blancco
CERTIFIED DATA ERASURE

Soluciones de borrado de datos para centro de datos y seguridad de computación en nube

Blancco White Paper
Publicado el 26 de marzo de 2013
Segunda edición

Indicé

Resumen

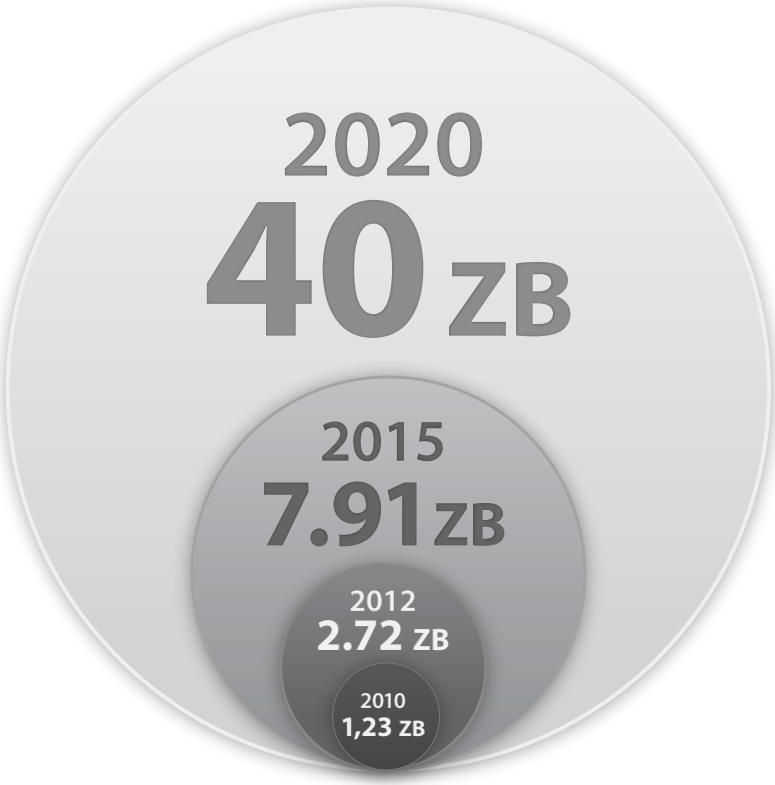
Los avances en las normativas actuales, en la consolidación, en el medio ambiente y en la computación en la nube hacen que los centros de datos necesiten herramientas fiables, rápidas y flexibles como el borrado de datos para asegurar la gran cantidad de datos de clientes. Los centros de datos son entornos de hardware complejos cuyas necesidades de borrado de datos son igualmente complejas. El borrado de datos certificado aborda estas necesidades con la eliminación automatizada de datos para diversos escenarios, desde el borrado de archivos seleccionados con fines PCI DSS, hasta la eliminación de datos de unidades lógicas, servidores, discos sueltos y matrices SAN de almacenamiento.

Al eliminar toda la información y ofrecer una prueba auditable de la eliminación de los datos en puntos vulnerables de transición del hardware, el borrado de datos certificado ofrece a los centros de datos la capacidad de:

- Dar respuesta a la demanda de operaciones sostenibles de los centros de datos mediante la reutilización de equipos.
- Atraer a los clientes de las industrias reguladas como el comercio minorista, la sanidad y la banca.
- Crear un entorno de computación en nube seguro y económico con sólidos procesos de eliminación de datos.
- Desarrollar nuevas fuentes de ingresos mediante la recomercialización segura de los equipos.
- Maximizar internamente el uso de activos mediante una reasignación segura del hardware.
- Atender a las exigencias de consolidación con procesos seguros de transición de equipos.

En este libro Blancco blanco examina las principales tendencias de la industria que afectan a los centros de datos, haciendo hincapié en la necesidad de un borrado de datos certificado. También describe las soluciones de borrado de datos certificadas para una variedad de hardware y configuraciones de almacenamiento masivo que encontramos comúnmente en los centros de datos y en infraestructuras de computación en nube.

La cantidad de datos digitales a nivel mundial



La explosión de datos y la seguridad de la información

Para 2020, IDC prevé que la cantidad de información digital creada y duplicada en el mundo crecerá hasta casi 40 trillones de gigabytes, o más de 40 veces lo que existe en la actualidad.[1] En algún momento, buena parte de esta información estará en centros de datos, gestionada por empresas o proveedores externos de almacenamiento de datos, especialmente con el crecimiento de entornos de computación en nube. Gartner prevé que en 2012 el gasto para hardware de los centros de datos de todo el mundo, incluidos servidores y equipos de almacenamiento y redes, alcanzará los 106.400 millones de dólares y que superará los 126.200 millones de dólares en 2015.[2]

Una gran cantidad de información almacenada en el hardware de los centros de datos es información sensible y debe protegerse para cumplir con un número cada vez mayor de estándares y normativas de la industria como la Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) y Sarbanes-Oxley. Por ello, los directores de activos de centros de datos necesitan una forma de asegurar la información en los puntos vulnerables de transición, a la vez que amplían los sistemas de almacenamiento de la empresa.

La eliminación de datos es una medida fundamental para evitar que los datos inactivos se conviertan de forma inadvertida en datos en tránsito. Normalmente, la protección de datos en tránsito se centra sólo en los datos que pasan por el cable, no en los datos que pasan por un equipo grande de centro de datos, que podría

ser el caso cuando se traslada un centro de datos a otra ubicación o simplemente cuando el hardware del centro de datos cambia de manos.

El boom de la información digital, la proliferación de los centros de datos, las nuevas normativas que exigen la seguridad de datos y otras tendencias de la industria necesitan para eliminar los datos, una solución segura como el software de borrado de datos certificado. El software de borrado de datos certificado satisface los requisitos para lograr una mayor seguridad de los centros de datos, con procesos de borrado automatizados para una variedad de hardware y configuraciones de almacenamiento masivo. Está certificado para la mayoría de estándares de borrado internacionales, protegiendo así la información confidencial de los clientes y cumpliendo al mismo tiempo con las normativas. El borrado de datos certificado es una tecnología segura y económica que permite la reutilización de complejos y costosos sistemas empresariales de almacenamiento, así como la retirada de dichos sistemas al final de su vida útil.

El boom de la información digital, la proliferación de los centros de datos, las nuevas normativas que exigen la seguridad de datos y otras tendencias de la industria necesitan para eliminar los datos, una solución segura como el software de borrado de datos certificado.

Tendencias de los centros de datos y necesidades de borrado

Con el crecimiento de los datos y las normativas en los últimos 10 años, los centros de datos se enfrentan a una serie de cambios y desafíos. Actualmente, existen diversas tendencias principales que afectan a los centros de datos y tienen implicaciones directas que exigen la necesidad de un borrado de datos certificado, como las operaciones sostenibles, el aumento de estándares y normativas sobre la seguridad de la información, el crecimiento de la computación en nube y la consolidación de los centros de datos.

OPERACIONES SOSTENIBLES

Las exigencias de los clientes por una mayor sostenibilidad han avivado un énfasis especial en las operaciones sostenibles en los centros de datos. Las tecnologías de ahorro energético como la virtualización de servidores suponen que menos equipos realizan el mismo trabajo y un crecimiento menor del consumo energético, sin embargo, existen otras consideraciones importantes para ser sostenibles: reducir los residuos electrónicos como ordenadores, servidores, smartphones, etc., a través de una gestión eficaz de los activos.

Los residuos electrónicos son un componente importante del flujo de materiales de los centros de datos y representan el flujo de materiales residuales que más crece en EE. UU. (y lo mismo ocurre en el resto del mundo), con informes que indican una tasa de crecimiento del 8,6 por ciento. Sólo en 2007, se desecharon en EE. UU. más de 41 millones de ordenadores, de los cuales sólo el 18 por ciento se recicló adecuadamente.3 El borrado de datos certificado permite a los centros de datos reducir sus residuos electrónicos eliminando todos los datos de los equipos para poder reutilizarlos o revenderlos, sin preocuparse de que los datos vayan a parar a manos equivocadas. Por ejemplo, debido a la cantidad de residuos electrónicos eliminados de forma incorrecta, Ghana es una de las fuentes del cibercrimen más importantes del mundo

según el Departamento de Estado de EE. UU. y, sufre la contaminación del aire, tierra y agua por los dispositivos electrónicos que se desechan.[4]

ESTÁNDARES Y NORMATIVAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN

El crecimiento de filtraciones de datos confidenciales ha hecho aumentar los esfuerzos por asegurar los datos confidenciales, y ahora 75 países tienen leyes de protección de datos y numerosas industrias que definen sus propias normativas. Muchos centros de datos y proveedores de servicios en nube buscan dar servicio a las industrias con datos altamente regulados, como por ejemplo, el comercio minorista, la banca, el gobierno o la sanidad. Para atraer a estos clientes, es fundamental cumplir con los estándares de la industria, normativas y certificaciones como PCI DSS, HIPAA y Sarbanes-Oxley respectivamente. Los proveedores de servicios en nube en especial se diferenciarán y competirán basándose en el cumplimiento y la efectividad, pero un aspecto clave para los centros de datos será la absorción del coste del cumplimiento a través de procesos automatizados.

Además, se están revisando normativas exhaustivas que requieren la eliminación de datos en EE. UU. con la Consumer Privacy Bill of Rights y en Europa con la legislación de la UE sobre la reforma de protección de datos. La Consumer Privacy Bill of Rights trata el modo de permitir una innovación continua en las tecnologías de la información mientras se ofrece una fuerte protección de la privacidad, incluido el requisito de la eliminación de datos. La legislación de la UE revisa las normas establecidas desde 1995 para dar cabida a avances tecnológicos como los sitios de redes sociales, la computación en nube y los servicios basados en la localización. Esta legislación está siendo revisada por todos los estados miembros de la UE. La legislación exigiría la eliminación de datos en línea y el uso de procedimientos auditables para las empresas que procesan datos personales. También anima a las empresas a utilizar procesos y herramientas certificados. Las empresas que ofrecen servicios en nube deben cumplir con esta legislación si procesan datos de ciudadanos de la UE, independientemente de dónde se encuentren sus servidores.

El software avanzado de borrado de datos ofrece un proceso que automatiza, audita e identifica el borrado de datos de archivos, LUN, discos, servidores y sistemas de almacenamiento que cumple la mayoría de estándares gubernamentales y de la industria.

El software avanzado de borrado de datos ofrece un proceso que automatiza, audita e identifica el borrado de datos de archivos, LUN, discos, servidores y sistemas de almacenamiento que cumple la mayoría de estándares gubernamentales y de la industria. Un aspecto clave de la conformidad es el informe de borrado auditable que demuestra que los datos se han eliminado completamente en los puntos de transición crítica, como la reasignación o recomercialización del hardware, las pruebas de restauración de copia de seguridad o de recuperación de desastres y la reubicación de instalaciones. El informe proporciona datos específicos del hardware como el número de serie, el número de unidades del servidor, el tamaño y la velocidad, así como información sobre el proceso de borrado como el tiempo que ha durado y quién lo ha realizado.

COMPUTACIÓN EN NUBE

Las empresas que pretenden evitar las inversiones en tecnología de la información (TI) por la volatilidad de su economía, junto con una generación de empleados acostumbrada a la tecnología a demanda, ha provocado que la computación en nube (servicios suministrados por Internet) aumente en el mercado global. Gartner prevé que en 2014 los ingresos de la computación en nube saltarán hasta los 148.800 millones de dólares, mientras que Forrester prevé una cantidad de hasta 241.000 millones de dólares para 2020.[5]

La virtualización es una tecnología clave para los entornos de computación en nube. La segmentación de discos físicos para máquinas virtuales (VM) es una tendencia en auge que permite un uso más eficiente y económico del

hardware. Según las previsiones de Gartner,[6] se calcula que en 2014 aproximadamente el 60 % de la carga de trabajo de los servidores será virtualizada. El borrado de VM supone un desafío para los centros de datos, ya que debe realizarse en un entorno activo, en línea y sin afectar a otras máquinas virtuales que se estén ejecutando en una parte específica del hardware.

El crecimiento en el mercado de la computación en nube seguirá conllevando inversiones en los centros de datos. Con este aumento de información almacenada y aplicaciones gestionadas viene la necesidad de los centros de datos de asegurar no sólo la instalación, sino también los valiosos datos que contiene el hardware. Además, mientras que antes el foco estaba en introducir información en la nube, ahora cada vez más lo importante es asegurar esta información cuando sale, por ejemplo cuando se produce un cambio en los proveedores del servicio. El borrado de datos ayuda a los proveedores de servicios en nube a lograr una seguridad mejorada borrando los datos cuando el equipo se reasigna, y puede identificar información específica para que se borre en un momento o caso concreto, como exigen los estándares PCI DSS.

Los centros de datos necesitan un informe auditable procedente de una herramienta de borrado de datos certificada para probar que los datos se han eliminado del equipo seleccionado para su retirada o transferencia.

CONSOLIDACIÓN

Las fusiones, las adquisiciones, los ajustes de producción y muchas otras iniciativas han llevado a la consolidación de los centros de datos. Por ejemplo, la iniciativa de 2010 U.S. Federal Data Center Consolidation incluye planes para cerrar 370 centros de datos durante todo 2012 para reducir los costes gubernamentales y el impacto medioambiental.[7]

A la hora de hacer un cambio, muchos centros de datos optan por actualizar el hardware, sin embargo, Gartner recomienda aprovechar los contratos para negociar una pronta disponibilidad del equipo de reemplazo en la nueva ubicación.[8] En cualquier caso, los centros de datos necesitan un informe auditable procedente de una herramienta de borrado de datos certificada para probar que los datos se han eliminado del equipo seleccionado para su retirada o transferencia.

Cinco niveles de borrado de datos

La tecnología de borrado de datos permite a los centros de datos asegurar información confidencial de los clientes y cumplir al mismo tiempo con las normativas. Asimismo, permite mantener la productividad y unas operaciones sostenibles. Estas soluciones de borrado de datos son especialmente importantes para protegerse contra la pérdida de datos en los puntos de transición de la cadena de custodia y uso del hardware. Para satisfacer las exigencias de una mayor seguridad de los centros de datos, los procesos de borrado automatizados trabajan para una variedad de hardware y configuraciones de almacenamiento masivo.

1. BORRADO A NIVEL DE ARCHIVOS

Los centros de datos con altas exigencias de disponibilidad guardan múltiples copias del mismo archivo de datos con fines de duplicación de la información. Dado que los estándares como PCI DSS exigen el borrado de datos a nivel de archivos y a intervalos concretos, los administradores necesitan una forma centralizada de ejecutar el borrado remotamente de archivos y carpetas seleccionados o duplicados en servidores y en áreas de almacenamiento de toda la red.

En entornos de Windows con sistema de archivos distribuidos (DFS), el borrado de datos debe producirse simultáneamente en sistemas duplicados o sistemas espejos para mantener el tiempo de funcionamiento, mientras se genera una auditoría como prueba de conformidad. En la mayoría de los casos, la herramienta de borrado es invisible en el nivel nodo del servidor y un administrador de sistemas lo gestiona centralmente.

En un entorno virtual, una VM podría configurarse con una unidad virtual que es en realidad un solo archivo en un área de almacenamiento de la red (SAN), en un dispositivo de almacenamiento o en una unidad local. En algunos casos, podría ser importante borrar la VM en un entorno en tiempo real, sin interrumpir las actividades del dispositivo físico de alojamiento.

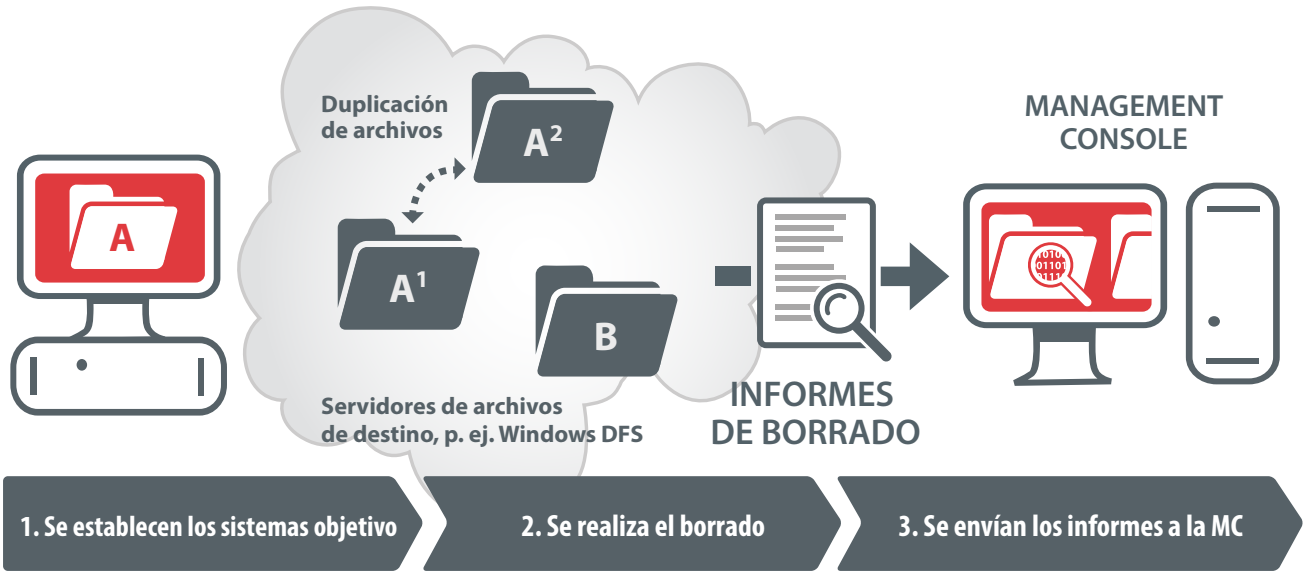


Figure 1. Borrado a nivel de archivos

ALGUNOS EJEMPLOS PARA EL BORRADO DE ARCHIVOS INDIVIDUALES SON:

Conformidad PCI DSS

La información de tarjetas de pago no se debe almacenar durante más de cinco años conforme a los requisitos PCI DSS. Esto indica que los centros de datos necesitan un producto de borrado que elimine datos concretos de los archivos en un momento o caso determinado.

Una herramienta profesional de borrado de datos destruye los archivos individuales en un tiempo y caso concretos, o según marque el usuario o el administrador de sistemas.

Mantenimiento de datos

El borrado es parte de una buena práctica de mantenimiento de datos para que no se almacenen de forma innecesaria demasiadas copias de datos en demasiados sitios, incrementado así el riesgo de pérdida de datos.

Fugas de información

En ocasiones, los datos sensibles o confidenciales se copian a un sistema o aplicación no acreditado o no autorizado. En otras palabras, los datos siguen estando en control de la empresa pero se han copiado en el sitio inadecuado. Los datos clasificados deben borrarse y no solo eliminarse de un sistema no clasificado, por ejemplo.

Fin de alojamiento de unidades virtuales

Cuando un cliente cambia de proveedor de servicios o la VM cambia de ubicación dentro del centro de datos, es necesario un borrado seleccionado para una VM con una unidad virtual que reside en un sistema de almacenamiento o una unidad local. Esto requiere una herramienta que pueda realizar el borrado sin necesidad de volver a arrancar el dispositivo de alojamiento. Tras del borrado, el almacenamiento puede reutilizarse de forma segura sin comprometer los datos del cliente.

Una herramienta profesional de borrado de datos destruye los archivos individuales en un tiempo y caso concretos, o según marque el usuario o el administrador de sistemas. Esta herramienta puede configurarse para que sustituya a todos los comandos de borrado de Windows mediante una destrucción segura de archivos seleccionados en tiempo real, tal como muestra la figura 1. Desde una interfaz central, los administradores seleccionan qué normas y qué áreas de almacenamiento desean borrar. De esta forma, no quedan ningún archivo temporal o información "borrada" como posible riesgo de pérdida de datos. Esta solución se puede supervisar como un servicio de control completo y donde todas las operaciones de destrucción de archivos quedan registradas.

Asimismo, el software de borrado de datos es compatible con la infraestructura de clasificación de archivos (FCI) de Windows Server 2008 R2 de Microsoft, que permite al administrador identificar y borrar información concreta, como información sanitaria (PHI) o datos PCI DSS, independientemente de su ubicación en la red. La herramienta flexible de back end también permite una fácil integración gracias a la clasificación de archivos desarrollada internamente y a los sistemas de gestión.

2. BORRADO A NIVEL DE LUN

En el entorno actual de computación en nube, los centros de datos necesitan opciones seguras y económicas para reutilizar las configuraciones de sistemas de almacenamiento de la empresa sin tener que reconstruirlas. Para conseguirlo, los administradores necesitan una herramienta centralizada que pueda borrar unidades lógicas como LUN en un entorno de almacenamiento activo, donde la matriz de almacenamiento no puede ponerse fuera de línea.

Este escenario abarca a las VM, que pueden configurarse con almacenamiento dedicado de uno o varios LUN en un sistema SAN.

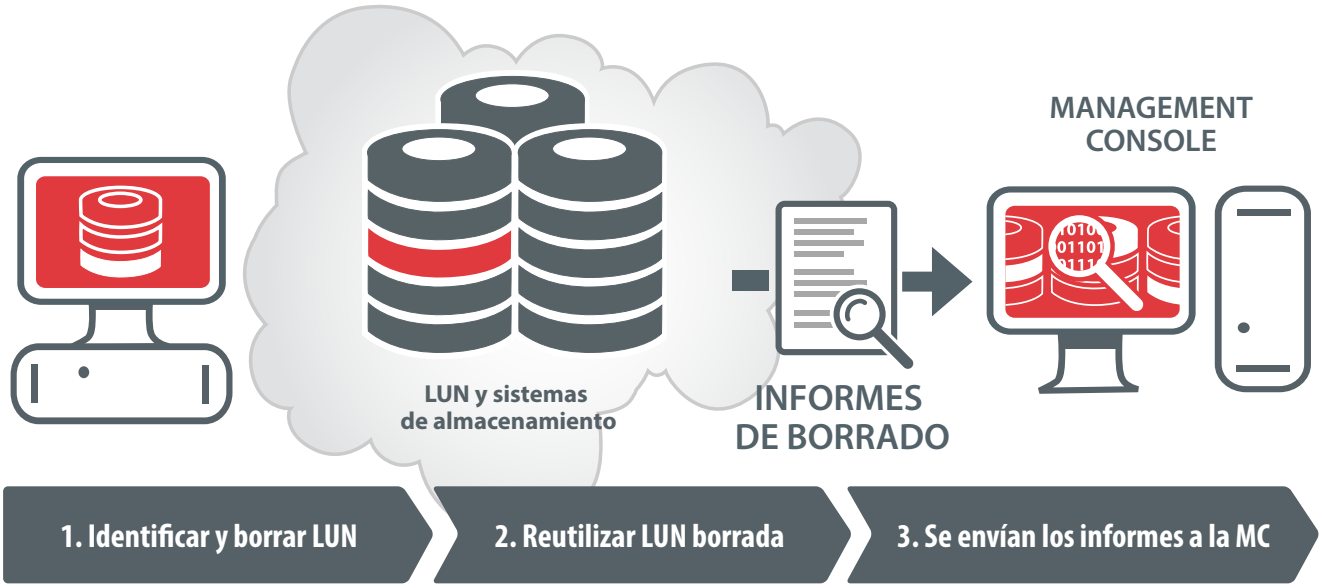


Figure 2. Borrado a nivel de LUN con datos activos.

Una herramienta de borrado debería cumplir con una amplia variedad de políticas, estándares y normativas de borrado como PCI DSS, HIPAA, y los estándares del Departamento de Defensa de EE. UU. (DoD). Esto incluye ofrecer informes de borrado auditables para probar el borrado de LUN, así como facilidad de uso y rapidez en la eliminación de los datos. El borrado de LUN se ejecuta desde el servidor de la aplicación, que tiene una visión del LUN seleccionado y permite el borrado simultáneo de múltiples unidades.

El borrado seguro de LUN puede ser crítico para los proveedores de alojamientos y computación en nube que cuentan con clientes que trabajan, por ejemplo, con el Gobierno de EE. UU. Si un cliente cambia de proveedor de servicios o cambia de plataforma con el mismo proveedor, es necesario que exista una prueba de que se hayan borrado todos los datos del cliente según los estándares del DoD. Sin un borrador de LUN que cumpla con los estándares DoD u otros estándares exigidos, el proveedor de servicios podría tener que tomar medidas drásticas para eliminar los datos de clientes antiguos, como por ejemplo, poner toda una matriz de almacenamiento fuera de línea para borrar unidades físicas o dejar en cuarentena LUN antiguos con datos de clientes, lo que conlleva costes de almacenamiento más altos. Con un borrador de LUN, el mismo proveedor de servicios puede borrar un LUN existente, conforme a un estándar DoD, sin afectar a otros usuarios de la matriz de almacenamiento.

> *Sin el product LUN Eraser, l el cual cumple con regualciones del Departamento de Defensa de los E.E. U.U. u otros estándares, el proveedor de servicio debe de tomar medidas drásticas para eliminar información anterior del cliente.*

ALGUNOS EJEMPLOS PARA EL BORRADO DE LUN SON:

Fin de la suscripción del servicio de alojamiento

Cuando en un entorno de alojamiento se marcha un cliente y se asigna otro usuario a la unidad LUN existente, el borrado es necesario para reutilizar la unidad LUN. Esto ocurre tanto para servidores físicos que utilizan LUN como almacenamiento, como para máquinas virtuales con almacenamiento dedicado en una LUN concreta.

Test de recuperación ante desastres

Tras realizar un test de recuperación ante desastres, existen múltiples copias de datos LUN que deben borrarse por motivos de seguridad.

Figure 3. Borrado de unidades sueltas.

Test de recuperación de copias de seguridad

Como ocurre en el caso de los test de recuperación ante desastres, una copia de seguridad producirá fácilmente terabytes de datos en múltiples copias de LUN y servidores que, por motivos de seguridad, deberían borrarse antes de que el próximo cliente utilice el mismo hardware.

> *El borrado de datos ofrece una solución de borrado personalizada para el entorno de servidores que garantiza un borrado rápido y simultáneo de todos los discos duros conectados (HDD).*

El borrado de datos ofrece versiones LUN que permiten la eliminación simultánea de datos en más de 200 unidades, iniciando instancias paralelas del software, que pueden iniciarse desde una interfaz central administrativa, tal como muestra la figura 2. El software puede borrar cualquier unidad (física o lógica) que un sistema Windows, Unix o Linux pueda detectar sobrescribiendo todo el área de escritura, sector a sector, en el disco o unidad lógicas y conforme al estándar de borrado seleccionado. A continuación, se obtienen los informes de borrado para cumplir con las necesidades de conformidad.

3. BORRADO A NIVEL DE DISCO

El borrado a nivel de disco es necesario para sanear discos duros fuera del alojamiento original, así como con las unidades sueltas de áreas de almacenamiento de servidores en red (SAN). Muchos de estos son unidades RMA (autorización de material devuelto) que necesitan borrado antes de volver al fabricante del equipo original (OEM) bajo garantía.

Debido a requisitos de manipulación y de la cadena de custodia, el borrado local de discos es necesario. De modo parecido al borrado completo de matrices, borrar unidades sueltas requiere un dispositivo externo host/boot y una correcta conectividad entre las unidades que vayan a borrarse y el dispositivo de borrado en cuestión. Una vez el borrado está en curso, una herramienta de borrado debería poder supervisar y generar informes de borrado finales en toda la red, cuando se pueda aprovechar la conectividad de la red.

ALGUNOS EJEMPLOS PARA EL BORRADO DE DISCOS INDIVIDUALES SON:

Sustituir unidades en garantía RMA

El borrado in-situ de discos "fallidos" elimina el contenido del disco para que la unidad puede transportarse sin riesgos al OEM para su sustitución en garantía, evitando así costosos gastos de retención de discos.

Figure 4. Borrado remoto de servidores.

Acumulación de unidades

Si en el pasado no se hubieran utilizado procesos de borrado seguros de final de vida útil, un centro de datos podría tener una acumulación de unidades con datos confidenciales que se deben borrar para evitar el riesgo de pérdida de datos.

Cambio de unidades para servidores de fin de servicio

Cambiar y utilizar unidades sueltas como recambios es un proceso rápido y habitual que agiliza la retirada de un servidor que utiliza unidades saneadas, pero genera unidades sueltas con datos intactos no seguros.

El borrado de datos certificado ofrece una solución de borrado personalizada para el entorno de servidores que garantiza un borrado rápido y simultáneo de todos los discos duros conectados (HDD). Se ejecuta desde un aparato para el borrado a nivel de disco, como muestra la figura [3], para eliminar los datos de las unidades RMA tal como especifique el administrador, que puede elegir entre varios estándares de borrado compatibles internacionalmente. Las unidades RMA de servidores y matrices de disco se sacan de su carcasa y se conectan al aparato de borrado, que se arranca con el software de borrado que reconoce las unidades que deben borrarse.

Con el borrado de datos certificado, se pueden borrar simultáneamente unidades SCSI, SAS, SATA, FC e incluso unidades IDE. Cuando finaliza el proceso de borrado, que como media supone un gigabyte por minuto, se genera automáticamente un informe de borrado y se envía por la red a una consola de administración o a una base de datos de gestión de activos. La consola valida el informe de borrado como genuino, verifica que el borrado sea completo y funciona como un depósito de informes de borrado. El borrado de datos certificado también permite el borrado de las cada vez más habituales unidades de estado sólido (SSD) mediante la opción de seleccionar estándares de soportes de almacenamiento basados en flash.

Para una seguridad completa, los centros de datos necesitan herramientas de borrado que detecten durante el proceso de borrado las áreas protegidas del disco y los sectores reasignados, marcando aquellos que no pueden borrarse.

4. BORRADO A NIVEL DE SERVIDOR

El borrado completo de servidores incluye el borrado de todas las unidades internas conectadas. El borrado a nivel de servidores puede realizarse de forma local o remota. Por ejemplo, el borrado remoto puede implementarse

Ilustración 5: Borrado total en arreglo.

fácilmente con una unidad de CD virtual para servidores con capacidades iLO/IPMI/DRAC. Los informes de auditoría sobre los atributos del hardware y el proceso de borrado de datos son necesarios para garantizar la seguridad de los clientes y cumplir con los requisitos PCI DSS y otras normativas.

Para una seguridad completa, los centros de datos necesitan herramientas de borrado que detecten durante el proceso de borrado las áreas protegidas del disco y los sectores reasignados, marcando aquellos que no pueden borrarse. Según la política y la tolerancia de riesgos, los centros de datos podrían restaurar o revender los servidores después de que se haya realizado el borrado de datos. En cualquier caso, el borrado de datos debe realizarse antes de que el servidor abandone las instalaciones.

ALGUNOS EJEMPLOS PARA EL BORRADO DE SERVIDORES ENTEROS SON:

Fin del servicio

Al final de un ciclo de actualización de hardware, los centros de datos deben borrar de forma segura toda la información de los servidores para cumplir con las normativas y proteger a los clientes. Esto permite revender y reciclar los discos útiles, mientras se genera un entorno sostenible de centros de datos y fuentes de ingresos adicionales.

Fin de la suscripción del servicio de alojamiento

Cuando un cliente finaliza los servicios de alojamiento, el borrado es necesario para la reutilización de un servidor en un entorno de alojamiento.

Reubicación de centros de datos

Los centros de datos se trasladan o se amplían con frecuencia; esto requiere la reubicación de servidores que, de no borrarse de forma segura, puede resultar en una pérdida de datos durante el transporte.

Como en el caso del borrado a nivel de disco, para servidores también hay disponible el borrado de datos certificado. Como en la imagen 4, el administrador arranca el software de borrado desde un CD, USB o mediante la red. A continuación, el software identifica las unidades instaladas que deben borrarse, procede a realizar el borrado y envía un informe a la consola de administración, a la base de datos o a un dispositivo de memoria USB.

Los servidores x86 y x64 se borran con software de borrado de datos certificado. Además, el borrado de datos certificado puede eliminar datos de servidores que sean o no RAID. Para los servidores con un controlador RAID integrado, el software de borrado "rompe" el RAID y directamente borra todos las discos duros internos siguiendo el estándar de borrado seleccionado por el

administrador. Dado que los centros de datos utilizan habitualmente servidores SPARC para satisfacer las necesidades de almacenamiento masivo de datos de las organizaciones, como las instituciones financieras, existe una versión del software de borrado de datos certificado que también funciona con la arquitectura SPARC de empresas como Oracle.

5. BORRADO A NIVEL DE ALMACENAMIENTO

Los centros de datos trabajan con una amplia gama de configuraciones complejas que pueden monetizarse en el momento de su retirada. Los discos SAN y otros dispositivos de almacenamiento masivo se pueden vender si los datos se han eliminado de forma segura en el momento de desecharlos.

Para evitar la necesidad de múltiples productos de borrado, los centros de datos con servidor de alta gama y entornos SAN, necesitan una herramienta que borre una amplia gama de hardware, como discos serial ATA, SAS, SCSI y Fiber Channel. Dado el tamaño de los centros de datos, el borrado simultáneo de múltiples discos es una necesidad.

ALGUNOS EJEMPLOS PARA EL BORRADO DE SISTEMAS DE ALMACENAMIENTO SON:

Fin del servicio de arrendamiento

Al final de un ciclo de actualización de hardware, los datos deben borrarse antes de transportar los sistemas de almacenamiento de vuelta a la empresa de arrendamiento. Mantener las unidades es extremadamente caro y lo mismo ocurre con la destrucción física, debido a los importantes gastos de liquidación del arrendamiento en caso de que se conserve el equipo.

Actualización competitiva del hardware

Al final de un ciclo de actualización de hardware, los centros de datos deben borrar de forma segura las matrices de almacenamiento para poder revender y reciclar discos útiles y crear un centro de datos con un entorno sostenible. Los datos pertenecen al centro de datos y no al OEM, por lo tanto, el centro de datos es el responsable del borrado para evitar fugas de datos.

Para evitar la necesidad de múltiples productos de borrado, los centros de datos con servidor de gama alta y entornos SAN, necesitan una herramienta que borre una gran variedad de hardware.

REUBICACIÓN DE CENTROS DE DATOS

Los centros de datos se trasladan o se amplían con frecuencia; esto requiere la reubicación de sistemas de almacenamiento que, de no borrarse de forma segura, puede resultar en una pérdida de datos durante el transporte.

Existe una versión del software de borrado de datos para los centros de datos que ofrece la destrucción de datos 100 % segura para matrices de almacenamiento de alta gama. El software se ejecuta en un servidor x86 acoplado externamente que no se conecta directamente a los puertos host SAN, sino que se acopla a la carcasa de acceso del dispositivo de almacenamiento (DAE). Algunas matrices de almacenamiento permiten el acceso directo y simultáneo a múltiples DAE mediante interruptores de lazo integrados. Este es el método preferido para acceder a las unidades que deben borrarse, ya que pueden borrarse muchas unidades adicionales simultáneamente. El servidor de arranque acoplado externamente debe configurarse con el adaptador de bus host adecuado, como SCSI o de canal de fibra. Para un rendimiento óptimo es importante utilizar el cable adecuado.

Una vez conectado, un administrador inicia el software de borrado de datos desde un servidor de arranque externo. El software es capaz de detectar y borrar simultáneamente más de 250 discos duros en el mismo array y puede eliminar rápidamente los datos en los discos duros ATA, SATA, SCSI, Fiber Channel y SAS. Esta versión también permite el borrado de sectores reasignados de discos duros ATA/SATA/SCSI/Fiber Channel y ofrece informes detallados de los activos de hardware con indicadores del estado del disco duro.

Borrado de datos certificado para requisitos complejos

Mientras la computación en nube aumenta y los centros de datos evolucionan para satisfacer las crecientes exigencias de almacenamiento, el software de borrado de datos aparece como una solución práctica, automatizada y auditable que permite operaciones eficientes y seguras. El software permite el borrado de hardware y configuraciones de almacenamiento en todo el centro de datos, así como un borrado seleccionado de carpetas, archivos y unidades lógicas. Para garantizar la mínima interrupción y la máxima seguridad de datos en centros de datos con entornos dinámicos, los administradores, usuarios y clientes pueden confiar en el borrado de datos certificado como una herramienta para las exigencias actuales y futuras.

Referencias

[1] IDC Digital Universe Study, sponsored by EMC, December 2012

[2] Gartner, "Forecast: Data Centers, Worldwide, 2010-2015," October 2011

[3] Emerson Network Power, "Recycling Ratios: The Next Step for Data Center Sustainability"

[4] Newsweek, "Digital Dump," July 2011

[5] Wall Street Journal, "More Predictions on the Huge Growth of Cloud Computing," April 2011

[6] Cloud Computing, "5 Cloud Computing Statistics You May Find Surprising," http://cloudcomputingtopics.com/2011/11/5-cloud-computing-statistics-you-may-find-surprising/, November 2011

[7] Federal Data Center Consolidation Initiative (FDCCI) Data Center Closings 2010-2012, http://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37

[8] Gartner, "Data Center Consolidation: Top 10 Best Practices for Project Success," Research Note, May 2011

Algunos textos de este white paper, aparecieron en la revista ITAK, Vol. 6 Articulo 8, publicado por la Asociación Internacional de Gerentes de Activos en Tecnologías de la Información.

C. Anabel Segura 7, 28108 Alcobendas, Madrid
900 112 012, www.ontrackdatarecovery.es