RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Good Fences Make Good Neighbors: Rethinking Your Cloud Selection Strategy

SESSION ID: CSV-W01

Bryan D. Payne

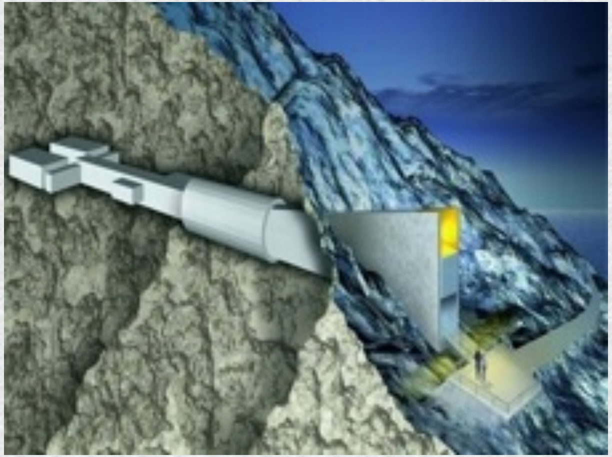
Director of Security Research
Nebula
@bdpsecurity

Cloud Security Today

- Cloud has lots of momentum
- Lots of concerns about security
- What's the real story?

What this talk will cover

- What does it take to secure an IaaS cloud?
- Specific ideas to improve your cloud or select a cloud provider.



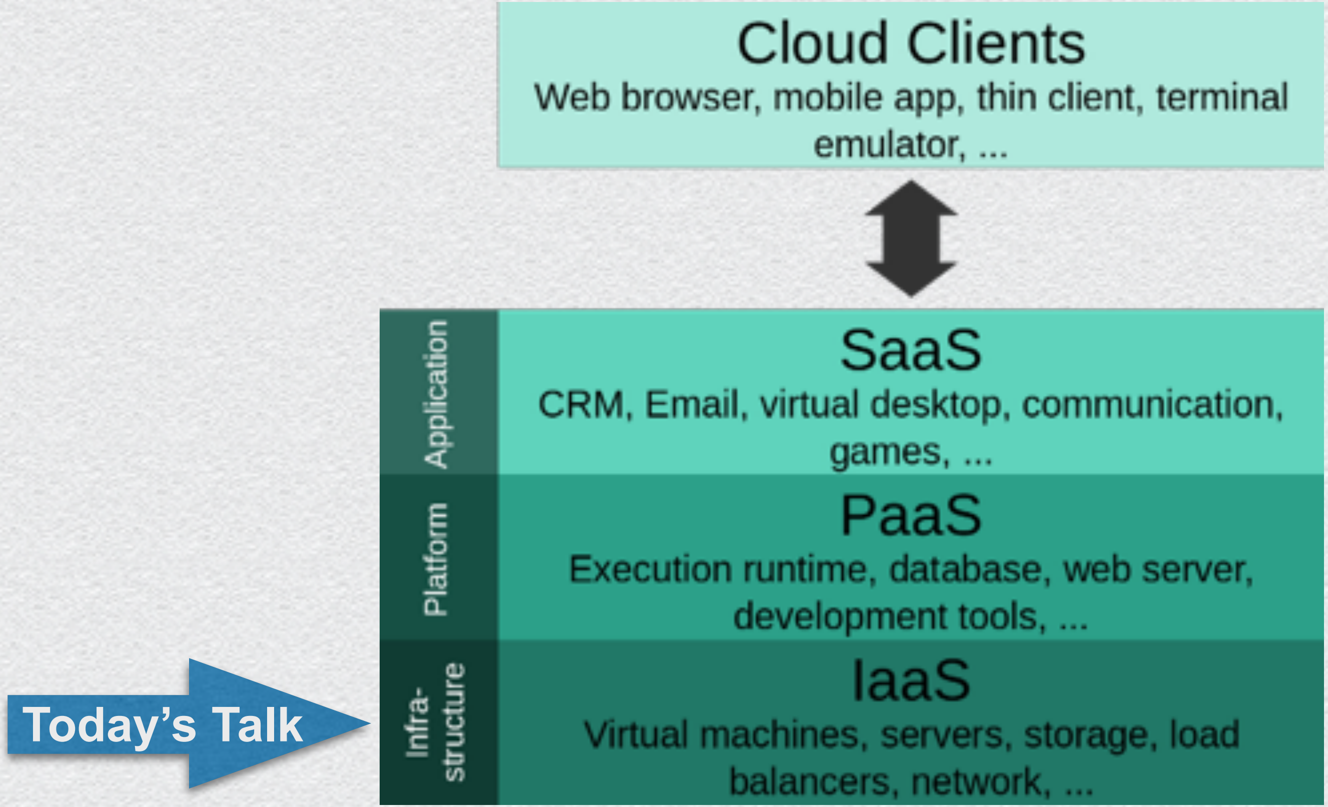
What this talk will **NOT** cover

- A cloud comparison
- A one-size-fits-all cloud security cookbook

Talk Outline

- Cloud Introduction (demo!)
- IaaS Architecture Details
- Security Differentiators
- Virtualization Stack Security (demo!)
- Questions & Wrap-up

Cloud Service Models



Cloud Clients

Web browser, mobile app, thin client, terminal emulator, ...

Application

SaaS

CRM, Email, virtual desktop, communication, games, ...

Platform

PaaS

Execution runtime, database, web server, development tools, ...

Infrastructure

IaaS

Virtual machines, servers, storage, load balancers, network, ...

Today's Talk

Public Cloud

- Users: Anyone with a credit card
- Provider
  - Doesn’t trust users
  - Doesn’t want to violate users privacy

- Monitoring at network edges
- Fraud prevention
- Network reputation concerns
- Broad compliance concerns

Private Cloud

- Users: Part of a common organization
- Provider
  - Trusts users (at some level)
  - Has full access to data / workloads

- Security from top to bottom
- Design undergoes great scrutiny
- Enterprise integration
- Targeted compliance concerns

Know Your Neighbors

- Who are your neighbors (other users)?
- Who is your cloud admin / operator / builder?
- Who else has privilege on the cloud?
  - Who should?
  - Who does?

Demo: How Things Can Go Very Wrong

nebula

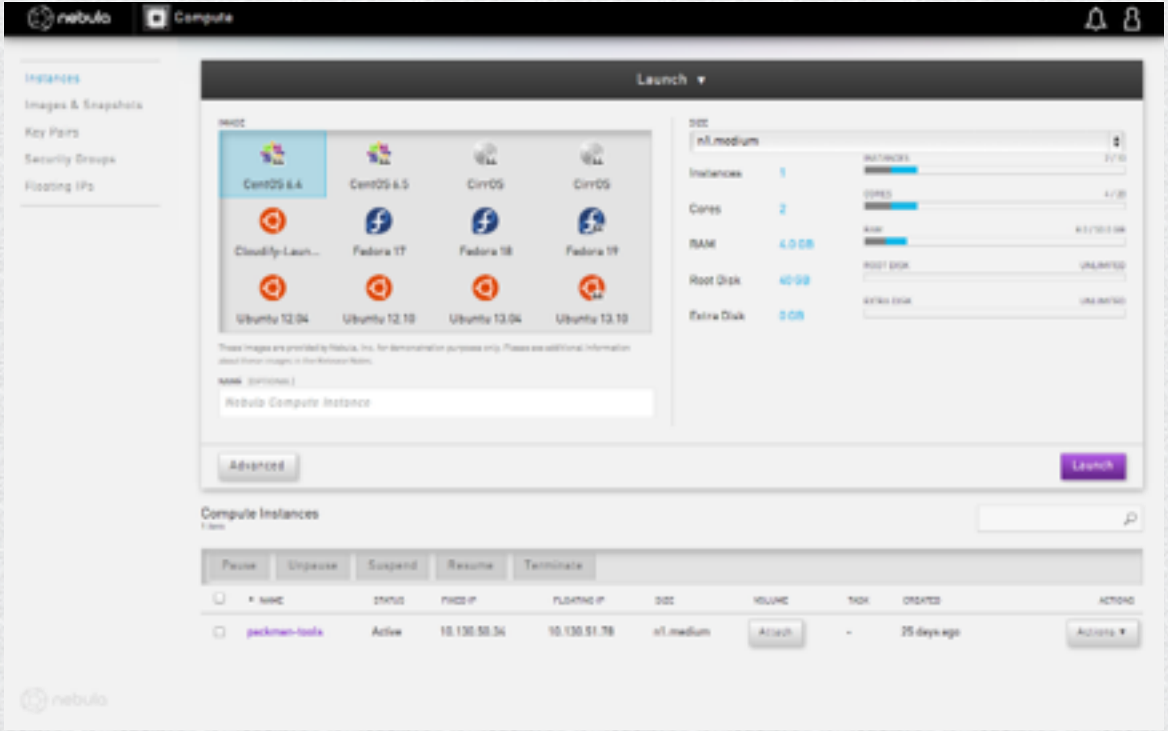
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Understanding IaaS Cloud Architectures

User Perspective

- Launch instances
- Take snapshots
- Flexible storage options
- API + web dashboard



SIZE: n1.medium

Instances 1

Cores 2

RAM 4.0 GB

Root Disk 40 GB

Extra Disk 0 GB

Compute Instances

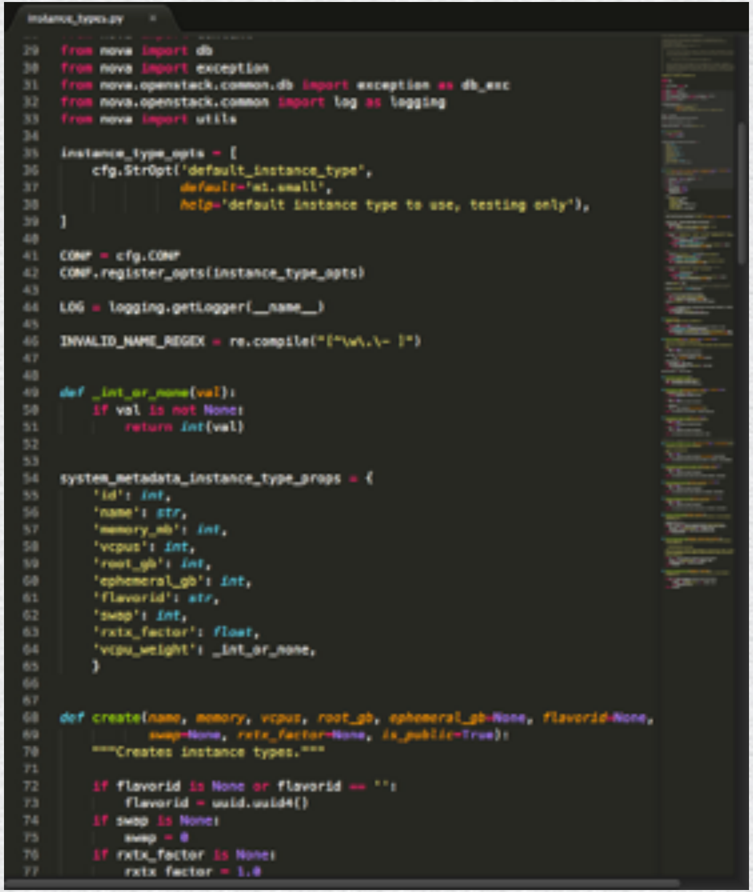
	NAME	STATUS	FIXED IP	FLOATING IP	SIZE	VOLUME	TASK	CREATED	ACTIONS
□	packman-tools	Active	10.130.50.34	10.130.51.78	n1.medium	Attach	-	25 days ago	Actions ▾

Admin / Operator Perspective

- Create & manage users, projects, quotas, etc
- Configure cloud
- Monitor cloud events, logs, health, etc
- API + web dashboard

Builder Perspective

- Software engineer & DevOps
- Designs and creates cloud
- Controls security domains
- Many services to setup & manage



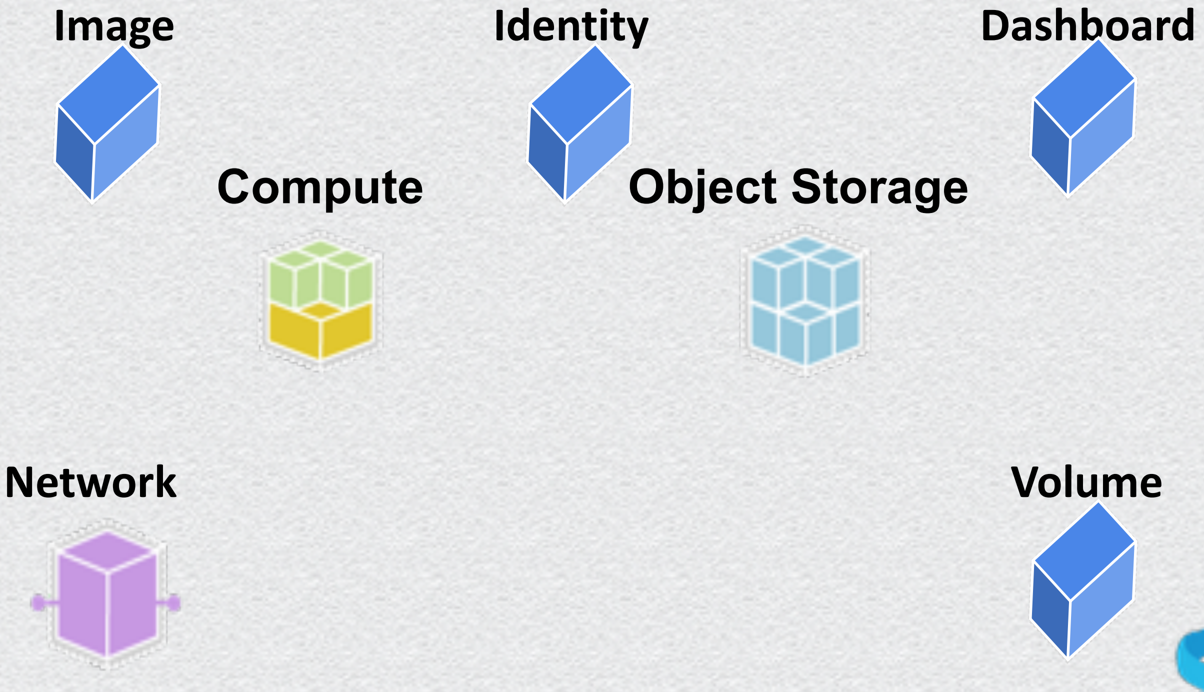
```python
from nova import db
from nova import exception
from nova.openstack.common.db import exception as db_exc
from nova.openstack.common import log as logging
from nova import utils

instance_type_opts = [
    cfg.StrOpt('default_instance_type',
               default='m1.small',
               help='default instance type to use, testing only'),
]

CONF = cfg.CONF
CONF.register_opts(instance_type_opts)

LOG = logging.getLogger(__name__)

INVALID_NAME_REGEX = re.compile("[^\w\.\- ]")


def _int_or_none(val):
    if val is not None:
        return int(val)


system_metadata_instance_type_props = {
    'id': int,
    'name': str,
    'memory_mb': int,
    'vcpus': int,
    'root_gb': int,
    'ephemeral_gb': int,
    'flavorid': str,
    'swap': int,
    'rxtx_factor': float,
    'vcpu_weight': _int_or_none,
    }


def create(name, memory, vcpus, root_gb, ephemeral_gb=None, flavorid=None,
           swap=None, rxtx_factor=None, is_public=True):
    """Creates instance types."""

    if flavorid is None or flavorid == '':
        flavorid = uuid.uuid4()
    if swap is None:
        swap = 0
    if rxtx_factor is None:
        rxtx_factor = 1.0
```

Cloud Simplicity

Compute **Object Storage**

Example services from OpenStack.

Individual Services



Image

Identity

Dashboard

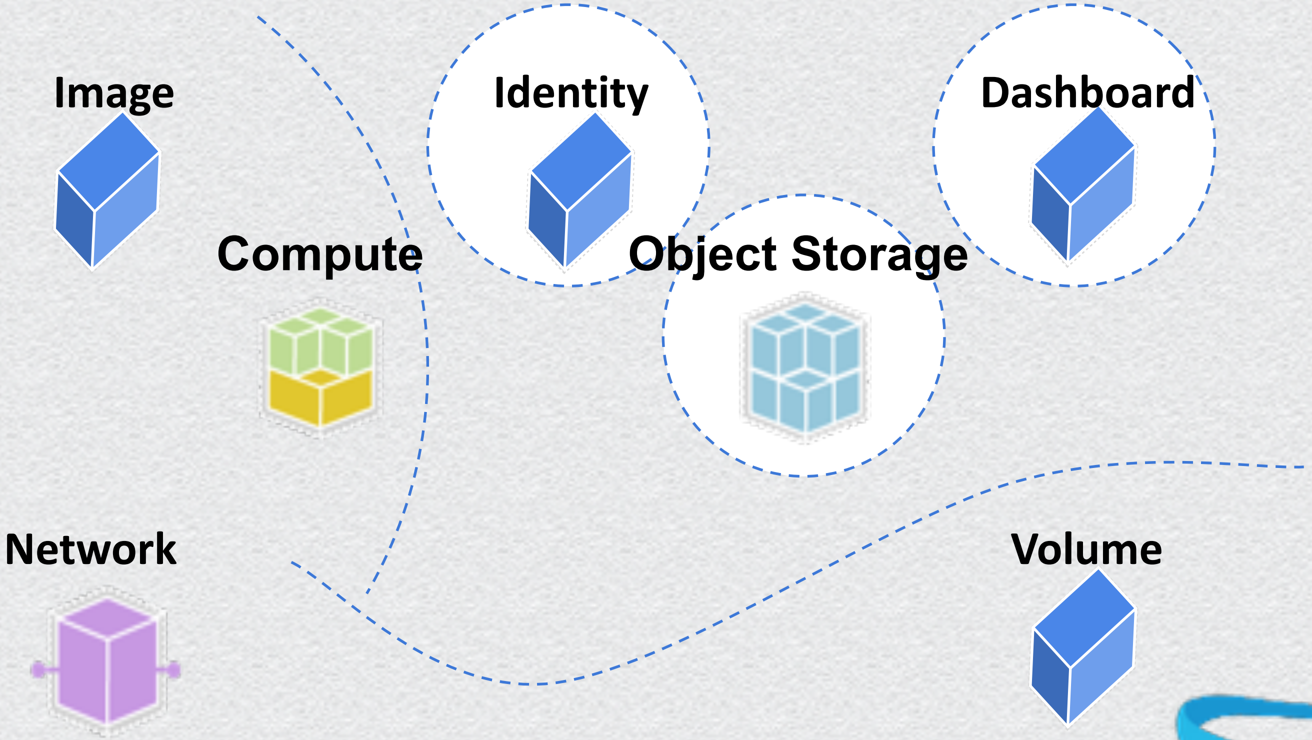
Compute

Object Storage

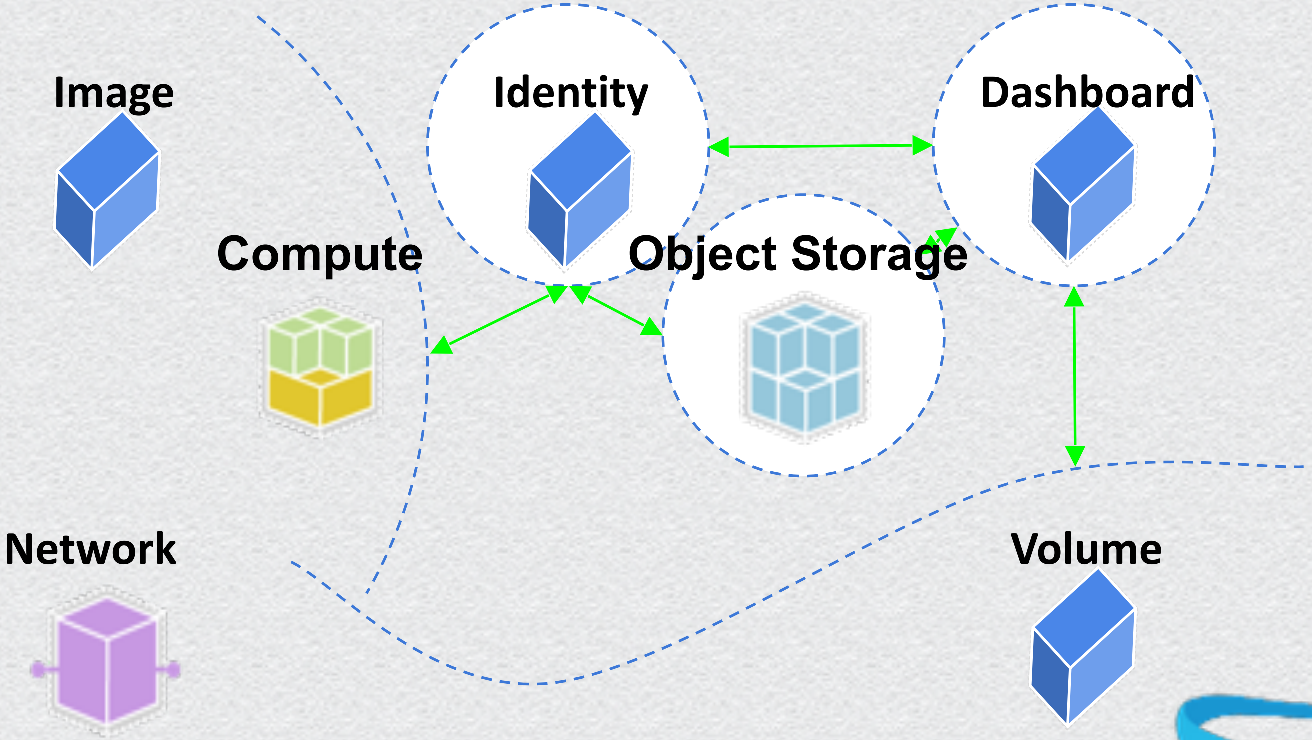
Network

Volume

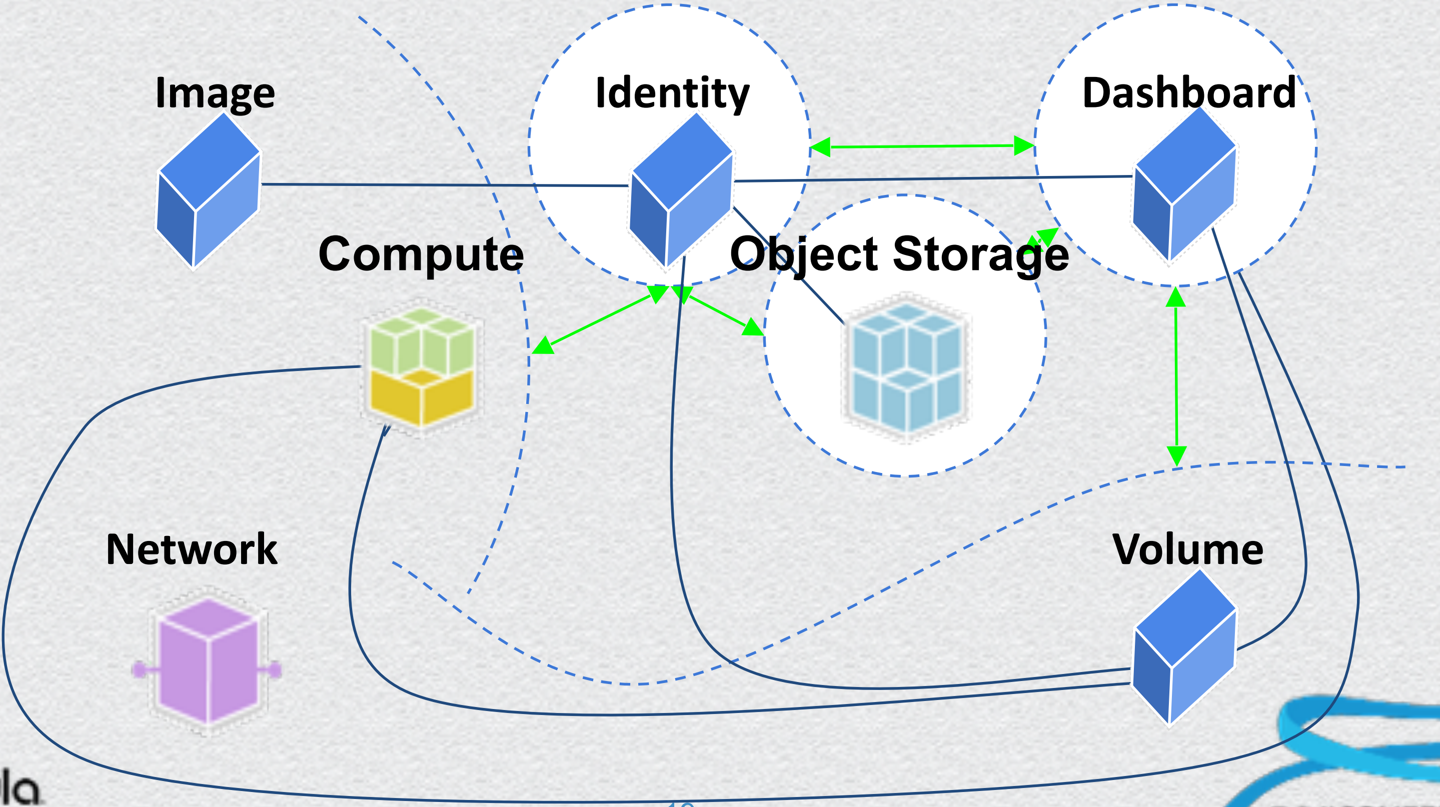
Security Domains



Gated Interconnects



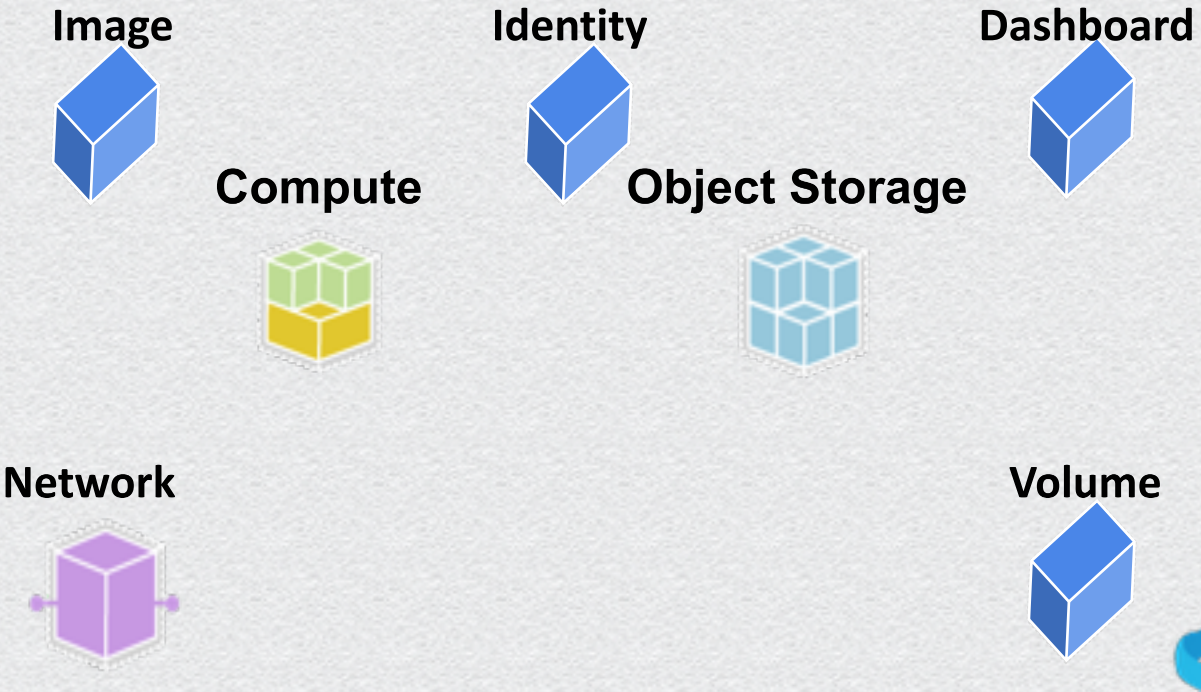
Map Data Paths



Secure design complete…

…or is it?

Individual Services



Image

Identity

Dashboard

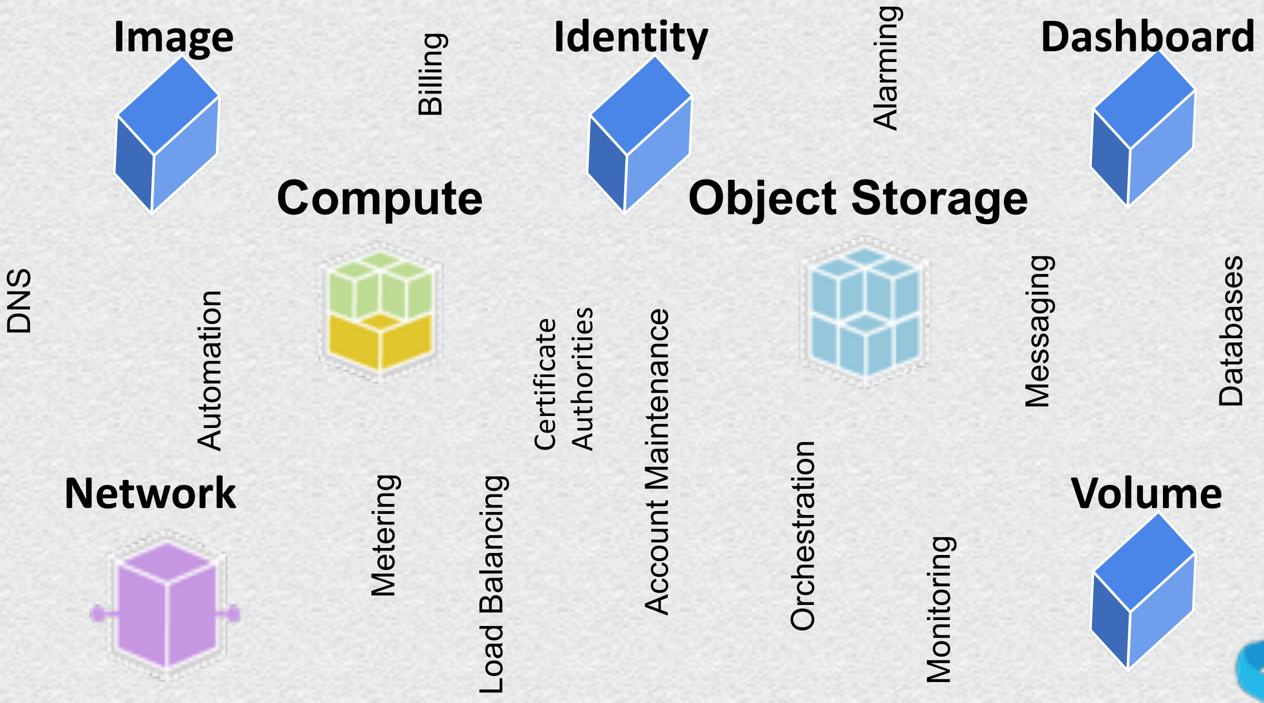
Compute

Object Storage

Network

Volume

Lots of Glue



Image

Billing

Identity

Alarming

Dashboard

Compute

Object Storage

DNS

Automation

Certificate Authorities

Account Maintenance

Messaging

Databases

Network

Metering

Load Balancing

Orchestration

Monitoring

Volume

Data Paths

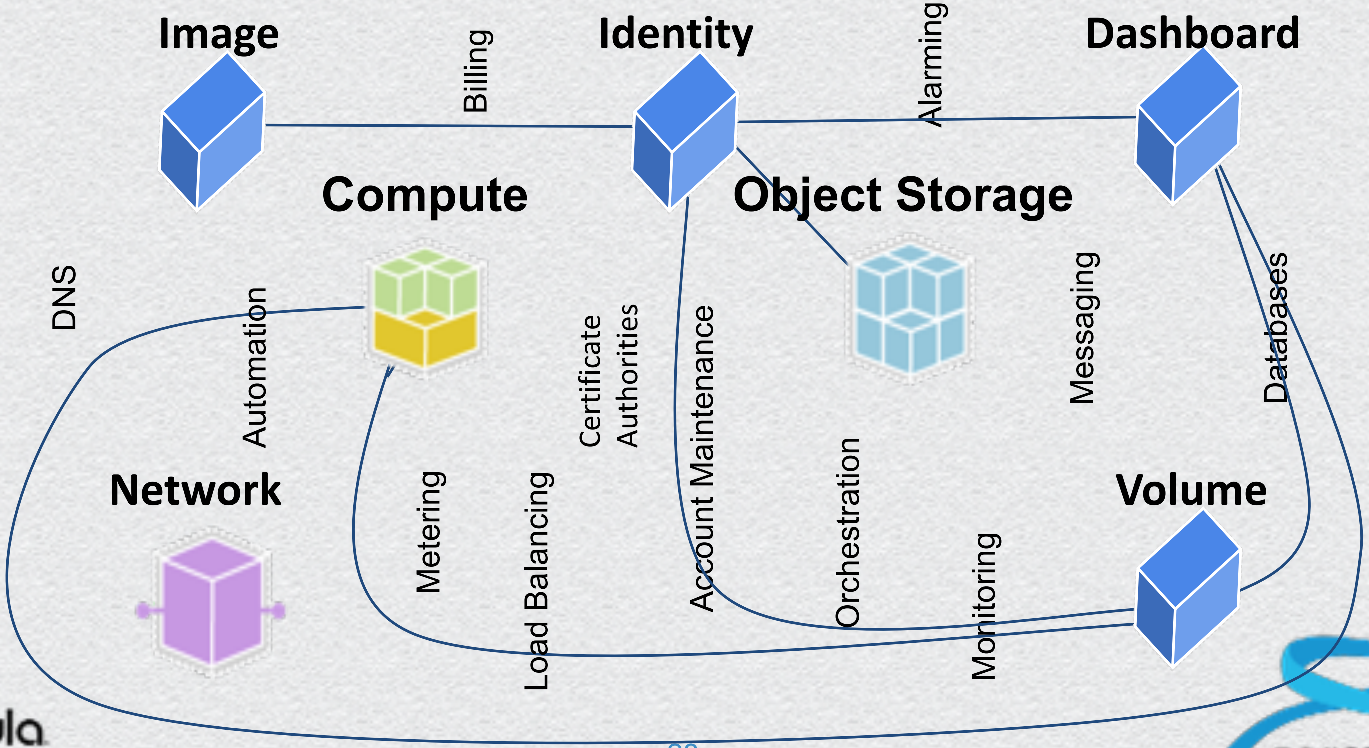
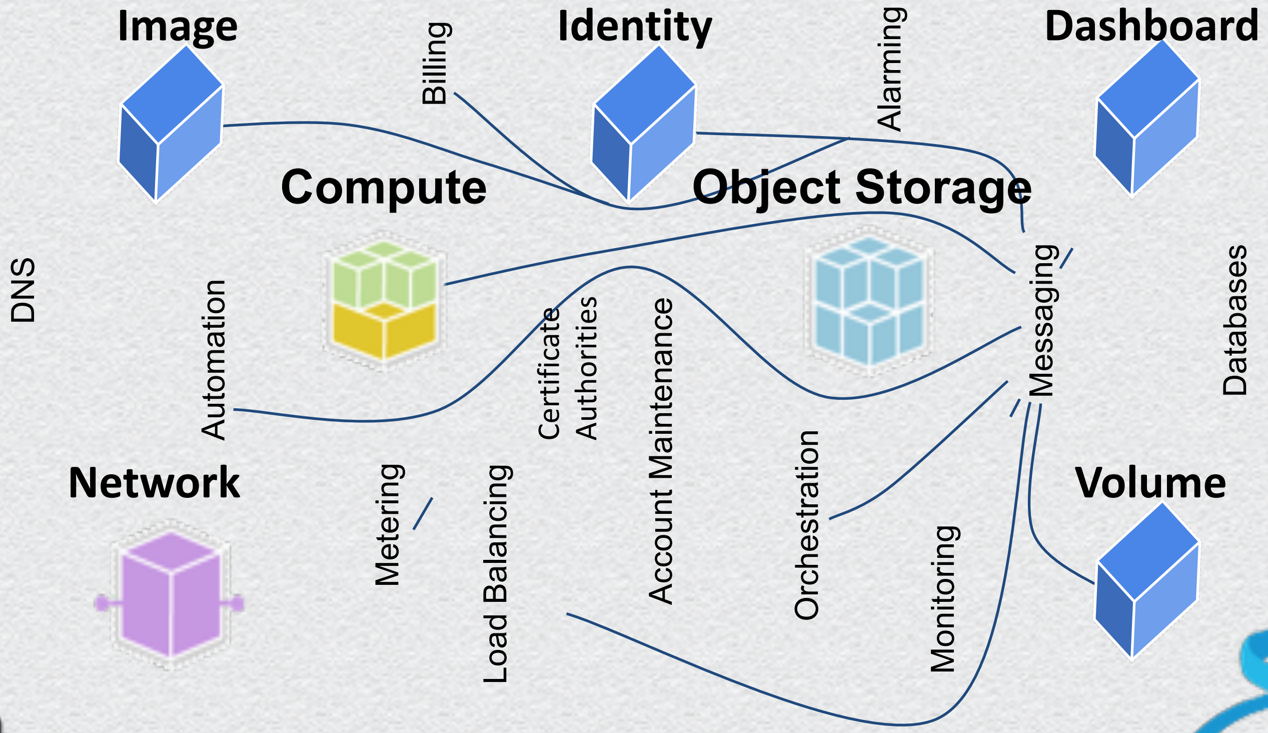
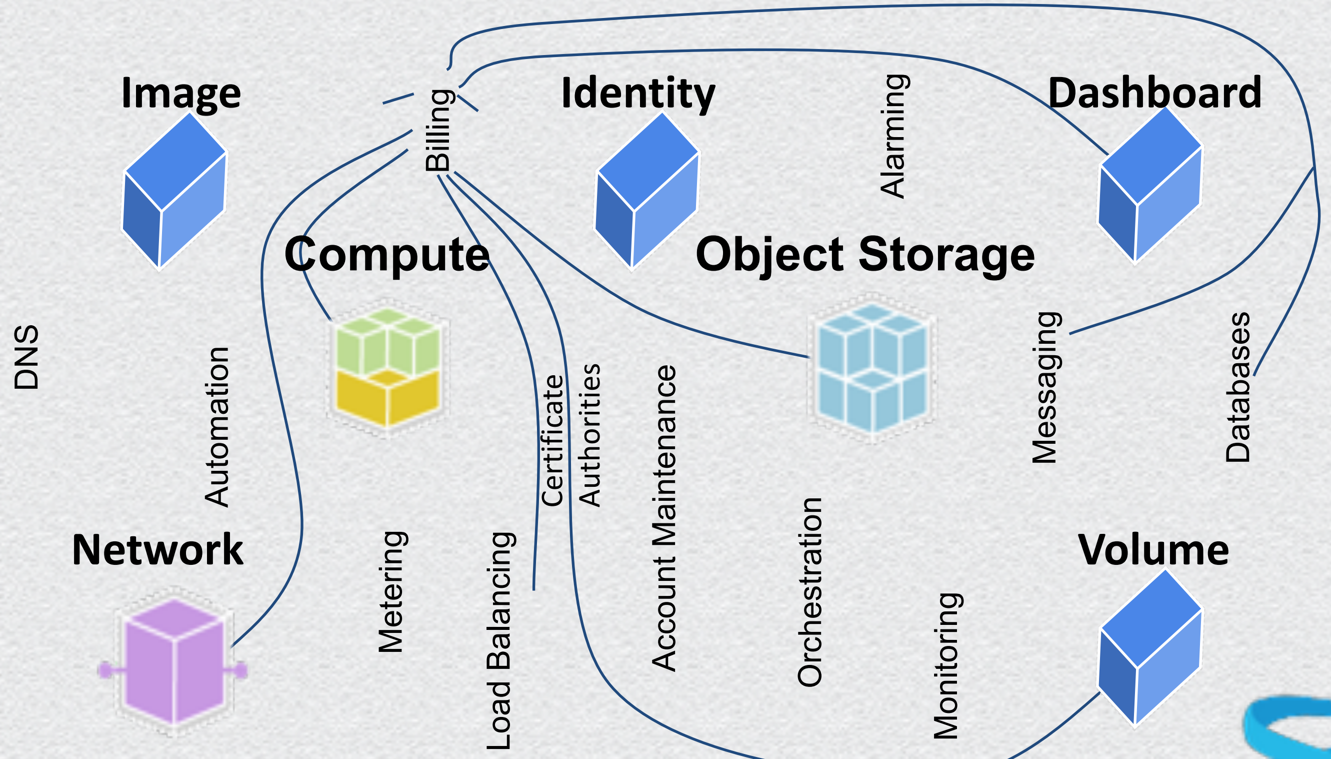


Image
Billing
Identity
Alarming
Dashboard
Compute
Object Storage
DNS
Automation
Certificate Authorities
Account Maintenance
Messaging
Databases
Network
Metering
Load Balancing
Orchestration
Monitoring
Volume

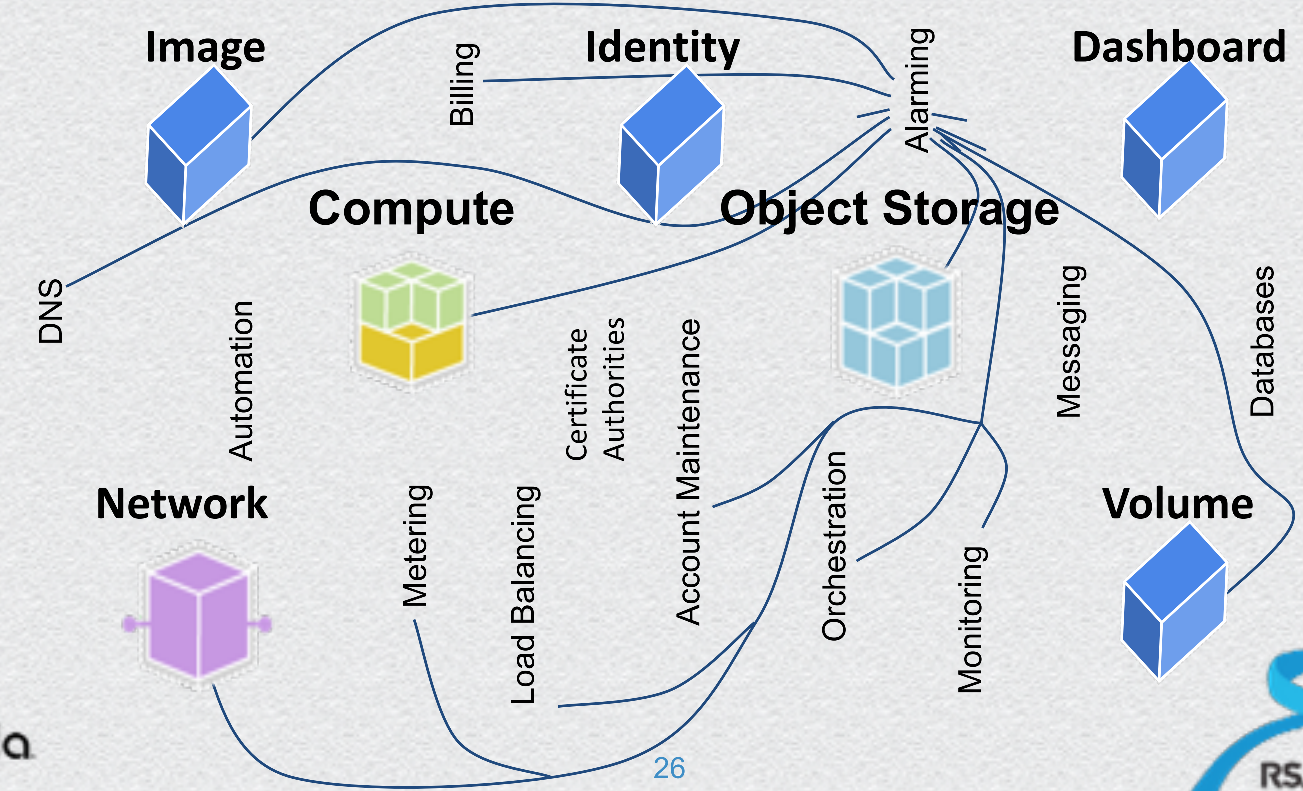
Message Plumbing



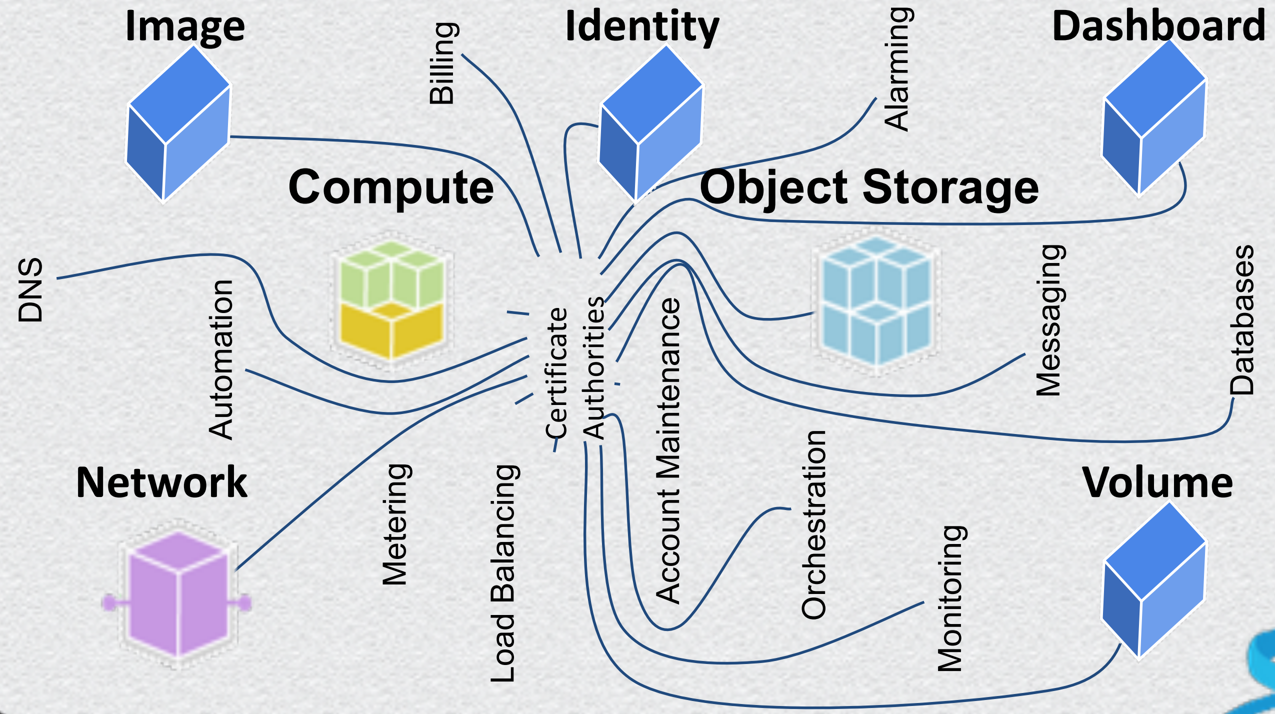
Billing Plumbing



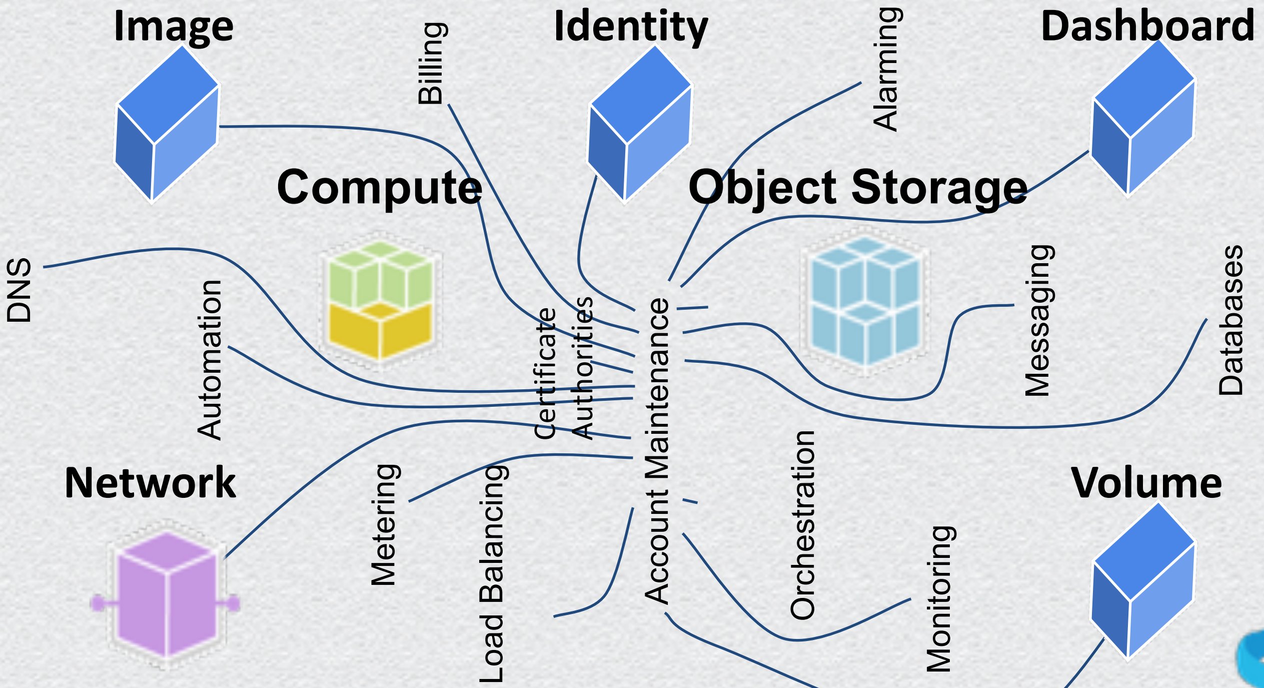
Alarm Plumbing



SSL / TLS Plumbing

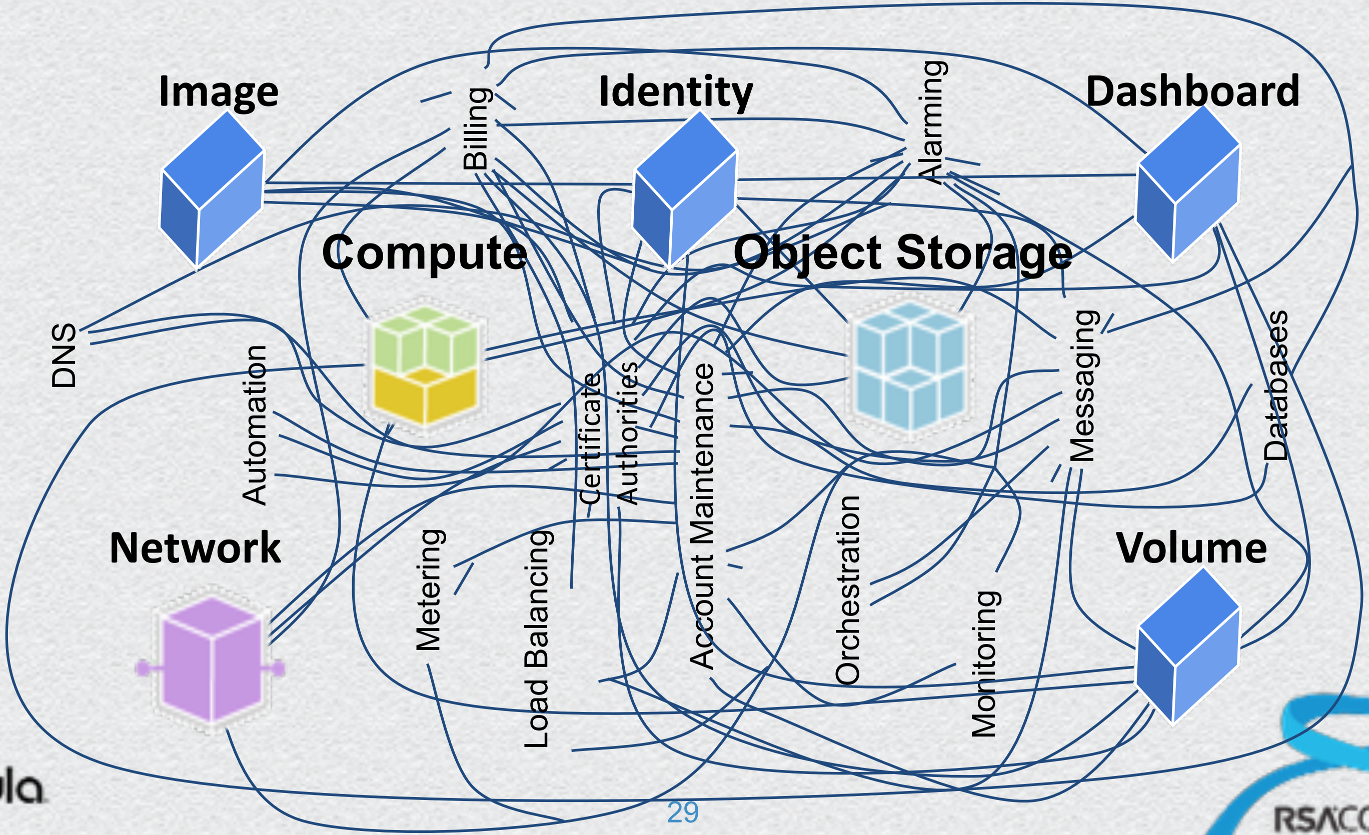


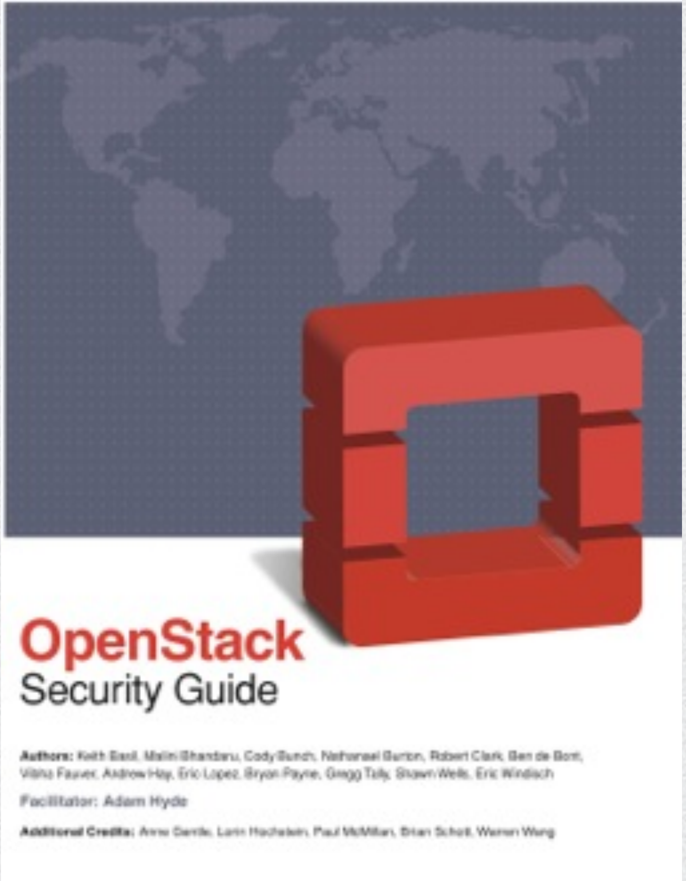
Under Cloud Admin Plumbing



nebula

So Much Plumbing!





OpenStack
Security Guide

Authors: Keith Basil, Malini Bhandaru, Cody Bunch, Nathanael Burton, Robert Clark, Ben de Bont, Vibha Fauver, Andrew Hay, Eric Lopez, Bryan Payne, Gregg Tally, Shawn Wells, Eric Windisch

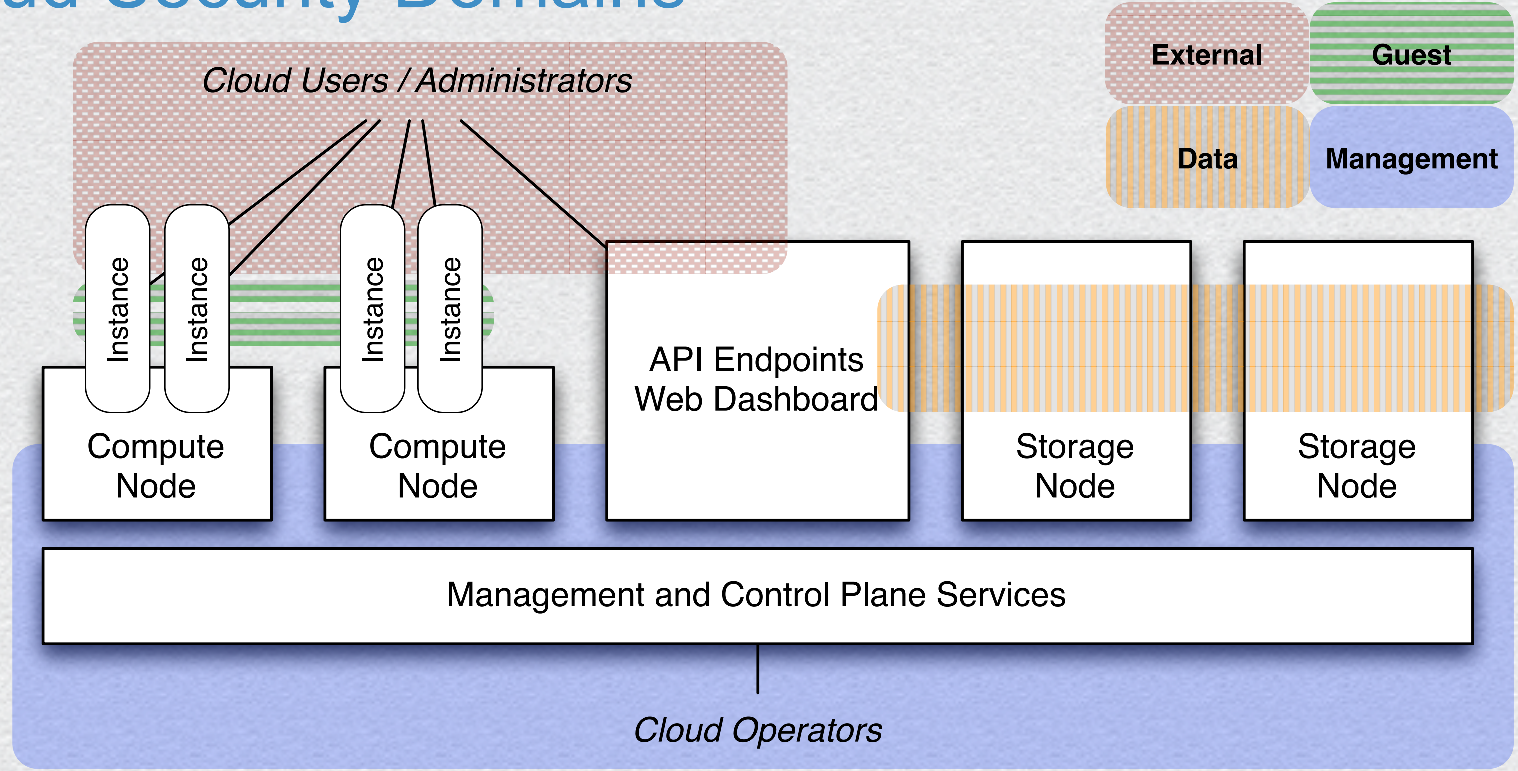
Facilitator: Adam Hyde

Additional Credits: Anne Gentle, Lorin Hochstein, Paul McMillan, Brian Schott, Warren Wang

OpenStack Security Guide

- http://doc.openstack.org/sec/
- Security guidance on deploying OpenStack (IaaS Cloud)
- Written in one week
- Diverse group of authors
- Continued contributions accepted through GitHub

Cloud Security Domains

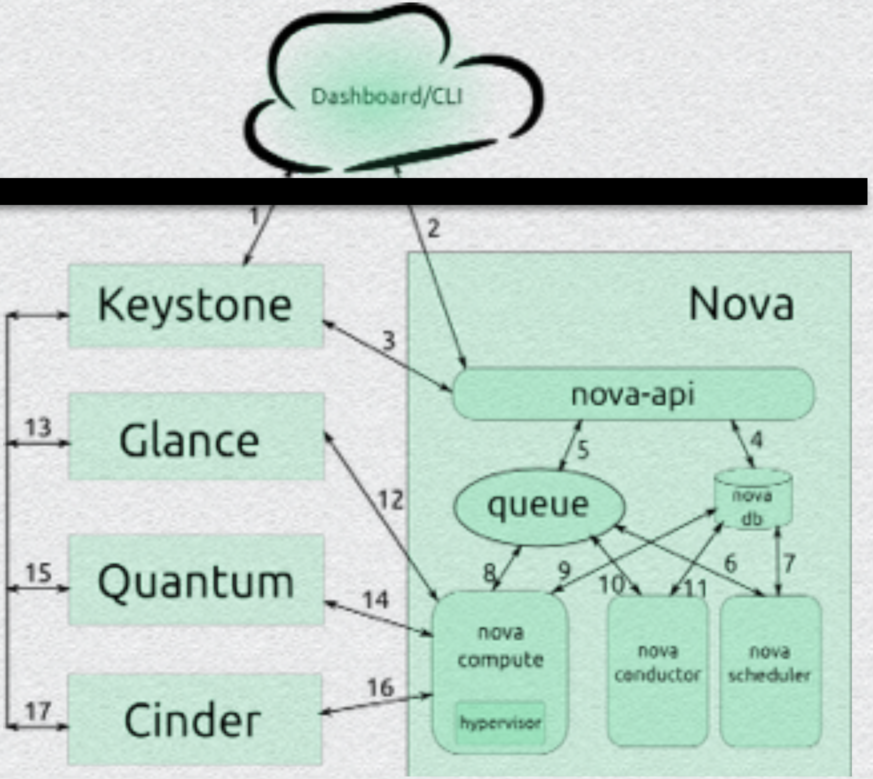


nebula

Example API Action: Launching an Instance

External

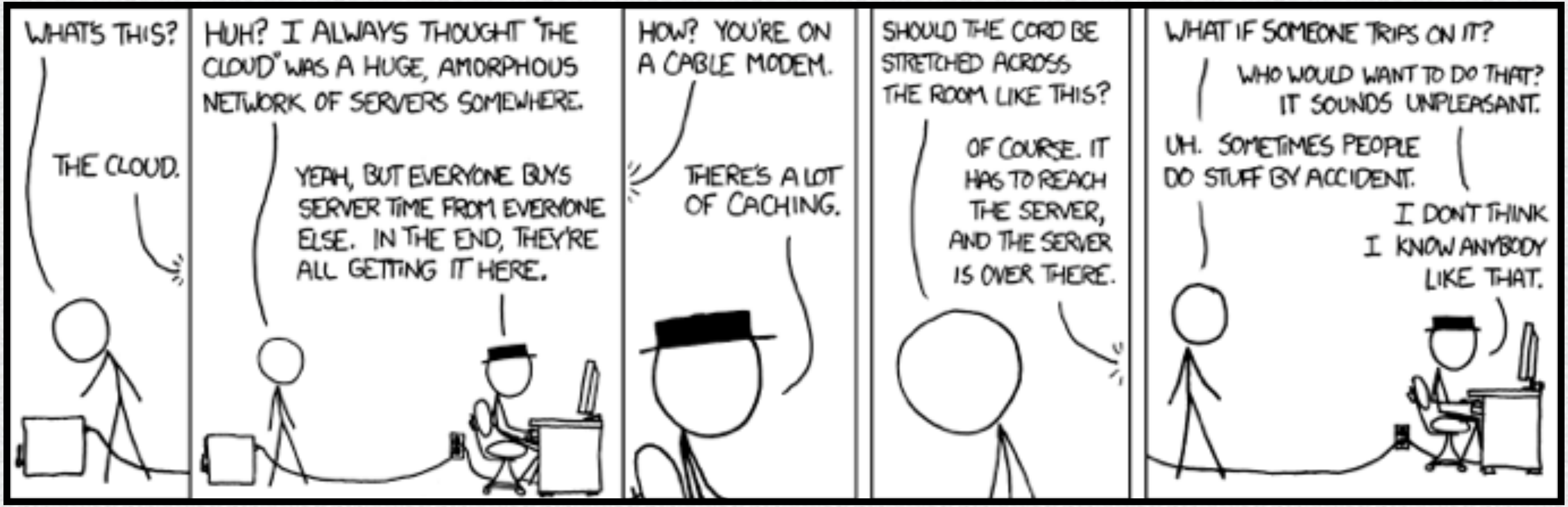
Management



Source: http://docs.openstack.org/training-guides/

Security Challenges in the Cloud

- Audit trails
- Controlling access
- Defense in depth / Layered security
- Protecting bridge points
  - API Endpoints
  - Virtualization Security


WHAT'S THIS?
THE CLOUD.
HUH? I ALWAYS THOUGHT "THE CLOUD" WAS A HUGE, AMORPHOUS NETWORK OF SERVERS SOMEWHERE.
YEAH, BUT EVERYONE BUYS SERVER TIME FROM EVERYONE ELSE. IN THE END, THEY'RE ALL GETTING IT HERE.
HOW? YOU'RE ON A CABLE MODEM.
THERE'S A LOT OF CACHING.
SHOULD THE CORD BE STRETCHED ACROSS THE ROOM LIKE THIS?
OF COURSE. IT HAS TO REACH THE SERVER, AND THE SERVER IS OVER THERE.
WHAT IF SOMEONE TRIPS ON IT?
WHO WOULD WANT TO DO THAT? IT SOUNDS UNPLEASANT.
UH. SOMETIMES PEOPLE DO STUFF BY ACCIDENT.
I DON'T THINK I KNOW ANYBODY LIKE THAT.

Source: http://xkcd.com/908/

RSACONFERENCE2014

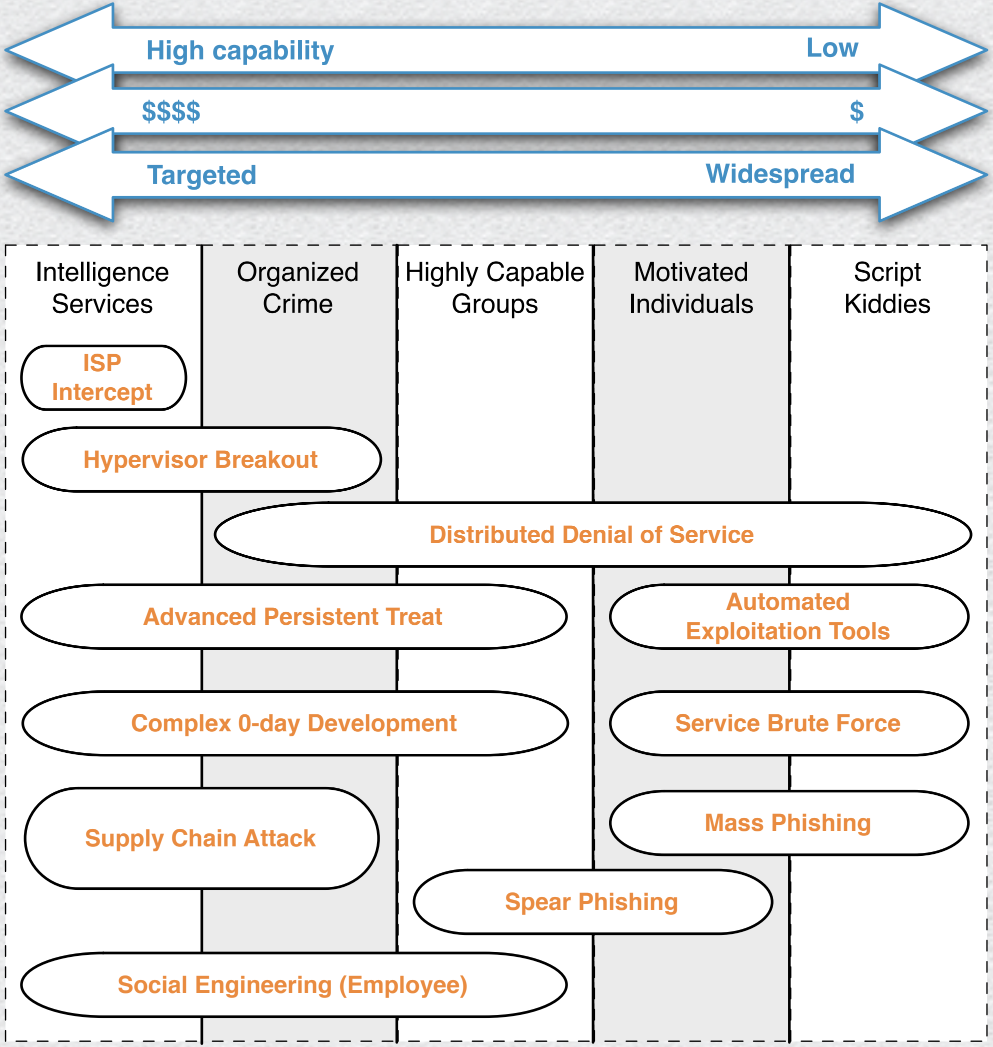
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Cloud Security Differentiators

Security Certifications

- Necessary, but not sufficient
- Mapping to cloud not always clear
- Not a useful place to differentiate

Threats



High capability — Low

$$$$ — $

Targeted — Widespread

Intelligence Services | Organized Crime | Highly Capable Groups | Motivated Individuals | Script Kiddies

ISP Intercept

Hypervisor Breakout

Distributed Denial of Service

Advanced Persistent Treat

Automated Exploitation Tools

Complex 0-day Development

Service Brute Force

Supply Chain Attack

Mass Phishing

Spear Phishing

Social Engineering (Employee)

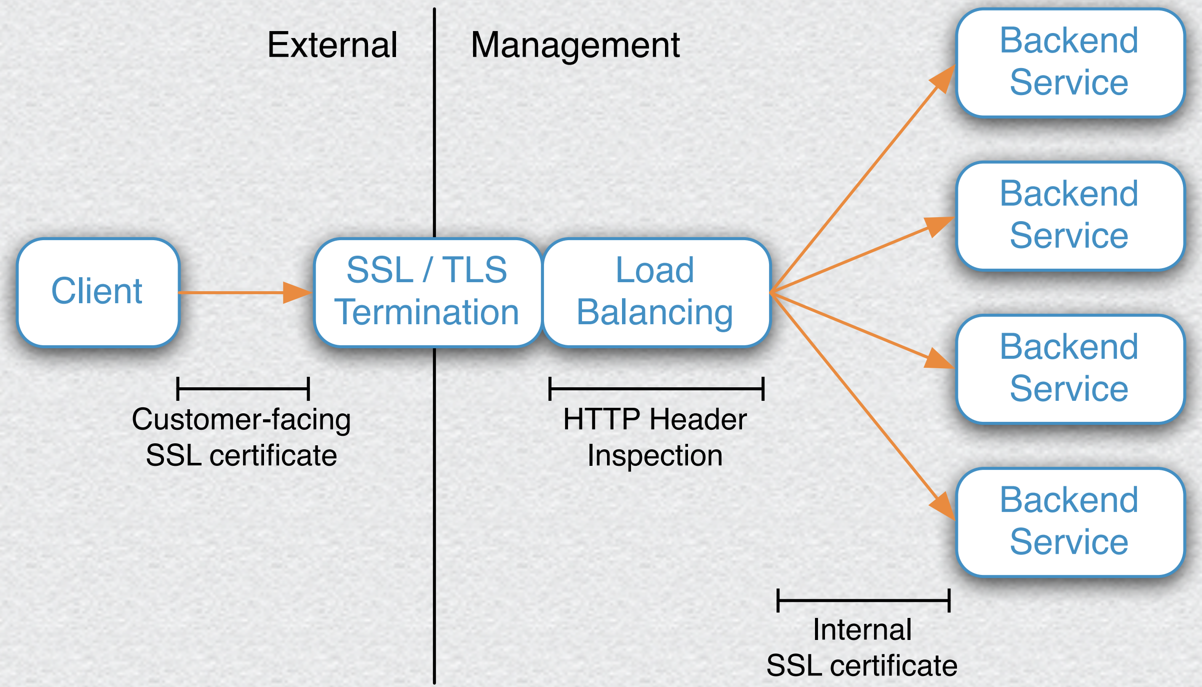
Source: OpenStack Security Guide

Cloud Attack Vectors	Mitigation Strategies
API Endpoints	*Service hardening, mandatory access controls, code audits*
Web Dashboard	*HTTPS, HSTS, CSP, allowed referrers, disable HTTP trace*
Information Leakage	*SSL/TLS, disable memory dedup, random assignments*
VM Breakout	*Service hardening, mandatory access controls, code audits*
Hardware Sharing	*Avoid bare metal instances / device pass-through*
Default Images	*Secure and maintain default images*
Unsecured Instances	*User and/or tenant level network isolation for instances*
Secondary Attacks	*Least privilege, mandatory access controls, strong auth*

Major Security Considerations

- High level architecture has different security domains
- End to end protection of network traffic
- Protected virtualization stack
- Protected API endpoints
- Ability to update easily
- Physical security at the datacenter

Case Study: TLS in the Cloud



External

Management

Client

SSL / TLS Termination

Load Balancing

Backend Service

Backend Service

Backend Service

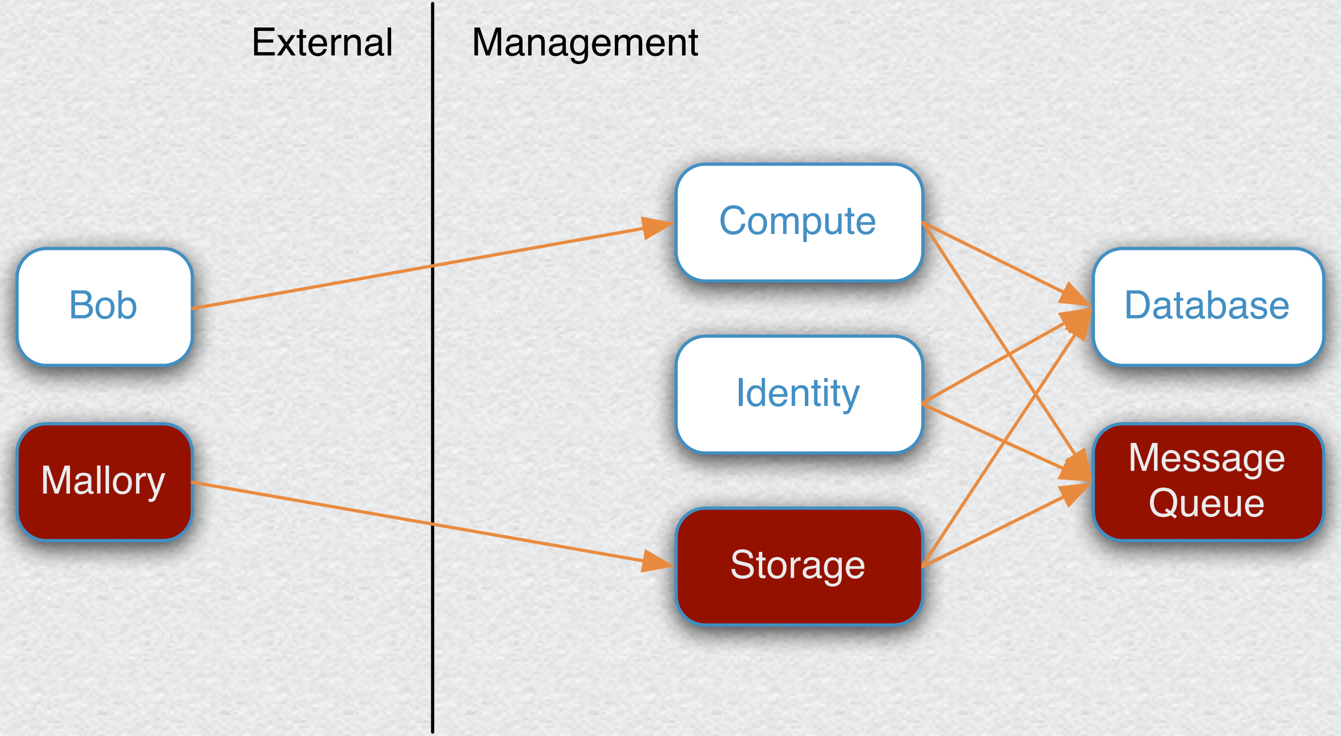
Backend Service

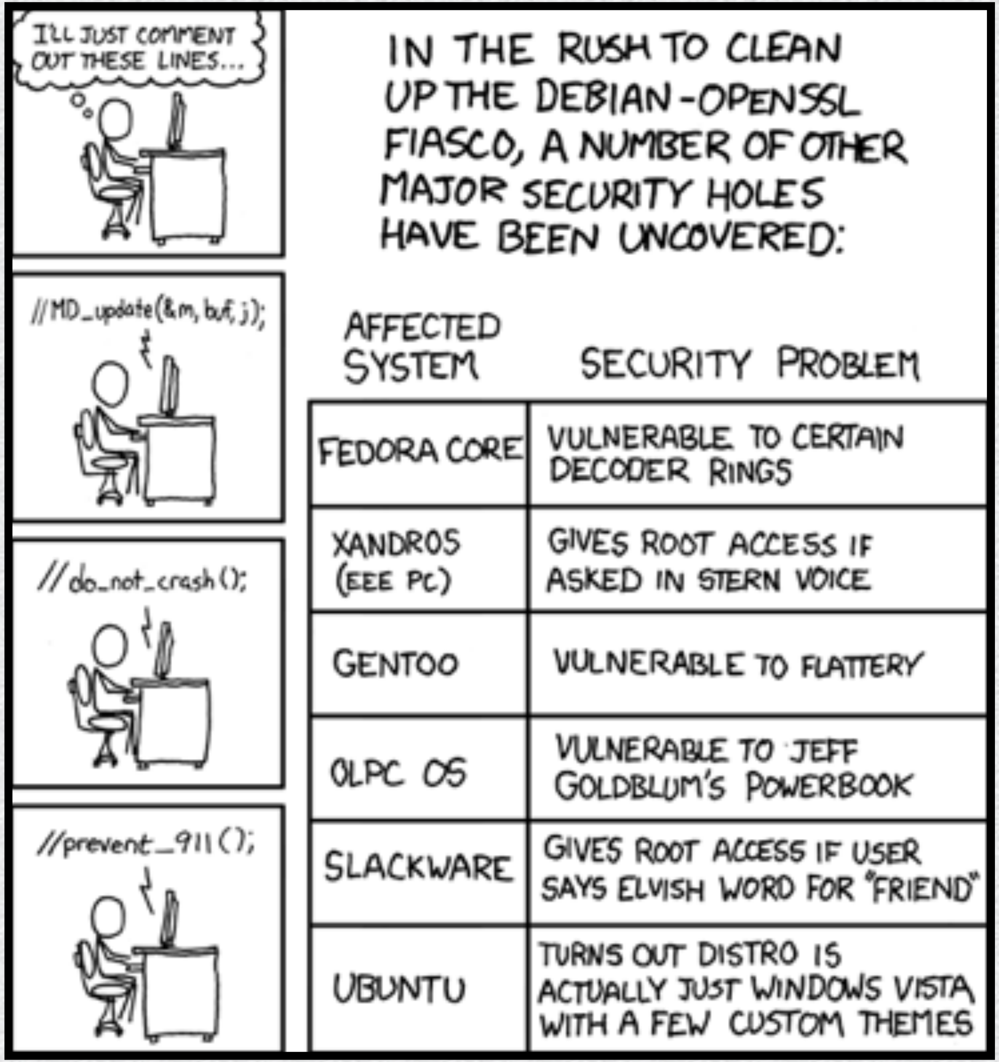
Customer-facing SSL certificate

HTTP Header Inspection

Internal SSL certificate

Case Study: API Endpoint Protection





IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

Source: http://xkcd.com/424/

RSA CONFERENCE 2014

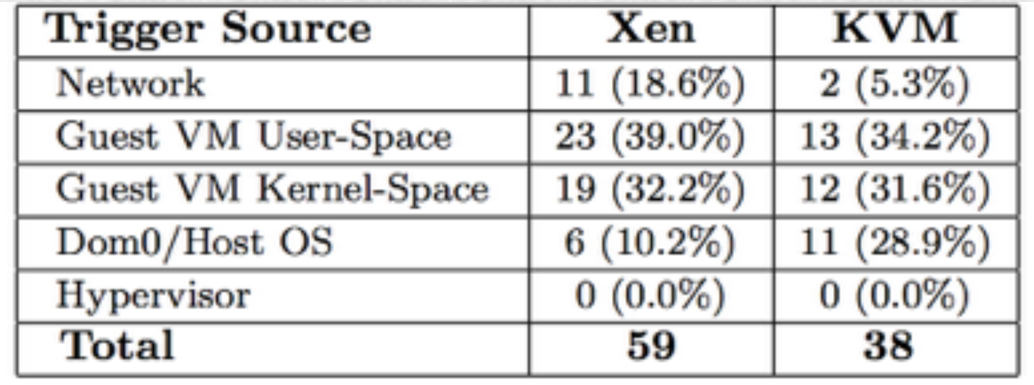
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Securing the Virtualization Stack

What Is The Security Concern?

- Hypervisors have vulnerabilities
- A VM-breakout is among the worst exploits for cloud

Breakdown of Hypervisor Vulnerabilities



Trigger Source	Xen	KVM
Network	11 (18.6%)	2 (5.3%)
Guest VM User-Space	23 (39.0%)	13 (34.2%)
Guest VM Kernel-Space	19 (32.2%)	12 (31.6%)
Dom0/Host OS	6 (10.2%)	11 (28.9%)
Hypervisor	0 (0.0%)	0 (0.0%)
Total	**59**	**38**

From Perez-Botero et al, Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers, In *Proceedings of the Workshop on Security in Cloud Computing (SCC)*, May 2013.

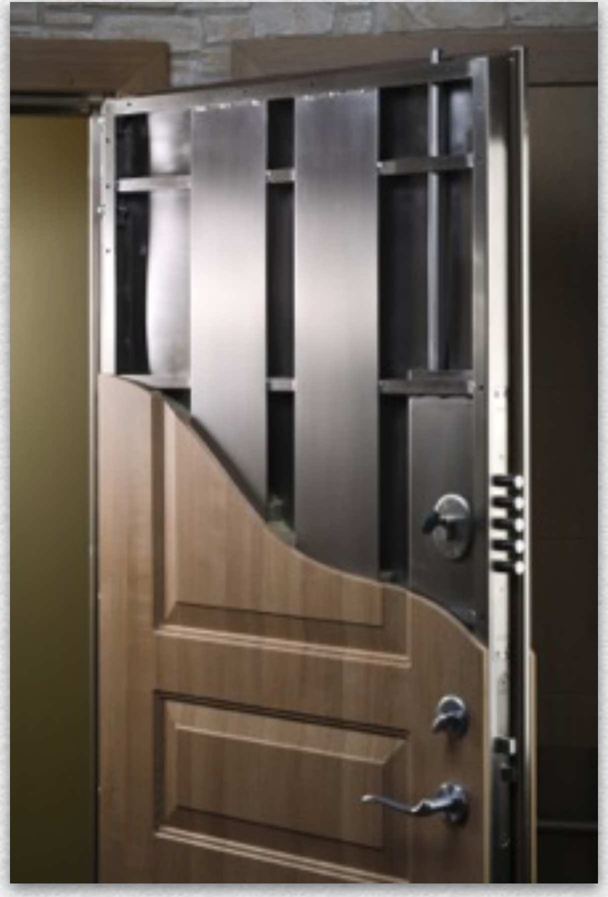
Other Virtualization Considerations

- Bad actors on the control plane
- Hardware emulation, entropy considerations for VM
- Side channel cache attacks

Mitigation Strategies

- Mandatory access controls (KVM+SVirt & Xen+XSM)
- Minimize & harden QEMU software stack
- Runtime monitoring
- Security updates

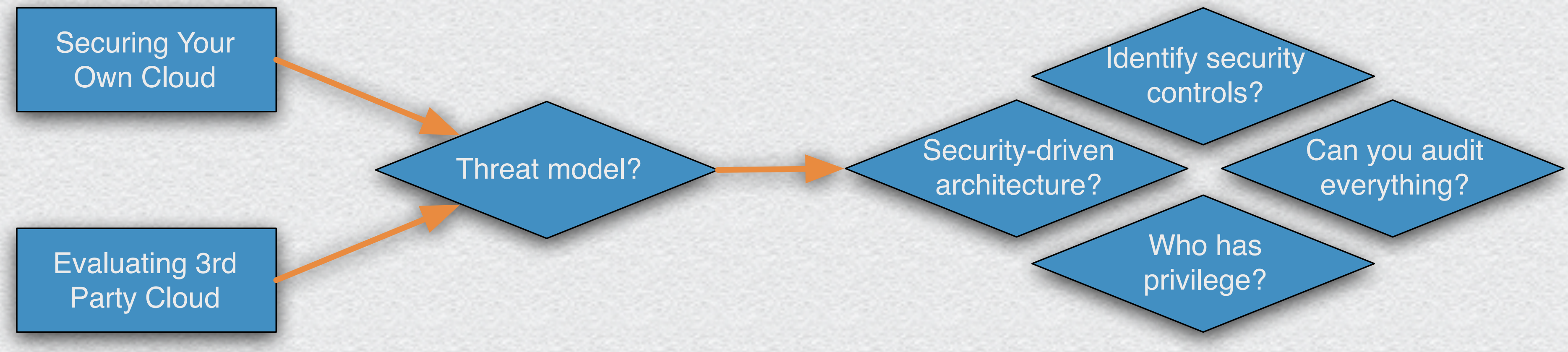
Demo: Layered Security Mitigates Attacks



Questions

Time For Action

Your Next Steps


Securing Your Own Cloud
Evaluating 3rd Party Cloud
Threat model?
Identify security controls?
Security-driven architecture?
Can you audit everything?
Who has privilege?

Bryan D. Payne

http://www.bryanpayne.org