Gestión de recursos tecnológicos

Breve descripción:

A través de este componente formativo, el aprendiz debe apropiar los elementos y conceptos necesarios para la gestión de los recursos tecnológicos, empleando herramientas de administración y monitoreo.

Octubre 2023

Tabla de contenido

Introducción 1

1. Conceptos básicos de la supervisión de redes 3

1.1. ¿Qué es el monitoreo de red? 3

Características de un "software" de monitorización de red eficaz 8

1.2. ¿Qué es la gestión de redes? 9

1.3. Gestión del rendimiento de la red 10

2. Herramientas de monitoreo de red 11

¿Cómo se debe seleccionar una herramienta de monitoreo de red? 11

2.1. ¿Qué es el monitoreo de red en tiempo real? 16

2.2. ¿Qué es la gestión de servidores? 16

2.3. ¿Qué es SNMP? 17

3. Gestión de servidor virtual 18

3.1. ¿Qué es la gestión de servidores virtuales? 18

3.2. ¿Qué es la supervisión de red sin agentes? 20

Síntesis 25

Material complementario 26

Glosario 27

Referencias bibliográficas 28

Créditos.....29

Introducción

Para comenzar con el estudio de la temática del componente formativo, lo invitamos a ver el siguiente video.

Video 1. Gestión de recursos tecnológicos

Enlace de reproducción del video

Síntesis del video: Gestión de recursos tecnológicos
Los recursos tecnológicos de cualquier organización, constituyen uno de los activos más importantes en cualquier empresa u organización, por lo tanto, es de suma importancia la prevención y el cuidado de todos aquellos elementos que conforman dichos recursos, debido a que son ellos, quienes otorgan la capacidad de

comunicar y administrar la información necesaria, para el libre y oportuno desarrollo de los procesos que ocurren al interior de la empresa.

Además, el constante avance de la tecnología obliga a que las organizaciones estén actualizándose periódicamente para sobresalir en sus respectivos nichos comerciales.

1. Conceptos básicos de la supervisión de redes

Partamos de la premisa de que una red de datos es tan sólida como su eslabón más débil y, en general, la capa 2 del modelo OSI se presenta como ese eslabón en las redes de datos. Esto representa para el administrador de la red un reto específico en la labor de monitoreo.

La monitorización de redes informáticas ha surgido como una norma obligatoria para mantener en óptimas condiciones este recurso tecnológico. Supervisar la red de datos es un proceso, mediante el cual los encargados escudriñan periódicamente componentes tales como enrutadores, conmutadores, servidores, etc., en busca de posibles fallos de funcionamiento que puedan distorsionar las tareas fundamentales de la red de información.

1.1. ¿Qué es el monitoreo de red?

Consiste en el proceso permanente de vigilancia al funcionamiento de la red, empleando herramientas como "software" de monitoreo, encargados de buscar fallos en la red con proactividad, debido a que es de suma importancia detectarlos tempranamente o de ser posible, antes que ocurran. Así, los tiempos de réplica ante una eventualidad, pueden ser ampliamente reducidos, lo que genera mayor disponibilidad de los servicios ofrecidos por la red, al mismo tiempo que la reducción de costos económicos.

En la planificación del proceso de monitoreo de red, es importante tener en cuenta:

a. **Seguimiento de lo esencial.** En una supervisión de red adecuada se deben establecer los dispositivos y las métricas de rendimiento relacionadas que serán supervisadas, para seguidamente proceder a decretar los tiempos de rastreo. El rendimiento de la red puede verse reducido o comprometido por todos aquellos elementos que presenten alguna falla. De ahí la importancia de la detección temprana de las falencias funcionales (proactividad), que se puede lograr con la programación periódica de un monitoreo exhaustivo. Los servidores, enrutadores y conmutadores representan la columna vertebral de la red, lo que significa que son los dispositivos que requieren de manera inmediata y esencial la monitorización de su comportamiento y funcionalidad, a la par que algunos otros dispositivos de la red no son críticos para su funcionamiento, lo que significa que no es necesario invertir tanto tiempo y recursos en su supervisión, por ejemplo, los computadores de escritorio, portátiles e impresoras hacen parte de este grupo.

b. **Intervalo de seguimiento.** El intervalo de monitoreo determina la frecuencia con la que se sondean los dispositivos de red y sus métricas relacionadas para identificar el estado de rendimiento y disponibilidad. La ordenación de los tiempos en los cuales se monitorea la red ayuda a sobrellevar la carga del sistema y aligerar recursos.

   El lapso establecido de monitoreo para un determinado elemento de la red depende del elemento en sí y de los parámetros a supervisar. La disponibilidad de cierto dispositivo debe monitorearse en la menor cantidad de tiempo posible periódicamente, pero sin abusar del recurso

tiempo, es decir, entre menos tiempo pase entre un monitoreo y otro, mejor; pero, tampoco es práctico monitorear en intervalos de tiempo demasiado cortos pues esto significa que se está relegando otros dispositivos y consumiendo demasiados recursos en la monitorización. Los dispositivos no críticos pueden ser verificados a intervalos amplios de tiempo, mientras que los críticos deben tener intervalos más cortos.

c. **Protocolo y sus tipos.** Es indispensable implementar o adoptar protocolos seguros y de bajo consumo de recursos a la hora de iniciar un proceso de monitoreo, pues el protocolo en sí también consumirá ancho de banda, un preciado recurso en la transmisión de datos. El protocolo SNMP ("Simple Network Management Protocol") es uno de los ampliamente aceptados y difundidos por los administradores de redes informáticas para tareas de administración y control, así como el protocolo Syslog y NetFlow, protocolos muy populares que a su vez poseen tanto puntos fuertes como puntos débiles. Estos a su vez, juntos, constituyen un buen conjunto de herramientas para comprender qué sucede en una red, también el protocolo NTP permite sincronizar la hora a través de los dispositivos, aspecto especialmente importante cuando se desea comparar archivos de registro en diferentes dispositivos.

d. **Monitoreo proactivo y umbrales.** Cuando un usuario informa al administrador sobre un problema con la red, se está presentando un caso de monitoreo proactivo deficiente, esto significa que la falla ya ha ocurrido y es hora de enmendarla; esta situación puede acarrear tiempo y dinero en la implementación de la solución. La clave para una buena monitorización,

es alertar sobre los posibles fallos o cuellos de botella antes de su ocurrencia o en el menor tiempo posible desde que suceden. Los umbrales juegan un papel definitivo en la proactividad del monitoreo, son ellos los que determinan dichos tiempos. Estos umbrales varían según el dispositivo, para un servidor de correos se puede determinar un bajo umbral por ser un dispositivo crítico, porque su funcionamiento no debe verse interrumpido, y cuando esto suceda, la interrupción debe durar el menor tiempo posible. Los umbrales también pueden ser usados para generar avisos o alertas en casos en los cuales el dispositivo alcance una condición preocupante y que pueda comprometer su funcionamiento o servicio prestado.

e. **Cuadros de mando y personalización.** La representación visual de los datos y estadísticas recolectadas en los procesos de monitorización, son útiles cuando se presentan de manera adecuada a las personas adecuadas. Un panel visual de control es muy acertado y necesario cuando brinda una descripción del estado actual de los dispositivos de red con métricas y umbrales críticos, que ayuden a tomar decisiones sobre la situación funcional de la red de información. Algunas herramientas visuales tales como "widgets" pueden facilitar la tarea del administrador, ya sea de manera local o remota.

f. **Alta disponibilidad y conmutación por error.** La disponibilidad de los recursos y servicios ofrecidos por la red deben ser totales y constantes. La alta disponibilidad de la gestión y monitoreo de la red debe ser continua e ininterrumpida, esto garantiza una supervisión constante de la

infraestructura en aras de mantener sus servicios activos para cuando los usuarios los requieran. La funcionalidad de conmutación por error, significa que habrá un segundo servidor presto a ofrecer todos los procesos que la monitorización y control requieran, en caso que el servidor primario falle en la realización de esta tarea. El sistema de conmutación por error proporciona beneficios como:

- El sistema reconoce instantáneamente la falla del servidor primario.
- Notificación inmediata por correo electrónico en caso de falla del servidor primario.
- 100 % de tiempo de actividad y gestión de red ininterrumpida.
- Conmutación automatizada y sin problemas entre el servidor primario y el servidor en espera y viceversa.

g. **Soluciones de monitorización de redes.** Para que haya una buena monitorización de la red, no solo es necesario el conocimiento y experticia de un administrador, sino también la ayuda de un "software" especializado de supervisión de red, que permita un régimen de monitoreo, lo que es primordial para enfrentar los cuellos de botella y contrariedades que podrían poner en riesgo la robustez del rendimiento de la red.

El incremento de la supervisión en las redes por parte de empresas y organizaciones, ha generado una amplia gama de servicios y productos creados para este fin, que pueden encontrarse en el mercado. Una óptima herramienta lógica o "software" de monitoreo de red puede ayudar en

los procesos de verificación de red, al mismo tiempo que reduce la carga de trabajo, brindando metodologías de solución de problemas.

Características de un “software” de monitorización de red eficaz

A continuación, se presenta un video, en el cual se explican las características que debe tener un sistema de monitorización de red:

Video 2. Características: “Software monitoreo”

Enlace de reproducción del video

Síntesis del video: Características: “Software” monitoreo
Características de un “software” de monitorización de red eficaz:

- Funciones de informes avanzados con posibilidad de programar y enviar por correo electrónico o publicar los informes automáticamente.
- Implementación de técnicas avanzadas de monitoreo del rendimiento de la red, para resolver rápidamente las fallas de la red, llegando a la raíz del problema.
- Supervisión de problemas del rendimiento de red, servidor y aplicaciones.
- Configuración automática de dispositivos e interfaces, con plantillas predefinidas.
- Visualización de toda su infraestructura de TI con clasificaciones basadas en tipos o grupos lógicos.

1.2. ¿Qué es la gestión de redes?

Según Ding (2016), la gestión de redes y servicios de las telecomunicaciones se basa en el monitoreo y control de los recursos y servicios de la misma, para aumentar su disponibilidad, eficiencia, rendimiento y favorecer la relación costo-beneficio en su diseño y operación.

La gestión de red exitosa tiene como tareas clave el monitoreo y control de todos los elementos de la red aplicadas a las áreas funcionales del modelo FCAPS: gestión de fallos, gestión de configuración, gestión de contabilidad, gestión de prestaciones o calidad del servicio y gestión de seguridad.

1.3. Gestión del rendimiento de la red

Así como el monitoreo proporciona la información necesaria para obtener una visión global del funcionamiento de la red en determinado momento o en tiempo real, la gestión de red a su vez permite ejecutar las acciones necesarias sobre la red en la búsqueda continua del óptimo rendimiento, la solución a los problemas detectados, el cumplimiento de los acuerdos de niveles de servicio, la proyección de crecimiento de la red y la optimización de la eficiencia versus la inversión realizada.

La red informática es la columna vertebral de la organización que la implementa y las aplicaciones informáticas basadas en el acceso a Internet, son primordiales para el libre desarrollo de las tareas y procesos al interior de la organización, por eso es vital que los usuarios de la red no se vean perjudicados debido a inconvenientes relacionados con los servicios de la red. Entonces, monitorear, preservar y mejorar el rendimiento de los servicios de la red se vuelve un objetivo principal para toda empresa que desea mantenerse comunicada en todos los aspectos.

Gestión de rendimiento de la red consiste entonces en las acciones necesarias para garantizar la calidad de servicio desde el punto de vista del usuario, lo cual implica medición de indicadores de servicio como disponibilidad, latencia, anchos de banda, "throughput" o tasa real de información transmitida, entre otros.

2. Herramientas de monitoreo de red

De acuerdo con Junco Romero y Rabelo Padua (2018), existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales como basadas en "software" libre. La elección depende de varios factores, tanto humanos, económicos como de infraestructura:

- El perfil de los administradores y sus conocimientos en determinados sistemas operativos.
- Los recursos económicos disponibles.
- El equipo de cómputo disponible.

¿Cómo se debe seleccionar una herramienta de monitoreo de red?

Claramente, la selección de la herramienta óptima para monitorear la red debe tener en cuenta los aspectos mencionados anteriormente, como también los alcances deseados, sin olvidar su importancia como herramienta valiosa para todos los procesos de seguridad, gestión, planeación y control; es claro afirmar que la robustez de la herramienta escogida será directamente proporcional al retorno de inversión obtenido por la empresa, así como a la estabilidad ofrecida por los sistemas. Así las cosas, en el mercado existen múltiples opciones tanto pagas como de "software" libre para el desarrollo de esta labor, el reto consiste en definir la más adecuada para las condiciones de la empresa.

Características básicas: las herramientas de diagnóstico y monitoreo de red deben ofrecer requisitos básicos de monitoreo, incluyendo factores como el monitoreo de mensajes "syslog", el monitoreo del ancho de banda, la disponibilidad o el uso; sin

embargo, deben tenerse en cuenta además características como la comunicación de las alertas e informes y que estos sean configurables, el soporte a la mayor cantidad de protocolos comunes (SNMP, WMI, CLI) y tecnologías ("NetFlow", "sFlow", "jFlow" y "Packet sniffing"), la seguridad, la flexibilidad para adaptarse a herramientas o software específico, la usabilidad de manera que proporcione el panel de control con presentación de datos óptima y personalizable.

Un "software" de monitoreo de red / solución de problemas de red con estas características, mejorará la tarea de monitoreo de red. Estas son características esenciales, sin embargo, también pueden buscarse atributos adicionales que optimicen el trabajo del personal de auditoría de la red, tales como:

- **Control remoto.** De manera que la herramienta se pueda usar en diferentes equipos de forma remota, sin tener que desplazarse al espacio físico en el que se encuentra el dispositivo.
- **Inventario de "hardware" y "software".** La capacidad de autogestión le permite ir descubriendo los nuevos dispositivos o elementos de la red, a la par que va guardando el estado y situación de cada uno en su inventario, registrando datos como el sistema operativo, IP, bios, memoria, CPU y "drivers", en el caso de "hardware" o programas instalados, parches y versiones, si se habla de "software".
- **Geolocalización y monitorización en la nube.** Con la expansión y el incremento en la accesibilidad a servicios ofrecidos en la nube por parte de los grandes de la industria como Amazon, diariamente un gran número de empresas mueven sus servidores y aplicaciones a la nube, por lo que es

importante comprobar que la herramienta de monitoreo de red tenga la posibilidad de monitorizar aplicaciones en la nube.

- **Inteligencia artificial y aprendizaje automático.** Característica muy deseable para una herramienta de monitoreo, porque a partir de los datos, puede incorporarse inteligencia artificial y aprendizaje automático, con los cuales las herramientas de supervisión de la red pueden adaptarse al entorno de la red y proporcionar sugerencias basadas en los datos disponibles.

- **Automatización.** De la mano de la inteligencia artificial, la automatización hace posible la reacción de la herramienta de monitoreo a partir de los datos recabados, los umbrales definidos o el conjunto de reglas / criterios enmarcados que se cumplan. La herramienta de monitoreo puede, mediante la automatización, detectar y solucionar problemas automáticamente (monitoreo proactivo), así como enviar notificaciones de alerta o proporcionar sugerencias para mejorar el rendimiento y mantenimiento de la red, basado en el uso y la prioridad.

- **Alcance.** Será útil que la herramienta de monitoreo de red proporcione visibilidad completa y detallada de varios aspectos de monitoreo de la red de manera consolidada. Además de brindar la flexibilidad para elegir lo que se desea ver, es lo que ayuda al administrador a mantenerse al tanto de la red. Es deseable que la información pueda presentarse en una pantalla común con cuadros de un vistazo y gráficos intuitivos, como herramienta de monitorización de red, se puede mejorar para realizar

operaciones más avanzadas con la ayuda de complementos y opciones para integrar otras herramientas.

- **Escalabilidad.** En tiempos recientes, donde las redes son virtuales y eternas es importante que una herramienta de monitoreo de red pueda ser escalable en la medida en que sea adaptable a las necesidades o demandas cambiantes de la empresa o los usuarios. Esta escalabilidad ayuda a una red a mantenerse a la par del aumento de la productividad, las tendencias, las necesidades cambiantes y las nuevas adaptaciones.

En el siguiente video, se presenta un resumen de los aspectos más relevantes que deben poseer las herramientas de monitoreo de red:

Video 3. Herramientas de monitoreo

Enlace de reproducción del video

Síntesis del video: Herramientas de monitoreo
La elección para la elección de herramientas de monitoreo de red, depende de factores humanos, económicos, o de infraestructura: El perfil de los administradores, sus conocimientos en determinados sistemas operativos. Los recursos económicos disponibles. El equipo de cómputo disponible. Aspectos: • Escalabilidad. • Automatización. • Control remoto. • Personalización de alertas. • Cuadros de mando configurables. • Informes personalizados. • Control de inventarios. • Monitoreo de mensajes “syslog”. • Soporte a protocolos comunes. • Monitoreo en la nube.

- Seguridad.

2.1. ¿Qué es el monitoreo de red en tiempo real?

El administrador de la red realiza las labores de monitoreo del estado de la red y demás verificaciones de manera periódica para garantizar su funcionamiento; sin embargo, al presentarse problemas técnicos resulta muy conveniente poder examinar los datos en tiempo real, directamente con la herramienta de monitoreo de manera que no sea necesario utilizar otra herramienta para acceder remotamente al dispositivo que presente el problema. A manera de ejemplo, se puede considerar el consumo de ancho de banda que puede ser elevado y ante esta situación el administrador de la red deberá cotejar los datos estadísticos en tiempo real del uso del puerto por donde se aumenta el ancho de banda, y así cerciorarse de la recurrencia del problema y sus potenciales causas.

2.2. ¿Qué es la gestión de servidores?

La gestión o gerencia de un servidor puede ser definida como el proceso mediante el cual se verifica y monitorea en busca de problemas en la infraestructura de cualquier servidor sin importar su naturaleza. El monitoreo y control constante del rendimiento del servidor permite que las aplicaciones alojadas y ofrecidas en este tengan un mejor desempeño y por lo tanto, unas mejoras en las prestaciones de los servicios ofrecidos a los usuarios que las requieren.

En el mercado se identifican herramientas de monitoreo de red ampliamente reconocidas tanto de “software” libre como Nagios, Zabbix o Pandora con versión

libre, o pagas como BMC, Opmanager o Solarwinds, las cuales por lo general utilizan el protocolo SNMP.

2.3. ¿Qué es SNMP?

"Simple Network Management Protocol" (SNMP) es el protocolo simple de administración de redes, es un protocolo de capa 7 o de aplicación, desarrollado para recolectar información del desempeño y funcionalidad de los componentes de una red informática. Es uno de los miembros del grupo de protocolos TCP / IP (Protocolo de control de transmisión / Protocolo de Internet), uno de los protocolos más populares y generosamente usados para tareas de administración y monitoreo de redes de computadores y está compuesto por:

- El administrador SNMP, responsable de gestionar la comunicación eficientemente con base en los datos recibidos del agente.
- Los dispositivos administrados son todos los elementos de la red a los que se monitorea.
- El "software" agente SNMP, "software" especial diseñado para la recopilación de información incluyendo la de su entorno local, almacenar y recuperar la información de gestión definida en la MIB, señalar eventos al gerente y actuar como "proxy" para algunos nodos de red administrables no SNMP.
- La base de información de gestión (MIB) almacena los objetos identificados para la gestión con sus tipos y relaciones en una entidad gestionada.

3. Gestión de servidor virtual

Es el proceso mediante el cual se verifica la disponibilidad, desempeño y funcionalidad de los servidores virtualizados, para así garantizar los servicios ofrecidos por estos.

3.1. ¿Qué es la gestión de servidores virtuales?

Con el objetivo de reducir costos y optimizar el uso de recursos tecnológicos, muchas empresas han optado por la virtualización de servidores. Esta tecnología permite ejecutar varios sistemas operativos en un mismo "hardware", lo que implica una serie de ventajas, como la reducción de "hardware", el consumo de energía eléctrica y los costes de mantenimiento.

Sin embargo, también implica algunas desventajas, como la necesidad de adquirir un nuevo "software" para ejecutar los procesos virtualizados y la posibilidad de que la instalación de varias máquinas virtuales en un solo servidor pueda suponer una disminución en el rendimiento.

A continuación, se enumeran algunos de los desafíos más comunes de la administración de servidores virtuales:

- Reducción de "hardware".
- Consumo de energía.
- Incremento en costos de "software".
- Aumenta carga de servidores por múltiples máquinas virtuales.
- Incremento en tráfico al servidor.

También es importante tener en cuenta:

- **Expansión de VM (“Virtual Machine”).** La ejecución de máquinas virtuales puede significar una serie de ventajas; sin embargo, la instalación de demasiadas VM puede convertirse en una tarea engorrosa, y la implementación de tantas VM puede reducir o agotar considerablemente los recursos tecnológicos. El alto índice de implementación de VM puede obligar a las empresas a adquirir un nuevo “hardware” para su alojamiento. Las herramientas de monitoreo de servidores virtuales pueden abordar de manera efectiva el problema de la expansión de VM en la red.

- **Congestión del tráfico de la red.** Alojar varias máquinas virtuales en un solo servidor, sabiendo que este solo cuenta con un puerto físico de red (NIC), puede aumentar considerablemente el tráfico de información. Las cargas de trabajo sensibles a la latencia de la red, pueden informar errores o incluso bloquearse, esto puede resultar un asunto costoso que se puede evitar con la ayuda de una solución de administración de red virtual adecuada.

- **Problemas de “hardware” del servidor.** La virtualización de servidores proporciona una gran flexibilidad en términos de continuidad empresarial y recuperación ante desastres; sin embargo, los recursos físicos subyacentes aún pueden verse afectados negativamente por la consolidación de servidores virtuales. La administración del servidor virtual ayuda a mantener estos recursos en una óptima utilización, así como a monitorear su estado y rendimiento.

3.2. ¿Qué es la supervisión de red sin agentes?

El monitoreo de red sin agentes es una técnica en la que el servidor de monitoreo sondea directamente los dispositivos en la red periódicamente, para monitorear su estado y rendimiento.

Esta técnica resulta más eficiente y práctica que aquella donde se implementan agentes donde son estos los que recopilan información sobre el estado de los dispositivos y la envían al respectivo "software" de monitoreo de la red.

¿Por qué la supervisión de redes sin agentes?

El debate entre el monitoreo basado en agentes y sin agentes, es uno que se viene produciendo desde hace mucho tiempo en la industria de la gestión de redes; sin embargo, la mayoría de las empresas prefieren la monitorización de red sin agentes, porque domina las siguientes ventajas:

- **Reducción del tiempo de implementación.** Dado que no hay agentes involucrados, solo es necesario configurar el servidor de monitoreo y, por lo tanto, implementar una herramienta de monitoreo de red sin agentes, que es un proceso sin complicaciones. Puede hacer que la infraestructura de monitoreo de red funcione en poco tiempo sin tener que pasar por complejos procesos de configuración.
- **Gastos generales de administración reducidos.** La ausencia de agentes hace que la infraestructura de monitoreo de red sea más fácil de mantener.

- **Fácil de actualizar.** En el caso de una infraestructura de monitoreo de red basada en agentes, cada vez que se actualiza la herramienta de monitoreo de red o un componente de red, todos los agentes de la red deben actualizarse. Los entornos de supervisión de redes sin agentes no tienen este problema.

- **Reducción de la sobrecarga de fallas.** En el caso de la supervisión basada en el agente, la falla de un agente detendrá el proceso de supervisión de todos los dispositivos conectados a ese agente. Este problema no ocurre en el monitoreo sin agentes donde el monitoreo de dispositivos no se ve afectado por factores externos.

En el siguiente video, se presenta una explicación de las diferencias de usar un sistema basado en agentes y otro sin agentes:

Video 4. Comparativo monitoreo

Enlace de reproducción del video

Síntesis del video: Comparativo monitoreo
Video donde se presenta una explicación de las diferencias de usar un sistema basado en agentes y otro sin agentes: • Facilidad de implementación. • Costos de implementación. • Facilidad de actualización. • Ciclos de monitoreo.

- Seguridad.
- Gastos de red.
- Cubrimiento del monitoreo.
- Consumo del servidor.

El agente se instala en cada servidor.

Costos de infraestructura necesaria para respaldar los agentes.

Debe realizarse en cada agente.

Hasta 1 seg.

Se encuentra en el servidor, no requiere configurar reglas adicionales de “firewall”.

Por su ubicación local, solo transporta resultados finales a la consola, lo que disminuye el consumo de ancho de banda.

Profundidad y amplitud en el monitoreo.

El agente consume ciclos de CPU en el servidor en que se instale, según la configuración de ciclos.

Solo se instala en el recopilador remoto.

No requiere costos adicionales.

No requiere actualización uno a uno.

Min c/60 seg en promedio.

Requiere configurar privilegios para que el recopilador se comunique con el sistema.

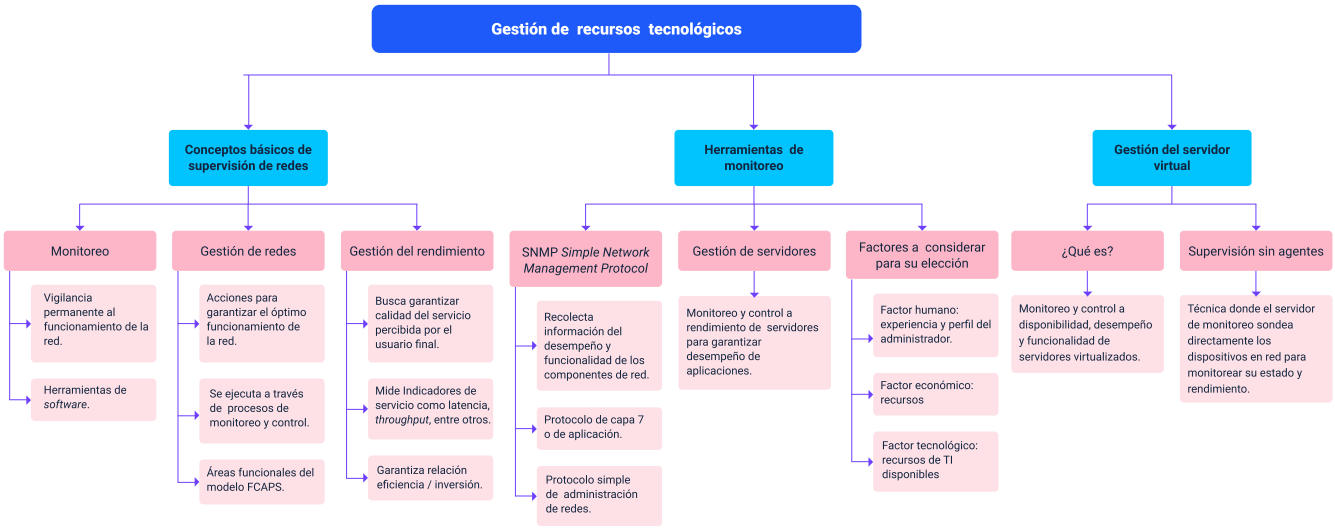
Requiere comunicación bidireccional, que consume tráfico al transportar los datos al recopilador remoto.

Limitado por las capacidades integradas de monitoreo en los dispositivos.

No reporta sobrecarga permanente al servidor destino.

Síntesis

A continuación, se resumen los conceptos vistos en este componente formativo.



El esquema presenta la síntesis de la temática estudiada en el componente formativo, comenzando por la gestión de recursos tecnológicos, la cual está compuesta por:

- Conceptos básicos de supervisión de redes: compuesto por el monitoreo, la gestión de redes y la gestión de rendimiento.
- Herramientas de monitoreo: compuesta por el SNMP “Simple Network Management Protocol”, la gestión de servidores y los factores a considerar para su elección.
- Gestión del servidor virtual: compuesta por la supervisión sin agentes.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
¿Qué es SNMP?	Briceño, C. R. (2004). Protocolo SNMP (protocolo sencillo de administración de redes). Télématique, 3(1), p. 90-102.	Artículo	https://www.redalyc.org/pdf/784/78430108.pdf
Gestión de servidor virtual	Chahin-Noreña, J. A. (2015). Metodología ACRD para la gestión de seguridad en entornos virtuales (Master's thesis). Repositorio digital UNIR.	Tesis de maestría	https://reunir.unir.net/handle/123456789/3510

Glosario

Administración dentro de banda: se utiliza para monitorear y realizar cambios en la configuración de un dispositivo de red.

Agente: "software" programado para realizar una función específica.

Dirección IP: 32 "bytes" que identifican a un equipo en una red. Se representa en notación decimal punteada.

Dispositivo: pieza de un equipo informático que realiza una función específica.

"Hardware": dispositivo, equipo, aparato. Parte física o tangible del ordenador.

"Host": dispositivo que participa directamente en la comunicación de la red.

Internet: conjunto de redes a nivel mundial interconectadas entre sí.

SNMP: es un protocolo de la capa de aplicación que facilita el intercambio de información y de administración entre dispositivos de red.

URL: localización uniforme de recursos. Cadena alfanumérica en un formato específico que representa un dispositivo.

WAN: redes que abarcan regiones, países, por ejemplo, empresas de telecomunicaciones.

WPAN: es la red inalámbrica más pequeña, utilizada para conectar varios dispositivos periféricos como "mouse", teclados y PDA a una computadora.

Referencias bibliográficas

Beekman, G. (2005). Introducción a la informática (traductor Díaz Martín, José Manuel). Pearson Educación.

Briceño, C. R. (2004). Protocolo SNMP (protocolo sencillo de administración de redes). Télématique, 3(1), p. 90-102. https://www.redalyc.org/pdf/784/78430108.pdf

Ding, J. (2016). Advances in network management. CRC Press.

Junco, G., y Rabelo, S. (2018). Los recursos de red y su monitoreo. Revista Cubana de Informática Médica, 10(1), p. 76-83.

Lorge, F., Ricci, S., Iglesias, A., Meloni, M., & Fernández, M. (2020). Protocolo SNMP.

Parra, A., y Mendieta, S. (2005). Protocolo SNMP simple network management protocol.

Créditos

Nombre	Cargo	Centro de Formación y Regional
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Jorge Eliécer Loaiza Muñoz	Instructor	Centros de Servicios y Gestión Empresarial - Antioquia
Carlos Mauricio Tovar Artunduaga	Instructor	Centros de Servicios y Gestión Empresa
Heidi Zuleyma Gil Castañeda	Experta temática	Centro de la Industria, la Empresa y los Servicios - Regional Huila
Ana Catalina Córdoba Sus	Metodólogo para formación virtual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Juan Daniel Polanco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Edward Leonardo Pico Cabra	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martínez Torres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Eduardo Garavito Parada	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andrés Bolaño Rey	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Centro de Formación y Regional
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para contenidos inclusivos y accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander