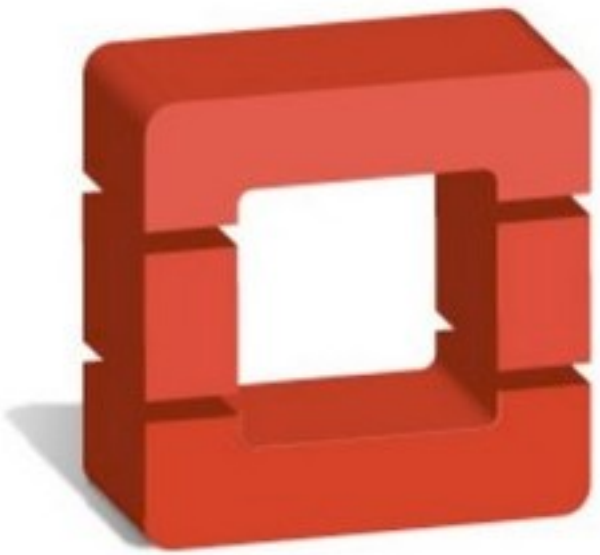
heinlein

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>



Heiter bis wolkig

OpenStack und CloudStack im Vergleich

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Einleitung

- OpenStack & CloudStack sind Cloud-Plattformen
- Hoher Automatisierungsgrad möglich
- Orchestrierungs-Tools für Large-Scale-Deployments
- Hoher Standardisierungsgrad notwendig
- Keine „All-Purpose“ Virtualisierungsplattformen
  - Kein direkter VMware vSphere Ersatz
  - VMware vCloud Suite / Director

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Cloud-Plattform

- Infrastructure as a Service (IaaS)
- Virtualization
- Automatization
- Software defined Networking
- Software defined Storage

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Geschichte

apachecloudstack™

- 2010 von Cloud.com freigegeben
  - ca 5% noch proprietär
- 2011 von Citrix gekauft
  - nun alles unter GPL
- 2012 von Citrix an die Apache Software Foundation
- 2013 „Top Level Project“ bei ASF

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Geschichte

- 2010 NASA und RackSpace
  - Nebula
  - Cloud Files
- 2011 Ubuntu
- 2012 Debian und RedHat

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Konzepte

apachecloudstack™

- Hierarchische Struktur
  - Regionen
  - Ausfallzonen (Availability Zones)
  - Pods
  - Cluster
- Dashboard
  - managed Availability Zones über Locations hinweg
  - grobes Monitoring
  - braucht SQL Backend
- Identity Management
  - LDAP und AD Integration

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

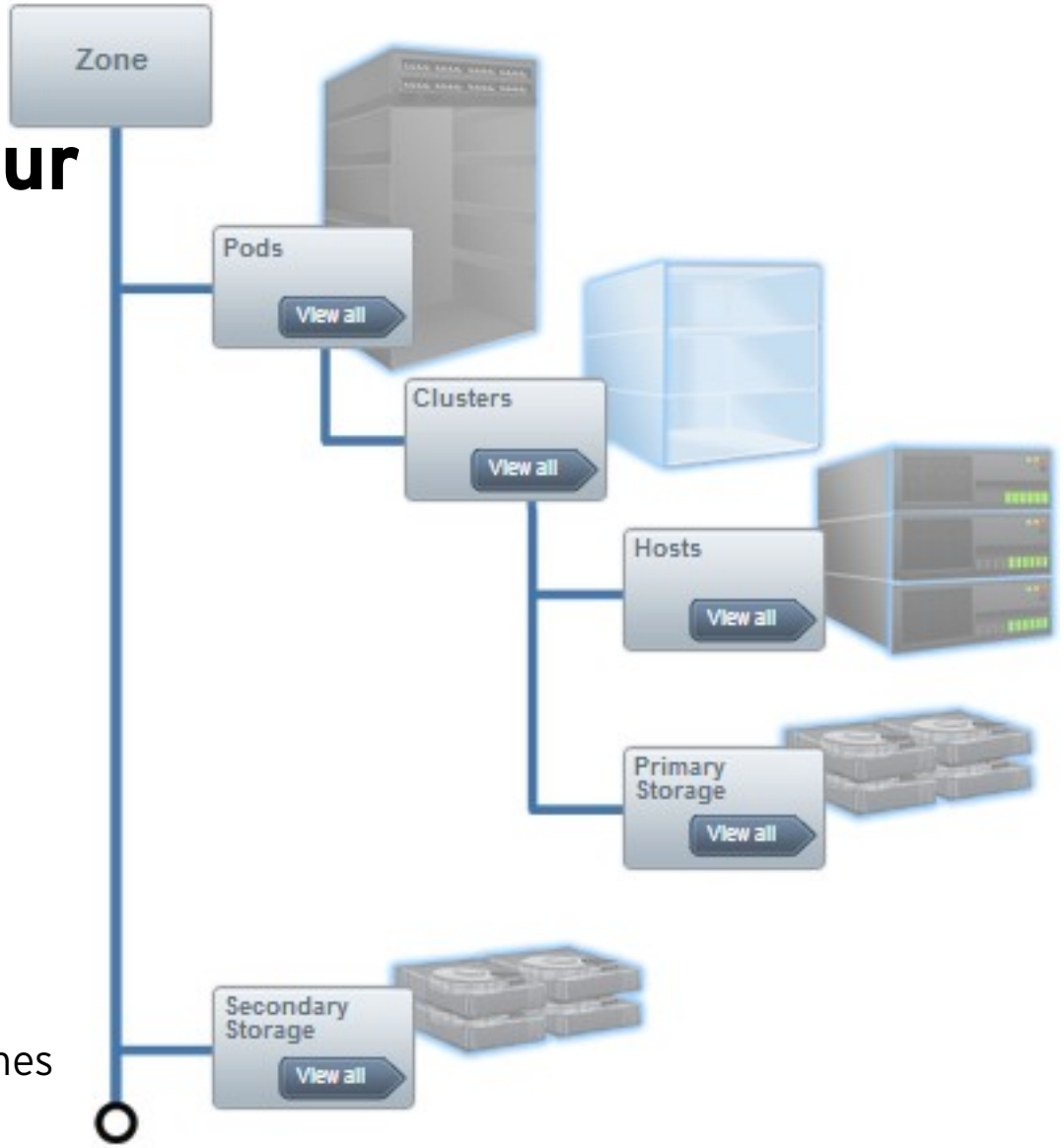
Was ist CloudStack?

apachecloudstack™

- Open-Source IaaS Plattform
  - Provisionierung und Orchestrierung von
    - Storage Pools
    - IPv4 und IPv6 Netzsegmenten
    - Compute Ressourcen
    - Software-defined und Bare-Metal
- Zentrales Management für
  - Automatisches Config-Management
  - Hypervisor und Container
    - Vsphere (via vCenter)
    - KVM
    - XenServer
    - LXC
    - Bare-Metal (via IPMI)

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Aufbau und Nomenklatur



- Zone (Verfügbarkeitszone)
  - Äquivalent zu einem DC
  - enthält PODs und 2nd. Storage
- POD
  - Üblicherweise ein Rack
  - enthält L2 – Switch und Cluster
- Cluster
  - Meist zwei bis drei Hosts
  - ein primäres Storage
- Primäres Storage
  - DAS oder shared, enthält Disk-Volumes
- Sekundäres Storage
  - VM Templates, Installations-ISOs, VM Disk Image Snapshots und Backup

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Was verwaltet CloudStack? apachecloudstack™

- Hardware und Cloud-Ressourcen
  - Storage Pools auf FC, iSCSI, Gluster, Ceph...
  - Netzwerkkomponenten
    - z.B. CloudStack Network Guru Plugin von Juniper Networks (lt. Juniper getestet mit KVM Hosts)
    - z.B. Cisco Nexus 1000v / Cisco ASA 1000v / Cisco VNMC (virtual Appliances) Cloudstack ← XML API → Cisco Virtual Network Management Platform
    - Firewall Regeln
    - SNAT, DNAT, Port Forwarding, ASA VPN
  - Bordergateways, SSL-Offloading-Appliances und Application-Delivery
    - z.B. Citrix NetScaler VPX
    - z.B. F5 Big-IP
- System-/Service-VM's
  - Router, Switch, VPN, Firewall, HA bzw. Keepalive Monitor

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Netzwerk Konzept

apachecloudstack™

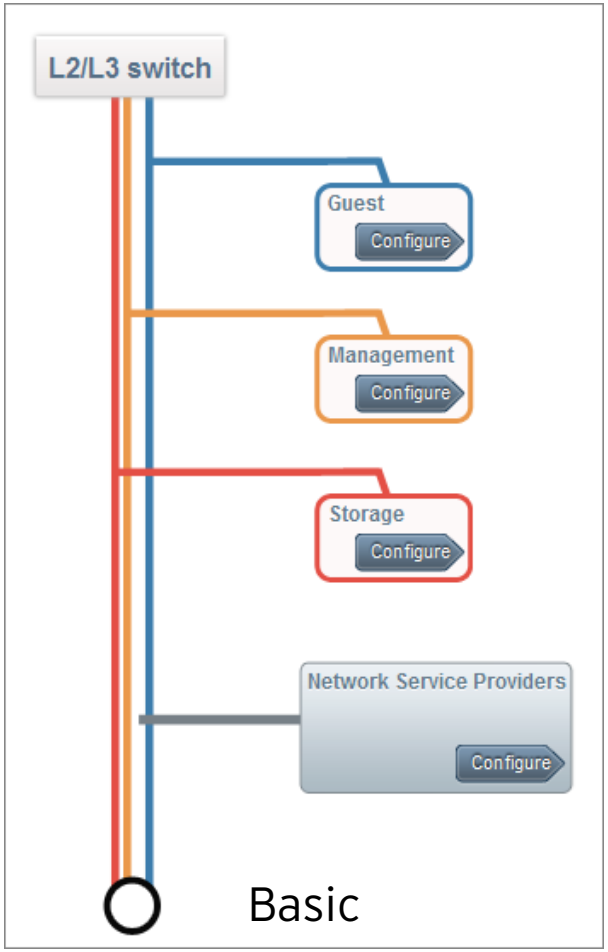
- Netzwerk Klassifizierung, Trennung durch VLANs.
  - Guest
    - Kommunikation der IaaS Ressourcen eines Benutzers bzw. eines Tenant.
    - Häufig sehr ähnlich einem Office-LAN (VPN Gateway, Router, RFC1618 LAN, ...)
  - Management
    - Kommunikation der internen Ressourcen zwischen Hosts und System-VMs
    - auch der Management-Node mit Dashboard nutzt dieses Netz
  - Storage
    - Anbindung der Primären und Sekundären Storages
    - Provisionierung findet über eine Storage-System-VM statt, d.h.
    - Anbindung auch dieser speziellen VMs
  - Public
    - Öffentliche IP Bereiche
    - Terminierung an Router, etc... System-VMs üblich

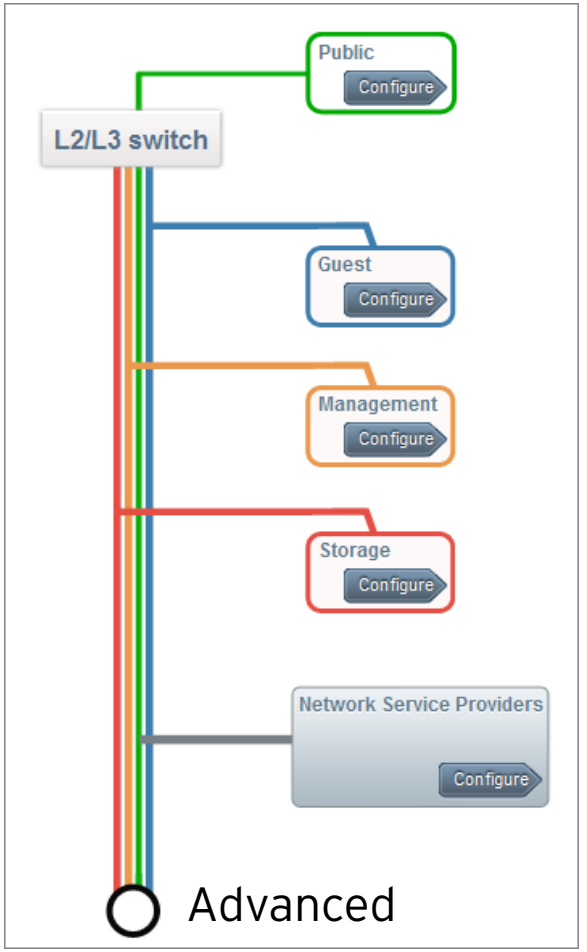
heinlein

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Netzwerk Modelle

apachecloudstack™





OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Basic Networking

apachecloudstack™

- Nutzung eines gemeinsamen IP-Bereichs für
  - Guest Instanzen
  - Cloudstack Verwaltung (Management)
  - Hosts und Hypervisors
- Beispiel:
  - Basic Networking mit RFC 1918 z.B. 172.16.0/20 für jede Zone
    - erlaubt mehr als 4000 IPs per Zone (Besser < /16 - Weitere Zonen berücksichtigen)
    - Addressbereiche für Management müssen (initial und in ausreichender Menge) definiert werden. Diese Addressen stehen dann natürlich nicht für Guests bereit...
  - Jeder POD in einer Basic Zone entspricht einer Broadcast Domain
    - Folgend hat jeder POD eine unterschiedliche IP Range für Guest Netze.
  - Jeder Host, jede System-VM und jeder Gast Instanz benötigt eine eindeutige IP im gleichen Segment.
- Schnell aufzusetzen, produktiv je nach Szenario bedingt sinnvoll

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Advanced Networking

apachecloudstack™

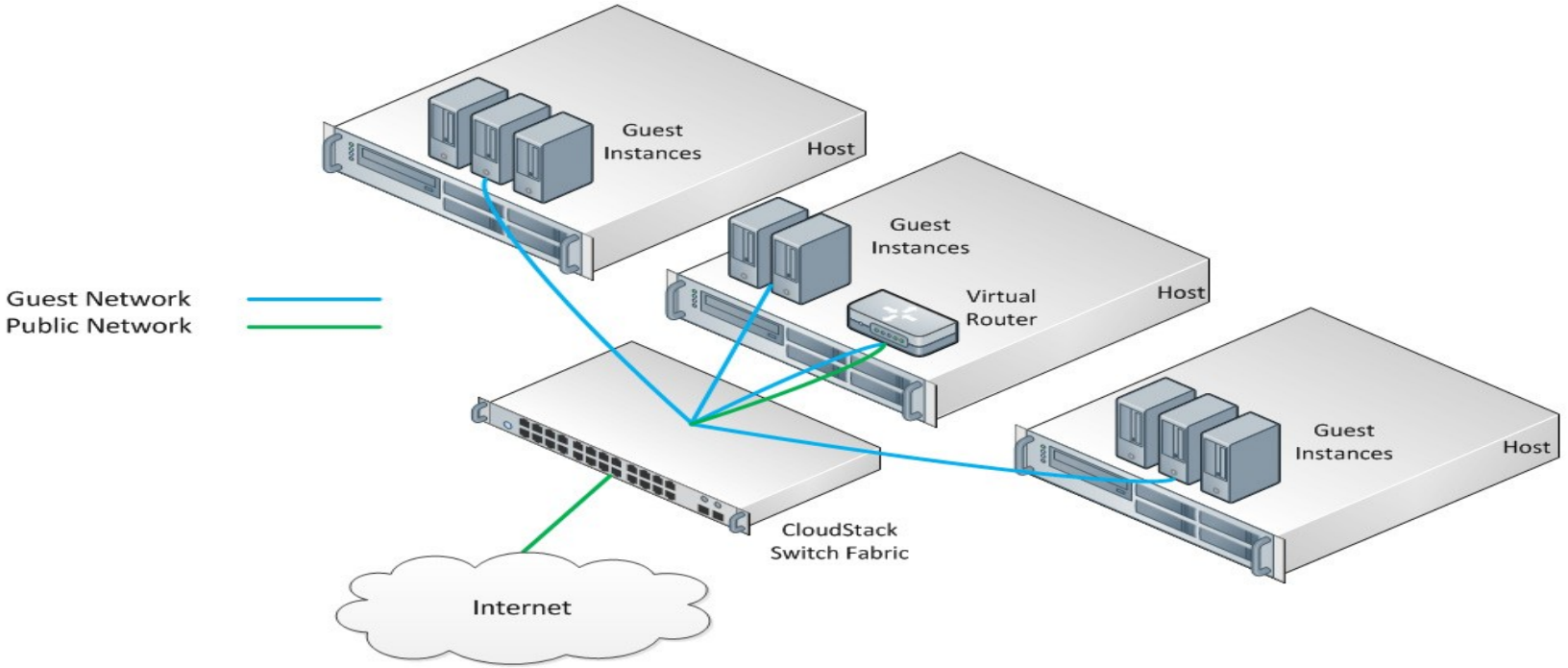
- Jeder Account erhält
  - Öffentliche IPs die der Router System-VM zugewiesen sind
  - Guest IP Bereich aus RFC 1918 z.B. 10.1.1/24
  - VLAN ID für das isolierte Guest Netzwerk
- Standard Guest IP-Bereich ist für alle Accounts einer Zone identisch
  - Trennung findet durch VLAN statt
- Kommunikation über eigenes VLAN
  - Guest Instanzen untereinander
  - Guest Instanzen mit dem Virtual Router (System-VM)
- Benötigt eingerichtete VLAN auf der Switch Fabric
  - Hostübergreifende Guest Kommunikation über VLAN Trunks auf den Switches

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Advanced Networking

apachecloudstack™

- Beispiel
  - Ein Account auf einem POD über drei Hosts



Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Netzplanung

apachecloudstack™

- System IP-Adressen
  - Ein POD benötigt üblicherweise etwa 10 IP-Adressen für
    - Hostsysteme
    - Secondary-Storage System-VM
    - Console-Proxy System-VM (werden automatisch instanziert, d.h. es können mehrere dieser Proxies von CloudStack gestartet werden)
  - Jeder Host und jede System-VM benötigen eine „cloud-weit" eindeutige IP.
  - Werden weitere Zonen angelegt, muss das berücksichtigt werden
- Link-Local Adressen
  - KVM und XenServer verwenden innerhalb der Hosts Link-Local Adressen für
    - alle System-VMs und
    - alle Virtual Router
  - KVM und XenServer PODs können ein vollständiges /24 für Host und Storage nutzen
  - VMware PODs erhalten idealerweise ein /21 um 2046 IP für Host und Storage zu nutzen

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Storage Modelle

apachecloudstack™

- Primary Storage
  - hält VM Disk Images im entsprechend unterstützten Format (qcow, vhd, vmdk, ...)
  - mindestens ein Primary Storage je Cluster
  - Primary Storage muss für laufende VM dauerhaft konnektiert bleiben
  - mehrere Primary Storages als Storage Repository (SR) möglich
  - Storage Migration zwischen identischen Formaten direkt möglich
- Secondary Storage
  - hält Template Images, VM Disk Snapshots und Backups
  - mindestens ein Secondary Storage je Zone
  - wird bevorzugt als NFS eingebunden
  - darf zu Maintenance im Betrieb *temporär* entfernt werden
  - mehrere Secondary Storages möglich
  - kann im Desasterfall (Ausfall eines Primary Storage) direkt VM Disk Images bereitstellen
  - ist Zwischenziel bei Storage Migrationen über Cluster und POD Grenzen hinweg

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Primary Storage Support

apachecloudstack™

	VMware vSphere	XenServer	KVM
Disk-, Template- und Snapshot-Format	VMDK / OVA	VHD	QCOW2
iSCSI	via VMFS	Clustered LVM	Shared Mountpoint
Fiber Channel	via VMFS	bei bestehendem Storage Pool	Shared Mountpoint
Local Storage	unterstützt	unterstützt	unterstützt
NFS	unterstützt	unterstützt	unterstützt
Thin / Overprovisioning	NFS und iSCSI	NFS	NFS

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Ceph Primary Storage

apachecloudstack™

- RBD als Storage **Pool** (kein RBD per VM)
  - vollständig unterstützt ab CloudStack Version 4.4.0 (möglich ab 4.2.0)
  - benötigt librbd ab Version 0.67 (Ceph Dumpling, Emperor oder Firefly)
    - Ideale Hostplattform enthält libvirt librbd in aktuellen Versionen, z.B. Ubuntu 14.04 LTS als KVM Plattform
    - Möglich auf auf XenServer (mit CentOS und Fedora Repositories) dadurch evtl. kein sauberer Update-Pfad auf dem Host
  - Aktuelle Beschränkung auf eine (1) MON-Verbindung
    - Workaround durch DNS Round-Robin möglich
  - Disk Image QCOW2 ↔ RAW Umwandlung für Ceph bei CloudStack < 4.4.0 in /tmp
    - benötigt >= 25 GB freien Platz in /tmp
    - ab 4.4.0 korrigiert
  - Konsolidierung der OSD auf den Compute-Nodes *möglich*, besser dezidierter Ceph Cluster mit jeweils einem RBD Storage Pool per Cluster
  - Fazit: Perfekte Lösung, wenn die aktuellen Workarounds akzeptabel sind

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Gluster Storage

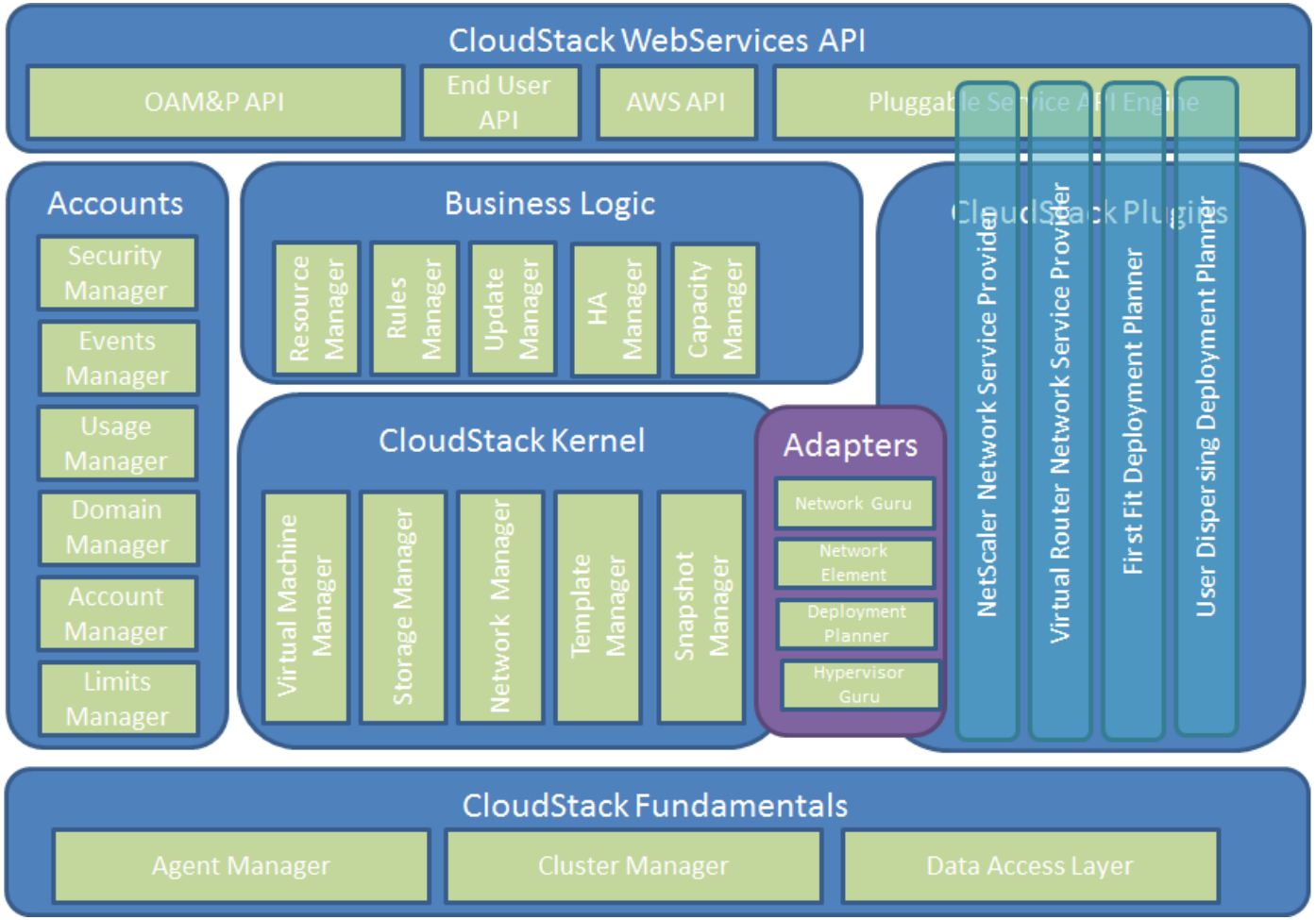
apachecloudstack™

- Aktuell work-in-progress
- Gluster als Primary Storage
  - Wird über den nativen GlusterFS FUSE client eingebunden
  - benötigt Entwickler Repository https://forge.gluster.org/cloudstack-gluster
- Gluster als Secondary Storage
  - Ebenfalls über GlusterFS FUSE möglich

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

API Struktur

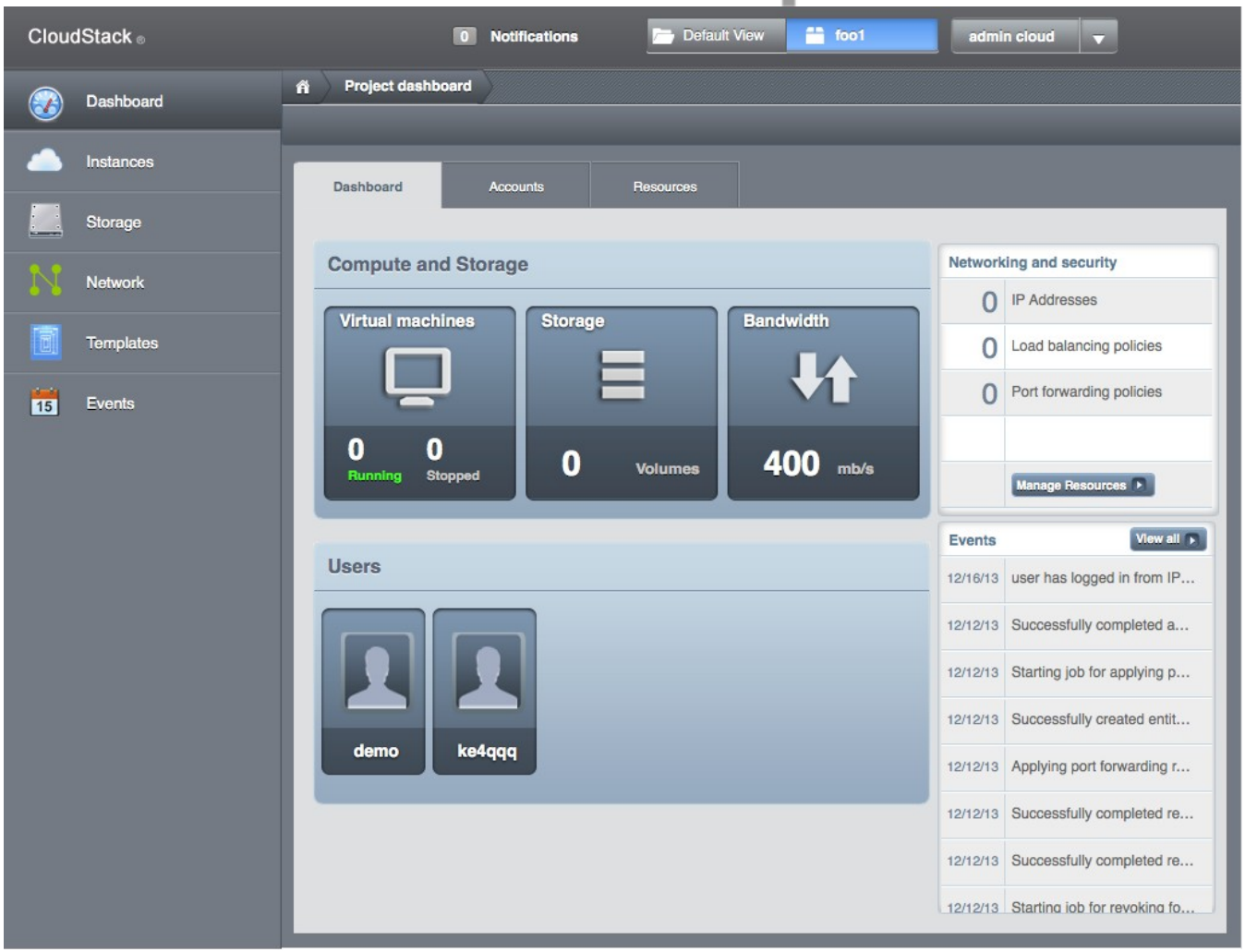
apachecloudstack™



OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Blick auf das Dashboard

apachecloudstack™



OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

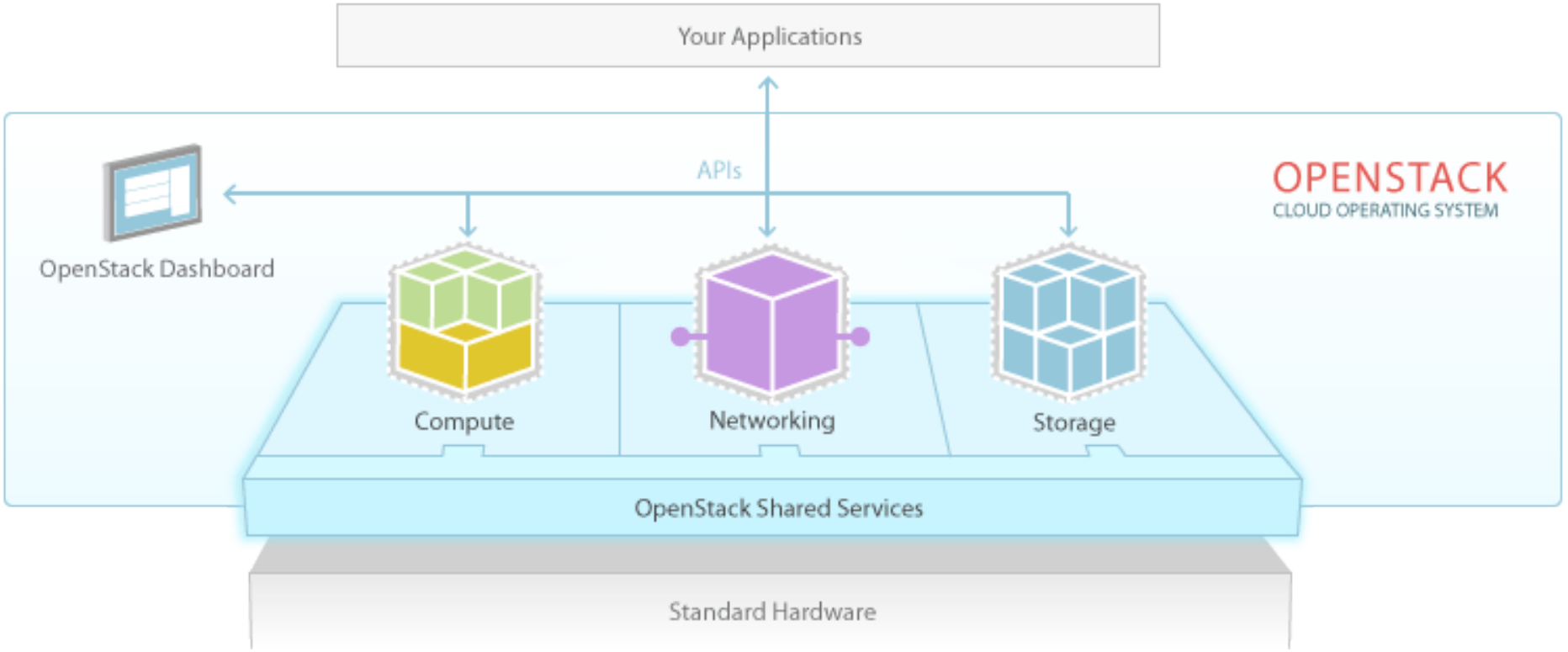
Konzept

- Flache Hierarchie
- Jeder Knoten kann prinzipiell jede Rolle übernehmen
  - Compute (Nova)
  - Object Storage (Swift)
  - Block Storage (Cinder)
  - Image Service (Glance)
  - Networking (Neutron)
  - Dashboard (Horizon)
  - Identity Service (Keystone)
  - Telemetry (Ceilometer)
  - Orchestration (Heat)

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Übersicht

openstack
CLOUD SOFTWARE



Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Compute
Nova

- Das Gehirn von OpenStack
- Steuert die Hypervisoren
  - KVM
  - Xen, XenServer
  - VMware
  - HyperV
  - LXC, Docker
- Verwaltet die Resourcen & VMs
  - In Projekten mit Benutzern von Keystone
  - Bare Metal mit OpenStack Ironic

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

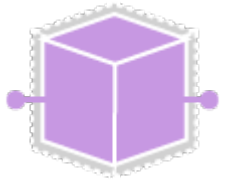
Storage
Glance / Cinder / Swift

- Images in Glance
  - Templates
  - Instanzen (VMs) flüchtig
- Blockstorage in Cinder
  - LVM auf iSCSI
  - Ceph, Gluster
  - NetApp, Nexenta, SolidFire etc.
- ObjectStorage in Swift
  - oder Rados-GW von Ceph

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Networking Neutron

openstack CLOUD SOFTWARE



- Vernetzt VMs
- Flaches Netzwerk
- Projekte in eigenen VLANs
- Software defined Networking
  - OpenFLOW / Open vSwitch
  - VMware NSX
  - ...
- LBaaS
- FWaaS
- VPNaaS

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Dashboard Horizon

- Weboberfläche
- Neben der API die Benutzerschnittstelle
- Alles auf einen Blick
- Spricht mit allen anderen Komponenten

- Für Admins und Kunden (bzw. deren Admins)

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Identity
Keystone

- Verzeichnis für Benutzerkonten
- Authentifizierung mit Passwort / Token
- Policies über Nutzer und Systeme
- Authorization für Computer, Storage, Network etc.

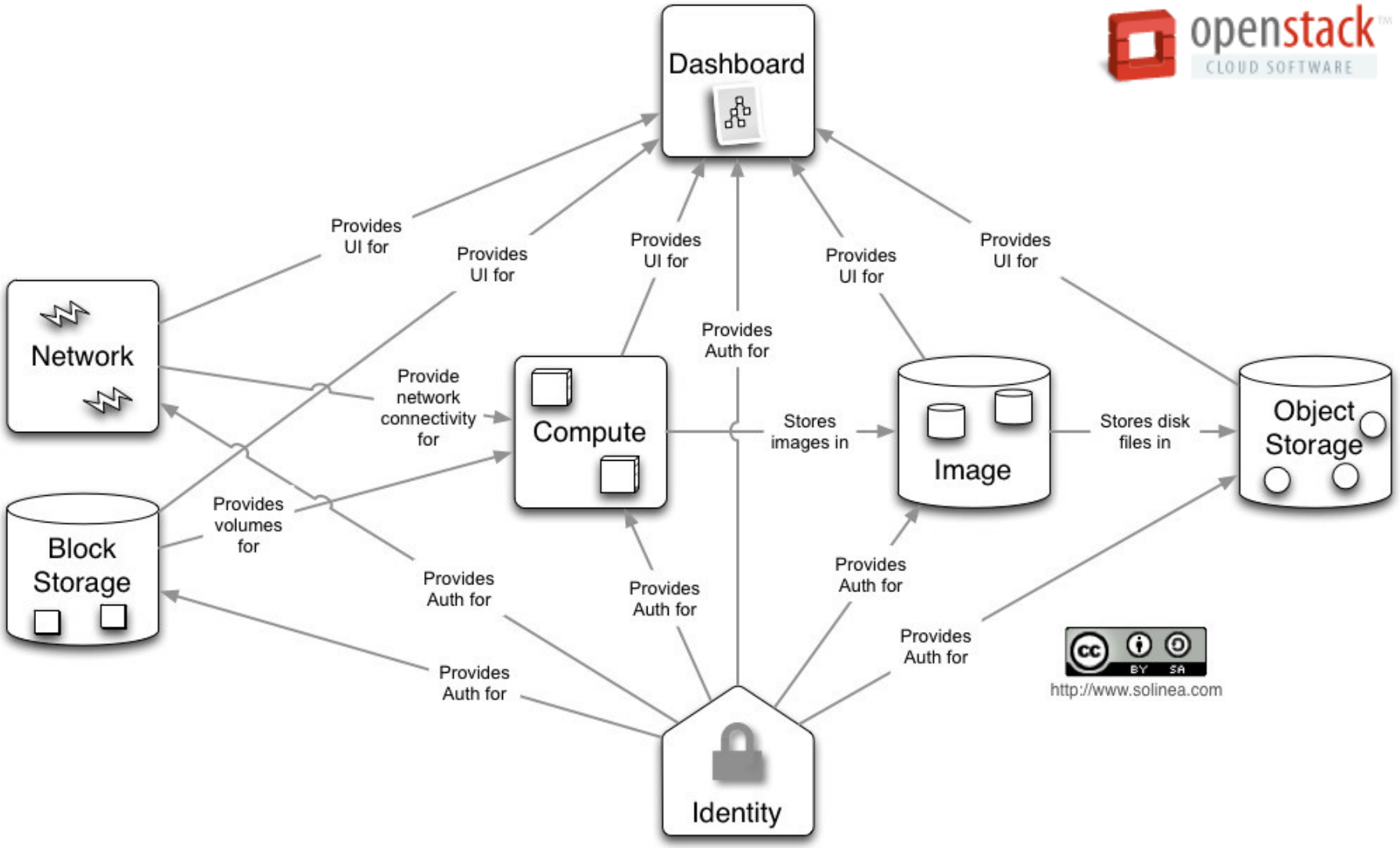
- Anbindung an LDAP o.ä. möglich

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Shared Services

- **Telemetry (Ceilometer)**
  - Messdaten
  - Schnittstelle zu Abrechnung
- **Orchestration (Heat)**
  - Automatisierung von Infrastrukturaufbau

OpenStack und CloudStack im Vergleich
[CeBIT 2014]
Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>



Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Testen

- DevStack
  - Ein Skript zum Installieren und Deploy
  - http://devstack.org
- Mirantis
  - Ein ISO all inclusive
  - Fuel-Master
  - Mehrere OpenStack-Instanzen möglich
  - VirtualBox-Support
  - Savannah für Hadoop
  - http://software.mirantis.com/
  - Download nach Registrierung

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Anwendungsgebiete

apachecloudstack™

- Klar definierte Requirements
- Skalierbarkeit
- S3 API
- Templatebasiertes Rollout
- IaaS
- kein „Vendor Lock-In“
- Support für eine Variante von mehreren ISVs

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Anwendungsgebiete

- Komplexe Integration
- Skalierbarkeit
- S3 API
- Templatebasiertes Rollout
- „Selberskripten“ von PaaS und SaaS Deployments
- Restrukturierung des gesamten Deployments möglich
- kein „Vendor Lock-In“
- Support für mehrere Varianten von mehreren ISVs

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Infrastruktur

apachecloudstack™

- Compute
  - KVM (ab RHEL 6.2)
  - Xen OSS
  - XenServer 6.1
  - VMware ESXi 5.1
  - Linux Container LXC
  - Bare Metal
- Storage
  - Ceph
  - NFS / Gluster
  - iSCSI / DAS

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Infrastruktur

openstack CLOUD SOFTWARE

- Compute
  - KVM
  - Xen OSS
  - XenServer
  - VMware ESXi 4.1
  - Hyper-V
  - Linux Container LXC
  - User Mode Linux UML
  - Docker
- Storage
  - Ceph
  - NFS / Gluster
  - iSCSI / DAS

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Fazit

- CloudStack ist ein (fast) fertiges Produkt
  - Installieren
  - Netzwerkmodell festlegen (Flat oder VLANs)
  - loslegen
- OpenStack ist eher ein Framework
  - muß durch eigene Entwicklung angepasst werden
  - viele ISVs haben OpenStack-Distributionen & Installer
  - genau schauen, was gebraucht wird

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

heinlein

Stephan Seitz <s.seitz@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.