Verbesserte Virtualisierung auf Servern mit Intel® Architektur

Nutzung optimieren, Flexibilität verbessern, Kosten senken

Die Servervirtualisierung auf Plattformen auf der Basis von Intel® Prozessoren unterstützt Unternehmen schon jetzt dabei, Server zu konsolidieren, Test- und Entwicklungsumgebungen zu vereinfachen, die Gesamtbetriebskosten zu senken und schneller auf sich ändernde Auslastungsanforderungen zu reagieren. Die Intel® Virtualization Technology wird darüber hinaus grundlegende unterstützende Architektur für heutige, ausschließlich auf Software basierende Lösungen zur Verfügung stellen und die Vorteile von Virtualisierung erweitern. Innovation wird beschleunigt und der Weg für Virtualisierungslösungen geebnet, die stabiler sind, mehr Interoperabilität bieten und besser zu unterstützen sind.

März 2005

Inhaltsverzeichnis

Kurzübersicht

„...Unternehmen sollten sich JETZT mit dem Thema Virtualisierungstechnik auseinandersetzen.“

– *The Future of Server Acquisition and Deployment,* Andrew Butler, Vice President & Research Area Leader, Server Technologies, Gartner, 18. März 2004

Virtualisierungstechnik resultiert bereits in veränderten Vorgehensweisen vieler IT-Abteilungen bei der Beschaffung und Verwaltung ihrer Systeme und Anwendungen. Servervirtualisierung ermöglicht die flexible und sichere Konsolidierung mehrerer Betriebssysteme und Anwendungen auf einer einzigen Plattform. Augrund dessen verringert sich die Anzahl der benötigten Server, während ihre Nutzung erhöht wird, die IT-Infrastruktur wird vereinfacht, und Verwaltungskosten werden gesenkt. Bei gleichzeitigem Einsatz von Tools für die schnelle Bereitstellung von Software kann Servervirtualisierung auch eine flexible und dynamische Verwaltung der Hardwareressourcen ermöglichen, die optimal auf sich ändernde Auslastungsanforderungen reagieren kann. Diese Funktionsmerkmale ermöglichen vielen Unternehmen eine beträchtlich erhöhte Produktivität, daher ist im Lauf der nächsten Jahre eine dramatische Zunahme der Implementierung zu erwarten. Schätzungen von IDC zufolge enthielten 8 % aller im Jahr 2003 gelieferten Server Bereitstellungs- und Virtualisierungsfunktionen; im Jahr 2007 soll dieser Anteil bereits bei 40 % liegen.[1]

Intel® Virtualization Technology, ursprünglich als Intel Vanderpool Technology bekannt, bietet die erforderliche Hardwareunterstützung, um die Produktivität der heutigen, ausschließlich auf Software basierenden Virtualisierungslösungen noch zu steigern. Diese Erweiterung der Intel® Architektur wird IT-Abteilungen dabei unterstützen,

- Kosten und Risiken zu reduzieren, die mit der Implementierung von Virtualisierungslösungen für Server verbunden sind;
- die Zuverlässigkeit, Verfügbarkeit und Sicherheit der Anwendungen zu erhöhen, die in virtuellen Partitionen ausgeführt werden;
- die Interoperabilität mit Legacy-Software zu verbessern.

Intel® Virtualisierungstechnik wird zudem die Entwicklung von Virtualisierungssoftware vereinfachen und einen Anstoß für weitere Innovationen geben. Die Spezifikationen wurden bereits freigegeben: Hardware-Unterstützung für Plattformen auf Basis von Intel® Itanium® 2 Prozessoren wurde bereits in 2005 implementiert, und Unterstützung für Plattformen auf Basis von Intel® Xeon® Prozessoren 64-Bit ist im ersten Halbjahr 2006 zu erwarten. Intel arbeitet derzeit mit führenden Drittanbietern zusammen, um die Einführung von Virtualisierungssoftware der nächsten Generation zu beschleunigen und einen effizienten Einsatz der verbesserten neuen Architektur zu ermöglichen.

Virtualisierung ist eine Technologie der Neugestaltung, und Intel verschreibt sich der Bereitstellung von marktführenden Virtualisierungsfunktionen auf Intel Architektur. Diese Funktionen werden ergänzend zu einer Reihe weiterer Intel Plattforminnovationen sein, mit denen einige der kritischsten IT-Herausforderungen angegangen werden. Das Zusammenwirken dieser Technologien wird zu erhöhter Flexibilität, Zuverlässigkeit, Sicherheit und Verwaltbarkeit der Intel Architektur beitragen, um Unternehmen weitergehende Produktivität für eine Bandbreite unterschiedlicher IT-Anforderungen zu ermöglichen.

[1] Quelle: IDC Adaptive Resource Management Report (2004).

Hohe IT-Betriebskosten

„Unternehmen, die das Virtualisierungspotenzial nicht nutzen, werden bis zum Jahr 2008 mit bis zu 40 % höheren Anschaffungs- und etwa 20 % höheren Verwaltungskosten rechnen müssen…“

– *The Future of Server Virtualization*, T. Bittman, Gartner Research Note, 17. Juli 2003

In der Regel verwenden IT-Abteilungen 70–80 Prozent ihres Budgets für die Verwaltung bestehender Systeme und Anwendungen.[2] In einem durchschnittlichen Datenzentrum stellt die große Anzahl nicht ausgelasteter Server einen wichtigen Kostenfaktor dar. In der Vergangenheit tendierten IT-Abteilungen dazu, jeweils nur eine Anwendung pro Server auszuführen. Aufgrund von relativ kostengünstigen Industriestandard-Servern folgte man damit einer kosteneffizienten Strategie, welche die Implementierung vereinfachte und mögliche Softwarekonflikte umging. In den letzten zehn Jahren ist die Anzahl der weltweit eingesetzten Server allerdings fast um das 150-fache gestiegen, und dementsprechend haben sich auch die damit verbundenen Wartungskosten erhöht.[3]

Auch die durchschnittliche Serverleistung hat sich erhöht, und moderne Server erbringen die zehnfache Leistung ihrer Vorgänger vor zehn Jahren. Mithilfe von Virtualisierung können IT-Abteilungen diese zusätzliche Leistungsfähigkeit nutzen, indem mehrere Anwendungen und Betriebssysteme auf einer einzigen Plattform konsolidiert, die Servernutzung erhöht und die Verwaltungs-, Energie- und Kühlanforderungen verringert werden.[4] Die heutigen Lösungen ermöglichen zudem eine flexible Ressourcenzuordnung im Falle eines unerwarteten Anstiegs der Auslastung. Viele IT-Abteilungen werden unter Verwendung dieser neuen Tools Kosten im Zusammenhang mit Servern (sowohl Anschaffungs- als auch Betriebskosten) verringern und gleichzeitig die Flexibilität ihres Datenzentrums erhöhen können (Abbildung 1).

VMware, ein führender Anbieter von Servervirtualisierungssoftware verweist auf die deutlichen Einsparungen seiner Kunden in Bezug auf Total Cost of Ownership (TCO) von Servern, die mittels Virtualisierung und Konsolidierung erzielt werden:[5]

- Kostensenkung bei Hardware: 28–53%
- Senkung der Betriebskosten: 72–79%
- Kostensenkung insgesamt: 29–64%

VMware führt auch eine Reduzierung der Softwarelizenzierungskosten von bis zu 20 Prozent an.[6] Angesichts von Vorteilen dieser Größenordnung verwundert es nicht, dass mit einer weiteren Verbreitung von Virtualisierungstechnologien in den nächsten Jahren zu rechnen ist.

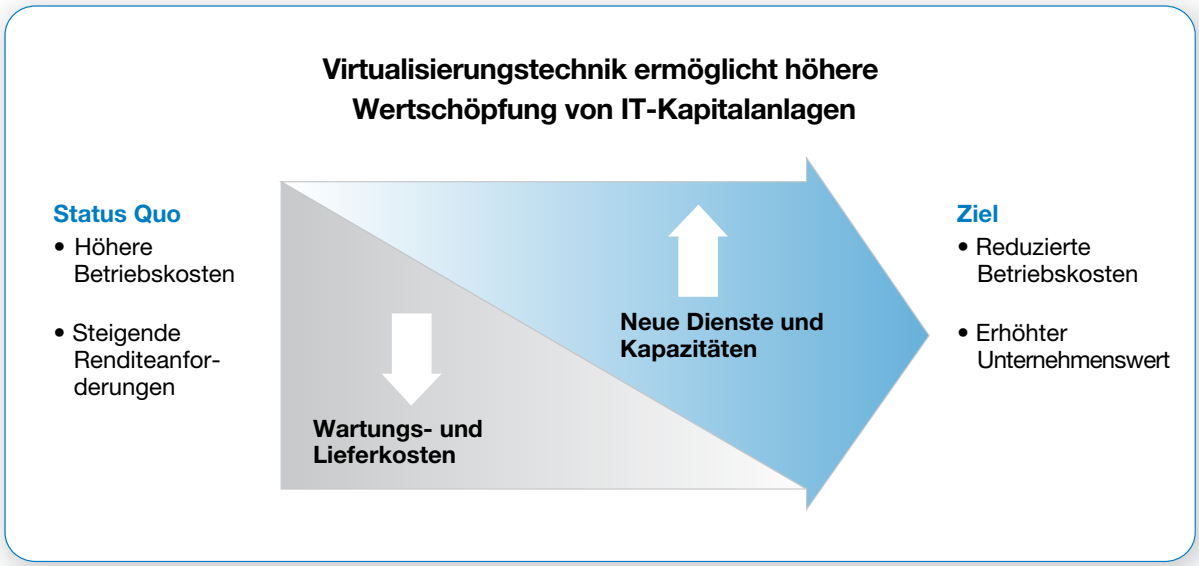

Abbildung 1. Die meisten IT-Abteilungen setzen derzeit einen Großteil ihrer Ressourcen für die Wartung bestehender Systeme und Anwendungen ein. Servervirtualisierung und –konsolidierung können zu einer höheren Nutzung, einer weniger komplexen Umgebung und verringerten Gesamtkosten beitragen, so dass Mittel für neue Projekte bereitgestellt werden können, die den IT-Unternehmenswert direkt erhöhen.

[2] Nach Aussagen von Kevin Rollins, President und COO, Dell Corporation, erschienen in: Dell and Sun Offer Different Visions, InformationWeek.com, von Larry Greenemeier, 17. September 2003.

[3] „Die Verarbeitungsleistung ist zwar relativ kostengünstig (und wird noch billiger), aber Raumbedarf, Strom, Installation, Integration und Verwaltung sind nicht kostengünstig…“ Quelle: *The Future of Server Virtualization,* T. Bittman, Gartner Research Note, 17. Juli 2003.

[4] Anmerkung: Man unterscheidet verschiedene Arten der Servervirtualisierung, einschließlich der Emulation von Betriebssystemen (z. B. Java Virtual Machine) und Workload-Management (mehrere Anwendungen teilen sich ein Betriebssystem). Das vorliegende Whitepaper beschränkt sich auf Ressourcenmanagement, wodurch mehrere Instanzen des Betriebssystems Plattformressourcen gemeinsam nutzen können. Weitere Informationen über andere Virtualisierungsmodelle finden Sie in: *„The Future of Server Virtualization”*, T. Bittman, Gartner Research Note, 17. Juli 2003.

[5] Weitere Informationen finden Sie auf der VMware Webseite unter: http://www.vmware.com/solutions/consolidation/index.html.

[6] Quelle: Michael Mullany, Vice President Marketing von VMware, zitiert von Mark Hall in seinem Artikel *„MAC Attracts New Support From...”* Computerworld, 10. Januar 2005; siehe http://www.computerworld.com/softwaretopics/os/macos/story/0,10801,98824,00.html.

Virtualisierung – eine Technologie der Neugestaltung

„Dank Virtualisierung können Unternehmen logische Nutzungseinheiten (z. B. ein Betriebssystem oder Speichervolumen) von physischen Betriebseinheiten (z. B. Server oder Laufwerk) entkoppeln, um die Nutzung zu maximieren – und erhöhte Flexibilität bei der Verlagerung und Verwaltung von IT-Ressoucen zu gewinnen."

– *Organic IT 2004: Cut IT Costs, Speed Up Business,* Frank E. Gillett, Forrester Research, 18. Mai 2004

Im Grunde genommen wird Software durch Virtualisierung von der zugrunde liegenden Hardwareinfrastruktur abstrahiert. In der Praxis sieht das so aus, dass die Verbindung zwischen einem bestimmten Software-Stack und dem entsprechenden Server getrennt wird. Dadurch lassen sich sowohl Hardware- als auch Softwareressourcen flexibler steuern, was sich in Produktivitätssteigerungen einer ganzen Reihe von IT-Anforderungen bemerkbar machen kann (Abbildung 2).

Serverinfrastruktur konsolidieren und standardisieren

Die heutigen Virtualisierungslösungen unterstützen Konsolidierung auf der gesamten Bandbreite an Plattformen auf Basis von Intel® Prozessoren. Sie können gleichermaßen für eine Nutzungsoptimierung kleiner 2-Wege-Server wie auch zur Unterstützung dutzender von Legacy-Anwendungen auf 4-, 8-, 16-Wege- oder noch größeren Plattformen eingesetzt werden.

Plattformressourcen – wie etwa Verarbeitungsleistung, Speicher, I/O und Kapazität – können entsprechend den Anforderungen des Unternehmens und der Anwendungen zugeordnet und priorisiert werden. Das ist besonders wichtig, da verschiedene Anwendungen unterschiedliche Anforderungen an die Auslastung stellen können. Die flexible Ressourcenzuordnung kann die Leistung verbessern, die Konsolidierungsraten erhöhen und eine bessere Ausgangsbasis für neu anzuschaffende Plattformen darstellen.

Da verschiedene Betriebssysteme auf einer gemeinsamen Plattform laufen können, vereinfacht Virtualisierung auch den Aufbau einer Hardwareinfrastruktur nach Enterprise-Standards. In Verbindung mit Konsolidierung bietet Virtualisierung zentrale Vorteile bei der Vereinfachung von Datencenterumgebungen und der Reduzierung der Total Cost of Ownership (TCO).[7]

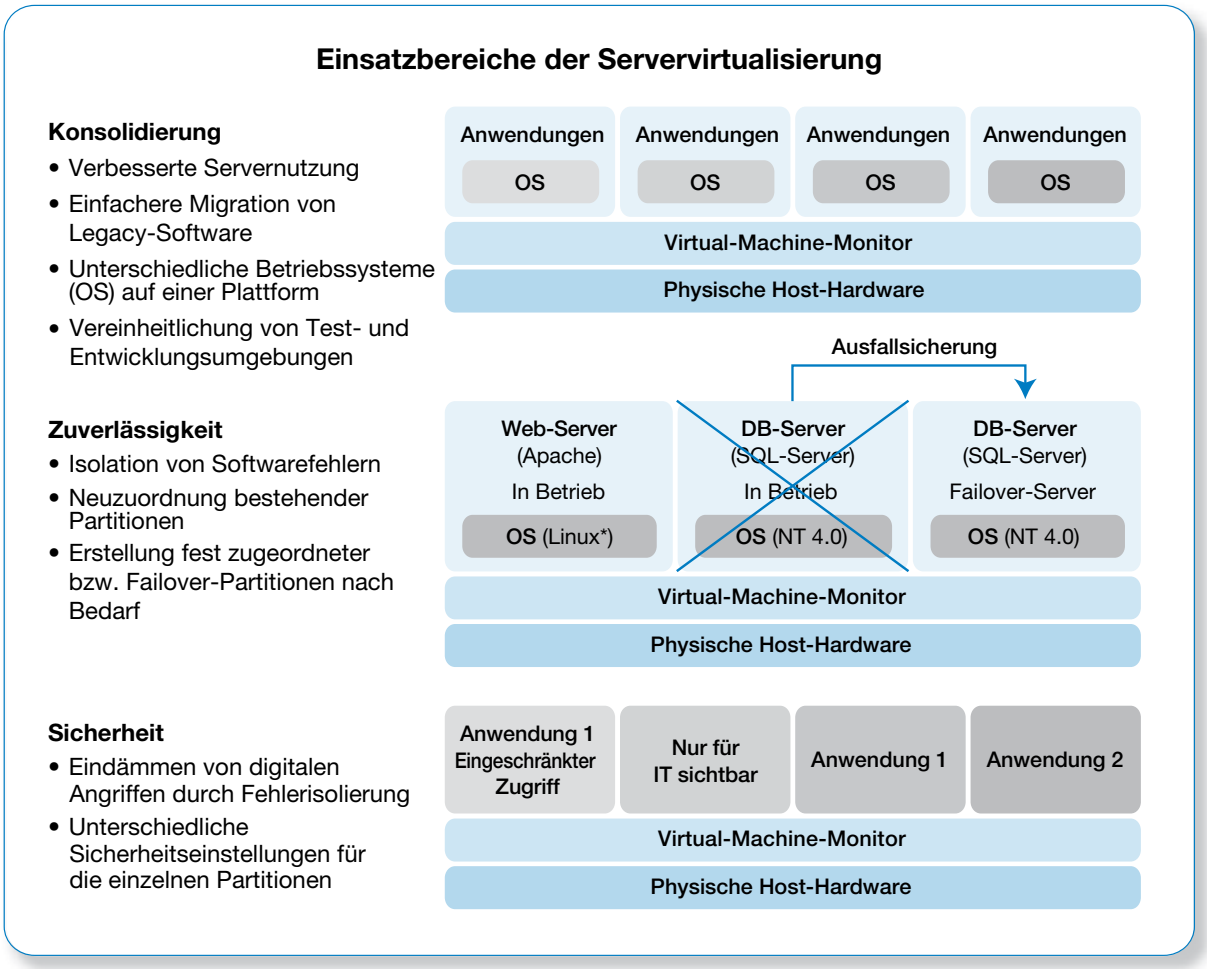

Abbildung 2. Servervirtualisierung kann zum Zweck einer verbesserten Servernutzung, höherer Zuverlässigkeit und Sicherheit eingesetzt werden. Zudem kann das Unternehmen flexibel auf neue Anforderungen reagieren und Betriebskosten senken.

[7] Eine detaillierte Diskussion finden Sie in: *„The Role of Standardization in Simplifying IT Infrastructure"*, IDC Executive Brief, September 2004.

Verfügbarkeit und Sicherheit verbessern

Virtualisierung unterstützt eine erhöhte Verfügbarkeit und Sicherheit auf verschiedene Art und Weise:

- **Fehlerisolierung** – Die meisten Ausfälle von Anwendungen werden durch Softwarefehler verursacht. Virtualisierung bietet die logische Isolierung der einzelnen virtuellen Partitionen, so dass ein Softwarefehler in einer Partition sich mit großer Wahrscheinlichkeit nicht auf die Anwendungen einer anderen Partition auswirkt. Die logische Isolierung unterstützt auch die Eindämmung von digitalen Angriffen und erhöht damit die Sicherheit konsolidierter Umgebungen.
- **Flexible Ausfallsicherung** – Virtuelle Partitionen lassen sich entsprechend konfigurieren, um einer oder mehreren Anwendungen automatische Failover-Sicherung zu bieten. Angesichts der Hochverfügbarkeitsfunktionen, die mittlerweile auf Plattformen auf Basis des Intel® Itanium® 2 Prozessors oder des Intel® Xeon® Prozessors MP unterstützt werden, können Service-Level-Anforderungen oft durch die Bereitstellung einer Failover-Partition auf derselben Plattform wie die primäre Anwendung erfüllt werden. Falls eine noch höhere Verfügbarkeit erforderlich ist, kann die Failover-Partition auch auf einer eigenständigen Plattform bereitgestellt werden.
- **Differenzierte Sicherheit** – Für jede Virtual Machine lassen sich verschiedene Sicherheitseinstellungen implementieren, so dass die IT-Abteilung die Zugriffsrechte von Benutzern und Administratoren gezielt steuern kann.

Migration von Betriebssystemen und Hardware vereinfachen

Ein wesentlicher Vorteil von Virtualisierung liegt darin, dass die Migration von Legacy-Anwendungen auf neue Plattformen vereinfacht wird, um die Leistung, Zuverlässigkeit und Verwaltbarkeit zu erhöhen. Anstatt die Anwendung auf ein neues Betriebssystem migrieren zu müssen, kann sie in Verbindung mit dem bestehenden Betriebssystem in einer virtuellen Partition auf der neuen Plattform untergebracht werden, ohne dass eine Modifizierung der Software erforderlich ist. Diese Strategie dient oftmals dazu, die Nutzungsdauer von Legacy-Anwendungen mit relativ geringen Kosten und Risiken zu verlängern.

Test- und Entwicklungsumgebungen vereinheitlichen

In Entwicklungs- und Testumgebungen bietet Virtualisierung ähnliche Vorteile: Aufeinander folgende Iterationen des Software-Stacks, einschließlich der Produktionsversion, können in eigenständigen virtuellen Partitionen auf derselben Plattform bereitgestellt werden. Dadurch wird die Nutzung der Hardware verbessert und das Lebenszyklusmanagement vereinfacht. In vielen Fällen können IT-Abteilungen dann neue oder aktualisierte Lösungen auf bestehenden Produktionsplattformen testen, ohne Unterbrechungen der Produktionsumgebung zu verursachen. Dadurch wird nicht nur die Migration vereinfacht, sondern es werden auch weitere Kosteneinsparungen ermöglicht, da die Umgebungen nicht dupliziert werden müssen.

Unternehmensflexibilität erhöhen

Es ist weitaus einfacher, eine virtuelle Partition bereitzustellen oder neu zu dimensionieren als eine neue Hardwareplattform zu kaufen und zu implementieren. Die mittlerweile verfügbaren automatischen Bereitstellungslösungen stellen einen weiteren Vorteil dar und können die Reaktionsfähigkeit der IT-Abteilung noch deutlich ausbauen. Unternehmen müssen weniger Plattformen implementieren und können die bestehenden Plattformen flexibler nutzen, um dynamisch auf sich ändernde Anforderungen reagieren zu können.

Eine neue Ära der Computerflexibilität
Virtualisierung für Desktops und Workstations

Intel® Virtualization Technology kann auch in Client-Plattformen integriert werden; die entsprechende Unterstützung ist bereits in 2005 angelaufen. Entscheidende Vorteile sind:

- **Verbesserte Verfügbarkeit und Verwaltbarkeit** – Die wichtigsten Tools für IT-Management und Netzwerksicherheit können in sicheren Partitionen isoliert werden, um den unbefugten Zugriff zu verhindern, die Verfügbarkeit und Wiederherstellungsfunktionen zu verbessern sowie Upgrades, Wartung und Verwaltung ohne Beeinträchtigung der Benutzer durchführen zu können. Diese Funktionen werden die Vorteile der Intel® Active-Management-Technologie noch ergänzen, die voraussichtlich innerhalb desselben Zeitrahmens zur Verfügung stehen wird (weitere Informationen finden Sie unter http://www.intel.com/technology/manage/iamt/).
- **Verbesserte PC-Sicherheit** – Virtuelle Partitionen dienen auch dazu, den Zugriff auf Personal Desktops in Multi-User-Umgebungen zu begrenzen und digitale Angriffe einzudämmen (Viren, Würmer, Hacker etc.). Beispielsweise kann das Surfen im Internet und der Zugriff auf E-Mail in isolierten Partitionen durchgeführt werden, um die Unternehmensanwendungen und -daten vor möglichen Angriffen zu schützen.
- **Höhere IT-Flexibilität** – Mehrere Benutzer können in sicheren, isolierten Partitionen auf einem einzelnen PC unterstützt werden; und verschiedene Betriebssysteme können für die Unterstützung unterschiedlicher Funktionen eingesetzt werden (z. B. Unix für Engineering-Anwendungen, Windows für Personal-Productivity-Software). Persönliche und geschäftliche Anwendungen können auf demselben Rechner bereitgestellt und isoliert werden, um die hohe Sicherheit und Verfügbarkeit zu gewährleisten.
- **Desktop-Flexibilität** – Der Desktop eines Benutzers kann verkapselt und problemlos auf eine sichere, virtuelle Partition auf einem beliebigen anderen PC übertragen werden.

Datenzentrum im Kasten:
Virtualisierung für kleine und mittelgroße Unternehmen

Zurzeit ist Servervirtualisierung vorrangig in Enterprise-Datenzentren zu finden. Im Lauf der Zeit wird sich die Technologie aber mit großer Wahrscheinlichkeit auch in kleineren Unternehmen verbreiten, da es ihnen durch die Isolierung von Anwendungen in virtuellen Partitionen ermöglicht wird, Implementierung zu vereinfachen und eine höhere Zuverlässigkeit, Verfügbarkeit und Sicherheit zu erzielen. Durch die Konfiguration von Sicherungspartitionen wird die Verfügbarkeit zudem noch gesteigert, und Kapazitäten lassen sich flexibel skalieren, indem Partitionen hinzugefügt oder Plattformressourcen neu zugeordnet werden. Wenn ein Unternehmen wächst und weitere Hardwarekapazitäten benötigt werden, können Anwendungen eingekapselt und problemlos in virtuelle Partitionen auf neuen Systemen migriert werden.

Servervirtualisierung auf Servern mit Intel® Architektur

„Zwischen 2003 und 2008 werden sich die Nutzungsraten von Intel® Servern verdoppeln."

– Predicts 2004: Server Virtualization Evolves Rapidly
T. Bittman, Gartner Research Note, 14. November 2003

Zurzeit bieten VMware* und Microsoft* Virtualisierungssoftware an und statten Server mit Intel Architektur mit Funktionen aus, die vormals nur auf Großrechnern verfügbar waren. Viele Unternehmen erzielen Konsolidierungsraten von 20:1 oder sogar 30:1, indem Legacy-Anwendungen auf 4- oder 16-Wege-Plattformen auf Basis von Intel® Prozessoren umgelagert werden.[8]

Im Zuge der Markteinführung von Intel® Dualcore-Prozessoren wird Virtualisierung eine zunehmend wichtige Rolle spielen. In Verbindung mit Hyper-Threading-Technologie‡ von Intel kann eine 2-Wege-Plattform mit Dualcore-Prozessoren bis zu acht Software-Threads unterstützen, eine 4-Wege-Plattform bis zu 16 Threads, eine 8-Wege-Plattform bis zu 32 Threads und eine 16-Wege-Plattform bis zu 64 Threads. Dadurch wird eine größere Flexibilität für die effiziente Unterstützung mehrerer Anwendungen auf einer einzelnen Plattform geboten.

Funktionsweise

Um virtuelle Partitionen auf einem Server zu erstellen, wird ein dünnes Software-Layer, der so genannte Virtual-Machine-Monitor (VMM), direkt auf der Serverhardware ausgeführt. Anschließend können auf den VMM ein oder mehrere „Gast"-Betriebssysteme und Anwendungs-Stacks geladen werden (Abbildung 3).

Der VMM:

- **Emuliert** die gesamte Hardwareumgebung – die Virtual Machine – für jeden Software-Stack. Im Idealfall fällt es dem Betriebssystem und den Anwendungen gar nicht auf, dass sie Hardwareressourcen mit anderen Anwendungen teilen.
- **Isoliert** die Ausführung in jeder Virtual Machine und bietet so hohe Sicherheit und Verfügbarkeit.
- **Ordnet** die Plattformressourcen **zu** (Verarbeitung, Speicher, I/O, Kapazität etc.), um die Systemleistung zu optimieren und Service Level auf die geschäftlichen Anforderungen abzustimmen.
- **Kapselt** die Software-Stacks **ein** (einschließlich Betriebssystem und Statusdaten), so dass sie problemlos kopiert und auf neue Virtual Machines auf derselben oder einer anderen Plattform übertragen werden können.

Alle diese Funktionen sind bereits in den aktuellen Virtualisierungslösungen integriert, aber die ausschließlich auf Software basierenden Lösungen erfordern oftmals äußerst komplexe Prozesse. In enger Zusammenarbeit mit führenden VMM-Anbietern hat Intel neue Architekturstandards definiert, um bessere und kosteneffektivere Virtualisierung mit einer weniger aufwändigen Softwareentwicklung zu ermöglichen. Diese Standards werden als Intel® Virtualization Technology bezeichnet und wurden bereits freigegeben, um schnellere Innovationen für Virtualisierungslösungen auf Enterprise-Plattformen mit Intel Architektur zu ermöglichen.

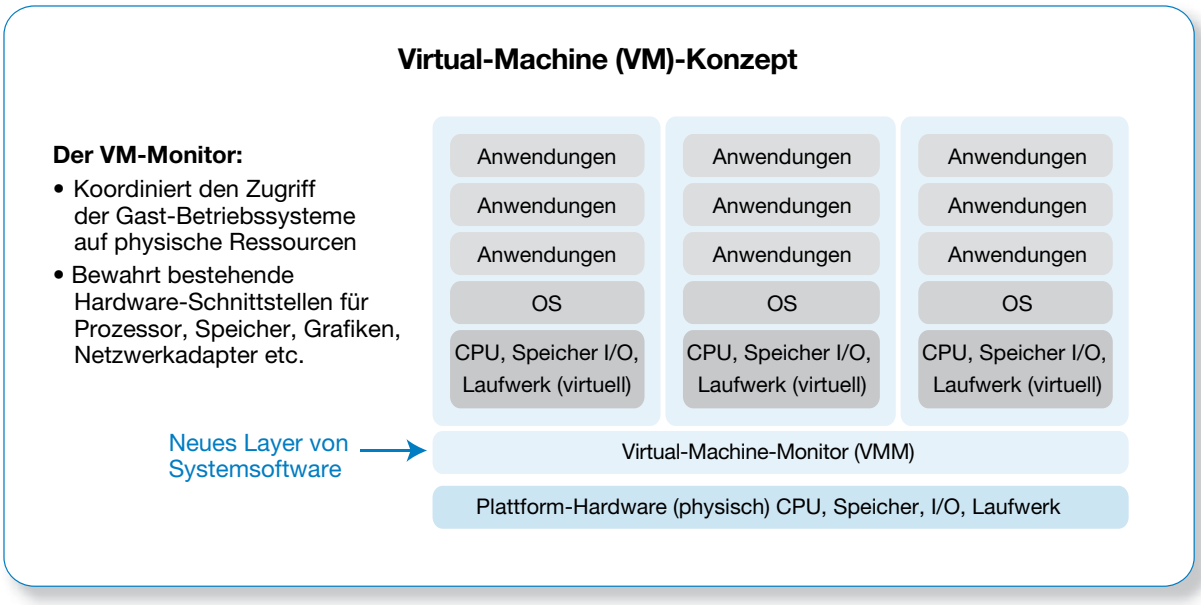

Abbildung 3. Der Schlüssel zu Servervirtualisierung ist der Virtual-Machine-Monitor (VMM), eine Softwareanwendung, die Hardwareressourcen verwaltet und die Anfragen der verschiedenen Betriebssysteme und Anwendungs-Stacks koordiniert.

[8] Weitere Informationen finden Sie auf der Intel Website unter http://www.intel.com/business/bss/products/server/consolidation/index.htm; oder im Intel Whitepaper: *Twenty-to-One Consolidation on Intel® Architecture,* das unter http://cache-www.intel.com/cd/00/00/14/88/148803_148803.pdf zum Download zur Verfügung steht.

Hardware-unterstützte Virtualisierung für Lösungen der nächsten Generation

„Die Vanderpool-Technologie von Intel [mittlerweile als Intel® Virtualization Technology bekannt] wird Produkte wie VMware und Virtual PC effizienter, stabiler, sicherer und flexibler machen.“

– *Intel's Vanderpool Will Spark Virtualization Innovation*
Martin Reynolds, Gartner Research, 21. Januar 2005

In einer typischen Plattformumgebung steuert ein einzelnes Betriebssystem die Plattformressourcen und koordiniert die Anfragen einer oder mehrerer Anwendungen. In einer virtualisierten Plattformumgebung können viele zusätzliche Gast-Betriebssysteme auf der VMM-Software laufen. Um Konflikte zu verhindern, muss der VMM die Kontrolle über kritische Plattformressourcen behalten und darf jedem Gast-Betriebssystem nur die jeweils erforderlichen Steuerungsmöglichkeiten übergeben. Die Effizienz und Integrität dieser Übergaben sind entscheidend, um optimale Leistung und Zuverlässigkeit zu bieten.

Die Herausforderung

In der aktuellen IA-32-Architektur werden alle Softwareprogramme auf einer von vier „Privilegienebenen“ oder „Ringen“ ausgeführt (Ring-0 bis Ring-3). Normalerweise läuft das Betriebssystem in Ring-0, der privilegierte Zugriffsrechte auf die breiteste Palette von Prozessor- und Plattformressourcen beinhaltet. Einzelanwendungen laufen in der Regel in Ring-3, der bestimmte Funktionen (z. B. Speicherzuordnung) einschränkt, da sie andere Anwendungen beeinträchtigen können. Auf diese Weise behält das Betriebssystem die Kontrolle, um einen reibungslosen Betrieb zu ermöglichen.

Da der VMM privilegierte Steuerungsmöglichkeiten für Plattformressourcen benötigt, bestimmt eine Lösung normalerweise, dass der VMM in Ring-0 ausgeführt wird, während die Gast-Betriebssysteme in Ring-1 oder Ring-3 laufen. Moderne Betriebssysteme sind jedoch speziell für die Ausführung in Ring-0 konzipiert, was gewisse Schwierigkeiten mit sich bringt. Eine besondere Bedeutung kommt den 17 „privilegierten“ Instruktionen zu, die kritische Plattformressourcen steuern und in den meisten aktuellen Betriebssystemversionen gelegentlich verwendet werden. Läuft ein Betriebssystem nicht in Ring-0, kann eine dieser Instruktionen einen Konflikt verursachen, der sich in einem Systemfehler oder einer Fehlreaktion niederschlägt.

Software-basierte Lösungen

Es gibt zwei Möglichkeiten, diese 17 privilegierten Instruktionen zu behandeln:

1. **Runtime-Anpassung des Gast-Betriebssystems** – In diesem Fall überwacht der VMM den Betrieb während der Runtime und übernimmt die Steuerung des Prozessors, sobald eine der 17 Instruktionen in einem Gast-Betriebssystem auftritt. Der VMM behebt den Konflikt und übergibt die Kontrolle dann wieder an das Gast-Betriebssystem.
2. **Statische Anpassung des Gast-Betriebssystems (Paravirtualisierung)** – In diesem Fall wird das Gast-Betriebssystem vor der Runtime angepasst.

Beide Ansätze haben Nachteile: Runtime-Anpassung zwingt den VMM dazu, komplexe Problemlösungen im laufenden Betrieb auszuführen, was sich nachteilig auf die Leistung auswirken kann. Paravirtualisierung hindert den VMM daran, nicht angepasste (Legacy-)Gast-Betriebssysteme laufen zu lassen. Beide Ansätze erfordern aufwändige Softwareentwicklungsansätze seitens der VMM- und/oder Betriebssystemanbieter. Zudem ist eine gleichzeitige Aktualisierung von VMM- und Betriebssystemsoftware erforderlich, was zu erhöhten Kosten und mehr Komplexität von IT-Support führt.

Verbesserte Lösungen mit Intel Virtualization Technology

Die Intel® Virtualisierungstechnik schließt die Lücken der aktuellen Virtualisierungslösungen, indem die Kernplattformarchitektur erweitert wird. Entscheidende Verbesserungen umfassen:

1. **Einen neuen, mit höheren Privilegien ausgestatteten Ring für den VMM** – Dadurch können Gast-Betriebssysteme und Anwendungen auf den Ringen laufen, für die sie ursprünglich ausgelegt sind, während der VMM die privilegierte Kontrolle über Plattformressourcen behält. Es werden viele potenzielle Konflikte im Vorfeld vermieden, die Anforderungen an den VMM werden vereinfacht und die Kompatibilität mit nicht angepassten Legacy-Betriebssystemen wird optimiert.
2. **Hardware-basierte Übergänge** – Die Übergabe zwischen VMM und Gast-Betriebssystemen wird von der Hardware unterstützt. Dadurch entfällt die Notwendigkeit für komplexe und rechnerintensive Softwareübergänge.
3. **Hardware-basierter Speicherschutz** – Die Statusdaten des Prozessors werden in dedizierten Adressspeichern für den VMM und für jedes Gast-Betriebssystem verwahrt. Dadurch können Übergänge beschleunigt und die Prozessintegrität sichergestellt werden.

Diese Verbesserungen werden sowohl für Softwareanbieter als auch IT-Abteilungen eine Reihe von Vorteilen mit sich bringen, z. B.:

- **Geringere Kosten und Risiken für IT-Abteilungen** – Die Unabhängigkeit von VMM- und Betriebssystemsoftware verbessert die Interoperabilität mit nicht angepassten Legacy-Betriebssystemen. Zudem müssen Upgrades und Patches im Datenzentrum nicht mehr synchronisiert werden. Die Kosten für Supportleistungen werden gesenkt, und IT-Abteilungen können eine weitaus größere Palette von Betriebssystemversionen auf einer konsistenten Hardware- und VMM-Plattform unterstützen.
- **Höhere Zuverlässigkeit und Verfügbarkeit** – Da der VMM kleiner, weniger komplex und unabhängig von den Gast-Betriebssystemen ist, ist es weniger wahrscheinlich, dass Softwarekonflikte auftreten, welche den Betrieb andernfalls verlangsamen oder unterbrechen können.
- **Verbesserte Sicherheit** – Die Verwaltung von VMM-Übergängen in den Hardwarekomponenten – und nicht in der Software – trägt dazu bei, die logische Isolierung der virtuellen Partitionen zu verstärken. Der kleinere und weniger komplexe VMM bietet zudem weniger Angriffspunkte für Software-basierte Angriffe.
- **Vereinfachte VMM-Entwicklung** – Eine wesentliche Zielsetzung der Intel Virtualisierungstechnik ist es, VMM-Software unabhängig von Betriebssystemsoftware zu machen. Dadurch entfällt für VMM-Anbieter die ressourcenintensive Aufgabe, ihren Code im Hinblick auf Patches und Upgrades des Betriebssystems anzupassen. Auch bestehende Lösungen können die Vorteile der neusten Plattformfunktionen relativ problemlos und ohne aufwändigen Bedarf an VMM-Entwicklung und -Anpassung nutzen. Unternehmen können davon ausgehen, von der schnelleren Marktreife der neuen Funktionsmerkmale zu profitieren.

Kontinuierliche Innovation

„…Unternehmen sollten die Virtualisierungsangebote und -strategien ihrer Serviceanbieter verstehen lernen und zu einem Entscheidungskriterium bei der Auswahl eines neuen Servers machen.“

– *Predicts 2004: Server Virtualization Evolves Rapidly,* T. Bittman, Gartner Research Note, 14. November 2003

Intel ist derzeit dabei, die Intel® Virtualisierungstechnik in alle Serverplattformen zu integrieren.

- Die Unterstützung von Systemen auf der Basis von Intel® Itanium® 2 Prozessoren wurde in der zweiten Jahreshälfte 2005 implementiert.
- Die Unterstützung von Systemen auf der Basis von Intel® Xeon® Prozessoren 64-Bit ist für die erste Jahreshälfte 2006 vorgesehen.
- Intel beschleunigt zudem die Integration in Client-Plattformen, und die entsprechende Unterstützung wurde für Desktops in 2005 eingeführt und ist für Laptops in 2006 zu erwarten (siehe Kasten auf Seite 5, *„Eine neue Ära der Computerflexibilität”*).

Die Intel Virtualisierungstechnik stellt den ersten Schritt in einer Reihe von innovativen Plattformentwicklungen dar, die zunehmend mehr Unterstützung für ausgereifte Virtualisierungslösungen bieten werden. Spezialisten bei Intel bewerten derzeit Alternativen für die I/O-Virtualisierung, die es den VMMs erleichtern sollen, die I/O-Bandbreite für verschiedene Anwendungen auf derselben Hardwareplattform verwalten und zuordnen können.

Intel arbeitet zudem weiterhin mit führenden Entwicklern von VMMs und Betriebssystemen (sowohl Drittanbietern als auch Open-Source-Anbietern) zusammen, um eine solide Grundlage für die Entwicklungsarbeit zu schaffen und sicherzustellen, dass die Neuerungen der nächsten Generation den besonders kritischen Anforderungen der Geschäftskunden Rechnung tragen. In den kommenden Jahren werden Virtualisierungslösungen auf Intel® Architektur weitergehend verbessert werden und IT-Abteilungen zunehmend leistungsfähige Tools an die Hand gegeben, um Anwendungen konsolidieren, Kosten reduzieren und die Unternehmensflexibilität optimieren zu können.

Die Intel Virtualisierungstechnik ist Bestandteil von Intels beständigem Streben, ein umfassendes Angebot marktführender Plattformtechnologien für Intel-basierte Server nach Industriestandard bereitzustellen. Beispiele für die aktuell erhältlichen Technologien umfassen Hyper-Threading-Technologie‡ (siehe oben) und die Intel® Extended-Memory-64-Technologie, die optimierte Unterstützung sowohl für 32-Bit- als auch für 64-Bit-Anwendungen auf einer einzigen Plattform bietet. Zukünftige Innovationen umfassen die Intel® Active-Management-Technologie und LaGrande-Technologie mit einem Schwerpunkt auf Plattformverwaltung beziehungsweise Sicherheit. Durch den kombinierten Einsatz dieser ausgereiften Plattformfunktionen werden IT-Abteilungen dabei unterstützt, selbst ausgesprochen kritische Aufgaben bewältigen und den Unternehmenswert ihrer IT-Investitionen erhöhen zu können.

Schlussfolgerung

„…im Lauf der nächsten Jahre wird Virtualisierung unsere Sichtweise auf Enterprise-Infrastruktur neu definieren und ein reichhaltigeres Angebot neuer Lösungen zur Auswahl stellen.”

– *Betting on Virtualization*, Mark Gibbs, Network World, Network World, 15. November 2004

Virtualisierung ist die Technologie der Zukunft für optimierte Hardwarenutzung und Flexibilität im Datenzentrum. Intel Architektur unterstützt bereits heute flexible und kosteneffiziente Virtualisierungslösungen unter Verwendung der Softwareprodukte von VMware und Microsoft. Diese Lösungen sorgen bereits in den unterschiedlichsten Produktionsumgebungen für erhebliche Produktivitätssteigerungen.

Die Intel Virtualisierungstechnik wird diese Vorteile noch verstärken, indem Plattformen auf Basis von Intel® Prozessoren die Virtualisierung nahtlos integrieren und unterstützen. Durch die Schaffung einer neuen Privilegienebene für VMM-Software und die Hardware-basierte Unterstützung zentraler Virtualisierungsfunktionen vereinfacht die Intel Virtualisierungstechnik die Entwicklung und Wartung von VMMs, verbessert die Interoperabilität mit Legacy-Betriebssystemen, erhöht die Sicherheit und Zuverlässigkeit der Systeme und reduziert die mit der Implementierung verbundenen Kosten und Risiken.

Die Intel Virtualisierungstechnik stellt eine der zahlreichen im Lauf der nächsten Jahre von Intel zu erwartenden innovativen Plattformverbesserungen dar, die wichtige Unterstützung für die erweiterte Flexibilität, Verwaltbarkeit und Sicherheit von Datenzentren bieten werden. Neben einer kontinuierlichen Steigerung der Gesamtleistung und optimierten Preis-Leistungs-Verhältnissen werden diese Innovationen den Unternehmenswert des gesamten Angebots an Servern mit Intel Architektur erhöhen.

Weitere Informationen zur Intel® Virtualization Technology finden Sie auf der Intel Website unter: http://www.intel.com/technology/ computing/vptech/.

‡ Hyper-Threading-Technologie erfordert ein Computersystem mit einem Intel® Pentium® 4 Prozessor mit mindestens 3.06 GHz, einem Chipsatz und BIOS, welche diese Technologie nutzen, und einem Betriebssystem, das die erforderlichen Optimierungen für diese Technologie enthält. Die Leistungseigenschaften sind je nach verwendeter Hardware und Software unterschiedlich. Weitere Informationen erhalten Sie unter http://www.intel.com/info/hyperthreading/.

304266-001-DE