

Tecnológico Nacional de México

Instituto Tecnológico de Reynosa



Equipo conformado por:

Bermudez Dominguez Juan Carlos 19580585  
Castillo Jr Gregorio 19580589

Flores Acosta Sheila Lizeth 19580595

Morales Calixto Daniel Alexander 19580867

Gongora Raga Perla Elizabeth 19580603

Perez Romero Julio Alberto 19580633

Administración de servidores

# Índice

[Índice 1](#_Toc128935586)

[2.1 Tipos de servidores aplicados a la seguridad informática 2](#_Toc128935587)

[2.2 Servicios de red: HTTP, Motor de aplicación WEB 9](#_Toc128935588)

[2.3 Administración de servidores 13](#_Toc128935589)

[2.3.1 Monitoreo de red 17](#_Toc128935590)

[2.3.2 Monitoreo de memoria 20](#_Toc128935591)

[2.3.3 Monitoreo de CPU 22](#_Toc128935592)

[2.3.4 Monitoreo de procesos 27](#_Toc128935593)

[2.4 Análisis de performance y optimización 30](#_Toc128935594)

[Bibliografía 34](#_Toc128935595)

# 2.1 Tipos de servidores aplicados a la seguridad informática

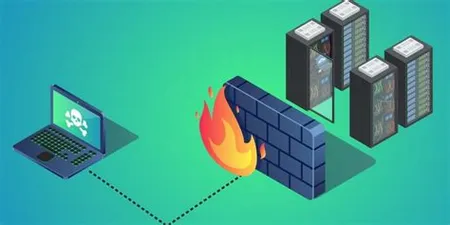
Los servidores aplicados a la seguridad informática sirven para proteger los sistemas y datos de una organización contra amenazas y ataques informáticos. Estos servidores son dispositivos de red especializados que están diseñados para detectar, prevenir y responder a los intentos de intrusiones maliciosas en los sistemas informáticos.

Los servidores de seguridad informática actúan como una barrera entre la red interna de una organización y el mundo exterior, monitoreando y controlando el tráfico de red para detectar y bloquear los ataques. Algunas de las funcionalidades que pueden proporcionar los servidores de seguridad incluyen:

Firewall: Un firewall es una medida de seguridad esencial que se utiliza para proteger las redes contra ataques externos. Los servidores de seguridad pueden incluir un firewall que permite o bloquea el tráfico de red en función de reglas predefinidas. Existen diferentes tipos de servidores firewall, algunos son hardware dedicado que se colocan en la red entre el enrutador y los dispositivos de la red interna, mientras que otros son software que se ejecutan en un servidor dedicado o en un sistema operativo existente.

Algunos de los más comunes son:

1. Firewall de red: Este tipo de firewall es un dispositivo de hardware que se sitúa entre la red interna y la red externa (internet). Se encarga de filtrar el tráfico de red basado en reglas de seguridad definidas por el administrador de red.
2. Firewall de software: Este tipo de firewall es un programa que se instala en una computadora y protege solo esa máquina. Se encarga de bloquear el tráfico de red no deseado y de controlar el acceso a la red.
3. Firewall de proxy: Este tipo de firewall actúa como intermediario entre la red interna y la red externa. Todos los pedidos de los usuarios pasan primero a través del servidor proxy, que filtra y analiza el tráfico antes de permitir que llegue a la red interna.
4. Firewall de aplicación: Este tipo de firewall se enfoca en la seguridad de las aplicaciones que se ejecutan en la red interna. Se encarga de bloquear los ataques dirigidos a aplicaciones específicas y de detectar y prevenir la explotación de vulnerabilidades en el código de la aplicación.
5. Firewall de estado: Este tipo de firewall mantiene un registro del estado de cada conexión de red y utiliza esta información para determinar si se debe permitir o bloquear el tráfico. Esto permite que el firewall controle de manera más precisa el tráfico de red y sea más eficiente en el filtrado de paquetes.

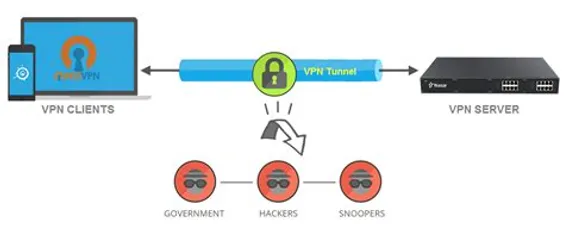


VPN: Los servidores de seguridad también pueden proporcionar conectividad VPN (red privada virtual) para permitir a los usuarios acceder a la red interna de forma segura desde cualquier lugar.

Los servidores VPN pueden ser operados por empresas, organizaciones, proveedores de servicios de Internet y otros proveedores de servicios. Hay varios tipos de servidores VPN, incluyendo:

1. Servidores VPN empresariales: utilizados por empresas para permitir a los empleados acceder a la red corporativa de forma segura desde ubicaciones remotas.
2. Servidores VPN de acceso remoto: utilizados por individuos para conectarse a una red privada desde una ubicación remota.
3. Servidores VPN de sitio a sitio: utilizados para conectar dos o más redes privadas separadas a través de Internet.
4. Servidores VPN de proveedores de servicios: utilizados por proveedores de servicios de Internet para ofrecer servicios de VPN a sus clientes.

En general, los servidores VPN cifran los datos que se transmiten a través de la red para proteger la privacidad y la seguridad de las comunicaciones en línea. También pueden proporcionar otras características de seguridad, como autenticación de usuarios y protección contra ataques de hackers y malware.



Detección y prevención de intrusiones: Los servidores de seguridad pueden detectar y bloquear intentos de intrusiones o ataques que intenten explotar vulnerabilidades en los sistemas de una organización.

Un servidor de detección de intrusos (IDS, por sus siglas en inglés) es un sistema que monitorea el tráfico de red en busca de actividad sospechosa o maliciosa. El objetivo principal de un IDS es detectar y alertar sobre posibles intrusiones en la red.

Los servidores IDS se pueden clasificar en dos categorías principales:

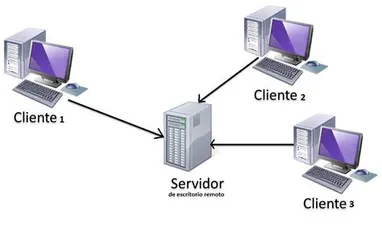
1. IDS basado en host: Este tipo de IDS se ejecuta en un host individual y supervisa la actividad en ese host. Por ejemplo, puede monitorear la actividad de los archivos de registro, el uso del sistema de archivos y los intentos de acceso no autorizado al host.
2. IDS basado en red: Este tipo de IDS se ejecuta en una red y monitorea el tráfico de red para detectar actividad sospechosa. Puede analizar paquetes de red en busca de patrones de comportamiento malicioso, como intentos de escaneo de puertos, ataques de denegación de servicio (DoS) y otros tipos de actividad sospechosa.

Gestión de accesos y autorizaciones: Los servidores de seguridad pueden gestionar los accesos y permisos de los usuarios para garantizar que solo los usuarios autorizados tengan acceso a los recursos de la red.

Los servidores de gestión de acceso y autorización pueden utilizarse en una amplia variedad de aplicaciones, desde sistemas de gestión de identidades y accesos (IAM) hasta servicios en la nube, aplicaciones web y móviles, sistemas de control de acceso físico, y más.

Entre las funciones principales de los servidores de gestión de acceso y autorización se encuentran:

1. Autenticación de usuarios: Verificar la identidad de los usuarios mediante contraseñas, tokens, certificados, biometría u otros métodos de autenticación.
2. Autorización de acceso: Conceder permisos de acceso a los recursos en función de los roles, perfiles y políticas de seguridad definidos para cada usuario.
3. Gestión de sesiones: Controlar el tiempo de sesión de los usuarios y su estado de autenticación durante la sesión.
4. Auditoría y reportes: Registrar y reportar los accesos y eventos de seguridad relevantes para su posterior análisis y seguimiento.
5. Integración con otros sistemas: Interactuar con otros sistemas, como directorios LDAP, bases de datos, servicios de autenticación externos y APIs.

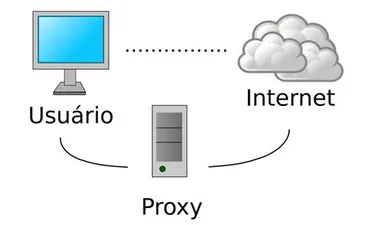


Servidores de proxy: los servidores proxy actúan como intermediarios entre los clientes de la red y los servidores externos. Los usuarios se conectan al servidor proxy en lugar de conectarse directamente a los servidores externos, lo que proporciona una capa adicional de seguridad y anonimato.

El servidor proxy actúa como un servidor web que puede recibir solicitudes de un usuario y transmitirlas al servidor final, o puede actuar como un servidor de cache para mejorar el rendimiento.

Hay varios tipos de servidores proxy, algunos de los más comunes son:

1. Proxy web: Este tipo de servidor proxy se utiliza para acceder a páginas web y es comúnmente utilizado por empresas para monitorear y controlar el acceso a Internet de sus empleados. Puede ser transparente para el usuario, es decir, que no requiere configuración especial en el navegador web.
2. Proxy de red: Este tipo de servidor proxy se utiliza para filtrar el tráfico de red en una red corporativa. Puede ser utilizado para bloquear el acceso a sitios web específicos o para proteger la red de ataques cibernéticos.
3. Proxy de caché: Este tipo de servidor proxy almacena en caché las páginas web visitadas anteriormente para que puedan ser accedidas más rápidamente en el futuro. Esto reduce el tiempo de carga de las páginas y ayuda a mejorar el rendimiento de la red.
4. Proxy inverso: Este tipo de servidor proxy se utiliza para servir contenido a los usuarios finales en lugar de un servidor web en línea. Por ejemplo, una empresa puede utilizar un proxy inverso para cargar el contenido de su sitio web de manera más rápida y eficiente.



Servidores de autenticación: estos servidores se utilizan para autenticar a los usuarios y controlar el acceso a los recursos de la red. Los servidores de autenticación pueden utilizar diferentes métodos de autenticación, como contraseñas, certificados digitales o tokens de seguridad.

La autenticación se realiza mediante un proceso de verificación de las credenciales del usuario, como el nombre de usuario y la contraseña.

Algunos ejemplos de servidores de autenticación incluyen:

1. Servidores de autenticación de dominio: Estos servidores se utilizan en entornos de red de Microsoft Windows y son responsables de autenticar a los usuarios en un dominio específico. Los servidores de autenticación de dominio utilizan el protocolo de autenticación de Kerberos para verificar la identidad del usuario.
2. Servidores de autenticación de directorios: Estos servidores se utilizan para autenticar a los usuarios en sistemas que utilizan un directorio, como LDAP o Active Directory. El servidor de autenticación de directorios consulta el directorio para verificar las credenciales del usuario.
3. Servidores de autenticación basados en tokens: Estos servidores se utilizan para autenticar a los usuarios mediante un token de seguridad, como un token de hardware o una tarjeta inteligente. El usuario presenta el token al servidor de autenticación para verificar su identidad.
4. Servidores de autenticación de contraseñas únicas: Estos servidores se utilizan para autenticar a los usuarios en múltiples sistemas y servicios utilizando una única contraseña. Los usuarios solo necesitan recordar una contraseña para acceder a todos los sistemas y servicios que utilizan la autenticación de contraseñas únicas.



Servidores de antivirus: los servidores de antivirus se utilizan para proteger los sistemas contra virus, malware y otras amenazas de seguridad. Estos servidores escanean los archivos y programas en busca de amenazas y los eliminan o colocan en cuarentena si se detecta algún problema.

Existen diferentes tipos de servidores de antivirus que pueden ser utilizados para proteger las redes de computadoras. A continuación, se describen algunos de los más comunes:

1. Servidores de antivirus dedicados: Estos servidores están diseñados específicamente para proporcionar protección antivirus a la red y se encargan exclusivamente de esta tarea. Pueden ser físicos o virtuales y suelen estar ubicados en el centro de datos de la empresa.
2. Servidores de correo electrónico antivirus: Estos servidores se encargan de analizar el correo electrónico en busca de virus y otras amenazas de seguridad. Son particularmente importantes para las empresas que manejan grandes volúmenes de correo electrónico, ya que pueden ayudar a prevenir la propagación de virus y malware a través del correo electrónico.
3. Servidores de seguridad de la red: Estos servidores utilizan software antivirus para proteger la red contra amenazas de seguridad en tiempo real. Monitorean el tráfico de red y detectan y eliminan cualquier amenaza de seguridad que se detecte.
4. Servidores de protección de puntos finales: Estos servidores utilizan software antivirus para proteger los dispositivos finales, como computadoras portátiles y de escritorio, teléfonos móviles y tabletas. Proporcionan una capa adicional de protección contra virus y malware, lo que ayuda a mantener seguros los dispositivos de la empresa.



# 2.2 Servicios de red: HTTP, Motor de aplicación WEB

HTTP (Hypertext Transfer Protocol) es un protocolo de red utilizado para la transmisión de datos en la World Wide Web (WWW). Es el protocolo de comunicación más utilizado para la transmisión de contenido web en Internet.

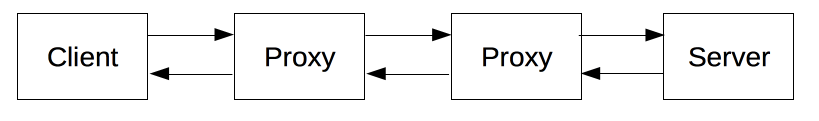
Cuando un usuario ingresa una URL (Uniform Resource Locator) en su navegador web, el navegador envía una solicitud HTTP al servidor que aloja el sitio web correspondiente. La solicitud incluye un conjunto de comandos que indican al servidor qué acción debe realizar, como recuperar un archivo o enviar un formulario. El servidor procesa la solicitud y envía una respuesta HTTP de vuelta al navegador, que puede contener el contenido solicitado o un código de error si la solicitud no se puede cumplir.

HTTP utiliza el puerto 80 para la comunicación, aunque también puede usar otros puertos, como el 8080. También hay una versión segura de HTTP llamada HTTPS, que utiliza un canal cifrado para garantizar la privacidad y la seguridad de los datos transmitidos entre el servidor y el cliente.

Arquitectura servicio red http

La arquitectura de servicios de red HTTP se basa en el modelo cliente-servidor, donde un cliente (generalmente un navegador web) solicita información a un servidor web, que a su vez proporciona esa información al cliente en forma de una respuesta HTTP.

En la arquitectura cliente-servidor, el cliente envía una solicitud HTTP al servidor a través de una conexión de red, que puede ser una conexión TCP/IP o una conexión segura HTTPS. El servidor procesa la solicitud y envía una respuesta HTTP al cliente. La respuesta incluye un código de estado HTTP que indica si la solicitud se ha completado correctamente o si se ha producido algún error.



La arquitectura de servicios de red HTTP también se basa en la arquitectura de estilo REST (Representational State Transfer). REST es un estilo de arquitectura de software que se utiliza para construir aplicaciones web escalables y mantenibles. La arquitectura REST utiliza el protocolo HTTP como base para la comunicación entre el cliente y el servidor y utiliza recursos bien definidos y URI (Uniform Resource Identifiers) para identificar los recursos a los que se accede. REST también utiliza los métodos HTTP (GET, POST, PUT, DELETE) para realizar operaciones en los recursos.

Además, la arquitectura de servicios de red HTTP utiliza el concepto de caché para mejorar el rendimiento y la eficiencia de la red. Los clientes pueden almacenar en caché las respuestas HTTP para solicitudes futuras, lo que reduce la carga en el servidor y acelera el tiempo de respuesta de las solicitudes.

Características de servicios de red http

Las principales características del servicio de red HTTP (Hypertext Transfer Protocol) son las siguientes:

* Protocolo de comunicación: HTTP es un protocolo de comunicación que permite la transferencia de información en la World Wide Web (WWW). Es un protocolo cliente-servidor, donde el cliente envía una solicitud HTTP al servidor y el servidor envía una respuesta HTTP al cliente.
* Basado en texto: HTTP es un protocolo basado en texto, lo que significa que las solicitudes y las respuestas se transmiten en formato de texto legible para el ser humano. Esto hace que sea más fácil para los desarrolladores depurar y solucionar problemas en la red.
* Stateless: HTTP es un protoclo sin estado, lo que significa que cada solicitud se procesa de forma independiente sin tener en cuenta las solicitudes anteriores. Cada solicitud se trata como una nueva solicitud y no hay ninguna información de estado guardada en el servidor entre solicitudes.
* Seguro: HTTP tiene una versión segura llamada HTTPS (Hypertext Transfer Protocol Secure), que utiliza un canal cifrado para garantizar la privacidad y la seguridad de los datos transmitidos entre el servidor y el cliente. HTTPS utiliza certificados SSL/TLS para cifrar los datos transmitidos y autenticar el servidor.
* Caché: HTTP utiliza caché para mejorar el rendimiento de la red. Los clientes pueden almacenar en caché las respuestas HTTP para solicitudes futuras, lo que reduce la carga en el servidor y acelera el tiempo de respuesta de las solicitudes.
* Métodos de solicitud: HTTP utiliza diferentes métodos de solicitud, como GET, POST, PUT y DELETE, para realizar operaciones en los recursos. GET se utiliza para recuperar datos, POST para enviar datos, PUT para actualizar datos y DELETE para eliminar datos

¿Qué se puede controlar con HTTP?

HTTP (Hypertext Transfer Protocol) permite controlar una serie de aspectos relacionados con la comunicación entre un cliente y un servidor web. A continuación, se detallan algunos de los aspectos que se pueden controlar con HTTP:

* Tipo de contenido: HTTP permite especificar el tipo de contenido que se está transmitiendo, como texto plano, HTML, XML, JSON, etc. Esto es útil para que el cliente pueda interpretar correctamente la respuesta del servidor.
* Caché: HTTP permite controlar el almacenamiento en caché de las respuestas del servidor. Los servidores pueden especificar si las respuestas se pueden almacenar en caché y durante cuánto tiempo. Los clientes pueden almacenar en caché las respuestas para solicitudes futuras, lo que reduce la carga en el servidor y acelera el tiempo de respuesta de las solicitudes.
* Autenticación: HTTP permite la autenticación de los usuarios mediante diversos mecanismos, como el uso de contraseñas o tokens de acceso. Esto permite restringir el acceso a ciertos recursos solo a usuarios autorizados.
* Control de acceso: HTTP permite controlar el acceso a los recursos en función del método de solicitud, la dirección IP del cliente, la hora del día, etc. Esto permite restringir el acceso a ciertos recursos solo a ciertos clientes.
* Redirección: HTTP permite redirigir al cliente a una nueva URL, lo que es útil para corregir errores en la URL o para redirigir a los usuarios a una página de inicio de sesión, por ejemplo.

Servicios de motor de red: Motor de aplicaciones WEB

Los motores de aplicación web proporcionan una variedad de servicios de red para permitir la comunicación entre el servidor web y los clientes que acceden a la aplicación a través de la red. Algunos de los servicios de red proporcionados por los motores de aplicación web son:

* Protocolos de red: Los motores de aplicación web admiten varios protocolos de red, como HTTP, HTTPS, WebSocket, etc., para permitir la comunicación entre el servidor web y los clientes.
* Enrutamiento de URL: Los motores de aplicación web proporcionan una forma de enrutar las solicitudes HTTP a la función correspondiente en la aplicación web.
* Manejo de solicitudes y respuestas HTTP: Los motores de aplicación web proporcionan una forma de manejar las solicitudes y respuestas HTTP, incluyendo la validación de entradas de usuario, el análisis de solicitudes, la generación de respuestas, etc.
* Manejo de sesiones: Los motores de aplicación web permiten el manejo de sesiones de usuario, que permiten que los usuarios inicien sesión y mantengan un estado entre las solicitudes.
* Acceso a bases de datos: Los motores de aplicación web proporcionan una forma de acceder a bases de datos para almacenar y recuperar datos de la aplicación.
* Autenticación y autorización: Los motores de aplicación web proporcionan mecanismos para autenticar a los usuarios y autorizar el acceso a ciertas áreas de la aplicación web.

# 2.3 Administración de servidores

La administración de servidores es una tarea que requiere de una correcta configuración para asegurarse de que el equipo no sufra ningún tipo de daños o sobrecargas por el uso del mismo.

Los servidores son fuentes de datos y de almacenamiento para las empresas, la tarea de la administración de servidores es hacer que el equipo funcione y de servicio correctamente. Evitar el tiempo de inactividad, garantizar la seguridad, realizar configuraciones y hacer una copia de seguridad de los datos del sevidor.

La administración de servidores incluye diversas funciones, dependiendo de las necesidades específicas de cada empresa o negocio. Sin embargo, es importante gestionar la instalación, soporte y mantenimiento del sistema o servidor informático para así lograr un desempeño óptimo de las actividades y operaciones de la empresa.

La administración de servidores consiste en la gestión, mantenimiento y monitoreo de los sistemas informáticos de una organización. Su función es importante para las empresas porque dependen en gran medida del manejo de la información.

Sin embargo, el papel de la administración de servidores es desempeñar la gestión del hardware, las aplicaciones, la configuración de los usuarios y la comprobación del funcionamiento del mismo. También del soporte técnico, la resolución de incidencias, el refuerzo de las medidas de seguridad y la actualización del equipo.

La administración de servidores engloba todas las tareas relacionadas con la gestión, optimización y monitorización de los servidores, redes y sistemas a fin de asegurar que funcionan de forma correcta y segura. Requiere de monitorización y disponibilidad 24/7 para garantizar las operaciones del negocio en todo momento.

El rol del administrador de servidores es el de instalar, gestionar, optimizar, monitorizar y solucionar problemas (en caso necesario) en los servidores de la empresa y en componentes relacionados. Para garantizar un alto rendimiento y seguridad, los administradores de servidores son responsables de completar una amplia lista de tareas, como:

* Gestión y mantenimiento del hardware.
* Mantenimiento y actualización de aplicaciones.
* Programa de backups.
* Monitorización de servidores y sistemas.
* Optimización del rendimiento.
* Gestión de accesos.
* Soporte técnico y gestión de tickets.
* Implementación de barreras de seguridad contra ciberataques.
* Protección de datos.
* Seguridad del centro de datos, si se opta por servidores on-premise.

Existen algunos aspectos principales a valorar cuando se administra un servidor.

* Copias de seguridad o backups: Aunque la seguridad puede ser un aspecto básico a la hora de administrar un servidor, son pocos los usuarios que se olvidan de poner su información a salvo. Por lo tanto, tener copias de seguridad o backups es un aspecto fundamental en caso de que ocurra cualquier tipo de incidente con el servidor, tu información no se pierda.

Al momento de realizar las copias de seguridad o backups es necesario considerar lo siguiente: Debe actualizarse de manera periódica, debe tener una localidad física externa donde se encuentra dicho servidor y debe incluir toda la información que se requiera respaldar.

Una vez realizada las copias de seguridad o backups, es indispensable comprobar que no ocupen espacio de almacenamiento. Todos los registros almacenados por el servidor deben ser eliminados automáticamente cada determinado tiempo.

* Monitoreo de procesos: Otro aspecto importante al momento de realizar una administración de servidores es la monitorización de las cargas del CPU, tanto el uso de la memoria como el ancho de la banda.

De esta manera, cuando haya mayor capacidad de almacenamiento, estás previniendo de que tu servidor no se sature. Así evitarás que el servidor se sobrecargue por el uso del mismo y no seas consciente de ello hasta que un usuario lo notifiqué.

* Fortalecimiento del servidor: Otro aspecto que debes tener muy presente en la administración de servidores es el fortalecimiento del mismo. Para ello, debes realizar un análisis detallado sobre qué procesos están corriendo en tu servidor, así como los puertos que tienes abiertos y si dispones de algún equipo o herramienta capaz de hacer frente a las amenazas y ciberataques. Y después, con toda la información en tu mano, apostar por las mejores soluciones en cuanto a seguridad para proteger el equipo.

Un tip a recordar es que ningún sistema es capaz de garantizar la seguridad de un servidor de manera integral, al 100%. No obstante, sí existen sistemas muy avanzadas tanto tecnológica como técnicamente que te ofrecen una protección al 99%.

* Actualizaciones de seguridad: En la administración de servidores es importante estar al pendiente de todas las novedades en relación a la seguridad de los servidores informáticos.
* Migración del servidor: Una de las razones por las que las empresas deciden cambiar su antiguo servidor por uno nuevo, es porque el equipo ya no es capaz de almacenar ni procesar más información y no es posible realizar actualizaciones.

Lo más importante al momento de elegir un servidor, es que este se adapte a las características y necesidades de cada empresa. Para su configuración es indispensable limpiar el nuevo servidor, eliminando cuentas de correo, páginas y copias de seguridad que hayan quedado obsoletas.

La solución más sencilla para migrar o transferir tus datos es basarse en el estado actual en el que se encuentra la información. Así, esta es transferida al nuevo servidor y finalmente, se configura la IP o el DNS.

* Sincronización con aplicaciones externas: Si tu servidor requiere el acceso continuo a una base de datos, lo más aconsejable es optar por una solución híbrida de migración de servidores. De este modo, el servidor se mantiene activo.

El proceso consiste en declarar a la base de datos actual a modo de “master”, para que esta sea capaz de subordinar a la nueva base de datos durante la configuración como “slave”. Así se consigue que ambas aplicaciones se sincronicen en tiempo real. Una vez ambas bases de datos están al mismo nivel, es posible invertir los roles para que así la nueva base de datos pase a ser “master”.

Una de las ventajas de la sincronización en tiempo real es que si ocurre cualquier tipo de error con el nuevo servidor, es posible acceder a la antigua base de datos.

* Servicios de autenticación y encriptación: Para la autenticación de un servidor, los usuarios deben de realizar una serie de pasos de manera previa. Para ello, es importante configurar todas las cuentas de usuario en el registro de autentificación.

Se ha comprobado que las empresas destinan cada vez más a la seguridad de sus servidores. Se rigen a través de estos cuatro pilares básicos: autentificación de un servidor, autorización, auditoría y encriptación de datos.

Se le denomina encriptación de datos al proceso de cifrar u ocultar datos a través del uso de determinada clave o contraseña. Es importante conocer que el cifrado no resuelve problemas de control de acceso, aunque si mejora la seguridad.

## 2.3.1 Monitoreo de red

¿Qué es?

El monitoreo de red proporciona la información que los administradores de redes necesitan para determinar, en tiempo real, si una red está funcionando de manera óptima. Con herramientas como el software de monitoreo de redes, los administradores pueden identificar deficiencias y optimizar la eficiencia de manera proactiva, y más.

Los sistemas de monitoreo de red incluyen herramientas de software y hardware que pueden hacer un seguimiento de diversos aspectos de la red y su funcionamiento, tales como:

* El tráfico
* El uso de ancho de banda
* El tiempo de actividad.

Estos sistemas pueden detectar dispositivos y otros elementos que componen o tocan la red, además de proporcionar actualizaciones de estado.

Administradores de red

Los administradores de red confían en los sistemas de monitoreo de red para detectar rápidamente las fallas de dispositivos o conexiones, o los problemas como los cuellos de botella de tráfico que limitan el flujo de datos. Estos sistemas pueden alertar a los administradores de los problemas por correo electrónico o mensaje de texto, y enviar informes mediante la [analítica de red](https://www.cisco.com/c/en/us/solutions/analytics.html).

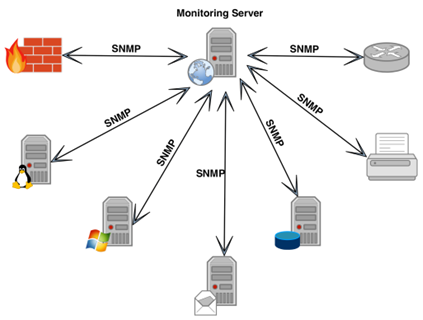
Protocolos para el monitoreo de red

Los protocolos son conjuntos de reglas e instrucciones para que los dispositivos de la red se comuniquen entre sí. El hardware de red no puede transmitir los datos sin usar los protocolos. Los sistemas de monitoreo de red usan los protocolos para identificar los problemas de rendimiento de red y enviar informes al respecto.

* SNMP
* ICMP
* CDP

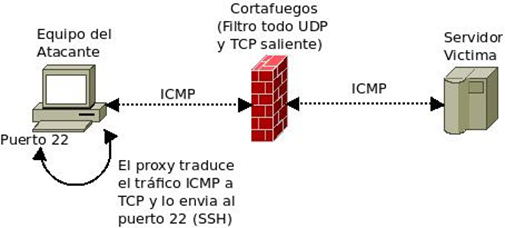
SNMP

El Protocolo simple de administración de redes es un protocolo de capa de aplicaciones que usa un sistema de llamada y respuesta para verificar los estados de muchos tipos de dispositivos, desde switches hasta impresoras. SNMP se puede usar para monitorear el estado y la configuración de los sistemas.



ICMP

Los dispositivos de red, como los routers y servidores, usan el Protocolo de mensajes de control de Internet para enviar información de operaciones por IP y para generar mensajes de error ante fallas de dispositivos.



CDP

[Cisco Discovery Protocol](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html) facilita la administración de dispositivos de Cisco al detectar estos dispositivos, determinar su configuración y permitir que los sistemas usan diferentes protocolos de capa de red para obtener información el uno del otro.



## 2.3.2 Monitoreo de memoria

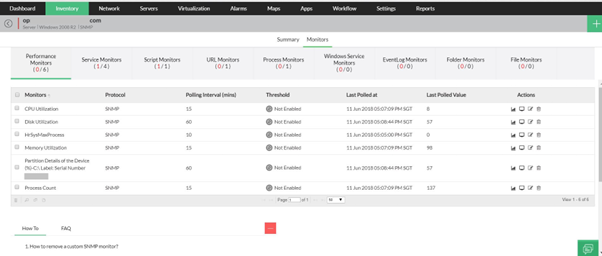
El monitoreo de memoria es esencial para garantizar el máximo rendimiento. Las altas tasas de utilización de la memoria se traducen en una disminución del rendimiento de los procesos asociados.

Además, un aumento constante de la utilización de la memoria a lo largo del tiempo puede indicar una fuga de memoria. Una fuga de memoria es cuando la memoria es asignada por los procesos cuando comienzan, pero no es liberada cuando terminan. Las fugas de memoria degradan el rendimiento del dispositivo con el tiempo. Típicamente, el dispositivo no responde cuando la memoria ya no está disponible.

El monitoreo de memoria mantiene un registro de la memoria libre disponible. El uso de la memoria es supervisado para que los cambios inesperados en el uso puedan ser detectados, analizados y corregidos.

El monitoreo proactivo de la memoria mediante informes personalizables proporciona una visión profunda del uso de la memoria. El acceso a esta información ayuda a garantizar que los problemas de utilización de la memoria no obstaculicen la disponibilidad o el rendimiento de la aplicación, y proporciona una experiencia más satisfactoria al usuario final.

La utilización de la memoria es el promedio derivado del porcentaje de memoria disponible en uso en un momento dado.



Con programas especializados en gestión de memoria, lo que hacen es  monitorear la utilización de la memoria en servidores basados en Windows y Unix usando [protocolos SNMP](https://www.manageengine.com/latam/network-monitoring/tutorial-fundamentos-protocolo-snmp.html), [WMI](https://www.manageengine.com/latam/network-monitoring/monitoreo-de-wmi.html) o CLI.

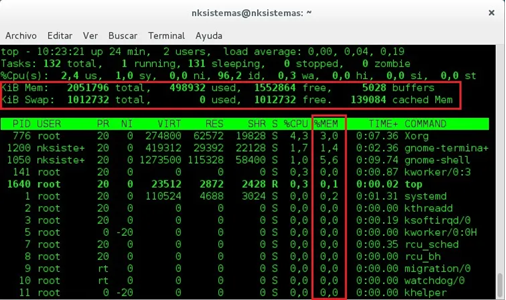
El monitoreo de memoria le permite establecer umbrales de memoria para que sea alertado si la utilización de la memoria de su equipo alcanza un nivel crítico predeterminado por usted.

Estos programas garantizan que:

* Las fugas de memoria son detectadas antes de que el rendimiento se vea afectado.
* La cantidad mínima de memoria física requerida por el sistema siga estando disponible.
* La cantidad total de memoria física asignada al servidor no se exceda.

También monitorean las siguientes métricas

* Memoria física libre
* Utilización de la memoria
* Fallos de página
* Lecturas de página
* Escrituras de página
* Páginas por segundo
* Tamaño de memoria de archivo de página disponible
* Memoria física disponible
* Memoria virtual disponible



## 2.3.3 Monitoreo de CPU

Lo que no se mide no se puede mejorar. El uso de la CPU es una de las métricas de rendimiento más importantes en el monitoreo de servidores. Es el valor principal a analizar para determinar la velocidad de procesamiento de las aplicaciones, que es un indicador clave de rendimiento de la salud de la red y del servidor. Si el uso de la CPU se dispara, la interfaz de usuario de ese servidor finalmente se ralentizará, y los procesos múltiples se bloquearán junto con la aplicación que se ejecuta en ese servidor, creando un efecto de avalancha. El alto uso de la CPU también puede causar problemas de alta utilización de la memoria que pueden hacer que un servidor se caiga. Dado que la utilización de la CPU afecta al monitoreo de los servidores y la red, es necesario medir el uso de la CPU ya que influye directamente en el rendimiento de la red.

La mayoría de las CPU tienen multi-núcleos y multi-hilos para permitir que muchos procesos se ejecuten de forma independiente y simultánea. El uso de la CPU se mide en velocidades de reloj indicadas en Hertz o ciclos por segundo. El uso de CPU es un término ampliamente utilizado en los entornos virtuales y aplicable a los servidores [VMware](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-vmware.html) e [Hyper-V](https://www.manageengine.com/latam/network-monitoring/monitoreo-hyper-v.html" \t "_blank). En el caso de los servidores físicos y otros dispositivos de red, el uso de la CPU se suele denominar utilización de la CPU.

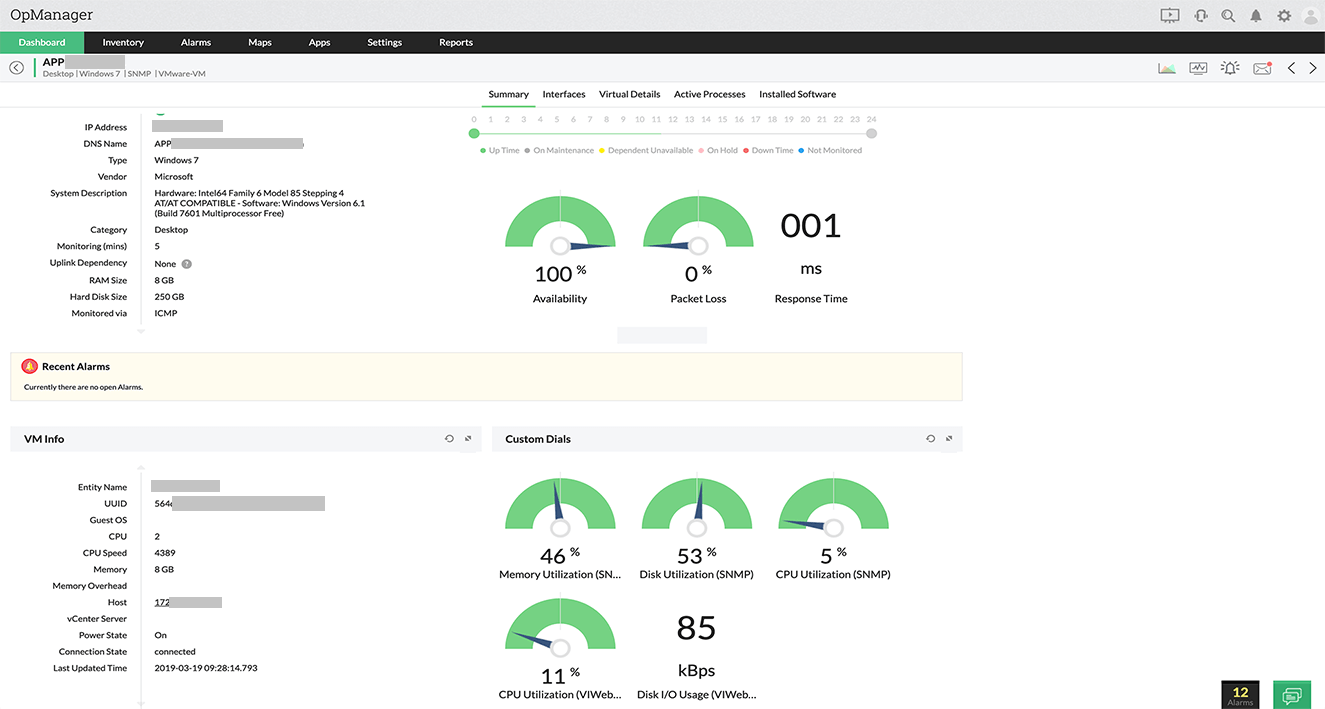
**Necesidad de un software de monitoreo del uso de la CPU**

Un desktop de oficina típico podría consumir sólo el 30 por ciento del uso de la CPU. Sin embargo, dependiendo de los requisitos de la aplicación para una red empresarial, se supone que entre el 70 y el 100 por ciento de la CPU debe ejecutar actividades de agotamiento de la CPU en promedio. Incluso entonces, la mayoría de los servidores funcionarán entre el 90 y el 98 por ciento en promedio, donde se considera que la CPU se utiliza en su totalidad. Si esto ocurre ocasionalmente, digamos para una aplicación ad hoc o una videoconferencia en equipo, es comprensible. No obstante, cuando la utilización de la CPU aumenta más del 80 por ciento con demasiada frecuencia, la CPU tiende a procesar las solicitudes a una velocidad inferior a la deseable y deja caer las solicitudes, lo que provoca un rendimiento lento de la CPU. Para los dispositivos de red, si la utilización de la CPU es alta, la caída de paquetes es inevitable.

En el caso de las redes grandes y empresariales, es casi imposible saber qué servidor tendría problemas de alta utilización de la CPU y requeriría acciones manuales por parte de los técnicos o los administradores de TI. Pero estos problemas pueden obstaculizar directamente la continuidad de las actividades durante un período de tiempo incierto, lo que podría costar a una organización millones de dólares. En un entorno virtual, no es fácil determinar qué dispositivo utiliza un alto recurso de CPU sin que el usuario informe al administrador de TI. Si el pico de la CPU pasa desapercibido, entonces el servidor puede caerse sin razón aparente, causando una interrupción en las operaciones. Con una herramienta de monitoreo del uso de la CPU, no es necesario que el usuario vigile el uso de la CPU. La herramienta logra esto supervisando el uso de la CPU y los posibles cuellos de botella de la CPU, permitiendo a los administradores de TI mejorar el rendimiento de la red.

**Herramienta de monitoreo de uso de la CPU en OpManager**

ManageEngine OpManager [monitorea periódicamente servidores](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-de-servidores.html), [máquinas virtuales (VM)](https://www.manageengine.com/latam/network-monitoring-msp/monitoreo-de-maquinas-virtuales-vm.html), [routers](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-routers-conexiones-wan.html" \t "_blank), [switches](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-de-switches.html), [firewalls](https://www.manageengine.com/latam/network-monitoring/software-gestion-logs-firewall.html), puertos, controladores de LAN inalámbrica (WLC), almacenamiento y dispositivos de red a través de los [protocolos de Instrumentación de Administración Windows (WMI)](https://www.manageengine.com/latam/network-monitoring/monitoreo-de-wmi.html), [Protocolo Simple de Administración de Redes (SNMP)](https://www.manageengine.com/latam/network-monitoring/software-procesamiento-traps-snmp.html) e interfaz de línea de comando (CLI). [OpManager es un software de monitoreo del uso de la CPU](https://www.manageengine.com/latam/network-monitoring/monitoreo-de-cpu.html?cpu-usage-monitor" \t "_blank) que permite monitorear el rendimiento de la CPU, verificar la salud de la CPU, monitorear la disponibilidad de los recursos de la CPU, verificar la velocidad de la CPU y más. OpManager es una consola de monitoreo de uso de CPU de Linux y Windows.



Monitorear el uso de la CPU significa monitorear lo siguiente:

* Utilización de la CPU: Monitorea la utilización de la CPU del dispositivo de red
* Zócalo de la CPU: Monitorea el número de zócalo físico del chip de la CPU
* Velocidad de la CPU: Monitorea la velocidad interna en megahertz de este procesador.
* Tiempo de inactividad: Monitorea el porcentaje de tiempo durante el intervalo de muestreo que el procesador estuvo inactivo
* Tiempo privilegiado: Porcentaje del tiempo de procesador no ocioso que pasa en modo privilegiado
* Tiempo del procesador: Monitorea el uso de la CPU de un proceso individual seleccionado
* Tiempo de usuario: Porcentaje del tiempo de procesador no ocioso que transcurre en el modo de usuario
* Cola de procesadores: Muestra el número de hilos de proceso (unidades de ejecución del programa) que esperan ser ejecutados en todos los procesadores
* Tamaño de la unidad: Monitorea el tamaño físico de la unidad en megabytes (MB)
* Redundancia del PSU: Monitorea el estado de redundancia de la fuente de alimentación
* Fallos de página: Tasa global de páginas con fallos que maneja el procesador
* Recuento de procesos de la CPU: Monitorea el número de procesos que se ejecutan

**Soluciones del Monitoreo del CPU**

**1.- En caso de virus**

Las redes de TI son susceptibles a malware y virus. Computadoras lentas, y quejas a soporte son algunas consecuencias. Con la herramienta de monitoreo de CPU de la marca, los administradores de sistemas pueden determinar si la carga es demasiado alta, incluso cuando realmente pocos empleados están trabajando. También podrán reconocer si el tráfico de datos es inusualmente alto. Como resultado, pueden partir de inmediato en busca de malware, encontrarlo y reparar el daño.

**2.- En procesos de trabajo lentos**

No es raro que ciertas áreas de una empresa detecten interrupciones, pero debido a que los problemas no son demasiado grandes, TI no está informada o se informa demasiado tarde. El resultado: gradualmente, todos los procesos de trabajo de la empresa se vuelven más lentos.

–El software de monitoreo PRTG permite a los administradores diagnosticar rápidamente la utilización del CPU de su servidor.

–Verá el efecto que el nuevo software tiene en los CPU tan pronto como se instale.

–Esto significa que puede actuar con prontitud.

**3.- La tienda en línea no funciona**

Una empresa lanza una campaña web. El tráfico de su sitio aumenta dramáticamente. En consecuencia, la utilización del CPU en el servidor web se dispara. En unas pocas horas, la tienda en línea está funcionando a paso de tortuga. Pocos pedidos llegan a la etapa final de pago. El efecto positivo de la campaña se ve aplastado a medida que los clientes se frustran con el lento sitio web o descubren que ya no pueden usar el servicio a medida que se agota su tiempo de espera.

Aquí también, los administradores son informados sobre el mayor uso del CPU. PRTG viene con un sistema de notificación configurable para enviar notificaciones por correo electrónico o en emergencias por SMS.

**4.- Temperatura del CPU**

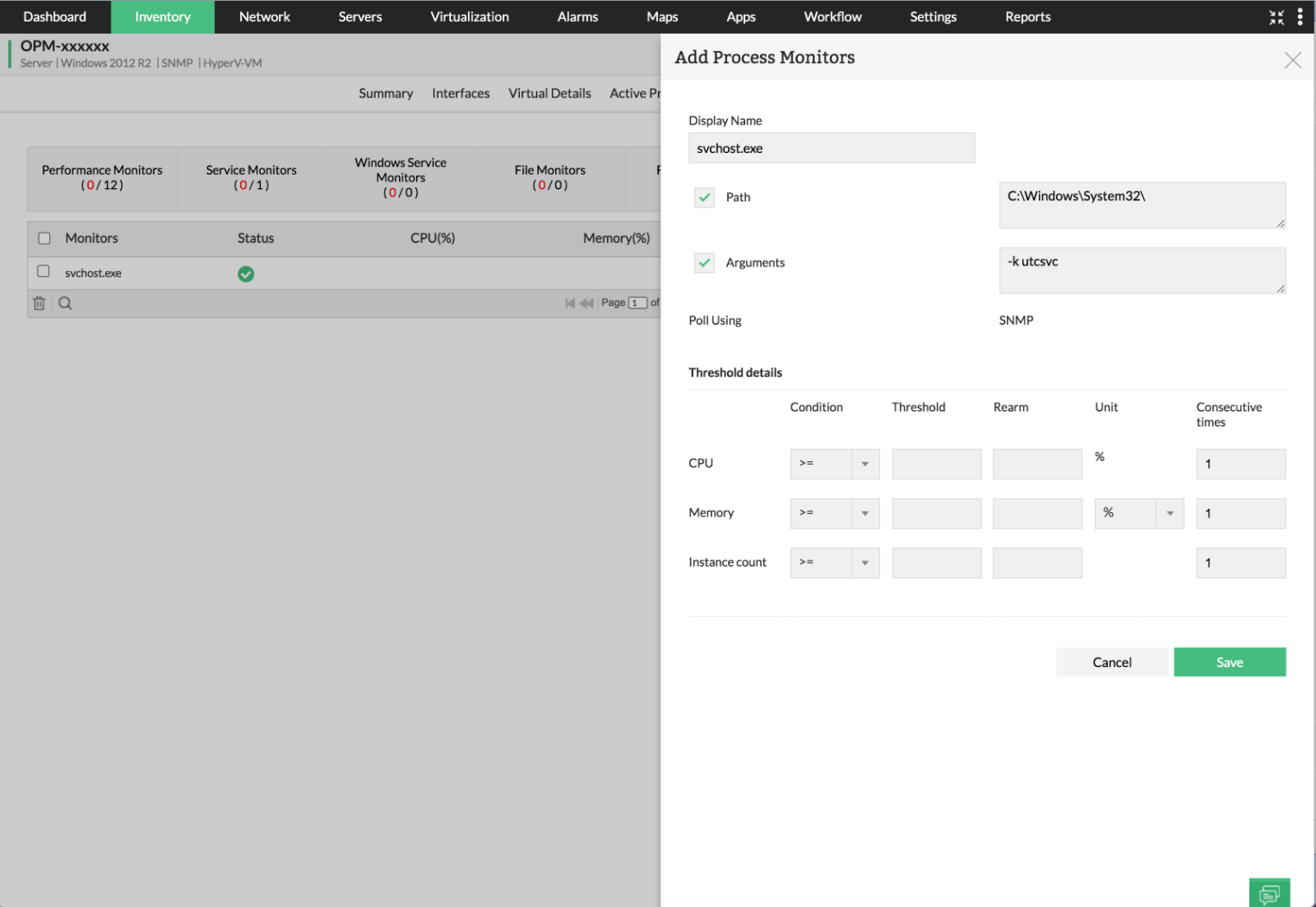
–Temperatura del procesador: es simple física: Cuando la carga aumenta, el núcleo del procesador se calienta más. El sobrecalentamiento puede ocurrir cuando se alcanzan ciertas cargas o cuando un ventilador funciona mal o se cae. A los administradores de sistemas inteligentes les gusta overclockear el CPU para aumentar el rendimiento. Pero el overclocking puede provocar sobrecarga y calor excesivo. La mayoría de los CPU vienen con protección contra sobrecalentamiento. Si se calientan demasiado, se apagan automáticamente.

–Comprobación de la temperatura del CPU: El fabricante suele proporcionar la temperatura máxima recomendada del procesador. Los sensores de estado del sistema PRTG verifican la temperatura de los CPU de una variedad de distintos fabricantes. Los administradores de sistemas también pueden usar el sensor personalizado SNMP para verificar la temperatura de los dispositivos (siempre que sean compatibles con SNMP) y definir las temperaturas que, cuando se exceden, activarán una alarma. En otras palabras, definen valores umbral para ellos mismos.

–Detener la falla del CPU en sus pistas: Si se alcanza un valor crítico, los gerentes de TI recibirán una notificación de inmediato. Esto les permite actuar rápidamente antes de que el CPU falle por completo. Su monitoreo aumenta la estabilidad de toda la red. La red se bloquea con mucha menos frecuencia, lo que ahorra a la empresa tiempo y dinero considerable.

## 2.3.4 Monitoreo de procesos

El monitoreo de los recursos del sistema ([utilización de la CPU](https://www.manageengine.com/latam/network-monitoring/monitoreo-uso-cpu.html), utilización de la memoria,  [temperatura de la CPU](https://www.manageengine.com/latam/network-monitoring/monitoreo-de-cpu.html) etc.) y la configuración de alertas para recibir una notificación cuando se alcancen niveles de utilización no deseados no garantizan completamente el óptimo rendimiento del servidor o la aplicación. Para comprender completamente el origen de la carga en los recursos del sistema, también es necesario conocer el rendimiento de cada proceso crítico asociado con la aplicación o los servicios que se ejecutan en el servidor.

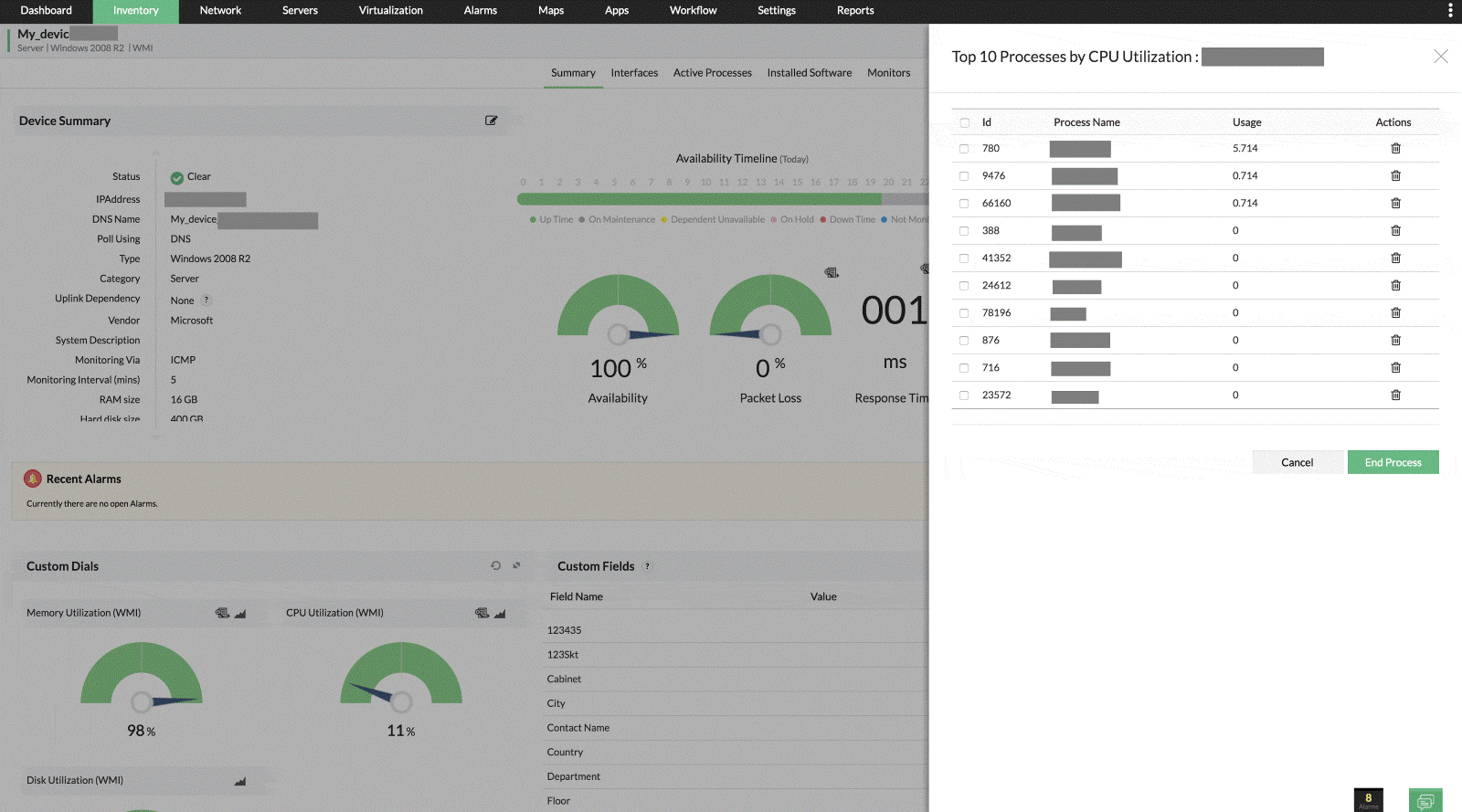


**Configuración fácil y rápida de los monitores de proceso**

Las 'plantillas de proceso' le permiten descubrir, administrar y establecer umbrales fácilmente en varios servidores, desde una sola ventana. Las opciones para configurar umbrales de proceso individuales también están disponibles desde la página de captura del dispositivo. Los monitores de proceso asignados muestran una captura inmediata del estado del proceso, la [utilización de la CPU y memoria](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-cpu-memoria-disco.html), junto con el número de instancias de cada proceso.

**Diagnóstico y monitoreo de procesos remotos**

Las situaciones similares a la aparición de un pico inesperado en la pérdida de memoria o CPU requerirán un diagnóstico inmediato y la solución del problema. El diagnóstico de procesos remotos de OpManager permite a los administradores ver los 10 principales procesos por utilización de CPU o memoria y también permite detener de forma remota los procesos que causan problemas para garantizar el óptimo funcionamiento del servidor.



**Alertas, notificaciones, acciones e informes**

El módulo de [gestión de fallos de OpManager](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-fallos-en-la-red.html) permite activar alertas (correo electrónico o SMS) o notificar a un técnico (alarma web o registro de un ticket) cuando un proceso en particular exceda el umbral establecido. Además de estas funciones de monitoreo proactiva, OpManager también permite ejecutar un script o archivo por lotes para resolver cualquier anomalía imprevista de la red. Por ejemplo, reiniciar un servicio / servidor en particular, cuando un proceso excede un límite establecido. Todos los datos de procesos monitoreados también se almacenan para generar gráficos, tendencias e informes.

**Funciones destacadas:**

* Descubrimiento integral y lista de los procesos que se ejecutan en los dispositivos descubiertos
* Listas que muestran la ID del proceso, nombre del proceso, ruta del proceso y argumento del proceso
* Monitoreo personalizado para identificar varios procesos que tienen diferentes rutas o argumentos y el mismo nombre de proceso
* Los parámetros monitoreados incluyen la utilización de la CPU, la utilización de la memoria y el número de instancias del proceso
* Umbrales individuales para los parámetros monitoreados
* Gestión avanzada de fallas - correo electrónico, SMS, alarma web, [registro de ticket](https://www.manageengine.com/latam/network-monitoring/integracion-mesa-de-ayuda.html), scripts de auto corrección, ejecución de un programa
* Informes sobre la tendencia del proceso para Hoy, Ayer, Últimos 7 días, Últimos 30 días o un período de tiempo personalizado
* Una plantilla de proceso para asociar los procesos a varios dispositivos
* Opción para detener de forma remota los procesos que causan problemas

# 2.4 Análisis de performance y optimización

El análisis de performance y optimización es un conjunto de procesos y técnicas utilizados para mejorar el rendimiento y la eficiencia de sistemas y aplicaciones. El análisis de performance implica la medición, monitoreo y análisis del rendimiento de sistemas y aplicaciones, mientras que la optimización implica la implementación de soluciones para mejorar el rendimiento y la eficiencia.

Se utiliza en una variedad de sistemas, incluyendo servidores, aplicaciones empresariales, redes y sistemas operativos, entre otros. El objetivo principal del análisis de performance y optimización es mejorar la calidad de servicio para los usuarios, al tiempo que se optimiza el uso de los recursos del sistema.

**¿Qué es el análisis de performance?**

El análisis de performance en la administración de servidores se refiere al proceso de monitoreo, medición y análisis del rendimiento de un servidor para identificar posibles problemas y optimizar su funcionamiento. El objetivo del análisis de performance en la administración de servidores es identificar y solucionar los problemas de rendimiento, antes de que afecten negativamente la experiencia del usuario o la disponibilidad de los servicios proporcionados por el servidor.

Implica la recopilación y análisis de datos del servidor, tales como el uso de CPU, memoria y disco, la carga de red y la respuesta del servidor a solicitudes de los usuarios. Además, implica el monitoreo del servidor de forma regular para identificar cualquier problema de rendimiento, como cuellos de botella, tiempo de respuesta lento o alta utilización de recursos, entre otros.

En la práctica, el análisis de performance en la administración de servidores puede implicar la implementación de soluciones de monitoreo de rendimiento, la configuración de alertas para notificar al equipo de administración de cualquier problema, la optimización de la configuración del sistema operativo y del software del servidor, la implementación de políticas de seguridad para proteger el servidor contra amenazas externas e internas, y la implementación de soluciones de backup y recuperación para garantizar la continuidad del negocio.

El análisis de performance en la administración de servidores es importante para garantizar que el servidor sea capaz de manejar la carga de trabajo de manera eficiente y segura, y para mejorar la experiencia del usuario. Además, puede ayudar a reducir los costos operativos y garantizar la continuidad del negocio en situaciones críticas.

**¿Qué es el análisis de optimización?**

El análisis de optimización en la administración de servidores se refiere al proceso de identificar áreas donde se puede mejorar el rendimiento y la eficiencia de un servidor, y aplicar soluciones para lograr una mejor utilización de los recursos del servidor. El objetivo del análisis de optimización en la administración de servidores es maximizar el rendimiento del servidor con los recursos disponibles, ya sea reduciendo los costos, mejorando la calidad o aumentando la velocidad de procesamiento.

Implica la recopilación y análisis de datos del servidor, la identificación de cuellos de botella, la evaluación de la capacidad del servidor para manejar la carga de trabajo y la identificación de problemas de seguridad y la implementación de soluciones para mejorar el rendimiento del servidor.

En la práctica, el análisis de optimización en la administración de servidores puede implicar la optimización de la configuración del sistema operativo y del software del servidor para reducir la utilización de recursos, la implementación de soluciones de virtualización para maximizar el uso de la capacidad del servidor, la actualización del hardware para mejorar el rendimiento, la implementación de soluciones de backup y recuperación para garantizar la continuidad del negocio, la implementación de políticas de seguridad para proteger el servidor contra amenazas externas e internas, entre otras soluciones.

El análisis de optimización en la administración de servidores es importante para garantizar que el servidor sea capaz de manejar la carga de trabajo de manera eficiente y segura, y para mejorar el rendimiento del servidor. Además, puede ayudar a reducir los costos operativos, mejorar la experiencia del usuario y garantizar la continuidad del negocio en situaciones críticas.

**Entornos donde se aplica**

El análisis de performance y optimización es un proceso continuo y dinámico que implica la identificación y solución de problemas de rendimiento en sistemas y aplicaciones. Es importante porque, en el mundo actual, los sistemas y aplicaciones de TI son esenciales para las empresas y organizaciones, y cualquier problema de rendimiento puede tener un impacto significativo en la calidad de servicio y en los resultados de negocio.

1. Servidores: los servidores son esenciales para la infraestructura de TI de las empresas, y cualquier problema de rendimiento puede tener un impacto significativo en la calidad de servicio y en los resultados de negocio. El análisis de performance y optimización se aplica en servidores para identificar y solucionar problemas de rendimiento, y para optimizar el uso de los recursos del sistema.
2. Bases de datos: las bases de datos son fundamentales para muchas aplicaciones empresariales, y el rendimiento de la base de datos puede tener un impacto significativo en la calidad de servicio y en los resultados de negocio. El análisis de performance y optimización se aplica en bases de datos para identificar y solucionar problemas de rendimiento, y para optimizar el uso de los recursos del sistema.
3. Aplicaciones empresariales: las aplicaciones empresariales son esenciales para muchas empresas y organizaciones, y cualquier problema de rendimiento puede tener un impacto significativo en la calidad de servicio y en los resultados de negocio. El análisis de performance y optimización se aplica en aplicaciones empresariales para identificar y solucionar problemas de rendimiento, y para optimizar el uso de los recursos del sistema.
4. Redes: las redes son esenciales para la comunicación y el intercambio de información entre los sistemas y usuarios de una empresa u organización. El análisis de performance y optimización se aplica en redes para identificar y solucionar problemas de rendimiento, y para optimizar el uso de los recursos de red.
5. Sistemas operativos: los sistemas operativos son la base de los sistemas informáticos, y el rendimiento del sistema operativo puede tener un impacto significativo en el rendimiento general del sistema. El análisis de performance y optimización se aplica en sistemas operativos para identificar y solucionar problemas de rendimiento, y para optimizar el uso de los recursos del sistema.

**Análisis de performance y optimización en un servidor**

El análisis de performance y optimización se aplica en un servidor mediante una serie de pasos que incluyen:

1. Monitoreo y medición: Se realiza una medición y monitoreo del rendimiento del servidor, incluyendo el uso de la CPU, memoria, disco y red. Esto se puede hacer mediante herramientas de monitoreo de rendimiento, como Nagios, Zabbix, Cacti y Munin.
2. Identificación de cuellos de botella: Se identifican los cuellos de botella y los puntos débiles del servidor, donde el rendimiento es más lento o limitado. Esto se puede hacer mediante la revisión de los registros del sistema, análisis de bases de datos y herramientas de monitoreo de rendimiento.
3. Diagnóstico de problemas: Una vez que se han identificado los cuellos de botella, se realiza un diagnóstico de los problemas específicos que están afectando el rendimiento del servidor. Esto puede requerir la revisión de los registros del sistema, análisis de bases de datos y la ejecución de pruebas de carga.
4. Optimización del servidor: Con los problemas identificados y diagnosticados, se procede a la optimización del servidor. Esto puede incluir la configuración de la red, la asignación de recursos del sistema, la eliminación de procesos innecesarios y la configuración de bases de datos y aplicaciones para un mejor rendimiento.
5. Monitoreo continuo: Después de la optimización, es importante monitorear continuamente el rendimiento del servidor para asegurarse de que se mantenga en niveles óptimos. Esto se puede hacer mediante la implementación de herramientas de monitoreo de rendimiento y la revisión regular de los registros del sistema.

**Aplicaciones y softwares**

Hay varias aplicaciones y softwares que se pueden utilizar para realizar análisis de performance y optimización en servidores. Algunas de las herramientas más populares incluyen:

* Nagios: Es una herramienta de monitoreo de red de código abierto que se utiliza para monitorear la salud del sistema y la disponibilidad de servicios en tiempo real.
* Zabbix: Es otra herramienta de monitoreo de red de código abierto que se utiliza para monitorear el rendimiento de servidores, redes y aplicaciones.
* Cacti: Es una herramienta de monitoreo de red de código abierto que se utiliza para monitorear el rendimiento de servidores, redes y dispositivos de red.
* Munin: Es una herramienta de monitoreo de red de código abierto que se utiliza para monitorear el rendimiento del sistema y generar gráficos y alertas.
* New Relic: Es una plataforma de monitoreo de aplicaciones y servicios en la nube que se utiliza para monitorear el rendimiento de servidores y aplicaciones.
* SolarWinds Server & Application Monitor: Es una herramienta comercial de monitoreo de servidores y aplicaciones que se utiliza para monitorear el rendimiento de servidores, aplicaciones y bases de datos.

# Bibliografía

*[1] M. (s. f.). Monitoreo de memoria | Software de gestión de memoria - ManageEngine OpManager.* [*https://www.manageengine.com/latam/network-monitoring/monitoreo-de-memoria.html*](https://www.manageengine.com/latam/network-monitoring/monitoreo-de-memoria.html)

*[2] ¿Qué es el monitoreo de red? (2022, 22 abril). Cisco.* [*https://www.cisco.com/c/es\_mx/solutions/automation/what-is-network-monitoring.html*](https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html)

*[3] M. (s. f.-a). Monitoreo de procesos | Software monitor de procesos y recursos del sistema - ManageEngine OpManager.* [*https://www.manageengine.com/latam/network-monitoring/software-monitoreo-de-procesos.html*](https://www.manageengine.com/latam/network-monitoring/software-monitoreo-de-procesos.html)

*[4] M. (s. f.-b). Monitoreo de uso del CPU | Software de monitoreo de rendimiento de uso del CPU - ManageEngine OpManager.* [*https://www.manageengine.com/latam/network-monitoring/monitoreo-uso-cpu.html*](https://www.manageengine.com/latam/network-monitoring/monitoreo-uso-cpu.html)

*[5] R. (2020, 15 julio). Monitoreo del CPU, su importancia en tiempos de Coronavirus. eSemanal - Noticias del Canal.* [*https://esemanal.mx/2020/07/monitoreo-del-cpu-su-importancia-en-tiempos-de-coronavirus/*](https://esemanal.mx/2020/07/monitoreo-del-cpu-su-importancia-en-tiempos-de-coronavirus/)

*[6]  A. (s. f.). AdministraciÃ3n de servidores: todos los secretos. https://axarnet.es/blog/administracion-de-servidores*

*[7] L. (2022, 10 junio). Administración de servidores: todo lo que debes saber.* [*https://www.lage.com.mx/blog/administracion-de-servidores*](https://www.lage.com.mx/blog/administracion-de-servidores)

*[8] A. (s. f.). AdministraciÃ3n de servidores: todos los secretos.* [*https://axarnet.es/blog/administracion-de-servidores*](https://axarnet.es/blog/administracion-de-servidores)

*[9] Carrero, L. (2023, 24 enero). ¿Qué engloba la administración de servidores? Stackscale.* [*https://www.stackscale.com/es/blog/administracion-servidores/*](https://www.stackscale.com/es/blog/administracion-servidores/)

*[10] Castillo, J. D. L. C. (s. f.). 2. Administracion de servidores. prezi.com.* [*https://prezi.com/6hstiv5pquiw/2-administracion-de-servidores/*](https://prezi.com/6hstiv5pquiw/2-administracion-de-servidores/)

*[11] L. (2022, 10 junio). Administración de servidores: todo lo que debes saber.* [*https://www.lage.com.mx/blog/administracion-de-servidores*](https://www.lage.com.mx/blog/administracion-de-servidores)

*[12] Z. (2015, 2 diciembre). Administración de servidores. Qué incluye. Zierzo Telecom.* [*https://zierzo.es/administracion-de-servidores-que-incluye/*](https://zierzo.es/administracion-de-servidores-que-incluye/)

*[13] McClure, S., Scambray, J., & Kurtz, G. (2009). Hackers Exposed: Network Security Secrets & Solutions. 6th Edition. McGraw-Hill Osborne Media.*

*[14] Nagios. (s.f.). Nagios - The Industry Standard In IT Infrastructure Monitoring. Recuperado el 21 de febrero de 2023, de* [*https://www.nagios.org/*](https://www.nagios.org/)

*[15] Zabbix. (s.f.). Zabbix:: The Enterprise-Class Open Source Network Monitoring Solution. Recuperado el 21 de febrero de 2023, de* [*https://www.zabbix.com/*](https://www.zabbix.com/)

*[16] Cacti. (s.f.). Cacti® - The Complete RRDTool-based Graphing Solution. Recuperado el 21 de febrero de 2023, de* [*https://cacti.net/*](https://cacti.net/)

*[17] Munin. (s.f.). Munin - Networked Resource Monitoring Tool. Recuperado el 21 de febrero de 2023, de* [*http://munin-monitoring.org/*](http://munin-monitoring.org/)

*[18] New Relic. (s.f.). Application Performance Monitoring and Management | New Relic. Recuperado el 21 de febrero de 2023, de* [*https://newrelic.com/*](https://newrelic.com/)

*[19] SolarWinds. (s.f.). Server & Application Monitor. Recuperado el 21 de febrero de 2023, de* [*https://www.solarwinds.com/server-application-monitor*](https://www.solarwinds.com/server-application-monitor)