3 fallos en el monitoreo de redes y cómo evitarlos

ipswitch

Nadie está contento cuando los sistemas están lentos

Los largos tiempos de espera causados por las respuestas lentas afectan la productividad en toda su organización. A medida que el tiempo pasa sin una solución, los usuarios comienzan a perder la paciencia.

Es incluso peor cuando tiene problemas de rendimiento recurrentes. Hasta los usuarios más pacientes se unirán en los reclamos. La gerencia superior comienza a quejarse. Y cada miembro de su equipo de TI siente que es responsable de ese objetivo. El ambiente se llena de negatividad.

Ningún equipo quiere sentirse como un fracaso. Pero identificar rápidamente la causa de problemas de rendimiento, en entornos de red cada vez más complejos e interdependientes, puede ser un verdadero desafío. Desafortunadamente, a veces nuestro deseo humano de encontrar la solución rápida nos lleva a procesos, herramientas y comportamientos que no son de ayuda. Esto es lo que causa los fallos.

Cada equipo de TI quiere ser y verse como el mejor así que puede ser útil ver algunos de los fallos comunes. También veremos cómo evitar estos fallos empleando las prácticas de algunos de los equipos de más alto rendimiento del mundo derivadas de un estudio reciente realizado por Enterprise Management Associates (EMA).

ES AÚN PEOR CUANDO ESOS PROBLEMAS SIGUEN PRESENTÁNDOSE

Los usuarios más pacientes se unirán a la tormenta de reclamos. La gerencia superior comienza a quejarse. Y cada miembro del equipo de TI siente que es responsable de ese objetivo.

Fallo #1: Pasar demasiado tiempo en modo reactivo

Todos los equipos de TI pasan parte del tiempo en modo reactivo. Todas las organizaciones experimentan interrupciones de servicio no planificadas. La medida de un buen equipo de operaciones, sin embargo, es cuán a menudo reaccionan en lugar de abordar de manera proactiva los problemas de rendimiento.

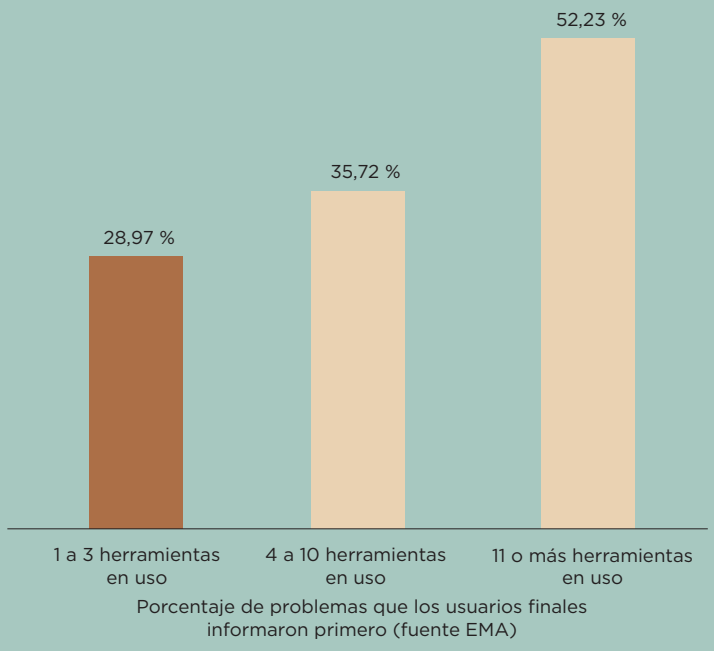
Cuando los usuarios informan un problema, y ya usted está trabajando en una solución, tiene una ventaja en el tiempo de resolución de problemas. Si toma conocimiento de un problema a partir del reclamo de un usuario, es más probable que se perciba que demora demasiado en resolver el problema.

LOS EQUIPOS DE TI DE BAJO RENDIMIENTO PASAN MÁS TIEMPO REACCIONANDO A PROBLEMAS PARA LOS QUE NO ESTÁN BIEN PREPARADOS PARA RESOLVER

La estrategia de la evasión

Un estudio reciente realizado por EMA midió el porcentaje de servicio que afecta los incidentes que se conocieron por primera vez a partir de los usuarios (no a través del monitoreo). Aunque parezca contrario a la intuición, descubrieron una correlación directa entre el porcentaje de problemas informados por los usuarios y la cantidad de herramientas específicas de silo en uso.

Los equipos de bajo rendimiento tienden a tener más herramientas monitoreando diferentes tecnologías (red frente a servidor frente a aplicación). Los equipos de alto rendimiento tienden a confiar en menos herramientas, algunas de estas monitorean una más amplia variedad de tecnologías.



La investigación sugiere que utilizar una pequeña cantidad de herramientas con un alcance más amplio de tecnologías ofrece una ventaja. La visibilidad de extremo a extremo y las alertas con reconocimiento de dependencia ayudan a permitir la detección más temprana de problemas en desarrollo.

Encontrar el problema antes que los usuarios requiere diligencia. Deben establecerse alertas de monitoreo basadas en umbrales para que brinden advertencias tempranas significativas de las condiciones en una tecnología que puede llevar a problemas corriente abajo.

Estos umbrales de alerta deben basarse en datos de rendimiento históricos. De este modo, pueden configurarse para lograr el equilibrio fino de no generar demasiados falsos positivos a la vez de detectar las condiciones problemáticas.

La estrategia de la evasión

En el estudio de EMA también se muestra la correlación entre la cantidad de herramientas de monitoreo y el tiempo utilizado en la resolución del problema. Adivinó, más herramientas no es igual a mejor en este caso.

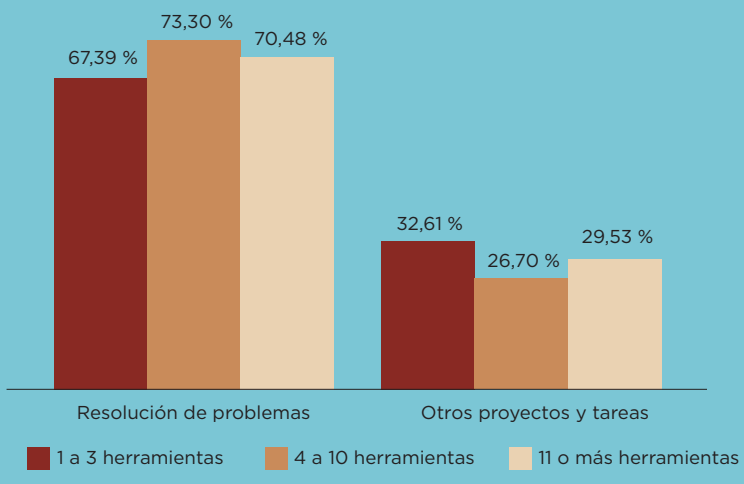
Las herramientas específicas de silo por lo general se configuran para detectar lo que el experto en la materia (SME) considera problemático. Eso puede no ser la misma condición que alguien responsable de un servicio de extremo a extremo observaría para indicar las posibles causas de problemas en etapas posteriores. Lo que pasa como una condición "saludable" en un nivel de la pila de prestaciones de servicios puede provocar resultados desastrosos en un nivel superior.

El enfoque de monitoreo de "demasiadas herramientas en silo" a menudo suma un retardo considerable al tiempo medio de resolución (MTTR), especialmente en entornos de TI más complejos. Además, los equipos de TI con una a tres herramientas de monitoreo utilizan casi 33 % de su tiempo en otras tareas y proyectos. Eso significa 10 % a 20 % más de tiempo en proyectos significativos con cuatro o más herramientas.

Fallo #2: Pasar demasiado tiempo resolviendo problemas

Como dijimos anteriormente, identificar la causa raíz de los problemas en entornos de red complejos puede ser un verdadero desafío. Desafortunadamente, muchos equipos de TI se preparan para perjudicarse al adoptar procesos, herramientas y comportamientos que no son de ayuda. Un buen ejemplo es confiar en una gran cantidad de herramientas dispares de monitoreo de tecnología específica.

En esas condiciones, los equipos de monitoreo operan sin una vista de "extremo a extremo" del problema que están intentando resolver. Esto lleva a una serie de mejores predicciones de las posibles causas. A medida que cada camino sucesivo de diagnóstico falla en abordar el problema, el tiempo pasa y los usuarios se frustran más.



Fallo #3: Imposibilidad de encontrar y solucionar la causa raíz

Cuanto más complejo el problema, menor es la probabilidad de encontrar la causa rápidamente. Algunos problemas, como aquellos que involucran interdependencias entre middleware, aplicaciones y bases de datos, son especialmente difíciles de aislar. Cuando los equipos de evaluación tienen dificultad para encontrar la causa real de un problema, se desesperan más por buscar una solución rápida. A menudo, un reinicio rápido de un servidor resolverá el impacto de rendimiento. El servicio se restablece y todos están felices, ¿cierto?

En realidad, los equipos de TI de alto rendimiento se dan cuenta de que este enfoque puede provocar la creación de problemas "zombi" que vuelven a acecharlos. Cuantos más incidentes de impacto en servicios se resuelven con un reinicio, mayor es el porcentaje de tiempo dedicado a solucionar problemas recurrentes.

La estrategia de la evasión

No es probable que pueda encontrar la causa raíz de cada problema que enfrenta. Los equipos de TI de alto rendimiento, sin embargo, encuentran más por lo que crean menos "zombis". ¿Pero cómo exactamente menos herramientas llevan a tasas más altas de identificación de causas raíz?

El truco aquí es que estos equipos sacan provecho de las herramientas que monitorean múltiples tecnologías para brindar una vista más completa de sus entornos. De acuerdo con Enterprise Management Associates (EMA) "Mientras que las herramientas de gestión de redes a menudo fallan al revelar las interdependencias entre las métricas que ellas y otras herramientas recolectan, los sistemas de gestión multifunciones revelan estas interdependencias y las presentan en las operaciones de red de diversas maneras, desde tableros personalizables hasta informes de alertas con reconocimiento de dependencias."

Utilizar una herramienta que provee una vista consolidada y de extremo a extremo de su entorno tiene múltiples beneficios. Recibe alertas de más problemas antes de que los usuarios los informen y podrá resolver los problemas más rápidamente. Estos dos beneficios combinados le dan más tiempo, sin presión, para encontrar la causa raíz de los problemas antes de que los usuarios se frustren. Esto permite que los equipos de alto rendimiento identifiquen las causas raíz del problema y creen menos "zombis".

Evite los 3 fallos del monitoreo de redes con WhatsUp® Gold

WhatsUp® Gold es la herramienta de monitoreo de redes favorita de decenas de miles de profesionales de TI. Le permite monitorear cualquier combinación de redes, servidores, máquinas virtuales, aplicaciones, flujos de tráfico y configuraciones en entornos de Windows, LAMP y Java. Es más, puede hacerlo todo con una licencia flexible y asequible que le permite combinar lo que monitorea a voluntad. No es necesario comprar licencias individuales para aplicaciones, dispositivos de red o fuentes de flujo de redes; está todo incluido.

Monitoree proactivamente las redes, el tráfico, los servidores físicos, las VM y aplicaciones con mapas, tableros y alertas potentes y fáciles de usar. Nuestro exclusivo mapa interactivo muestra rápidamente la salud de la red de extremo a extremo, de la infraestructura y de los dispositivos virtuales, lo que proporciona el contexto de la manera en que todo está conectado y responde dinámicamente a las interacciones para ofrecerle los tiempos de respuesta más rápidos.

WhatsUp Gold agiliza los flujos de trabajo permitiéndole iniciar las tareas de gestión directamente desde un mapa o área de trabajo interactivos. Cambie fácilmente entre las vistas física, virtual, inalámbrica y de dependencia para acelerar el análisis del origen. Los flujos de trabajo están optimizados, son más intuitivos y se inician desde el mapa de redes o desde una amplia gama de tableros fácilmente customizables. El resultado es una solución de problemas más simple e intuitiva que le permite encontrar y solucionar los problemas más rápido que antes.

Acerca de Ipswitch

Con más de 1 millón de usuarios de 42 000 empresas que gestionan más de 150 000 redes en 116 países, Ipswitch diseña y desarrolla software líder de la industria que permite la entrega simple de rendimiento y seguridad las 24 horas del día, los 7 días de la semana, en entornos locales, virtuales, de red. Equipos de TI de todo el mundo confían en 25 años de innovación para optimizar y asegurar sus transacciones comerciales, aplicaciones e infraestructura con la trasferencia segura de archivos Ipswitch MOVEit®, el monitoreo de redes Ipswitch WhatsUp® Gold e Ipswitch WS_FTP®. Disponible de manera directa o a través de alianzas estratégicas con proveedores estratégicos de TI y el ecosistema de socios globales de rápido crecimiento de la empresa, la amplia cartera de Ipswitch mejora el rendimiento de aplicaciones y de redes, monitorea entornos de TI diversos y garantiza el intercambio seguro de datos que cumple con PCI, HIPAA, GDPR y otros requisitos regulatorios y de seguridad de datos de la industria y del gobierno.

La empresa cuenta con oficinas en EE. UU., Europa, Asia y América Latina. Para obtener más información, visite https://es.ipswitch.com/ o conéctese en LinkedIn y Twitter. Para conocer acerca de las alianzas estratégicas de Ipswitch y de su red global de socios, visite https://es.ipswitch.com/partners.

ipswitch

Conozca cuán fácil es evitar los 3 fallos de monitoreo de red.

Descargue su versión de PRUEBA GRATUITA de Ipswitch WhatsUp® Gold