

Resolución de incidencias y asistencia técnica (Implantación de sistemas operativos)

Interpretación, análisis y elaboración de documentación técnica

Durante el proceso de administración de los sistemas hay que documentar los pasos que se van realizando, señalando las incidencias que van surgiendo, documentar las cosas es una buena práctica y ayuda a otras personas y a nosotros a saber qué es lo que se ha hecho con un equipo o qué configuración se ha utilizado, también controlar los tiempos dedicados a cada paso y las incidencias en el caso de que aparezcan.

Interpretación, análisis y elaboración de manuales de instalación y configuración de sistemas operativos y aplicaciones

La interpretación, análisis y elaboración de manuales de instalación y configuración de sistemas operativos y aplicaciones son componentes críticos en el contexto de la resolución de incidencias y asistencia técnica durante la implantación de sistemas operativos. Estos manuales proporcionan instrucciones detalladas sobre cómo instalar, configurar y mantener sistemas operativos y aplicaciones, lo

que ayuda a garantizar que se implementen de manera adecuada y eficiente en el entorno de la organización. Aquí se detalla cómo estos manuales son fundamentales para el proceso de resolución de incidencias y asistencia técnica:

1. **Interpretación de manuales:** Los técnicos de soporte y administradores de sistemas deben ser capaces de interpretar y comprender correctamente los manuales de instalación y configuración proporcionados por los fabricantes de sistemas operativos y aplicaciones. Esto implica leer y comprender el contenido técnico y las instrucciones proporcionadas, así como identificar los pasos necesarios para llevar a cabo tareas específicas de instalación, configuración o solución de problemas.
2. **Análisis de manuales:** Además de comprender el contenido de los manuales, los técnicos también deben ser capaces de analizar críticamente la información proporcionada y evaluar su relevancia y aplicabilidad en el contexto de la implantación de sistemas operativos. Esto implica identificar los requisitos del sistema, las configuraciones recomendadas, los pasos de solución de problemas y las mejores prácticas presentadas en los manuales, y determinar cómo aplicar esta información de manera efectiva en situaciones reales.
3. **Elaboración de manuales:** En algunos casos, los técnicos pueden necesitar elaborar manuales de instalación y configuración personalizados para satisfacer las necesidades específicas de la organización o documentar procedimientos internos. Esto implica recopilar información técnica relevante, escribir instrucciones claras y concisas, y organizar el contenido de manera lógica y coherente para facilitar su comprensión y uso por parte de otros miembros del equipo de soporte.
4. **Resolución de incidencias:** Los manuales de instalación y configuración son herramientas valiosas para la resolución de incidencias, ya que proporcionan

procedimientos detallados para diagnosticar y solucionar problemas comunes que pueden surgir durante la implantación de sistemas operativos y aplicaciones. Los técnicos pueden utilizar estos manuales para identificar la causa raíz de una incidencia, seguir pasos de solución de problemas recomendados y restaurar el funcionamiento normal del sistema lo más rápido posible.

5. **Asistencia técnica:** Los manuales de instalación y configuración también son recursos útiles para proporcionar asistencia técnica a los usuarios finales y otros miembros del personal de la organización. Los técnicos pueden utilizar estos manuales para guiar a los usuarios a través del proceso de instalación, configuración y solución de problemas, proporcionando instrucciones paso a paso y consejos útiles para maximizar la eficiencia y minimizar los tiempos de inactividad.

Licencias de cliente y licencias de servidor

Las licencias de cliente y licencias de servidor son elementos fundamentales en el ámbito de la implantación de sistemas operativos y la gestión de infraestructuras de TI. Estas licencias establecen los términos y condiciones para el uso legal y adecuado de los sistemas operativos y software en un entorno empresarial. Aquí se detallan las características y consideraciones clave relacionadas con las licencias de cliente y servidor:

Licencias de Cliente:

1. **Definición:** Las licencias de cliente se refieren a los permisos otorgados a los usuarios o dispositivos individuales para acceder y utilizar un software o

sistema operativo en un entorno de red. Estas licencias suelen ser necesarias para cada dispositivo o usuario que acceda al software o sistema operativo.

2. **Tipos:** Las licencias de cliente pueden ser de varios tipos, incluyendo licencias por usuario, que permiten a un usuario específico acceder al software desde múltiples dispositivos, y licencias por dispositivo, que permiten a un dispositivo específico acceder al software con múltiples usuarios.
3. **Modelos de licenciamiento:** Existen diferentes modelos de licenciamiento para las licencias de cliente, como el licenciamiento por volumen, que permite adquirir un gran número de licencias a un precio reducido, y el licenciamiento por suscripción, que permite acceder al software durante un período de tiempo determinado a cambio de una tarifa periódica.
4. **Gestión y cumplimiento:** Es crucial gestionar adecuadamente las licencias de cliente para garantizar el cumplimiento de los términos y condiciones establecidos por el fabricante del software. Esto incluye llevar un registro preciso de las licencias adquiridas, asignarlas correctamente a usuarios o dispositivos autorizados y realizar auditorías periódicas para verificar el cumplimiento.

Licencias de Servidor:

1. **Definición:** Las licencias de servidor se refieren a los permisos otorgados para instalar y ejecutar un software o sistema operativo en un servidor físico o virtual. Estas licencias suelen ser necesarias para cada instancia del software que se ejecute en un servidor.
2. **Tipos:** Las licencias de servidor pueden variar dependiendo del tipo de servidor y del software que se esté utilizando. Algunos ejemplos comunes incluyen licencias de servidor de aplicaciones, licencias de

servidor de bases de datos y licencias de servidor de sistemas operativos.

3. **Modelos de licenciamiento:** Al igual que con las licencias de cliente, existen diferentes modelos de licenciamiento para las licencias de servidor. Esto puede incluir licenciamiento por núcleo de CPU, licenciamiento por usuario o dispositivo, y licenciamiento por capacidad o uso del servidor.
4. **Virtualización y licenciamiento:** En entornos de virtualización, es importante tener en cuenta cómo se licencia el software en servidores virtuales. Algunos fabricantes ofrecen políticas de licenciamiento específicas para entornos virtualizados, que pueden variar dependiendo del proveedor y el tipo de software.
5. **Gestión y cumplimiento:** Al igual que con las licencias de cliente, es esencial gestionar y mantener un registro preciso de las licencias de servidor para garantizar el cumplimiento de los términos y condiciones establecidos por el fabricante del software. Esto incluye asegurarse de que se adquieran las licencias adecuadas para el número de instancias de software que se ejecutan en los servidores de la organización.

Instalaciones desatendidas

Las instalaciones desatendidas son un método eficiente y automatizado para implementar sistemas operativos y software en múltiples dispositivos sin requerir la intervención manual del usuario durante el proceso de instalación. Este enfoque es especialmente útil en entornos empresariales donde se necesitan desplegar grandes cantidades de sistemas operativos y aplicaciones de manera rápida y consistente. Aquí se presentan las características y beneficios clave de las instalaciones desatendidas:

1. **Automatización del proceso de instalación:** Las

instalaciones desatendidas permiten automatizar todo el proceso de instalación, desde la configuración del sistema operativo hasta la instalación de controladores y aplicaciones adicionales. Esto elimina la necesidad de intervención manual durante la instalación, lo que ahorra tiempo y reduce los errores humanos.

2. **Personalización y configuración predeterminada:** Con las instalaciones desatendidas, es posible personalizar y configurar de antemano todas las opciones de instalación, como la configuración regional, las preferencias de idioma, las opciones de red y las configuraciones de seguridad. Esto garantiza que todos los dispositivos se configuren de manera consistente y cumplan con los estándares de la organización.
3. **Flexibilidad y escalabilidad:** Las instalaciones desatendidas son altamente flexibles y escalables, lo que permite desplegar sistemas operativos y software en una amplia variedad de dispositivos, incluidos equipos de escritorio, servidores y dispositivos móviles. Además, este enfoque puede adaptarse fácilmente para satisfacer las necesidades cambiantes de la organización y escalar según sea necesario.
4. **Reducción de costos y tiempos de implementación:** Al eliminar la necesidad de intervención manual durante el proceso de instalación, las instalaciones desatendidas pueden reducir significativamente los costos operativos y los tiempos de implementación. Esto permite a las organizaciones desplegar sistemas operativos y aplicaciones de manera más rápida y eficiente, lo que aumenta la productividad y minimiza los tiempos de inactividad.
5. **Repetibilidad y consistencia:** Al utilizar instalaciones desatendidas, se garantiza que todas las implementaciones se realicen de manera consistente y reproducible, independientemente del número de dispositivos o la ubicación geográfica. Esto ayuda a mantener la coherencia en toda la infraestructura de TI

y facilita la administración y el soporte continuo de los sistemas operativos y aplicaciones.

6. Soporte para la automatización de tareas posteriores:

Además de la instalación inicial del sistema operativo y software, las instalaciones desatendidas también pueden incluir la automatización de tareas posteriores, como la configuración de políticas de grupo, la instalación de actualizaciones de seguridad y la aplicación de parches de software. Esto garantiza que los dispositivos se mantengan actualizados y seguros después de la instalación inicial.

Más información

- <https://www.jesusninoc.com/05/02/instalacion-en-red-sistemas-operativos-en-red/>
-

Implementación de ficheros de respuestas

La implementación de archivos de respuestas es una técnica comúnmente utilizada en el despliegue automatizado de sistemas operativos y aplicaciones. Estos archivos, también conocidos como archivos de respuesta o archivos de configuración automatizada, contienen información predefinida que guía el proceso de instalación, permitiendo una implementación más rápida y eficiente. Aquí se describen las características y beneficios clave de la implementación de archivos de respuestas:

1. **Automatización del proceso de instalación:** Los archivos de respuestas automatizan el proceso de instalación al proporcionar respuestas predefinidas a las preguntas que normalmente se presentarían durante una instalación manual. Esto elimina la necesidad de intervención humana durante la instalación, lo que ahorra tiempo y reduce los errores.
2. **Personalización y configuración predeterminada:** Los archivos de respuestas permiten personalizar y configurar de antemano todas las opciones de instalación, como la configuración regional, las preferencias de idioma, las opciones de red y las configuraciones de seguridad. Esto garantiza que todos los dispositivos se configuren de manera consistente y cumplan con los estándares de la organización.
3. **Flexibilidad y escalabilidad:** La implementación de archivos de respuestas es altamente flexible y escalable, lo que permite desplegar sistemas operativos y aplicaciones en una amplia variedad de dispositivos y entornos. Además, este enfoque puede adaptarse fácilmente para satisfacer las necesidades cambiantes de la organización y escalar según sea necesario.
4. **Repetibilidad y consistencia:** Al utilizar archivos de respuestas, se garantiza que todas las implementaciones se realicen de manera consistente y reproducible, independientemente del número de dispositivos o la ubicación geográfica. Esto ayuda a mantener la coherencia en toda la infraestructura de TI y facilita la administración y el soporte continuo de los sistemas operativos y aplicaciones.
5. **Reducción de errores y tiempos de implementación:** Al eliminar la necesidad de intervención manual durante el proceso de instalación, la implementación de archivos de respuestas puede reducir significativamente los errores humanos y los tiempos de implementación. Esto permite a las organizaciones desplegar sistemas operativos y aplicaciones de manera más rápida y eficiente, lo que

aumenta la productividad y minimiza los tiempos de inactividad.

6. Soporte para la automatización completa del despliegue:

Además de la instalación inicial del sistema operativo y las aplicaciones, la implementación de archivos de respuestas también puede incluir la automatización de tareas posteriores, como la configuración de políticas de grupo, la instalación de actualizaciones de seguridad y la aplicación de parches de software. Esto garantiza que los dispositivos se mantengan actualizados y seguros después de la instalación inicial.

Más información

- <https://www.jesusninoc.com/05/02/instalacion-en-red-sistemas-operativos-en-red/>
-

Servidores de actualizaciones automáticas

Cada día aparecen nuevas vulnerabilidades en los sistemas operativos y en los programas, es importante mantener el sistema operativo actualizado con los últimos parches de seguridad.

Las actualizaciones sirven para evitar problemas o corregirlos, de esta forma el sistema operativo se mantiene seguro, las actualizaciones son importantes y necesarias para los sistemas operativos.

Los sistemas de gestión de actualizaciones permiten que las

actualizaciones se descarguen y se instalen con orden, de no ser así puede suponer un problema si el sistema operativo comienza a descargar todas las actualizaciones a la vez y en algunos casos pueden llegar a saturar ciertos recursos como por ejemplo la conexión de red, para resolver este problema algunos sistemas operativos tienen programas que descargan las actualizaciones y las envían a otros ordenadores a la red de una manera ordenada.

Partes de incidencias

Las incidencias, en el contexto de la gestión de servicios de TI, son eventos no planificados que interrumpen o reducen la calidad de los servicios de TI. Las partes de una incidencia son los componentes fundamentales que ayudan a gestionar y resolver de manera efectiva estos eventos. Aquí se detallan las partes principales de una incidencia:

1. **Título o Asunto:** El título o asunto de una incidencia proporciona una descripción concisa y clara del problema que se está experimentando. Debe ser lo suficientemente descriptivo como para identificar el problema, pero también breve y fácil de entender.
2. **Descripción:** La descripción de la incidencia proporciona detalles adicionales sobre el problema reportado. Esto puede incluir información como la naturaleza del problema, los síntomas observados, cualquier mensaje de error recibido y cualquier acción realizada antes de que ocurriera la incidencia.
3. **Prioridad:** La prioridad de una incidencia indica la importancia relativa del problema y su impacto en las operaciones comerciales. Las prioridades suelen clasificarse en categorías como crítico, alto, medio o bajo, y ayudan a determinar el orden en que se deben abordar las incidencias.
4. **Impacto:** El impacto de una incidencia describe el efecto

que tiene el problema en el negocio o en los usuarios finales. Esto puede incluir la cantidad de usuarios afectados, el tiempo de inactividad asociado, el impacto en la productividad y cualquier pérdida de datos o ingresos.

5. **Urgencia:** La urgencia de una incidencia indica la rapidez con la que se necesita una solución. Se basa en la necesidad de restaurar el servicio afectado y puede influir en la priorización de la incidencia y en los plazos de resolución.
6. **Estado:** El estado de una incidencia refleja su situación actual en el proceso de gestión de incidencias. Los estados comunes incluyen «abierta», «en curso», «pendiente de usuario», «resuelta» y «cerrada». El estado proporciona visibilidad sobre el progreso de la resolución de la incidencia.
7. **Asignación:** La asignación de una incidencia indica quién es el responsable de gestionar y resolver el problema. Esto puede ser un técnico de soporte, un equipo de respuesta a incidencias o cualquier otro miembro del personal capacitado para abordar el problema.
8. **Registro de Actividades:** El registro de actividades documenta todas las acciones realizadas en relación con la incidencia, incluyendo las investigaciones realizadas, las soluciones probadas, las comunicaciones con el usuario y cualquier cambio en el estado de la incidencia.
9. **Comentarios y Actualizaciones:** Los comentarios y actualizaciones proporcionan una forma de comunicación entre los técnicos de soporte y los usuarios afectados. Esto puede incluir actualizaciones sobre el progreso de la resolución de la incidencia, solicitudes de información adicional y agradecimientos por la cooperación del usuario.

Más información

- <https://www.jesusninoc.com/05/02/instalacion-en-red-sistemas-operativos-en-red/>

Protocolos de actuación

Los protocolos de actuación son conjuntos de procedimientos y pautas diseñados para guiar la respuesta a diferentes tipos de situaciones o eventos. Estos protocolos establecen pasos específicos a seguir, roles y responsabilidades, y líneas de comunicación para garantizar una respuesta rápida, coordinada y eficiente ante una variedad de escenarios. Los protocolos de actuación pueden abordar una amplia gama de situaciones, desde emergencias y crisis hasta incidentes operativos y de seguridad. Su objetivo principal es minimizar el impacto negativo de los eventos adversos y facilitar la recuperación rápida y efectiva de las operaciones normales. Estos protocolos suelen ser desarrollados por equipos multidisciplinarios que incluyen a personal de diferentes áreas de la organización, como TI, seguridad, gestión de crisis y comunicaciones. Una vez establecidos, los protocolos de actuación deben ser revisados y actualizados periódicamente para garantizar su relevancia y efectividad en respuesta a los cambios en el entorno operativo y las nuevas amenazas o riesgos emergentes.

Más información

- <https://www.jesusninoc.com/05/02/instalacion-en-red-sistemas-operativos-en-red/>
-

Administración remota

Los sistemas operativos se pueden administrar de forma local y remota, gracias a la red se puede acceder a ordenadores sin necesidad de estar físicamente sentado delante de los mismos, para ello se necesitan herramientas, algunas herramientas (programas) están disponibles en modo texto y otras en modo gráfico.

Una operación de administración remota puede ser cualquier tarea que se realice en un sistema operativo como por ejemplo agregar y eliminar software, actualizar el sistema operativo, controlar procesos y servicios, crear tareas programadas, control de usuarios, encender y apagar equipos, etc.

Todas estas tareas que acabamos de ver se pueden realizar remotamente, en este capítulo hablaremos de dos de las principales operaciones de administración remota: el acceso remoto y la instalación de software, brevemente diremos algo de las dos:

- **Acceso remoto:** Consiste en acceder remotamente al escritorio de otro equipo, este tipo de acceso se basa en el sistema cliente-servidor, por lo tanto es necesario tener instalado un servicio de acceso remoto al que se puedan conectar clientes.
- **Instalación remota de software:** Consiste en realizar instalaciones utilizando la red, en este bloque también podemos meter las actualizaciones remotas del sistema operativo y programas.

Las herramientas que sirven para realizar accesos e instalaciones remotas lo hacen a través de protocolos, algunos de los más conocidos son: Telnet (TELEcommunication NETwork), SSH (Secure SHell), RDP (Remote Desktop Protocol), etc.

Principales protocolos que se utilizan para realizar accesos e instalaciones remotas:

- **Telnet** es un protocolo que funciona en el puerto 23, es un protocolo que se utilizó mucho en el pasado y que en la actualidad se utiliza poco por ser inseguro. El funcionamiento de este protocolo es simple, un cliente se conecta a una máquina remota (con el nombre del equipo o la IP) y mediante el usuario y una contraseña se accede, esta comunicación no se cifra y por eso decimos que es inseguro.
- **SSH** o intérprete de comandos seguro es un protocolo que permite conexiones cifradas desde un cliente a un servidor, el cifrado se realiza con algoritmos RSA aunque también se puede hacer con otros algoritmos. La conexión se realiza a través del puerto 22, además de la conexión en sí, este protocolo también ofrece otros servicios como por ejemplo la transmisión de ficheros. El funcionamiento de este protocolo consiste en que el cliente inicia una conexión al puerto 22 del servidor que tiene SSH, el servidor envía su clave al cliente, el cliente la compara con la lista de claves que tiene y si es la primera vez, es el usuario el que dice si es correcta la clave o no, después el cliente genera otra clave de sesión que se la envía al servidor dentro de un paquete cifrado la clave del servidor, a partir de este momento ya se ha establecido la comunicación cifrada.
- **RDP** es un protocolo de escritorio remoto que permite el acceso remoto a ordenadores con el sistema operativo Windows, el puerto que utiliza para realizar la conexión es el 3389. El funcionamiento consiste en que un cliente envía una petición al servidor y accede por ejemplo al

escritorio del servidor.

Acceso remoto

El acceso remoto consiste en la comunicación entre servidor y clientes, al servidor se conectan los clientes. Para conectar un cliente con un servidor lo único que necesita es conocer el puerto y el nombre del equipo o la dirección IP. El acceso de los cliente se hace utilizando usuarios por lo tanto es necesario que el usuario tenga permiso para acceder al servidor.

El funcionamiento de los accesos remotos en modo texto se realiza a través de las líneas de comando, en el caso del modo gráfico hay varios métodos aunque uno de ellos es enviar un fichero con la imagen de la pantalla del servidor, cada vez que se realiza un movimiento, se pulsa una tecla o un botón, se envían las coordenadas al servidor.

Una de las características que tienen los accesos remotos es que a un servidor de acceso remoto en Linux se puede conectar un cliente remoto desde Windows y lo mismo a la inversa, es decir que los ordenador no tienen porqué tener el mismo sistema operativo.

Ejemplos

Instalar y ejecutar SSH para PowerShell

- <https://www.jesusninoc.com/03/11/ejercicios-de-powershell-ssh/>

Conexión después de haber desconectado y quitado el módulo Posh-SSH (hay que volver a importar)

- <https://www.jesusninoc.com/03/11/ejercicios-de-powershell-ssh/>

Ejemplo: obtener información sobre la versión de Linux

- <https://www.jesusninoc.com/03/11/ejercicios-de-powershell-ssh/>

JuiceSSH – SSH Client

- <https://play.google.com/store/apps/details?id=com.sonelli.juicessh>

JuiceSSH Performance Plugin

- <https://play.google.com/store/apps/details?id=com.sonelli.juicessh.performancemonitor>

Instalación remota de software

En cualquier sistema operativo surge la necesidad de instalar nuevos programas, en el caso de los sistemas operativos en red además de instalar nuevos programas localmente, también disponen de herramientas que permiten instalar remotamente programas en otros ordenadores de la red.