

# Die Virtualisierungsreise geht weiter

Brought to you compliments of

**ARC**serve®  
More than Backup

# Inhaltsverzeichnis

<b>DIE VIRTUALISIERUNGSREISE GEHT WEITER .....</b>	<b>2</b>
<b>POTENZIAL DER VIRTUALISIERUNG VOLL AUSSCHÖPFEN .....</b>	<b>2</b>
<b>DATENSCHUTZ IN VIRTUELLEN UMGEBUNGEN .....</b>	<b>2</b>
<b>DISASTER-RECOVERY IN VIRTUELLEN UMGEBUNGEN .....</b>	<b>3</b>
<b>ERWEITERUNG DER VIRTUELLEN UMGEBUNGEN .....</b>	<b>4</b>
<b>FAZIT .....</b>	<b>5</b>



Copyright ©2010 CA TECHNOLOGIES. Alle Rechte vorbehalten. Alle erwähnten Warenzeichen, Marken, Dienstleistungsmarken und Logos sind Eigentum der jeweiligen Unternehmen. Dieses Dokument dient nur zur Information. CA TECHNOLOGIES übernimmt für die Genauigkeit oder Vollständigkeit der Informationen keine Haftung. Im durch das anwendbare Recht gestatteten Umfang stellt CA TECHNOLOGIES dieses Dokument wie besehen und ohne Garantie zur Verfügung. Dies umfasst ohne Einschränkungen jedwede konkludente Garantie der Handelsüblichkeit, Eignung für einen bestimmten Zweck oder Nichtverletzung von Rechten. In keinem Fall ist CA TECHNOLOGIES für direkte oder indirekte Verluste oder Schäden haftbar, die durch die Verwendung dieses Dokuments entstehen, insbesondere für entgangene Gewinne, Geschäftsunterbrechungen, Verlust von Vertrauen oder Daten, auch wenn CA TECHNOLOGIES im Vorfeld ausdrücklich über die Möglichkeit solcher Schäden in Kenntnis gesetzt wurde.

---

## DIE VIRTUALISIERUNGSREISE GEHT WEITER

Die Virtualisierung ermöglicht es Unternehmen aller Größenordnungen, geschäftliche Flexibilität und Kosteneffektivität zu steigern. Darüber hinaus bietet die Virtualisierung eine Reihe von Möglichkeiten, die IT-Abteilungen von einem reinen Kostenfaktor weg hin zu einem Instrument zur Generierung von höheren Unternehmensgewinnen umzuwandeln. Für viele stellt die Entscheidung zur Umstellung auf eine virtualisierte Umgebung jedoch nur den Anfang dar. Unternehmen stellen bald fest, dass die neue virtuelle Serverumgebung eine Palette an Möglichkeiten für Einsparungen und Produktivitätssteigerungen eröffnet, aber auch eine Reihe bisher nicht vorhandener betrieblicher Herausforderungen mit sich bringt.

Manche Unternehmen scheuen die Komplexität, die das weitere Vordringen in die Virtualisierungslandschaft bedeutet. Aber die Reise kann sich lohnen. In diesem White Paper möchten wir Ihnen eine Reihe von Ideen vorstellen, wie sich Ihre anfänglichen Investitionen in die Virtualisierung auszahlen können, wenn Sie Ihren Weg der Virtualisierung weiter beschreiten.

---

## POTENZIAL DER VIRTUALISIERUNG VOLL AUSSCHÖPFEN

Im Allgemeinen wird unter Servervirtualisierung der Prozess bezeichnet, bei dem Geschäftsanwendungen von einer großen Zahl physischer Server auf eine große Zahl virtueller Server verschoben werden, die aber auf eine relativ kleine Anzahl physischer Rechner verteilt sind. In vielen Rechenzentren wurde dieser Schritt durch den starken Serverzuwachs motiviert, der sich mit der Einführung neuer Anwendungen ergab. Um das Risiko eines Ressourcenmangels zu minimieren, wurden in physischen Umgebungen eigene Server für jede Anwendung eingesetzt, sodass diese voneinander isoliert ausgeführt wurden und sich damit die Wahrscheinlichkeit unvorhergesehener Ausfälle reduzierte. Die Servervirtualisierung verringert den Hardwarebedarf, da Anwendungen in der virtuellen Maschine weiterhin voneinander isoliert werden können, physische Ressourcen dabei jedoch gemeinsam genutzt werden und die Nutzung dieser Ressourcen so maximiert werden kann.

Die Virtualisierung wurde getrieben durch die Notwendigkeit einer vereinfachten Infrastruktur, der Kostensenkung und dem Wunsch nach mehr Flexibilität. Diese Ziele wurden für viele Unternehmen erreicht, und IT-Abteilungen suchen mittlerweile nach weiteren Möglichkeiten des Einsatzes der Virtualisierungsplattform, um den Nutzen noch weiter zu steigern. Die Disaster-Recovery ist einer der Bereiche, der die Flexibilität von virtuellen Umgebungen nutzen und hochverfügbare Umgebungen für unternehmenskritische Anwendungen bereitstellen kann. Dabei ist eine deutlich höhere Kosteneffektivität als bei ausschließlich physischen Rechenzentren möglich.

Manche Unternehmen stehen allerdings noch am Anfang ihrer Virtualisierungsreise und stellen gerade erst fest, dass für die volle Ausschöpfung der Möglichkeiten, die die Servervirtualisierung bietet, Geschäftspraktiken und Erwartungen des Managements angepasst werden müssen. Die ausufernde Zahl virtueller Server ist ein echtes Problem und potenziell gravierender als in physischen Rechenzentren. Neue Plattformen für Prüfung, Entwicklung und sogar Produktion können problemlos erstellt werden, da sich virtuelle Server schnell und leicht bereitstellen lassen. IT-Manager in virtuellen Rechenzentren müssen eine sich fortlaufend in Veränderung begriffene Landschaft verwalten. Einer der Bereiche, der in virtuellen Rechenzentren eine ganze Gruppe neuer Herausforderungen nach sich zieht, ist der Datenschutz. Bestehende Richtlinien müssen überarbeitet und angepasst werden, um die in vielen Fällen kombinierte Umgebung aus virtuellen und physischen Servern zu schützen.

---

## DATENSCHUTZ IN VIRTUELLEN UMGEBUNGEN

Unternehmen entwickeln und implementieren schon lange Datenschutzrichtlinien für ihre Rechenzentren. Als Anwendungen unternehmenskritisch wurden und Datenmengen stetig wuchsen, mussten diese Richtlinien immer wieder angepasst werden, aber die Herausforderungen veränderten sich im Wesentlichen nicht. Der Datenschutz war auf die Erstellung von ausreichenden Backups ausgerichtet, um den Datenverlust bei Ausfällen zu minimieren, ohne Performance und Verfügbarkeit von Anwendungen zu beeinträchtigen.

Die Datenschutzrichtlinien entwickelten sich von der Sicherung auf Band zur Sicherung auf Festplatte, von der Erfassung der Livedaten hin zur Erstellung von Snapshots als Quelle für die Backupdaten, von der externen Aufbewahrung einer Kopie hin zur Bereithaltung mehrerer Kopien für lokale und Remote-Wiederherstellung. Warum also verändert sich der Prozess des Datenschutzes, wenn Unternehmen auf virtuelle Umgebungen umstellen?

Datenschutz in virtuellen Rechenzentren wird mit demselben Ziel wie für physische Umgebungen entworfen: Backups sollen bei minimiertem Datenverlust und schneller Wiederherstellung ohne Auswirkungen auf Performance und Verfügbarkeit der Anwendung erstellt werden. Richtlinien müssen so entwickelt werden, dass bestimmte neue Herausforderungen gemeistert werden, während diese Vorgaben weiterhin erfüllt werden.

Die Leichtigkeit bei der Bereitstellung virtueller Maschinen bedeutet, dass fortlaufend neue Server für Prüfung, Entwicklung und Produktion hinzukommen. Diese Server müssen in den Backup-Plan aufgenommen und die für ihren Schutz erforderlichen zusätzlichen Ressourcen bereitgestellt werden. Je besser die Richtlinie neue Rechner automatisch erfasst, desto geringer ist die Gefahr, dass diese Rechner bei Backups vergessen werden. Wenn mit der gewählten Backup-Lösung keine automatische Erkennung möglich ist, müssen manuelle Verfahren für die Aktualisierung der Datenschutzrichtlinien definiert werden.

Außerdem ist es möglich, dass einmal erstellte virtuelle Server verschoben werden. Beispielsweise ist es möglich, dass ein Backup-Durchlauf auf einem bestimmten physischen Server ausgeführt wird, beim nächsten Durchlauf dagegen auf einem anderen. Der Backupvorgang sollte in der Lage sein, diese Verschiebung zu verfolgen und eine genaue Historie der virtuellen Maschine unabhängig von deren Standorten zu verwalten.

Auch der genaue Backup-Inhalt ist ein entscheidender Faktor. Liefert ein Abbild des gesamten virtuellen Servers die erforderlichen Wiederherstellungsfunktionen, oder muss ein differenzierter oder anwendungsspezifischer Backup erstellt werden? Diese Entscheidung bedingt die Art der Backup-Lösung: Wird sie auf Hypervisor-Ebene ausgeführt, um ein Abbild der gesamten virtuellen Maschine zu erfassen, oder läuft die Lösung unter direkter Übertragung der Anwendungen in der virtuellen Maschine? Die Konfiguration sollte aufgrund der Zielsetzungen für Wiederherstellungspunkte und Wiederherstellungszeiten eines Unternehmens definiert werden. Möglicherweise ist auch eine Kombination verschiedener Ansätze erforderlich, um das Recovery-SLA zu erfüllen.

Beim Sichern einer großen Anzahl virtueller Maschinen entsteht eine große Menge an duplizierten Daten. Wenn auf virtuellen Maschinen zehn Windows-Server ausgeführt werden, müssen zunächst zehn Kopien des Betriebssystems gesichert werden, bevor der Datenbackup erstellt wird. Dieser Grad an Doppelung zieht Kosten für die Bereitstellung einer Infrastruktur nach sich, um ausreichend Kapazitäten zum Speichern der einzelnen Kopien für die einzelnen Rechner zu bieten. Die Einbeziehung einer Deduplikationstechnologie in die Datenschutzlösung bildet daher einen wichtigen Aspekt, da sich so bedeutende Kosten sowie Betriebszeit einsparen lassen.

Schließlich muss bei den eingesetzten Backuplösungen berücksichtigt werden, dass eine vollständige Virtualisierung unwahrscheinlich ist. Viele Quellen nennen für die meisten Unternehmen einen Virtualisierungsgrad von zur Zeit weniger als 50 % der Server. Datenschutzlösungen mit nur einer Oberfläche und einem einzigen Satz an Richtlinien sowohl für physische als auch virtuelle Umgebungen bieten daher eine kosteneffektivere Lösung mit einem geringeren Risiko für das Unternehmen.

Unternehmen wie CA Technologies bieten umfassenden Datenschutz, insbesondere für Datenbackups für virtuelle Umgebungen. CA ARCserve Backup optimiert den Datenschutz dank der Migrationsmöglichkeit in Höchstgeschwindigkeit von Windows-, Linux- und UNIX-Servern. Die Lösung bietet Backup auf Festplatte, Band und VTL sowie Deduplikationspläne mit D2D2T (Festplatte-auf-Festplatte-auf-Band). Über nur eine Benutzeroberfläche kann auf Funktionen für die automatische Erkennung virtueller Server sowie für Verwaltung und Berichte zur Verfolgung und Dokumentation der virtuellen und physischen Umgebungen zugegriffen werden. CA ARCserve ist für eine breite Palette an Plattformen und Anwendungen zertifiziert und bietet Kompatibilität und Unterstützung für heterogene Umgebungen wie VMware, XenServer und Microsoft Hyper-V.

---

## DISASTER-RECOVERY IN VIRTUELLEN UMGEBUNGEN

Unternehmen ohne kritische Systeme sind selten. Der Ausfall eines solchen unternehmenskritischen Systems wirkt sich stark auf Umsatz, Produktivität und Kundentreue aus, sodass viele Unternehmen in großem Umfang in Hochverfügbarkeitslösungen investieren. Früher führte dies dazu, dass nicht nur Cluster aus Servern und replizierten Festplatten erforderlich waren, sondern außerdem dezentrale Standorte mit redundanten Standby-Servern benötigt wurden, die mit ungenutzten Kapazitäten auf einen Ausfall warteten.

Damit sind hohe Kosten verbunden, da bei vielen Hochverfügbarkeitslösungen äquivalente Hardwarekonfigurationen für Live- und Standbystandorte verwendet werden müssen. Der Ressourcenbedarf für physische Standby-Server ist vergleichsweise hoch, sodass diese das Betriebsbudget belasten.

In Kombination mit den Weiterentwicklungen bei der Netzwerk-Bandbreite, Softwarereplikation und Bare-Metal-Recovery können Unternehmen mit der Servervirtualisierung hochverfügbare Disaster-Recovery-Umgebungen mit einem sehr viel höheren Grad an Flexibilität und Kosteneffektivität bereitstellen.

Dank der Geschwindigkeit bei der Erstellung und Bereitstellung neuer Server lassen sich für Virtualisierungsplattformen anspruchsvolle Disaster-Recovery-Konfigurationen entwickeln, bei denen auf einen Großteil der komplexen Infrastruktur verzichtet werden kann, die für physische Umgebungen erforderlich ist.

Das Problem der Serverausfallzeit lässt sich über Hochverfügbarkeitslösungen mit Echtzeitreplikation lösen. Echtzeitreplikation erlaubt die Datenübertragung an eine neue Plattform bei kontinuierlicher Verfügbarkeit von Servern und Anwendungen für die Benutzer. Ein Failover auf den Standby-Server ist so bei nur minimaler Unterbrechung möglich.

Die Kombination der Replikation mit einer Funktion für kontinuierlichen Datenschutz bildet ein kosteneffektives Disaster-Recovery-System, das nicht nur „physische“ Ausfälle abdeckt, sondern auch Datenrewind zum Schutz vor Beschädigung in der virtuellen Welt möglich macht.

---

## ERWEITERUNG DER VIRTUELLEN UMGEBUNGEN

Der Markt für die Servervirtualisierung entwickelt sich derzeit schnell, und die Dominanz nur eines Anbieters ist durch die Präsenz neuer Anbieter in relativ kurzer Zeit ins Wanken geraten. Für Unternehmen, die erfolgreich mit der Migration von einer physischen auf eine virtuelle Umgebung begonnen haben, zieht dies häufig die Neubewertung der Hypervisor-Plattform und möglicherweise die Umstellung auf eine heterogene virtuelle Umgebung nach sich.

In einem solchen Fall entstehen neue Herausforderungen für Migration und Datenschutz. Was oft als einmalige P2V-Migration galt, hat sich zu einer potenziell mehrstufigen V2V-Serververschiebung gewandelt. Damit wird die Auswahl der passenden Tools für Datenschutz, Disaster-Recovery und Migration noch wichtiger. Heute besteht ein Bedarf an einer integrierten Übersicht für physische und heterogene virtuelle Umgebungen sowie an der Möglichkeit, Daten zwischen Plattformen verschieben und in sehr unterschiedlichen Architekturen wiederherstellen zu können.

Administratoren und Mitarbeiter, die mit der Umstellung von physischen auf virtuelle Server betraut sind, müssen außerdem berücksichtigen, dass im Zuge des Unternehmenswachstums in vielen Fällen Migrationen von virtuellen zu physischen Umgebungen erforderlich sind. Beispielsweise ist es möglich, dass eine gerade virtualisierte Anwendung wie eine SQL-Datenbank aufgrund des Größenzuwachses der Datenbank oder des Bedarfs an einer größeren Zahl an CPU-Zyklen wieder zurück in eine physische Umgebung verschoben werden muss.

Für die Migration stehen zwei Verfahren zur Verfügung: „kalt“ und „heiß“. Bei einer „kalten“ Migration befindet sich die virtuelle Maschine im Standbymodus oder ist ausgeschaltet. Für diese Art von Funktion steht CA ARCserve D2D zur Verfügung. Dank der Bare-Metal-Recovery-Funktion der Lösung können Migrationen von kompletten Servern, Anwendungen und Daten von einer physischen in eine virtuelle Umgebung, zwischen virtuellen Umgebungen sowie von virtuellen zu physischen Umgebungen realisiert werden.

Die IT kann so inkrementelle Snapshots von Daten auf einem physischen Server erstellen und die Daten in kürzester Zeit auf einem virtuellen Server wiederherstellen. Damit werden nicht nur Speicherplatzbedarf, Netzwerkverkehr und Last für Produktionsserver verringert, sondern auch eine Reihe möglicher Ausfallsituationen, von Anwendungsausfällen bis zu Serverfehlern und unvorhersehbaren Naturkatastrophen, abgedeckt. CA ARCserve D2D verringert außerdem den Zeitbedarf gegenüber der Wiederherstellung physischer Daten, die bei Erwerb neuer Hardware oder der Verlagerung von Daten in ein vollständig neues Rechenzentrum erforderlich ist.

Bei der „heißen“ Migration erfolgt die Serverkonsolidierung, ohne dass das System vollständig ausgeschaltet wird. Damit wird eine hohe Verfügbarkeit gewährleistet. Ein Server kann in Betrieb bleiben, während der Zielserver erstellt und die Daten übertragen werden. Der Vorgang lässt sich transparent und ohne wahrnehmbare Unterbrechung für die Benutzer oder bei der Verfügbarkeit von Anwendungen durchführen. Diese Art der Migration ist von entscheidender Bedeutung für Geschäftstätigkeiten und Benutzerverfügbarkeit, die rund um die Uhr gewährleistet sein müssen.

CA ARCserve High Availability bietet diese Art der Echtzeitreplikation, mit der sowohl die Verfügbarkeit rund um die Uhr als auch die Erfüllung von IT-Anforderungen sichergestellt sind. Durch die unmittelbare Übertragung von Workloads auf einen anderen virtuellen Server können Benutzer kontinuierlich auf Anwendungen zugreifen. Mit der CA ARCserve Replication-Funktion, Echtzeitüberwachung von Servern und Anwendungen sowie Funktionen für automatisiertes Failover und Failback wird sichergestellt, dass es praktisch zu keinen Ausfallzeiten für Benutzer oder von Anwendungen kommt.

---

## FAZIT

In diesem White Paper wurden eine Reihe an Herausforderungen aufgezeigt, die im Zuge der fortschreitenden Virtualisierung durch die Vielfalt der heute angebotenen Produkte entstehen. Sowohl die potenziellen Vorteile virtueller Umgebungen als auch die damit verbundenen Herausforderungen wurden erläutert. Um die Kontrolle über ein virtuelles Rechenzentrum zu behalten, müssen professionelle wie nicht professionelle Administratoren den Prozess aus einer ganzheitlichen Perspektive betrachten. Die Koordinierung unterschiedlicher Ansätze kann als große Herausforderung erscheinen. Die CA ARCserve-Produktfamilie bietet jedoch eine Palette an Tools und Ansätzen, die übergreifende Migration und umfassenden Schutz für Daten in der gesamten virtuellen Infrastruktur eines Unternehmens gewährleisten.