# Brennpunkt Windows Server „Longhorn“: Thomas Kuberek im Gespräch mit Jochen Katz

05.04.2007

**Jochen Katz** ist als Produkt Manager Windows Server für die Microsoft Deutschland GmbH tätig.

**http://technet.microsoft.com**

**Thomas Kuberek** ist Mitbegründer von MCSEboard.de, dem führenden deutschen Diskussionsforum zu den Themen Microsoft Zertifizierungen und Windows Problemlösungen.

**www.mcseboard.de**

Microsoft CommunityCast

**Was ist neu am Windows Server „Longhorn“?**

Konkret kann man das gut an drei Bereichen festmachen: Der erste ist effizientere Administration, der zweite ist stärkerer Schutz und der dritte ist größere Flexibilität.

**Wie ist es einfacher geworden, den neuen Server zu administrieren und zu installieren?**

Oft haben Administratoren gesagt, dass es schön wäre, wenn sie die CD einlegen könnten und die Installation danach nahezu von selbst laufen würde. Genau das ist jetzt auch der Fall. Beim Windows Server „Longhorn“ kann man die CD einlegen, gibt noch den Produkt-Key ein und dann installiert der Server sich selber mit den Default-Einstellungen. Wenn der Server fertig installiert ist, gibt man noch die Parameter ein, wie zum Beispiel, ob der Server Mitglied in der Domain sein soll, ob er eine feste IP Adresse haben soll, welche Rollen er besitzen soll und so weiter. Das Zweite, was viel einfacher geworden ist, ist die Administration. Bisher musste man sieben verschiedene Administrationstools bedienen, um den Windows Server verwalten zu können. Das ist jetzt alles in einem Tool-dem Server Manager-zusammen gefasst. Man hat vom Einlegen der CD bis zur vollständigen Konfiguration und Administration des Servers mit diesem Servermanager nur noch eine Anlaufstelle und darin liegt eine ganz starke Vereinfachung.

**Das heißt, es ist aus zwei Gründen einfacher für den Administrator geworden. Erstens erfolgt die Grundinstallation mit den Default-Einstellungen nahezu automatisch. Ich muss jetzt nicht mehr interaktiv sagen, „diese Werte nehmen“, sondern der Server installiert sich selber mit Default-Einstellungen, die ich später an mein Netzwerk anpassen kann. Das andere ist, dass die tägliche Verwaltungsarbeit einfacher wird, weil ich mich nicht mehr mit sieben Tools auseinandersetzen und beschäftigen muss, sondern eine zentrale Anlaufstelle habe, von der aus ich meinen Server administrieren kann.**

**Stichwort Administration: Es wird eine neue Kommandozeilenoberfläche geben, die deutlich mächtiger ist, als das, was wir bisher haben. PowerShell heißt diese Kommandozeilenumgebung. Was kann PowerShell? Wie kann diese Kommandozeilenoberfläche mein Leben als Administrator besser und einfacher machen?**

PowerShell ist eine neue Kommandozeilenumgebung und das Besondere daran ist, dass sie objektorientiert ist, so dass man alle Vorteile nutzen kann, die Objektorientierung bietet. PowerShell erlaubt zudem die Integration in die anderen Microsoft Server, wie zum Beispiel Microsoft Operation Manager 2007, oder System Center Virtual Machine Manager, die man dann auch skripten kann. Damit hat man die Möglichkeit, die eigene IT zu automatisieren. Dadurch spart natürlich der Administrator viel Zeit. PowerShell ist auch jetzt schon verfügbar für Windows XP, für Windows Vista, für Windows Server 2003 und dann auch für Windows Server „Longhorn“. Man kann sich PowerShell jetzt schon herunterladen und ausprobieren unter: www.microsoft.com/powershell .

**Mit Sicherheit ist auch gerade im Kundenumfeld eine stärker automatisierte Umgebungen sehr interessant, weil sie natürlich auf Kundenseite bzw. auf Seiten der Dienstleister die Arbeit effizienter gestaltet und dadurch Kosten spart. Mit Sicherheit ist das ein tolles Feature, das ihr da eingebaut habt.**

**Beim Windows Server 2003 wurde bereits erheblich viel Wert auf ein sicheres Betriebssystem gelegt. Der Windows Server 2003 wurde, im Gegensatz zu der 2000er Version gezielt auf höhere Sicherheit, schon bei der Installation ausgelegt, so dass viele Dienste, welche nicht grundsätzlich benötigt werden per Default abgeschaltet sind und erst gezielt aktiviert werden müssen. Bei dem Windows Server „Longhorn“ soll auch hier noch deutlich weiter gegangen worden sein, zum Beispiel durch ein restriktiveres Dienste-Modell. Wie sieht das aus?**

Zum Beispiel kannst Du jetzt ausschließen, dass neue Hardware installiert wird. Du kannst verhindern, dass Leute mit USB Sticks geistiges Eigentum der Firma entwenden. Manche Unternehmen sind bisher den Weg gegangen und haben mit Heißkleber die USB Ports versiegelt. Das kann man jetzt durch den Windows Server „Longhorn“ von Vornherein verhindern. Eine weitere Neuerung ist auch ein viel restriktiveres Dienste-Model. Die Dienste haben weniger Rechte und die Rechte sind genauer segmentiert. Ein Dienst darf daher im Wesentlichen jetzt nur noch das, was er auch „dürfen muss“, um seine Aufgaben zu verrichten. Es wird auch den Windows Server Core-eine eigene Edition vom Windows Server-geben. Das ist ein Server, der nur noch eine Kommandozeile besitzt. Diese Edition hat keine graphische Oberfläche und bringt dadurch auch viel weniger Code mit, was die Angriffsbasis bei diesem

Server stark verkleinert. Der Server kann die Rollen FILE, PRINT, DHCP, DNS und ACTIVE DIRECTORY.

**Es ist heute im Allgemeinen üblich, dass eine große Zahl der Mitarbeiter mobile Geräte benutzt. Wenn so ein mobiler User sich nach langer Zeit wieder im Firmennetzwerk anmeldet, kann es durchaus sein, dass er die Sicherheitsanforderungen des lokalen Netzes (Patch-Level/ aktuelle Virensignaturen) nicht erfüllt. Dies ist ein nicht zu unterschätzendes Risiko. Der Windows Server „Longhorn“ soll eine Technologie mitbringen, welche dieses Problem adressiert. Wie wird das aussehen?**

Also das ist natürlich ein Punkt, der bei Kunden ganz stark brennt. Was wir da getan haben, nennt sich Network Access Protection. Das ist ein Bestandteil vom neuen Windows Server, mit dem man die Möglichkeit hat, einen mobilen Client zu validieren, ob er die Sicherheitspolicies des Unternehmens erfüllt. Network Access Protection überprüft z.B., ob eine aktuelle Virensignatur und der aktuelle Patch-Status auf dem PC gegeben ist. Falls nicht, kommt dieser in einen abgeschirmten Bereich und bekommt dort die neuen Patches und die neue Antivirensignatur installiert. In einem weiteren Schritt wird er noch einmal validiert, ob er jetzt der IT Richtlinie entspricht und nur dann bekommt er den Zugang von Außen auf das Unternehmensnetzwerk. Das ist natürlich etwas, das noch mehr Sicherheit in dem Netzwerk erzeugt.

**Das bedeutet, dass auch hier wieder schon per Default ein höherer Sicherheitsstatus beim Betriebssystem mit dabei ist und ich mich nicht mehr darum kümmern muss, Drittanbieterlösungen dazuzukaufen und zu implementieren.**

Du bekommst Network Access Protection mit dem Betriebssystem mit und kannst es dir dann nach Deinen Wünschen konfigurieren.

**Ausfallzeiten in Rechenzentren kosten eine Menge Geld, weshalb der Trend immer mehr zu hochverfügbaren Lösungen geht. Der Windows Server 2003 war in der Enterprise Version bereits clusterbar. Allerdings gab es dabei einige Einschränkungen was zum Beispiel die räumliche Entfernung der Knoten untereinander anging. Wurde hier etwas unternommen um das Betreiben von Clustern zu vereinfachen?**

Es war ja bisher so, dass es einen relativ fundierten Wissensstand erforderte, ein Cluster einzurichten. Jetzt wurde das komplett überarbeitet. Vieles wurde durch einen Assistenten einfacher gemacht, so dass man jetzt durch den Prozess einfach durchgeführt wird. Bisher war es zudem so, dass die zwei Cluster im gleichen Sub-Netz sein mussten. Diese Beschränkung gibt es jetzt nicht mehr. Damit ist jetzt auch Geo-Clustering einfach möglich. Man kann einen Server in den USA stehen haben und einen in Europa, man kann die Heartbeat-Timeouts einstellen und so eben wirklich auch über zwei Kontinente Server clustern.

**Bisher war das ja ein Problem, dass Server, die im Cluster liefen, recht nah beieinander stehen mussten. Das macht die Sache jetzt natürlich einfacher. Womit wir auch schon bei dem nächsten Thema wären: Zweigstellen anbinden. Auch da habe ich gehört, dass sich Einiges getan hat, um die Anbinden von Zweistellen einfacher zu machen.**

Das ist richtig. Zweigstellen sind eine der ganz großen Herausforderungen der IT. Man kann sagen, dass 50% der IT-Kosten bei Großunternehmen für die Verwaltung von Zweigstellen benötigt werden. Hier gibt es im Windows Server „Longhorn“ verschiedene Ansätze, um Kunden zu helfen. Das Erste ist natürlich Virtualisierung. Diese ist jetzt auch im Windows Server „Longhorn“ integriert. Mit Virtualisierung hat man die Möglichkeit, in der Zweigstelle Server nur noch virtuell laufen zu lassen. Im Falle eines größeren Problems mit dem Server muss nicht ein Mitarbeiter physikalisch vor Ort hinfahren, sondern kann die virtuelle Maschine einfach austauschen, sie sich „zurückholen“, bei sich schnell aufsetzen oder neue Administrationseinstellungen machen und dann wieder zurück in die Zweigstelle schicken. Das Zweite ist der Read-Only-Domain-Controller. Der Server ist in der Zweigstelle teilweise nur bedingt überwacht und jetzt besteht die Gefahr, dass sich jemand am Domaincontroller zu schaffen macht und dadurch evtl. falsche Einstellungen oder falsche Daten des Active Directory ins ganze Netzwerk repliziert werden. Der Read-Only-Domain Controller ist „nur eine Art Puffer“. Er kann lesen, aber keine Änderungen zurück replizieren. Zusätzlich hat er im Standard auch keine Administratoren- und keine Benutzerpasswörter gespeichert. Wenn einem jetzt jemand zum Beispiel in der Zweigstelle den Domain Controller klaut, weil da oft die physikalische Sicherheitsumgebung nicht so hoch sind, wie in der Hauptstelle, ist das Risiko des Datenverlusts damit geringer. Das zweite Feature in diesem

Zusammenhang ist auch noch zusätzlich der BitLocker. BitLocker verschlüsselt die Festplatte sowohl auf der Systempartition, wie auch auf den anderen Partitionen. Dadurch kann ein Dieb, selbst wenn der Server im Offlinebetrieb geklaut werden sollte, mit den Daten auf dem Server nichts mehr anfangen, dank der Verschüsselung. Damit wird ermöglicht, die in der Zweigstelle etwas geringere physikalische Sicherheitsanforderung durch eine höhere Sicherheit des Servers zu kompensieren.

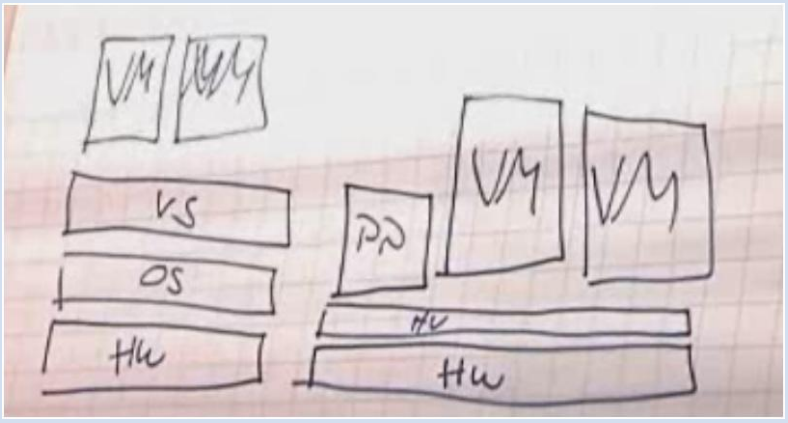
**Ich hatte einmal einen Kunden, der eigene Netzte auf einer Baustelle betreut hat und dem ist es zwei Mal passiert, dass Server komplett gestohlen wurden. Es ist klar, dass es damals nicht um die Serverhardware ging, sondern um die Planungsdaten. Wenn der Server hochverschlüsselt ist, verliert man zwar die Hardware, aber die Daten sind geschützt und das ist das Wichtigste daran.**

Genau. Und da sind eben BitLocker und Server Core zwei ganz wichtige Features.

**Du hast in dem Zusammenhang Zweigstellen auch schon die Virtualisierung angesprochen. Auch da hat sich etwas getan. Willst du uns kurz erzählen, was sich da getan hat?**

Sehr gern. Bisher war das Virtualisierungsprodukt Microsoft für den Serverbereich der Virtual Server. Jetzt wird Virtalisierung in das Serverbetriebssystem integriert werden. Virtualisierung wird eine eigene Rolle vom Windows Server werden. Ich versuche das einmal folgendermaßen zu verdeutlichen: Das alte Bild sieht wie folgt aus: Wir hatten die Hardware, auf dieser lief dann der Windows Server, darauf läuft der Virtual Server und in dem Virtual Server sind die einzelnen virtuellen Maschinen. Jetzt (Windows Server „Longhorn) gibt es einen Hypervisor. Der Unterschied in der Architektur ist ein sehr großer. Wir haben hier wiederrum die Hardware, und darauf den Hypervisor. Der Hypervisor ist eine ganz dünne Schicht Code (ca. 200- 400 KB groß)-das ist jetzt schon die Virtualisierungsschicht. Auf dieser Virtualisierungsschicht gibt es eine Partition-die sogenannte Parent Partition. Diese Parent Partition ist ein Windows Server „Longhorn“, der unter anderen den Hypervisor mit den nötigen Treibern versorgt. Daneben laufen auf dem Hypervisor beliebig viele andere virtuelle Maschinen. Diese können einen Windows Server als Betriebssystem haben oder auch andere x86 oder auch x64 Bit Betriebssysteme. Diese komplett neue Architektur ist eingebaut im Betriebssystem als eigene Rolle im Windows Server. Im

Virtual Server kann man aktuell ausschließlich 32 Bit Betriebssysteme virtualisieren. Mit dem Hypervisor können wir 32 Bit als auch x64 Bit Betriebssysteme. Ganz wichtig ist, dass der Hypervisor selber x64 Hardware benötigt. Damit kann dann Virtualisierung weit skaliert werden.




**Heißt das, dass der Windows Server „Longhorn“ nur als 64 Bit Plattform verfügbar sein wird, oder weiterhin auch als 32 Bit?**

Gut, dass Du das fragst. Windows Server „Longhorn“ gibt es als 32Bit, x64Bit und auch als Itanium Edition. Virtualisierung benötigt x64 Bit. Mit dem Windows Server „Longhorn“ R2 in zwei Jahren nach Longhorn, wird es nur noch 64 Bit Editionen geben.

**Die Terminal Services sind ja auch schon seit langem Produktbestandteil des Windows Servers gibt es da etwas Neues? Hat sich da etwas getan?**

Ja, also auch da tut sich sehr viel. Das wichtigste ist das Terminal Services Remote Programms. Bisher war teilweise Verwirrung bei vielen Anwendern da. Sie hatten zwei Desktops auf dem Bildschirm, einen von den Terminal Services und einen vom Client selber. Jetzt ist es möglich, dass Du nur eine einzelne Applikation in ihrem Applikationsfenster von dem Terminal Server auf den Client-Desktop zeigst. Dadurch hat der Benutzer den Eindruck, dass das Programm wie jedes andere auf dem Client läuft.

**Sehr gute Lösung. Bei den Terminaldiensten hatte ich bei vielen Kunden das Problem, dass die Anwender den Unterschied zwischen dem Arbeiten auf der lokalen Maschine und dem Arbeiten in einer Terminalsession nicht wirklich verstanden haben. Jetzt wird das Programm, wenn ich das richtig verstanden habe, ausgeliefert wie eine lokale Applikation. Für den User gibt es optisch**

**keinen Unterschied mehr. Das ist eine tolle Lösung, weil natürlich die Produktivität meiner Mintarbeiter dadurch steigt.**

Genau. Die Produktivität der Mitarbeiter steigt und Helpdesk Kosten werden gespart, weil natürlich auch die Anzahl der Anfragen für zum Beispiel Passwortverlust für die Terminalsitzung zurückgeht.

**Auch der Zugriff auf die Terminalservices von außerhalb des Unternehmensnetzes soll deutlich verbessert worden sein. Was hat sich hier getan?**

Man kann jetzt auch über den PC über http auf das Unternehmensnetz zugreifen und braucht also auch keinen VPN Tunnel mehr. Man kann ganz normal durch die Firewall mit http auf die Terminal Services zugreifen.  VPN hat teilweise Helpdesk Kosten verursacht.

**Das ist mit Sicherheit eine schöne Sache. Es vereinfacht auch die Administration, weil ich keine Infrastruktur für meine VPN Tunnel bereitstellen muss. Tolle Sache. Die brennende Frage ist jetzt natürlich: Wann kriegen wir es? Wann wird der neue Server verfügbar sein?**

In der zweiten Hälfte dieses Jahres wird der Windows Server fertig gestellt sein.

**Es gab ja für Windows Vista eine sehr erfolgreiche, öffentliche Beta. Wird es so etwas auch für den Windows Server „Longhorn“ geben?**

Ja. Es ist uns sehr wichtig, dass sich Administratoren so früh wie möglich mit dem neuen Server vertraut machen können. Es würde mich daher natürlich sehr freuen, wenn sich viele den Windows Server „Longhorn“  mal anschauen und testen.

**Sagst Du uns noch, wo wir uns für die Beta anmelden können?**

Es gibt folgenden Service: Wenn Ihr sofort die Information haben wollt, wenn die Beta verfügbar ist, dann könnt Ihr Euch anmelden und werdet dann automatisch benachrichtigt, wenn die Beta für den Windows Server „Longhorn“ zur Verfügung steht: http://www.microsoft.com/germany/technet/beta