

## APRESENTAÇÃO DO ESG

# Modernização do backup de VMs em grande escala sem dilemas – com a Dell Technologies

**Data:** agosto de 2021 **Autores:** Christophe Bertrand, Analista sênior; e Monya Keane, Analista sênior de pesquisas

**RESUMO:** os snapshots de VMs estão disponíveis para fins de proteção de dados há muitos anos. Porém, até hoje, os métodos alternativos eram "improvisados" e não atendiam a todos os requisitos de dimensionamento com desempenho, forçando as empresas a fazer concessões. É por isso que a Dell Technologies desenvolveu, com base em comentários dos consumidores, uma nova tecnologia que se integra aos produtos da VMware chamada Transparent Snapshots, para simplificar a forma com que as VMs em rápida expansão podem ser protegidas em grande escala nos ambientes atuais de cargas de trabalho muito transacionais e com uso intenso de dados.

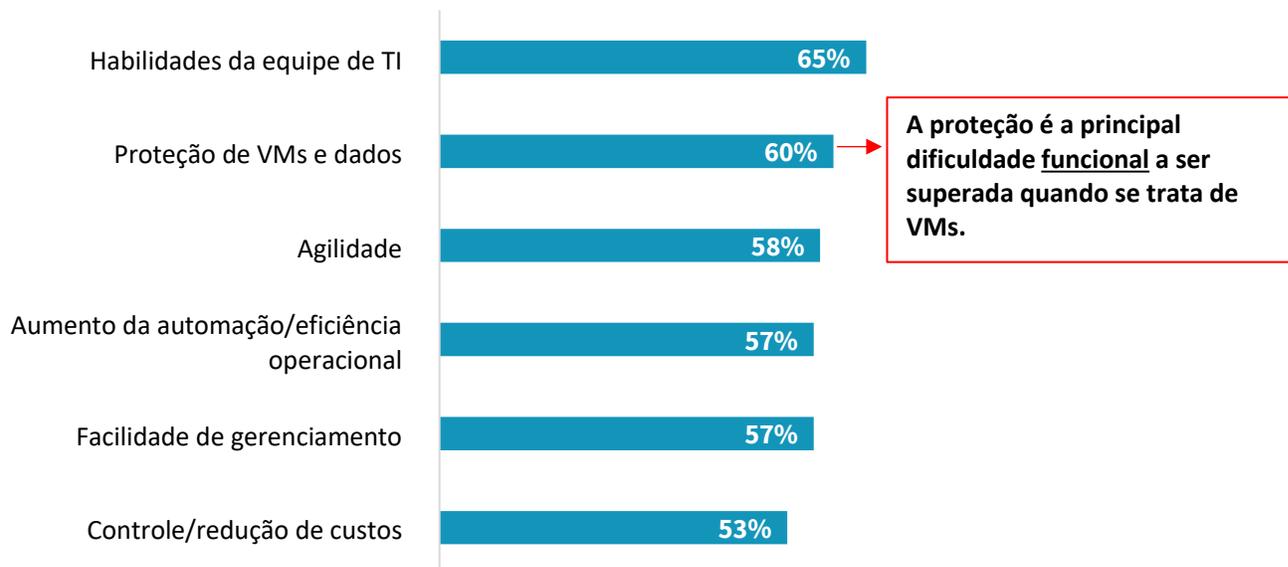
## Ambiente do mercado

O ESG conduziu uma pesquisa personalizada<sup>1</sup> para a Dell Technologies entender melhor as dificuldades enfrentadas por profissionais de TI a fim de proteger os ambientes de VM no local deles, sejam ambientes muito grandes ou que estão crescendo rapidamente. Os resultados (ver Figura 1) mostram que a proteção de dados se tornou uma das principais dificuldades funcionais relacionadas a implementações de VMs, com diversos mecanismos de proteção de dados usados com frequência para protegê-las.

<sup>1</sup> Fonte: Research Insights Paper do ESG encomendado pela Dell Technologies, *Data Protection Trends in Virtual Environments*, de fevereiro de 2020. Todas as referências e todos os gráficos do ESG nesta apresentação foram extraídos desta pesquisa personalizada, exceto se indicado de outra forma.

**Figura 1. Maiores dificuldades com a proteção de dados em implementações grandes de VMs**

No nível mais elevado, quais dificuldades ou desafios sua empresa está trabalhando para eliminar ou reduzir no ambiente atual de VMs? (Porcentagem de entrevistados, N = 300, várias respostas aceitas)



Fonte: Enterprise Strategy Group

O ambiente de backup por si só é o motivo para muitas empresas deixarem de cumprir com seus Acordos de Nível de Serviço de proteção de dados. Durante a pesquisa, 53% dos participantes relataram que os ambientes de backup são a causa mais frequente de falhas de RTO/RPO. É claro que as organizações precisam trabalhar melhor para corrigir as causas evitáveis por trás desses Acordos de Nível de Serviço descumpridos.

Embora as metodologias de backup específicas para virtualização estejam no mercado há anos, o sucesso dos processos de backup e recuperação ainda não é garantido. Os participantes afirmaram que, em média, só conseguem fazer backup e restaurar 77% das VMs locais com sucesso (isto é, backups concluídos sem erros e possibilidade de restaurar as VMs e cargas de trabalho associadas).

Backups com interrupção podem causar problemas graves para aplicativos e processos essenciais em toda a empresa. Até hoje, a maior parte das tecnologias de backup de VMs demonstrou ser limitada demais para ambientes em grande escala ou em rápida expansão. O resultado é que as organizações de TI foram forçadas a aceitar concessões, que, por sua vez, geram consequências negativas em termos de eficiência operacional.

A [Dell Technologies](#) reconheceu a necessidade óbvia de rever as opções atuais de proteção de dados para implementações de VMs e desenvolveu a tecnologia necessária para preencher esta lacuna. O resultado é uma melhoria nos indicadores-chave de desempenho, VMs protegidas de maneira confiável e processos de negócios com melhor suporte no mundo real.

## Por que os métodos tradicionais de backup de VMs não atendem às expectativas

Quando a VMware lançou as máquinas digitais, os backups eram feitos usando a metodologia baseada em um agente físico. Até que, em 2009, a VMware desenvolveu o VADP (APIs da VMware para proteção de dados). Este avanço permitiu a realização de backups baseados em imagens com políticas dinâmicas.

Desde 2009, no entanto, não houve muita inovação na área de proteção de VMs. As pessoas ainda utilizam as mesmas APIs para fazer backups baseados em imagem. Isso é lamentável, considerando o fato de que os dados em cargas de trabalho baseadas em VM têm aumentado muito.

Algumas organizações tentaram recorrer à proteção baseada em snapshots com a integração de storage arrays, mas ainda enfrentam dificuldades relacionadas à manutenção do desempenho aceitável em grande escala. Também surgem problemas de custos e dificuldades de gerenciamento. Outras empresas tentaram usar tecnologias de journaling/proteção contínua de dados (CDP) para cumprir com seus Acordos de Nível de Serviço rígidos. Essa metodologia reduziu o tempo de recuperação operacional dessas empresas. E, é claro, a CDP pode ser um processo caro.

O resultado é que as organizações que mantêm ambientes da VMware robustos ou em rápida expansão têm dificuldades para fazer o backup de grandes números de VMs e VMs grandes. As VMs essenciais que essas empresas estão tentando proteger com tecnologias preexistentes, como VADP, ficam predominantemente no local. Apesar disso, não faz sentido usar hoje as mesmas tecnologias que existem há mais de uma década para fazer backup e ainda esperar cumprir os prazos de Acordo de Nível de Serviço. É por isso que as empresas se depararam com o que parece ser um dilema impossível da proteção de dados: comprometer o desempenho da produção ou desistir de cumprir com as métricas de nível de serviço relacionadas a backups já estabelecidas.

As empresas tendem a encontrar problemas com prazo de backup quando os ambientes de VM crescem muito... ou muito depressa. Isso porque agora elas fazem muitos deltas (ou seja, backups de dados alterados). Problemas de desempenho no ambiente de produção são frequentes. O problema do impacto sobre o desempenho se agravou tanto que diversas organizações foram forçadas a voltar para backups menos granulares e baseados em agentes, evitando o backup de VADP baseado em imagem. Só que, assim, elas perdem as políticas dinâmicas. Basicamente, elas estão voltando a usar uma metodologia de 2003, não de 2009.

Esse é um dos motivos para a solução desenvolvida pela Dell Technologies ser tão promissora: ela pode ajudar as empresas a evitar impactos sobre o desempenho dos ambientes e oferecer, ainda assim, um jeito bem mais simples e menos intrusivo de fazer backups baseados em imagens e recuperações granulares, *tudo isso em grande escala*.

## Apresentamos o Transparent Snapshots: quem precisa dele?

A maioria das empresas deve cogitar os benefícios da nova tecnologia de snapshots de VMs, ainda mais as de médio porte que, em geral, têm equipes de TI menores. Essas organizações têm aumentado os ambientes de VMs delas em um ritmo bastante acelerado, algumas vezes até dobrando o número de VMs por ano, e têm enfrentado problemas. Empresas muito grandes, com milhares de implementações de VMs no local, também são naturalmente adequadas e certamente terão benefícios com uma metodologia de backup melhor.

## Como funciona

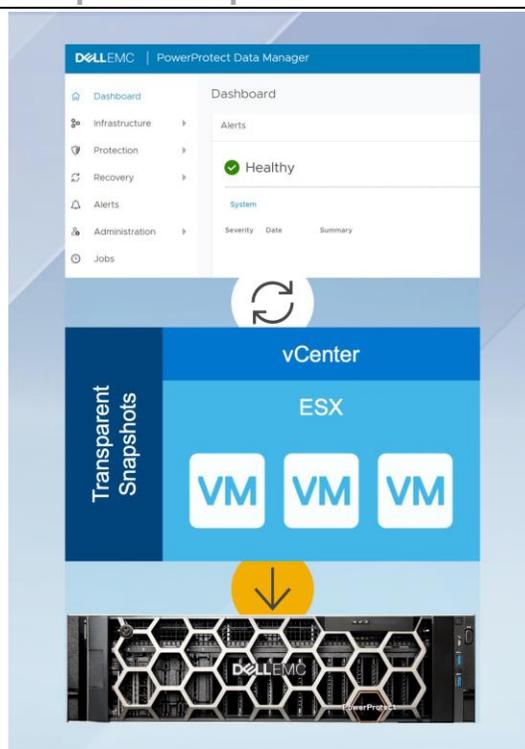
A metodologia da Dell Technologies não é centrada em uma API, mas em um novo plug-in do ESX chamado [Transparent Snapshots](#) (ver Figura 2), disponível com o Dell EMC PowerProtect Data Manager. Com certificação da VMware, ele realiza um monitoramento leve das VMs, capturando deltas à medida que eles ocorrem. Dessa forma, quando o PowerProtect Data Manager solicita um backup, ele recebe essa lista de deltas diretamente. Basicamente, como o Transparent Snapshots faz parte da camada do ESX, ele lê os discos das VMs para obter os deltas, enviando-os pelo plug-in diretamente aos equipamentos PowerProtect.

Essa é uma solução "sem concessões". Os benefícios de desempenho dos equipamentos PowerProtect continuam disponíveis, pois a Dell Technologies os integrou à biblioteca DD Boost. E todos os benefícios de proxies externos fazem parte do Transparent Snapshots. Desduplicação de dados no lado do client, compactação... tudo isso faz parte da movimentação de dados que ocorre dentro do plug-in do ESX.

O resultado é que todos os deltas são capturados da mesma forma que um backup tradicional por imagem, mas sem afetar a latência ou reduzir a velocidade do aplicativo a ponto de causar um backlog. Ele não tem quase nenhum impacto sobre as VMs e a sobrecarga do ESX. Em outras palavras, o backup de dados é realizado sem interrupção de negócios.

E o melhor de tudo é que a TI não precisa fazer nada em relação ao gerenciamento da implementação. A simplicidade é a grande marca desta solução. Ela é aplicada automaticamente em novos hosts do ESX sem nenhum trabalho extra. Não é necessário reinicializar o ESX. Também não é preciso entrar em modo de manutenção. À medida que as VMs forem adicionadas e precisarem de proteção, a Dell Technologies garantirá que a implementação ocorra.

## Figura 2. Integração do ESX ao Transparent Snapshots



Fonte: Dell Technologies

Esta solução também elimina a necessidade de lidar com proxies para a movimentação dos dados. A organização de TI não precisa se preocupar com o número de proxies que serão implementados ao colocar um determinado número de VMs em um host do ESX.

E, graças ao novo monitoramento leve, os backups ocorrem sem impactos sobre as VMs ou o ESX, especificamente em razão do novo delta contínuo na memória que a solução usa como parte do plug-in.

O Transparent Snapshots é independente de armazenamento e pode ser executado em um nível granular da VM. Com ele, a equipe de TI não precisa comprar nenhum tipo de armazenamento flash caro para aproveitar os snaps de storage arrays e contornar as dificuldades de desempenho enfrentadas com o VADP tradicional. O Transparent Snapshots também consegue selecionar VMs individuais para backup. Ele elimina o envolvimento de outras VMs, evitando, assim, impactos em todo o

ambiente para proteger apenas uma máquina virtual. Além disso, inclui transferência direta de dados para equipamentos PowerProtect, o que aumenta a eficiência operacional e facilita o cumprimento dos Acordos de Nível de Serviço.

## A grande verdade

Durante anos, a Dell Technologies inovou para integrar suas soluções de proteção de dados aos produtos da VMware com o objetivo de atender às necessidades dos clientes da VMware. Essa integração é, sobretudo, exclusiva e muito diferenciada. Ela muda muito o modo com que os backups de VMs são realizados, garantindo desempenho sem interrupção, de maneira simples e sem prejuízo.

Com esta solução, você não precisa mais decidir entre desempenho e capacidade nem se preocupar com os efeitos colaterais dos backups ao fazer dimensionamento do desempenho e a capacidade de uma só vez. Esse é um benefício até para quem ainda não tem uma grande empresa.

A solução tem inúmeros benefícios. Eles se concentram na melhoria do desempenho sem impactos negativos sobre as VMs ou os hosts do ESX ao realizar um backup completo. A Dell promete backups até 5 vezes mais rápidos e até 5 vezes menos latência nas VMs. E o plug-in é implementado automaticamente como parte do PowerProtect Data Manager, facilitando o dimensionamento. O Transparent Snapshots é independente de armazenamento e dá conta de orquestração, movimentação direta de dados e muito mais. Trata-se da simplificação dos backups de VMs.

A maioria das coisas evoluiu muito desde 2009. Por que isso não aconteceu com os backups baseados em imagem? Finalmente, estamos vendo essa evolução tão necessária. O Transparent Snapshots está mudando a forma de fazer backup de VMs ao solucionar os problemas de interrupção, diferente de outras "soluções", que não resolviam, de fato, o problema; só forçavam a escolha entre custo e desempenho. É o melhor dos dois mundos: backup de VMs baseado em imagem em grande escala sem interrupção de negócios. Usar o Transparent Snapshots é a maneira ideal de proteger VMs.

Todos os nomes de marcas comerciais pertencem às suas respectivas empresas. As informações contidas nesta publicação foram obtidas por fontes que o Enterprise Strategy Group (ESG) considera confiáveis, embora não sejam garantidas pelo ESG. Esta publicação pode conter opiniões do ESG, que estão sujeitas a alterações. Os direitos autorais desta publicação pertencem a The Enterprise Strategy Group, Inc. Qualquer reprodução ou distribuição desta publicação, no todo ou em parte, seja em formato impresso, eletrônico ou qualquer outro, a pessoas não autorizadas a recebê-la e sem o consentimento expresso do The Enterprise Strategy Group, Inc., é uma violação das leis de direitos autorais dos Estados Unidos e estará sujeita a uma ação por danos civis e, se aplicável, acusação criminal. Em caso de dúvidas, entre em contato com o Serviço de atendimento ao cliente do ESG pelo telefone +1 508-482-0188.



**Enterprise Strategy Group** é uma empresa de estratégia, validação, pesquisa e análise de TI que oferece inteligência de mercado e insights práticos à comunidade global de TI.



[www.esg-global.com](http://www.esg-global.com)



[contact@esg-global.com](mailto:contact@esg-global.com)



+1 508-482-0188