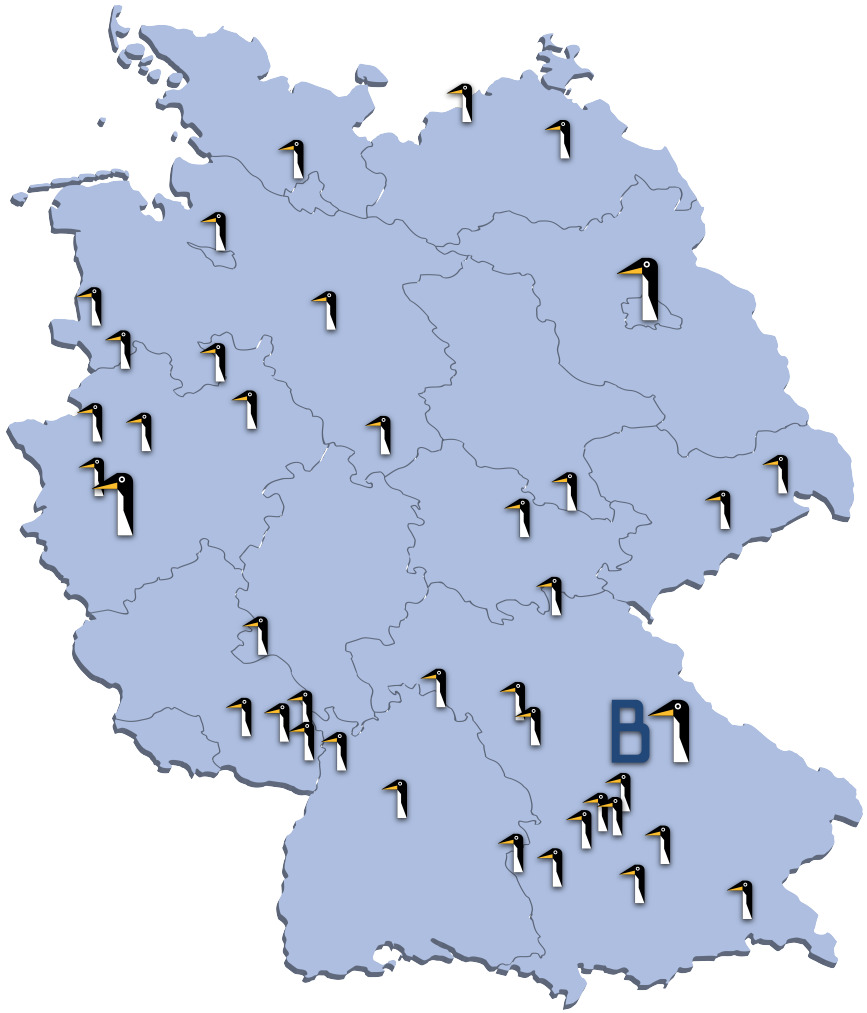
OpenStack: Cloud Management

Sebastian Zielenski
Linux / Unix Consultant & Trainer
B1 Systems GmbH
www.b1-systems.de
zielenski@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source Themen
- national & international tätig
- über 60 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Schwerpunkte:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- dezentrale Strukturen

B1 Systems in Ihrer Nähe



OpenStack: Cloud Management

- Einführung
- Patchmanagement

  M 4.CM.15: Patchmanagement für Cloud Komponenten
- Mandantenfähigkeit von OpenStack

  M 4.CM.16: Durchgängige Mandantentrennung von Cloud Diensten
- Benutzer- & Berechtigungsverwaltung

  M 2.CM.17: Geregelte Benutzer und Berechtigungsverwaltung im Cloud Computing
- Automatisierung

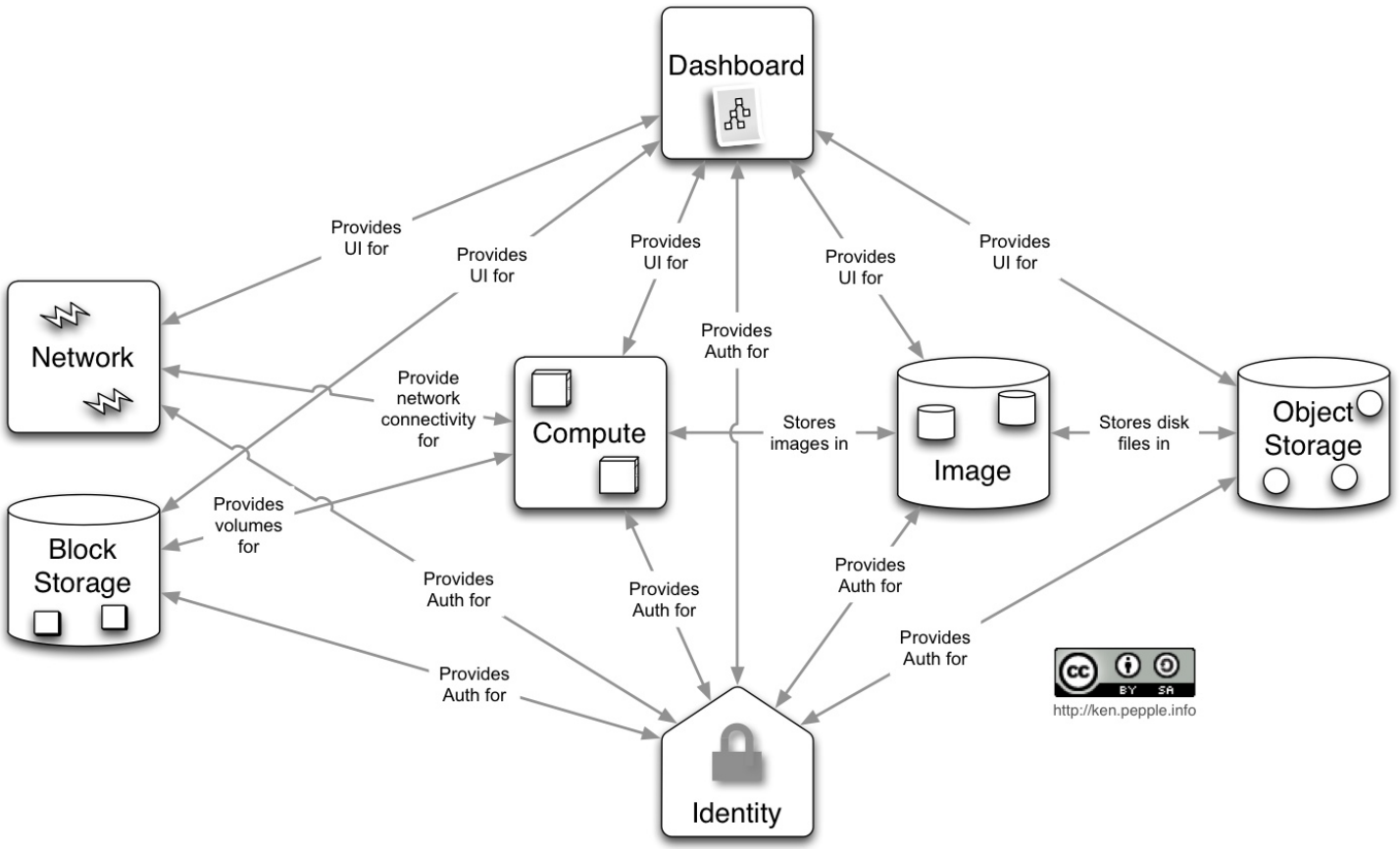
  M 2.CM.21: Sichere Automatisierung der Cloud Regelprozesse
- Allgemeine Sicherheitsaspekte

Einführung

Überblick über OpenStack

- Komponenten zur Umsetzung einer vollständigen Infrastructure as a Service (IAAS) Umgebung
  - Virtualisierung
  - Netzwerk
  - Storage
  - Identity Management
  - Orchestrierung
  - Messung
- hohe Akzeptanz in der Industrie

Architektur von OpenStack Grizzly



M 4.CM.15: Patchmanagement

Zuständigkeiten im Patchmanagement

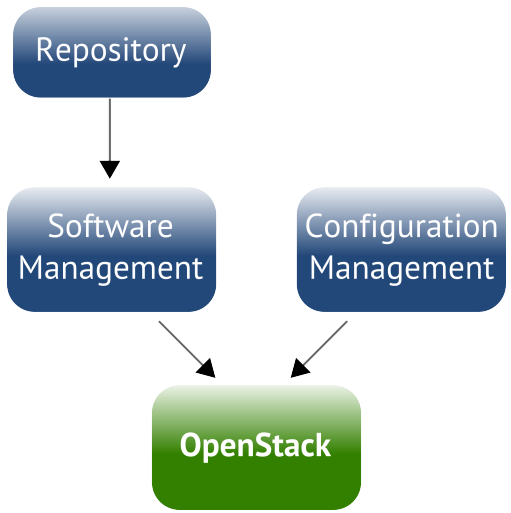
- Zuständigkeit des Bereitstellers liegt bei OpenStack Komponenten wie Keystone, Glance, Nova, ...
- bei Nutzung von externen Komponenten wie Database, Storage oder Networking erfolgt das Patchmanagement entsprechend der dort definierten Prozesse
- Kunden sind für das Patchmanagement innerhalb ihrer Instanzen zuständig

Bereitstellung der Softwarepakete

- durch die Community von Distributionen wie openSUSE oder Fedora
- durch Dritthersteller wie Rackspace oder SUSE
- Unterschiede in den Qualitätsanforderungen:
  - Durchführung von Funktionstests
  - Durchführung von Integrationstests
  - Backporting von kritischen Bugfixes

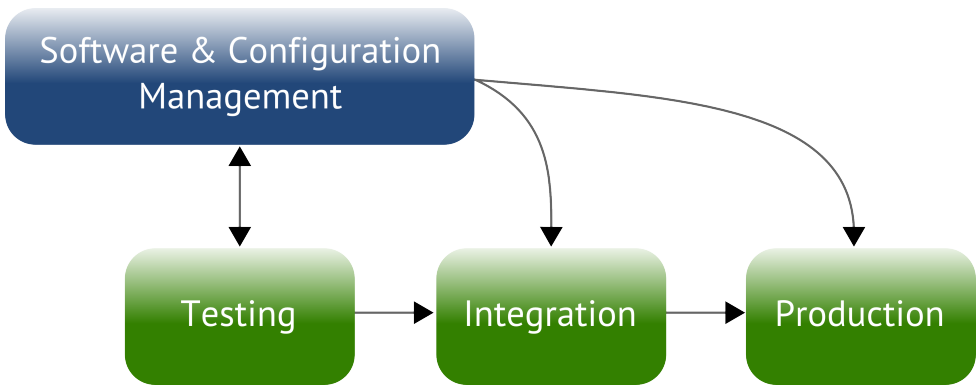
Umsetzung von Änderungen in der Umgebung

- Nutzung von Software Management wie Spacewalk oder Katello zur Bereitstellung der Softwarepakete sowie Review durch den Bereitsteller
- Nutzung von Configuration Management wie Puppet, Chef oder Ansible zur Bereitstellung und Pflege der Konfigurationen
- Nutzung von Deployment Frameworks wie Crowbar oder Foreman zum Deployment von Compute- und Storage Nodes



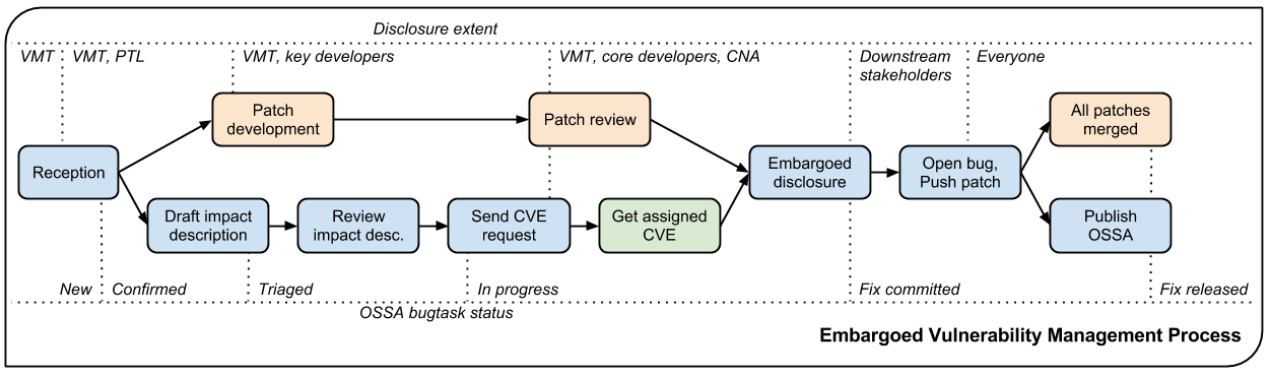
Staging zur Qualitätssicherung

- Staging von Paketen im Software Management durch Bereitsteller
- Nutzung von – bei Bedarf mehrstufigen – Staging-Umgebungen, um definierte Tests durchzuführen
- Identifizierung von Sicherheitsproblemen bereits vor der Produktion (z.B. durch Nutzung von Metasploit, . . .)



Vulnerability Management

- OpenStack Vulnerability Management Team (VMT) sowie OpenStack Security Group (OSSG) zuständig für Behandlung von Sicherheitsproblemen
  - OpenStack Security Advisories (OSSA)
  - OpenStack Security Notes (OSSN)
- definierter Prozess zur Behandlung von Sicherheitsproblemen



Bildquelle: https://wiki.openstack.org/wiki/File:VMTprocess.png

Maintenance von OpenStack

- Releases erfolgen alle sechs Monate
  - aktuell ist Grizzly, Havana erscheint im Oktober 2013
- Backports kritischer Patches bis zum Erscheinen des nächsten Releases
  - z.B. für Folsom bis zum Release von Havana
- Maintenance Releases erfolgen alle zwei bis drei Monate
  - z.B. Grizzly 2013.1.3 im August 2013

M 4.CM.16: Mandantenfähigkeit

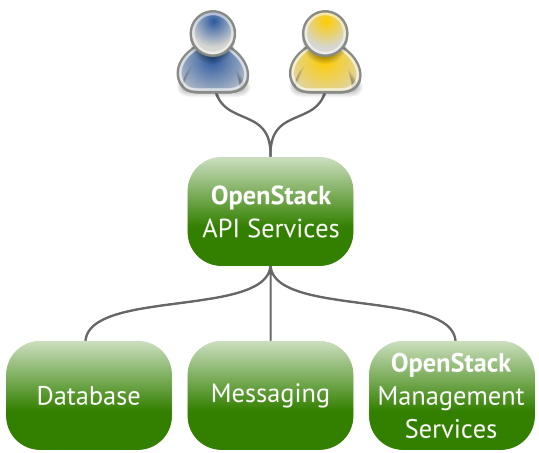
Mandantenfähigkeit von OpenStack

- direkter Zugriff von Kunden nur auf API Services (Management Netzwerk) und Instanzen (Public Netzwerk) möglich
- kein direkter Zugriff von Kunden auf Storage- und Compute-Syteme
- Bereitstellung von Storage über virtuelle Block Devices in Instanzen
- Bereitstellung von Netzwerken über virtuelle Netzwerkkarten in Instanzen

Shared Services

- gemeinsame Nutzung von OpenStack API Services sowie interner Management Services durch Kunden

- Zugriff auf nicht-autorisierte Daten prinzipiell möglich
- Nutzung von nicht-autorisierten API-Methoden prinzipiell möglich
- Auswirkung von Race Conditions auf nicht-autorisierte Daten prinzipiell möglich

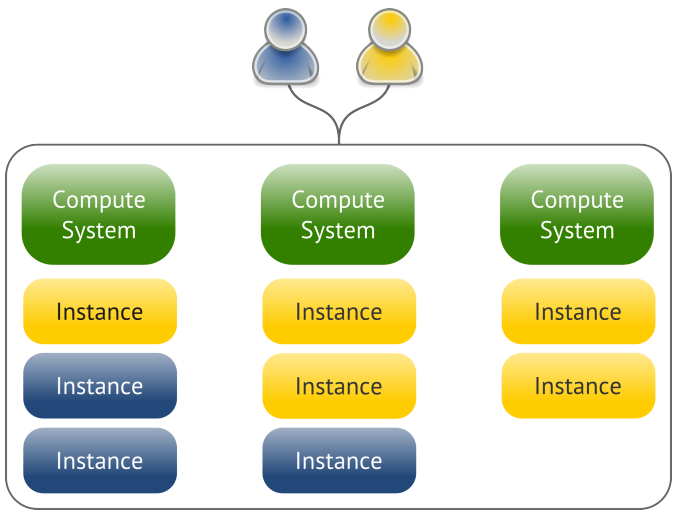


Maßnahme: Shared Services

- Bereitstellung weitestgehend oder vollständig unabhängiger OpenStack-Umgebungen
  - Nutzung von Verfügbarkeitszonen
  - Nutzung von Zellen
- Nutzung von Security Frameworks zur Reduzierung von Race Conditions
- regelmäßiges Auditing durch zentrales Logging

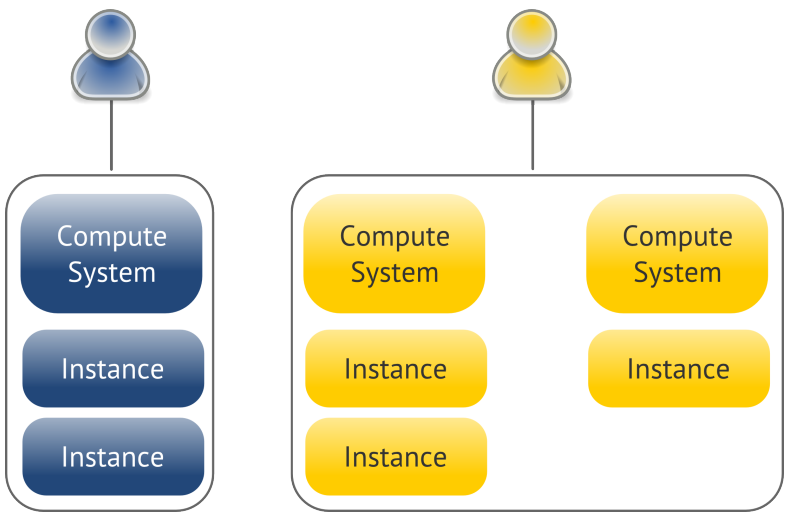
Geteilte Compute Systeme

- transparente Nutzung von physikalischen Systemen durch mehrere Kunden
- Zugriff auf nicht-autorisierte Instanzen, Netzwerke oder Storage durch Ausnutzen von Fehlern im Virtual Machine Monitor, mit resultierendem Zugriff auf die unterliegende Ebene, prinzipiell möglich



Maßnahme: Isolierte Compute Systeme

- Reduzierung der Risiken durch privilegierte Nutzung von physikalischen Systemen
- Umsetzung durch Nutzung von Verfügbarkeitszonen und angepasstes Scheduling



M 2.CM.17: Benutzer- & Berechtigungsverwaltung

Zentraler Authentifizierungsdienst

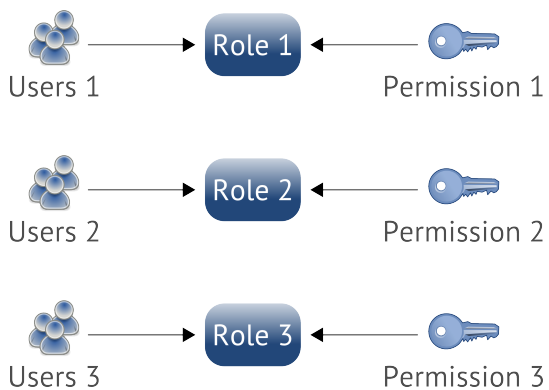
- Nutzung des OpenStack Identity Service (Keystone)
- zentrale Komponente für das Accountmanagement für alle OpenStack Komponenten
- Nutzung von bestehenden Backends (LDAP, Active Directory, ...) ist möglich
- übernimmt zusätzlich die Bereitstellung eines Service Katalogs

Benutzer- & Berechtigungskonzept

- Benutzer
- Tenants
- Token
- Rollen
- ab Havana:
  - Gruppen
  - Domains
  - Regeln

Policies mittels Rollen und Regeln

- Nutzung von Role Based Access Control (RBAC) für alle OpenStack API Services
- Rollen werden Benutzern auf dem OpenStack Identity Service zugewiesen
- Regeln definieren, welche Rollen zur Durchführung einer Aktion notwendig sind
- vor Durchführung einer Aktion wird geprüft, ob einer Aktion zugewiesene Regeln erfüllt werden



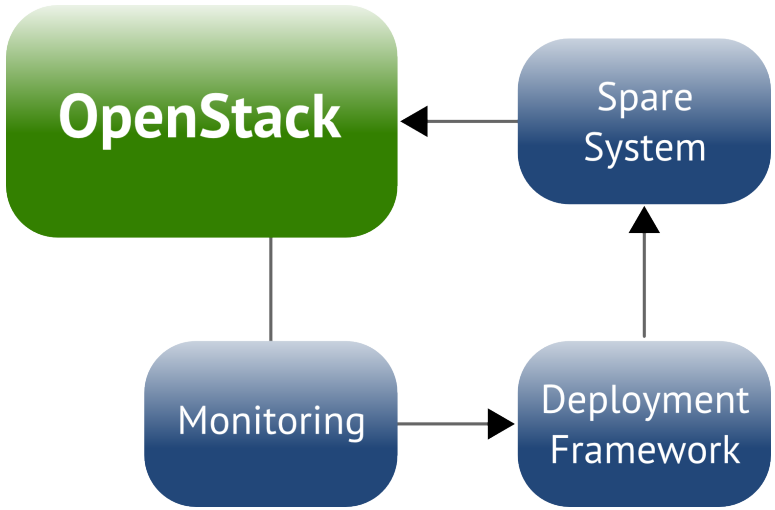
M 2.CM.21: Automatisierung

Automatisierung

- horizontales Skalieren aller OpenStack-Komponenten möglich
- Nutzung von Monitoring sowie Measurement & Orchestration Service zur Bereitstellung von Ressourcen
- Hochverfügbarkeit aller OpenStack-Komponenten zur Reduzierung von Ausfällen

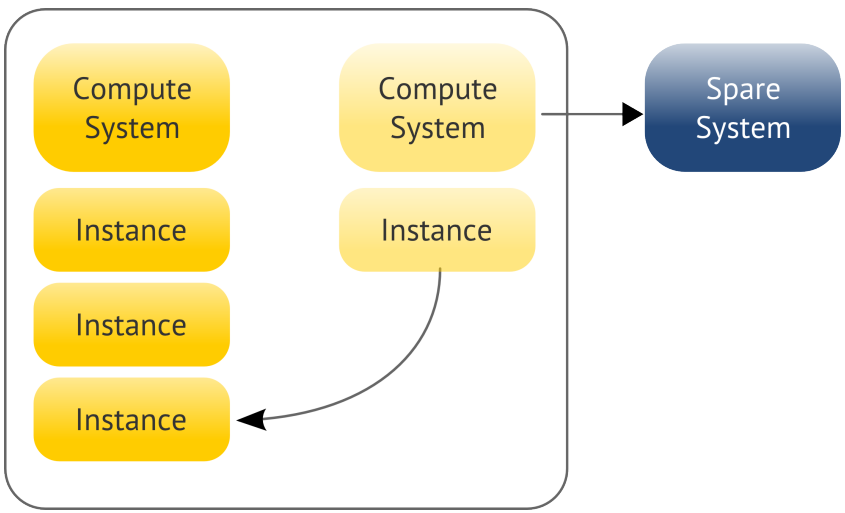
Skalierung 1/2

- Erweiterung der Ressourcen durch Einbindung neuer Compute- oder Storage-Systeme bei Bedarf durch den Bereitsteller



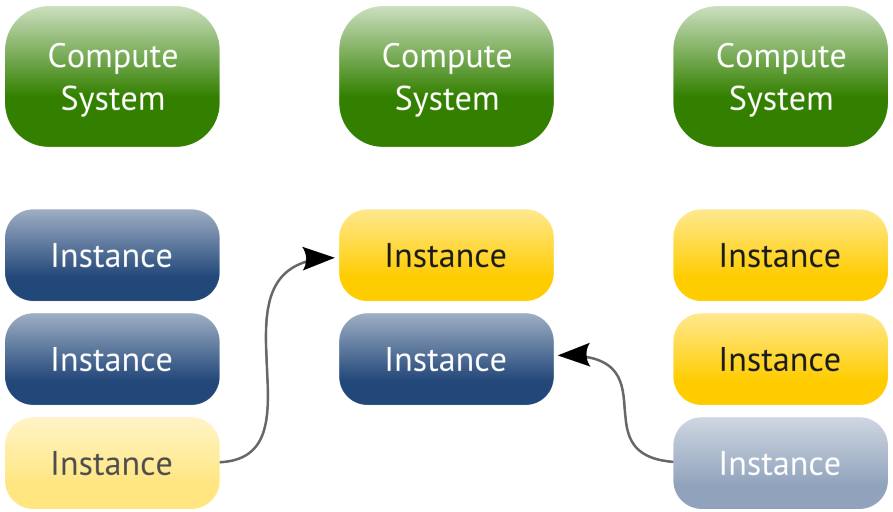
Skalierung 2/2

- Reduzierung verfügbarer Ressourcen durch Entfernung ungenutzter Compute- oder Storage-Systeme durch den Bereitsteller
- Live Migration von Block Storage und Instanzen zur Vorbereitung



Balancierung

- automatisiertes Ausbalancieren genutzter Ressourcen zur Optimierung der Auslastung
- angepasstes Scheduling ermöglicht definierte Auslastung verfügbarer Ressourcen



Allgemeine Sicherheitsaspekte

Verschlüsselung

- Zugriffe auf Datenbank, APIs sowie Messaging Bus mittels SSL verschlüsselbar
- Verschlüsselung von Objekten auf Storage Systemen teilweise möglich

Aufteilung der Netzwerke

- Nutzung von GRE, V(x)LAN
- Unterteilung der Netzwerke
  - Public Network
  - External Network
  - Internal Network
  - API Network
  - Management Network
  - Migration Network
  - Storage Network

Security Frameworks

- Nutzung von Security Frameworks zur transparenten Absicherung möglich
  - SELinux oder AppArmor: Mandatory Access Control (MAC) für Ressourcen (Nutzung von Linux Security Module (LSM))
  - RSBAC: Rule Set Based Access Control, ähnlich SELinux
  - Cgroups: Limitierung und Isolierung von Ressourcen
- Nutzung von Rootwrappern zur Reduzierung notwendiger Berechtigungen von OpenStack-Komponenten

Maßnahmen

- Reaktion auf definierte Events durch Notifications über Messaging Bus
- zentrales Logging sowie Nutzung von Logging Management
- regelmäßiges Auditing durch Nutzung von Configuration und System Management sowie SCAP (z.B. OpenSCAP)
- Nutzung von Intrusion Detection Systemen
  - OSSEC
  - AIDE
  - Tripwire

Nutzung externer Komponenten

- Risiken durch Nutzung externer Komponenten
  - cPython
  - Libvirt
  - KVM, Xen, ...
  - Memcached, Redis, ...
  - RabbitMQ, ZeroMQ, Qpid, ...
  - MySQL, PostgreSQL, ...
  - Citrix XenServer, VMWare vSphere, Microsoft Hyper-V, ...
  - Python Packages und Libraries: SQLite, Django, Eventlet, ...
- Empfehlung: Nutzung von Enterprise Distributionen und Software Support

Vielen Dank für Ihre Aufmerksamkeit!

Sebastian Zielenski
zielenski@b1-systems.de

Bei Fragen wenden Sie sich bitte an info@b1-systems.de