

Schwachstellen bei der Ressourcenoptimierung im virtuellen Raum

Steve Hampicke

Die Virtualisierung von physischen Systemen gewinnt mehr und mehr an Bedeutung. Mittlerweile ein alter Hase unter den Virtualisierungsarten ist die Servervirtualisierung. Sie hat sich bereits in Unternehmen und Behörden etabliert und verdrängt erfolgreich die „alte“ physische Serverstruktur.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Grundlagen zu den Speicherfunktionen (Memory Overcommitment, Ballooning) der Virtualisierungslösung VMware vSphere 4
- Sicherheitsanalyse der oben genannten Funktionen auf Basis des Bausteins der Virtualisierung vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

WAS SIE VORHER WISSEN SOLLTEN...

- Grundkenntnisse zum Thema Virtualisierung allgemein
- Grundkenntnisse zum Thema Sicherheit

Unternehmen und Behörden versprechen sich durch den Einsatz der Virtualisierung Kosteneinsparungen durch eine Reduzierung der Server-Hardware, Senkung der Energie und Minimierung des benötigten Platzes im Rechenzentrum. Doch die Virtualisierung von Servern bringt durch die neuen Techniken auch zusätzliches Gefahrenpotential gegenüber physischen Servern mit sich.

Untersuchung sicherheitsrelevanter Eigenschaften von Memory Overcommitment und Ballooning

Aktuell eine der am meisten verwendeten Servervirtualisierungslösungen kommt von der Firma VMware und ist momentan in der Version vSphere 4 erhältlich. Die Lösung besteht hauptsächlich aus dem ESX- und einem Verwaltungsserver (vCenter Server) und nutzt Technologien wie

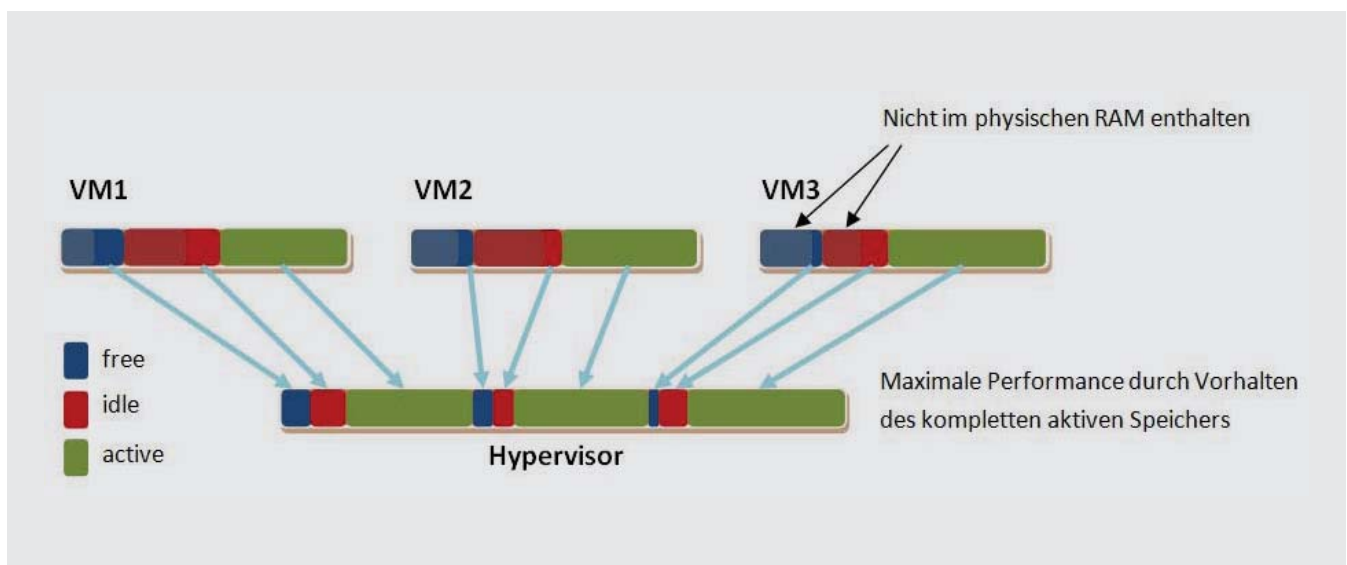


Abbildung 1. „total“ Memory Overcommitment

Snapshots, Memory Overcommitment oder das *Ballooning*. Administratoren wird dadurch eine Vielzahl an Planungs- und Konfigurationsmöglichkeiten für den Einsatz der neuen Technik geboten. Zunächst eine kurze Einführung.

Das *Memory Overcommitment*, die Überbuchung des Arbeitsspeichers, ist ein wichtige Technologie bei der Arbeit mit virtuellen Welten. Da sie mit einer Speichermanagementtechnik des *ESX(i)* realisiert wird, kann die virtuelle Maschine mehr Speicher nutzen, als physisch vorhanden ist. Mit dem „totalen“ *Memory Overcommitment* und dem „aktiven“ *Memory Overcommitment* gibt es zwei Arten. Unter „total“ *Overcommitment* versteht man, was gemeinhin als *Memory Overcommitment* bezeichnet wird. Es ergibt sich aus der Summe des konfigurierten Speichers der virtuellen Maschinen und durch den verfügbaren Host-Speicher für die virtuellen Maschinen (Abb. 1).

Die zweite Art, das „aktive“ *Memory Overcommitment*, ergibt sich aus der Summe des aktiven Speichers der virtuellen Maschinen. Ist das Ergebnis größer Eins, so besteht eine hohe Wahrscheinlichkeit, dass es zu einem Leistungsabfall der virtuellen Maschine kommt (Abbildung 2). Tritt dieser hohe Leistungsabfall auf, sollte die virtuelle Maschine mittels *vMotion* auf einen anderen Host übertragen werden.

Da der Reservierungsparameter eine große Bedeutung in diesem System hat, sollte er von Anfang an geschickt gewählt werden. Er sollte immer den kompletten aktiven Speicher im physischen Speicher haben, um somit eine gute Performance erreichen zu können. Der Speicher, der sich im Leerlauf befindet und der freie Speicher können durch das *Ballooning* genutzt werden.

Ballooning-Technik ermöglicht eine dynamische Anpassung der virtuellen Umgebung. Dies geschieht durch den *Balloon*-Treiber (*vmmemctl*), der durch die *VMwareTools* in das jeweilige Betriebssystem einer virtuellen Maschine integriert wird. Der Treiber belegt gezielt den Hauptspeicher, der vom Gast-Betriebssystem am wenigsten benutzt wird. Das Gast-Betriebssystem muss nun seinen eigenen Speicherverwaltungsalgorithmus nutzen. Sollte der Speicher zu knapp sein, wird festgelegt, welche Seiten zurück-

gewonnen werden und welche auf die virtuelle Festplatte auszulagern sind. Der durch den *Balloon*-Treiber belegte Speicherplatz wird durch den Hypervisor erkannt und kann nun an andere virtuelle Systeme vergeben werden. Der Ablauf ist in Abbildung 3 dargestellt. Speicherengpässe können so kurzzeitig ausgeglichen werden.

Vorgehensweise:

- *Balloon*-Treiber belegt Speicher
- *Balloon*-Treiber markiert belegten Speicher
- Gast kann anderen Speicher zurückfordern
- *Balloon*-Treiber teilt Hypervisor mit, welcher Speicher ihm zugeteilt ist
- Hypervisor macht den zugeteilten Speicher frei
- Hypervisor besitzt nun mehr freien physischen Speicher

Mithilfe des Parameters *sched.mem.maxmemctl* kann die Summe des Speichers bestimmt werden, die vom *Balloon*-Treiber maximal eingenommen werden kann. Dieser Parameter kann mittels *vSphere Client* geändert werden. Eine Anwendungsempfehlung hierfür ist:

- Auf allen virtuellen Maschinen sollten die *VMwareTools* installiert werden und das *Ballooning* aktiviert werden.
- Das Gast-Betriebssystem sollte außerdem genug Platz für die Auslagerungsdatei besitzen.

Potentielle Gefahren

Die Auswirkungen der Servervirtualisierung auf administrative und betriebliche Prozesse können beträchtlich sein. Aus der Sicherheitsperspektive betrachtet, bringen die neuen Techniken, wie das *Memory Overcommitment* und *Ballooning*, ein zusätzliches Gefahrenpotential gegenüber physischen Servern mit sich. So werden zum Beispiel zunehmend mehr firmenkritische Anwendungen in einer virtuellen Umgebung betrieben. Welche Virtualisierungssoftware dabei von den

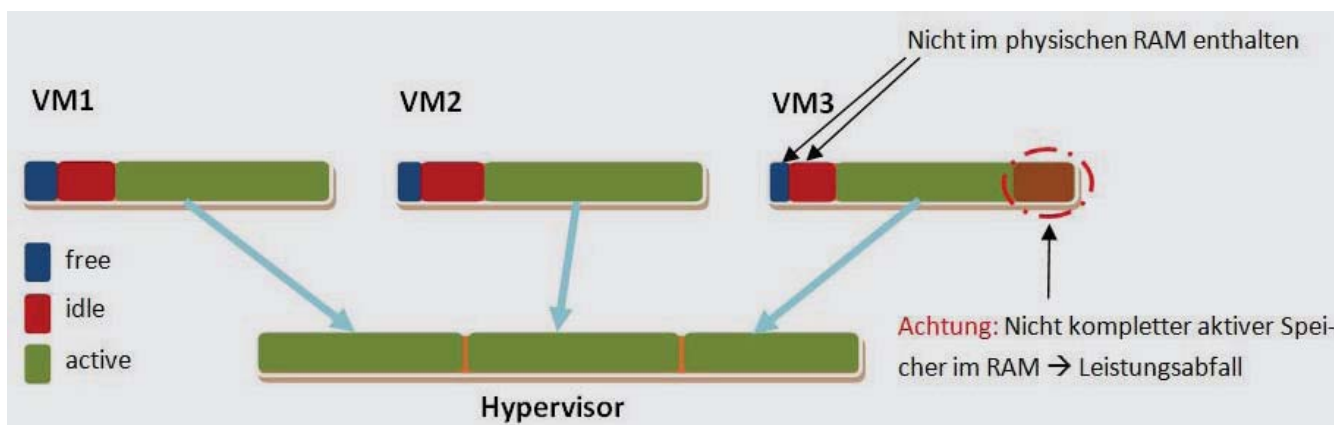


Abbildung 2. „aktives“ *Memory Overcommitment*

Unternehmen genutzt wird, hat ITIC und Stratus untersucht und dabei herausgefunden, dass 71 Prozent der Unternehmen die Software von VMware einsetzt. 28 Prozent setzen auf Microsoft und 9 Prozent wenden Virtualisierungslösungen von Citrix an. Laut einer aktuellen Umfrage von ITIC und Stratus, bei der 500 IT-Experten aus 19 Ländern befragt wurden, gaben 42% an, dass ein Viertel bis zur Hälfte der Anwendungen in ihren Unternehmen unternehmenskritisch seien. Bei PC-WARE beobachten wir einen ähnlichen Trend. In 78% der Unternehmen laufen diese kritischen Anwendungen auf virtuellen Maschinen. Um deren Sicherung gewährleisten zu können, ist es für jeden IT-Manager essentiell zu wissen, wo Gefahrenquellen liegen können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt hierzu folgende Gefährdungsbereiche in virtuellen Infrastrukturen an:

- Organisatorische Mängel
- Menschliches Fehlverhalten
- Technisches Versagen
- Vorsätzliche Handlungen

In der Abbildung 4 ist eine Art zusammenfassendes Angriffsszenario zu sehen.

Organisatorische Mängel

Da virtuelle Infrastrukturen meist eine hohe Komplexität aufweisen, sind eine gute Planung sowie eine Analyse der Rahmenbedingungen unausweichlich. Bereits hier können potentielle Gefahren entstehen. Bevor man an die richtige Auswahl des Virtualisierungsservers denkt, ist es wichtig zu wissen, ob die einzusetzenden

Anwendungen in einer virtuellen Maschine auch vom Hersteller der Anwendungssoftware unterstützt werden. Möglicherweise kann es passieren, dass der Hersteller keinen Support anbietet, sobald das Produkt in einer virtuellen Umgebung betrieben wird. Ist dies geklärt, kommt die Wahl der Virtualisierungssoftware und in diesem Zusammenhang, die Auswahl des richtigen Servers. Dabei spielt die Planung der Kommunikationsverbindungen zum Server eine wichtige Rolle. Die Entwicklung einer Strategie für das Netz- und Systemmanagement ist ebenfalls nicht außer Acht zu lassen. Für den richtigen Umgang mit den einzelnen Planungsschritten empfehlen sich die IT-Grundschutz-Kataloge des BSI. Sie listen die einzelnen Gefährdungen und die dazu passenden Gegenmaßnahmen auf und vermitteln so einen sicheren IT-Betrieb.

Menschliches Fehlverhalten

Menschliche Fehlhandlungen sind immer eine Gefahrenquelle innerhalb von IT Infrastrukturen und deren Management. Häufig werden Konfigurationen unzureichend getestet oder Administratoren unzureichend ausgebildet. Die Zugangsrechte zu virtuellen Maschinen und deren Anwendungen sollten nur in dem Umfang eingeräumt werden, wie sie für die Erfüllung der Aufgaben erforderlich sind. Dabei kann eine fehlerhafte Administration der Rechte zu Betriebsstörungen und Sicherheitslücken führen.

In Verbindung mit dem *Ballooning* gibt es die Gefahr, dass Benutzer die Gastwerkzeuge beenden und somit den *Balloon*-Treiber deaktivieren. Dies kann zu einem Speicherengpass der virtuellen Maschinen führen. Im Normalfall kann nur die Gruppe der Administratoren die

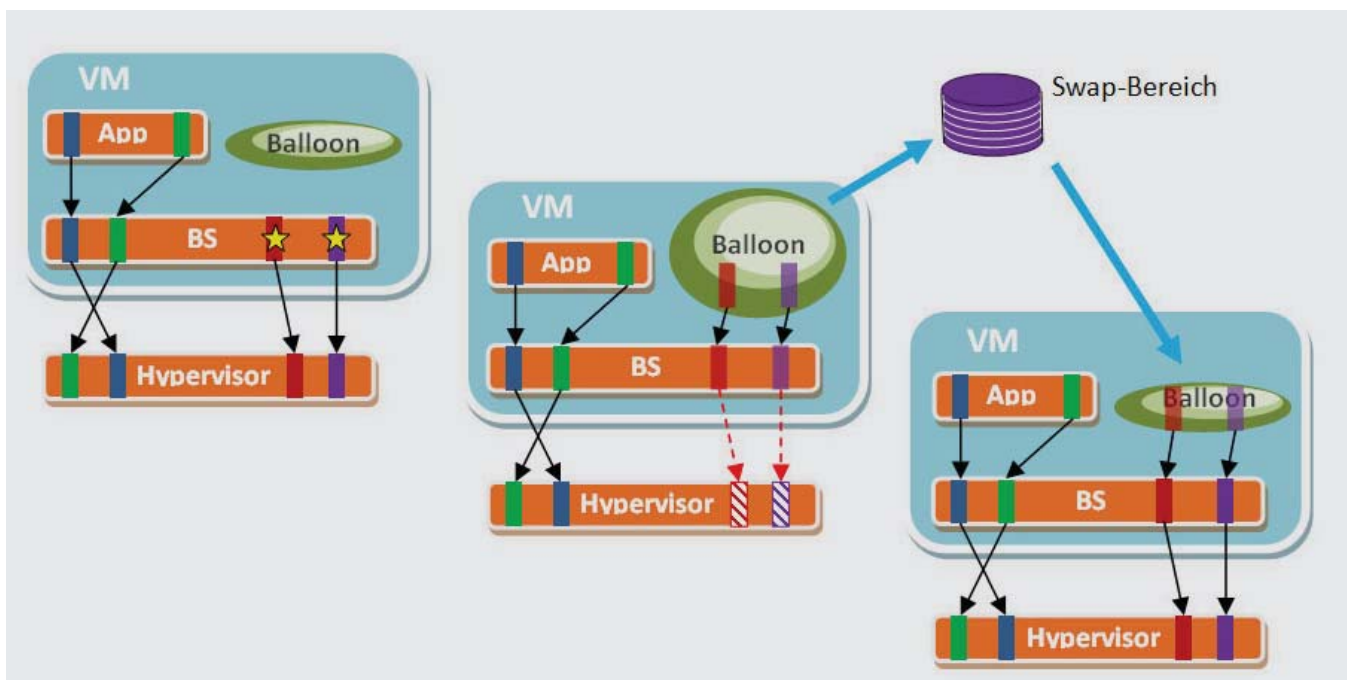


Abbildung 3. Ballooning-Verfahren

Gastwerkzeuge beenden. So kann in einem Windows-System nur der Administrator die Dienste im Taskmanager beenden oder den *TASKKILL*-Befehl in die Konsole eingeben. In einem Linux-System wird meist der *kill*-Befehl genutzt, um Prozesse zu beenden. Dieser kann jedoch nur mit dem *sudo*-Kommando gestartet werden, dass das Wissen des Root-Passwortes voraussetzt.

Technisches Versagen

Als technisches Versagen wird meist der Ausfall von Diensten in einer virtuellen Umgebung bezeichnet. Zudem fallen laut BSI noch Störungen der Netzinfrastruktur von Virtualisierungsservern, der Ausfall von Verwaltungsservern sowie der Ausfall von virtuellen Maschinen durch nichtbeendete Datensicherungsprozesse in die Gefahrenklasse des technischen Versagens.

Vorsätzliche Handlung

Wohl am schwersten einzuschätzen, sind die Gefahren, die sich aus vorsätzlichen Handlungen ergeben. Sie können sich von einem harmlosen Rahmen bis hin zu einer verheerenden Situation bewegen. Die vorsätzlichen Handlungen können dabei als folgende Aktionen auftreten:

- Angriffe gegen das Management (Servicekonsole)
- Angriffe gegen den Hypervisor
- Angriffe gegen das Gast-Betriebssystem
- Angriffe gegen den Festplattenspeicher

Da die Servicekonsole die meisten Schwachstellen aufweist, stellt sie einen der größten Gefahrenherde dar. Sollte ein Angreifer Zugang erlangen und über *root*-Rechte verfügen, besitzt er die volle Verwaltungskontrolle über den Host. Auf diese Weise könnte er Netzwerkeinstellungen manipulieren oder die Res-

ourcenparameter in den Konfigurationsdateien ändern, um nur eine Auswahl möglicher Eingriffe zu nennen. Eine explizite Sicherung der Konsole ist damit unerlässlich und wird deshalb im folgenden Abschnitt noch einmal näher betrachtet.

Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen Maschinen

Um die Überbuchungstechnik des *Memory Overcommitment* und das dazugehörige *Ballooning* optimal einzusetzen, empfiehlt es sich, die Gastwerkzeuge (*VMware Tools*) zu installieren. Sie werden mit sehr hohen Berechtigungen ausgeführt, um systemnah arbeiten zu können. Dadurch bekommt man die Möglichkeit, eine Überbuchung des Hauptspeichers zwischen dem Hypervisor und den virtuellen Maschinen zu koordinieren.

Maßnahmen

Die vorangegangene Analyse des *Memory Overcommitment* und *Ballooning* zeigt, welche Gefahren bei deren Einsatz entstehen können. Die Empfehlungen aus dem BSI IT-Grundschutzkatalogen bieten eine gute Grundlage, um ein ausgereiftes Sicherheitskonzept für virtuelle Welten zu erstellen. Fassen wir die wichtigsten zusammen.

Planung der virtuellen Infrastruktur

Eine sorgfältige Planung ist wie in allen Projekten essentiell für eine erfolgreiche Umsetzung. Die richtige Technik und funktionierende Produkte müssen sorgfältig ausgewählt werden. Auf diesen Schritt folgt die Verteilung der Kompetenzen in einer virtuellen Infrastruktur um einen reibungslosen Betrieb und eine klare Abgrenzung der Aufgaben zu gewährleisten.

Bei der Einsatzplanung für den Virtualisierungsserver müssen jedoch ein paar Besonderheiten beachtet

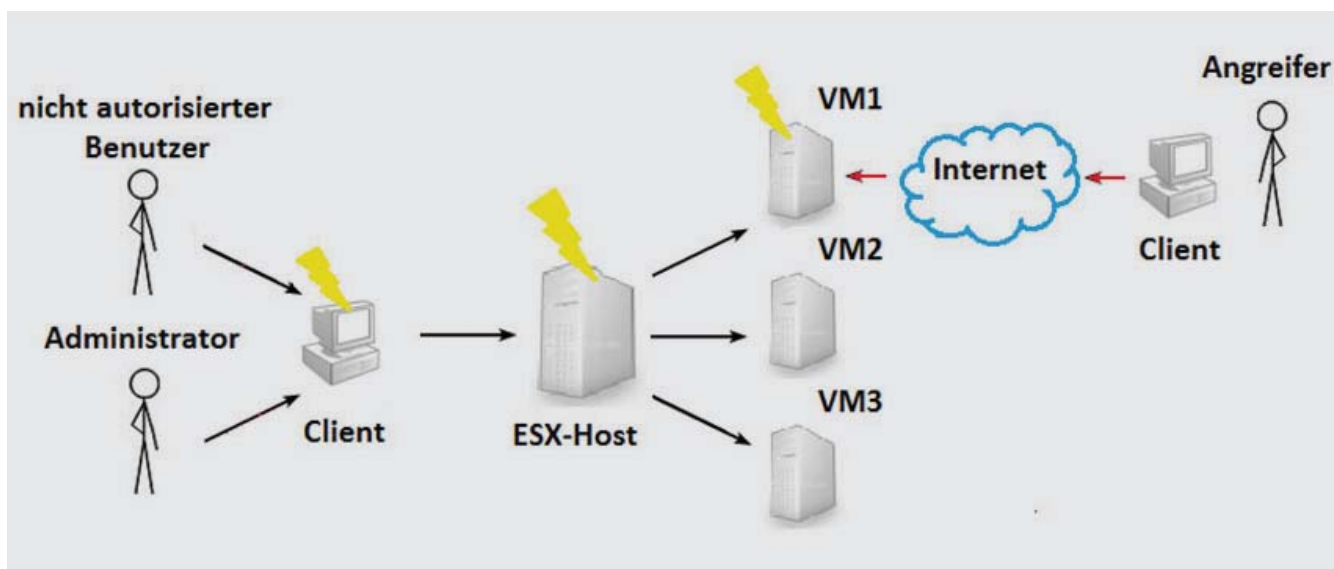


Abbildung 4. Zusammenfassendes Angriffsszenario

werden. Da auf ihm mehrere virtuelle Maschinen betrieben werden, sollte vorher bestimmt werden, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz benötigt wird. Dazu müssen die Performance und der Ressourcenverbrauch für die geplanten virtuellen Maschinen ermittelt werden.

Möchte man bereits vorhandene physische Systeme virtualisieren, kann der Ressourcenbedarf für die einzelnen Systeme nicht einfach addiert werden. Das BSI empfiehlt hier, die Performance der verschiedenen Systeme zu messen und auf dieser Basis die Werte festzulegen. Außerdem sollte man beachten, dass die Virtualisierungssoftware (*Snapshots*, Auslagerungsdatei, Ereignisprotokolle) sowie der Hypervisor (Servicekonsole) weitere Ressourcen benötigen.

Einsatzplanung für virtuelle Maschinen

Um einen reibungslosen Betrieb der virtuellen Maschinen gewährleisten zu können, muss bezüglich ihrer Lebenszyklen vielerlei beachtet werden. Bevor die virtuellen Maschinen in Betrieb genommen werden, sollten ihre realistischen und angemessenen Ressourcenanforderungen bestimmt werden. Danach ist zu prüfen, ob eventuelle Leistungseinschränkungen bei gelegentlichen Lastspitzen hingenommen werden können oder nicht. Zusätzlich muss die Performance virtueller Maschinen überwacht werden, um sicherzustellen, dass die Ressourcenanforderungen ausreichend erfüllt wer-

den. Um Ressourcenengpässe früh zu erkennen, muss ein Prozess integriert werden. Nur so kann man schnell genug darauf reagieren.

Sichere Konfiguration virtueller Maschinen

Virtuelle Maschinen sind in erster Linie genauso zu behandeln und zu modellieren wie physische Maschinen. Es sollte aber darauf geachtet werden, dass den virtuellen Maschinen der Zugang zu Geräten oft erst noch gewährt werden muss (z.B. DVDLaufwerk). Diese Geräte können meist aus der virtuellen Maschine über die Gastwerkzeuge gesteuert werden.

Sicherung der Servicekonsole

Die Sicherung der Konsole ist möglich, indem sie mithilfe eines abgeschotteten Managementnetzwerkes separiert wird. Dafür sollte eine eigene Netzwerkkarte sowie eine VLAN-ID vorgesehen werden.

Anschließend sollte der *root*-Zugriff eingeschränkt werden, da dieser eine enorme Bedeutung für die Verwaltung von Dateien und Diensten hat. Zudem muss ein kompliziertes *root*-Passwort gewählt werden, das in bestimmten Zeitabständen erneuert wird. Der Zeitabstand kann mithilfe des folgenden Befehls in der Konsole festgelegt werden:

```
esxcfg-auth --passmaxdays=[Anzahl-der-Tage]
```

```
Bsp. esxcfg-auth --passmaxdays=30
```

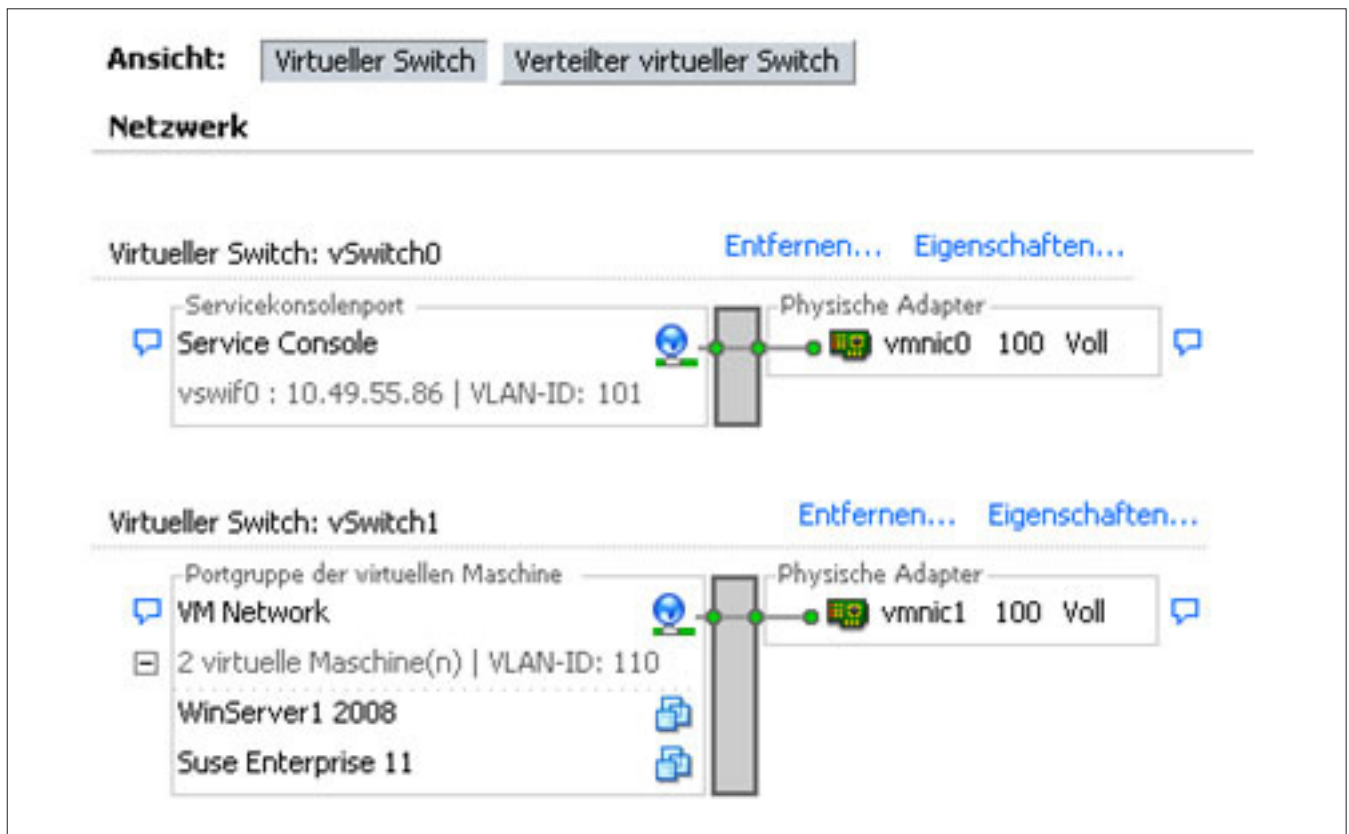


Abbildung 5. Separierung der Servicekonsole

Damit nicht jeder Benutzer mittels *sudo* oder *su root*-Rechte erlangen kann, wird eine *wheel*-Gruppe benutzt. Benutzer die in den *root*-Modus wechseln dürfen, müssen mit folgendem Befehl in die *wheel*-Gruppe hinzugefügt werden:

```
usermod -G wheel Benutzer Bsp. usermod -G wheel Max
```

Als nächstes wird der *su*-Befehl angepasst, damit nur *root* und die *wheel*-Gruppe die *root*-Rechte besitzen. Dies geschieht mittels:

```
chgrp wheel /bin/su  
chmod 4750 /bin/su
```

Damit die *wheel*-Gruppe den *sudo*-Befehl nutzen kann, muss die */etc/sudoers* mittels Befehl *visudo* in einem Editor gestartet und editiert werden. Dabei wird die Zeile *##wheel ALL = (ALL) ALL* auskommentiert. Einen zusätzlichen Schutz der Servicekonsole bietet die integrierte Firewall, die standardmäßig schon auf einer hohen Sicherheitsstufe eingestellt ist.

Sicherer Betrieb von virtuellen Infrastrukturen

Wenn ein Fehler auf einem Virtualisierungsserver entsteht, kann dieser Auswirkungen auf alle virtuellen Maschinen haben die auf ihm betrieben werden. Mithilfe von webbasierten Administrationsoberflächen oder einer Administrationssoftware (*VMware vSphere Client*, *VMware vCenter*), kann man lokal und über das Netz auf einen Virtualisierungsserver zugreifen. Somit hat man die Möglichkeit den Server oder dessen virtuelle Maschinen zu steuern, zu warten oder zu überwachen.

Ein weiterer Punkt ist die Überwachung des Betriebszustandes. Die Auslastung der Ressourcen sollte kontinuierlich geprüft werden. Nur so kann ermittelt werden, ob ausreichend Prozessorressourcen zur Verfügung stehen, die den Performanceanforderungen der virtuellen Maschinen genügen. Ob Hauptspeicherengpässe vorliegen, die die Verfügbarkeit der virtuellen Maschinen gefährden könnten, muss ebenfalls kontrolliert werden. Besonders bei der Verwendung des *Memory Overcommitments* sollte ein Prozess etabliert werden, der den Hauptspeicher ständig überwacht und einen drohenden Engpass früh erkennt. Diese Überwachungsaufgaben können automatisiert werden und zum Beispiel durch E-Mail-Benachrichtigungen über Unregelmäßigkeiten informieren.

Im Internet

- <http://www.vmachine.de>
- https://www.bsi-fuer-buerger.de/cln_030/ContentBSI/Aktuelles/Veranstaltungen/gstag/gstag_160310.html
- <http://www.vmware.com>
- <http://www.pc-ware.com>

Voraussetzungen für die empfohlenen Maßnahmen der BSI sind fachkundige und speziell geschulte Mitarbeiter. Hier sollte nicht gespart werden. Eine falsche Planung und nicht vorhandenes Fachwissen können zu einer späteren Behinderung oder sogar zu einem Ausfall des Produktivbetriebs führen. Damit ein fortlaufender und reibungsloser Betrieb möglich ist, sollte also nur einschlägig ausgebildetes Personal mit und in den virtuellen Welten arbeiten.

Sicherung zwischen Internet und virtueller Welt

Besitzen virtuelle Maschinen eine Verbindung zum Internet, ist selbstverständlich auch hier eine Sicherheitssoftware erforderlich. Diese kann als virtuelle Lösung oder in Form einer Hardware-Lösung bereitgestellt werden. Stellt beispielsweise ein Unternehmen seine vorhandene physische Infrastruktur auf eine virtuelle um und besitzt eine Hardware-Firewall- und Antivirus-Lösung, so kann diese weiterhin verwendet werden. Es entstehen keine weiteren Kosten für das Unternehmen. Soll die Firewall selbst in einer virtuellen Maschine betrieben werden, muss diese aus Sicherheitsgründen auf einem eigenen Host installiert werden. Dadurch entstehen für das Unternehmen zusätzliche Software- und Hardware-Kosten, die sich nur rechnen, wenn mehrere Sicherheitslösungen auf dem Host betrieben werden sollen. Ansonsten empfiehlt es sich, zu einer Hardware-Lösung zu greifen. Virtuelle Systeme, die keinen Zugang zum Internet besitzen, können mittels einer einfachen Firewall-Software überwacht werden. Bei einem sehr geringen Schutzbedarf, beispielsweise bei einem einfachen Test-System, reicht meist schon die in Windows Systemen integrierte Firewall aus.

Ausblick

VMware hat dieses Sicherheitsproblem erkannt und mit der Einführung der *vShield Zones* und der *VMsafe API* minimiert. Durch eine Zusammenarbeit mit zahlreichen Security-Software Herstellern wie beispielsweise *McAfee*, *Kaspersky* oder *Trend Micro* können neue Sicherheitskonzepte entwickelt werden und so die Sicherheit in einer virtuellen Infrastruktur immer weiter vorantreiben. Einige Vorreiter wie die *Deep Security* Lösung von *Trend Micro* gibt es bereits und es werden sicherlich weitere folgen.

STEVE HAMPICKE

Abgeschlossenes Studium (Diplom FH) der Automatisierungstechnik/Computersystemtechnik Diplomarbeit bei PC-WARE beschäftigte sich mit dem Thema „Analyse sicherheitsrelevanter Ressourcenoptimierung in virtuellen IT-Infrastrukturen“ beschäftigt sich weiterhin in seiner Freizeit mit VMware-Lösungen Kontakt mit dem Autor: steve.hampicke@googlemail.com