Acronis

Microsoft Partner
Gold Application Development

Sicherung einer Hybrid Cloud-Infrastruktur und von virtuellen Microsoft Azure-Maschinen

mit Acronis Backup 12

Dieser Anwendungsfall beschreibt die Sicherung einer kompletten Hybrid Cloud-IT-Umgebung (inkl. Microsoft Azure-VMs) mit Acronis Backup 12

Juni 2016

USECASE

Einführung

Das Microsoft Azure® IaaS-Angebot (Infrastructure as a Service) wird in dynamischen IT-Umgebungen zunehmend zur Norm – und das aus mehreren Gründen. Da wären zuerst einmal mögliche Kostensenkungen, weil auf physische Hardware, Storage oder ein Netzwerk verzichtet werden kann. Ein weiterer Grund besteht darin, dass sich die Komplexität von Rollouts drastisch senken lässt. Gemäß einer IDC-Studie[1] verwenden 79 Prozent aller Unternehmen eine Cloud-Umgebung oder implementieren diese gerade. Wenn ein Unternehmen eine IT-Umgebung hat, die gleichermaßen aus einer Cloud-Umgebung, virtuellen Maschinen (VMs) und physischen Servern besteht, wird diese von uns als „Hybrid Cloud-Umgebung“ bezeichnet.

Egal welche Umgebung (Cloud, physisch, virtuell, hybrid) Sie letztendlich verwenden – Ihre Daten müssen immer vor Verlust und katastrophalen Ereignissen („Desastern“) geschützt werden. Da sich diese Umgebungen jedoch in puncto Infrastruktur, Aktionen und Verwaltung unterscheiden, sind zur Sicherung ihrer Daten aber auch unterschiedliche Ansätze und Technologien erforderlich. Insbesondere die Datensicherung in Hybrid Cloud-Umgebungen stellt Unternehmen vor diverse Herausforderungen, weil die meisten Produkte auf dem Markt entweder unvollständig, umständlich und/oder sehr teuer sind.

Einige Hersteller bieten eine traditionelle 'Eine-für-alles'-Plattform mit einem intelligenten Backup Server als zentrale Komponente an, welcher eine einheitliche Datensicherung für die komplette IT-Umgebung durchführen und verwalten kann. Meistens unterstützen solche traditionellen Plattformen jedoch keine IaaS-Cloud-Umgebungen. Andere Hersteller bieten für verschiedene Datentypen, Betriebssystemplattformen und Applikationen nur jeweils separate Backup & Recovery-Produkte an. Die Kunden dieser Unternehmen müssen daher meist mehrere unterschiedliche Backup-Tools kaufen/einsetzen.

Acronis dagegen bietet ein einzelne, integrierte Data Protection-Lösung (inkl. einheitlicher Steuerung, Verwaltung und Berichtserstellung) für komplette IT-Umgebungen an – unabhängig von der Unternehmensgröße, der Art und Menge der Daten, der Betriebssystemplattformen und der verwendeten Anwendungen.

Dieses Dokument beschreibt die Herausforderungen, die Unternehmen bei der Sicherung ihrer Hybrid Cloud-Umgebung meistern müssen, und demonstriert anhand eines typischen Anwendungsfalls, wie Acronis Backup alle vorhandenen Daten zuverlässig sichern kann.

Die Lektüre dieses Anwendungsfalls empfiehlt sich für die CIOs, CTOs, IT-Direktoren/-Manager von mittleren Unternehmen sowie für die IT-Administratoren von kleineren Unternehmen.

[1] IDC CloudView 2016-Umfrage, Januar 2016

IT-Produktions-Workloads des Unternehmens

Das Unternehmen dieses Anwendungsfalls verfügt über ein primäres Datenzentrum, welches sich am selben Standort wie das Unternehmen selbst befindet. Dieses Datenzentrum hosted alle lokalen Produktionsserver, den Storage und die Netzwerkinfrastruktur. Die Desktop-PCs, Laptops und Mobilgeräte sind sowohl per Kabel (LAN) wie auch per WLAN vernetzt. Eine gewisse Anzahl der Workloads werden in Microsoft Azure bereitgestellt.

Die Produktionsserver

Das Unternehmen setzt auf eine gemischte Hybrid Cloud-IT-Umgebung, die aus physischen Servern sowie Microsoft Hyper-V®- und Azure-VMs besteht, über die unterschiedliche Workloads ausgeführt und Dienste für alle Abteilungen bereitgestellt werden. Es gibt einen MS SQL-Server (Focus SQL), der die SQL-Hauptdatenbank für eine der Business-Applikationen des Unternehmens ausführt. Wir werden uns im späteren Verlauf dieses Dokuments die Sicherung und Wiederherstellung dieses Servers genauer anschauen.

- Es gibt zehn physische Server, auf denen zwei primäre Microsoft® Active Directory® (AD) Domain Controller (DCs), eine ERP-Produktionssoftware (Enterprise Resource Planning) sowie einige herkömmliche Applikationen ausgeführt werden. Die IT arbeitet außerdem an der Virtualisierung der physischen Server, die bald abgeschlossen sein wird. Einige wenige physische Server sollen verbleiben, da ihre Applikationen nicht virtualisiert werden können (aufgrund mangelnder Unterstützung der entsprechenden Hersteller).
- Die Mehrheit der lokalen Workloads laufen auf Microsoft Hyper-V-VMs. Es handelt sich um 33 VMs, die von fünf Hyper-V-Hosts ausgeführt werden.
- Hyper-V verwendet einen 16 TB SAN-Storage zur zentralen Produktion, auf dem die meisten der VMs vorliegen. Hyper-V ist auf der logischen Ebene in zwei Bereiche aufgeteilt: Produktion und F&E/QS.
- Die Mehrzahl der Applikationen wird in der virtuellen Umgebung ausgeführt – Microsoft Exchange®, einige Microsoft SQL®-Server, einige von der F&E selbst entwickelte Applikationen sowie ein CRM-System (Customer Relationship Management) auf Basis eines Oracle®-Datenbankservers, welcher wiederum auf einem Windows®-Host läuft.
- Der Focus SQL-Server ist ein üblicher physischer 2U-Entry-Level-Datacenter-Server. Er hat zwei CPUs; 8 GB RAM, vier 2.5''-SAS-Festplatten (je 150 GB, per Onboard-Controller als RAID-6-Verbund organisiert) und zwei 1-Gbit-Ethernet-Controller.

- Das einzelne 300-GB-RAID-Volume auf dem Focus SQL-Server hat drei Partitionen:
  - Eine versteckte Partition mit 100 MB (während der Windows Server® 2012-Installation erstellt)
  - Eine primäre Boot-Partition für das System (Laufwerk C) mit 120 GB, von denen 45 GB durch das Betriebssystem und den Microsoft SQL Server® belegt werden
  - Eine primäre Partition mit 180 GB (Laufwerk D), von denen 75 GB durch die SQL-Datenbank und -Protokolle belegt werden

Das Netzwerk auf dem Focus SQL-Server ist standardmäßig organisiert – statische IP-Adresse, DNS-Name, Active Directory-Mitgliedschaft.

Das Produktionsnetzwerk

Das Unternehmen nutzt ein flach strukturiertes 1-Gbit-Netzwerk, in dem Netzwerk-Switches mittleren Niveaus verwendet werden. Der Datendurchsatz ist akzeptabel. Das Netzwerk des Datenzentrums hat drei große logische Subnetze:

- Ein physisches Segment, in welchem die physischen Server, das ERP-System und die primären DCs liegen
- Ein virtuelles Produktionssegment, per Hyper-V definiert und verwaltet
- Ein virtuelles F&E-/QS-Segment, ebenfalls per Hyper-V verwaltet
- Ein virtuelles Azure-Netzwerk (VNet), welches per Standort-zu-Standort-VPN mit dem On-Premise-Netzwerk verbunden ist

Der Storage für Produktion und Backup

Wie zuvor schon beschrieben, basiert der On-Premise-Storage für die Produktion auf einem zentralen 16-TB-SAN, welches von Hyper-V verwendet wird. Die On-Premise-Backups werden auf drei separaten NAS-Geräten (Network Attached Storage) gespeichert:

- NAS-1 dient als Backup-Ziel für die physischen Server. Es ist mit demselben Netzwerk-Switch verbunden, den auch die meisten der physischen Server verwenden. NAS-1 ist auch das Backup-Ziel des Focus SQL-Servers, wofür 8 TB Speicherplatz verwendet werden. Der Server und das NAS sind per 1-GBit-LAN an denselben Netwzerk-Switch angebunden.
- NAS-2 ist über einen kleinen, dedizierten Netzwerk-Switch mit demselben ESXi-Host verbunden. Auf diesem Host wurde Acronis Backup von der IT als virtuelle Appliance (VA) installiert, um ein 'LAN-freies' Backup der Produktions-VMs zu ermöglichen.
- NAS-3 (F&E/QS) ist wiederum mit einem der ESXi-Hosts der F&E/QS-Abteilungen verbunden – und auch hier ist Acronis Backup als VA zur Durchführung LAN-freier Backups installiert.

Die NAS-Geräte wurden von der IT netzwerkmäßig separiert, um die Backups über verschiedene Netzwerkzonen verwalten bzw. den Datenfluss in spezifischen Subnetze konzentrieren zu können.

Die Azure VM-Laufwerke befinden sich zur Ermöglichung einer hohen Performance auf einer Kombination aus Azure P10- und P20-Premium-Festplatten. Die Azure VM-Backups werden zum Azure File Storage erstellt und dann in die Acronis Cloud repliziert.

Backup-Richtlinie des Unternehmens

Die Backup-Richtlinie des Unternehmens ist Teil des übergeordneten Disaster Recovery (DR)-Plans. Sie beschreibt die erforderliche IT-Ausstattung und eine Strategie zur Bewahrung der Geschäftskontinuität (Business Continuity, BC), die sämtliche betrieblichen Bereiche des Unternehmens einbezieht: Kommunikation, Vertrieb und Buchung, Finanzen, Prüfung und Compliance, Logistik, Personalwesen (HR) usw.

Zielvorgaben für die Geschäftskontinuität

Die Backup- und DR-Richtlinie wurde von einem Planungsteam entwickelt und dann von der Geschäftsführung genehmigt.

Die erste Vorgabe des Plans definiert die gewünschten RTO- bzw. RPO-Werte (Recovery Time Objective, Wiederherstellungszeitvorgabe bzw. Recovery Point Objective, Wiederherstellungspunktvorgabe) für das Unternehmen.

Beim Festlegen der RTO- und RPO-Werte muss das verfügbare Budget berücksichtigt werden. Kürzere RTOs/RPOs sind kostenintensiver und erfordern mehr Ressourcen. Ein RTO- und RPO-Wert von Null würde beispielsweise erfordern, fehlertolerante Systeme über große Entfernungen zu implementieren. Ein RPO- und RTO-Wert von wenigen Sekunden würde eine Hochverfügbarkeitslösung über große Entfernungen erfordern. Das Unternehmen in diesem Anwendungsfall kann sich jedoch weder fehlertolerante Systeme noch eine Hochverfügbarkeitslösung leisten.

Um zu ermitteln, welchen RTO-Wert das Unternehmen benötigt bzw. wie lange es (maximal) ohne seine wichtigsten Systeme operieren kann, hat das Planungsteam die Geschäftsprozesse, die betrieblichen Aktivitäten, die Ausfallzeitkosten sowie das verfügbare Budget analysiert. Aus diesen Daten hat das Planungsteam dann ermittelt, dass der passende RTO-Wert zur vollständigen Wiederherstellung des normalen Geschäftsbetriebs 96 Stunden beträgt.

Für die Produktions-Workloads leitet sich daraus wiederum ein RTO-Wert von 72 Stunden ab. Der RTO-Wert für einen einzelnen Server beträgt 24 Stunden. Die RTO-Werte für einzelne Unterkomponenten des DR-Plans sind jeweils immer kürzer als der RTO-Wert für das komplette Unternehmen.

Als weiteres beschreibt der DR-Plan den RPO-Wert für das Unternehmen. Der RPO-Wert definiert, welcher (maximale) Zeitraum noch akzeptabel ist, während dem wichtige Ressourcen (wie z.B. die Erfassung/Verarbeitung wichtiger Daten) nicht verfügbar sind/sein dürfen. Obwohl die meisten Unternehmen ihre Ressourcen/Daten gerne zu 100% schützen bzw. bewahren wollen, ist dies wirtschaftlich jedoch meist nicht praktikabel.

Stattdessen sollte ein Unternehmen bei der Bestimmung seines RPO-Wertes besser entscheiden, welchen (maximalen) Datenverlust es hinnehmen kann – und zwar auf Basis der Zeitdauer vor dem DR-Ereignis bis zu dem Augenblick, wenn das Ereignis eintritt (gemessen in Sekunden, Minuten, Stunden oder Tagen). Im vorliegenden Anwendungsfall bestimmte das Planungsteam, dass der RPO-Wert für das Unternehmens 24 Stunden betragen

soll. Das bedeutet mit anderen Worten: das Unternehmen akzeptiert, im Fall eines Desasters alle Daten (und daraus resultierenden Produkte/Ressourcen) zu verlieren, die innerhalb der letzten 24 Stunden vor Eintritt des Desasters generiert wurden. Ein RPO-Wert von 24 Stunden bedeutet also, dass die IT jeweils täglich ein Backup der entsprechenden Unternehmensdaten erstellen muss.

Die RPO-Werte von Unterkomponenten eines übergreifenden DR-Plans können gleich oder kürzer als der Gesamt-RPO-Wert für das Unternehmen sein. Einige Unternehmen definieren für ihre Produktions-Workloads verschiedene Level und legen dann (je nach Bedeutung der generierten Daten) unterschiedliche RPOs für diese Level fest.

Die Backup-Lösung des Unternehmens

Das Unternehmen verwendet Acronis Backup, um seine Microsoft Azure-VMs und das Produktionsdatenzentrum zu sichern. Acronis Backup ist eine einheitliche Data Protection-Lösung für alle On-Premise-Workloads, Remote-Systeme, Benutzer-Endpunkte (Workstations, PCs etc.), Mobilgeräte sowie Daten in Private oder Public Clouds.

Das Unternehmen hat sich für Acronis Backup entschieden, weil es folgende Fähigkeiten und Möglichkeiten bietet:

- Data Protection für die komplette Hybrid-IT-Unternehmensinfrastruktur (physische Server, VMs, Cloud-Umgebung etc.)
- Eine einheitliche Webkonsole zur zentralen Installation, Konfiguration und Verwaltung der Lösung
- Eine bewährte Disk-Imaging-Technologie, welche die Laufwerke/Volumes beliebiger Maschinen (physisch, virtuell, Cloud) zuverlässig und vollständig erfasst
- Single-Pass-Backup für Microsoft Exchange, SQL Server, SharePoint® und Active Directory, welches die entsprechenden Applikations- und Betriebssystemdaten gleichzeitig sichern kann
- Unterstützung mehrerer Hypervisor (inkl. MS Hyper-V)
- Nahtlose, plattformübergreifende Migration, um Server/Maschinen (physisch, virtuell, Cloud) auch auf anderen Plattformen/Hardware-Konfigurationen wiederherstellen zu können
- Agentenloses Backup von virtuellen Maschinen

Die Wahl ist nicht zuletzt auch deswegen auf Acronis gefallen, weil es typische zentrale Fehlerquellen beseitigt. Denn jeder Data Protection-Workload verfügt über alle notwendigen Fähigkeiten, kann also beispielsweise Backups selbst auslösen und die dazugehörigen Datenströme ermöglichen. Die Webkonsole dient dagegen nur der zentralen Verwaltung und Berichterstellung.

Zu schützende Systeme (Backup-Quellen)

Das Unternehmen verwendet Acronis Backup, um alle Produktions-Workloads zu sichern – also die physischen Server und VMs für Produktion und F&E/QS, den Focus SQL-Server sowie alle Workloads in Microsoft Azure. Die vollständigen Backups erfassen etwa 2 TB an nicht komprimierten Daten. Die differentielle und inkrementelle Backups generieren deutlich weniger Daten, weil hier nur Datenänderungen gespeichert werden. Die durchschnittliche, täglich im Unternehmen geänderte Datenmenge beträgt etwa 1,5 Prozent (aller Daten). Die täglichen inkrementellen Backups erfassen 30 GB Daten, während es bei wöchentlichen differentiellen Backups 150 GB sind.

Mit Acronis Backup benötigt das Unternehmen kein synthetisches oder Konsolidierungs-Backup, weil sich die Daten per Single-Pass-Recovery automatisch aus den Backup-Punkten rekonstruieren lassen.

Die Backup Storage-Richtlinie

Seine On-Premise-Systeme sichert das Unternehmen zuerst auf seine lokalen NAS-Geräte. Von dort werden die Backups als Kopien in die Acronis Cloud repliziert. Seine Microsoft Azure-Systeme sichert das Unternehmen zuerst in den Azure File Storage. Die entsprechenden Backups werden dann in die Acronis Cloud repliziert. Acronis Backup kann Backup- und Replikationsaktionen auf jeder Plattform in einem gemeinsamen Plan kombinieren.

Der Vorteil einer lokalen Backup-Kopie besteht darin, dass die IT die gesicherten Workloads/Daten schnell und direkt wiederherstellen kann, ohne Backup-Kopien vorher von entfernten Standorten/Speicherorten abrufen zu müssen. Backup-Kopien, die in der Acronis Cloud gespeichert werden, sind dagegen als Schutz gegen größere Störfalle bzw. Desaster gedacht.

Dieser Ansatz entspricht der von Acronis empfohlenen „3-2-1"-Backup-Strategie: Bewahren Sie Ihre Daten an drei (3) Standorten auf (z.B. als Original im Produktionssystem, als Backup auf NAS/Azure Storage, als Backup in der Acronis Cloud), verwenden Sie für die Backups zwei (2) verschiedene Storage-Typen (z.B. Festplatte und Cloud), wobei eine (1) der Backup-Kopien extern gespeichert werden sollte (offsite, z.B. eine Cloud-Umgebung).

Die Backup-Planung

Nachdem die RPO-/RTO-Werte, die zu schützenden Systeme (Backup-Quellen) und die Backup Storage-Richtlinie definiert wurden, ist die letztendliche Festlegung der Backup-Planung eine eher leichte Aufgabe für die IT. Acronis Backup verfügt beispielsweise über das Backup-Schema „Großvater-Vater-Sohn" (GVS), welches gut zu den Anforderungen des Unternehmens passt. Das Unternehmen verwendet daher dieses Backup-Schema und entscheidet sich für monatliche Voll-Backups (aller Daten) sowie wöchentliche differentielle und tägliche inkrementelle Backups, um die Backup-Zeiten und Speicherplatzanforderungen zu verringern.

Die täglichen Backups werden um/ab 22:00 Uhr ausgeführt, damit sie außerhalb der üblichen Arbeits-/Betriebszeiten liegen. Die wöchentlichen und monatlichen Backups werden freitags um 22:00 Uhr ausgeführt.

Dabei muss die IT keine Blackout-Periode für das Backup-Fenster definieren. Die von Acronis verwendete Snapshot-Technologie beeinflusst die Systeme (egal ob virtuell, physisch oder Cloud) so wenig, dass keine Geschäftsvorgänge gestört werden. Die patentierte Disk-Imaging-Technologie von Acronis gewährleistet zudem, dass alle Daten im Backup konsistent sind. Dies gilt auch für Dateien, die bei Beginn der Datensicherung geöffnet sind.

Der Disaster Recovery-Plan

Naturkatastrophen sind in bestimmten Regionen durchaus gängig. In den USA gibt es beispielsweise über 1.200 Tornados pro Jahr. Erdbeben, Tsunamis, Überflutungen, Waldbrände, Wirbelstürme, Schlamm- und andere Lawinen – sie alle können ein komplettes Datenzentrum zerstören, manchmal sogar ohne Vorwarnung. Viele Naturkatastrophen können größere Gebiete betreffen, weshalb Sie eine Backup-Kopie immer in einer gewissen (sinnvollen) Entfernung vom Originalstandort aufbewahren sollten. Ein Unternehmen kann einen kontinuierlichen Geschäftsbetriebes folglich nur dann garantieren, wenn es auf Desaster gut vorbereitet ist.

Typische durch Menschen bedingte Desaster sind Krieg, Terrorismus oder Sabotage. Viele Desaster beruhen jedoch einfach auf menschlichem Versagen. Allerdings ist es auch unerheblich, ob ein Datenzentrum durch Brandstiftung oder augrund menschlichen Versagens zerstört wird. Das Ergebnis ist dasselbe. Desaster menschlichen Ursprungs lassen sich durch bestimmte Maßnahmen zwar verhindern oder minimieren – wirklich davor gefeit ist jedoch kein Unternehmen. Ein DR-Plan sollte also möglichst alle denkbaren Vorfälle abdecken, die den Geschäftsbetrieb stoppen oder Datenverluste verursachen können.

Im vorliegenden Fall erstellt das Unternehmen einen allgemeinen, übergeordneten DR-Plan und das IT-Team einen Plan für das Datenzentrum. Das IT-Team plant, dokumentiert und testet jeden einzelnen Schritt des DR-Prozesses.

Das IT-Team testet den DR-Plan regelmäßig, damit jeder zuständige Mitarbeiter seine Ziele und Aufgaben genau kennt. Von allen zuständigen Mitarbeitern wird verlangt, dass sie sich von Acronis zum zertifizierten Acronis Certified Engineer schulen lassen.

Wiederherstellung auf abweichender Hardware

Zu Acronis Backup gehört das bewährte Acronis Universal Restore, mit dem Systeme nicht nur auf denselben/ursprünglichen Maschinen, sondern auch auf abweichender Hardware wiederhergestellt werden können. Die Migration eines Workloads mit Acronis Universal Restore ist ein dreistufiger Prozess:

Stufe 1: Die Acronis AnyData Engine trennt den Server-Workload von der ursprünglichen Plattform

Der Prozess zur Wiederherstellung auf die abweichender Hardware beginnt damit, dass Acronis Backup ein Disk Image erstellt – also eine vollständige Backup-Kopie aller Daten, die sich auf den zu sichernden Laufwerken/ Partitionen der betreffenden Maschine (egal ob physisch, virtuell, Cloud) befinden.

Dabei gewährleistet Acronis Backup die Konsistenz der zu sichernden Daten dadurch, dass es – bevor die letztendliche Backup-Kopie erstellt wird – zuerst einen zeitlichen „Snapshot" des Laufwerks erfasst. Dazu wird entweder Microsoft VSS (Volume Shadow Copy Service), Linux® LVM (Logical Volume Manager) oder die eigene Snapshot-Technologie von Acronis (SnapAPI) verwendet. Das resultierende Disk-Image-Backp enthält anschließend alle Daten genau in dem Zustand, in dem sie zum Zeitpunkt der Snapshot-Erfassung auf dem Laufwerk vorlagen. Auf diese Weise wird ein „crash-konsistentes" Disk-Image erstellt.

Alle gerade laufenden Transaktionen auf/zu dem Laufwerk werden in einer Datenbank gesichert und alle Aktivitäten quasi „eingefroren" (auf den Zeitpunkt des Snapshots). Der Snapshot wird erfasst und das resultierende „applikationskonsistente" Disk-Image erstellt. Während des Kopiervorgangs werden die Daten „abstrahiert". Bei diesem Prozess werden plattformspezifische Eigenschaften der Datenelemente entfernt, sodass die Daten schließlich im Backup in einem allgemeinen, einheitlichen Format vorliegen und auf ihre essentiellen Eigenschaften reduziert sind.

Acronis Backup kopiert die Daten außerdem auf der Ebene der Laufwerkssektoren, sodass der Prozess nicht beeinflusst wird, wenn Dateien geöffnet oder vom Betriebssystem gesperrt sind. Im Disk Image sind nun alle Daten so enthalten, wie es für die Wiederherstellung eines Workloads erforderlich ist.

Stufe 2: Acronis Backup wendet das Server-Workload auf die neue Hardware an

Der nächste Schritt besteht darin, die Inhalte der gesicherten Laufwerke/ Partitionen auf die Zielmaschine (physischer Server/VM) anzuwenden. Wenn Sie einen physischen Server wiederherstellen wollen, muss dafür auf der neuen physischen Maschine kein Betriebssystem installiert sein. Stattdessen können Sie das Image direkt auf der fabrikneuen Hardware wiederherstellen (Bare Metal Recovery). Auch die Laufwerkskonfiguration der Zielmaschine muss nicht mit der der ursprünglichen Maschine übereinstimmen, denn Acronis Backup kann Laufwerke/Partitionen während

einer Wiederherstellung in der Größe anpassen. Die Ziellaufwerke müssen lediglich so groß sein, dass sie alle Backup-Daten aufnehmen können.

Zur Wiederherstellung virtueller Maschinen kann sich Acronis Backup direkt mit dem verwaltenden Hypervisor verbinden und auch eine vollständig neue VM (inkl. CPU, RAM, Laufwerkskonfiguration etc.) erstellen.

Stufe 3: Acronis Universal Restore passt den Workload an die neue Hardware an

Acronis Universal Restore analysiert die neue Hardware-Plattform oder den Hypervisor und passt die Betriebssystemeinstellungen an die Anforderungen des Ziels an.

CPU:

- Die Acronis AnyData Engine analysiert mögliche Änderungen beim CPU-Typ (Intel/AMD) und der CPU-Anzahl (CPU/SMP) und passt die Betriebssystemeinstellungen an die neuen Anforderungen an.

HAL (Hardware Abstract Layer):

- Die Acronis AnyData Engine analysiert den Maschinentyp, das Mainboard, den Chipsatz und die Hypervisor-Konfiguration – und passt die HAL-Einstellungen des Betriebssystems nach Bedarf an.

Boot-relevante Hardware-Treiber:

- Acronis Universal Restore analysiert die Ziel-Hardware und installiert alle Treiber, die das Betriebssystem zum Booten auf der neuen Maschine benötigt. Dazu gehören Treiber für SATA-, SAS-, SCSI- und RAID-Controller oder SAN-HBA-Adapter.
- Acronis Universal Restore deaktiviert möglicherweise kritische, auf der neuen Maschine nicht benötigte Hardware-Treiber, um Kompatibilitätsprobleme zu beseitigen.
- Sie können die benötigten Microsoft Windows®-Treiber (als INF-/SYS-Dateien) von einer CD/DVD oder einem Netzwerkordner aus laden und einbinden.
- Unter Linux kann Universal Restore die im Kernel integrierten Treiber-Module verwenden, auch wenn diese nicht aktiv sein sollten.

Netzwerktreiber:

- Acronis Universal Restore installiert und aktiviert alle erforderlichen Netzwerktreiber.
- Unter Windows kann Acronis Universal Restore alte Netzwerkadapter deaktivieren und entfernen, sodass Sie bei der Konfiguration des Netzwerks keine verborgenen oder fehlenden Geräte löschen müssen.

UEFI-BIOS-Konvertierung:

- Viele moderne Server verwenden den UEFI-Standard zum Booten des Betriebssystems, während virtuelle Server und ältere Maschinen oft noch mit dem BIOS-Standard arbeiten. Acronis Universal Restore kann das Partitionslayout, die Boot-Loader-Einstellungen und Boot-Konfigurationen so ändern, dass Sie das Image einer BIOS-Maschine auch auf einer UEFI-Plattform wiederherstellen können (und umgekehrt). Diese Konvertierung funktioniert mit den meisten Betriebssystemen (in beide Richtungen).

Focus SQL-Server Wiederherstellung

Betrachten wir jetzt genauer, wie ein IT-Mitarbeiter den Focus SQL-Server direkt auf einer Hyper-V-VM wiederherstellen kann.

- Der Mitarbeiter startet die Acronis Backup 12 Webkonsole und sucht den Focus SQL-Server in der Liste der Systeme.
- Der Mitarbeiter wählt die jüngste Backup-Version des Focus SQL-Servers aus und klickt anschließend auf die Schaltfläche „Recovery“, um die komplette Maschine wiederherzustellen.
- Der Mitarbeiter aktiviert die Option „Recovery-Ziel: Neue virtuelle Maschine“.
- Der Mitarbeiter wählt Hyper-V als entsprechenden Hypervisor aus und konfiguriert die VM:
  - Der Mitarbeiter übernimmt die CPU- und RAM-Konfiguration der ursprünglichen Maschine (2 CPUs, 8 GB RAM).
  - Der Mitarbeiter bestimmt in den Recovery-Optionen, dass die VM direkt nach der Wiederherstellung automatisch gestartet werden soll.
- Der Wiederherstellungsprozess wird gestartet.
- Nach dessen Abschluss wird die VM automatisch gestartet.
- Der Mitarbeiter verbindet sich über die Hyper-V-Verwaltungskonsole mit der VM, um zu überprüfen, dass diese korrekt gebootet wurde.
- Acronis Universal Restore installiert benötigte Netzwerktreiber in der VM. Der Mitarbeiter startet die VM neu, meldet sich an und legt die IP-Konfiguration fest.
- Der Mitarbeiter installiert die Hyper-V-Integrationsdienste, um die beste Performance für die VM zu ermöglichen.
- Der Mitarbeiter überprüft die korrekte Funktionsweise des SQL-Servers und dass dieser mit dem DNS und den AD-DCs kommunizieren kann.
- Die Wiederherstellung des Focus SQL-Servers ist damit abgeschlossen.
- Bei Bedarf kann der Mitarbeiter die neue Focus-SQL-Hyper-V-VM zu Microsoft Azure hochladen und damit die Cloud-Migration abschließen.

Der Wiederherstellungsprozess ist schnell, da der Mitarbeiter folgende Dinge nicht tun muss:

- Das Betriebssystem bereitstellen, weil dieses im Disk Image-Backup bereits enthalten ist
- Den Systemzustand wiederherstellen, weil dies bei der Wiederherstellung eines Disk Image-Backups nicht notwendig ist
- Backup-Agenten installieren, weil die entsprechenden Abläufe bei Hyper-V ohne Agenten durchgeführt werden können
- Eine separate (zusätzliche) Datenwiederherstellung durchführen, weil dies mit der Single-Pass-Backup-&-Recovery-Technologie nicht notwendig ist
- Inkrementelle Backups manuell wiederherstellen, weil der Single-Pass-Recovery-Prozess in einem Durchgang verläuft und dabei evtl. benötigte inkrementelle Backups automatisch einbezogen werden
- Ein Rollforward von SQL-/Exchange-Protokollen durchführen, weil das inkrementelle Disk-Image-Backup das komplette System mit allen Daten im aktuellsten Zustand enthält (statt nur Transaktionsprotokolle)

Zusammenfassung

Das Unternehmen ist auf jedes Recovery-Szenario gut vorbereitet. Das IT-Team hat einen Disaster-Recovery-Plan entwickelt, der Vorgaben für folgende Parameter definiert: Wiederherstellungspunktvorgaben (RPOs), Wiederherstellungszeitvorgaben (RTOs), Backup-Quellen (zu schützende Systeme), Backup Storage-Richtlinie und Backup-Planung. Dieser Disaster-Recovery-Plan wurde von der Geschäftsleitung genehmigt. Die IT testet den Plan regelmäßig mit verschiedenen Szenarien.

Das IT-Team verwendet Acronis Backup, um die komplette IT-Infrastruktur sichern und wiederherstellen zu können.

- **Physische Windows-Server:** Image- oder Datei-basiertes Backup von kompletten Windows-Maschinen, die mit einem Windows Server-Betriebssystem laufen
- **Microsoft Azure:** Backup von Azure-VMs und anderen IaaS-Cloud-Workloads, inkl. Applikationsunterstützung für Microsoft Exchange, SQL Server, SharePoint und Active Directory
- **Microsoft Hyper-V:** Agenten-loses Backup von Hyper-V-Hosts/-VMs, inkl. Applikationsunterstützung für Microsoft Exchange, SQL Server, SharePoint und Active Directory
- **Microsoft Exchange:** Single-Pass-Backup von Microsoft Exchange Servern, inkl. granularer Wiederherstellung von Postfächern, Ordnern und E-Mails
- **Microsoft SQL Server:** Single-Pass-Backup von Microsoft SQL Server, inkl. applikationskonformer Wiederherstellung von einzelnen Datenbanken oder kompletten Servern
- **Microsoft SharePoint:** Single-Pass-Backup von jeder Server-Rolle in einer SharePoint-Farm, inkl. applikationskonformer Wiederherstellung von einzelnen Dokumenten oder kompletten Servern
- **Microsoft Active Directory:** Konsistentes Single-Pass-Backup/-Recovery von Domain-Controllern, Active Directory-Datenbanken, System-Volumes (SYSVOLS) und Protokollen
- **Acronis Cloud:** Es sind flexible Abonnements für skalierbaren Cloud-Speicherplatz (in einem sicheren deutschen Datenzentrum von Acronis) verfügbar; Initial Seeding- und Large Scale Recovery-Service sind ebenfalls verfügbar

Acronis Backup basiert auf der Acronis AnyData Engine, die Backup, Bare Metal Recovery und Systemwiederherstellung so kombiniert, dass sich beliebige Daten von beliebigen Orten (egal ob lokal, remote oder in der Cloud) effizient sichern und wiederherstellen lassen. Mit Acronis Backup können Unternehmen ihre Backup- und Disaster-Recovery-Prozesse soweit vereinfachen, dass Daten deutlich schneller und leichter wiederhergestellt werden können.

3 Hauptargumente für Acronis Backup

Umfassende Data Protection

- On-premise
- Remote
- Private Cloud
- Public Cloud
- Mobilgeräte

Schnellstes Backup auf dem Markt

- Installation mit 3 Klicks
- 15 Plattformen, 1 Lösung
- 4 Verschlüsselungs-Standards
- 2x schneller als direkte Mitbewerber
- 500.000 Unternehmen vertrauen auf Acronis

6 eindeutige Unterscheidungs-merkmale

- Eine zentrale Konsole, um alle Daten zu sichern und zu verwalten
- Besonders schnelle RTOs/RPOs dank Acronis Instant Restore™
- Unterstützung von Azure und Amazon (als Backup-Quelle und -Storage)
- Data Protection für alle gängigen Geräte/ Endpunkte
- Unterstützung von VMware und Hyper-V (Hosts, VMs)
- Sie kontrollieren, wo und wie Ihre Daten gespeichert werden

Nützliche Links Acronis Website Acronis Backup

ÜBER ACRONIS

Acronis setzt mit seinen Lösungen für Backup, Disaster Recovery und EFSS (Enterprise File Sync & Share) den Standard in den Bereichen Data Protection und Hybrid Cloud-Integration. Auf Basis seiner AnyData Engine und dank seiner herausragenden Disk Imaging-Technologie bietet Acronis einfache, vollständige und kostengünstige Data Protection-Lösungen für beliebige Daten (Dateien, Applikationen, Betriebssysteme) und in allen IT-Umgebungen (virtuell, physisch, Cloud oder mobil).

Acronis wurde im Jahr 2003 gegründet und schützt die Daten von über 5 Millionen Kunden und 500,000 Unternehmen in über 145 Ländern. Acronis verfügt über mehr als 100 Patente. Seine Produkte wurden von namhaften Magazinen und IT-Profis als bestes Produkt des Jahres ausgezeichnet und decken einen weiten Funktionsbereich ab (inkl. Migration, Klonen und Replikation). Die Lösungen von Acronis sind über ein globales Netzwerk von Service-Providern, Distributoren und Cloud-Resellern weltweit verfügbar.

Weitere Informationen finden Sie unter www.acronis.com.

Acronis

Weitere Informationen finden Sie unter http://www.acronis.com

Copyright © 2002-2016 Acronis International GmbH. Alle Rechte vorbehalten. Acronis und das Acronis Logo sind eingetragene Markenzeichen der Acronis International GmbH, in den Vereinigten Staaten und/oder in anderen Ländern. Alle hier erwähnten oder registrierten Markenzeichen sind Eigentum der jeweiligen Besitzer. Technische Änderungen, Abweichungen der Abbildungen und Irrtümer vorbehalten. 2016-10