caso de fallas o desastres.
9. **Servidores de Virtualización**: Permiten la consolidación de servidores físicos mediante la ejecución de máquinas virtuales, lo que optimiza el uso de recursos y la escalabilidad.
10. **Servidores de Cumplimiento y Auditoría**: Utilizados para el registro y la auditoría de actividades de usuarios y sistemas para cumplir con regulaciones y estándares de la industria.
11. **Servidores de Copias de Seguridad y Recuperación de Desastres**: Aseguran la disponibilidad de datos y aplicaciones en caso de pérdida de datos o interrupciones críticas.

7 Capítulo 7: Conclusiones

7.1 Resumen de los hallazgos y conclusiones clave

Ya para finalizar, cabe resaltar un par de hallazgos y conclusiones que parecen “clave” y fueron detectados al hacer ser un administrador de sistemas de Windows en TCS.

Hallazgos:

La alta disponibilidad es fundamental: Los sistemas en estado de producción deben mantenerse altamente disponibles para respaldar las operaciones financieras críticas de la empresa. La interrupción en la disponibilidad puede resultar en pérdida de ingresos y daños a la reputación.

Seguridad es una prioridad crítica: La seguridad de los servidores y los datos financieros es de máxima importancia. Los administradores deben estar alerta ante las amenazas cibernéticas, implementar medidas de seguridad sólidas y mantener actualizadas las defensas.

Cumplimiento normativo: Morgan Stanley debe cumplir con regulaciones estrictas en la industria financiera. Los servidores deben configurarse y administrarse de manera que cumplan con los requisitos regulatorios, y se debe llevar un registro adecuado para fines de auditoría.

Rendimiento óptimo: La optimización del rendimiento de los servidores es esencial para garantizar que las aplicaciones financieras se ejecuten de manera eficiente y sin retrasos. Esto incluye la asignación de recursos adecuados y la monitorización constante.

Conclusiones clave:

Gestión proactiva es clave: La gestión de servidores en un entorno financiero de alta demanda debe ser proactiva y preventiva. Identificar y abordar problemas antes de que se conviertan en interrupciones críticas es fundamental.

Automatización y eficiencia: Utilizar herramientas de automatización para tareas repetitivas y procesos de mantenimiento puede mejorar la eficiencia operativa y reducir errores humanos.

Colaboración interdepartamental: Trabajar en estrecha colaboración con equipos de seguridad, cumplimiento normativo y desarrollo de aplicaciones es esencial para garantizar que las prácticas de TI estén alineadas con los objetivos del negocio.

Planificación de contingencia: Tener planes sólidos de recuperación ante desastres y de alta disponibilidad es esencial para minimizar el tiempo de inactividad y garantizar la continuidad del negocio en caso de fallos críticos.

Actualización constante: Mantener los servidores actualizados con las últimas actualizaciones de seguridad y parches es una parte fundamental de la estrategia de seguridad de la empresa.

7.2 Importancia del administrador de sistemas en el entorno de Windows

La importancia del administrador de sistemas en el entorno de Windows en Morgan Stanley se puede resumir en varios puntos clave que afectan tanto a la eficiencia operativa como a la seguridad de la información en una de las principales instituciones financieras del mundo.

En Morgan Stanley, la infraestructura de TI es esencial para las operaciones diarias y la toma de decisiones financieras. Los administradores de servidores debemos mantener esta infraestructura en funcionamiento y garantizar que las aplicaciones y servicios críticos sean accesibles en todo momento.

La Continuidad del Negocio: Donde se realiza la planificación y ejecución de estrategias de recuperación ante desastres, lo que asegura que Morgan Stanley pueda continuar sus operaciones incluso en situaciones de crisis.

Seguridad de Datos: La seguridad de los datos es de suma importancia, ya que Morgan Stanley maneja información financiera altamente confidencial. Se implementan medidas de seguridad avanzadas, como firewalls, sistemas de detección de intrusiones y políticas de acceso, para proteger contra amenazas cibernéticas y garantizar la integridad de los datos.

Cumplimiento Normativo: La industria financiera está sujeta a estrictas regulaciones. Los administradores de sistemas deben asegurarse de que la infraestructura cumpla con estos requisitos normativos y mantener registros para auditorías.

Optimización de Recursos: Los recursos de TI, incluyendo servidores y almacenamiento, deben utilizarse eficientemente para maximizar el rendimiento y minimizar los costos. Los administradores de sistemas en Windows son responsables de gestionar estos recursos de manera efectiva.

Actualizaciones y Parches: Mantener los sistemas actualizados con las últimas actualizaciones de seguridad y parches es crítico para protegerse contra vulnerabilidades conocidas. Los administradores de sistemas gestionan la aplicación de parches de manera regular.

Automatización y Eficiencia: La automatización de tareas rutinarias y la escritura de scripts pueden mejorar la eficiencia operativa y reducir los errores humanos, lo que es fundamental en un entorno financiero de alta velocidad.

Solución de Problemas: La capacidad de identificar y solucionar problemas técnicos de manera rápida y efectiva es esencial para mantener la continuidad del negocio y la satisfacción del cliente.

Documentación y Registro: Mantener documentación detallada de la configuración de sistemas, políticas y procedimientos es esencial para la resolución eficiente de problemas y la auditoría.

La recomendación que puedo dar en base a mi experiencia es mantenerse siempre actualizado con las nuevas tecnologías, las tendencias al administrar sistemas de Windows incluyen estar capacitado y certificado en Azure cloud, AWS (Amazon Web Services) y GCP (Google Cloud Platform).

Son realmente vitales para muchas organizaciones debido a su capacidad para ofrecer recursos de cómputo, almacenamiento y servicios de TI de manera eficiente, escalable y segura. Materias que facilitaron bastante el aprender estas anteriores plataformas fueron Sistemas Operativos y Administración de Sistemas de Cómputo, ayudaron a establecer las bases para comprender los conceptos y aspectos principales del diseño de los mismos.

8 Bibliografía

Felber, W. (1995). *Linux: Unleashing the Workstation in Your PC.*

Halvorsen, O. H., Clarke, D., & Manning, J. (2011). *OS X and iOS Kernel Programming.*

Mueller, S. (2004). *"Windows Through the Ages" (Windows a través de las edades).* Que Publishing.

Nebbett, G. (2000). *Windows NT/2000 Native API Reference .* New Riders.

Stanley, M. (06 de Febrero de 2023). *Knowledgewebased.* Obtenido de https://knowledgewebase.com/windowserver

Yosifovich, P. (2020). *Windows Internals.*