Lecture 10

CloudStack

CS CloudStack

- GUI IP: 192.168.252.200:8080/client
- username: admin
- password: password

CloudStack Cloud

CloudStack has a monolithic architecture

- which may have some advantages over OpenStack’s distributed architecture, in terms of installation and maintenance
- although the jury is still out on these issues

CloudStack Cloud

- CloudStack was originally started in 2008 by a company named first VMOps and then Cloud.com
- Citrix bought Cloud.com in 2011
- In 2012, Citix released CloudStack to the Apache Incubator under the Apache software license.
- In 2013, CloudStack was released from the Apache Incubator

CloudStack Cloud

The Apache CloudStack Management server runs in an Apache Tomcat container. It is responsible for:

- allocating virtual machines to host computers
- assigning IP addresses
- allocating and managing storage
- It also provides all APIs

CloudStack Cloud

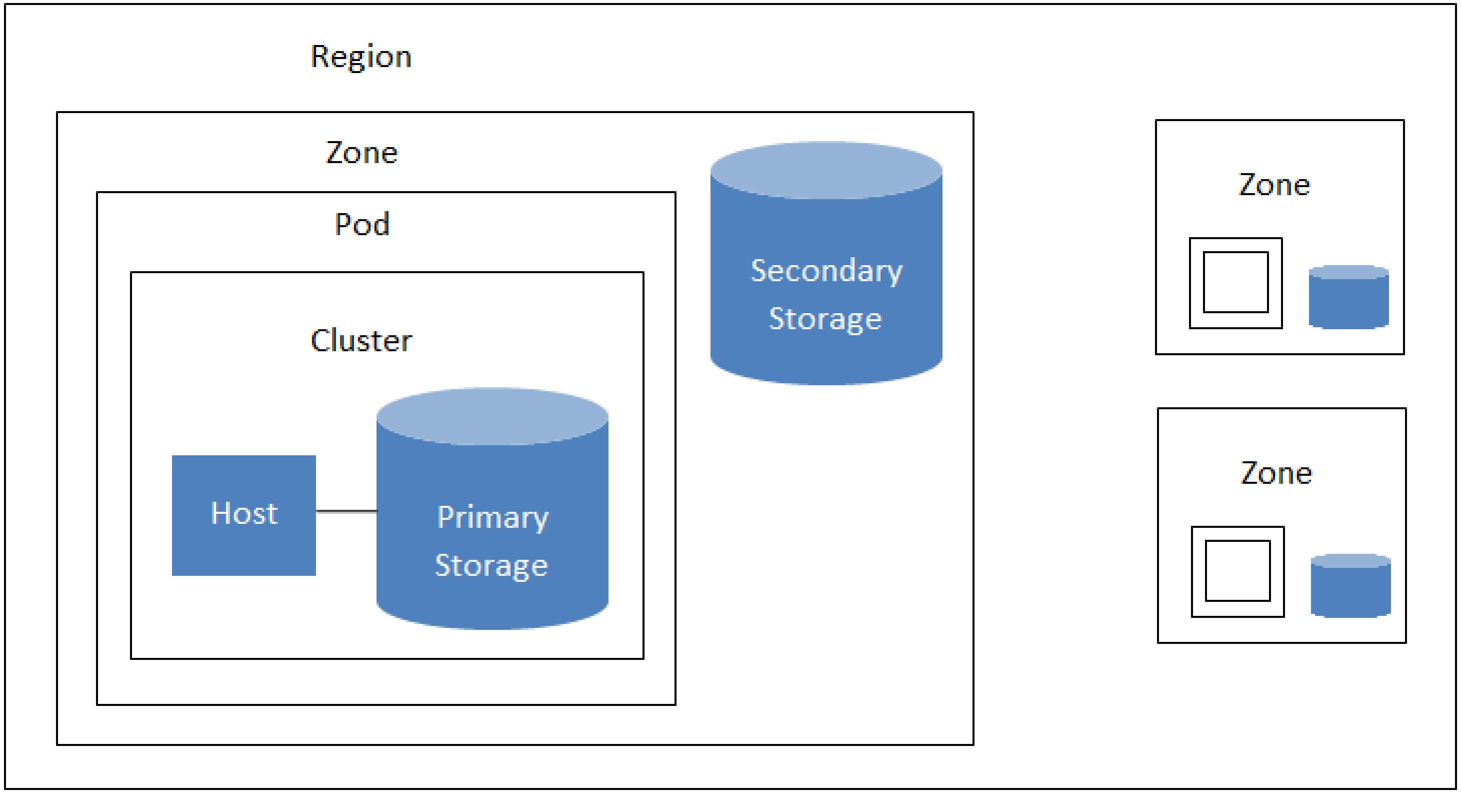
In CloudStack deployment, the following terms are used:

- Region
  - a collection of one or more zones (geographically near each other) that is managed by at least one management server
  - the largest organizational unit in a CloudStack cloud
- Zone
  - represents one data center
  - consists of one or more pods plus secondary storage.
  - secondary storage is zone wide, contains disk templates, ISO images, snapshots
    - secondary storage is always accessed using NFS
  - note that primary storage is normally cluster wide
    - however, if using either the KVM hypervisor or the VMware vSphere hypervisor, primary storage can be done per zone

CloudStack Cloud

- Pod
  - rack (or row of racks) + layer2 switch and one or more clusters
- Cluster
  - one or more hosts plus primary storage
    - if use only local disk for an installation, can skip separate primary storage.
  - primary storage are basically virtual hard drives, used to actually run instances
  - at least one primary storage server is required per cluster
    - Network File System (NFS)
      - NFS allows a computer user to treat a file system and its files that are located on a remote computer as if they were on the user's own computer. It is based on Open Network Computing (ONC) Remote Procedure Calls (RPC)
    - Internet Small Computer System Interface (iSCSi)
      - iSCSI emulates SCSI commands over an IP network. SCSI is a standard for connecting computers to peripherals.
- Host
- a single compute node, often a hypervisor

CloudStack Cloud



A region with multiple zones

CloudStack Cloud

- With CloudStack, an account represents a customer
  - It is possible for an account to have multiple users although normally an installation would associate one user with one account
  - Users in the same account are not isolated from each other; however, users in one account are isolated from users in a different account

- Resources belong to the account, not to an individual user within the account
- Domains contain multiple logically related accounts

CloudStack Cloud

There are three types of accounts:

- Root administrator
  - has complete access to the system
- Domain administrator
  - can access the current domain, but cannot see into physical servers or other domains
- User
  - username is unique across accounts in a domain

- Note that a user *within* an account is not a root administrator or a domain administrator
  - Rather, the account *itself* is a root administrator or a domain administrator

CloudStack Cloud

- The root administrator can dedicate resources to a domain or to an account
- For example, a zone, cluster, pod, or host can be dedicated to an account

CloudStack Cloud

- A project in CloudStack is associated with both people and resources
- A project is located within a single domain, that is, a project cannot be associated with more than one domain
- An administrator can set global limits to control the quantity of resources that each project can own
- A project administrator can add people to a project, or, alternately, an invitation can be sent to a person that the person could then accept (or decline)

CloudStack Cloud

- The different methods for authentication in CloudStack:
  - CloudStack login API
  - access key and secret key method (EC2 interface)
  - external LDAP server
  - SAML 2.0 identity provider plugin

CloudStack Cloud

- When authentication is done through the CloudStack login API, the user receives a JSESSIONID cookie
  - which the user includes with all messages (until the session times out)

CloudStack Cloud

- a JSESSIONID cookie is generated by a Servlet container such as Tomcat (remember that the CloudStack Management server runs in an Apache Tomcat container)
- Since HTTP is stateless, there is no way within HTTP itself to connect multiple request/response pairs into an ongoing session
  - However, this can be done by the use of cookies
- Any HTTP request or HTTP response that includes the JSESSIONID cookie is considered to be part of the session

CloudStack Cloud

Weber (2014) on the cloudstack-users mailing list archives gives the following example of how to use the CloudStack login API with cURL:

Begin quoted material: “

Remember that parameters has [sic] to be encoded if they contain any kind of special characters.

```
curl -i '
http://localhost:8080/client/api?command=login&user=admin&password=MyPassword&response=json
```

returns a snippet like this:

```
Set-Cookie: JSESSIONID=07CA185081E6A476775ECA9D190EF1F8; Path=/client

 { "loginresponse" : { "timeout" : "1800", "lastname" : "cloud",
 "registered" : "false", "username" : "admin", "firstname" : "admin",
 "domainid" : "6f920fbd-94fc-11e3-b2e0-0050568c15a3", "type" : "1", "userid"
 : "d68e7072-94fc-11e3-b2e0-0050568c15a3", "sessionkey" :
 "WxjAu9zZzbmrBGDarnW1cVfm+/g=", "account" : "admin" } }
```

CloudStack Cloud

Then you take the JSESSIONID and sessionkey and pass them as Ove said.

List Zones example using above

```
curl -i -H "Cookie: JSESSIONID=07CA185081E6A476775ECA9D190EF1F8;
Path=/client" '

http://localhost:8008/client/api?command=listZones&sessionkey=WxjAu9zZzb
mrBGDarnW1cVfm%2B%2Fg%3D&response=json
‘
```

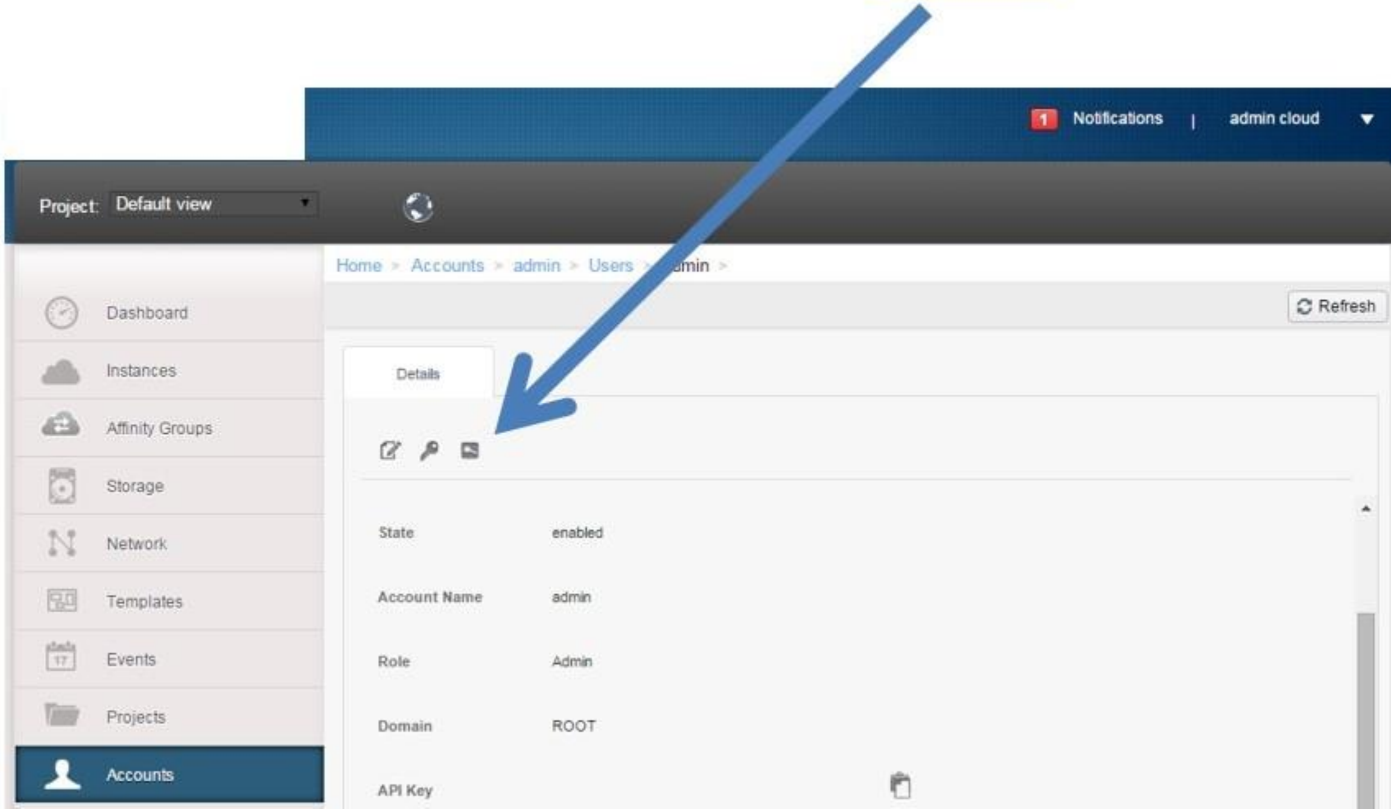
“: End quoted material

(NOTE: Ove was the author of a previous response on the mailing list.)

CloudStack Cloud—CloudStack EC2 API

Download Access Key and Secret Key from CloudStack GUI

Click on Generate Keys Icon



State	enabled
Account Name	admin
Role	Admin
Domain	ROOT
API Key	

CloudStack Cloud—CloudStack EC2 API (cont’d)

The format used by CloudStack commands using access key and secret key is in the following format:

- http://localhost:8080/client/api?apikey=… &command=… &response=json&signature=…

So the different subparts of this format is:

- baseurl:8080/client/api?
- &apikey-…the api key that was previously downloaded…
- &command=...a command that corresponds to a method on the CloudStack API…
- &response=json
- &signature=…

CloudStack Cloud—CloudStack EC2 API (cont’d)

The signature that is attached to the command is generated using the earlier parts of the command as input:

- apikey=… &command=… &response=json
  - This is made lowercase
  - Then do an HMAC-SHA1 hash on the lowercased earlier parts of the command, using the secret key to do the hash
  - Then do a base64 encode of the hashed value
  - Then append this to the rest of the command as:
    - &signature=…the base64 encoded, HMAC-SHA1 hash of the earlier parts of the command…

CloudStack Cloud—CloudStack EC2 API (cont’d)

CloudStack commands for version 4.9 can be seen at the following url:

https://cloudstack.apache.org/api/apidocs-4.9/

CloudStack Cloud

The Lightweight Directory Access Protocol (LDAP) is a protocol that runs on an IP network and provides directory look up services

- there are variations that run on TCP/IP and others that run on UDP over IP

With CloudStack, you use an external LDAP server to implement username/password lookup

According to CloudStack (2016):

> “To set up LDAP authentication in CloudStack, call the CloudStack API command addLdapConfiguration and provide Hostname or IP address and listening port of the LDAP server.”

CloudStack Cloud

- CloudStack allows use of Security Assertion Markup Language (SAML) 2.0 for authentication, through use of a SAML 2.0 identity provider plugin
- SAML 2.0 is an example of trusted third party authentication
- The general concept should be familiar to you from Public Key Infrastructure
  - SAML is an (OASIS) standard
- Single Sign On in SAML uses third party authentication and basically works as follows, see IBM (2016):

  “The SAML web SSO flow includes three actors: the end user, the identity provider (IdP), and the service provider (SP). The user always authenticates to the IdP, and the SP relies on IdP assertion to identify the user.”

CloudStack Cloud

- In CloudStack, the identity provider is the SAML plugin and the service provider is CloudStack itself

- The SAML 2.0 plugin is implemented using OpenSAML (an opensource Java library), see Yadav (2014)

CloudStack Cloud—Networking

- In CloudStack, each new Virtual Machine (VM) receives its very own public IP address
- Static Network Address Translation (NAT) maps the private IP address assigned to the VM to that VM’s public IP address (at a router)
- If instead a VM is using Elastic IPs, then whenever an elastic IP is acquired, the VMs public IP address is returned to the public IP address pool

CloudStack Cloud

- A zone can have either basic networking or advanced networking
- A zone must use one or the others, that is, a particular zone is either basic or advanced for its entire lifetime.
- However, within a cloud, different zones can use different networking models
  - that is, one zone may use advanced networking and another basic networking

CloudStack Cloud—Networking

- Basic networking in a zone (a basic zone) has the following characteristics:
  - Supports only one physical network
  - In a basic zone, you do not have VLANs, but you can split traffic across multiple
  - physical NICs
    - CloudStack uses a separate NIC (called storage NIC) for storage network traffic
    - Recommend separate NICs for management traffic and guest traffic
  - Each VM is assigned an IP directly from the network
  - Each pod is a broadcast domain
  - Each pod has a unique CIDR
    - CloudStack will assign IP addresses in the CIDR associated with a pod to guests in that pod
  - Has Domain Name System (DNS) 1 and Domain Name System (DNS) 2 for use by guest

CloudStack Cloud—Networking

Basic Networking (cont'd):

- Has Domain Name System (DNS) 1 and Domain Name System (DNS) 2 for use by guest
- VMs. These are accessed by public IP addresses.
- Has internal Domain Name System (DNS) 1 and Domain Name System (DNS) 2, accessed by
- the management traffic network. Used by system VMs (virtual routers, console proxies, secondary storage VMs, etc.). Private IP addresses for the pods must have a route to these internal DNS servers.
- Optional guest isolation via layer 3 means allows use of security groups. For example,
  - filtering of IP addresses
  - Possible traffic types are: management, public, guest, and storage

CloudStack Cloud—Networking

Advanced networking in a zone (advanced zone) has the following characteristics:

- Supports multiple networks
- Supports both physical and virtual networks
- Allows the use of tagged VLANs
- Networks defined by VLAN identifier, IP range, and gateway
  - Good practice involves setting different CIDRs for different zones
  - Guest network can be isolated or shared
  - In isolated network, VLANs ranges assigned to each CloudStack account
  - Administrator can create additional networks for use by guests
    - Can be associated with a single account, or
    - Can be available to all accounts

CloudStack Cloud—Networking

Advanced Networking (cont’d)

- Has Domain Name System (DNS) 1 and Domain Name System (DNS) 2 for use by guest VMs
    - These are accessed by public IP addresses
- Has internal Domain Name System (DNS) 1 and Domain Name System (DNS) 2, accessed by the management traffic network.
    - Used by system VMs (virtual routers, console proxies, secondary storage VMs, etc.)
        - Private IP addresses for the pods must have a route to these internal DNS servers

CloudStack Cloud—Networking

Networking Feature	Basic Network	Advanced Network
Number of networks	Single network	Multiple networks
Firewall type	Physical	Physical and Virtual
Load balancer	Physical	Physical and Virtual
Isolation type	Layer 3	Layer 2 and Layer 3
VPN support	No	Yes
Port forwarding	Physical	Physical and Virtual
1:1 NAT	Physical	Physical and Virtual
Source NAT	No	Physical and Virtual
Userdata	Yes	Yes
Network usage monitoring	sFlow / netFlow at physical router	Hypervisor and Virtual Router
DNS and DHCP	Yes	Yes

CloudStack Cloud—Networking

- In each zone, the management network has a range of reserved IP addresses
  - These reserved IP addresses must be unique across the entire cloud
- Hosts in a pod are assigned private IP addresses

CloudStack Cloud—Networking

- It is possible to configure secondary storage traffic to travel over a separate storage network
  - by default, CloudStack storage traffic travels over the management network
- Management network handles traffic between Management servers and Hosts, System VMs, and (optionally) storage
- Guest traffic can go only between VMs inside one zone.
  - For virtual machines in different zones to communicate with each other, they must communicate with each other using a public IP address

CloudStack Cloud

- CloudStack uses System Virtual Machines to perform certain tasks in the cloud
- A system virtual machine is a special kind of virtual machine with system privileges
- All System VMs come from a single template

CloudStack Cloud—Networking

- A “Virtual Router” is a type of System Virtual Machine
- A virtual router runs in a virtual machine on the hosts
- Typically the Management Service automatically creates a virtual router for each network
  - Networking features are provided for guest traffic by using a virtual router
  - . The virtual router serves as a DHCP server for the local network, and assigns IP addresses to the guest VMs

- There is an Open vSwitch plugin for CloudStack

CloudStack Cloud—Object Storage

In CloudStack, Object Storage is provided as plugins, this includes:

- Swift from OpenStack
  - With Swift, still must have NFS based secondary storage enabled per zone, it serves as as staging area in that artifacts from swift are copied to NFS shares and from there to primary storage
- Amazon S3
  - Has to be available within an entire region, is not per zone
  - Data cannot be copied between different regions