

ESG SHOWCASE

Ein moderner Ansatz für große VM-Backups ohne Kompromisse – mit Dell Technologies

Datum: August 2021 **Autoren:** Christophe Bertrand, Senior Analyst, und Monya Keane, Senior Research Analyst

ZUSAMMENFASSUNG: VM-Snapshots für die Data Protection gibt es bereits seit vielen Jahren. Alternative Ansätze erweckten bislang aber eher den Eindruck eines Palliativs. Sie waren den Anforderungen in puncto Skalierung bei gleichzeitiger Wahrung der Leistung nicht gewachsen, sodass Unternehmen Abstriche machen mussten. Aus diesem Grund hat Dell Technologies auf Basis von umfangreichem Kundenfeedback Transparent Snapshots entwickelt, eine neue, mit VMware-Produkten integrierte Technologie. Damit steht eine einfachere Möglichkeit zum Sichern schnell wachsender VMs in den heutigen Umgebungen mit hoher Transaktionsdichte und datenintensiven Workloads zur Verfügung.

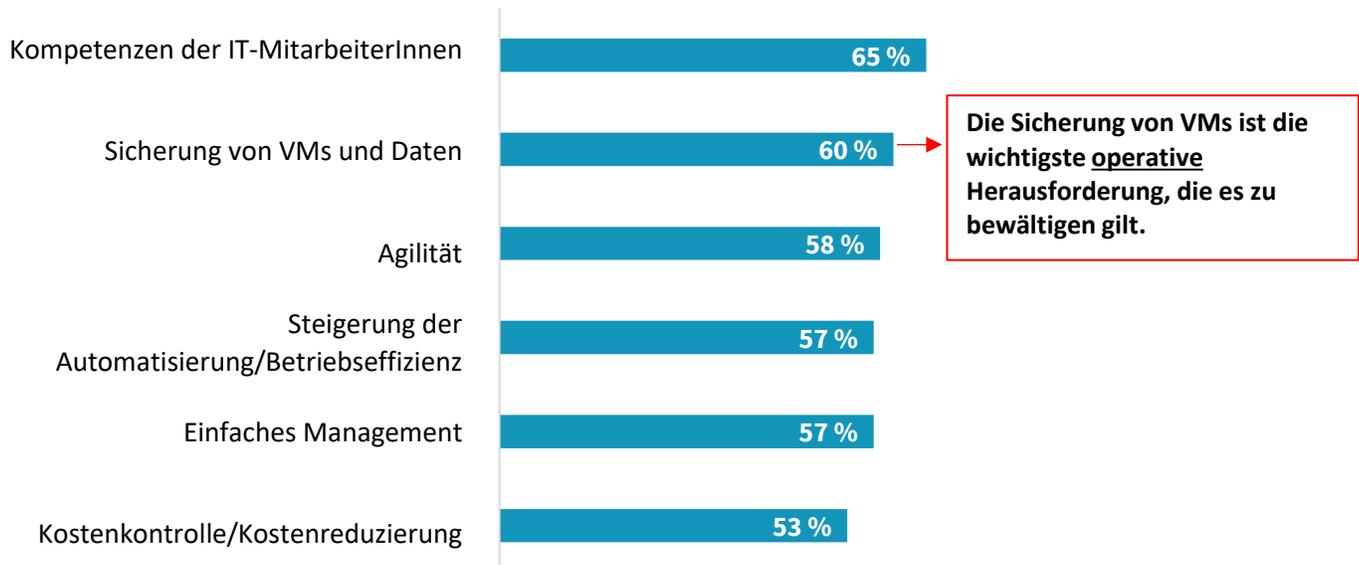
Marktlandschaft

Durch individuelle Untersuchungen¹ im Auftrag von Dell Technologies machte sich ESG ein besseres Bild von den Herausforderungen, mit denen IT-ExpertInnen beim Sichern ihrer On-Premise-VM-Umgebungen konfrontiert sind – ganz gleich, ob diese Umgebungen schnell wachsen oder bereits sehr groß sind. Die Ergebnisse (siehe Abbildung 1) zeigen, dass die Data Protection zu einem wesentlichen operativen Problem bei VM-Bereitstellungen geworden ist. Tatsächlich kommen zwecks Sicherung der VMs oft mehrere Data-Protection-Mechanismen zum Einsatz.

¹ Quelle: ESG Research Insights Paper im Auftrag von Dell Technologies, *Data Protection Trends in Virtual Environments*, Februar 2020. Sofern nicht anders angegeben, stammen alle ESG-Referenzen und -Diagramme im vorliegenden Showcase aus diesen individuellen Untersuchungen. Dieser ESG Showcase wurde von Dell Technologies in Auftrag gegeben und wird unter Lizenz von ESG zur Verfügung gestellt.

Abbildung 1: Die wesentlichen Data-Protection-Herausforderungen bei großen VM-Bereitstellungen

Welche Probleme oder Problembereiche im Zusammenhang mit der vorhandenen VM-Umgebung möchte Ihr Unternehmen vorrangig beheben oder verbessern? (% der Befragten, N = 300, mehrere Antworten möglich)



Quelle: Enterprise Strategy Group

Die Backupumgebung selbst ist der Grund, aus dem viele Unternehmen ihre Data-Protection-SLAs nicht einhalten können. 53 % der Umfrageteilnehmer gaben an, dass ihre Backupumgebungen in den meisten Fällen die Ursache für RTO/RPO-Versäumnisse sind. Unternehmen müssen definitiv effektiver vorgehen, um die vermeidbaren Ursachen für diese nicht erfüllten SLAs zu beseitigen.

Virtualisierungsspezifische Backupmethoden gibt es zwar bereits seit vielen Jahren, sie garantieren aber nicht, dass Backup- und Recovery-Vorgänge auch erfolgreich sind. Die Umfrageteilnehmer berichteten, dass sie im Durchschnitt nur 77 % ihrer On-Premise-VMs erfolgreich sichern und wiederherstellen können (das heißt, dass die Backups ohne Fehler abgeschlossen werden und die VMs und zugehörigen Workloads wiederhergestellt werden können).

Disruptive Backups können beträchtliche Probleme für kritische Anwendungen und Prozesse im gesamten Unternehmen verursachen. Bislang haben sich die meisten VM-Backuptechnologien als zu beschränkt für große oder schnell wachsende VM-Umgebungen erwiesen. Das hat dazu geführt, dass IT-Abteilungen zu Abstrichen gezwungen waren, was schlussendlich negative Konsequenzen in Sachen Betriebseffizienz nach sich zieht.

[Dell Technologies](#) erkannte die offensichtliche Notwendigkeit, bestehende Data-Protection-Optionen für VM-Bereitstellungen zu überarbeiten, und entwickelte Technologie zum Schließen der vorhandenen Lücke. Das Ergebnis sind verbesserte Leistungskennzahlen, zuverlässig gesicherte VMs und eine bessere Unterstützung von Geschäftsprozessen in der Praxis.

Warum klassische VM-Backupmethoden unzureichend sind

Als VMware die ersten virtuellen Maschinen herausbrachte, setzte für die Sicherung jeder auf einen physischen, Agent-basierten Backupansatz. 2009 führte VMware dann VADP (VMware APIs for Data Protection) ein. Diese Neuerung ermöglichte Image-basierte Backups mit dynamischen Richtlinien.

Seit 2009 hat es aber keine wirklichen Innovationen mit Blick auf die VM-Sicherung mehr gegeben. Im Allgemeinen verwendet jeder immer noch die gleichen APIs, um Image-basierte Backups auszuführen. Das ist bedauerlich, vor allem in Anbetracht der Tatsache, dass die Daten in VM-basierten Workloads unglaublich zugenommen haben.

Einige Unternehmen haben versucht, Array-basierte Snapshots für die Sicherung zu nutzen, hatten dabei aber nach wie vor Schwierigkeiten, beim Skalieren eine akzeptable Leistung sicherzustellen. Kosten- und Managementprobleme kamen auf. Andere Unternehmen versuchten, mit Technologien für Journaling/Continuous Data Protection (CDP) ihre strikten SLAs zu erfüllen. Durch diesen Ansatz wurden ihre Zeitfenster für die betriebliche Recovery geschmälert. Zudem kann CDP ein kostspieliger Prozess sein.

Im Endeffekt haben Unternehmen mit großen oder schnell wachsenden VMware-Umgebungen Probleme, zahlreiche VMs oder große Einzel-VMs zu sichern. Bemerkenswert ist, dass die erfolgskritischen VMs, die diese Unternehmen mit Legacy-Technologie wie VADP zu sichern versuchen, sich überwiegend On-Premise befinden. Dessen ungeachtet macht es heute wenig Sinn, die gleiche Technologie wie vor zehn Jahren für Backups zu nutzen und trotzdem zu hoffen, dass SLA-Zeitfenster eingehalten werden. Genau das ist der Grund, aus dem Unternehmen mit einem scheinbar unmöglichen Data-Protection-Kompromiss konfrontiert waren: Leistungseinbußen in der Produktionsumgebung oder Nichteinhalten der Servicelevel-Kennzahlen bei Backups.

Bei wirklich großen oder schnell wachsenden VM-Umgebungen erleben Unternehmen meistens Probleme aufgrund von Sicherungszeitfenstern. Das ist darauf zurückzuführen, dass eine Vielzahl von Deltas (Sicherung geänderter Daten) bewältigt werden muss. Die Folge sind oft Leistungsprobleme in der Produktionsumgebung. Die Leistungsbeeinträchtigungen sind so gravierend geworden, dass viele Unternehmen von den Image-basierten VADP-Backups auf wieder weniger granulare, Agent-basierte Backups umsteigen mussten. Damit können sie aber auch ihre dynamischen Richtlinien nicht mehr nutzen. Im Prinzip arbeiten sie also nicht mehr mit einem Ansatz aus 2009, sondern 2003.

Unter anderem aus diesem Grund ist es eine so verheißungsvolle Entwicklung, dass Dell Technologies eine Möglichkeit gefunden hat, durch die Unternehmen Leistungsbeeinträchtigungen in ihren Umgebungen vermeiden und dennoch auf bedeutend einfachere und deutlich weniger disruptive Weise Image-basierte Backups sowie granulare Recoveries ausführen können – *auch bei massiven Skalierungen*.

Die neue Transparent Snapshots-Technologie: Wer benötigt sie?

Die meisten Unternehmen sollten es wirklich in Betracht ziehen, neuere VM-Snapshot-Technologie zu nutzen. Das gilt insbesondere für mittelständische Unternehmen, die in der Regel weniger IT-MitarbeiterInnen haben. Diese Unternehmen haben ihre VM-Umgebungen unglaublich schnell ausgebaut – manchmal haben sie die Anzahl der VMs sogar jedes Jahr verdoppelt – und stehen vor Problemen. Sehr große Unternehmen mit Tausenden von On-Premise-VM-Bereitstellungen sind auch gute Kandidaten, die mit Sicherheit von einem besseren Backupansatz profitieren würden.

Funktionsweise

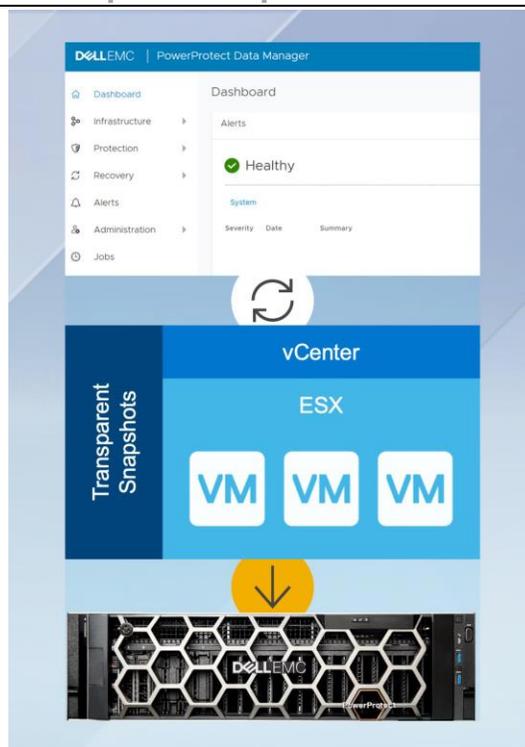
Beim Ansatz von Dell Technologies steht nicht eine API im Mittelpunkt, sondern ein neues ESX-Plug-in namens [Transparent Snapshots](#) (siehe Abbildung 2), das mit Dell EMC PowerProtect Data Manager verfügbar ist. Die von VMware zertifizierte Technologie basiert auf einem unkomplizierten Monitoring der VMs, wobei Deltas direkt bei ihrem Auftreten erfasst werden. Auf diese Weise erhält PowerProtect Data Manager beim Anfordern eines Backups direkt die Liste der Deltas. Da die Transparent Snapshots-Technologie zum ESX-Layer gehört, liest sie im Grunde direkt die Laufwerke der VMs aus, um diese Deltas zu ermitteln, und sendet sie dann über das Plug-in direkt an PowerProtect Appliances.

Das ist eine Lösung „ohne Kompromisse“. Sie profitieren weiterhin von den Leistungsvorteilen der PowerProtect Appliances, da Dell Technologies sie in die DD Boost-Bibliothek eingebettet hat. Und Transparent Snapshots bietet auch alle Vorteile externer Proxys. Die clientseitige Deduplizierung, Komprimierung usw. sind alle Teil der Datenverschiebung im ESX-Plug-in.

Deltas werden also wie bei einem klassischen Image-Backup erfasst, aber ohne dass sich Latenzen ausweiten oder Anwendungen so sehr verlangsamen, dass dann ein Rückstand entsteht. Es gibt praktisch keinerlei Auswirkungen auf die VMs oder den ESX-Overhead. Anders ausgedrückt: Daten werden ohne Betriebsunterbrechungen gesichert.

Und das Beste ist, dass IT-Verwaltungs- und -Bereitstellungsaufgaben komplett entfallen. Einfachheit ist eines der wichtigsten Merkmale dieser Lösung. Sie wird automatisch auf neuen ESX-Hosts platziert, ohne dass zusätzliche Arbeit anfällt. Unter ESX ist kein Neustart erforderlich. Auch kein Wartungsmodus. Beim Hinzufügen von VMs, die gesichert werden müssen, sorgt Dell Technologies dafür, dass die Bereitstellung stattfindet.

Abbildung 2: ESX-Integration für Transparent Snapshots



Quelle: Dell Technologies

Durch diese Lösung entfällt auch die Notwendigkeit, sich um Proxys für die Datenverschiebung zu kümmern. Die IT-Abteilung muss sich keine Gedanken darüber machen, wie viele Proxys bereitgestellt werden müssen, wenn eine bestimmte Anzahl an VMs auf einem ESX-Host platziert wird.

Und mit dem neuen, unkomplizierten Monitoring werden Backups ohne Auswirkungen auf VMs oder ESX aufgeführt. Ermöglicht wird dies insbesondere durch die neue, kontinuierliche In-Memory-Delta-Erfassung, die die Lösung als Teil des Plug-ins nutzt.

Transparent Snapshots ist Storage-unabhängig und kann auf granularer VM-Ebene agieren. Die IT muss keinen teuren Flash-Storage erwerben, um mit Storage-Array-Snapshots die Leistungsprobleme umgehen zu können, die bei klassischer VADP-Technologie auftreten. Transparent Snapshots kann auch für einzelne VM-Backups genutzt werden. Dabei werden alle anderen VMs übergangen, so dass das Sichern der einzigen VM keinerlei Auswirkungen auf die Gesamtumgebung hat.

Außerdem gibt es eine Funktion zur direkten Datenverschiebung auf PowerProtect Appliances, wodurch die Betriebseffizienz weiter verbessert wird und SLAs einfacher eingehalten werden können.

Das Gesamtbild

Dell Technologies hat jahrelang Innovationen geschaffen, um seine Data-Protection-Lösungen mit VMware-Produkten zu integrieren und so die Anforderungen von VMware-Kunden zu erfüllen. Diese Integration ist etwas ganz Besonderes, mit der wir uns stark von anderen abheben. Durch sie wird die Art und Weise, wie VM-Backups ausgeführt werden, grundlegend verändert. Kunden genießen Leistung ohne Unterbrechungen, einfach und ohne Kompromisse.

Mit dieser Lösung müssen Sie sich nicht mehr zwischen Leistung oder Kapazität entscheiden, denn Sie können beides gleichzeitig skalieren – ganz ohne sicherungsbedingte Einbußen. Das ist nicht nur für Großunternehmen ein Plus.

Diese Lösung punktet mit zahlreichen Vorteilen. Im Mittelpunkt steht dabei eine höhere Leistung, ohne negative Auswirkungen auf VMs oder ESX-Hosts bei einem kompletten Backup. Dell zufolge werden Backups sogar bis zu 5-mal schneller ausgeführt und die VM-Latenz fällt 5-mal niedriger aus. Zudem wird das Plug-in automatisch als Teil von PowerProtect Data Manager bereitgestellt, wodurch eine einfache Skalierung sichergestellt ist. Transparent Snapshots ist Storage-unabhängig und übernimmt die Orchestrierung, direkte Datenverschiebung und mehr. Hier geht es um die Vereinfachung von VM-Backups.

Seit 2009 haben sich die meisten Dinge deutlich weiterentwickelt, nicht jedoch Image-basierte Backups. Doch das ändert sich jetzt endlich. Denn Transparent Snapshots bietet einen neuen Ansatz für VM-Backups ohne Unterbrechungen, der das Problem wirklich löst, anstatt wie andere „Lösungen“ einfach nur Abstriche bei Kosten und Leistung zu forcieren. Sie erhalten damit das Beste aus zwei Welten: Image-basierte, skalierbare VM-Backups ohne Betriebsunterbrechungen. Transparent Snapshots ist die ideale Option zum Sichern Ihrer VMs.

Alle Marken sind Eigentum der jeweiligen Unternehmen. Die Informationen in dieser Veröffentlichung stammen aus Quellen, die The Enterprise Strategy Group (ESG) als zuverlässig ansieht. Dennoch übernimmt ESG für diese Informationen keine Haftung. Dieses Dokument kann Meinungen von ESG enthalten, die sich ändern können. Das Urheberrecht für diese Publikation liegt bei The Enterprise Strategy Group, Inc. Die komplette oder teilweise Vervielfältigung und/oder Verbreitung dieser Publikation in gedruckter, elektronischer oder sonstiger Form für bzw. an nicht berechnigte Personen ohne ausdrückliche Zustimmung von The Enterprise Strategy Group, Inc. stellt einen Verstoß gegen die Urheberrechtsgesetze der USA dar und wird mit zivilrechtlichen Klagen geahndet, gegebenenfalls auch strafrechtlich verfolgt. Bei Fragen wenden Sie sich bitte an die ESG Kundenbetreuung unter 508.482.0188.



Enterprise Strategy Group ist ein IT-Analyse-, Forschungs-, Prüfungs- und Strategieunternehmen, das Marktforschung betreibt und der globalen IT-Community wertvolle Einblicke liefert.