

El próximo desafío para la Seguridad de base de datos: Virtualización y Cloud Computing

Autor: [Slavik Markovich](#) (Co-Founder y CTO de Sentrigo)

Edición y Corrección: Lic. Cristian Borghello, CISSP

Fecha Publicación: 11 de abril de 2010

Publicado en [Segu-Info](#)

Original: <http://www.dbta.com/Articles/Editorial/Trends-and-Applications/The-Next-Challenge-for-Database-Security--Virtualization-and-Cloud-Computing-66367.aspx>

Introducción

Ya es bastante difícil bloquear los datos sensibles sabiendo exactamente en qué servidor se está ejecutando la base de datos, pero ¿qué vas a hacer cuando se implemente la virtualización y estos sistemas estén en constante movimiento?

Asegurarse de que los administradores de la propia base de datos (DBAs) y los administradores de sistemas no están copiando o consultando expedientes confidenciales, ya es un desafío; ¿cómo vas a saber cuando los miembros de tu proveedor en la nube no esté utilizando sus privilegios indebidamente?

Estos son sólo dos de los obstáculos que cualquier empresa debe superar para implementar una plataforma de base de datos segura en un entorno virtual, o en la nube. En algunos casos, estas preocupaciones han impedido a las organizaciones que se muevan a la virtualización y al cloud computing.

Seguridad en un entorno de Sistemas Dinámicos

Ya sea que estemos hablando de tu propio centro de datos de VMware, o una nube de Amazon EC2, una de las principales ventajas es la flexibilidad. Mover servidores, y añadir o quitar recursos según sea necesario, te permite maximizar el uso de tus sistemas y reducir el gasto. Pero, también significa que tus datos sensibles, que residen en nuevas instancias de tus bases de datos. Mientras que ganas más flexibilidad, el control del acceso a datos se hace mucho más difícil. Si la información contenida en dichas solicitudes está sujeta a normativas, tales como Payment Card Industry Data Security Standard (PCI DSS) o Health Insurance Portability and Accountability Act (HIPAA), necesitas ser capaz de demostrar a los auditores que estás seguro.

Al buscar soluciones para controlar estos servidores "transitorios" de base de datos, la clave del éxito estará en encontrar una metodología que sea fácil de implementar en las nuevas máquinas virtuales (VM) sin participación de la administración. Cada una de estas máquinas virtuales tendrán que tener un sensor o un agente que se ejecutan localmente - y este software debe ser capaz de dotarse de forma automática junto con el software de base de datos, sin necesidad de administración de sistemas intrusivos, tales como reiniciar, por ejemplo cada vez que necesites para instalar o actualizar los agentes. Incluso mejor, si puede conectarse automáticamente al servidor de control, evitando la necesidad de reconfigurar constantemente para agregar o eliminar nuevos servidores de la

consola de administración. La arquitectura correcta te permitirá ver exactamente dónde se alojan las bases de datos en cualquier momento, registrar toda la actividad y los eventos sospechosos en todos los servidores, dondequiera que se encuentren en ejecución.

Seguimiento intra-Server y tráfico WAN

La virtualización de centros de datos y las arquitecturas cloud computing difieren significativamente en términos de su topología de red. Como resultado, se plantean diferentes desafíos cuando se trata del control de acceso a datos. Si bien muchos de las actuales soluciones de control de las actividades de la base de datos utilizan una red de modelo "sniffing" para identificar las consultas maliciosas, en entornos virtuales de nubes esto no será suficiente. Por otra parte, en cada caso, añadir simplemente un agente local que envía todo el tráfico a un servidor para su procesamiento no será eficiente en estos modelos. Se tendrá que encontrar una solución que esté diseñada para el procesamiento distribuido, donde el sensor local sea capaz de analizar el tráfico de forma autónoma.

Para cloud computing, el ancho de banda de red - y aún más importante, la latencia de red - hará que el procesamiento fuera del host sea demasiado ineficiente. Todo el concepto de cloud computing impide ser capaz de localizar un servidor porque simplemente no se sabe dónde están. Por lo tanto, el tiempo y los recursos invertidos en el envío de cada transacción a un servidor remoto para que sea analizado, necesariamente van a disminuir el rendimiento de la red.

En el caso de la virtualización de centros de datos, el problema se presenta exactamente al revés. Tienes que estar preocupado por el tráfico local de un VM a otra VM, que potencialmente podría ser el mismo servidor. Por ejemplo, tu aplicación de CRM puede estar ejecutándose en el mismo hardware físico que las instancias de Oracle que guardan los datos del CRM. Este tráfico ni siquiera llega a la red - que va directamente de VM a VM, a velocidades de memoria. Intentar enviar fuera todo este tráfico para el análisis, se convertiría rápidamente en un cuello de botella, afectando la eficiencia que se esperaba de la virtualización en el primer lugar.

En ambos casos, usted desea asegurarse de que cualquier solución que elija utilice un "agente inteligente", para que una vez que se establezca la política de seguridad de una base de datos, el agente o el sensor sea capaz de aplicar la protección necesaria y alertas a nivel local.

Esto asegurará que la red no se convierta en el factor determinante en el rendimiento de las aplicaciones de servidor. Para cloud computing (o de hecho, para la gestión remota de los centros de datos distribuidos), se debe cifrar todo el tráfico entre la consola de administración y de los sensores ya que se tiene que limitar la exposición de datos sensibles. El rendimiento también puede mejorarse a través de diferentes técnicas de compresión para que las actualizaciones de políticas y alertas se transmitan de manera eficiente.

Los externos ahora son internos

Uno de los elementos más difíciles de supervisar en cualquier aplicación de base de datos es la actividad de los usuarios con privilegios. Los DBAs y administradores de sistemas tienen muchas opciones a su disposición para acceder y copiar la información sensible, a menudo sin ser detectados por completo o en

formas que pueden ser fácilmente escondidas. El hecho de que en un entorno de cloud computing puede haber personal desconocido en sitios desconocidos con estos privilegios, junto con el hecho de que no tienes el mismo nivel de verificación de antecedentes con respecto a terceros como lo hacías para tu propio personal, hace esto aún más difícil.

Una manera de resolver esto es a través de "separación de funciones," esencialmente garantizar que las actividades de dichos terceros privilegiados sean supervisadas por su propio personal, y que las soluciones en el lado de la nube no sean capaces de ser eliminadas sin alertas.

Otra capacidad crítica es ser capaz de seguir de cerca los activos correspondientes a datos personales (por ejemplo, una tabla de tarjeta de crédito), sin importar el método utilizado para acceder a ella. Usuarios con privilegios pueden crear nuevas vistas, introducir procedimientos almacenados en una base de datos, o generar *triggers* que comprometan la información incluso sin parecer sospechosos.

Estas arquitecturas son en su futuro

Para algunos, la dificultad del seguimiento de bases de datos en una arquitectura virtual o en la nube puede llevarlos a la conclusión de que simplemente no vale la pena el cambio de sistemas. Sin embargo, la mayoría de las empresas probablemente determinarán que es simplemente una cuestión de tiempo hasta que implementen las aplicaciones con datos sensibles sobre uno de estos modelos.

Las organizaciones líderes ya han comenzado a hacerlo, y las herramientas están recuperando el tiempo perdido con los requisitos del cliente e impulsado por las cuestiones antes planteadas. Si estás listo para tratar de virtualizar la base de datos o bases de datos en la nube, la seguridad no debe evitar que te muevas hacia adelante. Sólo asegúrate de que tus metodologías de seguridad son adecuadas frente a los casos especiales que se indican aquí.