

CLOUD: ZERO TO SIXTY

DEPLOY A CLOUD IN 40 MINS

Will Stevens  @swillops

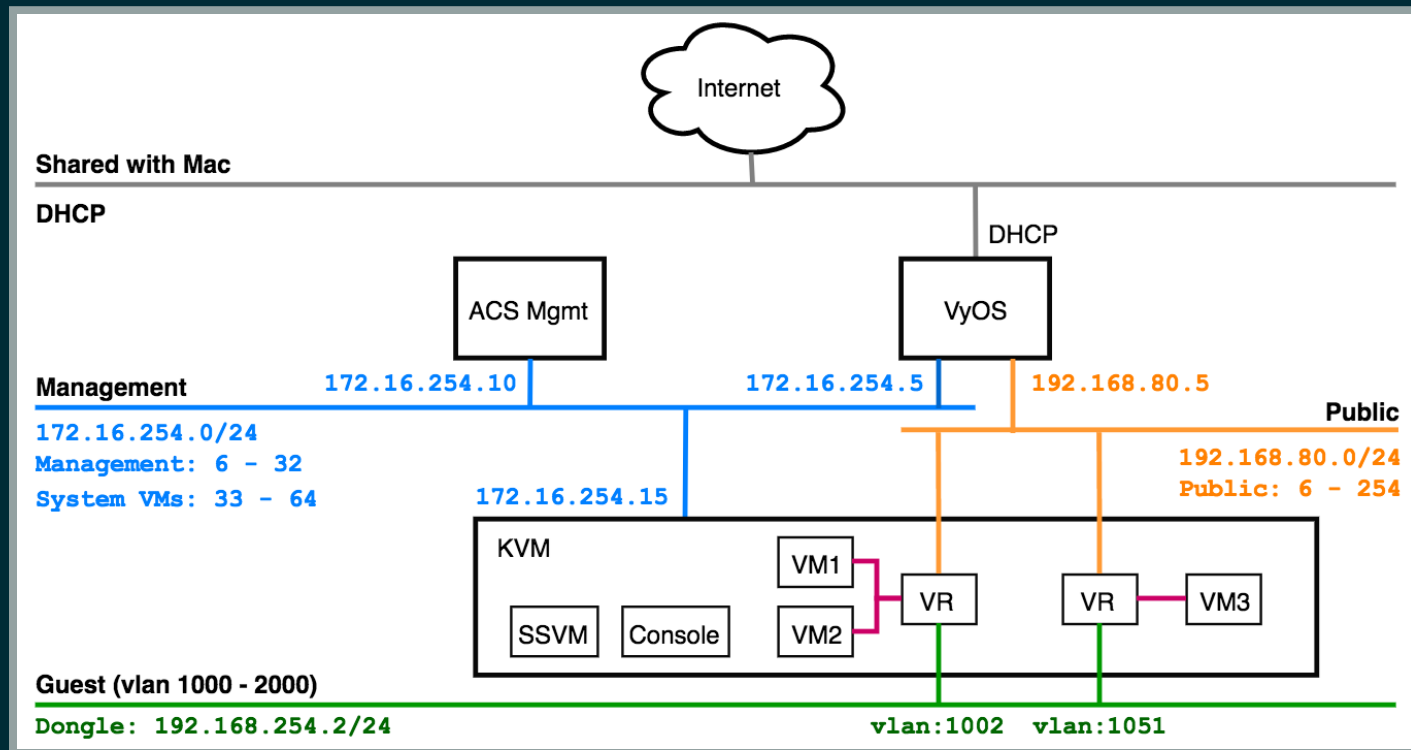
VP @ Apache CloudStack

Lead Developer @ CloudOps

github.com/swill/apachecon2016

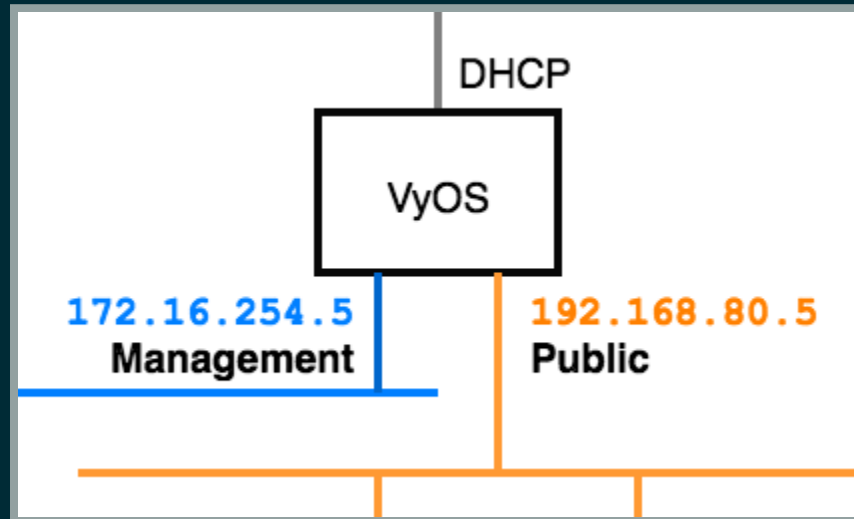
ON THE MENU

We will be configuring an Apache CloudStack (ACS) cloud on my laptop using VMware Fusion.



UPSTREAM NETWORKING

The ACS environment will be connected to my Mac's network through a VyOS router.



```
./vyos/01_configure.sh
```

VYOS DUTIES

- The network uplink for the entire environment.
- Gateway for both Management and Public networks.
- Edge firewall. In this case just a pass through.
- Firewall to protect the Management network.

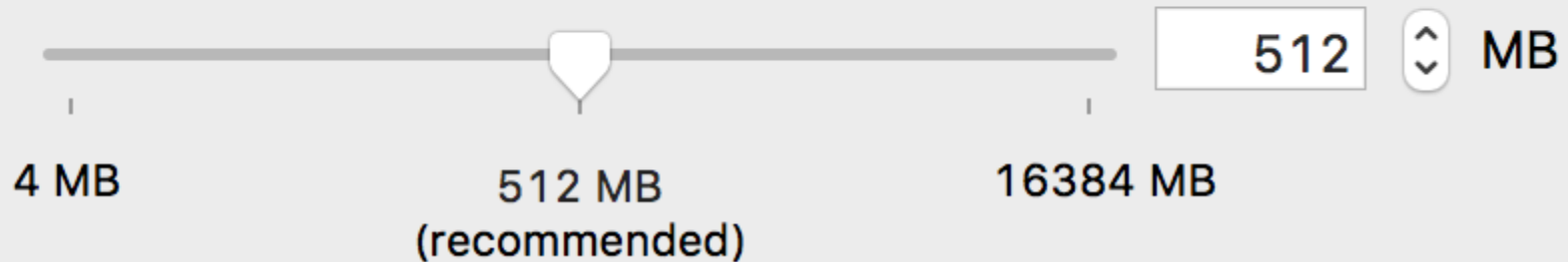
VYOS VM RESOURCES

Small VM since we don't expect much load.

Processors

1 processor core

Memory



INTERNET NIC (ETH0)

Internet Sharing

☒ Share with my Mac ☒

Bridged Networking

☒ Autodetect ☐

☒ Wi-Fi ☐

☐ Thunderbolt Ethernet ☐

☐ swilldroid ☐

☐ Thunderbolt Ethernet 2 ☐

☐ iPhone USB ☐

☐ Bluetooth PAN ☐

Custom

☒ Private to my Mac ☐

The virtual machine shares the IP address of the Mac on the external network. The Mac provides Network Address Translation (NAT) for network traffic from the virtual machine.

ACS PUBLIC NIC (ETH1)

Bridged Networking

- ☒ Autodetect
- ☐ Thunderbolt Ethernet
- ☐ Wi-Fi
- ☐ swiildroid
- ☐ Thunderbolt Ethernet 2
- ☐ iPhone USB
- ☐ Bluetooth PAN

Custom

- ☐ Private to my Mac
- ☐ vmnet2
- ☒ vmnet3

The virtual machine uses a custom network connection.

Name: **vmnet3**

Type: **Custom**

Subnet IP: **192.168.80.0**

Subnet Mask: **255.255.255.0**

ACS MANAGEMENT NIC (ETH2)

Bridged Networking

- ☐ Autodetect
- ☐ Wi-Fi
- ☐ Thunderbolt Ethernet
- ☐ swilldroid
- ☐ Thunderbolt Ethernet 2
- ☐ iPhone USB
- ☐ Bluetooth PAN

Custom

- ☐ Private to my Mac
- ☒ vmnet2
- ☐ vmnet3

The virtual machine uses a custom network connection.

Name: **vmnet2**

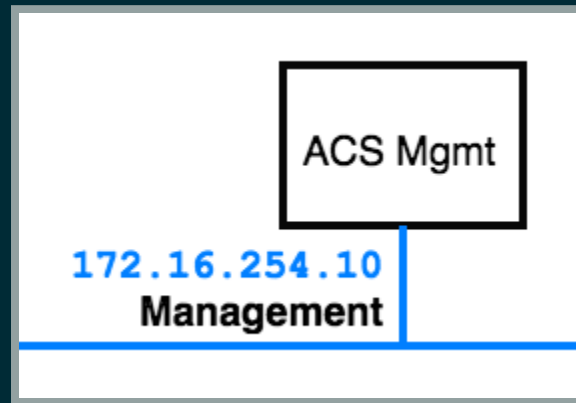
Type: **Custom**

Subnet IP: **172.16.254.0**

Subnet Mask: **255.255.255.0**

ACS MANAGEMENT VM

ACS Management node, MySQL and NFS mounts.



```
./acs/01_network_config.sh  
./acs/02_install_acs.sh
```

ACS MANAGEMENT DUTIES

- Management entry point for both Web and API.
- Orchestrates all the host compute resources.
- Orchestrates the Guest and Public networks.
- Orchestrates VM storage (Root and Data).
- Our Case: MySQL database for ACS.
- Our Case: NFS mounts for storage.

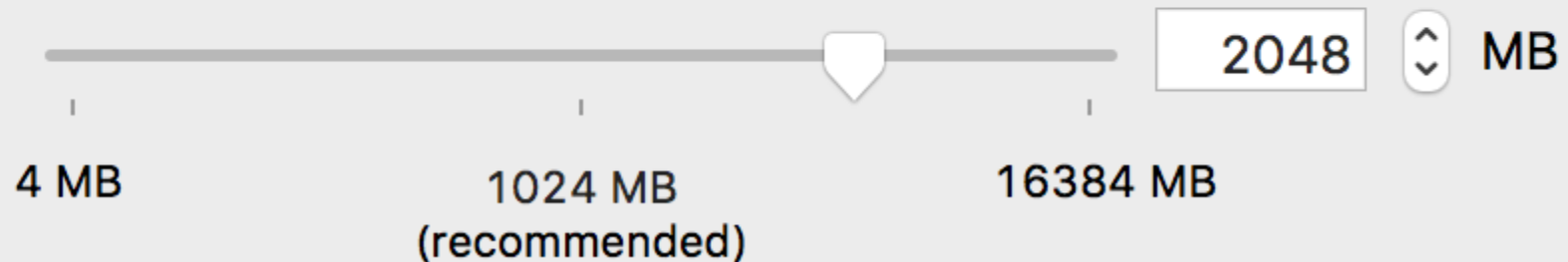
ACS MANAGEMENT VM RESOURCES

Restricted by the size of my laptop obviously.

Processors

2 processor cores

Memory



ACS MANAGEMENT NIC (ETH0)

Bridged Networking

- ☐ Autodetect
- ☐ Wi-Fi
- ☐ Thunderbolt Ethernet
- ☐ swlldroid
- ☐ Thunderbolt Ethernet 2
- ☐ iPhone USB
- ☐ Bluetooth PAN

Custom

- ☐ Private to my Mac
- ☒ vmnet2
- ☐ vmnet3

The virtual machine uses a custom network connection.

Name: **vmnet2**

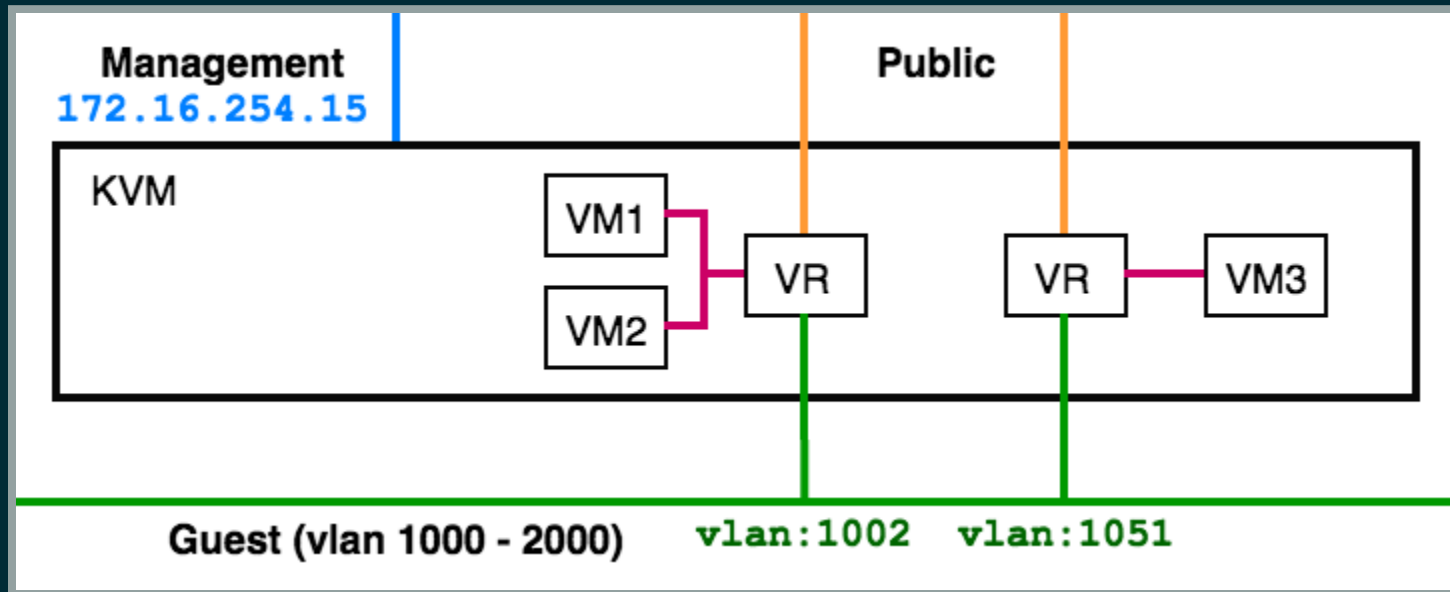
Type: **Custom**

Subnet IP: **172.16.254.0**

Subnet Mask: **255.255.255.0**

KVM HYPERVISOR VM

KVM Hypervisor Host for ACS to orchestrate.



```
./kvm/01_network_config.sh  
./kvm/02_install_kvm.sh
```

KVM DUTIES

- Provide compute resources to be orchestrated.
- Hosts the System VMs (more on this later).
- Guest network isolation and hosts the Guest VRs.
- Implements the snapshotting functionality.
- Implements the VM recovery point feature.

KVM HOST VM RESOURCES

Again, very limited due to the size of my Mac.


Processors

2 processor cores

Memory

4 MB1024 MB (recommended)16384 MB

6144 MB

 10240 MB remaining for your Mac

▼ Advanced options

☒ Enable hypervisor applications in this virtual machine

Enables running modern virtualization applications by providing support for Intel VT-x/EPT inside this virtual machine.

ACS MANAGEMENT NIC (ETH0 / CLOUDBRO)

Bridged Networking

- ☒ Autodetect
- ☒ Wi-Fi
- ☐ Thunderbolt Ethernet
- ☐ swilldroid
- ☐ Thunderbolt Ethernet 2
- ☐ iPhone USB
- ☐ Bluetooth PAN

Custom

- ☐ Private to my Mac
- ☒ vmnet2
- ☐ vmnet3

The virtual machine uses a custom network connection.

Name: **vmnet2**

Type: **Custom**

Subnet IP: **172.16.254.0**

Subnet Mask: **255.255.255.0**

ACS PUBLIC NIC (ETH1 / CLOUDBR1)

Bridged Networking

- ☒ Autodetect
- ☒ Wi-Fi
- ☐ Thunderbolt Ethernet
- ☐ swlldroid
- ☐ Thunderbolt Ethernet 2
- ☐ iPhone USB
- ☐ Bluetooth PAN

Custom

- ☒ Private to my Mac
- ☒ vmnet2
- ☒ vmnet3

The virtual machine uses a custom network connection.

Name: **vmnet3**

Type: **Custom**

Subnet IP: **192.168.80.0**

Subnet Mask: **255.255.255.0**

ACS GUEST NIC (ETH2 / CLOUDBR2)

Bridged Networking

☐ Autodetect

☒ Thunderbolt Ethernet 2

☐ Wi-Fi

☐ Thunderbolt Ethernet

☐ swilldroid

☐ iPhone USB

☐ Bluetooth PAN

Custom

☐ Private to my Mac

☐ vmnet2

☐ vmnet3

The virtual machine appears as an additional computer on the physical Ethernet network "Thunderbolt Ethernet 2".

Name: **Thunder...thernet 2**

Type: **Ethernet**

IP: **192.168.254.2**

Subnet Mask: **255.255.255.0**

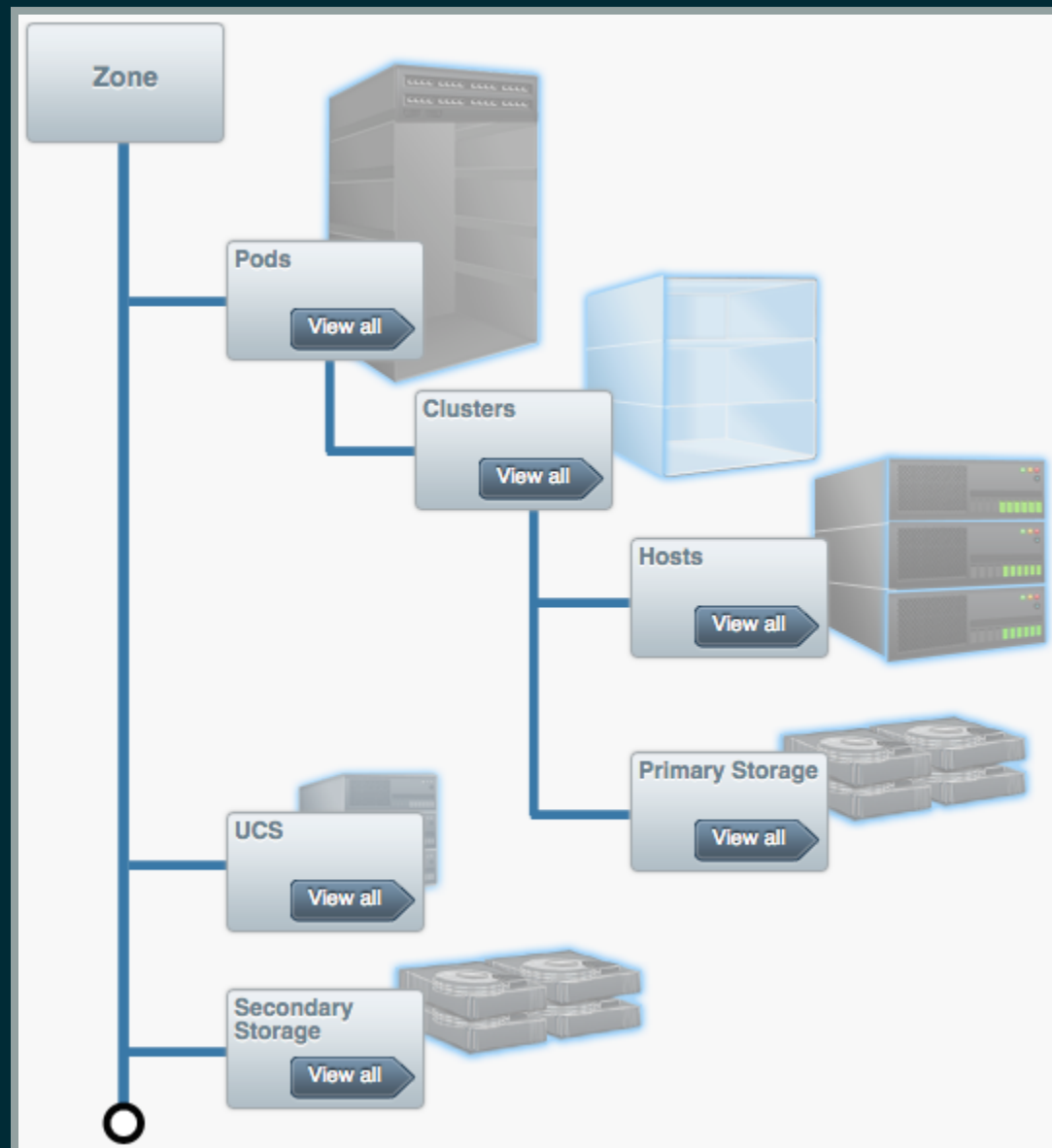
System Preferences...

DEPLOY DATACENTER

ACS and KVM are both ready to go now, but not configured...

- Setup Zone, Pod, Cluster and KVM Host.
- Configure the orchestrated network ranges.
- Start System VMs (SSVM + Console)

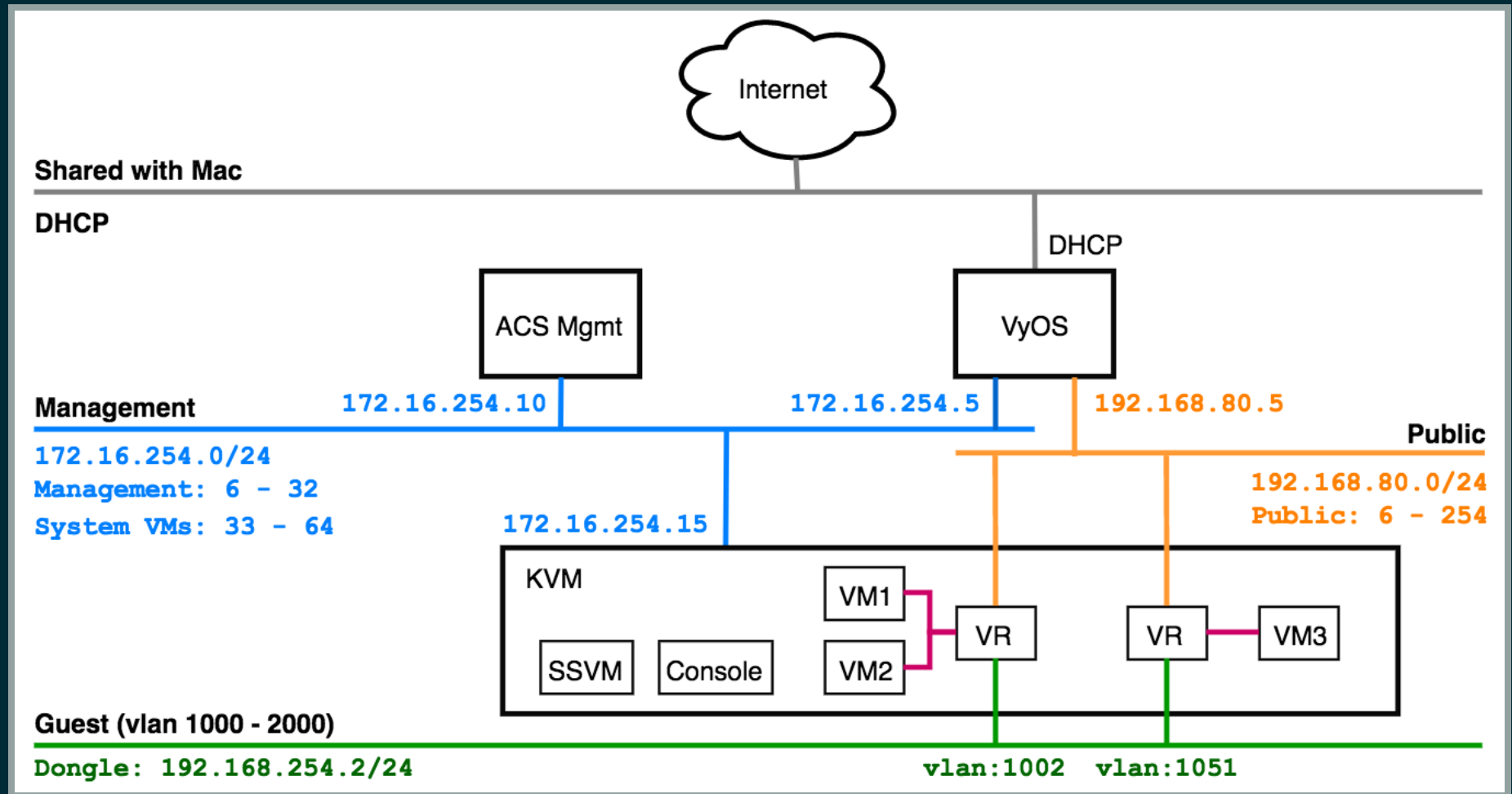
```
./acs/03_configure_zone.sh
```



FUNCTIONAL GROUPINGS

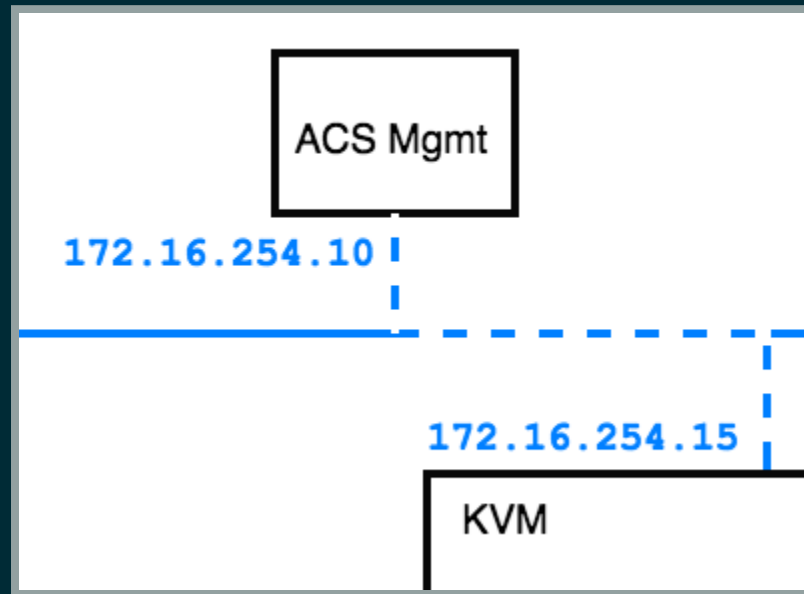
- Region: A grouping of Zones.
- Zone: Usually a single data center.
 - Secondary Storage, Guest & Public IP Ranges
- Pod: Usually a rack with one or more Clusters.
 - Management Network, Cluster connectivity
- Cluster: A group of hosts of the same hypervisor type.
 - Primary Storage
- Host: The actual hypervisor host being orchestrated.
 - VMware, XenServer, KVM, HyperV

ARCHITECTURE REVIEW



ACS & KVM

ACS orchestrates the resources on the KVM Host.



MORE DETAILS

- ACS Mgmt is exposing Primary Storage over NFS.
- ACS Mgmt is exposing Secondary Storage over NFS.
- KVM hosts the guest VMs provisioned by ACS.
- KVM hosts the Guest networks provisioned by ACS.
- KVM hosts the System VMs (SSVM + Console VM).

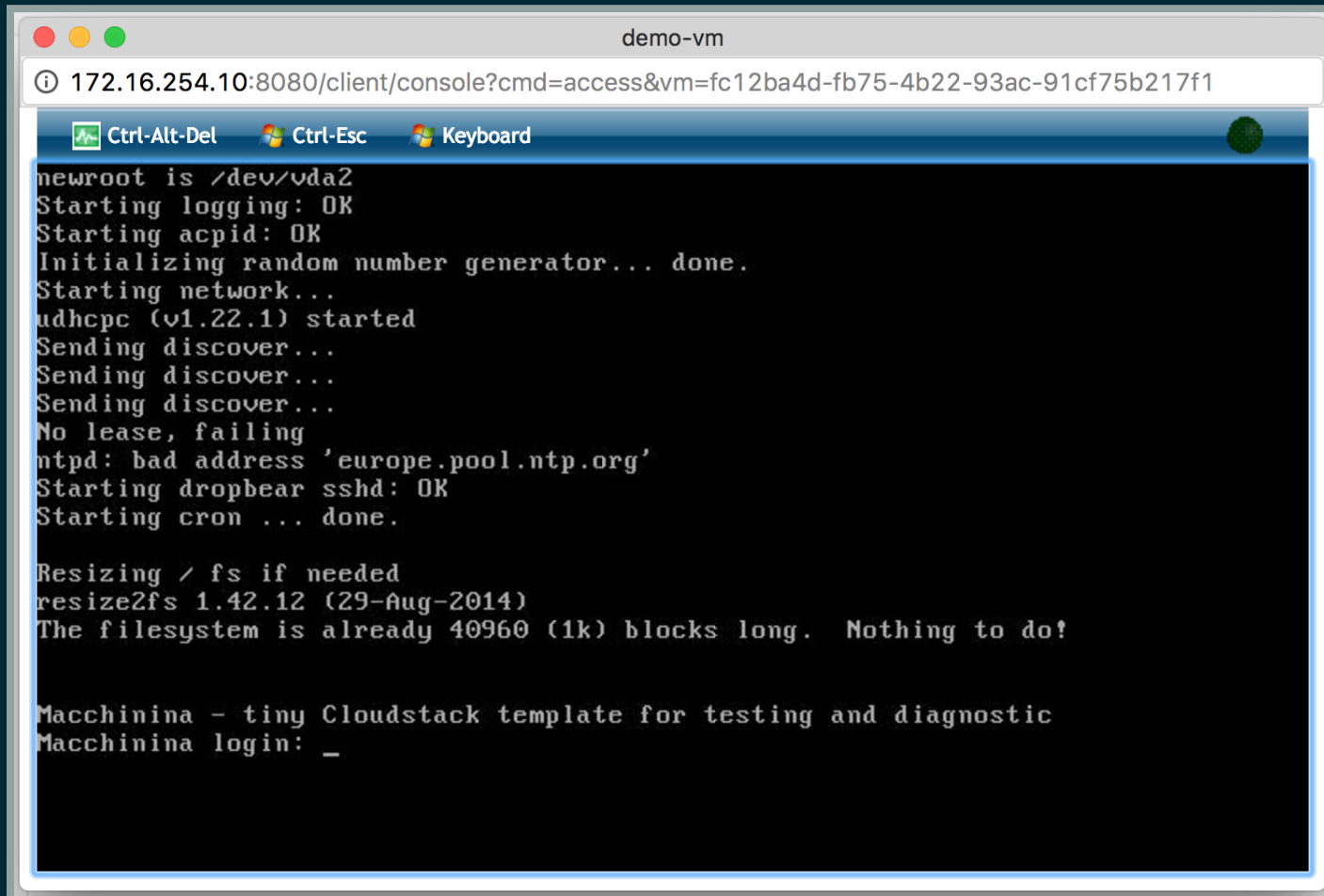
SECONDARY STORAGE VM (SSVM)

Handles everything related to templates and snapshots.

- Transfer snapshots from Primary to Secondary storage.
- Converting snapshots to templates to launch VMs.
- Uploading and exposing templates to launch guest VMs.

CONSOLE PROXY VM

Exposes VM consoles through a web UI.



The screenshot shows a web browser window with the title "demo-vm". The address bar contains the URL "172.16.254.10:8080/client/console?cmd=access&vm=fc12ba4d-fb75-4b22-93ac-91cf75b217f1". Below the address bar is a toolbar with three icons: a keyboard icon labeled "Ctrl-Alt-Del", a keyboard icon labeled "Ctrl-Esc", and a keyboard icon labeled "Keyboard". The main content area is a black terminal window with white text. The text shows the boot process of a VM, including starting logging, acpid, network, and various services. It also shows a message about the filesystem size and a login prompt for "Macchinina".

```
newroot is /dev/vda2
Starting logging: OK
Starting acpid: OK
Initializing random number generator... done.
Starting network...
udhcpd (v1.22.1) started
Sending discover...
Sending discover...
Sending discover...
No lease, failing
ntpd: bad address 'europe.pool.ntp.org'
Starting dropbear sshd: OK
Starting cron ... done.

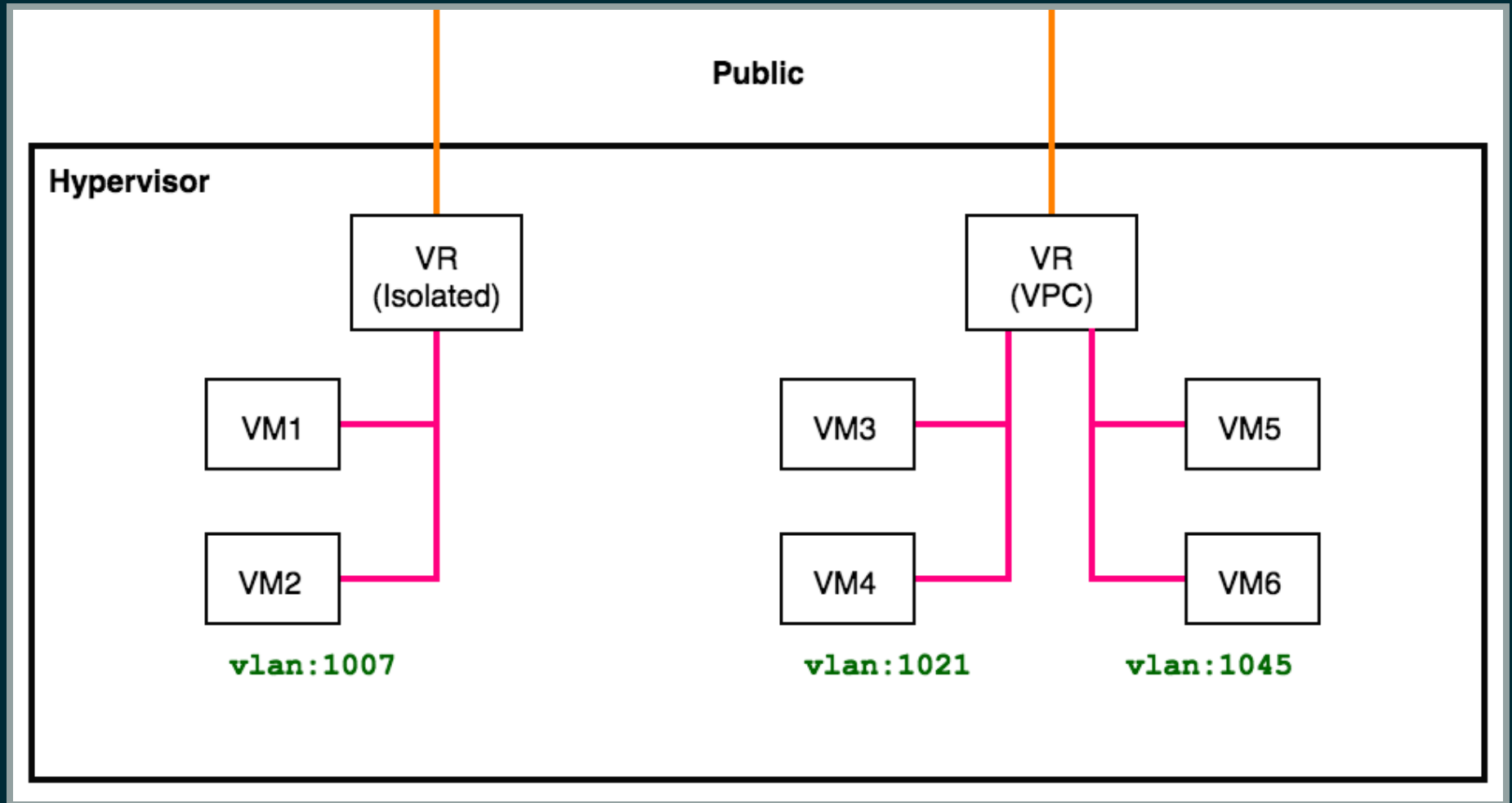
Resizing / fs if needed
resize2fs 1.42.12 (29-Aug-2014)
The filesystem is already 40960 (1k) blocks long.  Nothing to do!

Macchinina - tiny Cloudstack template for testing and diagnostic
Macchinina login: _
```

LET'S GO EXPLORE...

`172.16.254.10:8080/client`

CLOUDSTACK ADVANCED NETWORKING



ISOLATED GUEST NETWORKS

- Single tier network.
- Network Features:
 - Source Nat
 - Static Nat
 - Port Forwarding
 - Load Balancing
 - Firewall Rules (Ingress & Egress)
 - DHCP & DNS
 - Remote Access VPN

VPC NETWORKS

- Multi-tier network.
- Network Features:
 - Source Nat
 - Static Nat
 - Port Forwarding
 - Load Balancing
 - Network ACLs (like Firewall Rules)
 - DHCP & DNS
 - Remote Access VPN
 - Site-to-Site VPN
 - Private Gateways (datacenter connect)
 - Static Routes