SOBRE LOS SERVICIOS ADICIONALES

COBERTURA DEL MONITOREO PROACTIVO

Los servicios adicionales son opcionales, pero sumamente recomendables para tener la mayor tranquilidad posible. A continuación, se detalla cada uno de los servicios que cubre el monitoreo proactivo sobre su servidor.

MONITOREO PROACTIVO

Red: Monitoreamos tanto la capacidad de hacer "ping" al servidor como el estado del propio agente de monitoreo para detectar cualquier problema relacionado con la red.

Uso de CPU: Buscamos un uso elevado de la CPU de dos maneras diferentes: uso actual elevado y promedios históricos elevados.

Uso de memoria (RAM): Monitoreamos tanto eventos de falta de memoria (OOM) como promedios históricos altos.

Sshd: El servicio se supervisa para garantizar que se esté ejecutando.

Chkservd y Tailwatchd: Los procesos chkservd y tailwatchd se monitorean para garantizar que se estén ejecutando.

DNS: Monitorizamos BIND (named), MyDNS, NSD y PowerDNS

Ipalias: ipaliases es responsable de administrar IP adicionales en su servidor. Si falla, las IP adicionales serán completamente inalcanzables, por lo que queremos asegurarnos de que esté funcionando.

Servidor web/httpd: Monitoreamos tanto Apache (httpd) como Litespeed usando detección avanzada de flaps que nos permite detectar no sólo si su servidor está activo o inactivo, sino también si ha estado "flapping" hacia arriba y hacia abajo (es decir, múltiples reinicios dentro de un período determinado) incluso entre nuestras comprobaciones.

Mysql: Monitoreamos MySQL y MariaDB con detección avanzada de solapas para que podamos saber si ha estado subiendo o bajando.

SMTP: SMTP es responsable del envío de correos electrónicos. Supervisamos el servidor SMTP para garantizar que se puedan realizar conexiones al servidor.

POP3 e IMAP: POP3 e IMAP son formas de descargar correo electrónico a través de correo web o a un cliente de correo electrónico. Monitorizamos ambos tipos de servicios.

Cron: El servicio cron programa todo, desde actualizaciones del sistema hasta la funcionalidad necesaria para sus sitios. También monitoreamos su estado.

Uso del disco: Monitoreamos diferentes umbrales de uso del disco, ya que una raíz llena o la partición /tmp provocarán que los servicios fallen, o una partición de copia de seguridad llena en servidores dedicados significa que no se generarán nuevas copias de seguridad.

Cola de correo electrónico: Buscamos grandes colas de correo electrónico que puedan ser indicativas de SPAM saliente. El SPAM saliente puede dañar la reputación de su IP y afectar la capacidad de entrega del correo electrónico.

ConfigServer Firewall (CSF) y demonio de error de inicio de sesión (LFD)

El proceso CSF/LFD debe estar ejecutándose para que el firewall funcione correctamente.

Versiones de sistema operativo y panel

No activamos alertas automáticas basadas en las versiones del sistema operativo/panel, pero usaremos los datos para comunicarnos con usted si surge algún problema. No lo hacemos automáticamente ya que una versión desactualizada no causará por sí sola un tiempo de inactividad.

¿Qué sucede cuando detecta un problema?

Cuando nuestro sistema detecte un problema, automáticamente abriremos un ticket con nuestro equipo de soporte. El ticket se abre con la prioridad establecida en crítica y se asigna a un técnico que comenzará a investigar el problema.

Tomaremos las medidas necesarias y razonables para resolver el problema sin su intervención. Una vez que hayamos resuelto el problema, le avisaremos que hicimos y la causa del problema, si se puede determinar.

En raras circunstancias, le solicitaremos su opinión antes de poder tomar medidas correctivas si la acción necesaria involucra cosas fuera de nuestro alcance de trabajo.

Acceso al servidor

Como parte de nuestros servicios proactivos de monitoreo/administración, instalaremos ps-openssh-service desde nuestro repositorio RPM. Esto nos dará acceso privado para trabajar en su servidor sin necesitar su contraseña de root.

Este sistema utiliza autenticación segura basada en claves a través del proceso SSH existente en su servidor. No nos permite acceso global: nuestro equipo solo puede usar el sistema para acceder a su servidor cuando tiene un ticket de soporte proactivo abierto. Además, el sistema está bloqueado para que nadie fuera de nuestra red física pueda acceder a él.