CIRCLE

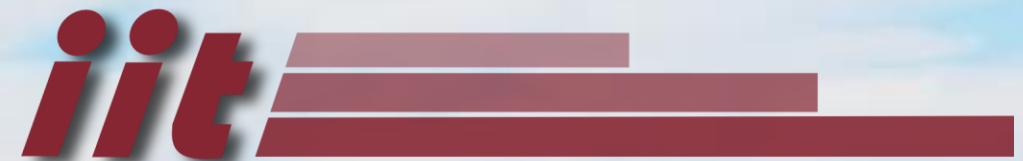## Cloud Infrastructure for Research Computing and Laboratory Environment

CIRCLE Cloud Services for Research and Education Communities

Eva Geist, Peter Dobe

MŰEGYETEM 1782

iit

What is "CIRCLE"?

- A business model - complete cloud solution for education and research communities

- Supporting the special requirements for education and research communities

- Includes open source IaaS or PaaS cloud manager

- No extra IT knowledge required from the users - trainers, students, researchers

https://circlecloud.org

CIRCLE
IaaS for everyone

Requirements for education and laboratory environments

- Education demands dynamic environment

- Different trainings have different software requirements

- Difficult to maintain complex software dependencies on heterogeneous physical machines

- Need for multi-host environments

- Infrastructure for small projects

- Easy to deploy, portable

Requirements for education and laboratory environments

- Easy to use, easy to understand
  - Not everyone has deep knowledge about IT who wants to use the cloud
- Separate main roles like teachers and students
  - Students' actions need to be supervised by the teachers
- Burst virtual machine deployments
  - At the start of the lecture everyone starts machine at the same time
- Effective resource usage
  - Users are not charged for their resource usage
  - Lease is the chosen solution in CIRCLE

CIRCLE
IaaS for everyone

Challenges

- Efficient and cost effective solution needed especially for short-term usage

- Available e-learning solutions and experience have to be maintained, extended with parallel working possibilities

- Educational community should be able to enforce its own strategy depending on its courses and other services, frequently changing environment

- Sharing possibility/co-working with different institutions and students

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Challenges

- Access to data centers, services from any given location within the university – easy accessibility

- Pay as you go/use as you need - Flexibility

- QoS/SLA is fundamental

- Easy reproducibility without special IT knowledge - Simplicity

- Portability

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Respond to the Challenges

- Cloud computing
  - Definition, standardization – NIST –self management, virtualization, pay per use, network access
  - Cloud computing is a cluster of distributed computers that offer on-demand resources and services over a networked medium commonly the internet
- IaaS vs SaaS vs PaaS
  - Most of the use cases require IaaS from service provider point of view, which does not rule out that an end user sees it as a PaaS or SaaS.
- Public vs Community vs Private vs Hybrid
  - Differentiation mainly important from cloud management, security, SLA and QoS point of view. It is usually categorized as community or private cloud.

MŰEGYETEM 1782
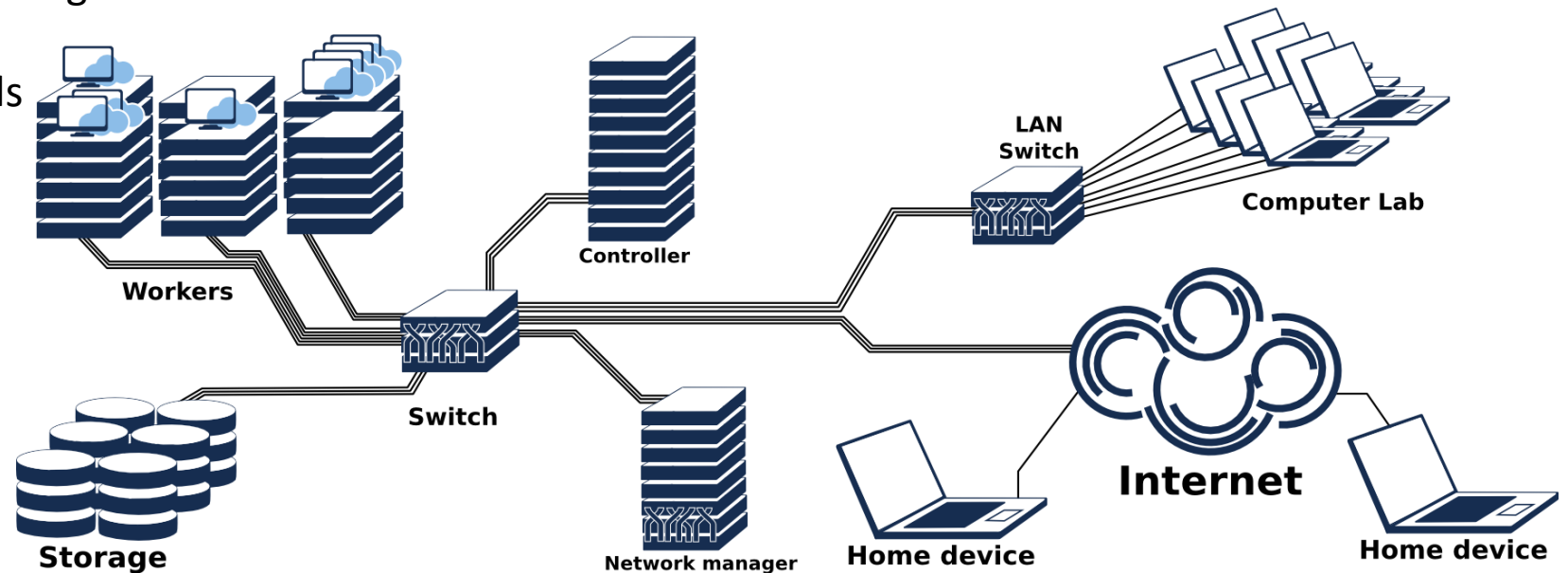
CIRCLE
IaaS for everyone

Cloud reference model
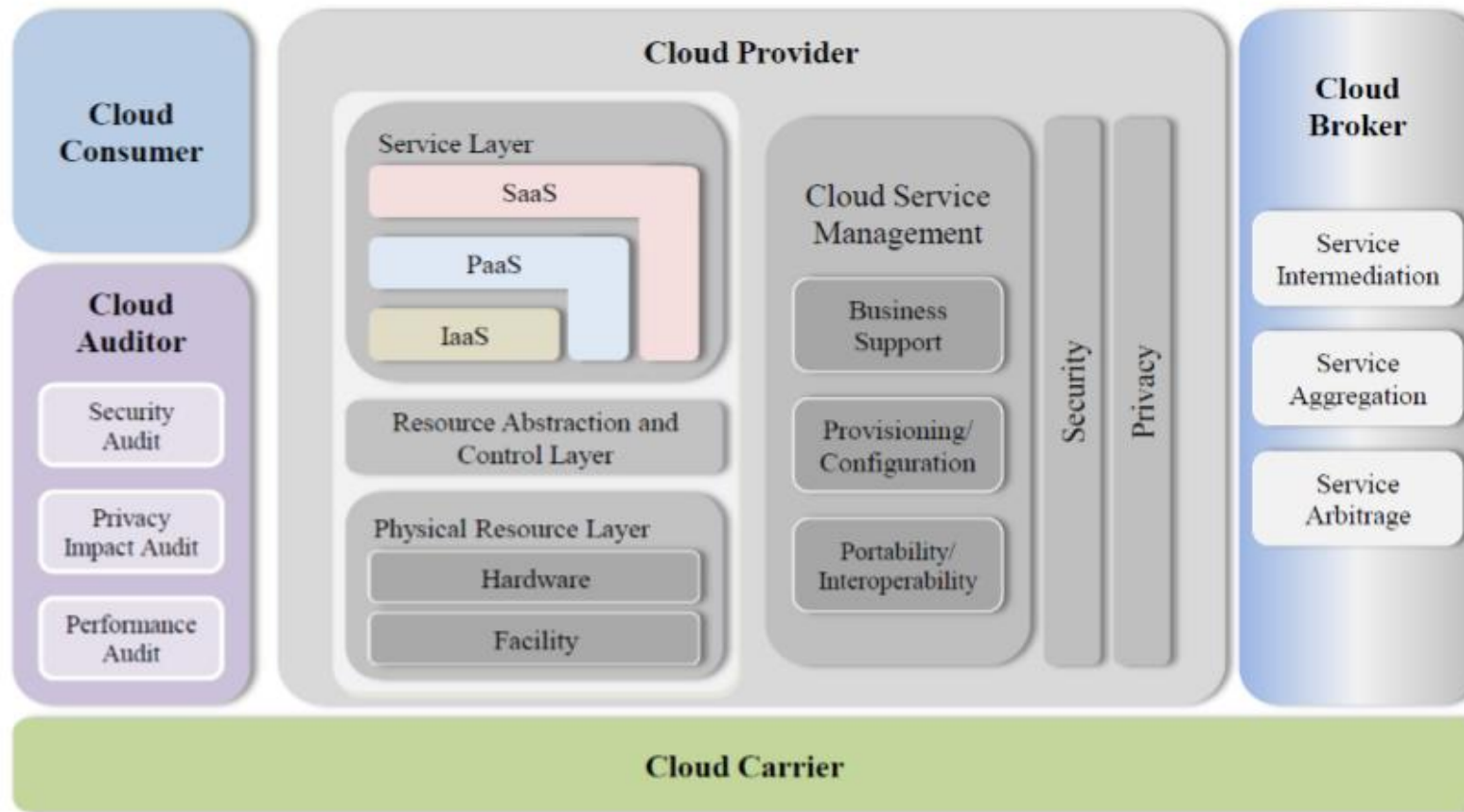
Solution – IaaS Cloud with self developed cloud manager

Benefits

Multiple virtual environments on a single physical machine

Dynamic load balancing (live migrations)

Management tasks delegated to users

More efficiente resource use

Difficulties

Image creation needs special knowledge

Security risk

Network zone administration needs
expertise and high permission

Workers

Controller

LAN Switch

Computer Lab

Switch

Storage

Network manager

Home device

Internet

Home device

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

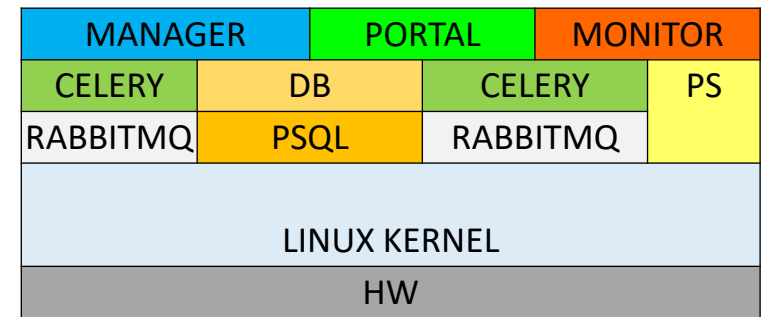# Solution – IaaS Cloud with self developed cloud manager

Modules:

- Portal - web interface
- Node - supervise virtual machine instances
- Storage - store the disk images
- Network - manage complex network infrastructures
- Cloud Manager
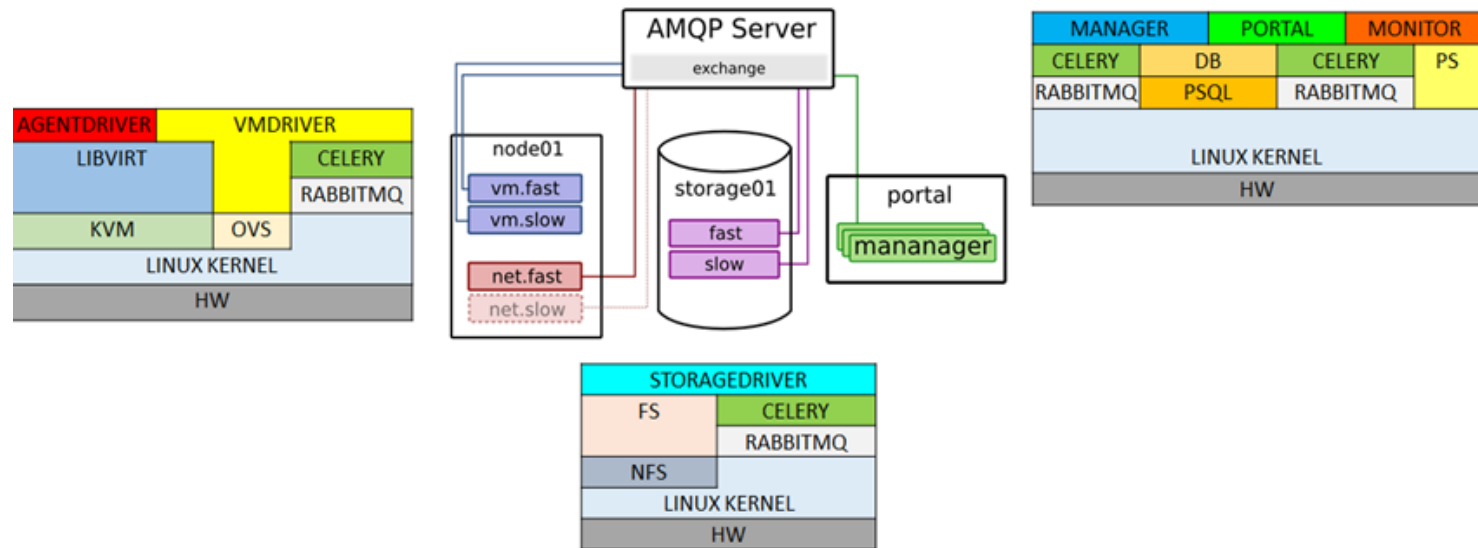
Portal – User interface

- User-friendly web interface

- Supports SAML2 authentication (SSO)

- Role-based ACL

- Personal file store

- Notification about expiration times

MANAGER	PORTAL	MONITOR
CELERY	DB	CELERY	PS
RABBITMQ	PSQL	RABBITMQ	
LINUX KERNEL		
HW		

CIRCLE
IaaS for everyone

MŰEGYETEM 1782

Portal – Dashboard

Portal – Virtual machine instances

Virtual machines

Group actions | Select all ▶ ⚙ ☾ ↻ ⚡ ⚞ 🚚 ✖

owner:75558@bme.hu | all ▼ | ☐ | 🔍

ID	Name	State	Owner	Lease	Memory	IP address	Node
549	tarokkk	▶ running	Sándor Guba (TFDAZ6)	szerver (1 év / 10 év)	2048 MiB	152.66.243.78	mega1
4493	StoreServer	▶ running	Sándor Guba (TFDAZ6)	szerver (1 év / 10 év)	4096 MiB	152.66.243.127	mega3
4536	Test	⚞ pending	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	2048 MiB	-	-
4968	Matlab Tarokkk	❚❚ suspended	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	4096 MiB	10.9.0.169	-
5012	Tarokkk Windows Office	❚❚ suspended	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	2048 MiB	10.9.0.128	-
5122	Superdev	❚❚ suspended	Sándor Guba (TFDAZ6)	szerver (1 év / 10 év)	1024 MiB	152.66.243.50	-
5151	CPorta teszt	❚❚ suspended	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	1024 MiB	10.9.0.160	-
5571	Circle devenv	❚❚ suspended	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	2048 MiB	10.9.1.148	-
5830	Sphinx	❚❚ suspended	Sándor Guba (TFDAZ6)	projekt (1 hónap / 6 hónap)	1024 MiB	10.9.0.167	-

MŰEGYETEM 1782

CIRCLE
IaaS for everyone
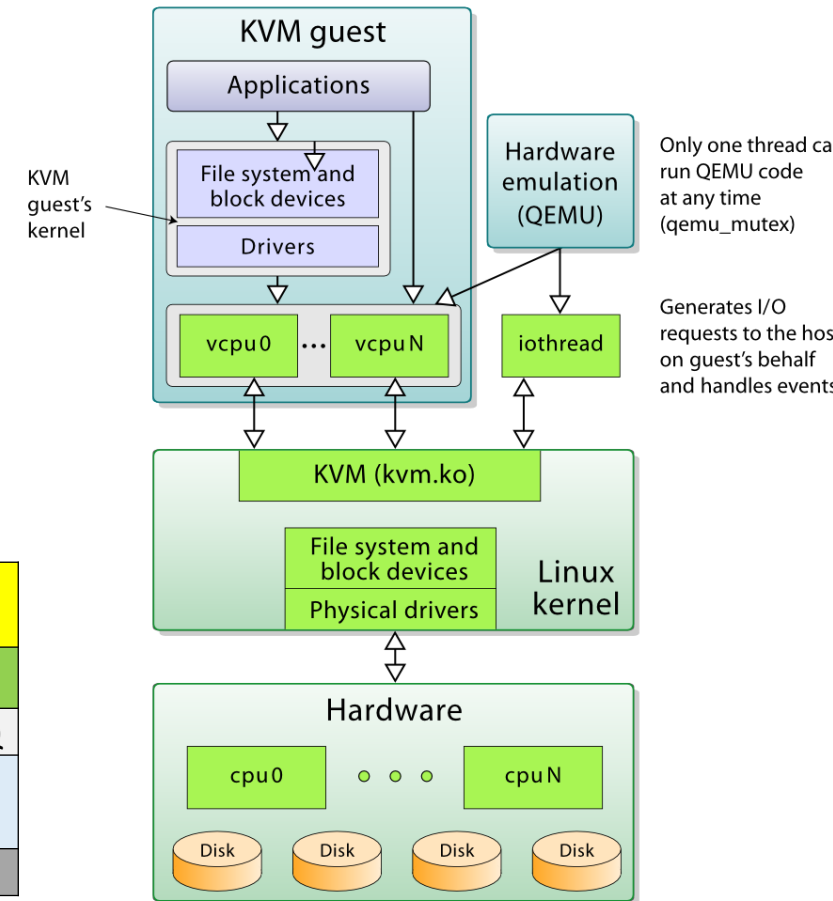
Portal – Resources of a selected VM

Portal – Network

Nodes

- Deploy and destroy virtual machines

- Use KVM and libvirt for virtualization

- Manage Open vSwitch and Flow rules

- Monitor virtual machines

- Provide agent service
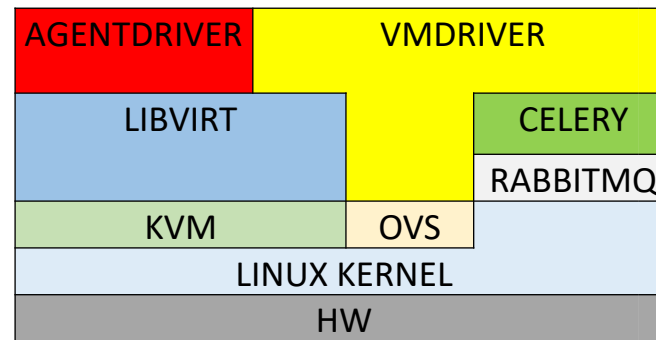
Agent

- CIRCLE comes with Agent support
  - Python agent
  - Communication through virtual serial port
- Agent service responsible for virtual instance customization (pw, ip, mount, etc.)
- Linux and Windows guest machines
- Customization
- Configuration:
  - Network
  - Password
  - SSH Keys
- Comfort
  - Alert for expiring lease times

Activity

⚙ (3x) Agent
  Restart networking – 2 days ago
  Change ip – 2 days ago
  Starting – 2 days ago

>_ Console access 8 days ago

⚙ Agent 12 days ago
  Stopping – 8 days ago
  Restart networking – 12 days ago
  Change ip – 12 days ago
  Starting – 12 days ago

Connection details

Protocol	SSH
Host	vm.ik.bme.hu:**7347**
Host (IPv6)	cloud-9258.vm.ik.bme.hu:**22**
Username	cloud
Password	•••••••••• Show password 👁

Generate new password!

MŰEGYETEM 1782

Deployment

- The deployment can be
  - Stand-alone - All components on a single node
  - Cluster - VM's run on a cluster, other services on a single head node
  - Distributed - VM's run on a cluster, all services on separate nodes
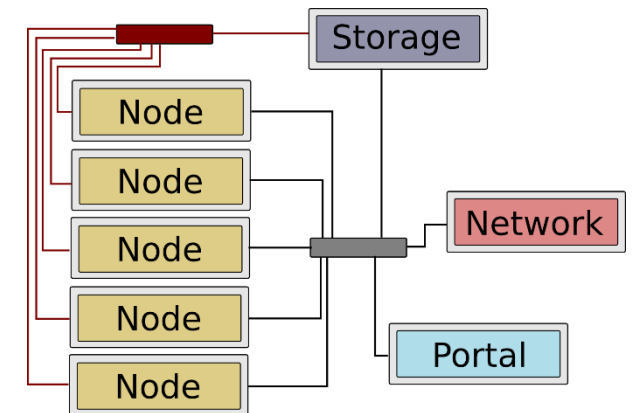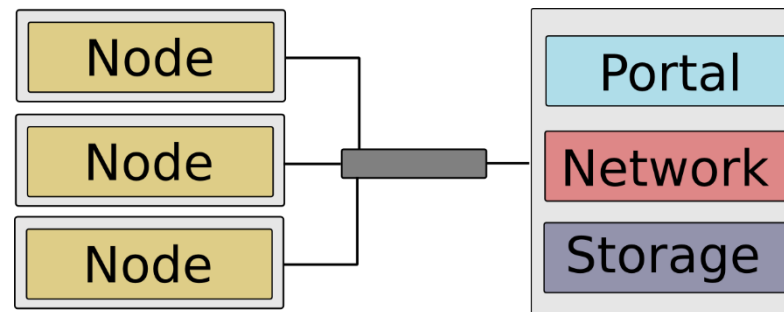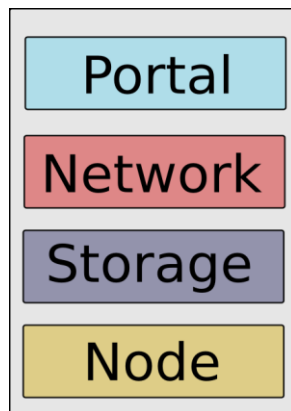
Storage

- Various disk image formats (iso, raw, qemu copy-on-write) are supported

- Any shared file system can be used, e.g. NFS

- Shared storage – to store the virtual machine images (qemu copy-on-write file format), live migration possible between the worker nodes

- More than 100 virtual machines deployed within minutes - the virtual machine images' Qcow2 format makes it possible to deploy virtual machines without copying the base disk image

STORAGEDRIVER		
FS	CELERY	
	RABBITMQ	
NFS		
LINUX KERNEL		
HW		

MŰEGYETEM 1782

CIRCLE
IaaS for everyone
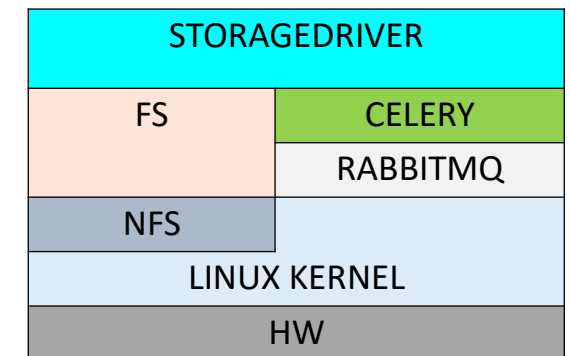
Storage

- Saving a virtual machine will create a new image from the base and the differential image. This image can be used as base image for future deployment

- Free space managed by the storage module, can be defined in percentages

- Destroying a virtual machine on the dashboard will only move the image file in a trash folder

- The images are not destroyed permanently as long as the specified space is available. The garbage collector checks occasionally and destroys the oldest images until there is enough free space again.

Networking

Complex physical and virtual network administration

- network management with OpenFlow rules

Manages:

- VLAN

- Zone management

- DNS service

- DHCP service

- IPv6 supported

Hosts list of all hosts

⊕ Create a new host

Filter by vlans | ALL | cporta | DMZ | grid | HOT | iitint | iitlab | iitman | INT | VPN | WAR | Search... | 🔍

Hostname	Vlan	MAC Address	IPv4 Address	IPv6 Address	WAN IPv4 Address	Created At	Owner
cloud-846	managed - VM-NET	02:00:0A:09:01:35	10.9.1.53	2001:738:2001:4031:9:1:53:0	152.66.243.62	08/02/2014 1:48 p.m.	48806@bme.hu
cloud-908	managed - LAB	02:00:00:38:C0:07	10.7.0.15	2001:738:2001:4031:7:0:15:0	—	04/27/2015 12:07 p.m.	48806@bme.hu
1022	managed - WAR	02:00:98:42:F3:53	152.66.243.83	2001:738:2001:4031:66:243:83:0	—	08/02/2014 1:48 p.m.	92428@bme.hu
1023	managed - VM-NET	02:00:0A:09:01:CA	10.9.1.202	2001:738:2001:4031:9:1:202:0	152.66.243.62	08/02/2014 1:48 p.m.	92428@bme.hu
1086	managed - VM-NET	02:00:0A:09:01:64	10.9.1.100	2001:738:2001:4031:9:1:100:0	152.66.243.62	08/02/2014 1:48 p.m.	92428@bme.hu
1400	managed - VM-NET	02:00:0A:09:02:1F	10.9.2.31	2001:738:2001:4031:9:2:31:0	152.66.243.62	08/02/2014 1:48 p.m.	65700@bme.hu
1470	managed - WAR	02:00:98:42:F3:40	152.66.243.64	2001:738:2001:4031:66:243:64:0	—	08/02/2014 1:48 p.m.	92428@bme.hu
1762	managed - VM-NET	02:00:0A:09:01:1B	10.9.1.27	2001:738:2001:4031:9:1:27:0	152.66.243.62	08/02/2014 1:48 p.m.	53646@bme.hu
1772	managed - VM-NET	02:00:0A:09:01:22	10.9.1.34	2001:738:2001:4031:9:1:34:0	152.66.243.62	08/02/2014 1:48 p.m.	92428@bme.hu
1807	managed - VM-NET	02:00:0A:09:01:3F	10.9.1.63	2001:738:2001:4031:9:1:63:0	152.66.243.62	08/02/2014 1:48 p.m.	5048@bme.hu
1824	managed - VM-	02:00:0A:09:01:4B	10.9.1.75	2001:738:2001:4031:9:1:75:0	152.66.243.62	08/02/2014 1:48	92428@bme.hu

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Networking

Manages:

- Ipfilter – Linux based netfilter, firewall
- Several ways to connect VM to Internet
- Public and private network using NAT → LAN,WAN
- Prevent malicious or accidental abuse
- Access control lists
- Blacklist – IDS interface, monitoring tool
- GUI – web based management interface
- Port forwarding

Cloud Management Speciality for Education and Research environment

Templates

- Possible to save any VM Instance as a Template
- Fine tune resource usage like CPU, Memory and Disk size
- Define networks suited for the exercise
- Share with ACL
- Customize your template like any other virtual machine

Templates

Name	Resources	Operating System	Access Method	Lease	Owner	Created At	Running	Actions
Circle devenv	2048MiB RAM 1 CPU core	Ubuntu 14.04 LTS Server amd64	SSH	labor (5 óra / 1 hét)	István Gergely Oláh (HN02A6)	3 months ago	3	
Tesztelés és minőség labor (ügynökkel)	2048MiB RAM 2 CPU cores	Windows 7 Enterprise x86_64	RDP	házi feladat (5 óra / 1 hónap)	Sándor Guba (TFDAZ6)	9 months ago	0	
Ubuntu 14.04 v1 régi	1024MiB RAM 1 CPU core	Ubuntu 14.04 LTS Server amd64	SSH	labor (5 óra / 1 hét)	Sándor Guba (TFDAZ6)	8 months ago	1	
Ubuntu 14.04 v5	1024MiB RAM 1 CPU core	Ubuntu 14.04 LTS Server amd64	SSH	labor (5 óra / 1 hét)	Dániel Bach (JI1M92)	a month ago	0	

Leases

Name	Suspend Interval	Delete Interval	Actions
házi feladat (5 óra / 1 hónap)	5 hours	1 month	
labor (5 óra / 1 hét)	5 hours	1 week, 2 days	
projekt (1 hónap / 6 hónap)	1 month	6 months	
szerver (1 év / 10 év)	1 year	10 years, 1 month	

Leases

- All virtual machines have two parameters for lease time
  - Suspension – Time until the VM is suspended
  - Destruction – Time until the VM is destroyed
- Defined lease types
  - Laboratory (S - 5 hours, D - 7 days)
  - Diploma/Home work (S - 1 m, D - 6 m)
  - Server (S - 1 year, D - 10 years)
- Renew
  - Every user can renew their own VMs

Do you want to perform the following operation on Sphinx (5830): **renew**?

Virtual machines are suspended and destroyed after they expire. This operation renews expiration times according to the lease type. If the machine is close to the expiration, its owner will be notified.

☐ Set expiration times even if they are shorter than the current value.

☐ Save selected lease.

Length

projekt (1 hónap / 6 hónap) (suspend: 1 month, remove: 6 months)   ▾

Cancel   ⏩ Request longer lease   📅 Renew

Expiration 📅 renew

Suspended at:
🌙 in 6 days
Destroyed at:
✖ in 5 months

CIRCLE
IaaS for everyone

Cloud Management Speciality for Education and Research environment

Authentication

- Password based authentication

- SAML2 SSO authentication for eduID

- Optional two-factor authentication for either method

- Pre-defined groups (ACL)

  - Based on the courses

  - Add members even before logged in

ACL

- Three types of users
  - Student/end user
  - Teacher/lab manager/etc.
  - Operators
- Resource sharing via 3 roles
  - User: Access the resource
  - Operator: Share with users and do modifications
  - Owner: Supervise the resource
- Every resource has its owner – Can't be demoted
  - You can transfer this ownership

Cloud Management Speciality for Education and Research environment

Requests

- Resources are limited
- Further resources are usable only after permission is granted
- Requests provide interface for the students to ask for more
  - Processor
  - Memory
  - Disk space
  - Lease time
- Administrator can Accept / Decline with one click

Activity

- Track the history of your virtual machines

- Activities are created on every action
  - User action
  - Monitoring event
  - Administrator action

- Time, user, and action type are logged

Activity

- **Shutdown** 21 days ago
- **Migrate** a month ago
  - Deploy network – a month ago
  - Shutdown network – a month ago
  - Migrate to mega2 – a month ago
- **(2x) Migrate**
  - Deploy network – a month ago
  - Shutdown network – a month ago
  - Migrate to mega5 – a month ago
  - Schedule – a month ago
- **(3x) Console access**
- **Console access** 2 months ago
- **Migrate** 3 months ago
  - Deploy network – 3 months ago
  - Shutdown network – 3 months ago
  - Migrate to mega4 – 3 months ago
  - Schedule – 3 months ago
- **Deploy** 3 months ago
  - Wait operating system loading – 3 months ago `failed`
  - Boot virtual machine – 3 months ago

Third-party components – SaltStack installer

- CIRCLE based on several software components
  - Python
  - Libvirt (KVM based virtualization)
  - Django (portal)
  - Open vSwitch
  - Celery with AMQP for module communication
- SaltStack is an easy-to-use configuration manager
- Installer is available from the git repository

Comparison to other Open-source frameworks

Capability/features	OpenStack	CloudStack	Eucalyptus	OpenNebula	Nimbus	CIRCLE
Established	2010	2010	2008	2008	2009	2011
Origin	Rackspace, NASA, Dell, Citrix, Cisco, Canonical etc.	Cloud.com	Santa Barbara University, Eucalyptus System Company	European Union	University of Chicago	Budapest University of Technology and Economics
Philosophy	Offers Cloud Computing services		Mimic Amazon EC2	Private, highly customizable cloud	Cloud tailored to scientific researchers	Cloud services for education and research
Suitability	Enterprises, service providers and researchers	Enterprises, service providers and researchers	Large commercial enterprises, Research institutions	Large commercial companies and public institutions	Research institutions	Schools, research institutions, SMEs
Architecture	Integration of OpenStack object and OpenStack compute	Hierarchical with four main components	Hierarchical Minimum two servers	Centralized, Minimum two servers	Centralized Minimum two servers	Scalable from a standalone node to a cluster of 10+ nodes

Theo Lynn et al., A Comparative Study…, CLOSER 2015

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Comparison to other Open-source frameworks

Capability/features	OpenStack	CloudStack	Eucalyptus	OpenNebula	Nimbus	CIRCLE
API Support	Native API, Amazon EC2 API, CloudFiles REST API.	Amazon EC2 API, S3	Amazon EC2 API,	Native API in Ruby and JAVA. XML-RPC API for interfaces creation. OGF OCCI & Amazon EC2 APIs.	EC2 APIs, S3 APIs, JAVA client APIs.	Native API in Python, OGF OCCI
Amazon Support	EC2, S3	EC2, S3	EC2, S3, EBS, IAM, AMI	EC2, EBS, AMI	EC2, S3	none
Deployment model	Public	Public	Private	Private	Private	Private
	Hybrid	Hybrid	Hybrid	Hybrid	Community	Community
	Private	Private				
Hypervisor	KVM, Xen, VMware ESX, ESXi, Hyper-v, LXC, QEMU, UML, PowerVM, Bare metal	VMware, Oracle VM, KVM, XEN	KVM, Xen, VMware	KVM, Xen, VMware ESX, ESXi	Libvirt+KVM, Libvirt+Xen	Libvirt+KVM, Libvirt+ESXi
Programming Language	Python	Java	Java, C, Python	Java, Ruby and C++	Java, Python	Python

Theo Lynn et al., A Comparative Study..., CLOSER 2015

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Comparison to other Open-source frameworks

Capability/features	OpenStack	CloudStack	Eucalyptus	OpenNebula	Nimbus	CIRCLE
Community	+++++	++++	+++	+++	++	+
Release Frequency	<4 months	4 months	>4 months	>6 months	<4 months	>6 months
Ease of use	+++++	+++++	++	+++	+++	++++++
Supported OS	Linux, Windows, Requires x86 Server	Mac OS X, Linux distributions, FreeBSD, Novell Netware, Sun Solaris, Windows	Linux (Ubuntu, Fedora, CentOS, OpenSUSE, Debian)	CentOS, Debian, Fedora, RHEL OpenSUSE, SLES, and Ubuntu	Most Linux distributions	RHEL, CentOS, Scientific Linux, Ubuntu, Debian
Storage	Object and block storage supported. Volumes are persistent. File storage is supported through Swift	Supports for iSCSI, NFS, SMB/CIFS; support for OpenStack Swift and Amazon S3	Support for iSCSI, EBS, Amazon S3. Hardware support for industry-standard Storage Hardware.	Hardware support for Fibre Channel, iSCSI, NAS shared storage, SCSI / SAS / SATA. Non-shared and shared file systems (NFS, LVM with CoW, VMFS, etc.).		Centralized storage with NFS or distributed storage with Ceph. Disk images stored in qcow2 format.

Theo Lynn et al., A Comparative Study..., CLOSER 2015

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

Comparison to other Open-source frameworks

| Capability/features	OpenStack	CloudStack	Eucalyptus	OpenNebula	Nimbus	CIRCLE
Networking	VLAN, Public IP's, Private IP's, SDN, IDS, Load-balance, Firewalls VPN;	VLAN, Public IP	VLAN, Public IP's, Private IP's	VLAN, Public IP's, Private IP's, OVSwitch; Manual configuration	DHCP server installed on nodes	IPv4/IPv6, VLAN, Public IP's, Private IP's; user configurable NAT, VPN, IDS, OVSwitch
User Interface	Web interface (i.e. Dashboard) and Command line interface to deploy VMs and a console to manage the VMs.	Web interface and Command Line Interface (CLI)	euca2ools (CLI)	Web interface and Command Line interface (CLI)	Web-Services, specifically: Nimbus Web	Web interface and command line interface
Load Balancing	The Cloud Controller	TCP Load Balancer	The Cloud Controller	Nginx	Le Context Broker	Nginx, Celery
Licensing	ApacheLicence Version2	ApacheLicence Version2	BSD-Licence	ApacheLicence Version2	ApacheLicence Version2	GNU GPLv3
Document Support	+++++	+++++	+++	+++	++	++

Theo Lynn et al., A Comparative Study..., CLOSER 2015

CIRCLE
IaaS for everyone

MŰEGYETEM 1782

Comparison to other Open-source frameworks

Capability/features	OpenStack	CloudStack	Eucalyptus	OpenNebula	Nimbus	CIRCLE
Security	Protection against DoS. Keystone used for identity management.	CloudStack Security Groups	The Cloud Controller generates a public/private key code pairing for user authentication	Passwords, secure shell and RSA key code pairings, LDAP, Various administration roles. Multi-tenancy for public clouds.	Public Key Infrastructure	Password authentication or SAML2 SSO and optional Two-Factor Auth. Extended role and ACL based permission model.
Error Robustness	Replication	Replication	Separate clusters reduce likelihood of correlated errors; Cluster controller's separation	Permanent database to store information about hosts, networks and virtual machines; Database backend (registers virtual machine information)	Regular check and backup of worker nodes; Periodic verification of cloud nodes	Self-managed Salt based configuration management (maintenance and installation), VM templates for easy rollback

Theo Lynn et al., A Comparative Study..., CLOSER 2015

MŰEGYETEM 1782

CIRCLE
IaaS for everyone

What is "CIRCLE"?

- Open source (GPLv3) IaaS cloud manager
- Complete system ready to deploy
- Easy-to-use web interface even for non-IT users
- User-friendly interface for template customization
- Scalable
- Advanced networking
- All modules written in Python
- Easy to install with SaltStack
- → it is an operation model for education and research environment
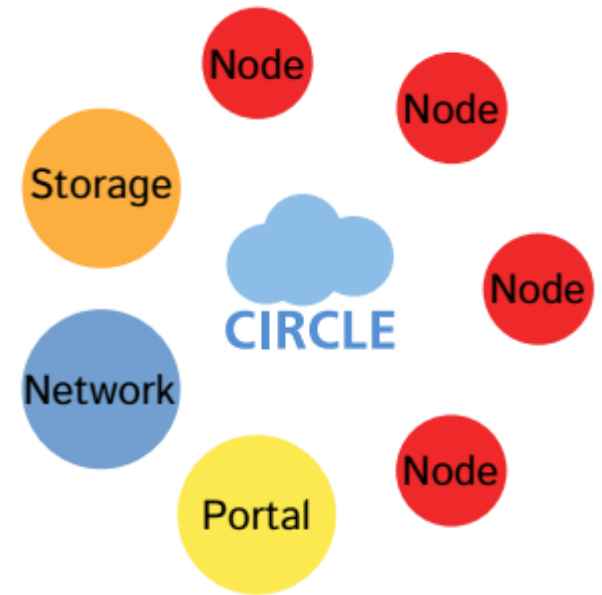
DEMO

- Teacher point of view

- Student point of view

CIRCLE
IaaS for everyone

Cloud **I**nfrastructure for **R**esearch **C**omputing and **L**aboratory **E**nvironment

Thank you for your attention!

https://circlecloud.org