# Server-Virtualisierung im regulierten Umfeld

Aktuelle IT-Technologie unterstützt den Betrieb validierungspflichtiger Anwendungen

**Dr. Bernhard Appel** • Roche Diagnostics GmbH, Mannheim, Fachgruppe IT, APV, Mainz
**Dr. Eberhard Klappauf** • COMLINE AG , Bad Homburg, Fachgruppe IT, APV, Mainz

**Korrespondenz:** Dr. Eberhard Klappauf, IT-Consulting GxP, COMLINE Computer + Softwarelösungen AG, Du-Pont-Str. 6, 61352 Bad Homburg; **e-Mail:** eberhard.klappauf@comlineag.de



## Zusammenfassung

Virtualisierung bei Computersystemen, genauer Server-Virtualisierung, steht für das Konzept, zwischen dem Betriebssystem mit Anwendung und der physischen Hardware eine Software als Abstraktionsschicht einzufügen, die „Virtualisierungssoftware" oder Hypervisor. Dadurch werden proprietäre physische Eigenschaften der Hardware gegenüber dem Betriebssystem und den Anwendungen verdeckt. Die wichtigsten technischen Plattformen basieren auf der CPU-Architektur x86 von z. B. Intel oder AMD sowie Windows-Betriebssystemen von Microsoft oder UNIX-Derivaten.
Virtualisierung ist geprägt durch die Implementierung eines oder mehrerer Gast-Betriebssysteme, „virtueller Maschinen" (VMs) auf nur einem physischen Rechner oder einem Rechner-Verbund (mehrere Hosts in einem Cluster).
Die einfache Bereitstellung „virtueller Maschinen" bietet den Vorteil, auch für eine größere Anzahl Anwendungen, eine jeweils eigene VM bereitzustellen. Sie werden dadurch voneinander isoliert, ohne das Risiko gegenseitiger Beeinträchtigung, dies eine ideale Eigenschaft im regulierten Umfeld. Darüber hinaus müssen die erforderlichen Betriebssysteme nicht übereinstimmen. Es leiten sich zwei Besonderheiten ab. Die Erstellung einer virtuellen Maschine mit ihrer Anwendung ist dem Kopiervorgang einer Datei vergleichbar. Dabei unterstützen Tools des Hypervisor-Herstellers die Erzeugung von Vorlagen für VMs. So werden kurzfristig Systeme z. B. für Test oder Qualitätssicherung verfügbar gemacht.
Zum anderen können selbst überalterte Betriebssysteme mit ihren validierungspflichtigen Anwendungen auf hoch performanter aktueller Hardware weiterhin betrieben werden. Außerdem wird durch die schnelle Wiederherstellbarkeit virtueller Maschinen, z. B. in einem zweiten Rechenzentrum, ein Beitrag zu hoher Verfügbarkeit (high availability durch failover) geleistet. Die Technologie der Server-Virtualisierung mit Gastsystemen bietet im regulierten Umfeld besondere Vorteile hinsichtlich Qualifizierung bzw. Validierung und Betrieb Computerisierter Systeme. Dazu wird ein erweitertes Modell für „Computerized Systems" (s. PIC/S PI 011) vorgeschlagen, in dem das „Computerized System" zu einem „virtual Computerized System" wird und das zwischen „physical Computer Systems", pCS, und „virtual Computer Systems", vCS, unterscheidet. Die Virtualisierungsschicht (Hypervisor) lässt sich zwangslos in das erweiterte Modell integrieren.

## Einleitung

Unter dem Begriff Virtualisierung ist in den letzten Jahren eine große Zahl unterschiedlicher Lösungen und Techniken entwickelt worden, die sich von Servern bis in die Bereiche Storage und Netzwerk erstrecken.

Im Folgenden soll jedoch nur die Server-Virtualisierung diskutiert werden. In den letzten 5 bis 6 Jahren wurden mit der breiten Verfügbarkeit der Server-Virtualisierung eine Reihe zusätzlicher Konzepte in die IT-Umgebung eingeführt. Doch die Idee der Virtualisierung und ihrer Realisierung ist nicht so neu wie es scheint. Es waren die Mainframe-Systeme von IBM mit ihren Betriebssystemen, die bereits in den 60-er Jahren die gleichzeitige Bereitstellung mehrerer voneinander unabhängiger Anwendungssysteme durch Hardware-Partitionierung ermöglichten. War

damals der finanzielle Aufwand für den Einsatz virtualisierter Server-Umgebungen für den produktiven Einsatz noch hoch, so hat sich das Blatt inzwischen komplett gewendet. Zum einen wird die Verlässlichkeit der Hypervisor-Software nicht mehr ernsthaft angezweifelt und zum anderen bietet gerade die Server-Virtualisierung die Möglichkeit, im Störungsfall auf eine andere Hardware und sogar an einen anderen Standort (sekundäres Rechenzentrum) auszuweichen und von dort den gestörten IT-Service wieder bereitzustellen. Heute sind größere produktive virtualisierte IT-Umgebungen in Betrieb, in denen Dutzende von Rechner-Clustern (mit z. B. 8 – 12 Host-Rechner) betrieben werden. Auf Ihnen sind jeweils mehrere hundert virtuelle Maschinen (VMs) mit mindestens ebenso vielen Anwendungen installiert. Die große technische Reife dieser Technologie gilt inzwischen als erwiesen.

Aber das Konzept ist bezüglich einsetzbarer Hardware-Plattformen nicht ganz so flexibel, wie Anwender es sich vielleicht wünschen. Die für eine Virtualisierungslösung von ihrem Anbieter zugelassene Hardware ist vom Anwender gegen die jeweilige Kompatibilitätsliste abzugleichen, nur dann ist der Support durch den Hersteller auch in der nächsten Zukunft zu erwarten. Die Kompatibilität ist für die Computer-Hardware ebenso wie für Schnittstellen zu Massenspeichern und zum Netzwerk einzuhalten. Dies gilt jedenfalls für die wichtigsten Marktteilnehmer wie VMware mit ESX bzw. ESXi, Microsoft mit Hyper-V und Citrix mit XEN-Server.

Daneben gibt es Nischenlösungen, die mit ihrer Virtualisierungssoftware z. B. auf dem „Standard-Betriebssystem“ (Wirtsbetriebssystem) des physischen Rechners (Wirtssystem oder Host) aufsetzen oder direkt auf der Rechner-Hardware implementiert werden.

Für die weitere Diskussion wird für die Server-Virtualisierung auch die gängige Bezeichnung Virtuelle Infrastruktur oder kurz VI benutzt werden.

## Virtualisierungsarten

In diesem Abschnitt wird das Thema Virtualisierung auf den Bereich der Server-Virtualisierung für regulierte Umgebungen begrenzt. Hierzu werden zwei wichtige Varianten zum Thema Virtualisierung kurz charakterisiert, um dem Leser die Unterscheidung der verschiedenen Lösungen zu ermöglichen.

### Anwendungsvirtualisierung

Bei der Anwendungsvirtualisierung werden Anwendungen nicht mehr auf dem Endgerät des Anwenders installiert und dort ausgeführt. Vielmehr wird die Anwendung zentral auf einem Server installiert und für jeden berechtigten Anwender wird eine private Kopie dieser Anwendung in dem Augenblick erstellt und für ihn gestartet, in dem er diese Anwendung von seinem Endgerät aus anfordert.

Die zentrale (statt lokale) Bereitstellung optimiert vor allem Pflege (Software-Verteilung) und Überwachung der Anwendung. Wichtige Anbieter von Tools zur Anwendungsvirtualisierung sind die Firmen Microsoft und CITRIX.

### Desktopvirtualisierung

Die Desktopvirtualisierung (Client-Virtualisierung) beschreibt, über die Variante Anwendungsvirtualisierung hinaus, eine Virtualisierung, in der das Endgerät für jegliche Funktionen und Anwendungen nur noch Ein- und Ausgabegerät ist. Im Rechenzentrum auf einer entsprechenden Rechner-Plattform wird für jedes Endgerät im Moment der Anmeldung ein eigener virtueller Desktop erstellt. Die vom Anwender aufgerufenen Anwendungen werden ebenso im Rechenzentrum bereitgestellt und ausgeführt.

Zwischen den oben genannten wichtigsten Virtualisierungsformen haben sich weitere Mischformen entwickelt, die eine einfache scharfe Abgrenzung zunehmend erschweren.

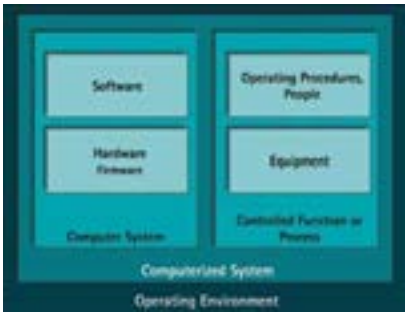


*Abb. 1: Computerized System auf physischer Plattform (nach PIC/S PI011).*

## Struktur der Server-Virtualisierung

### Computerized Systems

Die wichtigsten technischen Plattformen der Server-Virtualisierung basieren auf der CPU-Architektur x86 bzw. x64 von z. B. Intel oder AMD sowie Windows-Betriebssystemen von Microsoft.

Die folgende Abb. 1 greift das Grundmodell des Operating Environment nach PIC/S-PI011 auf, mit dem Computerized System und darin dem Computer System. Dieses Modell orientiert sich an einem physischen Rechner als „Computer System“.

Dieses Modell lässt sich ohne Bruch für die Virtuelle Infrastruktur weiterentwickeln, indem unterschieden wird zwischen einem „physischen Computer System“ (pCS), und einem „virtuellen Computer System“ (vCS). Das pCS kann durch einen oder mehrere physische Rechner (Pool oder Cluster) realisiert werden. Das vCS, oder auch Gastsystem, besteht in der Regel aus der „virtuellen Maschine“ mit dem auf ihr installierten Betriebssystem und einer oder auch mehrerer darauf implementierter Anwendungen.

Die Details unter „Controlled Function or Process“ im obigen Modell bleiben unverändert, sie sind dem jeweiligen vCS zugeordnet (wie im herkömmlichen Modell zuvor einem „Computer System“ (Hardware)). Die Implementierung in einer Virtuellen Infrastruktur ist für sie somit völlig transparent. vCS und „Con-




TechnoPharm 2, Nr. 5, 333–342 (2012)

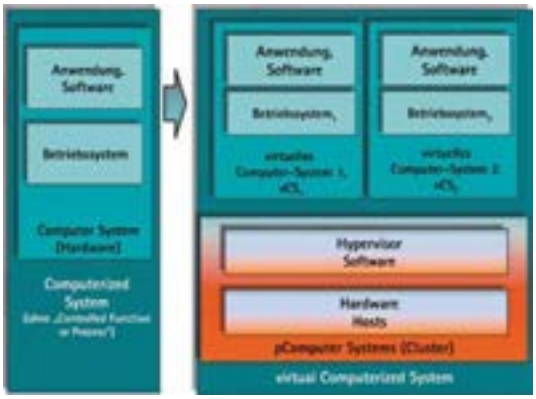


*Abb. 2: Modell-Projektion von physischer in virtuelle Umgebung.*

trolled Function or Process“ bilden das „virtual Computerized System“.

Die Funktionseinheit, die die Virtualisierung leistet (Hypervisor), lässt sich als Element im „virtual Computerized System“ zusätzlich zu „Computer System“ und „Controlled Function or Process“ einführen.

In der folgenden Abb. 2 ist die Projektion des Modells in die virtualisierte Umgebung dargestellt. In der virtuellen Umgebung sind bereits zwei Anwendungen auf dem jeweils eigenen virtuellen Computer-System vCS dargestellt, das „virtuelle Computer-System“ zur Vereinfachung aber ohne „Controlled Function or Process“.

Die nächste Abb. 3 interpretiert das eben entworfene Modell des vCS für zwei typische Produkte der Server-Virtualisierung. Sie dienen als Grundlage für die weitere Diskussion.

## Eigenschaften von VI gegenüber physischen Servern

Das Format, in dem Gastsysteme, vCS, in einer VI bereitgestellt werden, ist eine Datendatei. In ihr ist die virtuelle Maschine mit den darauf installierten Anwendungen vollständig abgebildet. Der Hypervisor benötigt keine weiteren Daten, um eine VM mit ihren Anwendungen zu starten und zu betreiben und kann für die einzelne VM dynamisch die Rechner-Ressourcen (CPUs, Hauptspeicher, Input/Output-Bandbreiten) zuteilen. Daraus folgern einige wichtige Eigenschaften:

- Um einen Klone (identische Kopie) einer virtuellen Maschine zu erstellen, muss lediglich eine Kopie der Datei dieser VM erstellt werden. Die Administrationsumgebung des Hypervisor entscheidet, in welcher Form eine neue System-Identifikation vergeben wird und ob und unter welchen Randbedingungen diese zweite (identische) Maschine auf dem Hypervisor (u. U. gleichzeitig mit der ersten) gestartet werden kann. Diese Eigenschaften zur Erzeugung eines Klons erlaubt die einfache schnelle Erzeugung eines jedenfalls aus Anwendungssicht identischen Systems z. B. eine Kopie des Produktionssystems für Zwecke der Entwicklung, zum Testen oder für die Qualitätssicherung.
- Ein zweiter Vorteil ergibt sich für die Verfügbarkeit bei einem Ausfall eines Wirtssystems oder der kompletten primären Produktionsumgebung. Das Migrieren einer VM mit ihren Anwendungen innerhalb des Clusters bzw. in eine zweite noch verfügbare Produktionsumgebung ist, je nach Lösung, sogar unterbrechungsfrei und ohne Datenverlust möglich. Diese Eigenschaft erlaubt in Clustern mehrerer Hosts den Austausch oder die Wartung einzelner Hardware- oder Software-Komponenten der VI ohne Beeinträchtigung der laufenden VMs mit ihren Anwendungen. Gegenüber den Anwendern und Prozessen kann so eine sehr hohe Verfügbarkeit zugesagt werden.
- Ein dritter wichtiger Vorteil ergibt sich für die Lastanpassung (workload balancing) und die Skalierbarkeit (scalability) der bereitgestellten Rechner-Leistung für die einzelne VM. Die Skalierbarkeit erstreckt sich auf die zugewiesene Rechenleistung (CPU-Anzahl und Taktrate), den Hauptspeicher und die Input- und Output-Bandbreiten zu Massenspeicher und Netzwerk. Diese Parameter können von den zugehörigen Tools in vordefinierten Grenzen für den aktuellen Bedarf der VM automatisch optimiert werden. Selbstverständlich können diese Parameter bei Ausdehnung der System-Nutzung auch dauerhaft nach oben verändert werden. Gegebenenfalls muss die Rechnerkapazität durch zusätzliche Hosts im Cluster erweitert werden.
- Wie zuvor erwähnt, kann durch die Installation jeder Anwendung auf ihrer eigenen VM in virtueller Umgebung schon auf Betriebssystemebene wirkungsvoll für die Isolation der Anwendungen gesorgt werden (Prinzip: „jede Anwendung auf eigenem Rechner“).

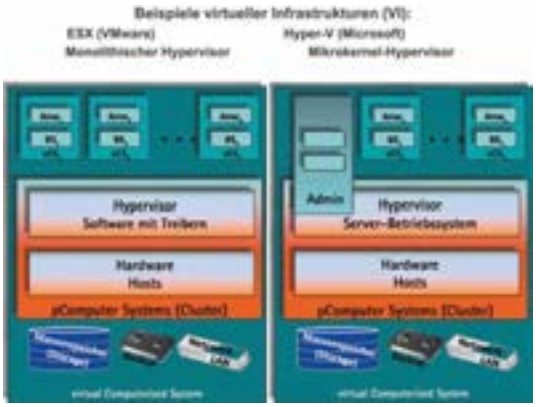


*Abb. 3: Strukturen einer VI mit pCS und vCS am Beispiel zweier wichtiger Marktteilnehmer.*

## Host und Cluster der Server-Virtualisierung

Für das regulierte Umfeld sollten die technischen Strukturen so entworfen werden, dass sich die Qualifizierungs- und Validierungsaufwendungen und der regulierte IT-Betrieb optimieren lassen. Dies gelingt, indem

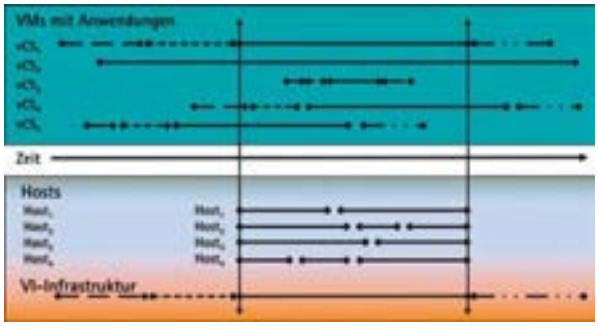


*Abb. 4: Entkopplung der Lebenszyklen der VI mit Hosts und VMs mit Betriebssystemen und Anwendungen.*

mehrere Hosts gleicher Konfiguration zu einem Cluster zusammengefasst werden. Dazu ist denkbar die Anwendungen vergleichbarer Kritikalität auf einem Cluster zu konsolidieren, sofern Risikobewertung und technische Ressource dies erlauben. In der Betriebsphase müssen dann Changes für das Cluster für nur eine gemeinsame Risikostufe durchgeführt werden.

Die Design-Varianten einer Server-Virtualisierung bieten einige Grundformen:

- Mehrere VMs auf einem physischen Host
- Viele VMs auf mehreren physischen Hosts (Cluster)
- Mehrere Cluster (mit in der Regel mehreren Hosts)
- Hochverfügbarkeit/Failover-Funktion für VMs auf einem oder mehreren Clustern (verteilt auf 1 oder 2 Standorte): Restart bei Störung oder HW-Ausfall eines Hosts; Migration von einem Host zu einem anderen mit Service-Unterbrechung für Wartungszwecke
- Hochverfügbarkeit/Failover-Funktion für VMs auf einem oder mehreren Clustern (verteilt auf 1 oder 2 Standorte): keine Service-Unterbrechung

In der Regel werden nur die beiden letztgenannten Varianten implementiert, gleichzeitig mit hochverfügbaren Storage-Ressourcen für die Datenhaltung.

### Entkopplung der Lebenszyklen von Hardware und Software

Auf einem Hypervisor können verschiedene, auch ältere Betriebssysteme – mit ihren Applikationen – implementiert werden. Damit lassen sich die Lebenszyklen von sich schnell weiter entwickelnder Computer-Hardware und sehr viel langsamer sich ändernden Betriebssystem mit Applikation stark voneinander entkoppeln (Abb. 4). Die Qualifizierung der IT-Infrastruktur und Validierung der Applikation (EU-GMP Vol.4., Annex 11 neu) sind so weitgehend unabhängig durchzuführen. Im regulierten Umfeld können damit die Updatezyklen validierungspflichtiger Anwendungen an den eigenen Bedarf angepasst werden.

Diese Flexibilität in der verlängerten Nutzung des unterliegenden Betriebssystems erlaubt die verlängerte Nutzbarkeit von Anwendungen. Dies reduziert oder vermeidet Aufwendung für Qualifizierung und Validierung aus Gründen eines IT-Technologiewechsels.

Aus IT-Sicht baut sich damit aber das Risiko auf, dass die Notwendigkeit von Updates für das Betriebssystem oder ein Update oder sogar die Ablösung der Anwendung wegen Überalterung den nutzenden Fachbereichen schwerer zu vermitteln ist. Die Risiken fehlenden Supports steigen kontinuierlich an und die Verfügbarkeitszusage für die betreffende Anwendung muss reduziert werden. Gleichzeitig hat das IT-Service Management natürlich seine eigenen Kenntnisse für dieses veraltete Betriebssystem weiter aufrechtzuerhalten.

Ein Endpunkt ist endgültig erreicht, wenn auch durch den Hersteller der Hypervisor-Lösung das veralte Betriebssystem nicht mehr als Gastsystem unterstützt wird. Beispielhaft kann hier das Betriebssystem Windows NT als Legacy-System angeführt werden. Zu diesem Betriebssystem kompatible Hardware kann nicht mehr beschafft werden, ebenso fehlt jeglicher Support. Aber auf Hypervisor-Lösungen wird es aktuell noch unterstützt.

## Auswirkungen der Server-Virtualisierung

Im Folgenden sollen einige wichtige technische und regulatorische Auswirkungen der virtualisierten Umgebung gegenüber physischen Systemen diskutiert werden.

### Technische Ressourcen

Die Server-Virtualisierung wird i. d. R. in Form von auch mehreren Clustern mit jeweils mehreren Hosts implementiert. Neben der internen Vernetzung der Hosts im eigenen Cluster ist die Verbindung in das Netzwerk des Unternehmens zu realisieren. Gleiches gilt für die Anbindung an die Massenspeicher für die Datenhaltung.

Auf technischer Ebene sind regelmäßig zusätzliche logische und physische Netzwerke erforderlich für Funktionen wie Host-Management, VM-Management, Host-Kommunikation und Netzwerke für einzelne oder Gruppen von Anwendungen auf ihren VMs. Nur in Einzelfällen wird das „externe“ Netzwerk nicht benötigt, weil die kommunizierenden Anwendungen so implementiert sind, dass sie über den Hauptspeicher kommunizieren können. Die Flexibilität zur Migration von einem Host im Cluster zu einem anderen nimmt damit natürlich ab, sofern diese Kopplung bei Bedarf nicht auch aufgelöst werden kann.

### Lizenzen

Es ist für die virtualisierte Umgebung zu prüfen, wie das Lizenz-Modell des jeweiligen Software-Herstellers die Zahl der Hosts im Cluster und ihrer ev. große Anzahl CPUs sowie die Anzahl der VMs interpretiert. Dies ist




TechnoPharm 2, Nr. 5, 333–342 (2012)

für die Betriebssysteme der VMs ebenso festzustellen wie für die Anwendungen. Extremfälle verlangen die Lizensierung für alle Hosts und CPUs eines Clusters, obwohl die lizensierte Anwendungssoftware zu einem Zeitpunkt auf nur einem Host des Clusters in nur einer VM lauffähig ist.

### Backup und Restore / Recovery

Das Backup für computerisierte Systeme auf virtueller Plattform ist vielfältiger und komplexer als das für physische Systeme, es werden andere Verfahren und Tools benötigt, Backup-Verfahren für physische Maschinen sind ungeeignet. Es ist beim Backup von VMs zu beachten, dass sie in der Regel gleichzeitig durch Backup-Verfahren erfasst und gesichert werden und die technischen Ressourcen CPU, Hauptspeicher und Input/Output für diese Belastung ausgelegt sein müssen.

### Konvertierung zwischen physischen und virtuellen Plattformen

Konvertierungen von Quell- zu Zielumgebungen werden nur außerhalb der Projektphasen benötigt. Gegenstand von Konvertierungen zwischen den beiden Plattform-Arten (seltener ebenfalls als Migration bezeichnet) sind auf der physischen Plattform das Betriebssystem mit Anwendungen und auf der virtuellen Plattform die VM mit Betriebssystem und Anwendungen.

Die Einführung und Nutzung einer virtuellen Plattform ist nicht irreversibel, da technologisch alle drei Konvertierungsarten unterstützt werden:

- Physisch nach virtuell (P2V),
- Virtuell nach virtuell (V2V) zwischen verschiedenen ausgewählten Hypervisor-Produkten,
- Virtuell nach physisch (V2P).

Für die Konvertierung auf physischer Plattform betriebener CS auf die virtuelle Plattform sind natürlich erhöhte Aufwendungen erforderlich. Sie entsprechen etwa denjenigen, die bei umfangreicherem Austausch der physischen Plattform entstehen würden.

Die Rückmigration von virtuell nach physisch setzt voraus, dass die zukünftige physische Hardware und Betriebssystem-Software noch verfügbar sind und unterstützt werden; gerade sie waren in der Vergangenheit vielleicht der Grund für den Umzug auf eine virtuelle Plattform.

Soll eine validierte Anwendung nach einer der drei Varianten konvertiert werden, ist natürlich ein Change aufzusetzen, der belegt, dass die Konvertierung von Anwendung und Daten korrekt und vollständig erfolgt ist.

Tools zu Konvertierungen werden sowohl von Herstellern der Hypervisor wie von Drittanbietern bereitgehalten. Es ist auf die Fähigkeit des Tools zu achten, dass Quell- und Ziel-Umgebung unterstützt werden.

### Security der virtuellen Plattform

Die Security im Folgenden bezieht sich auf die Abwehr des unberechtigten Zugriffs (von innen oder außen) von Personen und Schadsoftware auf Funktionen und Daten. Die Security-Anforderungen im virtualisierten Umfeld erstrecken sich ergänzend zu denen einer physischen Plattform auf weitere Komponenten. Denn neben dem Betriebssystem, installiert auf der VM, sind die Zugriffe auf die VM, den Hypervisor und die Host-Ebene zu begrenzen oder ganz zu unterbinden. Dies sollte auch eine wohl überlegte Segmentierung des Netzwerks einschließen. Denn Angriffe auf diese zentralen Komponenten gefährden nicht nur die die Sicherheitslücke enthaltende Komponente, sondern eröffnet womöglich von dort auch noch eine andere zu korrumpieren wie z. B. den Übergriff von einer VM auf das eigene Betriebssystem und die darauf implementierte Anwendung und ihre Daten oder sogar auf eine andere VM. Neben durch Personen unmittelbar geführte Angriffe sind auch solche durch Schadsoftware zu befürchten. Eine Maßnahme zum Schutz der virtuellen Plattform sind das „Härten" sowohl der physischen Rechner (Hosts), ggf. einschließlich ihres Betriebssystems, als auch des Hypervisor. Gleiches gilt selbstverständlich für das Gastbetriebssystem.

Gegen Security-Risiken im administrativen Bereich virtualisierter Umgebungen sind also ergänzende technische und organisatorische Vorkehrungen zu treffen und ein geeignetes Security-Monitoring zu etablieren.

### Risiken einer Hypervisor-Lösung

Die zusätzlichen Risiken einer Virtualisierungslösung lassen sich in zwei Bereiche gliedern, die Architekturrisiken, bedingt durch die eingesetzte zentralistische Hypervisor-Architektur, und diejenigen Risiken, die sich aus den zusätzlichen Funktionen des Hypervisor mit Einfluss auf die VMs und Anwendungen ergeben.

Die Architekturrisiken ergeben sich als Risiko-Clusterung, da alle VMs einer Hypervisor-Lösung von der Funktion des Hypervisor abhängen. Ergibt sich bei ihm ein Funktionsausfall, sind alle auf ihm implementierten Anwendungen betroffen, ggf. auch diejenigen am zweiten Standort.

Der andere Risikobereich resultiert aus dem Einfluss der eingesetzten Tools, die den Betrieb der VMs mit ihren Anwendungen unterstützen. Auch hier kann sich eine Fehlfunktion auf alle virtualisierten Anwendungen erstrecken.

Die Server-Virtualisierung birgt diesbezüglich aber keine zusätzlich Risiken im Vergleich zu vielen anderen zentralen Architekturen wie Storage-Umgebungen.

## Einschränkungen durch Virtualisierung

Virtualisierung basiert auf der Realisierung einer begrenzten Zahl von Standard-Funktionen des Gast-Betriebssystems durch den Hypervisor. So erklären sich mehrere Einschränkungen dieser Technologie.

Zum einen wird die Performance der physischen Maschinen nicht zu 100 % für die VMs verfügbar, die dynamische Umschaltung und Zuwei-

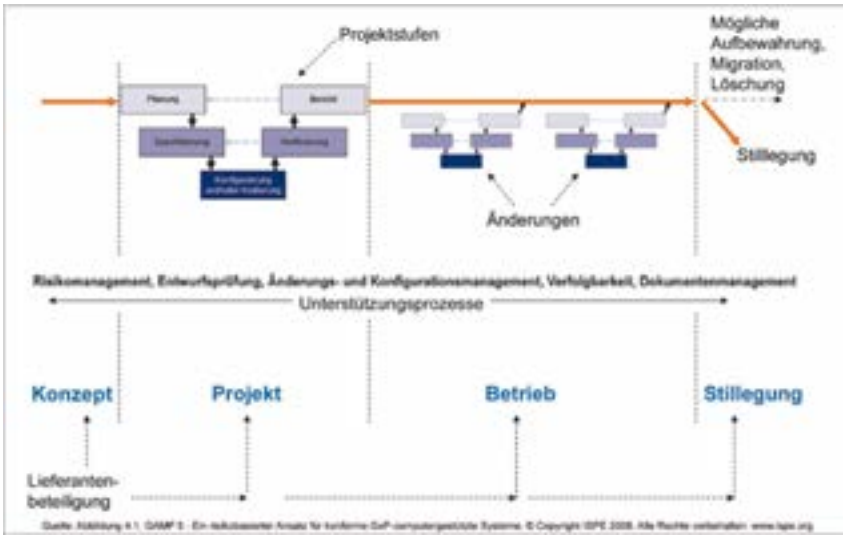


*Abb. 5: Quelle: GAMP® 5, Abb. 4.1: Projektstufen und Unterstützungsprozesse innerhalb des Lebenszyklus.*

sung der Ressourcen zu den VMs benötigt einen wenn auch kleinen Teil der insgesamt verfügbaren Hardware-Ressourcen. Gleiches gilt für den Durchsatz zum Storage und zu den Netzwerken.

Zum zweiten sind die führenden Hypervisor für nur eine kleine Anzahl CPU-Architekturen (vor allem x86-/x64-kompatible) und eine begrenzte Anzahl Hardware-Anbieter verfügbar.

Drittens ist die Integration z. B. spezieller Hardware-Interfaces, selbst für Standard-Funktionen, häufig nicht unterstützt, die Interfaces können nicht eingesetzt werden.

Dagegen steigt die Zahl der auf VMs zugelassenen Betriebssysteme. Auch die Grenzen bzgl. der Anzahl je VM konfigurierbarer (und real nutzbarer) CPUs verschieben sich mit jeder neuen Hypervisor-Generation nach oben und stellen nur noch selten eine echte Einschränkung dar. Gleiches gilt für die Hauptspeichergröße und die gleichzeitig je Host zugelassene Anzahl VMs.

Zunehmend unkritischer wird auch die ggf. nicht vorliegende (technische) Freigabe einer Anwendung für die Nutzung auf einer virtuellen Plattform. Die Nutzung der Anwendung auf einer virtuellen Umgehung trotz der fehlenden Betriebsfreigabe durch deren Hersteller ist im Einzelfall regulatorisch durch eine Risiko-Bewertung zu rechtfertigen. Aber die Lizensierung und der Support durch den Hersteller in Störungsfällen werfen eventuell unlösbare Fragen auf.

## SOPs gültig für die Server-Virtualisierung

Sollen validierungspflichtige Anwendungen in einer virtualisierten Umgebung betrieben werden, so bestehen Qualifizierungs- und Validierungspflicht nicht nur bzgl. der VM sondern auch bzgl. der sie tragenden virtuellen Server-Plattform. Bevor über ihre Qualifizierung und Validierung diskutiert werden kann, sind die zugehörigen Policies und SOPs auf Gültigkeit auch für diese Technologie zu überprüfen (s. Diskussion des eingeführten Modells der pCS und vCS).

Abweichungen und Regelungsbedarf zu physisch gestützten IT-Umgebungen ergeben sich hier vor allem durch die zusätzlichen Technologie-Komponenten und die Entkopplung der Lebenszyklen (s. Abb. 2 und 4). In diesem Zusammenhang kommt zu Hilfe, dass der EU-GMP Annex 11 eine Trennung zwischen IT-Infrastruktur und IT-Anwendungen feststellt.

## SOPs für virtuelle Infrastruktur anpassen

Das Projekt Qualifizierung der VI-Struktur (und auch der spätere IT-Betrieb) kann in Anlehnung an das Lebenszyklus-Modell in GAMP® 5 (s. Abb. 5) durchgeführt werden, vorausgesetzt, die SOPs berücksichtigen Eigenheiten „virtueller Computerisierter Systeme“ bzgl. der Anforderungen von EU-GMP Annex 11 und 21 CFR Part 11.

Im Unterschied zu physischen Plattformen, die im Wesentlichen aus Rechner-Hardware, dem darauf installierten Betriebssystem und implementierter Anwendung bestehen, sind in virtualisierter Umgebung zwei weitere Komponenten enthalten, die Hypervisor-Software und die virtuelle Maschine (virtuelle Hardware mit Betriebssystem). Die Einordnung beider als GAMP-Software-Kategorie 1 wird zu verteidigen sein.

Ebenfalls spezifisch für die virtuelle Umgebung sind die Tools für die Administration der virtuellen Infrastruktur, z. B. die Verwaltung von Betriebsmodi der Hosts und VMs, der Ressourcen einschließlich Migration zwischen Hosts und Berechtigungen. Die Einordnung dieser Tools in die Software-Kategorie 1 wird auch hier die Regel sein. Die umfangreichen Einstellmöglichkeiten dieser Tools und deren Eingriff in den Betrieb von Hypervisor, VM, Betriebssystem und Anwendungen erfordern jedoch ein differenzierteres Vorgehen. Daher sind entsprechende SOPs erforderlich, die mindestens eine Verifizierung für diese Tools spezifizieren und Administration und Betrieb dieser Tools regeln. Dazu können auch Regelungen für die automatische Protokollierung der administrativen Tätigkeiten hinzukommen. Neu erstellt werden müssen Vorgaben für Changes der Host-Hardware, des Hypervisor und der VMs. Denn diese Komponenten sind die Grundlage für alle Anwendungen auf der virtuellen Server-Infrastruktur, dies sollte eine Risiko-Bewertung berücksichtigen.




TechnoPharm 2, Nr. 5, 333–342 (2012)

Changes der Betriebssysteme auf den VMs sind wieder vergleichbar denjenigen in physischen Umgebungen. Gleiches gilt für Changes der Anwendungen.

Eine weitere Herausforderung stellt die Außerbetriebnahme der virtuellen Infrastruktur oder die Migration auf eine neue Plattform dar, jedenfalls sofern nicht nur die Host-Rechner sukzessive gegen funktionsidentische ausgetauscht werden. Denn vor der Stilllegung oder Migration müssen alle VMs mit ihren Anwendungen und Daten für die neue Plattform konvertiert (V2V), dorthin umgezogen und ihr validierter Zustand festgestellt worden sein.

## Verifizierung der virtuellen Infrastruktur

In Anlehnung an den GAMP® 5 Lebenszyklus sollen im Folgenden die Konzept- und vor allem die Projekt-Phase diskutiert werden.

Die virtuelle IT-Infrastruktur ist in Qualifizierung und Validierung den Ansprüchen zu unterwerfen, die für die darin betriebenen validierungspflichtigen Anwendungen bestehen, und müssen entsprechend der Risiken und der Kritikalität der eingesetzten Anwendungen für Produktqualität, Patientensicherheit und Datenintegrität geführt werden.

### User Requirements Specification (URS)

Vor Erstellung der URS für eine virtuelle Server-Infrastruktur, aber spätestens in ihr, sollten die im Folgenden diskutierten Fragen und Zusammenhänge geklärt werden.

In der URS für die „Virtuelle Infrastruktur" sollte entschieden und festgehalten werden, ob das Design für eine bestimmte Anwendungslandschaft mit identifizierten Anwendungen erstellt wird, oder ob es ein „Standard-Design" für sowohl derzeit vorhandene wie zukünftig zu implementierende Anwendungen sein soll.

Zusätzlich sollte festgelegt werden, ob neben validierungspflichtigen Anwendungen nicht validierte Anwendungen zwar in verschiedenen VMs, aber auf dem gleichen Host bzw. Cluster betrieben werden dürfen. Dies hat Auswirkungen auf die Risiko-Analyse der virtuellen Infrastruktur, sowohl für die Qualifizierung wie für den späteren IT-Betrieb.

Zentraler Ausgangspunkt ist die Auswahl der Hypervisor-Plattform und ihr Design, bestehend aus der Rechner-Architektur und der Hypervisor-Lösung selbst. Diese beiden entscheiden maßgeblich über die Vielfalt der auf den VMs einsetzbaren Betriebssysteme und eine Reihe technischer Eigenschaften bei Konfiguration und „Sizing" der VMs (Anzahl CPUs, Größe des Hauptspeichers, „live"-Migration von VMs u. a.). Das Design der Server-Infrastruktur für die Server-Virtualisierung muss die innere Struktur des Clusters beschreiben (Typ und Anzahl von Hosts), deren Vernetzung untereinander, die Anbindung an die Massenspeicher-Systeme und das Netzwerk sowie die Technologie für die Datensicherung. Neben diesen essentiellen Grundlagen sind Auswahl und Festlegungen der Tools zu Monitoring und Administration zutreffen. Schließlich wird noch ein Notfall-Konzept mit Maßnahmen zur Beherrschung von Ausfall-Szenarien erforderlich. Es wird Informationen enthalten wie Anzahl Hosts im Cluster, Anzahl und Standorte der Cluster (Notfall-Rechenzentrum) und hochverfügbare und redundante Anbindungen an Massenspeicher und Netzwerke, und Verfahren der Wiederherstellung der Infrastruktur, der Daten und der Anwendungen in einem validen Zustand.

Parallel dazu sollte eine Erhebung durchgeführt werden, für welche Anwendungen aus technischer Sicht eine Virtualisierung zweckmäßig ist. Gegen sie können extreme Anforderungen sprechen in den Bereichen CPU-Last, Hauptspeicher-Ausbau, Daten-Austausch mit dem Massenspeicher (I/O-Last) oder Netzwerk-Bandbreite im Local Area Network (LAN). Anwendungsfälle mit diesen Anforderungen können z. B. Datenbanken, Anwendungen, die den Datenaustausch zwischen anderen Anwendungen gewährleisten oder Systeme mit extremen Anforderungen an die Antwortzeiten (Realtime-Anforderungen) sein.

Ist eine Anwendung bereits produktiv in Betrieb, so ist auch zu klären, ob technische Verfahren für die Konvertierung von der physischen auf die virtuelle Plattform verfügbar sind und mit welchen Risiken diese Verfahren verbunden sind. Andernfalls müsste eine neue Implementierung mit entsprechendem Validierungsaufwand durchgeführt werden.

### QbD in der Server-Virtualisierung

Die Umsetzung von Quality by Design (QbD) spiegelt sich im Bereich der Server-Virtualisierung vor allem in einer einfachen und möglichst standardisierten Technologie-Struktur und weitgehend automatisierten Betriebsformen wieder. So sollten alle Hosts eines Clusters technisch identisch ausgestattet und konfiguriert sein, sowie nach Anzahl und Typ die gleichen CPUs enthalten. Ein späterer Ausbau kann durch Hinzufügen weiterer Hosts in das Cluster ohne Nachteil für das Design-Konzept erfolgen.

Erstreckt sich das Cluster über zwei Brandabschnitte (Mindest-Anforderung) oder Standorte, sollte eine Gleichverteilung der Ressourcen (Anzahl Hosts) angestrebt werden. Die Anbindungen an Massenspeicher und Netzwerke sind mehrfach redundant auszulegen und die Leitungswege soweit wie möglich unabhängig voneinander zu wählen.

Der ausgewählte Hypervisor sollte die aktuell (noch) in Nutzung befindlichen Betriebssysteme unterstützen und von einem Anbieter stammen, der voraussichtlich auch längerfristig im Markt etabliert sein wird und längerfristig den Support und die Weiterentwicklung seines Hypervisor unterstützen wird. Selbstverständlich sollte der Hypervisor die momentan genutzten und weitere marktgängi-

gen Storage-Lösungen unterstützen. Dieser Punkt ist besonders relevant im Kontext von Backup und Restore bzw. Recovery und der Forderung eines unterbrechungsfreien Betriebs von Anwendungen bei der Migration von einem Host auf einen anderen oder dem Weiterbetrieb der Anwendungen bei einer Störung. Die Security-Einstellungen der Lösung sollten den Zugriff auf die Host-Ebene, den Hypervisor und die VM so weit wie möglich einschränken. Das Design der Netzwerkanbindungen sollten unsichere Netzwerksegmente soweit wie möglich abgrenzen.

Die für die Hypervisor-Lösung verfügbaren Tools für Planung und Betrieb, auch von Drittanbietern, sollten folgende Anforderungen abdecken:

- „Sizing" der virtuellen Plattform (Grundlage: Mengengerüste der physikalischen Systeme).
- Monitoring, Betrieb und Administration des Cluster mit seinen Hosts.
- Monitoring, Betrieb und Administration der VMs mit Betriebssystemen und Anwendungen.
- Security- und Ressourcen-Management für Cluster, Hosts und VMs.
- Konvertierungen zwischen verschiedenen physikalischen und virtuellen Plattformen
- Backup- und Restore-/Recovery-Aufgaben

## Qualifizierung der virtuellen Plattform

Für das regulierte Umfeld ergibt sich im Rahmen der Qualifizierung anfänglich ein Mehraufwand, denn es ist zunächst die virtuelle Plattform mit ihren Funktionen zu qualifizieren. Durch gleich konfigurierte Hosts im Cluster ist die Qualifizierung der Hardware zu optimieren, zusätzlich ist aber das Cluster selbst zu qualifizieren.

Hinzu kommt der Aufwand für die Verifikation der Hypervisor-Plattform und der Administration-Tools für die VI. Schließlich sind die VMs der Qualifizierung zu unterwerfen. Allerdings ergibt sich hier später der Vorteil, dass eine qualifizierte „Master-VM" als Vorlage für mehrere Kopien dienen kann, mit nur noch minimalem Qualifizierungsaufwand.

Die Qualifizierung der IT-Infrastruktur, bestehend aus dem Cluster mit den Host-Rechnern und ihren Anbindungen an Storage und Netzwerke sowie Installation eines Betriebssystems, entspricht weitgehend der Qualifizierung hochverfügbarer physischer Server in Cluster-Konfiguration. In der Risikobewertung muss allerdings berücksichtigt werden, welche Kritikalität die später in der virtuellen Umgebung zu betreibenden Anwendungen haben werden. Die kritischste Anwendung setzt bereits hier den Maßstab.

## Verifizierung der Hypervisor-Implementierung

Die Verifizierung der Hypervisor-Implementierung kann mehrere Verläufe nehmen. So kann sich hinter ihr die etwas aufwändigere Überprüfung der funktionalen Korrektheit einer Software-Installation einschließlich der Konfiguration ergeben (Bsp.: VMware ESX oder ESXi), oder die einfachere Überprüfung der Korrektheit der Hypervisor-Funktionen nach der minimalen Umkonfiguration des in der Qualifizierung des Server-Clusters bereits installierten Server-Betriebssystems (Bsp.: Microsoft Windows 2008 R2).

## Verifizierung der Administration-Tools

Unter Administrations-Tools sollen im Folgenden Software-Hilfsmittel verstanden werden, die für die Implementierung und den Betrieb vom Host bis zur Anwendung eingesetzt werden. Sie können vom Hersteller der Hypervisor-Lösung wie von Drittanbietern stammen.

Verfügbar und dringend zu empfehlen sind sie u. a. für diese Aufgaben:

- Unterstützung der Konvertierung von der physischen in die virtuelle Umgebung.
- Monitoring der Nutzung der Host-Ressourcen im Cluster und der Performance der VMs.
- Ressourcen-Management und Migrationen von VMs innerhalb des Clusters auf Hosts mit verfügbaren Ressourcen bzw. auf störungsfreie Hosts.
- Administration der Hosts wie der VMs einschließlich Protokollierung der Tätigkeiten.
- Verwaltung und Kontrolle von Zugriffsrechten auf die Ebenen Host, Hypervisor und VMs einschließlich Protokollierung der Tätigkeiten; die Verwaltung der Betriebssystem-Ebene erfolgt häufig nicht über diese Tools sondern in separaten Anwendungen.
- Patch- und Update-Management für den Hypervisor und die VMs, teilweise auch für die auf den VMs installierten Betriebssysteme.
- Backup- und Restore-/Recovery-Funktionen für Hosts und VMs mit ihren Anwendungen und die zugehörigen Datenbestände.

Da die genannten Aufgaben zumindest teilweise in den Betrieb der Anwendungen eingreifen, sind sie regulatorisch relevant. Für diese Aufgaben werden in der Regel eine Spezifikation und deren Verifizierung erforderlich sein, im Umfang ausgerichtet an den Ergebnissen der Risiko-Bewertung.

Ein Ausweg, um nicht die ganze Vielfalt aller Tools bzw. aller Funktionen verifizieren zu müssen, kann über die Auswahl derjenigen Tools und ihrer Funktionen gefunden werden, die regelmäßig im IT-Betrieb genutzt werden bzw. automatisch ablaufen. Für diese sollten SOPs vorhanden sein. Alle anderen Funktionen werden nur anlassbezogen genutzt und damit in Verfahren wie CAPA, Abweichungsmanagement und Changes eingesetzt werden, in denen der Nachweis der korrekten Funktion individuell erbracht wird.

## Qualifizierung der VMs

Virtuelle Maschinen bestehen ausschließlich aus Software-Komponenten. Sie stellen für das Betriebssys-




TechnoPharm 2, Nr. 5, 333–342 (2012)

tem die Verbindung zur Hypervisor-Plattform und die Standard-Treiber bereit.

Häufig wird unter diesem Begriff zusätzlich das jeweilige Betriebssystem eingeschlossen. Letztere Sicht soll im Folgenden Grundlage sein, da so die Parallele zur physischen Plattform gezogen werden kann.

Die Qualifizierung einer virtuellen Maschine mit Betriebssystem kann der GAMP Software-Kategorie 1 zugeordnet werden. So ist eine vergleichsweise einfache Verifizierung entsprechend der Spezifikation der zu implementierenden Anwendung durch Prüfungen durchzuführen. Die Qualifizierung einer virtuellen Maschine unterscheidet sich insoweit nur geringfügig von der des Betriebssystems einer physischen Maschine. Erleichtert wird die Bereitstellung durch den Rückgriff auf eine bereits als Typ qualifizierte VM (Master-VM), unter besonderer Beachtung von hinzugekommenen Updates und Patches. Nicht erspart bleiben Einstellungen und Anpassungen wie Anzahl CPUs, Größe des Hauptspeichers, Konfiguration und Anbindung an den Storage und Integration in die Netzwerke. Selbstverständlich müssen auch alle Vorbereitungen für den späteren IT-Betrieb erfolgen wie für Monitoring, Administration, Backup und Restore sowie Security-Monitoring. Diese Aktivitäten werden in der Regel über einen Change in den Administrations-Tools der virtuellen Umgebung konfiguriert.

## Betrieb im Umfeld der Server-Virtualisierung

Für den Betrieb validierter Anwendungen in einer virtualisierten Umgebung sind einige Festlegungen erforderlich:

- Es ist regulatorisch nicht relevant, dass in einem Cluster, auf einem Host mehrere VMs nebeneinander betrieben werden; die Isolation der Applikationen gegeneinander ist gegeben.
- Es ist regulatorisch nicht relevant, auf welchem physischen Host/in welchem Standort eine VM (mit OS und Applikation) aktuell läuft (das Cluster erstreckt sich auf beide Standorte).
- Es ist regulatorisch nicht relevant, wenn eine VM (mit OS und Applikation) von einem Host auf einen anderen innerhalb des Clusters, „live“ migriert (verschoben) wird

Die Betriebsführung für eine VM mit ihrem Betriebssystem und der implementierten Anwendung ist derjenigen für ein System auf der physischen Plattform zunächst vergleichbar. Doch es ändern sich die zentralisierten Betriebsaufgaben, wie das Monitoring der Maschinen-Performance und des Backup.

Zusätzliche, gleichwohl gut abgrenzbare Aufgaben der Betriebsführung sind durch die Virtualisierung bedingt, wie Monitoring und Administration des Clusters mit seinen Hosts, deren Anbindungen an Storage und Netzwerke, Monitoring und Administration des Hypervisor, sowie Administration und Überwachung aller durch Tools automatisierten Verfahren zur Betriebsoptimierung der virtuellen Infrastruktur und der VMs.

In der folgenden Aufstellung sind Funktionen der Ebene der Hosts im Cluster zusammengefasst, die ohne bzw. mit Auswirkungen auf die VMs mit ihren Anwendungen sind.

- Starten und Stoppen einzelner Hosts, jedenfalls in einem Rechner-Cluster.
- Aktualisierung der Host-Software durch Updates und Patches.

Funktionen mit Auswirkungen auf die Gastsysteme.

- Backup und Restore/Recovery des einzelnen Gastsystems.
- Update und Patching der virtuellen Hardware (die Arbeiten bzgl. des Betriebssystems der VM unterscheiden sich wenig von denen für das Betriebssystem einer physischen Maschine).
- Update und Patching des Hypervisor (im Cluster mit mehreren Hosts ggf. auch ohne jegliche Beeinträchtigung der Gastsysteme).
- Update und Patching der Hardware der Wirtssysteme, (im Cluster mit mehreren Hosts ggf. auch ohne jegliche Beeinträchtigung der Gastsysteme).

### Update, Patch und Change

Aufwand durch die Virtualisierung entsteht durch Monitoring und Administration (System-Pflege durch Updates und Patching). Dabei ist die Frage nach Mehraufwendungen nicht eindeutig zu beantworten, da sich auf der anderen Seite die Wartungstätigkeiten für die physischen Systeme reduzieren. Hierbei ist der Bezug entscheidend, um welchen Faktor die Zahl der physischen Systeme abnimmt. Die Zahl der verschiedenen von der IT zu betreuenden Betriebssysteme lässt sich durch Virtualisierung aber i. d. R. nicht verringern (s. o. Legacy-Systeme).

Besondere Sorgfalt ist den Verfahren für Updates und Patches zu widmen, da durch die zusätzlichen Komponenten komplexere Abhängigkeiten entstanden sind. Eine sorgfältige Überprüfung aller Hardware- und Software-Komponenten auf ihre gegenseitige Verträglichkeit ist unerlässlich. Die Durchführung von Updates und Patches von VMs und ihren Betriebssystemen bzgl. der Verfügbarkeit (Downtime) unterscheiden sich nicht von physischen Plattformen. Gleiches gilt für Updates und Patches der Anwendungen.

Updates und Patches der Hypervisor sind in der Regel ohne Beeinträchtigungen der Produktion möglich, da die Hosts, genauer die Hypervisor-Software auf dem einzelnen Host, nacheinander aktualisiert werden. Dazu wird ein einzelner Host, nach Migration der VMs auf die anderen Hosts des Clusters, in einen Wartungsmodus versetzt und nach erfolgreicher Durchführung wieder in Produktion genommen.

In diesem Zusammenhang entscheidend ist ein lückenloses Change-Management auch für die Änderungen an der virtuellen Platt-

form, nicht nur wie es regulatorisch gefordert ist, sondern weil hiermit Risiken für die Infrastruktur vermindert werden.

### Audit Trail

Eine Aufzeichnung (Logging) der regelmäßigen wie Anlass-bezogenen Aktivitäten und Changes kann in vielen Administration-Tools aktiviert werden und automatisch erfolgen. Es muss festgestellt werden, in wieweit die Anforderungen an Audit Trails von den Logging-Verfahren erfüllt werden. Reviews der Log-Protokolle sind durch die Administratoren und die Qualitätssicherung durchzuführen.

## Zusammenfassung

Es ergeben sich also, neben den rein technischen Vorzügen wie Rechner-Konsolidierung und Hochverfügbarkeit für Anwendungen, die branchenunabhängig durch eine Virtualisierung der Compute-Ressourcen erzielt werden, folgende wesentlichen Vorteile für die regulierte Umgebung:

- Jede validierungspflichtige Anwendung kann ihre eigene Maschine (VM) erhalten (Isolation der Anwendung).
- Deutliche Entkopplung der Innovationszyklen von Hardware und Betriebssystem-Software von denen der Anwendungen, und Flexibilität für den Betrieb älterer Betriebssysteme.
- Reduzierte Qualifizierungsaufwendungen bei der Implementierung neuer validierungspflichtiger Anwendungen auf Basis bei bereits vorhandener Typ-qualifizierter virtueller Maschinen.
- Vereinfachter Aufbau von Test- und Entwicklungssystemen (Kopie der Produktiv genutzten Anwendung).
- Vereinfachtes Belegen der Entsprechung bei Aufbau des Qualitätssicherungssystems aus dem Produktivsystem

Natürlich sind mit der Nutzung der Server-Virtualisierung auch einige zusätzliche Risiken und einige wenige Einschränkungen verbunden, die Vorteile sowohl in technischer wie regulatorischer Hinsicht überwiegen aber deutlich.

Es war das Ziel, die Vertrauenswürdigkeit des Konzepts einer VI für den Einsatz auch im regulierten Umfeld zu diskutieren und aufzuzeigen, dies über die technischen Vorteile hinaus, die dieses Konzept grundsätzlich längst nachgewiesen hat.

## Fachliteratur

(Links geprüft am 10. 9. 2012)

GAMP® 5, A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008
Server-Virtualisierung, Leitfaden und Glossar, Version 2, April 2009, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM):
http://www.bitkom.org/files/documents/BITKOM_Server-Virtualisierung_Leitfaden_und_Glossar.pdf
http://www.bitkom.org/de/publikationen/38337_40545.aspx
Vergleich von Lösungen der Server-Virtualisierung für die x86/x64-Plattform
http://www.searchdatacenter.de/themenbereiche/virtualisierung/loesungen/articles/260767/
Backup und Restore bei Server-Virtualisierung:
http://www.searchstorage.de/themenbereiche/backup-recovery/grundlagen/articles/281982

## Glossar

- Hypervisor / VMM
  Software-Plattform, die ermöglicht mehrere Virtuelle Maschinen (VMs) gleichzeitig auf einem physischen Server zu betreiben.
- Parent-VM
  VM als Ursprung eines Snapshots oder Klons.
- Klon
  Vollständige Kopie einer VM mit allen Daten oder Kopie der Parent-VM, wobei alle Änderungen zur Parent-VM in Differenzdateien gespeichert werden.
- Snapshot
  Aufnahme / Einfrieren einer Parent-VM mit allen Daten in beliebigem Betriebszustand, zu dem zurückgekehrt oder der mit der Parent-VM vereinigt werden kann.
- Compute Ressource
  Server auf dem die Virtuelle Infrastruktur betrieben wird und der als Host für Virtuelle Maschinen dient.
- Template einer VM
  Master Image einer konfigurierten VM in Form eines Klons, meist auch schon mit installiertem Betriebssystem.
- Gastwerkzeuge
  Installationspaket mit Software zur Steuerung der VM und Treiberpaket für die virtuelle Hardware der VM.
- Konvertierung und Migration
- ‚P2VP'-Migration (VMware vCenter Converter; Microsoft WSMT)
  Überführung einer Installation einer Applikation mit Betriebssystem von einem physischem Server in eine VM. Austausch der Treiber der physischen Hardware mit Treibern für die virtuelle Hardware der VM und Überführung der Systemkonfiguration und der Laufwerke mit allen Daten in entsprechendes Virtual Image Dateiformat. Weitere Konvertierungen: V2V und V2P.
- „live"-Migration (VMware vMotion; Microsoft Hyper-V 2008 R2)
  (fast) unterbrechungsfreie Überführung einer VM im Betrieb vom physischen Ursprungs-Server auf den physischen Ziel-Server. Für das Betriebssystem in der VM erfolgt live-Migration transparent.
- Cluster Ressource
  Zusammenführung von physischen Servern (auch an unterschiedlichen Standorten / RZs) zu einer gemeinsamen Ressource (=cluster compute ressource) für den Betrieb von VMs

Techno Pharm

# Anzeigen- und Druckunterlagen-schluss

für **06/12**

ist am **13.11.12**

**anzeigen-tp@ecv.de**
**Telefon +49 (0) 7525 - 940 132**
**Fax +49 (0) 7525 - 940 155**