Acronis

POR NICK
CAVALANCIA

Retirando de forma Segura WINDOWS SERVER 2003

Por Nick Cavalancia

Tiene menos de un año. Este mensaje puede provocar nervios incluso a los mejores profesionales de IT. Después de todo, su entorno de producción depende de Windows Server 2003 para ejecutar muchas de sus aplicaciones, y ahora toca cambiarlo.

Debe estar haciendo un inventario mental de servidores y aplicaciones que corren actualmente en Server 2003, y algunas de ellas solo son un recuerdo, no es sencillo, y piensa que algunos de ellos no se van a comportar adecuadamente cuando intente el cambio.

Entonces se da cuenta .... No va a ser sencillo.

Por suerte aún queda tiempo. El 14 de Julio de 2015, no es que sus servidores vayan a dejar de funcionar, pero si el día 15 de Julio algo va mal, no habrá soporte de Microsoft para volver a poner en marcha el entorno de producción.

El objetivo es retirar los Windows Server 2003 y mitigar el riesgo cuanto sea posible. Aunque este documento no cubre todos los pasos para el reemplazo de Servidores 2003, cubre los cuatro pasos básicos acerca del riesgo al retirar los servidores Windows Server 2003 y como afrontarlo:

- Falta de Motivación
- Sin Backups
- Consistencia en la Implementación
- Sin Puntos de Referencia o Vuelta atrás

Riesgo 1 – Falta de Motivación

Debe estar pensando, "¿Si no falla porqué debo cambiarlo?". La compatibilidad de aplicaciones y como planifique la migración, son algunas de las razones por las que puede querer no migrar, pero normalmente la principal suele ser Porque requiere mucho esfuerzo realizar una migración.

Pero existe un riesgo al no migrar. A parte de la obviedad de la falta de soporte en sus más importantes servidores de aplicación de producción, es que está ejecutando aplicaciones antiguas. Recuerde que Windows Server 2003 tiene técnicamente 11 años de antigüedad, y muchas de las aplicaciones en ejecución son de 2003, lo que es mucho tiempo. Puede encontrarse que no haya nuevas versiones, e incluso que la empresa que las creo ya no exista.

Es importante tener presente que no se puede contar con un sistema operativo o aplicación para ejecutar las operaciones de la empresa indefinidamente. Debe planificar la obsolescencia tanto para sistemas operativos como aplicaciones, y realizar la migración de Windows Server 2003 a 2012.

Eliminando el Riesgo

Desde que el riesgo es real, y la cuenta atrás no se detiene, cuando antes comience, menor será el riesgo. Necesitará tiempo para planificar el nuevo hardware, infraestructura de virtualización, aplicaciones a reemplazar y para crear un plan de ejecución para retirar sus servidores 2003 e implementar sus nuevos servidores con 2012. No hay sorpresas, solo debe darse cuenta de que debe empezar cuanto antes.

Riesgo 2 –
La Protección de Datos

Puede parece obvio, pero va a necesitar backups de sus datos. Siempre ha sido la regla numero uno, y es aún más importante en este caso. Mientras puede estar pensando "todavía tengo el servidor antiguo, ¿que más puedo necesitar?" recuerde que la razón por la que va a emprender la migración es el "¿Y si...?", es decir "¿Y si mi antiguo servidor ejecutando un Sistema Operativo falla y no hay soporte?". Solo podrá depender de un servidor antiguo con un hardware antiguo como backup tras la migración. Si esta falla necesitará volver a su entorno anterior y volver a comenzar, por lo que necesitará un plan para la protección de datos.

Microsoft recomienda instalaciones limpias, lo que tiene sentido, ya que puede ser que no pueda instalar Server 2012 en su antiguo hardware. Pero muchas empresas pueden considerar realizar una migración de 2003 a 2008, y después a 2012. Esta opción no se recomienda en ningún caso.

Por lo tanto, para muchas empresas, el resultado es la adquisición de nuevos servidores, dejando el entorno anterior intacto. Pero aunque no se modi iquen los servidores antiguos, no podrá utilizarlos para siempre. Necesitara un plan para proteger los diferentes tipos de datos para que estén disponibles tras la migración:

1. **Sistema Operativo Completo –** Tener una imagen del servidor completo o un backup completo del mismo, puede ser su iciente para una recuperación sin Sistema Operativo (Bare Metal Recovery) de cualquier servidor, lo que es muy recomendable. Crear un servidor virtual desde un backup puede ser muy útil (lo veremos más adelante en este documento).

2. **Aplicaciones y Datos –** Piense en Exchange, por ejemplo. Pensará en que tiene copias de sus bases de datos de Exchange, pero si se trata de Exchange 2003, posiblemente no haya tenido en cuenta los grupos de datos que casi siempre se olvidan, como los certi icados SSL, que deben tener copia. Por lo que es importante, no centrarse solo en los grupos de datos obvios, recuerde los soportes a esos datos, tanto los de la empresa como los de aplicaciones de terceros.

3. **Datos de Empresa –** Esta es la parte sencilla. Asegurarse de que se dispone de backups de todas las carpetas compartidas, las carpetas de datos de usuario, etc.

4. **Pefiles de Usuario –** Algunas empresas siguen utilizando perfiles de roaming en clientes con Windows 7. Tener backup de las carpetas que los contienen es crítico.

Eliminando el Riesgo

El riesgo en este caso es no tener acceso a sus datos y entorno antiguo. No piense solo en los backups en términos de migración únicamente. Piense en ellos como un modo de volver a tener datos de referencia de la aplicación que no puede instalar en Server 2012, y que ha tenido que reemplazar por una nueva, así como en términos de cumplimiento normativo y retención de datos.

Puede elegir realizar backups independientes de cada grupo de datos, pero los backups de imagen pueden proporcionarle un backup más completo que simplifique la restauración en caso de ser necesario.

Es también importante que dependiendo de la aplicación, el tipo de industria y las regulaciones aplicables acerca del tiempo de retención de datos, deberá conservar sus backups solo dos o tres años o por el contrario de siete a más años.

Riesgo 3 – La Implementación

Este documento no es acerca de cómo implementar Windows Server 2012 específicamente, queremos dar una visión de cómo eliminar el riesgo de implementación. Una vez ya nos encontramos en esta fase, nos damos cuenta del gran número de servidores, aplicaciones, con iguraciones, parámetros de seguridad y datos que supone, y no puede dedicar todo su tiempo a determinar porque un servicio no se inicia o porque una aplicación no funciona.

Uno de los elementos claves para reducir los ensayos y errores es ser consistente con la implementación. Piénselo, si cada servidor tiene su propia instalación independiente, corre el riesgo de tener distintas con iguraciones, por lo que resolver un problema será mucho mas costoso en lo que a tiempo se re iere.

Windows Server 2008 y 2012 han implementado un signi icativo grupo de nuevas Políticas de Grupo. Y además disponen de nuevas funcionalidades, mejoras de las ya existentes y mucho más. Una migración de esta magnitud, es una oportunidad de establecer unos estándares de con iguración y seguridad para los nuevos servidores. Por lo que la consistencia, de nuevo, es la clave para un proyecto de migración exitoso.

Eliminando el Riesgo

Para eliminar el riesgo de implementación va a necesitar revisar la con iguración de cada servidor. Con Microsoft Deployment Toolkit obtendrá una primera visión de las mejores practicas antes de comenzar. Pero si es como la mayoría de profesionales de IT, necesitará una solución que automatice y simpli ique el proceso, aplicaciones de terceros le pueden ayudar a hacer un despliegue masivo consistente.

Riesgo 4 –
Sin Referencias o Vuelta atrás

¿Recuerda esos backups que iba a realizar? Bien, ahora serán útiles. Server 2012 no es un simple cambio de interface sobre 2003, es una plataforma completamente nueva en comparación, con muchas y mejoradas tecnologías que ni siquiera se habían concebido cuando Windows Server 2003 se lanzó. Por lo tanto no hay garantías de que lo que funcionaba sobre 2003 funcione en 2012. Una búsqueda rápida en los foros de TechNet le devolverá muchas aplicaciones antiguas, independientemente del fabricante, que una vez migradas a la nueva plataforma no funcionan correctamente. No es un fallo de Microsoft, y no es razonable pensar que una aplicación de más de 10 años debería funcionar en el nuevo Sistema Operativo, incluso si es de Microsoft.

Por ejemplo, como parte de su implementación puede empezar a beneficiarse de algunas de las funcionalidades de Windows Server 2012 R2 (algunas de ellas eran nuevas en la versión 2008), como el Dynamic Access Control (un modelo de seguridad que mejora NTFS), y comprobar si rompe la funcionalidad de una aplicación de terceros que funcionaba correctamente en 2003. Es plausible que algo así pueda ocurrir facilmente.

Eliminando el Riesgo

Para eliminar el riesgo, debe mantener al menos una copia de su entorno de Servidores 2003, así mientras implementa los Servidores 2012 y empiece a encontrar problemas, podrá tener ambos entornos como referencia y ver como funcionan las aplicaciones, al tiempo que puede volver atrás (rollback) en caso de que su entorno de producción se vea afectado por un problema que no pueda ser resuelto a tiempo.

Dependiendo del nivel de riesgo que haya determinado al que se va a enfrentar en el proyecto, tiene algunas opciones de mitigarlo utilizando los backups que previamente haya creado. Un entorno en sandbox puede servir como punto de referencia, manteniendo listo para producción la instancia de sus servidores 2003, posibilitando el rollback en caso de ser necesario.

Entorno de Sandbox

Esta táctica se refiere a tener el entorno antiguo en funcionamiento y ver como se utiliza para trabajar, no un solo servidor o aplicación. Es muy sencilla de implementar usando la virtualización; hay muchas soluciones físico a virtual (P2V) en el mercado. Puede conseguir un hypervisor asequible y desplegar el antiguo entorno usando redes virtuales a través de la creación de un entorno en Sandbox, Los sistemas en el sandbox, seguirán funcionando con cualquier otro pero sin acceso al exterior de la red.

Recuerde, este entorno no necesita estar operativo en todo momento. No necesita del uso de costoso hardware ya que no se encuentra en producción, se trata de cómo funciona, lo que es distinto de una nueva implementación que no funciona y como es la antigua, no de que funcione bien.

Rollback Virtual

Tener una copia del equipo con 2003 en espera por si es necesaria le permite responder rápidamente ante cualquier inconveniente: Si es necesario, puede decir al CIO que el entorno de producción no se va a ver afectado por la migración. Si algo va mal, simplemente se inicia el servidor virtual y se puede volver al estado anterior, retrasando la migración al siguiente fin de semana.

Puede que necesite volver a poner su entorno 2003 en producción, por tanto su planificación debería incluir un slot en su infraestructura virtual que tenga los requisitos equivalentes al servidor 2003 que tenía antes.

Retirada sin Riesgo

El tiempo corre. Pero no es necesario que corra y retire sus servidores 2004 poniendo en riesgo su negocio. Poniendo en practica los principios básicos detallados en este documento, no solo será capaz de retirar sus servidores Windows Server 2003, si no de hacerlo de un modo que le permita recuperarse de cualquier problema que pueda surgir en el proceso. La planificación es esencia, pero utilizar los métodos adecuados para automatizar y simplificar el proceso, al tiempo que se permite el acceso al entorno anterior es mucho más seguro.

Con cerca de 20 años de experiencia en IT corporativa, Nick Cavalanc es un reconocido consultor, ponente, formados, escritor y columnista y ha obtenido distintas certificaciones, incluyendo MCSE, MCT, MCNE y MCNI. Ha sido autor y coautor y ha contribuido en más de una docena de libros sobre Windows, Active Directory, Exchange y otras tecnologías de Microsoft. Ha sido ponente en distintas conferencias como en la Microsoft Exchange Conference, TechEd, Exchange Connections, y en incontables webinars y tradeshows en todo el mundo.

Acronis

Acerca de Acronis

Acronis define el estándar para la Nueva Generación de Protección de Datos a través de sus soluciones de backup, recuperación frente a desastres y acceso seguro. Basado en AnyData Engine y su tecnología de imagen, Acronis proporciona backup de todos los ficheros, aplicaciones y Sistemas Operativos a través de cualquier entorno, ya sea físico, virtual, en Cloud o en Movilidad. Todo ello de forma fácil, completa y segura.

Fundada en 2002, Acronis protege los datos de más de 5 millones de clientes residenciales y más de 300.000 empresas en más de 130 países. Con más de 100 patentes, Acronis ha sido galardonado con la nominación de mejor producto del año por Network Computing, TechTarget e IT Professional y cubre un amplio rango de funcionalidades, incluyendo la migración, clonación y réplica.

Para información adicional, por favor visite **www.interhand.net/acronis**
Siga a Acronis en Twitter: **http://twitter.com/acronis.**

InterHAND Servicios Profesionales S. A. es Canal Autorizado por Acronis para Costa Rica
+506 2441-2411 ● acronis@interhand.net

interHAND
Internet en sus manos...