UNITEQ
INNOVATE

MANUAL DE MANTENIMIENTO PREVENTIVO

Edición Servidores 2024

REALIZADO POR:
Pauletto Giovanni

ÍNDICE

1. Introducción

El mantenimiento preventivo es esencial para asegurar la operación continua y eficiente de los servidores, los cuales son el núcleo de las operaciones tecnológicas de cualquier organización. En UniTeq Innovate, entendemos la importancia de mantener nuestros servidores en óptimas condiciones para prevenir fallos, minimizar tiempos de inactividad y prolongar la vida útil del hardware y software. Este manual ofrece una guía detallada de los pasos y procedimientos necesarios para llevar a cabo un mantenimiento preventivo integral en servidores.

2. Frecuencia de Mantenimiento

El mantenimiento preventivo debe realizarse de manera regular para asegurar la estabilidad y funcionalidad del servidor. Se recomienda llevar a cabo inspecciones básicas semanalmente, tareas más detalladas mensualmente, y revisiones exhaustivas trimestralmente o semestralmente, dependiendo de la criticidad del servidor.

3. Mantenimiento Preventivo de Hardware

3. 1. Inspección Visual

La inspección visual es clave para detectar problemas visibles que podrían afectar el rendimiento del servidor. Antes de empezar, asegúrate de apagar el servidor y desconectarlo de la corriente para tu seguridad. Trabajá en un espacio limpio y bien iluminado para facilitar la tarea.

Primero, abrí el gabinete del servidor sacando los tornillos que lo mantienen en su lugar. Una vez adentro, revisá todos los cables internos para asegurarte de que estén bien conectados y sin signos de desgaste. Mirá los conectores y las tarjetas de expansión para verificar que estén correctamente instalados y sin acumulación de polvo.

No te olvides de chequear los discos duros y otras unidades de almacenamiento. Asegúrate de que estén bien montados en sus bahías y que los cables estén conectados correctamente. También inspeccioná los ventiladores y disipadores de calor: los ventiladores deben girar libremente sin hacer ruidos raros y los disipadores deben estar firmemente sujetos a los procesadores.

Revisá las rejillas de ventilación del gabinete para asegurarte de que no haya obstrucciones que impidan el flujo de aire. Un buen flujo de aire es crucial para evitar el sobrecalentamiento de los componentes.

Finalmente, inspeccioná el estado exterior del gabinete y las conexiones a la red. Buscá daños visibles y asegúrate de que todos los periféricos, como monitores y teclados, estén bien conectados y funcionando.

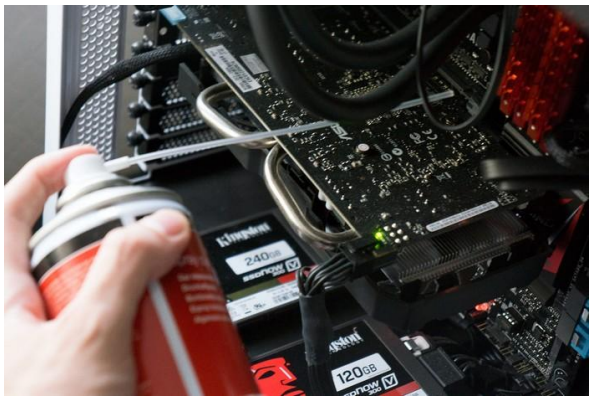
Una vez completada la inspección, volvé a montar el gabinete, reconectá el servidor a la corriente y hacé pruebas para asegurarte de que todo esté funcionando bien.

3. 2. Limpieza física

La limpieza física del servidor es fundamental para mantenerlo en buen estado y prolongar su vida útil. Empezá apagando el servidor y desconectándolo de la corriente para evitar cualquier riesgo eléctrico. Trabajá en un lugar limpio y libre de estática, usando una superficie adecuada para evitar dañar los componentes.

Accedé al interior del servidor sacando la tapa del gabinete. Utilizá aire comprimido para eliminar el polvo acumulado en áreas difíciles de alcanzar, como ventiladores, disipadores de calor y unidades de almacenamiento. Mantené el bote de aire comprimido en posición

vertical y hacé ráfagas cortas para evitar la acumulación de humedad.



Limpiá las superficies externas de los componentes internos con paños anti-estáticos para evitar la electricidad estática. También limpiá el exterior del gabinete con un paño ligeramente húmedo, evitando productos de limpieza agresivos que puedan dañar el acabado.

Después de la limpieza, revisá todos los componentes para asegurarte de que no haya residuos de polvo y que todo esté en su lugar. Volvé a montar el gabinete, reconectá el servidor y hacé pruebas para confirmar que todo funcione bien. Registrá la limpieza realizada y actualizá el historial de mantenimiento.

3. 3. Verificación de Conexiónes

La verificación de conexiones es clave para asegurar que el servidor funcione de manera estable. Apagá el servidor y desconectalo de la corriente antes de comenzar. Trabajá en un lugar limpio y ventilado, usando una superficie antideslizante para evitar daños a los componentes.

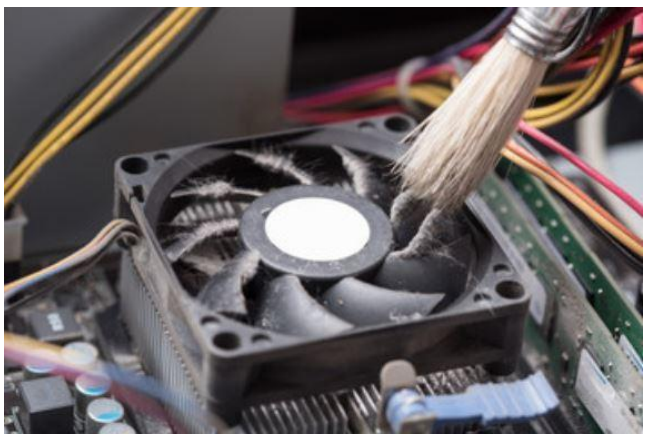
Desmontá el gabinete para acceder a las conexiones internas. Revisá todos los cables internos para asegurarte de que estén bien conectados y sin signos de desgaste. Verificá que los cables de alimentación, cables de red y conexiones internas estén en buen estado.

Usá aire comprimido para limpiar el polvo acumulado en las rejillas y puertos de las unidades de almacenamiento. Asegúrate de que los componentes internos no estén obstruidos por polvo o residuos que puedan afectar su funcionamiento.

Después de la limpieza, volvé a montar el gabinete y reconectá el servidor a la corriente. Encendé el servidor y verificá que todos los componentes funcionen correctamente. Registrá cualquier hallazgo durante la verificación y actualizá el historial de mantenimiento.

3. 4. Comprobación de Componentes de Refrigeración

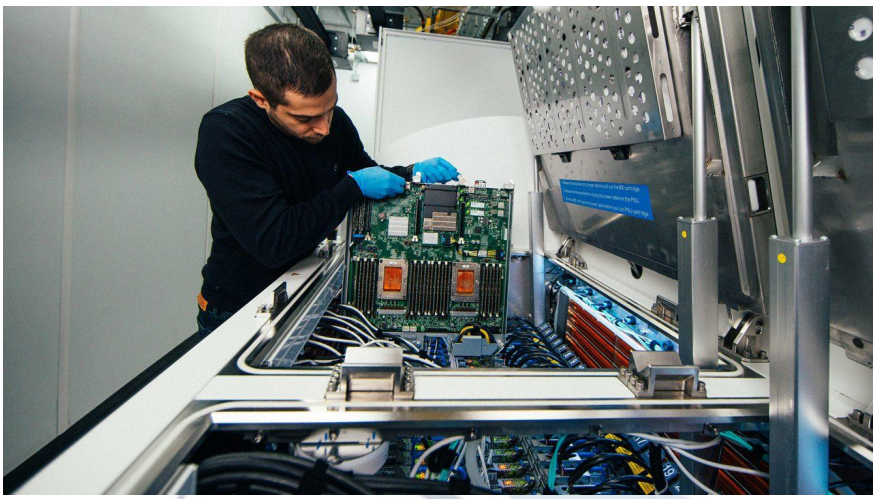
Los componentes de refrigeración son cruciales para mantener la temperatura adecuada en el servidor. Apagá el servidor y desconectalo de la corriente antes de empezar. Abrí el gabinete para acceder a los ventiladores y disipadores de calor.



Verificá que los ventiladores giren libremente al darles un leve empujón manual. Deben girar sin resistencia ni ruidos extraños. Si encontrás algún problema, como ruidos raros, puede ser señal de desgaste o acumulación de polvo.

Chequeá que los disipadores de calor estén bien colocados sobre los procesadores y que no

haya movimiento. También revisá la pasta térmica entre el procesador y el disipador; debe estar en buen estado para asegurar una adecuada transferencia de calor.



Encendé el servidor y observá el funcionamiento de los ventiladores. Usá herramientas de software para monitorear las temperaturas de los componentes críticos y asegurarte de que no haya sobrecalentamiento. Si encontrás ventiladores defectuosos, reemplazalos y programá revisiones periódicas para evitar problemas futuros.

3. 5. Verificación del Estado de las Fuentes de Alimentación

La fuente de alimentación es un componente crítico que debe operar dentro de los parámetros especificados. Apagá el servidor y desconectalo de la corriente para trabajar de forma segura. Accedé a la fuente de alimentación retirando la tapa del gabinete.

Hacé una inspección visual para identificar signos de daño, como abolladuras o acumulación de polvo en las rejillas de ventilación. Verificá que todos los cables de alimentación estén correctamente conectados y sin cables sueltos.

Revisá la etiqueta de especificaciones para confirmar que la fuente de alimentación esté funcionando dentro de los parámetros recomendados. Si tiene un ventilador incorporado,

escuchá su funcionamiento para asegurarte de que gire suavemente y sin ruidos raros.

Usá un multímetro para medir los voltajes de salida y verificá que estén dentro de las tolerancias especificadas. Revisá todos los rails de voltaje para confirmar que estén operando correctamente. También chequeá la temperatura de la fuente de alimentación para asegurarte de que no esté sobrecalentada y limpiá cualquier acumulación de polvo en las rejillas de ventilación.

Si encontrás problemas con la fuente de alimentación, considerá reemplazarla por una nueva que cumpla con las especificaciones adecuadas. Registrá todo y actualizá el historial de mantenimiento para un seguimiento adecuado.

4. Mantenimiento Preventivo de Software

4. 1. Actualizaciones de Software y Firmware

Para asegurar el funcionamiento óptimo del servidor, es esencial instalar todas las actualizaciones de software y firmware recomendadas por los proveedores del hardware y el

software. Este proceso abarca la aplicación de parches de seguridad y actualizaciones del sistema operativo.

Preparativos Iniciales: Antes de comenzar con las actualizaciones, realiza un respaldo completo del sistema y de los datos importantes para prevenir la pérdida de información en caso de que surjan problemas durante el proceso. Es fundamental revisar la documentación proporcionada por los proveedores para entender las nuevas características, correcciones de errores y posibles impactos de las actualizaciones.

Actualización del Sistema Operativo: Para iniciar, accede al gestor de actualizaciones del sistema operativo y verifica las actualizaciones disponibles. En sistemas basados en Ubuntu, por ejemplo, puedes usar los comandos sudo apt update y sudo apt upgrade. Luego, procede a instalar las actualizaciones, siguiendo las recomendaciones del proveedor para asegurar una instalación correcta. Algunas actualizaciones pueden requerir el reinicio del servidor, por lo que es importante planificarlo en un momento que minimice el impacto en los usuarios y servicios.

Actualización de Software de Aplicación: Revisa si hay actualizaciones disponibles para el

software de aplicación en el servidor, como bases de datos o servidores web. Descarga e instala las actualizaciones siguiendo las instrucciones del proveedor. Después de la actualización, verifica que todas las aplicaciones funcionen correctamente.

Actualización del Firmware: Descarga las últimas versiones del firmware desde el sitio web del fabricante del hardware, asegurándote de seleccionar la versión adecuada para tu modelo de servidor. Lee las instrucciones proporcionadas para la actualización, que pueden incluir la preparación de medios de instalación como una unidad USB. Sigue las instrucciones para aplicar el firmware, ya sea a través de una herramienta específica del fabricante o la interfaz de configuración del servidor. Finalmente, verifica que el servidor se inicie correctamente y que el nuevo firmware esté instalado y funcionando.

4. 2. Gestión de Almacenamiento y Backup

Para mantener la integridad de los datos en el servidor, realiza un análisis para confirmar que los archivos críticos del sistema y las aplicaciones no estén corruptos o dañados. Utiliza herramientas específicas para verificar la integridad de archivos y bases de datos, y ejecuta herramientas de chequeo de sistemas de archivos para detectar y corregir errores en los discos duros.

Revisión y Configuración de Políticas de Backup: Verifica que las políticas de backup estén actualizadas y adecuadas para las necesidades del servidor. Esto incluye la frecuencia de los backups y los procedimientos para la recuperación. Asegúrate de que los backups se realicen de acuerdo con el cronograma establecido, ya sea diario, semanal o mensual, dependiendo de la criticidad de los datos.

Ejecución de Backups: Realiza las copias de seguridad según el plan establecido, asegurándote de que se realicen tanto los backups completos como los incrementales o diferenciales. Verifica que el proceso de backup haya finalizado correctamente revisando los logs y resolviendo cualquier error o advertencia.

Almacenamiento Seguro de Backups: Asegúrate de que los backups se almacenen en ubicaciones seguras y accesibles, como discos duros externos, servidores de backup dedicados o servicios de almacenamiento en la nube. Implementa medidas de seguridad para proteger los backups, como cifrado de datos y controles de acceso, y asegura que existan copias redundantes en ubicaciones físicas separadas para prevenir la pérdida de datos en caso de desastre.

Realiza pruebas periódicas de restauración para confirmar que los backups sean funcionales y que los datos puedan ser recuperados correctamente. Realiza restauraciones en un entorno de prueba para evitar afectar el servidor en producción, y documenta los resultados de estas pruebas.

4. 3. Optimización del Rendimiento

Desfragmentación de Discos: Utiliza herramientas de desfragmentación para analizar el estado de los discos duros y determinar el nivel de fragmentación. En sistemas Windows,

puedes usar el Desfragmentador de disco; en sistemas Linux, herramientas como e4defrag son adecuadas para sistemas de archivos ext4. Ejecuta el proceso de desfragmentación para reorganizar los archivos en el disco, reduciendo el tiempo de acceso a los datos y mejorando el rendimiento del sistema.

Limpieza de Archivos Temporales: Identifica y clasifica los archivos temporales y cachés acumulados en el sistema, incluyendo archivos del sistema, cachés del navegador y registros antiguos. Utiliza herramientas de limpieza de disco, como Disk Cleanup en Windows o bleachbit en Linux, para eliminar estos archivos de manera segura. Configura el sistema para realizar limpiezas automáticas en intervalos regulares.

Revisión del Uso de Recursos: Utiliza herramientas de monitoreo del sistema, como top o htop en Linux y el Administrador de Tareas en Windows, para revisar el uso de CPU, memoria y disco. Identifica procesos que consumen una cantidad excesiva de recursos y ajusta la configuración del sistema y los servicios para optimizar el uso de recursos.

Actualización y Mantenimiento de Software: Asegúrate de que todas las aplicaciones y servicios del servidor estén actualizados a sus versiones más recientes, ya que las actualizaciones suelen incluir mejoras de rendimiento y corrección de errores.

Revisión de la Configuración del Sistema: Revisa los servicios y aplicaciones que se inician automáticamente al arrancar el servidor, desactivando aquellos innecesarios para reducir el tiempo de arranque y liberar recursos.

4. 4. Verificación de Seguridad

Revisión de Configuraciones de Seguridad del Firewall: Revisa las reglas actuales del firewall para asegurarte de que solo se permitan las conexiones necesarias y se bloqueen las no autorizadas. Ajusta las reglas para bloquear puertos o servicios innecesarios y permitir el tráfico legítimo. Realiza pruebas para asegurarte de que las reglas del firewall funcionen correctamente y utilice herramientas de escaneo de puertos y pruebas de penetración para validar la configuración.

Revisión y Actualización de Políticas de Acceso: Verifica los permisos de acceso de los usuarios y grupos, asegurándote de que solo tengan acceso a los recursos necesarios. Revisa y actualiza las políticas de contraseñas para cumplir con las mejores prácticas de seguridad.

Verificación de Sistemas de Detección y Prevención de Intrusiones: Revisa la configuración del sistema de detección y prevención de intrusiones (IDS/IPS) para asegurarte de que esté correctamente configurado. Monitorea los registros y alertas del IDS/IPS para identificar patrones inusuales o intentos de intrusión, y actualiza las firmas y reglas de detección para proteger contra amenazas recientes.

Actualización de Software de Seguridad: Asegúrate de que todos los parches de seguridad y actualizaciones del software de seguridad estén instalados. Revisa y ajusta la configuración del software de seguridad para proporcionar la máxima protección,

configurando opciones como escaneos periódicos y protecciones en tiempo real.

4. 5. Revisión de Hardware y Componentes

Monitoreo del Estado de los Componentes: Utiliza herramientas de monitoreo para revisar el estado de los componentes críticos del hardware, como la temperatura del procesador, el uso del disco y el estado de la fuente de alimentación. Configura alertas para recibir notificaciones sobre posibles problemas de hardware, como temperaturas elevadas o fallos en los discos duros.

Pruebas de Rendimiento del Hardware: Realiza pruebas de rendimiento para evaluar la funcionalidad de los componentes de hardware. Utiliza herramientas de benchmarking y pruebas de estrés para comprobar el rendimiento del procesador, la memoria y los discos duros. Analiza los resultados para identificar cualquier componente que pueda estar funcionando por debajo de sus especificaciones.

5. Registro y Documentación de Mantenimiento

Para asegurar el buen funcionamiento del servidor, es fundamental documentar todas las actividades de mantenimiento, tanto de hardware como de software. Este registro debe incluir detalles de cada tarea realizada, como actualizaciones de software, reemplazos de hardware, backups, y cualquier problema detectado y resuelto. Mantener un historial

completo y organizado permite un mejor seguimiento y planificación de futuras intervenciones, garantizando que el servidor opere siempre de manera eficiente y segura.

6. Conclusiones y Recomendaciones

El mantenimiento preventivo es esencial para asegurar que los servidores sean confiables y tengan una larga vida útil. En UniTeq Innovate, aconsejamos seguir las pautas detalladas en esta guía y llevar a cabo revisiones regulares.

Es importante realizar revisiones periódicas para ajustar las estrategias de mantenimiento según las necesidades del servidor y los avances tecnológicos. De esta manera, se pueden anticipar posibles problemas y evitar fallos que podrían afectar el rendimiento del sistema.

A medida que la tecnología avanza, las necesidades de los servidores también cambian. Por eso, es clave estar atentos a las nuevas tendencias y adaptarse a ellas, actualizando las prácticas de mantenimiento cuando sea necesario. Con un enfoque cuidadoso y proactivo, los servidores pueden mantenerse en un estado óptimo, asegurando su rendimiento y seguridad a lo largo del tiempo.