Planungen zum Umgang mit Datenverlusten

Lösungen für eine zuverlässige Gewährleistung der Geschäftskontinuität

Kroll Ontrack

Einleitung

Geschäftskontinuität wurde als Lösung entwickelt, um Mainframe-Systeme und erste Rechenzentren zu schützen. Das Konzept hieß zunächst „Notfallwiederherstellung“ und umfasste die Projektplanung genauso wie die Unterstützung durch Ausrüstungshersteller. Im Zuge der Weiterentwicklung der Lösung wurde die Planung der Notfallwiederherstellung zu einem Bestandteil des Geschäftskontinuitätsplans von Unternehmen. Ein Geschäftskontinuitätsplan stellt eine übergeordnete Richtlinie dar, mit der sichergestellt wird, dass alle Abteilungen eines Unternehmens bei Störungen möglichst ohne Beeinträchtigung weiterarbeiten können.[1] Ein Notfallwiederherstellungsplan ist mit seinen Maßnahmen Teil des Geschäftskontinuitätsplans. Was als formales Verfahren zum Schutz der teuren Computerausrüstung begann, dient heute dem Schutz aller Elemente eines Unternehmens.

Durch den Einsatz von Virtualisierungstechnologie können viele Unternehmen Geschäftskontinuität planen und gewährleisten. Eine Virtualisierung ist jedoch hochkomplex und setzt bei IT-Mitarbeitern und Führungskräften besondere Kenntnisse und Fähigkeiten voraus, damit ein optimaler Return on Investment erzielt werden kann. Bei einer nachlässigen Bereitstellung oder Verwaltung kann es passieren, dass Virtualisierung selbst geschäftliche Störungen oder Datenverluste verursacht.

Verwaltung des Host-Speichers in virtuellen Umgebungen

In diesem Artikel geht es um die Rolle von Virtualisierung in der Unternehmenswelt. Zudem geben Anbieter von Datenrettungsservices praktische Tipps zur Virtualisierung, mit denen sich die Datenrettung optimieren und zum Teil auch die damit verbundenen Kosten senken lassen.

Ermittlung von Ressourcen

Die Ermittlung und Verwaltung von Ressourcen in physischen Hardwaresystemen ist relativ einfach. Die Ermittlung in virtuellen Umgebungen mit ihren kryptischen Namenskonventionen ist hingegen komplex und wird durch das explosive Systemwachstum erschwert. (Siehe Abbildung 1 – Gelingt es Ihnen, den Development Domain Controller zu finden?) Die Taxonomie zur Ermittlung virtueller Maschinen, die bei physischen und virtuellen Systemen nicht einheitlich ist, führt bei Störungen des Geschäftsbetriebs oftmals zu menschlichen Fehlern.

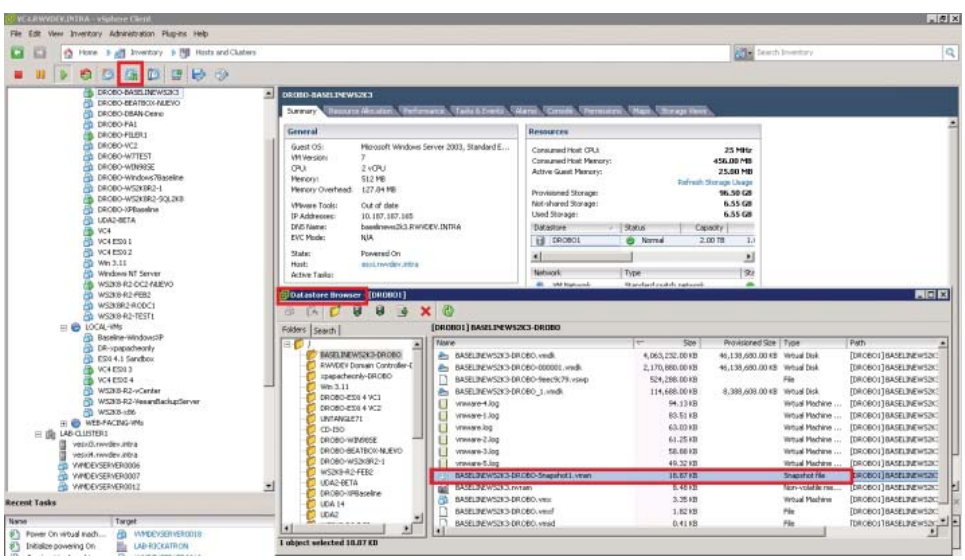


Abbildung 1 – „Identifying Virtual Machine Snapshots in vSphere“, Rick Vanover

Quelle: www.techrepublic.com

1 Im Sinne dieses Artikels sind Betriebsstörungen Vorfälle, die die Erledigung der täglichen Aufgaben behindern. Hierzu gehören Stromausfälle, gestörte Telefonleitungen usw. Als Datenverluste gelten Daten, die beschädigt sind. Somit gehören auch Datenverluste zur Kategorie Betriebsstörung.

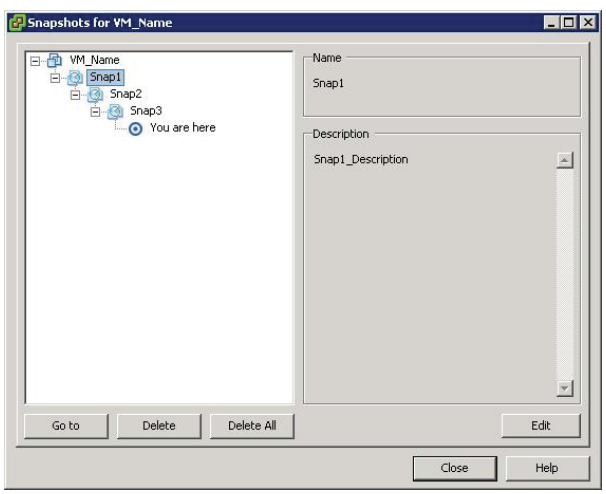
Anbieter von Datenrettungsservices berichten, dass Unternehmen bei IT-Notfällen meist nur über wenige oder gar keine Dokumentationen zu den ausgefallenen Speichersystemen verfügen. Datenrettungsexperten empfehlen Unternehmen, einen einfachen, aktuellen Screenshot der virtuellen Maschinen einzelner Host-Server zu erstellen, um die Wiederherstellung zu beschleunigen, da sich Systeme so priorisieren lassen.

Die Snapshot-Funktion von Hypervisoren war niemals als Ersatz für Sicherungslösungen gedacht. Sie dient vielmehr als Methode zur Bewahrung des momentanen Zustands einer virtuellen Maschine sowie von deren Laufwerksdaten.

Snapshot-Verwaltung in virtuellen Umgebungen

Die Snapshot-Funktion von Hypervisoren war niemals als Ersatz für Sicherungslösungen gedacht. Sie dient vielmehr als Methode zur Bewahrung des momentanen Zustands einer virtuellen Maschine sowie von deren Laufwerksdaten. Ein Routine-Snapshot vor der Systemwartung zum Beispiel sollte nach der erfolgreichen Wartung auf das primäre virtuelle Laufwerk verschoben werden. (Siehe Abbildung 2.)

Durch die Existenz mehrerer Snapshots verlangsamt sich der Zugriff auf virtuelle Laufwerksdaten, da Snapshot-Dateien eine Untermenge der in der primären virtuellen Laufwerksdatei gespeicherten Daten enthalten. Snapshots belegen wertvollen Speicherplatz und füllen so den Datenspeicher. Wenn nicht mehr benötigte Snapshots nicht gelöscht werden, kann die gesamte virtuelle Umgebung darunter leiden. Wenn es zu einem Vorfall kommt, müssen alle virtuellen Laufwerksdateien wiederhergestellt werden, damit sich die Wiederherstellungspunktziele einhalten lassen.



Anbieter von Datenrettungsservices betrachten zahllose Snapshots als Hindernis für eine erfolgreiche Rettung, wenn virtuelle Laufwerksdateien gelöscht wurden oder ein Datenspeicher-Volume neu formatiert wurde.

Abbildung 2 – „Troubleshooting Virtual Machine Snapshot Problems", Ruben Garcia, Februar 2010

Nicht getestete Geschäftskontinuitätspläne

Experten für Geschäftskontinuität und Anbieter von Datenrettungsservices berichten immer wieder, dass Unternehmen ihre Geschäftskontinuitäts- und Notfallwiederherstellungspläne nicht ausreichend testen. Don Stewart, Director of Professional Services bei Ongoing Operations, einem gemeinnützigen Anbieter von Geschäftskontinuitätslösungen für US-amerikanische Genossenschaftsbanken, meint: „Viele Geschäftskontinuitätspläne werden nicht richtig ausgeführt. Beim Testen eines Plans erklärte der Wiederherstellungskoordinator eines Unternehmens kürzlich, dass er zunächst nach dem über 500-seitigen Geschäftskontinuitätsplan suchen müsse. Hierfür bat er um mehr Zeit." Stewart berichtet, dass viele Unternehmen eine jährliche Planübung durchführen. Dabei wird jedoch oft nur das Dokument überprüft und die Telefonnummern der Beteiligten aktualisiert. Stewart erklärt, dass sich Kontinuitäts- und Wiederherstellungspläne ausschließlich in der Praxis verifizieren lassen. Das Durchspielen von Notfällen liefert Führungskräften Informationen über Methoden zur Eindämmung geschäftlicher Störungen sowie über die Dauer der Wiederherstellung von Services. So lassen sich auch die Kosten einer Störung besser einschätzen.

Stewart empfiehlt, Störungen bei Übungen anhand finanzieller Zahlen (also in Dollar und Euro) zu messen und nicht anhand der maximal zulässigen Ausfallzeit in Stunden oder Tagen. Wenn die finanziellen Auswirkungen einer Störung bekannt sind, lassen sich auf Grundlage realistischer Ziele Prioritäten festlegen.

Das Mercy Medical Center in Cedar Rapids (Iowa, USA) ist ein Erfolgsbeispiel für die Nutzung eines Geschäftskontinuitätsplans im ganzen Unternehmen. Als es im Jahr 2008 zu Überschwemmungen kam, wurde der Plan erfolgreich angewendet. Laut offizieller Website (hospital's website) befand sich das Krankenhaus nach drei Wochen wieder im Normalbetrieb. Im *Health Blog* des *Wall Street Journal*[2] finden Sie ein interessantes Interview zu den Evaluierungs- und Wiederherstellungsverfahren des Plans.

Anbieter von Datenrettungsservices berichten, dass Unternehmen die Planung der Geschäftskontinuität ernster nehmen, die Wahl eines Datenrettungsservice jedoch nur selten formaler Bestandteil des Notfallwiederherstellungsplans ist. Erfolgt die Auswahl des Anbieters erst mitten im Notfall, werden die Kriterien wahrscheinlich weniger durchdacht sein als die Entscheidung über die richtige Kaffeemaschine für den Pausenraum. Da unerfahrene oder unzureichend ausgestattete Anbieter von Datenrettungsservices Krisensituationen noch verschlimmern können, sollten Unternehmen den geeigneten Anbieter schon vor einem Notfall auswählen. Bei der Entscheidung für einen Anbieter sollten Sie die folgenden fünf Kriterien beachten:

- Suchen Sie nach Unternehmen, die über die richtigen Technologien und Mitarbeiter verfügen, um verschiedenste Datenverluste beheben zu können. Ein Datenverlust kann verschiedene Plattformen betreffen. Eine Störung kann sich zum Beispiel auf UNIX-, Linux- und Windows®-basierte Systeme auswirken, die alle auf einem virtuellen Server ausgeführt werden.
- Suchen Sie nach Unternehmen, die Datenrettungslösungen für Ihre speziellen Anforderungen anbieten.

[2] „When Hospitals Fall Victim to Disaster", Shirley S. Wang, Wall Street Journal, Juni 2008

- Suchen Sie nach Unternehmen, die Ihnen alle Informationen bereitstellen, damit Sie eine fundierte Kaufentscheidung treffen können.
- Suchen Sie nach Unternehmen, die Ihnen einen professionellen Kundendienst bieten, egal wann und wo Sie ihn benötigen.
- Suchen Sie nach Unternehmen, die umfassend dokumentierte und etablierte Verfahren zur Gewährleistung der Sicherheit und Vertraulichkeit Ihrer Daten aufweisen. Nur wenige Anbieter von Datenrettungsservices haben sich einer Compliance-Prüfung für IT-Sicherheit unterzogen und diese bestanden. Wenn Ihnen die Sicherheit Ihrer Daten wichtig ist, sollten Sie nach einem Unternehmen suchen, das eine externe Sicherheitsprüfung bestanden hat.

Evaluierung der häufigen Vorboten von Datenverlusten

IT-Mitarbeiter und Datenrettungsexperten nennen die folgenden Vorboten als häufigste Ursachen für Datenverluste:

- Menschliches Versagen
- Fehler in der Speicherhardware
- Notfallwiederherstellungspläne, die zu ungenau sind oder nicht regelmäßig getestet werden
- Zu hohes Vertrauen in die Redundanz von SAN-Speichern
- Beschädigte oder nicht lesbare Sicherungskopien bzw. Archive mit fehlenden Daten

Im Folgenden berichten IT-Experten über die Bedeutung ihrer Projekte, über deren Umfang und über die möglichen Auswirkungen von Datenverlusten.

> *„Wir befinden uns seit drei Monaten in der Planungsphase. Ich kann Ihnen gar nicht sagen, wie viele Vorstudien und Analysen der Geschäftsauswirkungen ich durchgeführt habe. Ich vertraue keinem Speichermedium, weder SSD noch Band oder der Cloud. Darum speichere ich meine Daten an verschiedenen Standorten. Ich plane für Ausfälle und verfüge über eine Lösung zum Schutz der Daten." – Ein IT-Architekt, der kurz vor der E-Mail-Migration für 40.000 Benutzer steht*

> *„Unser Business Intelligence-Projekt läuft bereits seit sechs Jahren und umfasst Daten im 100-TB-Bereich. Wir verbringen viel Zeit mit der Erstellung von Kennzahlen und der Zuordnung der Daten. Die Rohdaten umfassen 30 bis 40 Milliarden Zeilen in einer einzelnen Tabelle. In meinem Team können wir uns keine Fehler leisten." – Ein Geschäftsanalyst im Einzelhandel*

> *„Kaum jemand testet seine Sicherungskopien. Sie sind entweder unvollständig oder ungetestet. Viele Unternehmen wiegen sich angesichts virtueller Speicher in falscher Sicherheit und führen keine Sicherungen durch. Wenn sie es doch tun, werden die Daten im gleichen SAN gesichert, in dem sich auch die Originaldaten befinden. Wenn das SAN ausfällt, gibt es keine Zugriffsmöglichkeit mehr. So verzögert sich die Wiederherstellung."*
> *– Ein Datenrettungsexperte*

„Ausfälle von RAID-Controllern sind bei uns die häufigste Ursache für Support-Anrufe. Derartige Ausfälle lassen sich nur schwer beheben, verursachen jedoch große Schäden. Nur wenige IT-Administratoren verfügen über einen Plan zum Umgang mit diesen Vorfällen. So kann es passieren, dass das gesamte System abstürzt. Wenn wir mit der Problemlösung beginnen, stürzen wir uns nicht sofort auf die Sicherungskopien. Zunächst analysieren wir die E/A-Ereignisprotokolle, um zu ermitteln, wann die Probleme angefangen haben. Dann stellen wir mithilfe unserer Replikationslösung und der Bestandteile anderer Sicherungskopien die fehlenden Daten gezielt wieder her. Hierbei handelt es sich um eine geplante Wiederherstellung, so dass wir die Ziele hinsichtlich der Wiederherstellungszeit einhalten können. Auf diese Weise können wir auch Wiederherstellungspunktziele erfüllen, die von den Unternehmen festgelegt worden sind."
– Ein Anbieter von Geschäftskontinuitätsservices

Laut einer weltweiten IDC-Analyse externer Laufwerkspeichersysteme betrug die Gesamtkapazität der ausgelieferten Laufwerkspeicher mehr als 5.100 Petabyte – eine Steigerung um 55,7 % im Vergleich zum Vorjahr.[3]

Diese Berichte zeigen, dass angesichts der steigenden Speicher- und Datenvolumen Vorbereitungen auf geschäftliche Störungen und Datenverluste immer wichtiger werden. IT-Projekte werden immer umfangreicher, die Planung dauert länger, und Unternehmensdaten erreichen inzwischen den Petabyte-Bereich. Sicherungskopien bieten keinen ausreichenden Schutz, und Datenverluste können für Unternehmen in umkämpften Märkten fatale Folgen haben.

Planungen zum Umgang mit Datenverlusten

Laut einer weltweiten IDC-Analyse externer Laufwerkspeichersysteme betrug die Gesamtkapazität der ausgelieferten Laufwerkspeicher mehr als 5.100 Petabyte – eine Steigerung um 55,7 % im Vergleich zum Vorjahr.[3] Angesichts dieses Wachstums ist eine zuverlässige IT-Verwaltung mit einer ausführlichen Dokumentation der Notfallwiederherstellung sowie regelmäßigen Übungen der Notfallpläne erforderlich. Nur so lassen sich Störungen des Geschäftsbetriebs, die mit Datenverlusten in virtuellen Umgebungen zusammenhängen, wirkungsvoll minimieren bzw. ganz verhindern.

Geschäftliche Störungen infolge von Datenverlusten stellen eine extreme Herausforderung dar. IT-Mitarbeiter sind damit beschäftigt, die wichtigsten Systeme wieder zum Laufen zu bringen, während die Geschäftsführung sich Gedanken über die Auswirkungen auf das Unternehmen und seine Kunden machen muss.

Erfolgreiche Unternehmen wissen, dass jede Störung – und sei sie noch so klein – den gesamten Geschäftsbetrieb beeinträchtigen kann. Darum haben viele IT-Führungskräfte und Planer von Geschäftskontinuitätslösungen Datenrettungsservices proaktiv in ihre Notfallpläne integriert. Wenn IT-Teams einen geeigneten Anbieter von Datenrettungsservices wählen, bevor es zu tatsächlichen Störungen kommt, können sie Probleme im Geschäftsbetrieb verhindern.

[3] „Worldwide Disk Storage Systems Finishes 2010 with Double-Digit Growth on Strong Fourth Quarter Results", IDC, März 2011

Die wichtigsten Tipps

Virtualisierung bringt im Host-System mehr Komplexität mit sich. Bei einem Datenverlust muss ein Anbieter von Datenrettungsservices beauftragt werden, der sich mit der Wiederherstellung in virtuellen Systemen auskennt. Im Folgenden finden Sie Tipps zur sicheren Wiederherstellung verlorener Daten in virtuellen Umgebungen:

- Stellen Sie Sicherungskopien auf einem anderen Laufwerk wieder her. So können Sie gewährleisten, dass alle wichtigen Dateien gut gesichert sind, falls Sie Daten auf dem aktiven Laufwerk überschreiben.
- Erzeugen Sie bei RAID-Problemen vor der Wiederherstellung ein Abbild aller RAID-Laufwerke. Manchmal funktioniert die RAID-Wiederherstellung nicht richtig. Dies kann eine Lösung der Probleme erschweren. Testen Sie Sicherungskopien, indem Sie sie an einem anderen Speicherort wiederherstellen, bevor Sie das RAID-Array überschreiben.
- Erstellen Sie auf dem wiederherzustellenden Laufwerk keine neuen Dateien, und stoppen Sie alle virtuellen Maschinen, bis die wichtigen Daten gerettet sind. Neue Dateien können die zu rettenden Dateien überschreiben, so dass die Wiederherstellung fehlschlägt. Auch auf Snapshots basierende virtuelle Maschinen sowie per Thin Provisioning bereitgestellte virtuelle Laufwerke, die nach dem Datenverlust weiter genutzt werden, können zu rettende Dateien überschreiben.
- Überprüfen Sie durch Wiederherstellung auf einem anderen Laufwerk, ob die Sicherungskopie in Ordnung ist, bevor Sie FSCK-, CHKDSK- oder andere Reparaturprogramme auf eine virtuelle Festplatte anwenden. Solche Reparaturprogramme funktionieren nur dann ordnungsgemäß, wenn eine fehlerfreie Sicherungskopie vorhanden ist. So müssen zur Gewährleistung eines konsistenten Dateisystems bestimmte Dateizeiger überschrieben werden. Auf Wunsch können Sie die Programme im Lesemodus ausführen, um mögliche Fehler aufzuspüren, bevor Sie eine Reparatur vornehmen.
- Wenn ein virtuelles Laufwerk gerettet werden soll, auf dem gleichen Volume jedoch weitere virtuelle Laufwerke ausgeführt werden, die sich bei der Rettung nicht schließen lassen, klonen oder migrieren Sie die Laufwerke auf ein anderes Volume. Wenn ein gelöschtes virtuelles Laufwerk oder ein Snapshot wiederhergestellt werden sollen, erzeugen Sie Kopien oder Klone der virtuellen Maschinen. Bei einer Migration könnten sie Bestandteil der gelöschten Rettungskopie sein.
- Schließen oder klonen/kopieren Sie alle anderen aktiven virtuellen Maschinen, die sich auf dem gleichen Laufwerk befinden und per Thin Provisioning bereitgestellt werden bzw. auf Snapshots basieren. Beim Schreiben in den neuen Blöcken des Laufwerks können zu rettende Daten überschrieben werden.

Kroll Ontrack

Mehr Informationen im Internet oder
über unsere kostenlose Hotline:
0800 10 12 13 14
www.krollontrack.de