

Xen für UCS

Thema:	Einführung, Installation und Konfiguration von Xen-Virtualisierung unter UCS
Datum:	17. Mai 2010
Seitenzahl:	11
Versionsnummer:	5089
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Installation der Xen-Umgebung auf dem Wirtssystem	3
3	Installation von Xen-Gastsystemen	4
3.1	Installation eines unmodifizierten Gastsystems (z.B. Windows)	4
3.2	Installation der Treiber zur Paravirtualisierung von Windows-Betriebssystemen	5
3.3	Installation eines UCS-Gastsystems mit Unterstützung für Paravirtualisierung	6
4	Administration, Migration und Snapshots von DomUs	8
5	Fernzugriff auf Gastinstanzen (DomUs)	9
5.1	Konfiguration der Netzwerkanbindung einer Gastinstanz (DomU)	9
5.2	Terminal-Zugriff auf Linux-basierte Gastinstanzen	10
5.3	VNC-Zugriff auf grafisch betriebene Gastinstanzen	10
5.4	RDP-Zugriff auf grafisch betriebene Gastinstanzen	10
5.5	Lokaler Zugriff auf grafisch betriebene Gastinstanzen	11

1 Einführung

Xen ist eine ursprünglich an der Universität Cambridge entwickelte Virtualisierungslösung, die innerhalb einer Betriebssystem-Instanz den Betrieb weiterer Gastinstanzen ermöglicht.

Auf x86er-CPUs können Prozesse mit verschiedenen Privilegienstufen ausgeführt werden, den sogenannten Ringen. Direkter Hardwarezugriff, etwa für Geräte-Treiber, ist unter Linux nur im Ring 0 möglich, der im Betriebssystem durch den Kernel-Mode repräsentiert wird. Nicht-privilegierte Prozesse, der sogenannte Userspace, werden in einem getrennten Ring ausgeführt.

Xen implementiert einen **Virtual Machine Monitor**, in Xen-Terminologie als **Hypervisor** bezeichnet. Ein als Gastinstanz verwendeter Linux-Kernel wird hierbei in Ring 1 betrieben, während der Hypervisor in Ring 0 gestartet wird. Für den Betrieb des Hypervisors muss ein modifiziertes Betriebssystem verwendet werden, für den Start von Gastinstanzen existieren zwei verschiedene Ansätze:

- Ein Betrieb mit modifiziertem Gast-Betriebssystem ermöglicht hohe Performance, da Hardware-Zugriffe mit geringem Overhead an die Wirt-Instanz weitergereicht werden. Dieser Modus kann auf den meisten 486er-CPU aufwärts betrieben werden und wird als Paravirtualisierung bezeichnet.
- Wenn die CPU des Wirtsystems über Virtualisierungserweiterungen verfügt, besteht zusätzlich die Möglichkeit des Betriebs unmodifizierter Betriebssysteme wie Microsoft Windows. Intel bezeichnet diese Technologie als **Intel VT**, auch bekannt als Vanderpool, AMD als **AMD-V**, auch bekannt als Pacifica. Während CPU-Zugriffe durch diese Hardware-Erweiterungen direkt weitergegeben werden, müssen die übrigen Hardware-Bestandteile (Grafikkarte, Netzwerkkarte, Soundkarte) emuliert werden. Dies geschieht durch Bestandteile des Emulators **qemu**.

In einem Xen-Systemen werden verschiedene Hardware-Domänen betrieben. Es gibt zwei verschiedene Typen von Domänen:

- Das **Wirtsystem**, auch als **Domain-0** oder **Dom0** bezeichnet, ist die privilegierte Domain. Sie ist nur einmal auf einem System vorhanden und sorgt unter anderem für die Ressourcen-Zuteilung für die virtualisierten Systeme.
- Die nicht-privilegierten **Gastsysteme** werden auch als **DomUs** bezeichnet.

2 Installation der Xen-Umgebung auf dem Wirtsystem

In Univention Corporate Server wurde Xen in Version 3.2 integriert. Neben den notwendigen Management-Tools und dem Hypervisor existieren auch für Xen angepasste Kernel-Pakete. Die für Xen angepassten Kernel-Pakete mit Dom0-Unterstützung stehen in den Kernelversionen 2.6.18 und 2.6.26 zur Verfügung. In UCS 2.3 wird ein zusätzlicher Kernel auf Basis von UCS 2.6.30 bereitgestellt, der aber nur Unterstützung für den Betrieb

als DomU bietet (auf der i386-Architektur muss hierfür die 64-GB-Variante des Kernels verwendet werden).

Die Xen-Komponenten können im Univention Installer in der Software-Auswahl unter **Virtualisierung** ausgewählt werden.

Durch Installation des Pakets **univention-xen** werden alle benötigten Pakete installiert. Sofern bisher keine andere Xen-Kernelversion im System installiert ist, wird bei der Installation des Pakets **univention-xen** automatisch Version 2.6.26 des xen-fähigen Kernel installiert. Bei Bedarf kann die jeweilige fehlende Kernelversion über das Paket **univention-kernel-image-2.6.18-xen** bzw. **univention-kernel-image-2.6.26-xen** nachinstalliert werden.

Im Zuge der Installation werden im Bootloader Grub neue Einträge für den direkten Systemstart in den Hypervisor eingerichtet. Nach erfolgter Installation muss ein Neustart durchgeführt werden und ein Kernel-Image ausgewählt werden, dass mit **Xen 3.2** beginnt.

Anders als bei Standard-Kernen wird beim Systemstart der Kernel mit Xen-Dom0-Support kein grafischer Bootsplash mit Fortschrittsbalken angezeigt, wodurch die Meldungen der startenden Systemkomponenten sichtbar sind. Auf Xen Dom0-Systemen wird seit UCS 2.2-0 nicht mehr automatisch der grafische Desktop-Login Bildschirm gestartet, da X-Server des Typs Vesa derzeit auf diesen Systemen in Kombination mit dem 2.6.26er Kernel nicht korrekt funktionieren. Falls ein anderer X-Server oder Kernel verwendet wird, kann die Univention Configuration Registry-Variable `gdm/autostart` auf **yes** gesetzt werden und der grafische Desktop-Login Bildschirm zur Probe direkt durch Aufruf von `invoke-rc.d gdm start` gestartet werden.

Der Hypervisor wird durch den **xend**-Dienst bereitgestellt. Nach Veränderungen der Konfiguration muss dieser neu gestartet werden.

Die Konfigurations-Parameter einer Gastinstanz (DomU) werden in textbasierten Konfigurations-Dateien abgelegt. In einer UCS-Installation werden diese standardmässig unter `/etc/xen` abgelegt. Die Image-Dateien für die Partitionen einer Gastinstanz (DomU) werden unter `/var/lib/xen` abgelegt.

Als Management-Tool für die Verwaltung von Xen-Instanzen kann das Programm **ConVirt** verwendet werden.

3 Installation von Xen-Gastsystemen

3.1 Installation eines unmodifizierten Gastsystems (z.B. Windows)

Im folgenden werden die notwendigen Schritte für den Betrieb eines unmodifizierten Betriebssystemes am Beispiel von Microsoft Windows XP dokumentiert.

Zuerst sollte ein Name für die Gastinstanz ausgewählt werden, in diesem Beispiel **winxp**.

Die Daten der virtuellen Festplatte der Gastinstanz (DomU) werden in einer Image-Datei gespeichert, die nun angelegt werden muss: Mit den folgenden Befehlen wird ein 8 GB

großes Festplattenimage erzeugt:

```
mkdir -p /var/lib/xen/winxp/  
dd if=/dev/zero of=/var/lib/xen/winxp/hdimage bs=1M count=1 seek=8000
```

Xen erlaubt das Einbinden von ISO9660-Images als virtuelle CD-ROM-Laufwerke. In diesem Beispiel wird davon ausgegangen, dass ein CD-Image von Microsoft Windows XP unter `/var/lib/xen/winxp/winxp.iso` zu finden ist.

Eine Beispiel-Konfiguration für den Betrieb unmodifizierter Betriebssysteme ist unter `/usr/share/doc/univention-xen/examples/basis-vmx.cfg` zu finden. Diese sollte als Basis kopiert werden:

```
cp /usr/share/doc/univention-xen/examples/basis-vmx.cfg /etc/xen/winxp.cfg
```

Die folgenden Einstellungen dieser Beispiel-Konfiguration müssen mindestens verändert werden:

- Als **name** sollte **winxp** eingetragen werden.
- Mit folgender Zeile werden die oben angegebenen Image-Dateien in die Gastinstanz eingebunden. Das Festplattenimage wird dabei schreibbar, das virtuelle CD-ROM-Laufwerk nur lesbar eingebunden.

```
disk = [ 'file:/var/lib/xen/winxp/hdimage,hda,w',  
        'file:/var/lib/xen/winxp/winxp.iso,ioemu:hdc:cdrom,r' ]
```

Soll die Gastinstanz über eine Netzanbindung verfügen, so muss außerdem mindestens eine virtuelle Netzwerkkarte konfiguriert werden, deren MAC-Adresse dabei vorgegeben wird. Ein Beispiel für eine Netzwerkkarte in einem unmodifizierten Betriebssystem:

```
vif = [ 'type=ioemu', 'mac=00:16:3E:27:1F:A6' ]
```

Wird als Betriebssystem-Kernel der Gastinstanz (DomU) ein Xen-fähiges Linux verwendet, so kann ein direkter Zugriff auf das Gast-Interface erfolgen:

```
vif = [ 'mac=00:16:3E:27:1F:A6' ]
```

Auf die weitergehende Einrichtung des Netzwerk-Betriebs wird in Kapitel 5 eingegangen.

Die Konfiguration eines Remote-Zugriffs über VNC und RDP wird in Kapitel 5.3 und 5.4 erläutert.

Abschließend kann die neu angelegte Domain mit dem Befehl `xm create /etc/xen/winxp.cfg` gestartet werden.

3.2 Installation der Treiber zur Paravirtualisierung von Windows-Betriebssystemen

Wird ein unmodifiziertes Betriebssystem wie in Kapitel 3.1 beschrieben installiert, werden die Zugriffe auf die Netzwerkkarte und Block-Devices wie Festplatten durch den Hardware-Emulator QEMU emuliert.

Werden im DomU-System Treiber installiert, die einen direkten Zugriff auf die Hardware des Dom0-Systems erlauben, so ergibt sich ein Zuwachs an Performance und Zuverlässigkeit. Neben proprietären Treibern existiert ein Open-Source-Treiber, genannt GPLPV. Dieser kann von <http://www.meadowcourt.org/downloads/> herunter geladen werden, der Dateiname lautet **Xen PV Drivers.exe**. Für eine erfolgreiche Installation der GPLPV-Treiber unter Windows XP muss das Service Pack 2 installiert sein.

Der Installer kann direkt ausgeführt werden, im ersten Bildschirm sollte die zu verwendende Windows-Variante ausgewählt werden. Der Shutdown-Manager sollte ebenfalls installiert werden.

Die meisten Treiber für Windows-Betriebssystemen sind durch den Hersteller signiert, was aber für die GPLPV-Treiber nicht erfolgt ist. Auf einigen Windows-Varianten (z.B. Windows 2003) können bei der Installation Ausnahmen für den "Logotest" und "Authenticode" hinzugefügt werden. Aktuelle 64-Bit-Windows-Varianten müssen wie anhand der Anleitung im Microsoft Developer Network beschrieben signiert werden: <http://msdn.microsoft.com/en-us/library/aa906283.aspx>

Für GPLPV-Treiber einer Version vor 0.9.12-pre9 muss nach der Installation die zentrale Boot-Konfigurationsdatei **boot.ini** angepasst werden: **Rechtsklick auf Arbeitsplatz > Eigenschaften > Erweitert > Starten und Wiederherstellen > Einstellungen > Systemstart > Bearbeiten**. Die aktive Zeile unter **operating systems** muss kopiert werden und ein zusätzliches /GPLPV angehängt werden, z.B: (Je eine Zeile und ohne den Backslash)

```
multi(0) disk(0) rdisk(0) partition(1)\WINDOWS="Windows Server 2003, \
Enterprise, GPLPV" /noexecute=optout /fastdetect /gplpv
multi(0) disk(0) rdisk(0) partition(1)\WINDOWS="Windows Server 2003, \
Enterprise" /noexecute=optout /fastdetect
```

Für GPLPV-Treiber einer Version ab 0.9.12-pre9 wird der Treiber standardmäßig verwendet, es sein denn es ist /NOGPLPV angegeben. In diesem Fall kann sinnvoll sein, zur Sicherheit analog zum oben beschriebenen Vorgehen die Boot-Konfigurationsdatei so anzupassen, daß eine Zeile mit /NOGPLPV eingetragen ist.

Anschliessend muss die DomU neu gestartet werden und beim Windows-Start der GPLPV-Eintrag ausgewählt werden. Die folgende Hardwareerkennung wird eine Reihe von Treibern einrichten, die Xen im Namen tragen. Die Netzwerkverbindung muss ebenfalls neu konfiguriert werden. Es ist zu beachten, dass die ursprünglich konfigurierte QEMU-Netzwerkkarte dabei deaktiviert wird, die Einrichtung sollte also nicht über RDP erfolgen. Nach einem erneuten Neustart sind die paravirtualisierten Treiber aktiv.

3.3 Installation eines UCS-Gastsystems mit Unterstützung für Paravirtualisierung

Im folgenden werden die notwendigen Schritte für die Installation einer modifizierten Gastinstanz (DomU) am Beispiel von Univention Corporate Server 2.3 beschrieben, die Anleitung kann aber auch analog für UCS 2.2 verwendet werden. Es besteht ebenfalls die Möglichkeit Univention Corporate Server unmodifiziert zu installieren, allerdings wird es dabei durch die Emulation von **qemu** zu Geschwindigkeitseinbußen kommen.

Das hier beschriebene Vorgehen verwendet den Univention Installer mit einer angepassten Initial Ramdisk (auch als Initrd bezeichnet).

3.3.1 Generierung der Initial Ramdisk

Die Initial Ramdisk muss nur einmalig erzeugt werden und kann für weitere Installationen weiterverwendet werden.

Zuerst muss das ISO-Image der Installations-DVD kopiert werden und über das Loopback-Device eingebunden werden:

```
mkdir -p /mnt/iso
mount -o loop ucs_2.3-0-*-dvd-amd64.iso /mnt/iso
```

Anschließend muss die Initrd entpackt werden, hier am Beispiel der Initrd für den 2.6.26-Kernel. Es können auch die Initrds für die anderen Kernelvarianten verwendet werden. Unter UCS 2.3 lautet der Dateiname `linux-2.6.bin`.

```
gunzip < /mnt/iso/boot/linux-2.6.26.bin > /tmp/ucs_2.3-initrd.ext3
```

Nun muss das Dateisystem vergrößert werden, da der Installationskernel mehr Module enthält:

```
dd if=/dev/zero bs=1M count=50 >> /tmp/ucs_2.3-initrd.ext3
resize2fs -f /tmp/ucs_2.3-initrd.ext3
```

Im Folgenden wird die Initrd eingebunden und durch die Module des aktuellen Kernels ersetzt:

```
umount /mnt/iso
mount -o loop /tmp/ucs_2.3-initrd.ext3 /tmp/iso/
rm -rf /mnt/iso/lib/modules/2.6.*
cp -Rf /lib/modules/$(uname -r) /mnt/iso/lib/modules/$(uname -r)
```

Da die Terminalemulation der Xen-Console nur eingeschränkte Darstellungsmöglichkeiten bietet, wird nun der Grafikmodus des Univention Installer auf eine einfachere Ausgabe umgestellt:

```
sed -i 's|params=""|params="--simple |' /mnt/iso/sbin/univention-installer
```

Abschließend wird die Initrd ausgehängt und wieder komprimiert:

```
umount /mnt/iso
gzip < /tmp/ucs_2.3-initrd.ext3 > /tmp/ucs_2.3_$(uname -r)_initrd
```

3.3.2 Installation mit dem Univention Installer

Zunächst sollte ein Festplatten-Image für die Gastinstanz erzeugt werden. In diesem Beispiel wird eine 12 GB Datei für die Festplatte angelegt.

```
mkdir -p /var/lib/xen/ucs-master/  
dd if=/dev/zero of=/var/lib/xen/ucs-master/disk bs=1M count=1 seek=12000  
fdisk /var/lib/xen/ucs-master/disk
```

Nun müssen zwei Xen-Konfigurations-Dateien erzeugt werden, eine für die Installation und eine für den späteren Produktivbetrieb. Die Angaben in diesem Beispiel sollten entsprechend an die jeweilige Umgebung angepasst werden. Für RAMDISK sollte der Pfad zur oben erzeugten Initial Ramdisk angegeben werden:

```
# /etc/xen/ucs-master-installation.cfg  
name = 'ucs-master'  
kernel = "/boot/vmlinuz-2.6.18-ucs105-xen-686"  
memory = 512  
vcpus = 1  
disk = [ 'file:/var/lib/xen/ucs-master/disk,hda,w',  
         'file:/var/lib/xen/ucs-master/ucs_2.3-0*-dvd-amd65.iso,scd0,r' ]  
vif = [ 'type=ioemu', 'mac=00:16:3E:27:1F:FF' ]  
boot = 'c'  
ramdisk='RAMDISK'  
root='/dev/ram ro'  
extra='xencons=tty vt.default_utf8=0 ramdisk_size=224800 flavor=linux  
       text forceascii'
```

```
# /etc/xen/ucs-master.cfg  
name = 'ucs-master'  
kernel = "/boot/vmlinuz-2.6.18-ucs105-xen-686"  
memory = 512  
vcpus = 1  
disk = [ 'file:/var/lib/xen/ucs-master/disk,hda,w' ]  
vif = [ 'type=ioemu', 'mac=00:16:3E:27:1F:FF' ]  
boot = 'd'  
root = "/dev/hda2 ro"  
extra='xencons=tty'
```

Anschließend kann die Xen-Installation mit dem Befehl `xm create -c /etc/xen/ucs-master-installation.cfg` gestartet werden.

Nach erfolgter Installation sollte die für den Produktivbetrieb vorgesehene Konfigurations-Datei zum Starten der DomU verwendet werden.

4 Administration, Migration und Snapshots von DomUs

Das zentrale Administrationswerkzeug innerhalb des Wirtsystems (Dom0) ist `xm`. Eine Übersicht der wichtigsten Befehle:

Befehl	Erklärung
<code>xm list</code>	Eine Übersicht der Domains im aktuellen System. Mit dem Parameter <code>-l</code> kann eine ausführliche Übersicht der Domänenressourcen angezeigt werden.

xm console DOMAIN	Verbindet zur Terminal-Console einer Linux-basierten Domain.
xm create CONFIGFILE	Startet eine Domain anhand der in CONFIGFILE spezifizierten Konfiguration.
xm save DOMAIN SNAPSHOTDATEI	Sichert einen Snapshot des Arbeitsspeichers einer Domain und beendet diese anschliessend. Soll die Domain nicht beendet werden, so muss der Parameter -c übergeben werden.
xm restore SNAPSHOTDATEI	Laden eines zuvor mit xm save gespeicherten Snapshots einer Domain.
xm migrate DOMAIN HOST	Mit diesem Befehl kann eine Domain auf ein anderes Xen-System verschoben werden. Wird die Option -live übergeben, so erfolgt die Migration im laufenden Betrieb und ist für die Nutzer der Domäne transparent.
xm top	Gibt eine Übersicht über die aktuell laufenden Domains und deren Ressourcen-Verbrauch aus.
xm shutdown DOMAIN	Leitet einen Shutdown der Domain ein. (Vergleichbar mit dem halt-Befehl unter Linux.)
xm destroy DOMAIN	Forciert eine direkte Abschaltung einer Domain. (Vergleichbar mit dem Betätigen des Netzschalters eines Systems.)
xm reboot DOMAIN	Neustart einer Domain.
xm pause DOMAIN	Stoppt die Ausführung einer Domain.
xm unpause DOMAIN	Wiederaufnahme einer pausierten Domain.

5 Fernzugriff auf Gastinstanzen (DomUs)

5.1 Konfiguration der Netzwerkanbindung einer Gastinstanz (DomU)

Die durch **univention-xen** verwaltete Netzanbindung verwendet eine **Bridge** zur Anbindung der Gastinstanzen an das Wirtssystem.

Die Bridge wird unter dem Namen **xenbr0** angelegt. Die Netzwerkkarte des Wirtsystems (Dom0) erscheint innerhalb der Bridge als **vif0.0**, die Netzwerkkarten der Gastinstanzen (DomUs) als **vifX.Y**, wobei **X** die Gastinstanz (DomU) kennzeichnet und **Y** von 0 an aufsteigend die virtuellen Netzdevices repräsentiert, also beispielsweise **vif1.0** und **vif1.1** für ein System mit einer Gastinstanz (DomU) mit zwei virtuellen Netzwerkkarten.

Die Anbindung der Bridge an die physisch vorhandene Netzwerkkarte des Systems erfolgt über das **peth0**-Device. Standardmässig ist kein Interface für die Bridge definiert. Es kann über die Univention Configuration Registry-Variable `xen/bridge/interface` konfiguriert werden. Nach dem Setzen von `xen/bridge/interface` muss der **xend**-Dienst durch das Ausführen des Befehls `/etc/init.d/xend restart` neu gestartet werden.

Innerhalb der Gastinstanz erscheinen die Netzwerkkarten unverändert. Netzwerkkarten

unter Linux lassen sich etwa als **eth0** ansteuern und unter Windows in der Netzwerkübersicht konfigurieren. Auch das Default-Gateway und die DNS-Auflösung müssen wie gewohnt konfiguriert werden.

Neben der Bridge existieren noch zwei weitere Ansätze eine Netzanbindung herzustellen: über eine direkte Konfiguration des Routings und Auflösung der MACs über Proxy-ARP oder über Network Address Translation. Beide werden jedoch momentan von **univention-xen** noch nicht unterstützt und müssen ggf. von Hand in `/etc/xen/xend-config.sxp` konfiguriert werden..

5.2 Terminal-Zugriff auf Linux-basierte Gastinstanzen

Mit `xm console DOMAIN` kann auf die Terminal-Console einer Linux-basierten Gastinstanz zugegriffen werden. Mit der Tastenkombination **Strg + J** kann die Console wieder beendet werden. Die aktiven DomU-Instanzen können mit `xm list` ermittelt werden.

5.3 VNC-Zugriff auf grafisch betriebene Gastinstanzen

Um einen Zugriff über VNC zu ermöglichen, müssen in der Konfigurationsdatei der Gastinstanz folgende Einträge vorgenommen werden:

```
vnc = 1
vncpasswd="geheim"
```

Standardmässig ist der Zugriff nur über localhost erlaubt, über die Univention Configuration Registry-Variable `xen/vnc/listen` kann jedoch ein abweichender Netzbereich zugelassen werden, etwa **0.0.0.0** für netzweiten Zugriff.

Unter der IP-Adresse des Wirtsystems kann dann mit einem VNC-Viewer (unter Univention Corporate Server mit `vncviewer` oder `krdc`) auf die grafische Ausgabe zugegriffen werden. Standardmässig ist das erste freigegebene VNC-Display unter **:0** erreichbar.

5.4 RDP-Zugriff auf grafisch betriebene Gastinstanzen

Für den produktiven Betrieb einer Windows-Gastinstanz empfiehlt sich der Einsatz des **Remote Desktop Protocols** (RDP). Der Zugriff über RDP - und insbesondere die Anzeige des Mauszeigers - erfolgt deutlich flüssiger im Vergleich zu VNC.

RDP-Zugriff kann in Microsoft Windows Server 2003, Windows XP Professional und Windows Vista Business/Enterprise/Ultimate unter **Systemsteuerung > Systemeigenschaften > Remote** durch Aktivierung der Optionen **[Remoteunterstützung]** und **[Remotedesktop]** aktiviert werden.

RDP-Clients werden unter Microsoft Windows ab Windows XP standardmässig mitgeliefert. Für den Zugriff von Linux-basierten Systemen werden in Univention Corporate Server die Pakete `rdesktop` und `krdc` mitgeliefert.

5.5 Lokaler Zugriff auf grafisch betriebene Gastinstanzen

Die Xen-Pakete in Univention Corporate Server sind mit Unterstützung für die Grafikbibliothek **Simple DirectMedia Layer** (SDL) übersetzt. Dadurch kann auch ein direkter, lokaler Zugriff aus dem Hostsystem erfolgen. Hierzu muss der Zugriff über VNC deaktiviert werden:

```
sdl = 1  
vnc = 0
```

Nach einem `xm create` erfolgt dann eine grafische Ausgabe der Gastinstanz.