DESCRIPCIÓN DE ESG

# Modernización del respaldo de VM a escala y sin concesiones con Dell Technologies

**Fecha:** agosto de 2021 **Autores:** Christophe Bertrand, analista ejecutivo, y Monya Keane, analista de investigación ejecutiva

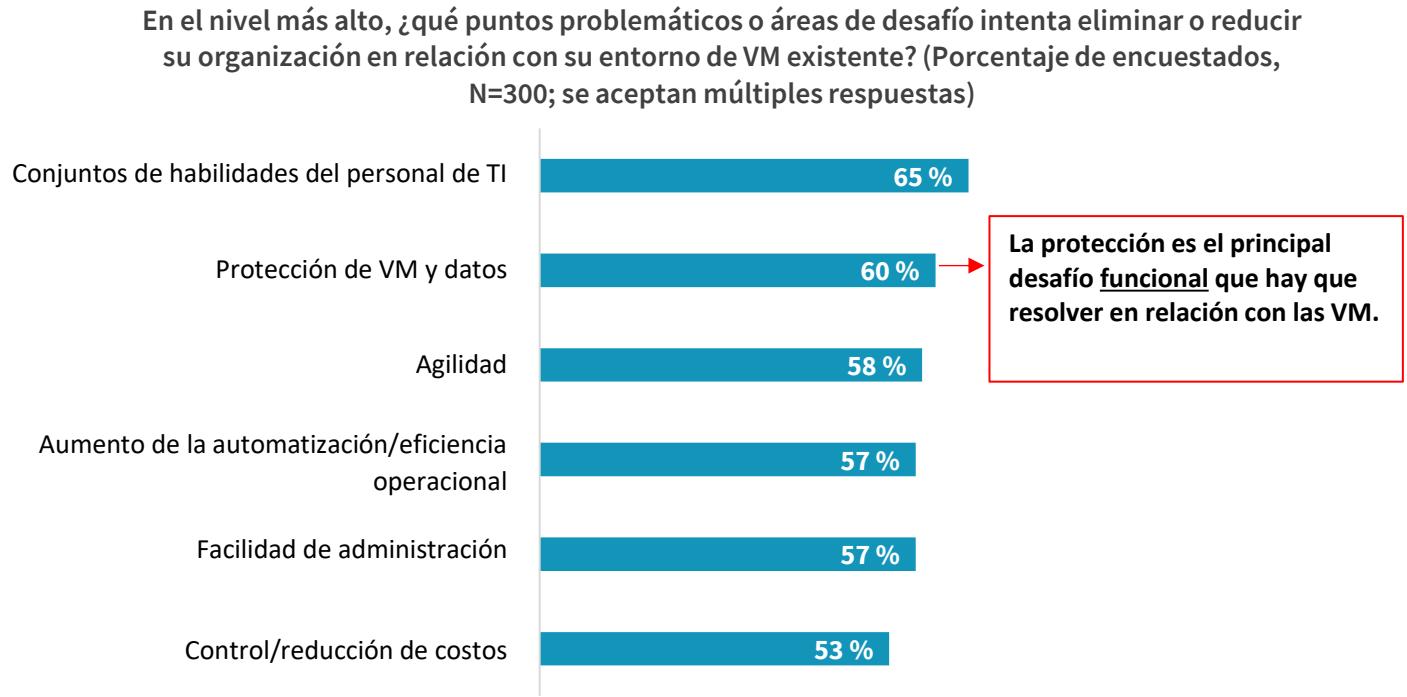
**RESUMEN:** Desde hace años, las instantáneas de VM están disponibles con finalidades de protección de datos. Pero, hasta ahora, los enfoques alternativos no eran más que "parches". No podían cubrir todos los requisitos de escalamiento con un buen rendimiento, lo que forzaba a las organizaciones a hacer concesiones. Por eso, Dell Technologies, basándose en numerosos comentarios de los clientes, desarrolló una nueva tecnología que se integra con los productos de VMware, llamada Transparent Snapshots. De este modo, simplificó la manera de proteger a escala las VM en rápido crecimiento en los entornos actuales con sobrecarga intensiva de datos y gran cantidad de transacciones.

## Panorama del mercado

ESG realizó una investigación personalizada[1] para que Dell Technologies obtuviera una comprensión más profunda de los desafíos que enfrentan los profesionales de TI para proteger sus entornos de VM en las instalaciones, tanto si dichos entornos están creciendo con rapidez como si ya tienen un gran tamaño. Las conclusiones (consulte la figura 1) muestran que la protección de datos se ha convertido en un punto problemático funcional importante en los entornos de VM, ya que a menudo, para protegerlos, se utilizan varios mecanismos de protección de datos.

[1] Fuente: Informe de investigación con información valiosa de ESG encargado por Dell Technologies, *Data Protection Trends in Virtual Environments*, febrero de 2020. Todas las referencias y los gráficos de investigación de ESG provienen de esta investigación personalizada, a menos que se indique lo contrario.

**Figura 1. Principales desafíos de protección de datos en implementaciones de VM de gran tamaño**




*Fuente: Enterprise Strategy Group*

El propio entorno de respaldo es la razón por la que muchas organizaciones incumplen sus SLA de protección de datos. El 53 % de los encuestados afirmaron que sus entornos de respaldo son, en la mayoría de los casos, la causa principal de las fallas de RTO/RPO. Claramente, las organizaciones deben abordar mejor las causas evitables que subyacen a dichos incumplimientos de los SLA.

Aunque ya hace muchos años que las metodologías de respaldo específicas de la virtualización están en el mercado, el éxito de los procesos de respaldo y recuperación sigue sin estar asegurado. Los encuestados afirmaron que, en promedio, solo el 77 % de las VM en las instalaciones pueden finalizar correctamente el proceso de respaldo y restauración (es decir, que los respaldos se completan sin errores y las VM y sus cargas de trabajo relacionadas se pueden restaurar).

Los respaldos disruptivos pueden causar problemas considerables para las aplicaciones y los procesos cruciales de toda la empresa. Hasta ahora, la mayoría de las tecnologías de respaldo de VM demostraron ser demasiado limitadas para los entornos de VM de gran escala o en rápido crecimiento. Como resultado, las organizaciones de TI se vieron obligadas a hacer concesiones, lo cual, en última instancia, tiene consecuencias negativas en la eficiencia operacional.

Dell Technologies reconoció la necesidad obvia de revisar las opciones de protección de datos existentes para las implementaciones de VM y desarrolló tecnología para eliminar esta brecha. El resultado fue una mejora en los indicadores clave de desempeño, la protección confiable de las VM y un mejor soporte para los procesos de negocios en el mundo real.

## Por qué los métodos tradicionales de respaldo de VM son insuficientes

Cuando VMware presentó las máquinas virtuales por primera vez, todos las respaldaban con un enfoque basado en agentes físicos. Luego, en 2009, VMware lanzó VADP (API de VMware para protección de datos). Este avance permitió los respaldos basados en imágenes con políticas dinámicas.

Sin embargo, desde 2009, no hubo muchas novedades con respecto a la protección de las VM. Todos siguen utilizando las mismas API para hacer respaldos basados en imágenes. Esto supone un problema, si tenemos en cuenta el hecho de que los datos de las cargas de trabajo basadas en VM crecieron sin freno.

Algunas organizaciones intentaron aprovechar la protección basada en instantáneas mediante la integración de arreglos de almacenamiento, pero aun así enfrentaron desafíos para mantener un rendimiento aceptable a escala. Surgieron problemas de costos y dificultades de administración. Otras organizaciones intentaron aprovechar tecnologías de registro/protección continua de datos (CDP) para cumplir con sus estrictos SLA. Este método redujo las ventanas de recuperación operacional. Además, claramente, la CDP puede ser un proceso costoso.

Como resultado, las organizaciones que mantienen entornos de VMware grandes o en rápido crecimiento tienen problemas para respaldar VM individuales de gran tamaño o grandes cantidades de VM. Lo más importante es que las VM de misión crítica que estas organizaciones están tratando de proteger con tecnología heredada, como VADP, están principalmente en las instalaciones. Más allá de esto, hoy en día no tiene mucho sentido utilizar la misma tecnología que existía hace más de diez años para realizar respaldos y aun así pretender cumplir con las ventanas de los SLA. Por eso, las organizaciones se enfrentan a una decisión que parece imposible en cuanto a la protección de datos, ya que deben elegir entre comprometer el rendimiento de producción o renunciar al cumplimiento de las métricas de nivel de servicio establecidas en relación con el respaldo.

Las empresas tienden a afrontar problemas con las ventanas de respaldo cuando sus entornos de VM crecen mucho o muy rápido. Esto se debe a que ahora realizan muchos deltas (es decir, respaldos de los datos modificados), lo que a menudo conlleva problemas de rendimiento en el entorno de producción. El problema del impacto en el rendimiento llegó a ser tan grave que muchas organizaciones se vieron obligadas a volver a un respaldo menos granular basado en agentes y a evitar el respaldo de VADP basado en imágenes. Pero, de esta manera, pierden sus políticas dinámicas. Esencialmente, vuelven a aplicar un enfoque que no es de 2009, sino de 2003.

Esta es una de las razones por las que es tan prometedor el hecho de que Dell Technologies haya descubierto cómo ayudar a las organizaciones a evitar un impacto en el rendimiento de sus entornos y, aun así, lograr una manera considerablemente más sencilla y mucho menos intrusiva de realizar respaldos basados en imágenes y recuperaciones de nivel granular, *todo a una escala masiva*.

## Presentamos Transparent Snapshots: ¿quién necesita esta tecnología?

La mayoría de organizaciones deben plantearse seriamente aprovechar una tecnología de instantáneas de VM más reciente, en especial aquellas del mercado del segmento intermedio, que suelen tener un personal de TI más reducido. Estas organizaciones ampliaron sus entornos de VM a un ritmo muy veloz y, en ocasiones, llegaron a duplicar la cantidad de VM cada año, por lo que se enfrentaron con problemas. Las organizaciones de muy gran tamaño con miles de implementaciones de VM en las instalaciones son también candidatas ideales y sin duda se beneficiarían de un mejor enfoque de respaldo.

## Cómo funciona

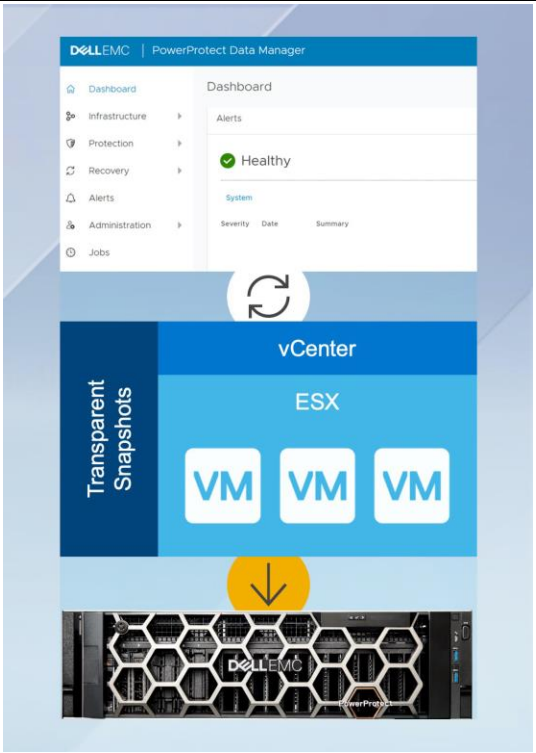
El enfoque de Dell Technologies no se centra en una API, sino más bien en un nuevo plug-in de ESX llamado Transparent Snapshots (consulte la figura 2), disponible con Dell EMC PowerProtect Data Manager. Este plug-in, certificado por VMware, realiza un monitoreo ligero de las VM y captura los deltas a medida que se producen. De esta manera, cuando PowerProtect Data Manager solicita un respaldo, recibe directamente esa lista de deltas. Básicamente, dado que Transparent Snapshots forma parte de la capa de ESX, lee de forma directa los discos de las VM para obtener los deltas y los envía mediante el plug-in a los dispositivos PowerProtect directamente.

Esta es una solución “sin concesiones”. Los beneficios de rendimiento de los dispositivos PowerProtect siguen estando disponibles, ya que Dell Technologies los incluyó en la biblioteca de DD Boost. Además, todos los beneficios de los proxies externos forman parte de Transparent Snapshots. Desduplicación en el cliente, compresión… Todo forma parte de la transferencia de datos que se produce dentro del plug-in de ESX.

El resultado es que todos los deltas se capturan con un respaldo de imágenes tradicional, pero sin que ello afecte a la latencia ni ralentice la aplicación hasta el punto de generar retrasos. Casi no tiene ningún impacto en las VM ni en la sobrecarga de ESX. Dicho de otro modo, los datos se respaldan sin interrupción comercial.

Y lo mejor de todo es que el departamento de TI no tiene que hacer nada para administrar la implementación. La sencillez es uno de los distintivos principales de esta solución. Se coloca automáticamente en los nuevos hosts ESX sin necesidad de tareas adicionales. En ESX, no es necesario realizar reinicios. Tampoco se necesita el modo de mantenimiento. A medida que se agregan VM que hay que proteger, Dell Technologies garantiza que se realice la implementación.

**Figura 2. Integración de ESX para Transparent Snapshots**




*Fuente: Dell Technologies*

Esta solución también elimina la necesidad de lidiar con proxies para transferir datos. La organización de TI no debe preocuparse de cuántos proxies implementar al colocar una cantidad de VM determinada en un host ESX.

Además, debido al nuevo monitoreo ligero, los respaldos se realizan sin afectar a las VM ni a ESX, específicamente gracias al nuevo delta continuo en la memoria que la solución aprovecha como parte del plug-in.

Transparent Snapshots es independiente del almacenamiento y es capaz de funcionar a un nivel granular de VM. Permite que el departamento de TI no tenga que comprar costoso almacenamiento flash para aprovechar las instantáneas de arreglo de almacenamiento a fin de evitar los desafíos de rendimiento que plantea la tecnología tradicional de VADP. Transparent Snapshots también puede dirigir el respaldo a VM individuales: elimina la participación de otras VM, con lo que evita que se vea afectado todo el entorno para proteger una sola máquina virtual. Además, incluye la transferencia directa de datos a dispositivos PowerProtect, lo que mejora aún más la eficiencia operacional y facilita el cumplimiento de los SLA.

## La gran verdad

Durante años, Dell Technologies innovó para integrar sus soluciones de protección de datos con los productos de VMware y ocuparse de las necesidades de los clientes de VMware. Además, esta integración es particularmente única y diferenciada. Cambia de manera fundamental la manera de llevar a cabo el respaldo de VM, ya que aporta rendimiento sin interrupciones, de manera sencilla y sin concesiones.

Con esta solución, ya no es necesario elegir entre el rendimiento y la capacidad: no hay que preocuparse sobre los efectos secundarios relacionados con el respaldo al escalar el rendimiento y la capacidad a la vez. Esto es un beneficio incluso para las empresas que aún no son muy grandes.

Los beneficios de esta solución son numerosos. Se centran en el aumento del rendimiento, sin un efecto negativo en las VM ni en los hosts ESX al realizar un respaldo completo: Dell afirma conseguir respaldos hasta 5 veces más rápidos y una latencia hasta 5 veces menor en las VM. Asimismo, el plug-in se implementa automáticamente como parte de PowerProtect Data Manager, lo que facilita el escalamiento. Transparent Snapshots es independiente del almacenamiento y maneja la orquestación, la transferencia directa de datos y otros aspectos. Se trata de simplificar los respaldos de las VM.

Desde 2009, la mayoría de las cosas evolucionaron drásticamente. Entonces, ¿por qué no lo hicieron los respaldos basados en imágenes? Por fin, estamos viendo esta evolución tan necesaria. Transparent Snapshots está cambiando la manera en la que se respaldan las VM, gracias a que aborda los problemas de interrupción (a diferencia de otras “soluciones” que en realidad no resuelven el problema, sino que solo obligan a realizar concesiones de costo y rendimiento). Es lo mejor de ambos mundos: respaldo de VM basado en imágenes a escala y sin interrupción comercial. Utilizar Transparent Snapshots es la manera óptima de proteger las VM.



**Enterprise Strategy Group** es una empresa de análisis, investigación, validación y estrategia de TI que ofrece inteligencia de mercado e información útil a la comunidad mundial de TI.

www.esg-global.com contact@esg-global.com 508 482 0188