

Benutzungsordnung für virtuelle Server am RRZ der Universität Hamburg

Das RRZ der Universität Hamburg bietet seinen Nutzerinnen und Nutzern virtualisierte Server für eigene IT-Dienste an. Hierfür werden mit einer Virtualisierungssoftware mehrere virtuelle Serverinstanzen als „Gastsysteme“ auf dem „Wirtssystem“ einer physikalischen Maschine betrieben.

Für den Betrieb einer solchen virtuellen Serverinstanz gelten folgende Bestimmungen, zusätzlich zu den allgemeinen IT-Betriebsregelungen der Universität Hamburg (siehe <http://www.rrz.uni-hamburg.de/kommunikation/betriebsregelungen.html>):

- 1) Ein virtueller Server wird auf Antrag eingerichtet. Hierfür stellt das RRZ ein entsprechendes Formular auf den Webseiten des RRZ bereit. Antragsberechtigt sind alle Mitglieder der Universität Hamburg.
- 2) Ob ein Projekt für einen virtuellen Server geeignet ist, muss vorab mit der Gruppe Zentrale Dienste im RRZ besprochen werden. Als Gastsysteme eignen sich besonders Systeme, die auf eine hohe Verfügbarkeit angewiesen sind, ohne durchgängig eine hohe CPU-, Netz- oder Festplattenlast zu erzeugen; ein Gastsystem sollte dauerhaft nicht mehr als 25 Prozent einer CPU beanspruchen. Ein hardwarebasierter Kopier- und Zugriffsschutz wie z.B. ein Dongle kann gegenwärtig nicht unterstützt werden.
- 3) Das RRZ installiert auf Wunsch eine aktuelle Version von Open SuSE-Linux; andere Betriebssysteme können eingesetzt werden, müssen aber vom Projekt selbst beschafft und installiert werden. Mit Übergabe ist jedes Projekt für sein Gastsystem selbst verantwortlich. Dies schließt insbesondere die volle Verantwortung für die Sicherheit ein. Dazu gehört, dass die Betriebssysteme auf dem aktuellen Patchstand gehalten werden, ebenso eigene oder Open-Source-Softwareprodukte wie z.B. PHP- oder Perl-Skripte.
- 4) Das RRZ wird sich zu keinem Zeitpunkt auf dem Gastsystem anmelden. Das Root/Administrator-Passwort sollte nach Übergabe sofort geändert werden. Nach Absprache kann im RRZ dem Projekt Zugang zum „Root-Terminal“ des Gastsystems verschafft werden. Dies ist auf Ausnahmesituationen beschränkt, falls auf andere Weise kein Zugang zum Gastsystem möglich ist.
- 5) Das RRZ betreibt die Festplattenressourcen aller Gastsysteme auf einem redundanten Plattensystem, um Ausfällen und Datenverlusten auf unterster Ebene so weit wie möglich vorzubeugen. Darüber hinaus ist jedes Projekt für die Sicherung seines Systems selbst verantwortlich. Es wird dringend empfohlen, regelmäßig Backups des Systems und der Daten durchzuführen. Hierfür steht das zentrale Backup- und Archivsystem des RRZs zur Verfügung.

- 6) Das RRZ sorgt für die Sicherheit des Wirtsystems. Zu diesem Zweck werden die notwendigen Betriebssystemupdates oder Konfigurationsanpassungen vorgenommen. Wartungsarbeiten am Wirtssystem, für welche die Gastsysteme vorübergehend abgeschaltet werden müssen, werden den Projekten eine Woche vorher an vereinbarter Stelle bekannt gegeben. Nur bei akuter Gefährdung des Gesamtsystems kann auf eine Vorankündigung oder Rücksprache verzichtet werden.
- 7) Jedes Projekt benennt gegenüber dem RRZ einen technischen Ansprechpartner; er ist verantwortlich für die ständige Betreuung des Gastsystems und wird auch im Nameserver als Verantwortlicher für die IP-Adresse des Gastsystems eingetragen. Der technische Ansprechpartner des Projektes ist für die in Punkt 3 genannten Administrationsaufgaben zuständig. Er wird bei Wartungsarbeiten, Störungen oder Missbrauch des Gastsystems per Mail oder telefonisch vom RRZ benachrichtigt. Ein Wechsel oder zeitweilige Vertretung des technischen Ansprechpartners (z.B. aufgrund von Urlaub) muss dem RRZ mitgeteilt werden.
- 8) Wird ein Gastsystem nicht oder nur unzureichend administriert oder missbraucht oder werden andere Gastsysteme durch einen zu großen Ressourcenbedarf im Betrieb behindert, kann das Gastsystem automatisch oder manuell gesperrt werden. Falls ein Gastsystem wiederholt gesperrt werden musste oder permanent Überlast erzeugt, kann das RRZ das Projekt als ungeeignet für die Nutzung einer virtuellen Instanz einstufen und auf Dauer sperren.