Link: https://www.tecchannel.de/a/virtualisierungstrends-virtuelle-desktops-clouds-und-intelligente-netzwerke,1827310

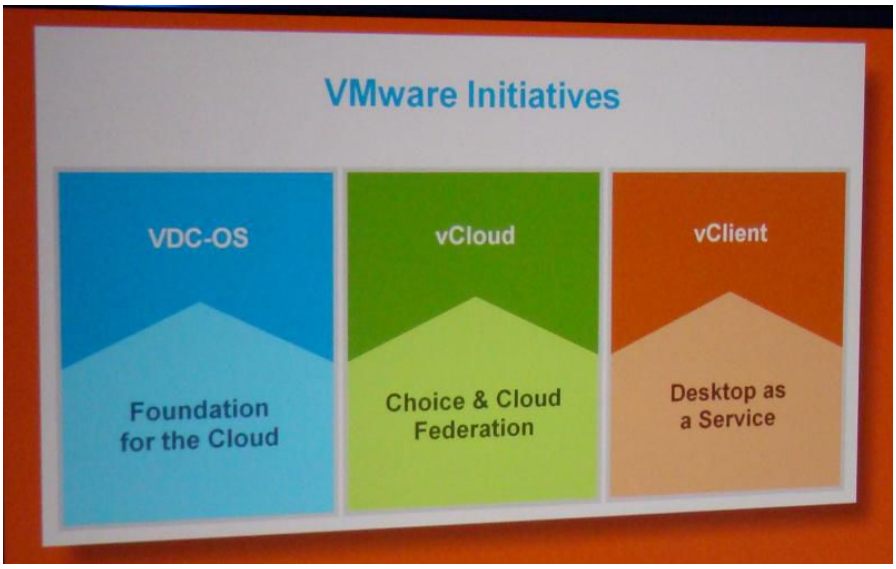
VMWorld Europe 2009

Virtualisierungstrends: Virtuelle Desktops, Clouds und intelligente Netzwerke

Datum: 04.03.2009
Autor(en): Moritz Jäger

Auf der VMWorld Europe 2009 zeigten VMware und andere Hersteller, welche Trends und Technologien bei der Virtualisierung wichtig sind. Neben Cloud Computing und VDI stehen Hypervisor-Sicherheit und virtuelle Netzwerk im Zentrum.

Wer auf die VMWorld Europe 2009 in der Hoffnung auf viele Neuigkeiten gefahren ist, wurde enttäuscht. Weder VMware noch die anderen Aussteller hatten wirklich bahnbrechende Neuheiten zu bieten. Das liegt wohl unter anderem auch daran, dass die US-Schwester **VMWorld**[1] erst wenige Monate zurückliegt.

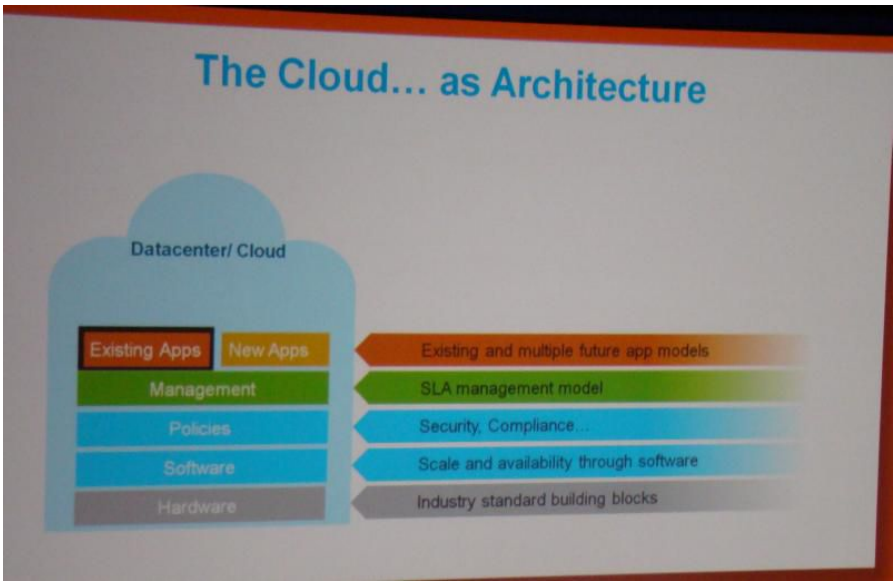


Drei Säulen: Das sind die künftigen Themen von VMware.

Dennoch war die Hausmesse von VMware ein guter Ort, um allgemein mehr über kommende Technologien im Bereich der Virtualisierung zu erfahren. TecChannel gibt Ihnen in diesem Artikel einen Ausblick auf künftige Trendthemen, die von der Virtualisierung von Smartphones bis hin zu intelligenten virtuellen Netzwerk-Switchen reichen.

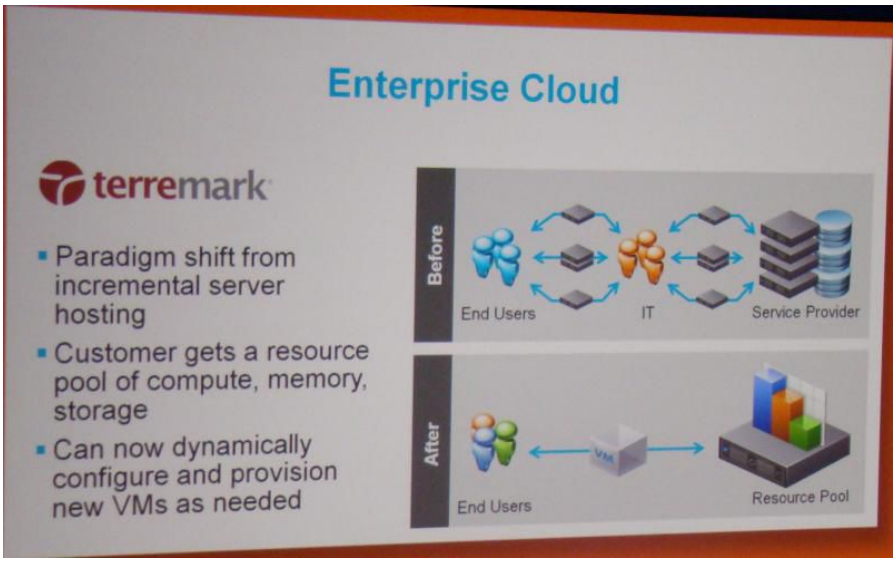
1. Cloud-Technologien halten Einzug ins LAN

Mit der größte Themenblock auf der VMWorld Europe 2009 und der vorhergehenden US-Veranstaltung war das Thema**Cloud Computing**[2]. Grob zusammengefasst fallen darunter Hosting-Ansätze, bei denen der Nutzer sich seine Bedürfnisse aus einem Pool von Speicher, CPUs und Netzwerk zusammenschnürt, und nur für die eigentliche Nutzung bezahlt. VMware sieht hier in jedem Fall die Zukunft des Datencenters. Allerdings tummeln sich derzeit immer mehr proprietäre Cloud-Anbieter, etwa **Amazon EC2**[3], **Microsoft Azure**[4] oder **Googles App Engine**[5], deren Technologien sind aber untereinander nicht kompatibel. VMware CEO Paul Maritz nutzte als Vergleich häufiger in Anspielung auf den Eagles-Song „Hotel California“ das Bild von einem Motel, in das man zwar eincheckt, das man aber nie wieder verlässt. VMware will hier eine komplett andere und offene Strategie fahren.



Rechenwolken: VMware will interne und externe Clouds verbinden.

Helfen soll dabei die kommende Version der Datacenter-Lösung namens vSphere. Unter dem plakativen Oberbegriff „Datacenter-OS“ tummelt sich eine Reihe von Lösungen, mit denen lokale Ressourcen abstrahiert und zu Pools für Netzwerk, Rechenleistung und Speicher zusammengefasst werden können. Aus diesen kann man dann einzelne Abteilungen, Server oder Anwendungen bedienen. Maritz und andere Experten nutzen in ihren Vorträgen dafür immer wieder den Begriff des Software-Mainframes.



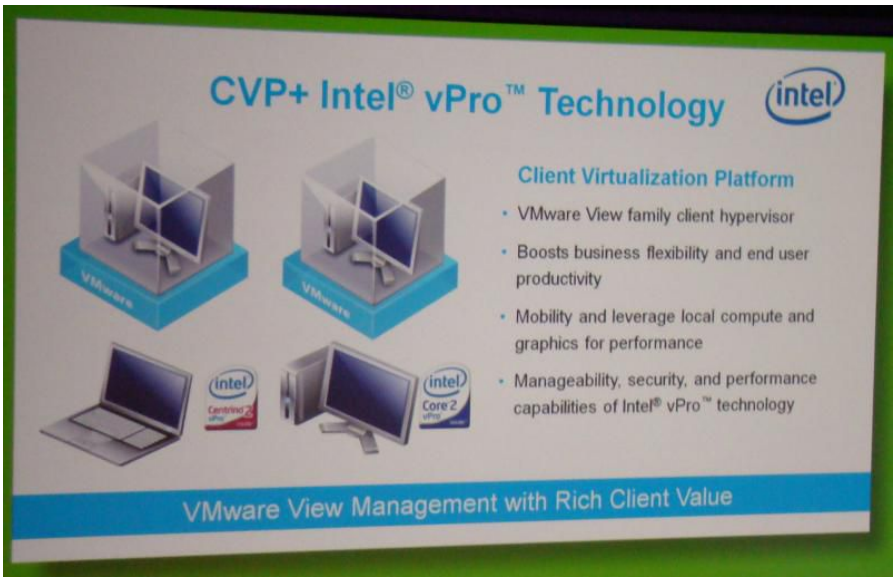
Vereinfachung: Terremark zeigt, wie sich mittels Clouds die Infrastruktur vereinfachen lässt.

Die notwendige Verwaltungsoftware samt Hypervisor soll als vSphere noch 2009 auf den Markt kommen. Der genaue Veröffentlichungstermin ist aber noch unbekannt. vSphere soll zudem nicht nur lokale Clouds unterstützen, sondern auch extern zugekaufte Ressourcen kompatibler Anbieter mit in die eigene Verwaltungsoberfläche integrieren können. In den gezeigten Demos ließen sich ganze Server-Umgebungen per Mausklick vom LAN in die Clouds verlagern – und umgekehrt.

2. Virtuelle Desktops und virtualisierte Smartphones

Das zweite große Thema war die virtualisierte Desktop-Umgebung, auf die der User mittels Netzwerk zugreift. Dabei liegt die komplette Arbeitsumgebung des Nutzers auf einem Server im Datencenter, der Rechner des Endnutzers wird zu einer Art Thin Client umfunktioniert. Zusammengefasst ist die Technologie unter dem Schlagwort VDI für Virtual Desktop Infrastructure.

Die Vorteile liegen auf der Hand: Alle Daten sind sicher aufbewahrt, und im Notfall, etwa einem Hardwareausfall, erhält der User ein neues Endgerät und kann sofort weiterarbeiten, ohne dass Zeit für eine erneute Systeminstallation verschwendet wird. Problematisch ist derzeit aber noch, dass die existierenden Lösungen, etwa **VMware View**[6], meist eine ständige und stabile Netzwerkverbindung erfordern. Auch hier soll sich einiges ändern. VMware hat mit Intel eine Kooperation angekündigt, die zum Ziel hat, Computer, die **Intels vPro-Technologie** [7] unterstützen, mit einem eigenen Hypervisor auszustatten. Diese Geräte können anschließend direkt auf das im Server abgelegte virtuelle Image zugreifen, ohne dass zuvor ein Betriebssystem installiert werden muss.



Joint Venture: Intel und VMware arbeiten gemeinsam an einem Hypervisor für vPro-Geräte.

Zusätzlich soll die kommende Version von VMware View einen Offline-Modus erhalten. Die Arbeitsumgebung ist dann auch ohne Netzwerkanschluss einsatzbereit, etwa während einer Reise. Sobald eine passende Verbindung zur Verfügung steht, kann sich die lokale virtuelle Maschine mit dem Image auf dem Server synchronisieren, wobei nur die Änderungen übertragen werden. Ein weiteres Ziel ist, die nächsten Versionen des virtuellen Desktops deutlich leistungsfähiger zu machen. Aufgaben wie 3D-Rendering oder grafiklastige Anwendungen sollen dann auch auf virtuellen Systemen in akzeptabler Geschwindigkeit möglich sein. Ziel sei es, dass der Nutzer keinen Unterschied mehr zwischen einem physischen und einem virtuellen Desktop bemerkt.

Neben den Desktops hat VMware auch die Virtualisierung von Smartphones im Blick. Dies zeigte eindrucksvoll ein Prototyp der Mobile Virtualization Plattform, MVP. Mit dem System sollen Smartphones unterschiedliche Betriebssysteme starten können, unabhängig vom ursprünglich vorgesehenen OS. Als Prototyp gab es ein Nokia N800 zu sehen, auf dem je eine virtuelle Maschine mit Windows CE und Android lief. Beide Betriebssysteme waren voll funktionsfähig und liefen erstaunlich flüssig.

Virtualisiert: Auf dem N800 läuft Windows CE und Google Android.

Als praktische Anwendung kann man sich beispielsweise ein Smartphone vorstellen, das neben dem privaten Betriebssystem des Anwenders noch ein speziell gesichertes E-Mail-System enthält. Dieses verwaltet dann etwa die sensiblen Daten der Firma. Bis es hier allerdings finale Produkte zu sehen gibt, wird es wohl noch eine Zeit dauern, vor allem der Stromverbrauch der Geräte ist noch zu hoch.

3. Einzelanwendungen virtualisieren und streamen statt installieren

Eher am Rande der VMWorld Europe 2009 wurden Technologien rund um die Virtualisierung von Programmen besprochen und vorgestellt. Das Ziel dabei ist, dass statt kompletten Umgebungen lediglich einzelne Programme virtualisiert und dem Nutzer zur Verfügung gestellt werden. Klickt der Nutzer auf ein Programm-Icon startet keine Installation, sondern die benötigten Teile der Anwendung werden von einem zentralen Server auf den Rechner des Nutzers gestreamt.

Ein Beispiel für solch eine Integration ist das ehemalige SVS Pro von Altiris, das nach der Symantec-Übernahme nun in einer neuen Version als **Symantec Endpoint Virtualization Suite**[8] auf den Markt kommt. Im Gespräch mit TecChannel erklärt Doug Coombs, Director Product Management Endpoint Virtualization bei Symantec, den Nutzen der Applikationsvirtualisierung. Einer der größten Vorteile sei demnach der gesparte Speicherplatz. Denn die Nutzer erhalten nur exakt den Teil der Anwendung, den sie auch benötigen. Er selbst habe sein Word virtualisiert und benötige für seine tägliche Arbeit nur einen Bruchteil des Gesamtprogramms.

Praktisch ist auch, dass die Software ein ausgefeiltes dynamisches Lizenzmanagement enthält. Dabei ist es möglich, dass die Lizenzen für eine Software in den Pool des Unternehmens zurückwandern, wenn diese über einen definierten Zeitraum nicht genutzt werden. Die Lizenzen stehen dann für andere Nutzer zur Verfügung. Benötigt der ursprüngliche Nutzer das Programm wieder, so erhält er eine neue Lizenz aus dem Pool.

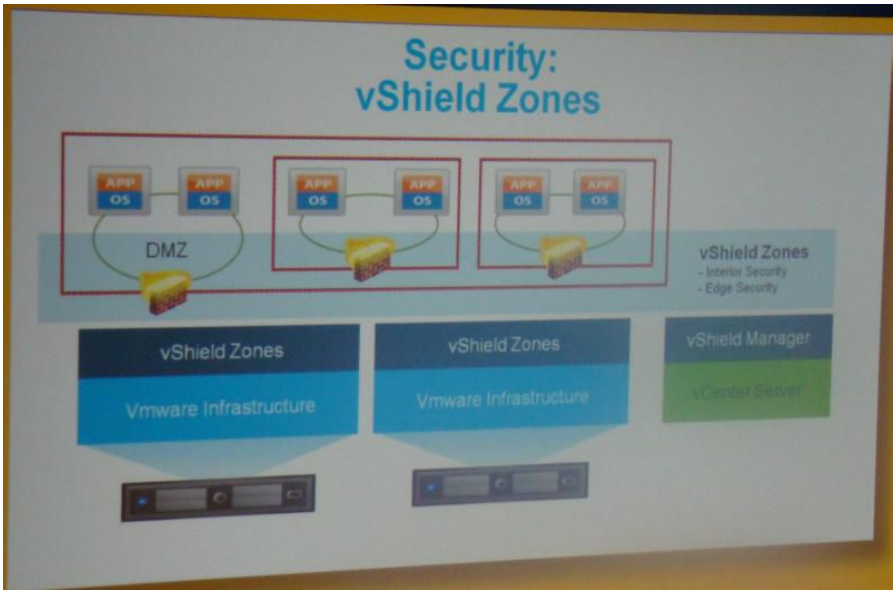
Ein anderes Beispiel für die Technologie ist **VMware Fusion**[9]. Damit lassen sich Windows-Programme auf Mac OS ausführen, ohne dass der Nutzer eine Änderung in der Oberfläche bemerkt.

4. Sicherheit der virtuellen Infrastruktur und des Hypervisors

Das Thema Sicherheit stand ebenfalls auf der Agenda der VMWorld 2009. Virtuelle Umgebungen sind mittlerweile lohnende Ziele für Cyberkriminelle und Malware-Autoren. Künftige Malware könnte versuchen, den Hypervisor direkt zu übernehmen oder sich an ihn anzuhängen. Danach hätte die Malware theoretisch die gleichen Rechte wie der Hypervisor, wäre also den meisten Anti-Malware-Systemen übergeordnet – etwa, wenn diese in einer virtuellen Maschine laufen.

Dieses Szenario kann VMware direkt verhindern. Im Gespräch mit TecChannel erklärt uns Bogomil Balkansky, Senior Director Product Marketing, dass VMware versucht, den Hypervisor so klein wie möglich zu halten, um so keinerlei Angriffsmöglichkeiten zu bieten. Je weniger Code im Hypervisor stecke, desto weniger Angriffsfläche gäbe es. Auch habe VMware einen Vorteil gegenüber normalen Betriebssystemen, da die Architektur auf Sicherheit ausgelegt werden könne und sie nur einzelne Treiber direkt unterstützen müssten, so Balkansky.

Für die interne Sicherheit plant VMware für die kommende ESX-Version eine Technologie namens **vShield Zones**[10]. Damit sollen sich virtuelle Umgebungen voneinander abkapseln können und der Traffic zwischen den Maschinen überwacht und notfalls unterbunden werden können.



Getrennt: vShield Zones soll virtuelle Umgebungen besser absichern.

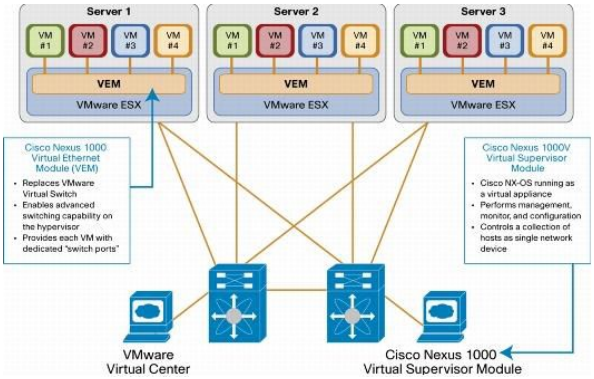
Das zweite Szenario betrifft virtuelle Maschinen, die auf offline geschaltet wurden. Anders als bei physischen Desktop-Systemen bedeutet das nämlich keineswegs eine absolute Sicherheit. Vielmehr gibt es APIs, über die Programme mit Offline-VMs kommunizieren können. Hier wäre also ein Szenario denkbar, in dem eine Malware an die Daten von Offline-VMs gelangt und diese infiziert. Sobald die Maschinen gestartet werden, etwa als Fallback-System nach einer Attacke, wird die Malware aktiv und übernimmt das jeweilige System.

Hier sieht es derzeit noch schlecht mit schlüsselfertigen Lösungen aus, so Harish Sunderam Agastya von Trend Micro im Gespräch mit TecChannel. Bislang gäbe es keine Produkte, mit denen sich virtuelle Maschinen im Offline-Zustand überwachen und patchen lassen würden. Hier sind also der Admin und sein Sicherheitskonzept gefragt. Auch Fallback-Systeme sollten regelmäßig geprüft und aktualisiert werden.

5. Intelligentere virtuelle Netzwerke

Rund um die Neuerungen wie VDI blieb das Thema Netzwerkinfrastruktur ein wenig auf der Strecke: Vor allem, wenn virtuelle Desktops unternehmensweit ausgerollt werden, benötig man skalierbare und flexible Netzwerke. Hier kommt noch ein weiterer Makel hinzu: Virtuelle Umgebungen, die untereinander kommunizieren, lassen sich nur sehr kompliziert überwachen. Zur Konfiguration müssen Netzwerkadministratoren zudem auf das meist unvertraute Interface des vCenters zurückgreifen. Und selbst wenn alle Netzwerkoptionen passend eingerichtet sind, kann eine verschobene virtuelle Maschine, etwa mittels vMotion, alle Bemühungen zunichte machen.

Das sind mit die Gründe, warum die kommende ESX-Generation vSphere eine verbesserte Netzwerkvirtualisierung erhält. Damit lassen sich Erweiterungen von Drittherstellern direkt in vSphere integrieren. Einer der ersten Konzerne, der eine passende Software vorgestellt hat, ist Cisco. Gezeigt wurde der virtuelle Switch **Nexus 1000v**[11]. Dieser ersetzt das integrierte Switchboard des ESX und besteht aus zwei Teilen: dem VSM (Virtual Supervisor Module), der als separate Appliance virtuell oder physisch installiert wird, und dem VEM (Virtual Ethernet Module), der in jedem EXS-Server den VMware-Netzwerklayer ersetzt.



Nexus 1000v: Die Cisco-Erweiterung ersetzt den virtuellen Switch von VMware. (Quelle: Cisco)

Sobald die Software installiert ist, lässt sie sich wie jeder andere Cisco-Datacenter-Switch mittels NX-OS konfigurieren. Die einzelnen Konfigurationen kann der Administrator im vCenter anschließend den einzelnen virtuellen Maschinen zuweisen. Vorteil ist dabei, dass jeder Administrator auf seiner bekannten Oberfläche weiterarbeitet. Der Nexus 1000v verknüpft jede Konfiguration fest mit der jeweiligen virtuellen Maschine. Zieht dieses System nun auf einen anderen ESX-Server, folgt die Netzwerkkonfiguration automatisch.

In der Demo und dem Hands-on-Lab konnte der Nexus 1000v bereits getestet werden und machte durchaus einen soliden Eindruck. Der virtuelle Switch arbeitet mit allen Standard-Ethernet-Switches zusammen. Wann entsprechende Software von anderen Herstellern verfügbar ist, wurde noch nicht genannt. Cisco koppelt den Release der Software an die Verfügbarkeit von vSphere.

6. Fazit

Virtualisierung ist definitiv immer noch eine Technologie mit Zukunft. Denn egal ob Server oder Desktop, nur wenige Systeme lasten eine moderne Hardware wirklich richtig aus. Auch der Cloud-Ansatz macht durchaus Sinn, denn so erreicht man eine komplette Abstraktion von der Hardware. Sobald es halt eng wird, holt man sich zusätzliche Rechenleistung, sei es durch einen weiteren lokalen Server oder eben einen externen Anbieter.

Die zunehmende Virtualisierung wird zwar die Desktops entlasten und Server optimieren, allerdings wird das wohl zu Lasten des Netzwerkes gehen. Stellen Sie sich einfach vor, wenn alle Ihre Mitarbeiter übers Netz auf ein Desktop Image eines Servers zugreifen – zusätzlich zum normalen Netzwerk-Traffic. Hier werden wohl Gigabit-Leitungen zum Arbeitsplatz künftig zunehmen, während die Server mindestens mit 10 Gbit/s angebunden werden müssen.

Dennoch erlaubt die Virtualisierung immer weitere, faszinierende Szenarien, mit denen Mitarbeiter in das System integriert werden können. Stellen Sie sich einfach vor, dass Sie künftig auf die privaten Rechner der Nutzer ein sicheres System mit aufspielen können, ohne sich um die Hardware zu kümmern. Oder dass Sie dem Smartphone des Nutzers einfach eine gesicherte BlackBerry-Installation aufspielen, ohne dass dieser deswegen ein neues Endgerät erhalten muss. Das ist zwar derzeit noch Zukunftsmusik, aber wenn Sie sich vor Augen halten, dass seit der ersten VMware Workstation erst zehn Jahre vergangen sind, liegt die Zukunft vielleicht näher, als wir denken. (mja)

Links im Artikel:

[1] **http://www.vmworld.com/index.jspa**
[2] **https://www.tecchannel.de/server/virtualisierung/1759881/dynamic_it_mit_cloud_computing/**
[3] **http://aws.amazon.com/ec2/**
[4] **http://www.microsoft.com/azure/default.mspx**
[5] **http://code.google.com/appengine/**
[6] **http://www.vmware.com/products/view/**
[7] **https://www.tecchannel.de/netzwerk/management/442760/vpro_2008_komfortable_verwaltung_von_business_pcs_und_notebooks/**
[8] **http://www.symantec.com/business/endpoint-virtualization-suite**
[9] **http://www.vmware.com/products/fusion/**
[10] **http://www.vmware.com/products/vshield-zones/overview.html**
[11] **http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data_sheet_c78-492971.html**

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.