Werkzeugkasten ohne Anleitung

Vielfältige Tools für die Planung einer virtuellen Infrastruktur

Kai-Oliver Detken

Die Virtualisierung von Client- und Server-Systemen schreitet voran und macht auch nicht vor Unternehmensgrenzen halt. So werden auf der einen Seite externe, auf unterschiedlichen Virtualisierungsplattformen basierende Cloud-Lösungen angeboten, auf der anderen Seite private Cloud-Infrastrukturen innerhalb der Firma aufgebaut. Dafür bietet das Virtualisierungsumfeld einen Dschungel an neuen Lösungen, Software und Systemen. Cloud-Themen wie OpenStack, Quantum, libvirt, VDE, Open vSwitch und KVM führen zu Begriffsverwirrungen und lassen kaum ganzheitliche Planungen zu. Es ist Zeit, eine Struktur in dieses Wirrwarr zu bringen und Kombinationsmöglichkeiten aufzuzeigen, die gleichermaßen leistungsfähige wie verwaltbare Virtualisierungslösungen ermöglichen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Virtualisierungs-Tools wie VMware, Xen Source oder KVM (Kernel-based Virtual Machine) ermöglichen die Simulation/Emulation von IT-Komponenten und teilweise sogar von komplexen IT-Infrastrukturen. Auch die Kabelemulation ist mittels VDE (Virtual Distributed Ethernet) möglich. Diese Techniken und Lösungen lassen sich im Prinzip zur Konzeption und Provisionierung von IT-Sicherheitsarchitekturen und Infrastrukturen nutzen. Mit ihnen könnten nicht nur einzelne virtuelle Einheiten, sondern letztlich auch die gesamte IT-Infrastruktur eines Unternehmens abgebildet werden.

Allerdings muss man in einer komplexer werdenden Umgebung neben den verschiedenen Virtualisierungs-Tools auch die Management- und Netzlösungen betrachten. In Zeiten der Einzelserver-Emulation war dies noch kein Problem. Doch inzwischen müssen die verschiedenen virtuellen Machinen (VM) auch zentral verwaltet werden. Hinzu kommt, dass nicht die Virtualisierung selbst für Unternehmen problematisch ist, sondern die Simulation ganzer IT-Umgebungen. Das Zusammenspiel von Virtualisierungsarten mit anderen Infrastrukturkomponenten steht daher bei der Planung einer virtuellen Infrastruktur im Vordergrund.

Management von VMs

Jede Virtualisierungslösung hat unterschiedliche Verwaltungslösungen. Dadurch ist es in heterogenen Rechenzentren (RZ) nicht möglich, mit einem einzelnen Tool jede verwendete Virtualisierungslösung zu verwalten. Zur Lösung dieses Problems wurde daher die Bibliothek libvirt (www.libvirt.org) entwickelt. Hierbei handelt es sich um freie Software, die unter der „GNU Lesser General Public License" veröffentlicht wurde. Sie stellt einheitliche Schnittstellen (API) bereit, um verschiedene Virtualisierungslösungen verwalten zu können, die sich wiederum in ihrem Funktionsumfang unterscheiden können. Aus diesem Grund stellt libvirt nicht alle Funktionen einer Virtualisierungslösung bereit. Ebenso gibt es spezifische libvirt-Funktionen, die nicht von jeder Virtualisierungslösung unterstützt werden.

Die Liste der unterstützten Hypervisors wurde im Laufe der Entwicklung der Bibliothek stetig erweitert. Den Zugriff auf die unterschiedlichen Hypervisors übergibt libvirt intern an eigens entwickelte Treiber, die für die meisten gängigen Virtualisierungslösungen zur Verfügung stehen.

Grundlegende Funktionen der API sind Erstellung, Provisionierung, Modifikation, Monitoring, Migration und Laufzeitkontrolle von VMs (Domains). Daneben bietet libvirt auch die Möglichkeit, die Ressourcen des Host-Systems (Node) zu verwalten und zu konfigurieren. Hierzu gehören die Verwaltung der virtuellen Speichermedien (Storage-Pools und -Domains), die Konfiguration der Netzschnittstellen sowie die Verwaltung von virtuellen Netzen (*Bild 1*). Libvirt selbst stellt das Kommandozeilen-Tool virsh zur Verfügung, das einen Großteil der durch die API zur Verfügung gestellten Befehle abdeckt. Weitere Tools, die auf libvirt aufbauen, sind u.a.:

- virt-manager: grafisches Managementtool zur Verwaltung von VMs, mit dem sich mehrere Hypervisors/Nodes gleichzeitig verwalten lassen; zusätzlich werden Funktionen zur Laufzeitkontrolle sowie zur Performance- und Ressourcenkontrolle der von libvirt verwalteten Domains angeboten;
- virt-install: dient zum Anlegen möglicher VMs; die Konfiguration wird über eine Kommandozeile oder eine grafische Oberfläche angeboten; unterstützt auch Installationen über eine Netzverbindung;

- virt-image: Erstellen neuer VMs auf Basis einer XML-Beschreibungsdatei oder auch von vordefinierten VMs (sog. Templates); zum Austausch bestehender VMs mit anderen Virtualisierungslösungen einsetzbar;
- virt-clone: Klonen von VMs durch Kopieren der Image-Dateien; kümmert sich u.a. darum, dass eine neue UUID und MAC-Adresse für den Klon benutzt wird.

Eine andere Managementlösung ist OpenStack (**www.openstack.org**), die sich speziell im Cloud-Umfeld durchzusetzen scheint. OpenStack ist eine Sammlung mehrerer Open-Source-Projekte, die es Unternehmen und Service Providern ermöglicht, ihre eigene Cloud aufzubauen. Die NASA und Rackspace waren die ersten Gründer des Projektes. Mit der Plattform „Cloud Files" hat Rackspace dabei die Objektspeicherverwaltung beigesteuert, während die NASA mit der Plattform „Nebula" die Compute-Verwaltung eingebracht hat. Mittlerweile unterstützen über 175 Unternehmen das Projekt. Die Architektur wird in *Bild 2* exemplarisch dargestellt.

Die OpenStack-Software besteht aus:

- OpenStack Compute (Nova): Verwaltungskomponente für die VMs, wobei die VMs über beliebig viele Knoten verteilt werden können; verwaltet die jeweiligen Ressourcen, Netze und benötigten Autorisationen; steuert die VMs nicht selbst, sondern nutzt die libvirt-API;
- OpenStack Identity Service (Keystone): Identitätsmanagement zur Authentifizierung und Autorisierung aller OpenStack-Komponenten;
- OpenStack Imaging Service (Glance): verwaltet die Images von OpenStack; nutzt dazu folgende Speicher-Backends: lokales Dateisystem, S3 Storage direkt, OpenStack Object Storage (Swift), S3 Storage mit Swift als Zwischenkomponente und http;
- OpenStack Admin Web-Interface (Horizon): webbasierte Administrationsoberfläche, mit deren Hilfe VMs gestartet, gestoppt, neu gestartet und Snapshots erstellt werden; an VMs können darüber öffentliche IP-Adressen vergeben, die iptables-Regeln manipuliert und mit VNC auf die VMs zugegriffen werden;
- OpenStack Object Storage (Swift): Bereitstellen eines verteilten, virtuellen Objektspeichers; Swift kann Milliarden von Objekten von verschiedenen Knoten speichern; hat eine eingebaute Redundanz und eine Failover-Verwaltung;
- OpenStack Network (Quantum): virtueller Netzservice, der eine leistungsstarke API bereitstellt, um die Netzverbindungen zwischen Geräten von anderen Open-Stack-Services zu definieren; besitzt eine API, die eine logische Abstraktion für die Beschreibung von Netzverbindungen ermöglicht; basiert auf einem Plugin, um die virtuellen und/oder physischen Switche zu steuern; die Plugins ermöglichen die Verwendung verschiedener Switche.

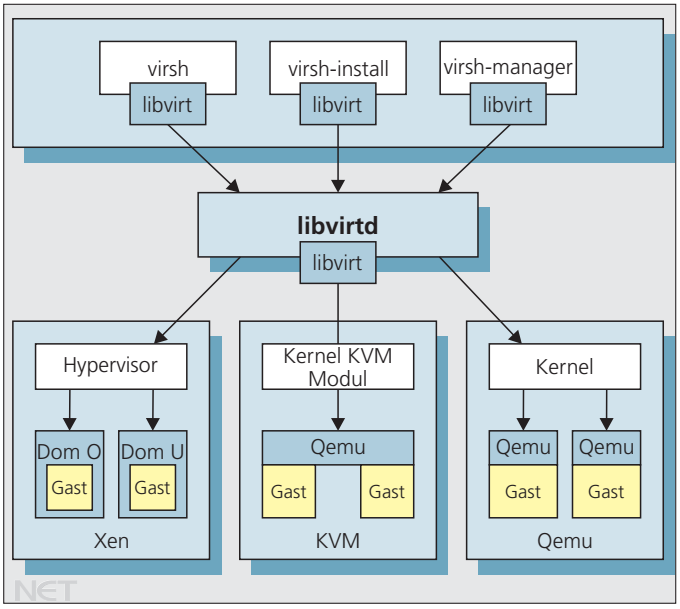

Bild 1: Libvirt-Tools und der Zugriff auf den libvirt-Dämon

Virtuelle Netzumgebungen

Neben den diversen VMs, die verwaltet werden müssen, lassen sich heutzutage auch virtuelle Netzumgebungen umsetzen, z.B. mit Virtual Distributed Ethernet (VDE, **vde.sourceforge.net**) oder Open vSwitch (**www.openvswitch.org**).

VDE stellt eine allgemeine, virtuelle Infrastruktur zur Verbindung verschiedener Softwarekomponenten zur Verfügung. Es lassen sich so VMs verschiedener Virtualisierungslösungen, Emulatoren, reale Betriebssysteme sowie Netze miteinander verbinden. Auf Basis von VDE lassen sich daher sehr einfach und flexibel virtuelle Netze erstellen, deren Teilbereiche sich auf mehreren physischen Rechnern verteilen lassen. VDE ist Ethernet-konform und stellt virtuellen Infrastrukturen virtuelle Switche und virtuelle Kabel zur Verfügung. VDE-Netze bestehen aus folgenden Hauptkomponenten:

- VDE-Switch: übernimmt in der virtuellen Umgebung die gleiche Funktion wie ein physischer Ethernet-Switch in einem realen Netz; verfügt über mehrere Ports, über die verschiedene Systeme einer virtuellen Infrastruktur verbunden werden;
- VDE-Plug: Hilfsprogramm, das sich mit einem Port eines VDE-Switches verbinden kann; universelles Tool, mit dem sich der Datenstrom des virtuellen Netzes auf die Betriebssystemschnittstellen „stdin" und „stdout" umleiten lässt;
- VDE-Wire: Programme zur bidirektionalen Verbindung von Datenströmen miteinander;
- VDE-Cable: besteht aus der Kombination zweier VDE-Plugs und einem VDE-Wire; stellt das virtuelle Pendant zu einem Netzkabel eines realen Netzes dar.

VDE-Switche lassen sich durch VDE-Cables untereinander verbinden. Um Loop-Verbindungen zwischen Switchen zu verhindern, unterstützen sie das Fast-Spanning-Tree-Protokoll. Da ein VDE-Wire sich auch über Netzprotokolle realisieren lässt, können Verbindungen zwischen VDE-Switchen auch über ein physisches Netz hergestellt werden. So lassen sich virtuelle Netze z.B. über eine verschlüsselte SSH-Verbindung sehr einfach zu VPNs zusammenschließen. Zudem unterstützt VDE VLANs nach dem IEEE-802.1Q-Standard.

Open vSwitch ist ein Multilayer-Softwareswitch, der unter der Open-Source-Lizenz Apache 2.0 veröffentlicht wurde. Zielsetzung war es, einen leistungsstarken Softwareswitch zu entwickeln, der einen umfassenden Funktionsumfang bietet und Standardmanagementschnittstellen bereitstellt. Ein großer Nachteil vieler virtueller Umgebungen war bislang deren einfache Netzstruktur. Die meisten Virtualisierungslösungen setzten daher bisher auf einfachen Netz-Bridges auf, um die VMs untereinander sowie mit dem Netz des Host-Systems zu verbinden. Dies will Open vSwitch ändern.

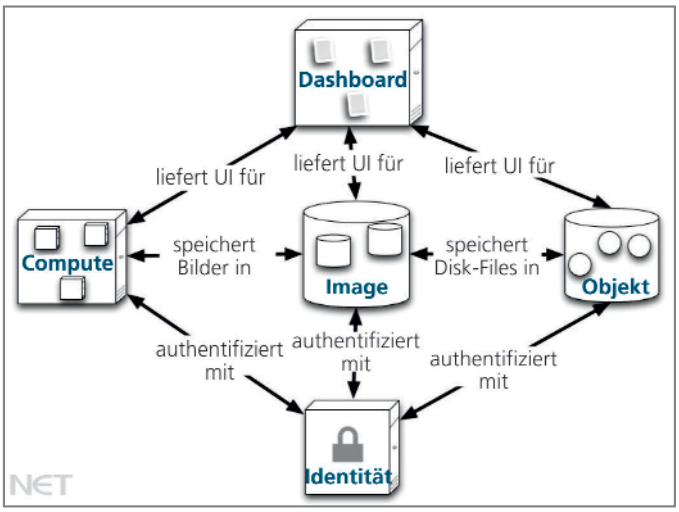

Bild 2: OpenStack-Architektur (Quelle: http://docs.openstack.org)

Netz-Bridges sowie einfache Switche arbeiten auf Schicht 2 des OSI-Referenzmodells. Sobald ein Paket auf dem Switch eintrifft, verarbeitet er die MAC-Adresse des Rechners, von dem das Paket gesendet wurde und legt einen Eintrag in der sog. Source Address Table (SAT) an, die auch den physischen Port, auf dem das Paket eingetroffen ist, enthält. So lernt der Switch, über welchen Port er welche Zieladresse erreichen kann. Falls noch kein Eintrag vorliegt, sendet er das Paket an alle aktiven Ports. Sobald die SAT aufgebaut ist, werden die Pakete nur noch an den Port weitergeleitet, der mit der Zieladresse verknüpft wurde.

Generell unterscheidet man zwischen Layer-2- und Layer-3-Switchen. Professionelle Layer-3-Switche verfügen i.d.R. über Managementfunktionen. Dazu gehören z.B. Steuer- und Überwachungsfunktionen, die auch auf Informationen aus höheren Schichten des OSI-Modells beruhen können, wie z.B. IP-Filterung, VLAN, QoS, Routing.

Für virtuelle Umgebungen fehlten bisher entsprechende Lösungen. Im Bereich der proprietären Produkte entwickelte VMware in Zusammenarbeit mit Cisco Systems den virtuellen Switch Nexus 1000V, der sich in die VMware-Umgebung integriert und entsprechend fortgeschrittene Funktionen bietet. Daneben gibt es Open-Source-Software wie VDE und Open vSwitch. Sie eignet sich insbesondere für den Einsatz als virtueller Switch in virtuellen Umgebungen, wobei sich die virtuellen Netze auch über mehrere physische Server hinweg verteilen lassen. Zugleich bietet sie direkte Unterstützung für verschiedene Linux-basierte Virtualisierungslösungen wie z.B. Xen/XenServer, Virtualbox und KVM.

Open vSwitch hat einen umfassenden Funktionsumfang, der dem realer Switche nahe kommt. Folgende Funktionen seien exemplarisch genannt:

- Standard 802.1Q VLANs mit Trunk und Access-Ports;
- Spanning Tree Protocol (STP) nach IEEE 802.1D-1998;
- Unterstützung von NetFlow, sFlow(R), SPAN, RSPAN und GRE-getunnelten Mirror-Ports;
- OpenFlow-Unterstützung;
- NIC-Bonding mit Source-MAC Load Balancing, Active Backup und L4 Hashing;
- Link Aggregation Control Protocol (LACP) nach IEEE 802.3ad;
- Tunneling-Protokolle (Ethernet-over-GRE, CAPWAP, IPsec, GRE-over-IPsec);
- Quality of Service (QoS), Hierarchical Fair Service Curve (HFSC);
- Continuous Controls Monitoring (CCM) von Links nach IEEE 802.1ag;
- IPv6-Support.

Das Projekt erfreut sich regen Interesses der Open-Source-Community. Ab Version 0.9.11 wird auch die libvirt-API unterstützt. Mittlerweile bieten auch diverse Managementlösungen für virtuelle Umgebungen eine Unterstützung von Open vSwitch an, z.B. openQRM, OpenNebular sowie OpenStack.

Fazit

Die Vielfalt der Lösungen mag zuerst abschrecken. Um allerdings nicht wahllos VMs im Unternehmen aufzusetzen, die alle einzeln verwaltet werden müssen, sollten Management-Tools zu einem ganzheitlichen Konzept vereinigt werden. Dabei können auch Netzverbindungen zwischen den VMs beachtet werden, da sich ganze Netzsegmente virtualisieren lassen. Dies hat u.a. auch Cisco Systems erkannt und mit VMware einen Partner für die Virtualisierungsumgebung eingebunden. Das Forschungsprojekt Visa (**www.visa-project.de**) untersucht aktuell das Zusammenspiel der unterschiedlichen Lösungen und adaptiert sie auf eine gemeinsame Plattform. Dabei stellte sich heraus, dass es diesen Lösungen noch an Dokumentation und teilweise Stabilität mangelt. Mit den unterschiedlichen Bausteinen hat man zwar einen mächtigen Werkzeugkasten zur Hand, nur leider fehlt es momentan an einer detaillierten Beschreibung, wie er zu handhaben ist.

Da aber jedes hier genannte Open-Source-Projekt hauptsächlich seine eigenen Ziele verfolgt, ist dies auch schwer umzusetzen. Allerdings werden Schnittstellen zu den jeweiligen Bausteinen geschaffen, die die gemeinsame Nutzung ermöglichen. OpenStack ist daher bereits heute bei den Cloud-Providern als Verwaltungslösung gesetzt, da diese Softwareverbindungen zu libvirt-API, KVM und Open vSwitch gleichermaßen anbietet und sozusagen als gemeinsamer Nenner fungiert.

OpenStack ist auch die Basis für das Visa-Projekt. Durch die Kombination der unterschiedlichen Bausteine lassen sich ganzheitliche Virtualisierungslösungen schaffen, die auch eine automatisierte Konfiguration ermöglichen. Dies eröffnet Unternehmen zukünftig ganz neue Virtualisierungsmöglichkeiten. *(bk)*