Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)

Lee Badger
Tim Grance

May. 20, 2010

Outline

1. Brief review of clouds, and introduction to SAJACC. (15 minutes)
2. Security issues in the cloud. (15 minutes)
3. Preliminary Cloud Computing Use Cases. (20 minutes)
4. Questions! (10 minutes)

more feedback?

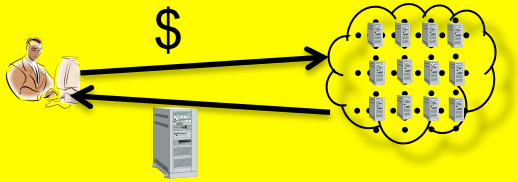
Note: Any mention of a vendor or product is NOT an endorsement or recommendation.

1 Brief review of clouds, and introduction to SAJACC

NIST Working Cloud Definition (1 of 3)

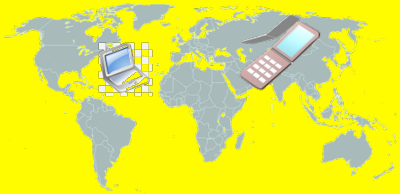
5 Key Characteristics

1 On-demand self service



renting takes minutes

2 Ubiquitous network access

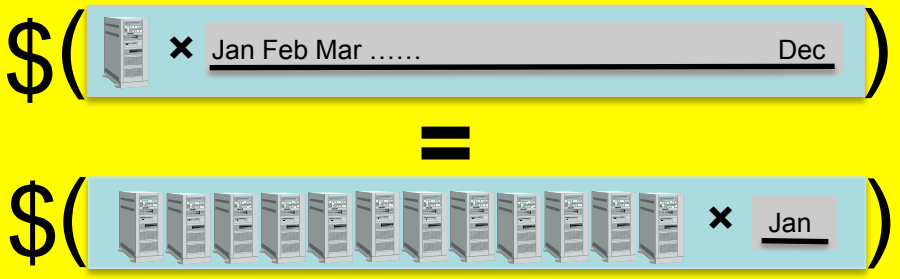


anywhere / any device

3 Metered use

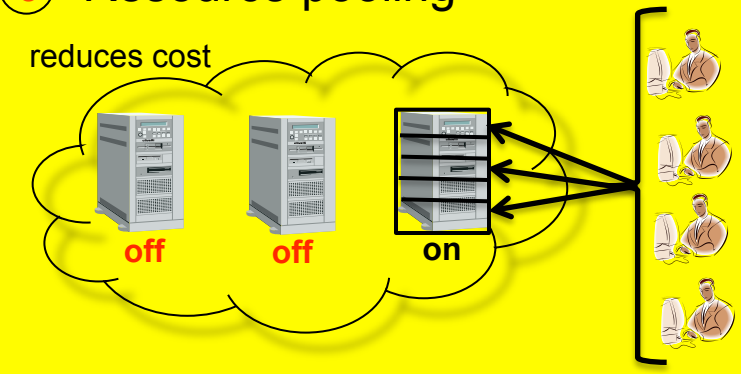
conserve resources

4 Elasticity



rent it in any quantity

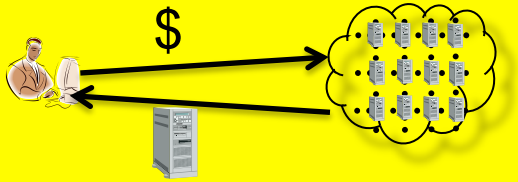
5 Resource pooling



NIST Working Cloud Definition (1 of 3)

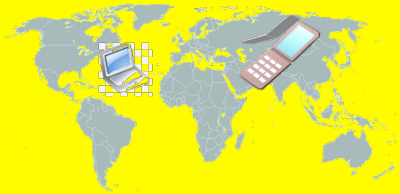
5 Key Characteristics

1 On-demand self service



renting takes minutes

2 Ubiquitous network access



anywhere / any device

3 Metered use

=

conserve resources

4 Elasticity

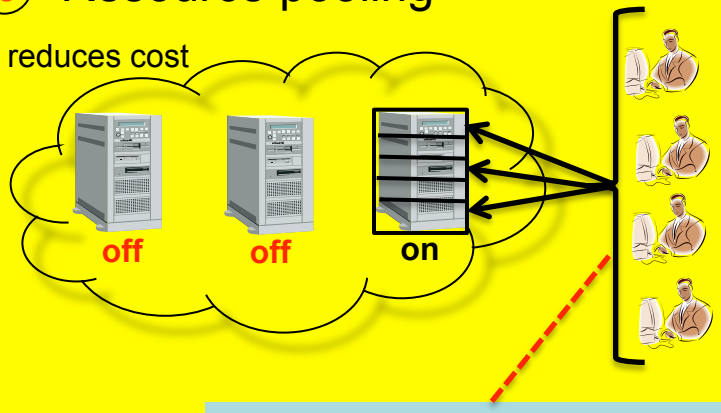
$(× Jan Feb Mar …… Dec)

=

$(× Jan)

rent it in any quantity

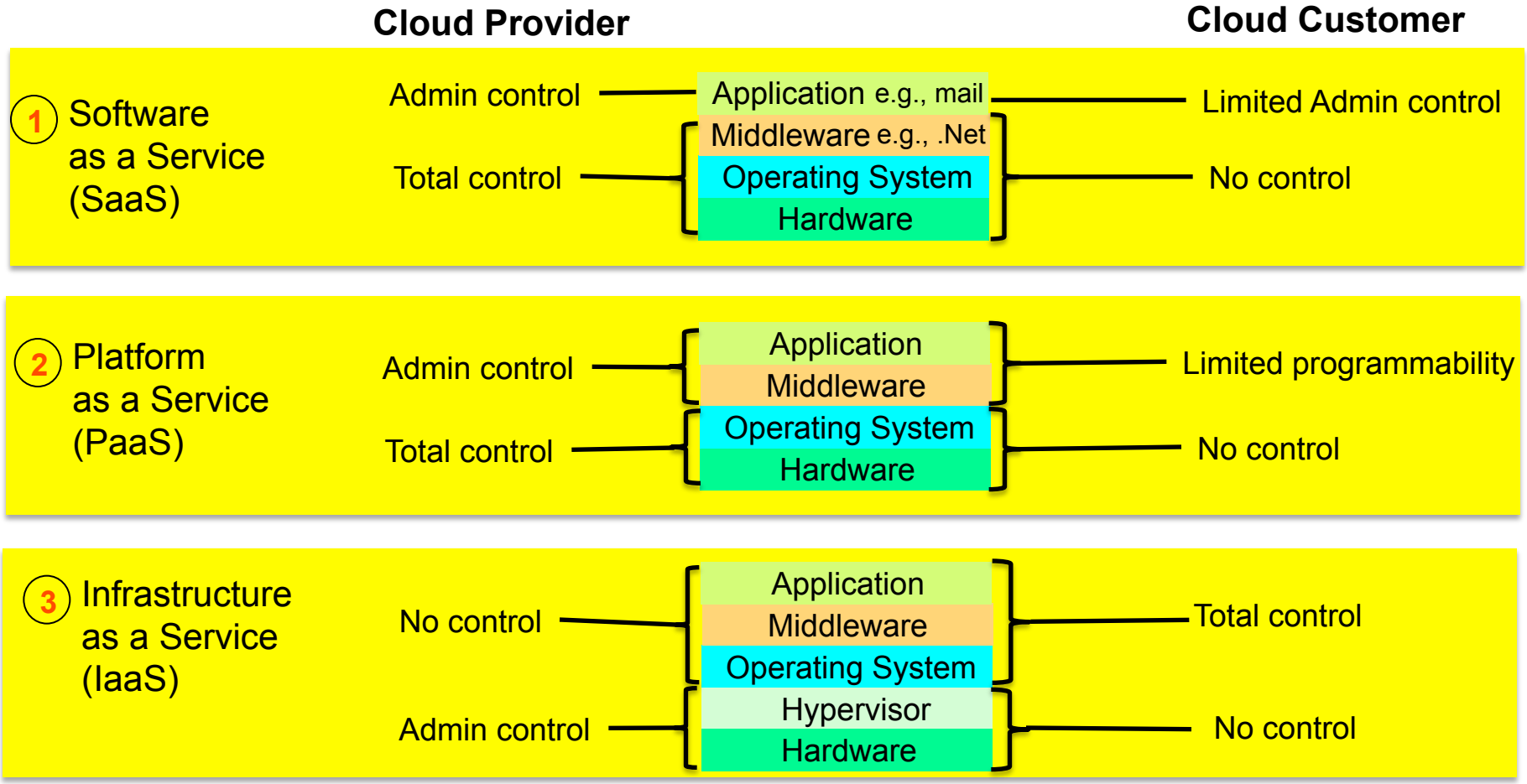
5 Resource pooling



where is my workload?

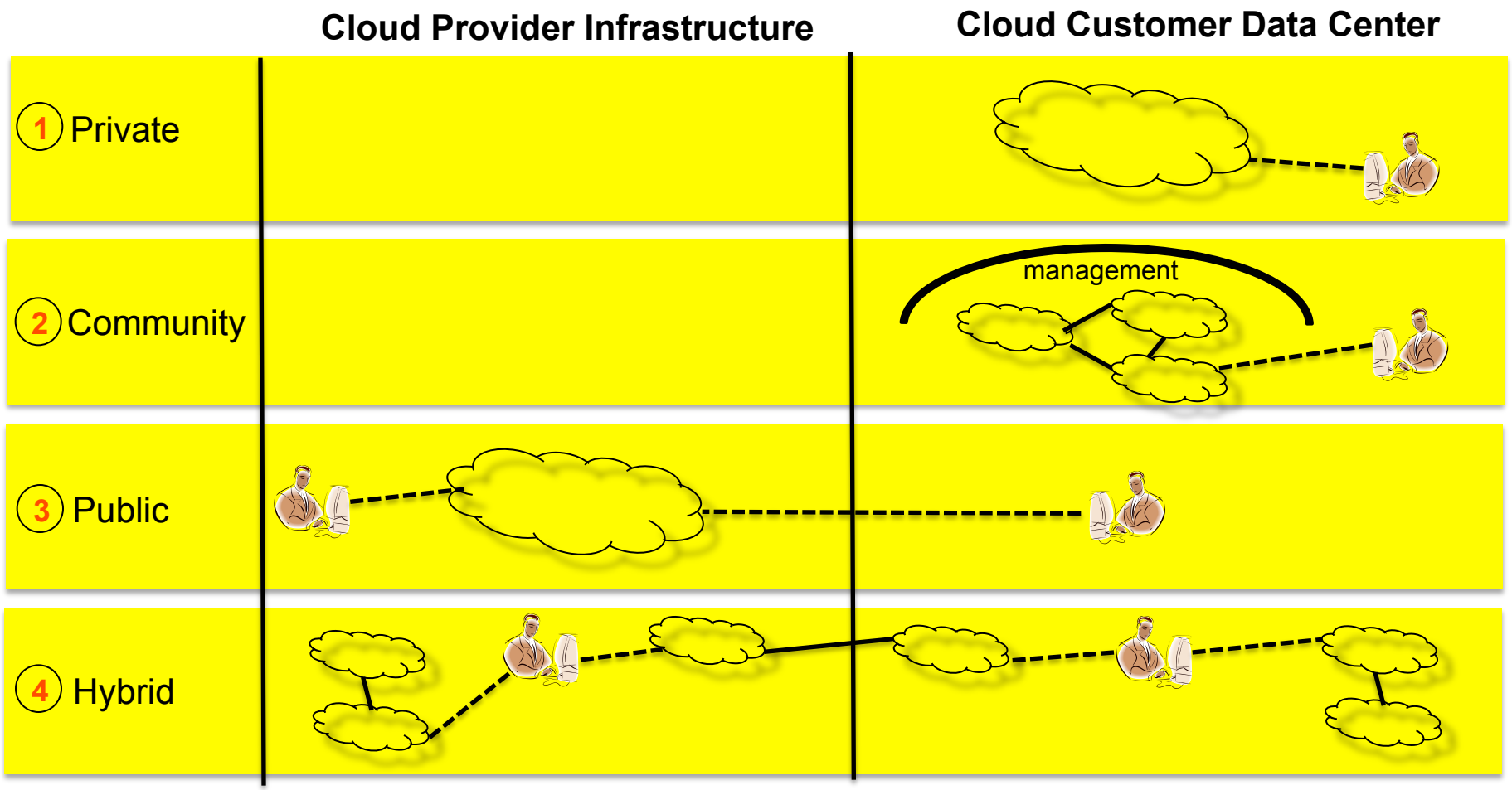
NIST Working Cloud Definition (2 of 3)

3 Deployment Models

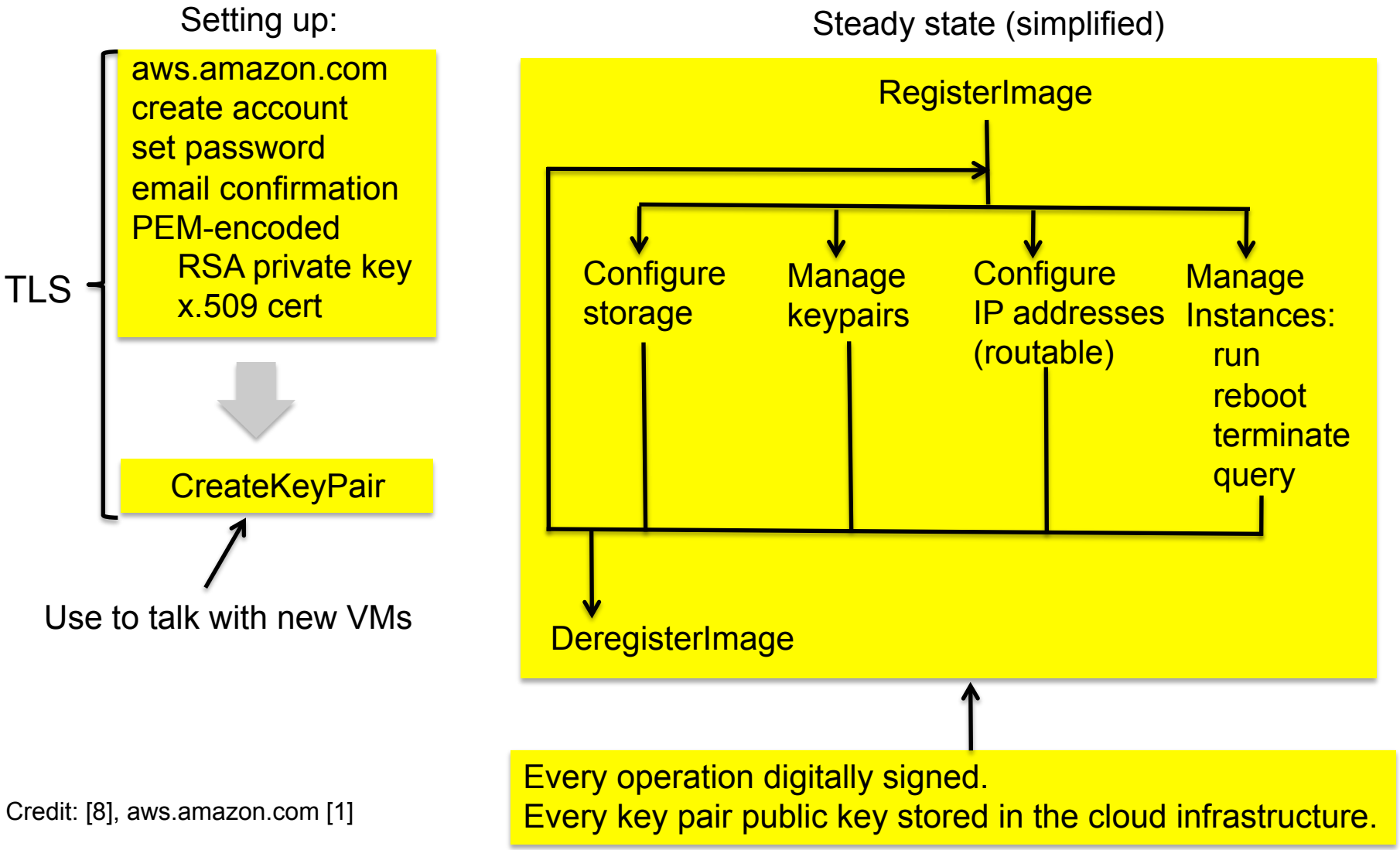


NIST Working Cloud Definition (3 of 3)

4 Delivery Models



A Quick Trip Through the (simplified) API



Credit: [8], aws.amazon.com [1]

Important Cloud Computing Requirements

- **interoperability:** clouds work together
- **portability:** workloads can move around
- **security:** customer workloads protected (to the extent possible)

- Well-formulated standards could help, but…

Standards Creation is Time Consuming

- Critical features (interoperability, portability) *require* high quality, mature standards.
- **But** standards development is a **consensus-oriented** process: often years to complete.
- Even longer for international standards.

Shorter Term Standards Effort

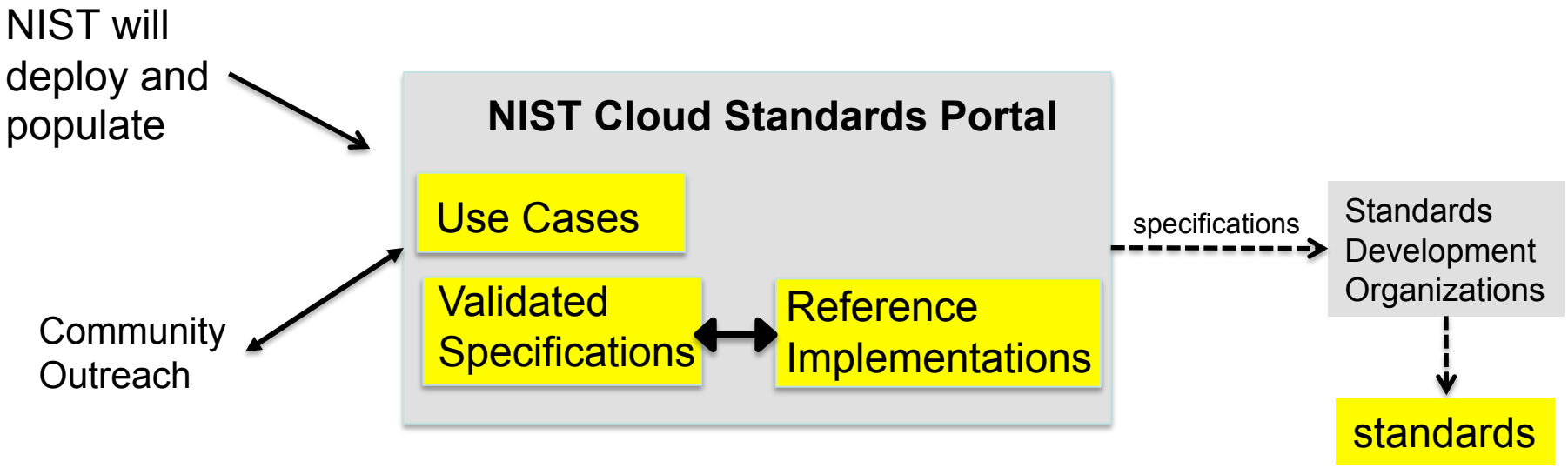
- Until standards mature:
- What is needed is a **process** to test important cloud system requirements --- NIST will provide that.

SAJACC

Portable
Interoperable
Secure (as possible)

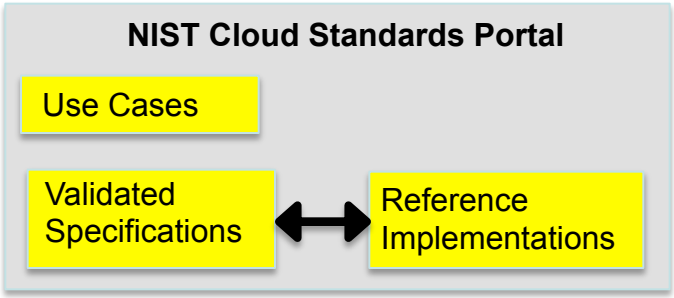
Standards **A**cceleration **J**umpstarting **A**doption of **C**loud **C**omputing

SAJACC Communication Strategy



- Populate a web portal that distributes cloud specifications and reference implementations that are:
  - **Known to work** for critical use cases (e.g., interoperability, portability, bulk data transfer).
  - Can be **easily used** by cloud service providers and consumers.
  - Provide a basis for innovation i.e. are **extensible**.
    - Enables future innovation.

Populating the Portal



Three complementary activities, all performed in collaboration with other agencies and standards development organizations:

(1) **NIST inserts** existing standards and de-facto interfaces as specifications.

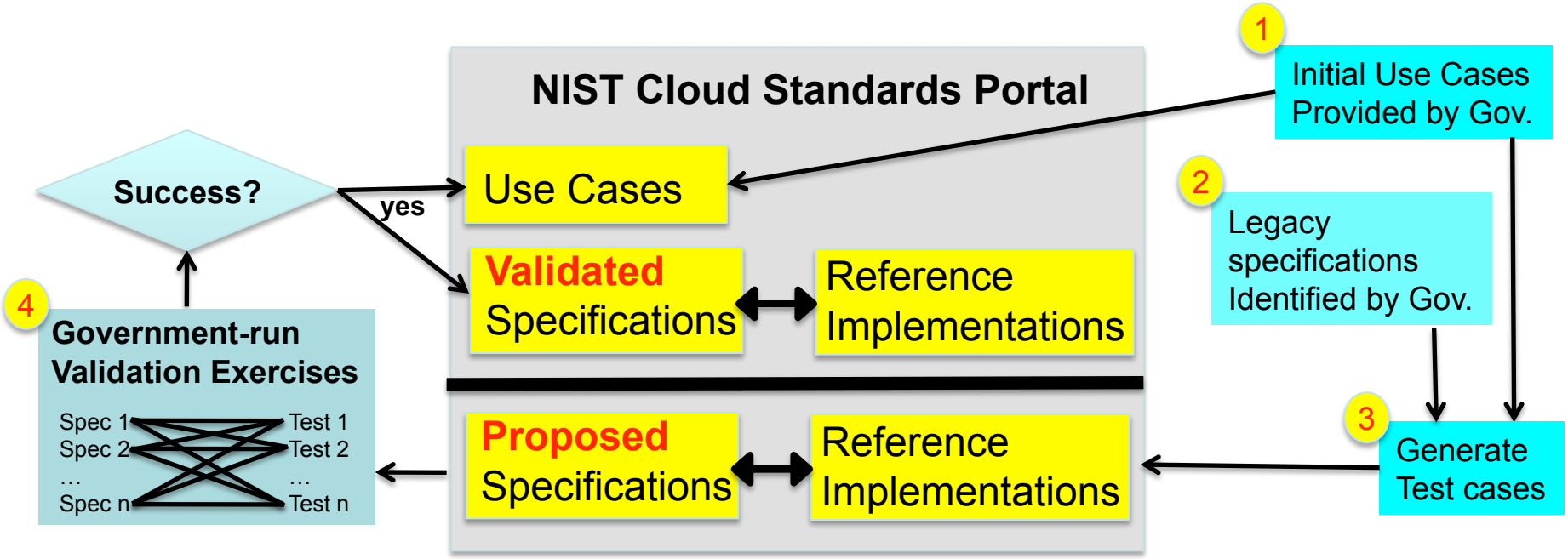
- NIST identifies and validates specifications using use cases.

(2) **Organizations contribute** open specifications.

- NIST receives and coordinates the prioritization of specifications, and validates using use cases.

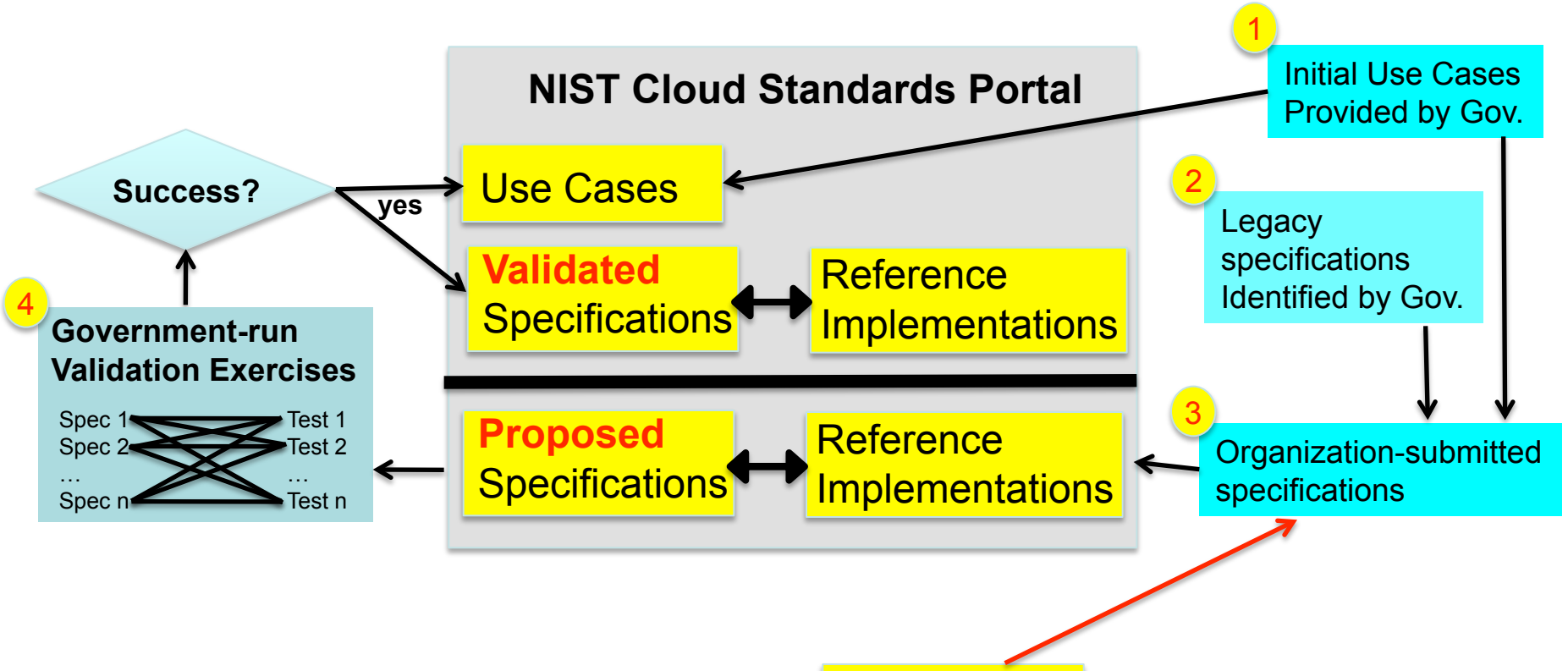
(3) **NIST identifies gaps** in cloud standards (and specifications) and publishes the gaps on the portal: produces opportunity for outside organizations to fill them.

(1) NIST Inserts Existing Standards and De-facto Interfaces



- **specifications, use cases:** provide insight on how clouds can work
- **reference implementations**: enable validation exercises
- **continuously growing portal**: new content added over time
- **publically available**: anyone can access

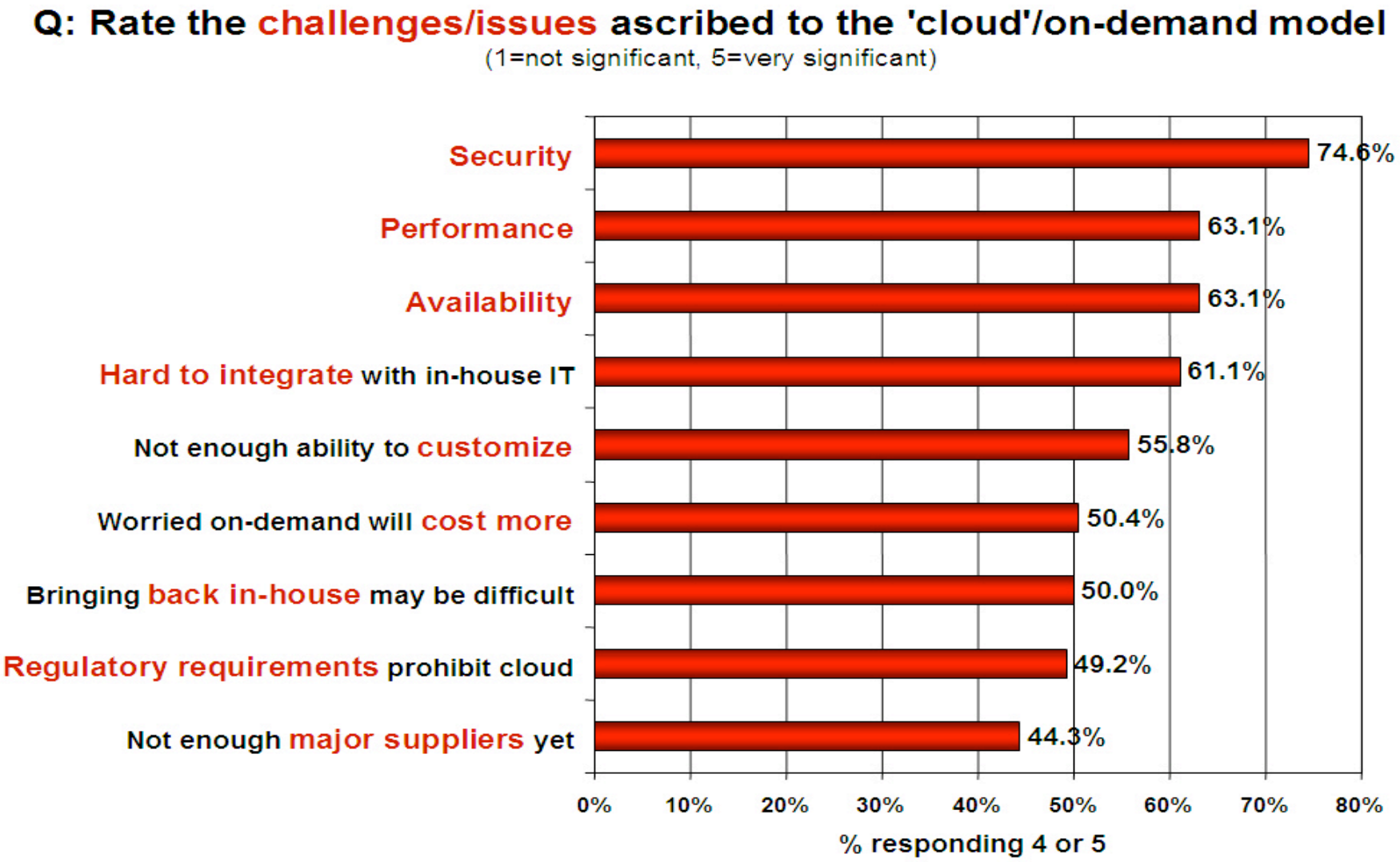
(2) Organizations Contribute Open Specifications



- **continuously growing portal**: new content added over time
- **publically available**: anyone can access or submit

2 Security issues in the cloud.

Security is a Major Issue



Source: IDC Enterprise Panel, August 2008 n=244 [3]

What is Security?

- Traditionally, approximately:
  - **confidentiality**: your data not leaked
  - **integrity**: your data or system not corrupted
  - **availability**: your system keeps running
- What does this mean in the cloud?
  - without user physical control
- Some issues
  - with dynamically changing infrastructure
  - secure access to the cloud
  - protecting different users from one another

Analyzing Cloud Security

- Some key issues:
  - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** that can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
  - There are both advantages and challenges

Former Intel CEO, Andy Grove: “only the paranoid survive”

General Security Advantages

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

General Security Challenges

- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control

Data Storage Services

- Advantages
  - Data fragmentation and dispersal
  - Automated replication
  - Provision of data zones (e.g., by country)
  - Encryption at rest and in transit
  - Automated data retention
- Challenges
  - Isolation management / data multi-tenancy
  - Storage controller
    - Single point of failure / compromise?
  - Exposure of data

Cloud Processing Infrastructure

- Advantages
  - Ability to secure masters and push out secure images
- Challenges
  - Application multi-tenancy
  - Reliance on hypervisors
  - Process isolation / Application sandboxes

Additional Issues

- Issues with moving sensitive data to the cloud
  - Privacy impact assessments
- Risk assessment
  - Contingency planning and disaster recovery for cloud implementations
  - Using SLAs to obtain cloud security
    - Suggested requirements for cloud SLAs
    - Issues with cloud forensics
- Handling compliance
  - FISMA
  - HIPAA
  - SOX
  - PCI
  - SAS 70 Audits

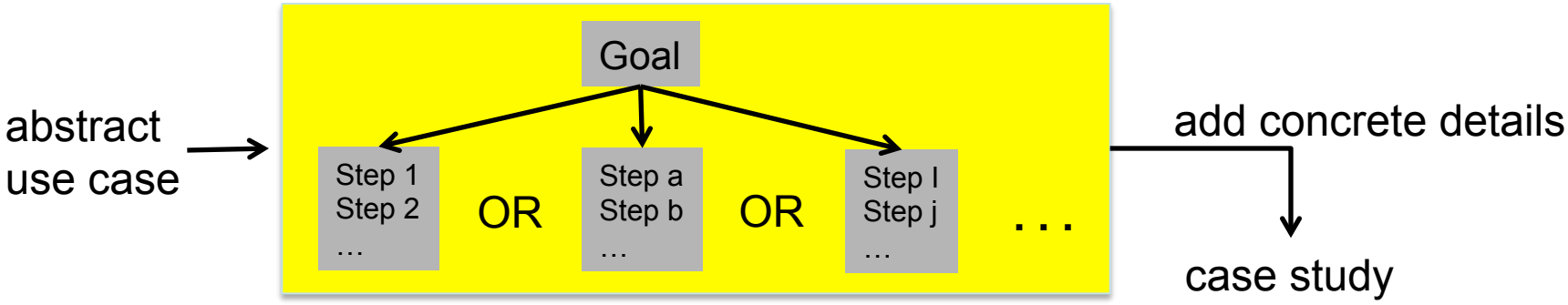
Putting it Together

- Most clouds will require very strong security controls
- All models of cloud may be used for differing tradeoffs between threat exposure and efficiency
- There is no one “cloud”. There are many models and architectures.
- How does one choose?

3 Use Cases to drive portability, interoperability, security in clouds

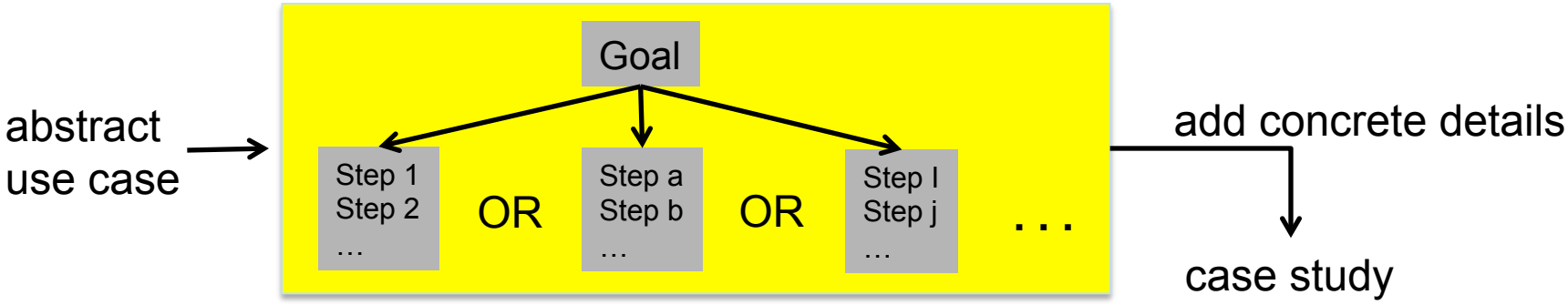
Use Cases

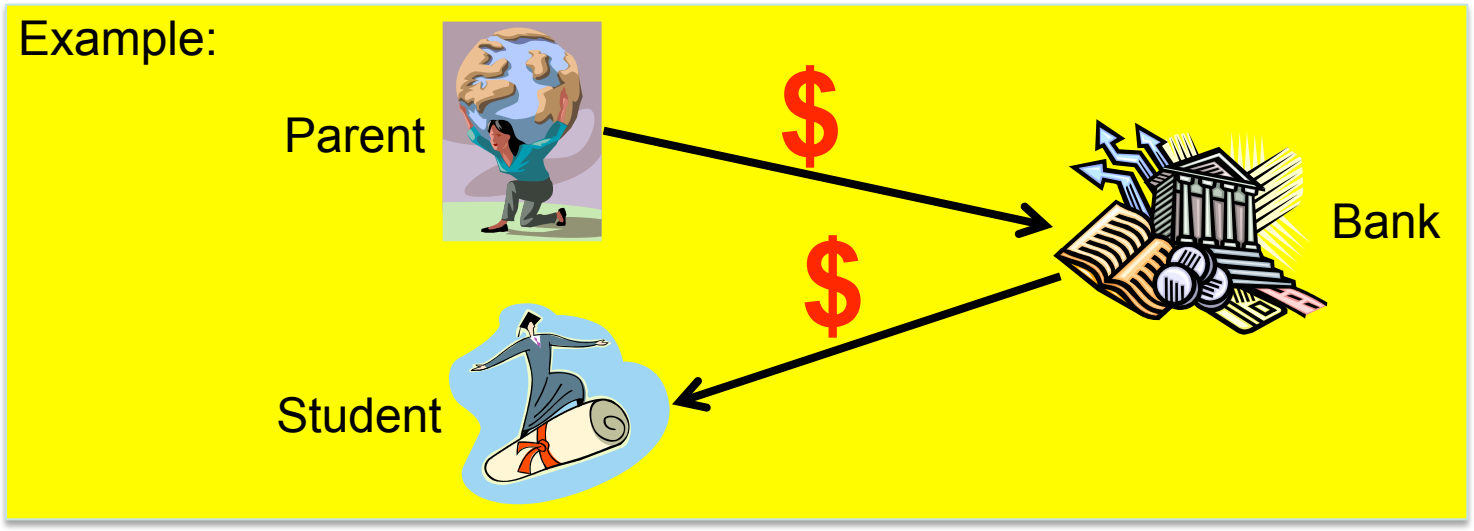
Use Case: a description of how groups of users and their resources may interact with one or more systems to achieve specific goals.



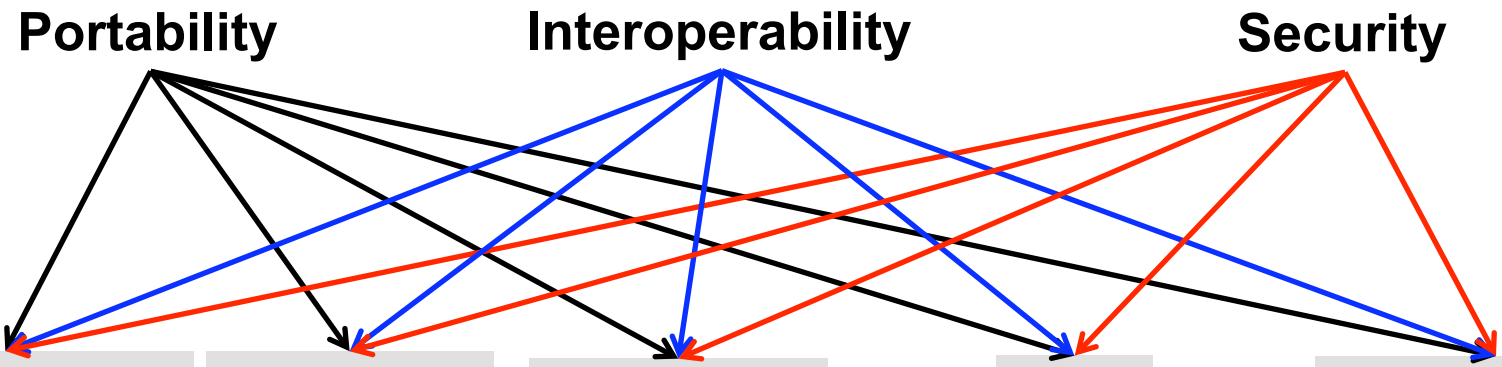
Use Cases

Use Case: a description of how groups of users and their resources may interact with one or more cloud computing systems to achieve specific goals.





Preliminary Use Case Taxonomy for a Public Cloud (focus on IaaS)



File/Object System Like

- sharing access
- access by name
- access by pattern
- strong erase
- cloud drive[7]
  - synchronization

Job Control & Programming

- alloc/start/stop…[1]
- queueing[1]
- horizontal scaling of data/ processing
- services

Cloud-2-Cloud

- inter-cloud data transfer
- multi-hop data transfer
- storage peering[7]
- backup between clouds[7]
- cloud broker[4]
- cloud burst
- VM migration
- dynamic dispatch[5]
- fault-tolerant group

Admin

- SLA comparison
- info discovery[7]
- user Acct mgmt
- compliance[4]
- special security[4]

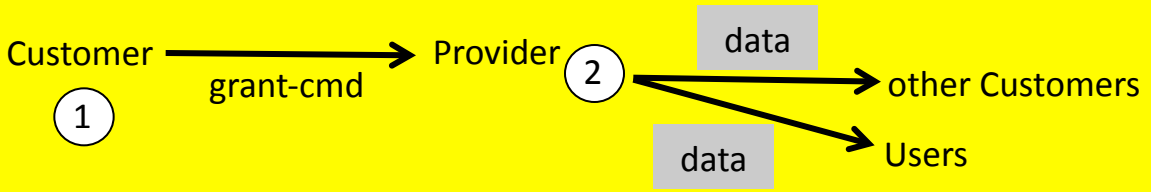
Data Management

- transfer data in
- transfer data out
- backup to cloud[7]
- restore from cloud[7]
- archive/preservation to cloud[7]

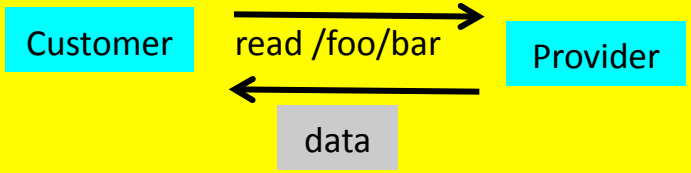
Note: these use cases are preliminary.
Credits: SNIA [7], aws.amazon.com [1], DMTF [4], libcloud [5]

File/Object System Like

Sharing access

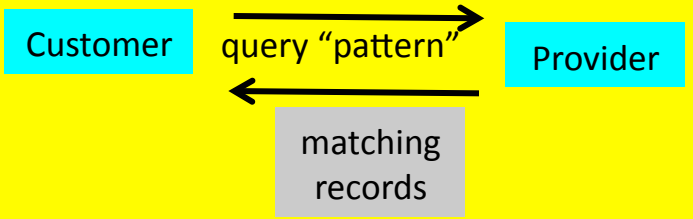


Access by name



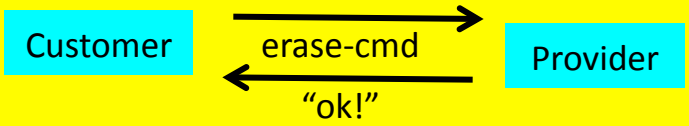
Compatible modes: read, write, append, truncate, chown, chmod, chgrp, …

Access by pattern



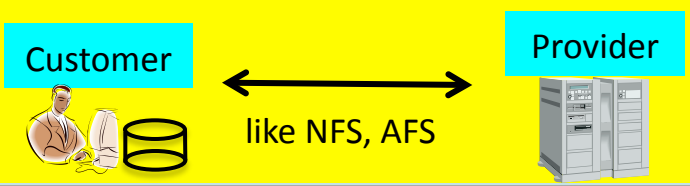
Specifying patterns, records. Access control?

Strong erase



Getting confidence? Zero out, multi-pass? DoD 5220-22?

Cloud Drive

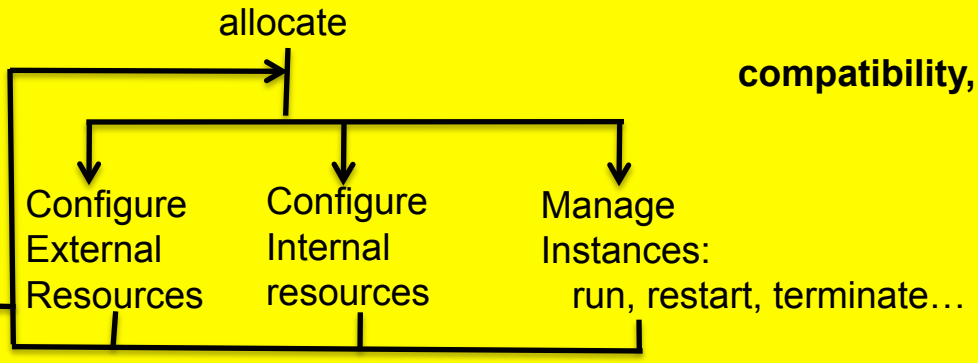


Looks like a local disk Synchronization? Security defaults?

credit: SNIA [7]

Job Control and Programming

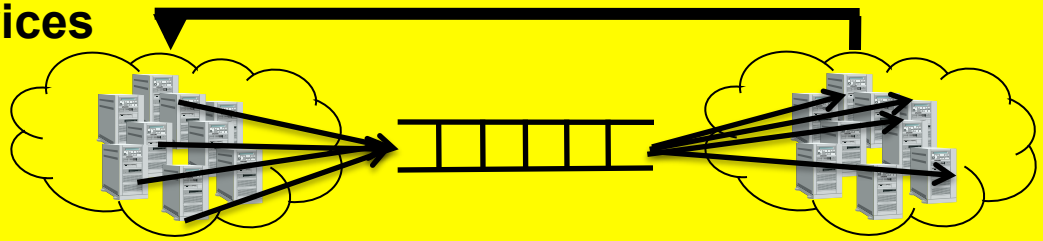
Alloc/start/stop



compatibility, portability…

credit: aws.amazon.com [1]

Queue services



(thread synchronization in the large)

compatibility, portability…

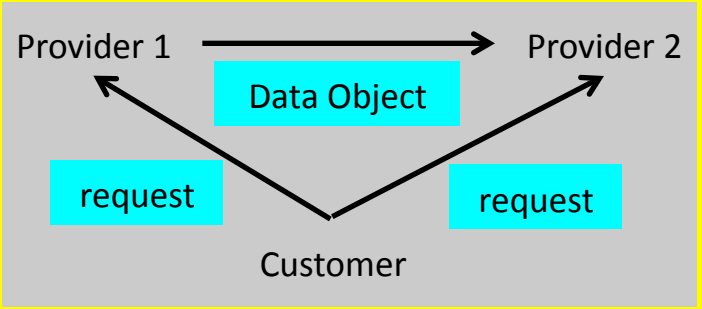
credit: aws.amazon.com [1]

Services

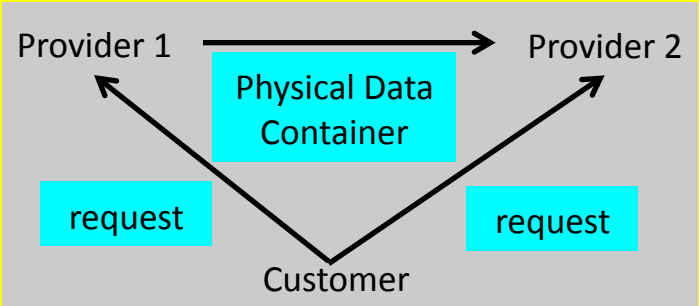
like ordinary hosting, but with more scale, less location awareness.

Cloud-2-Cloud

Inter-cloud data transfer



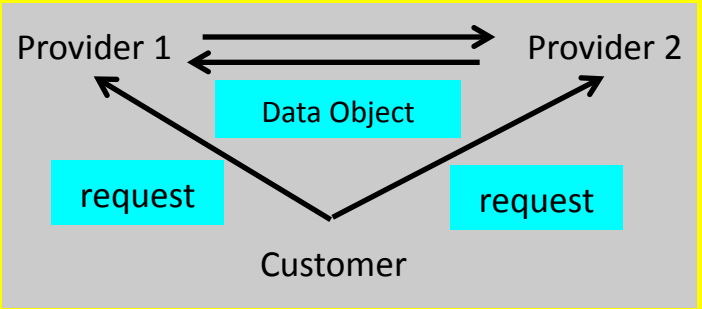
Network Scenario



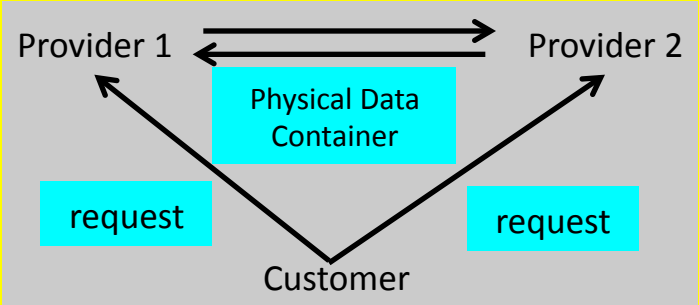
Physical Scenario

some issues:
- **protection of data in transit**
- **verification of data received**
- **coherent naming**
- **compatible crypto**
- **compatible access control metadata, ownership**

Multi-hop inter-cloud data transfer



Network Scenario

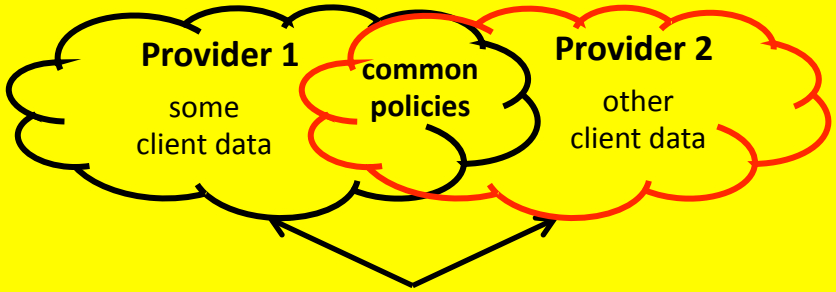


Physical Scenario

same issues, and in addition: after round trip, data is still as useful

Cloud-2-Cloud (2)

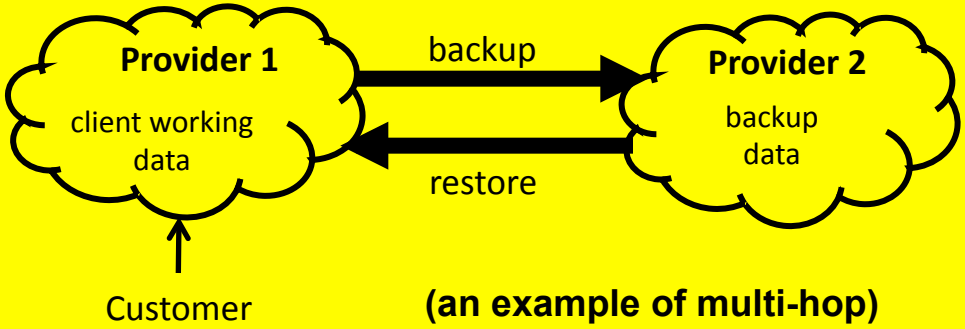
Storage peering



credit: SNIA [7]

need common policies for naming of data objects, access control, snapshot/ cloning, etc.

Backup/restore between clouds

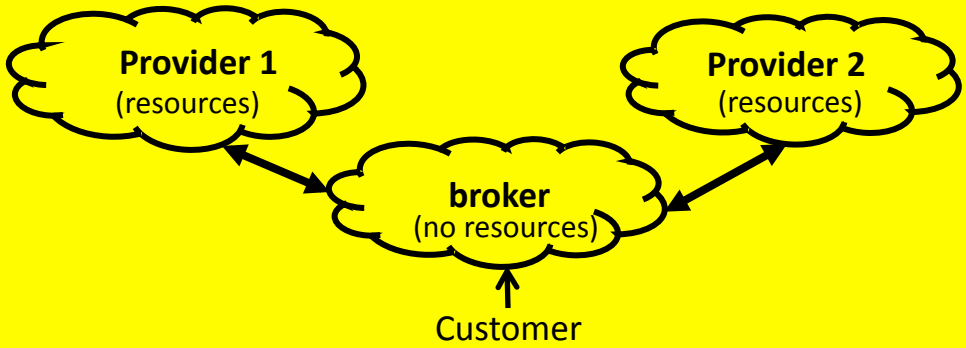


credit: SNIA [7]

(an example of multi-hop)

common archival format, procedures, data protection in transit, verification, key management, …

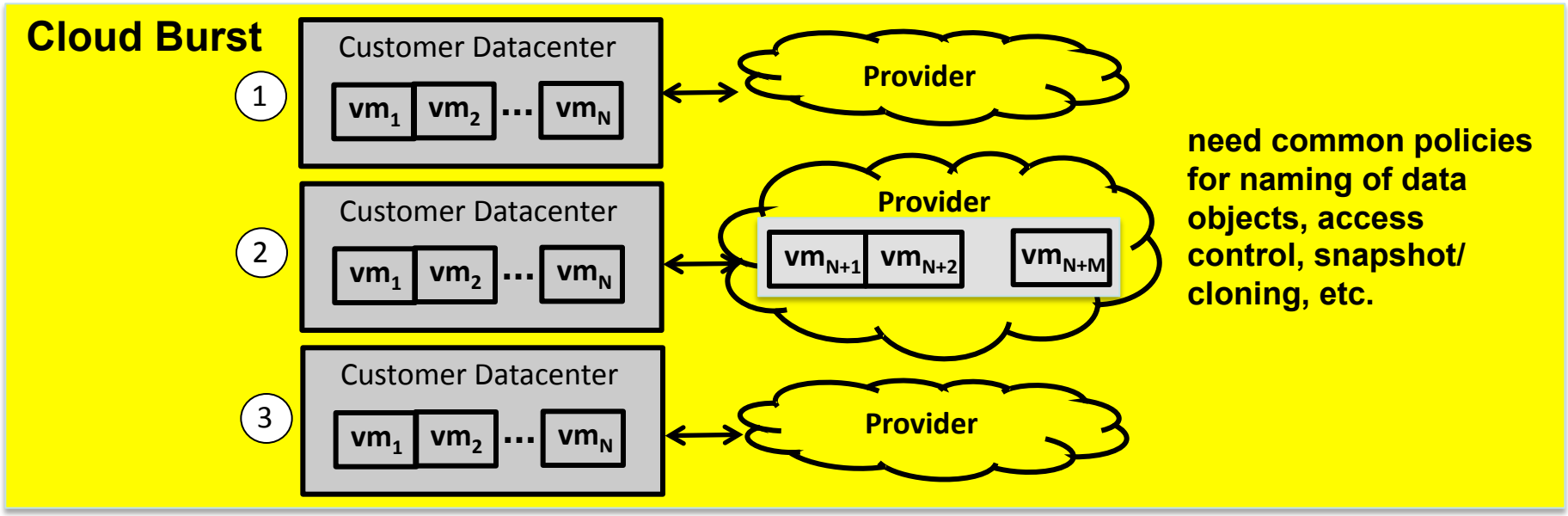
Cloud broker

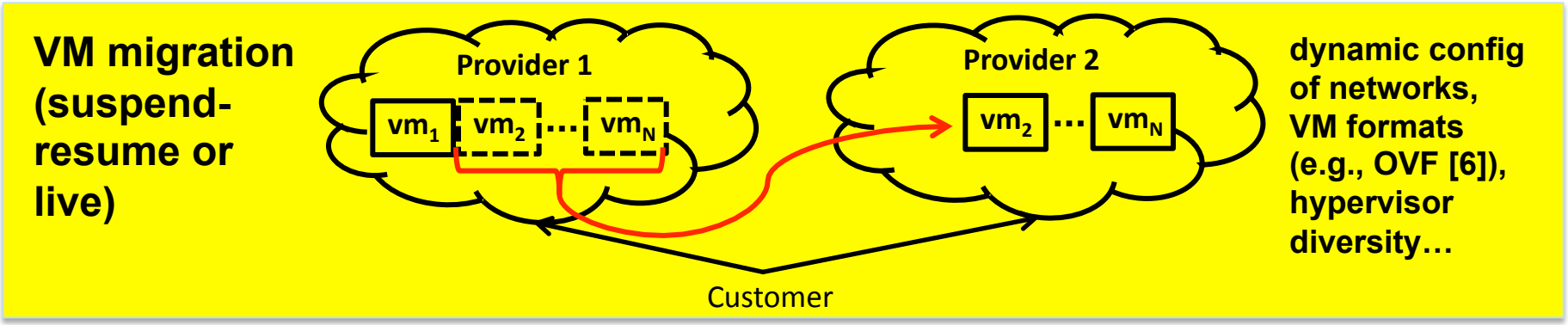


credit: DMTF [4]

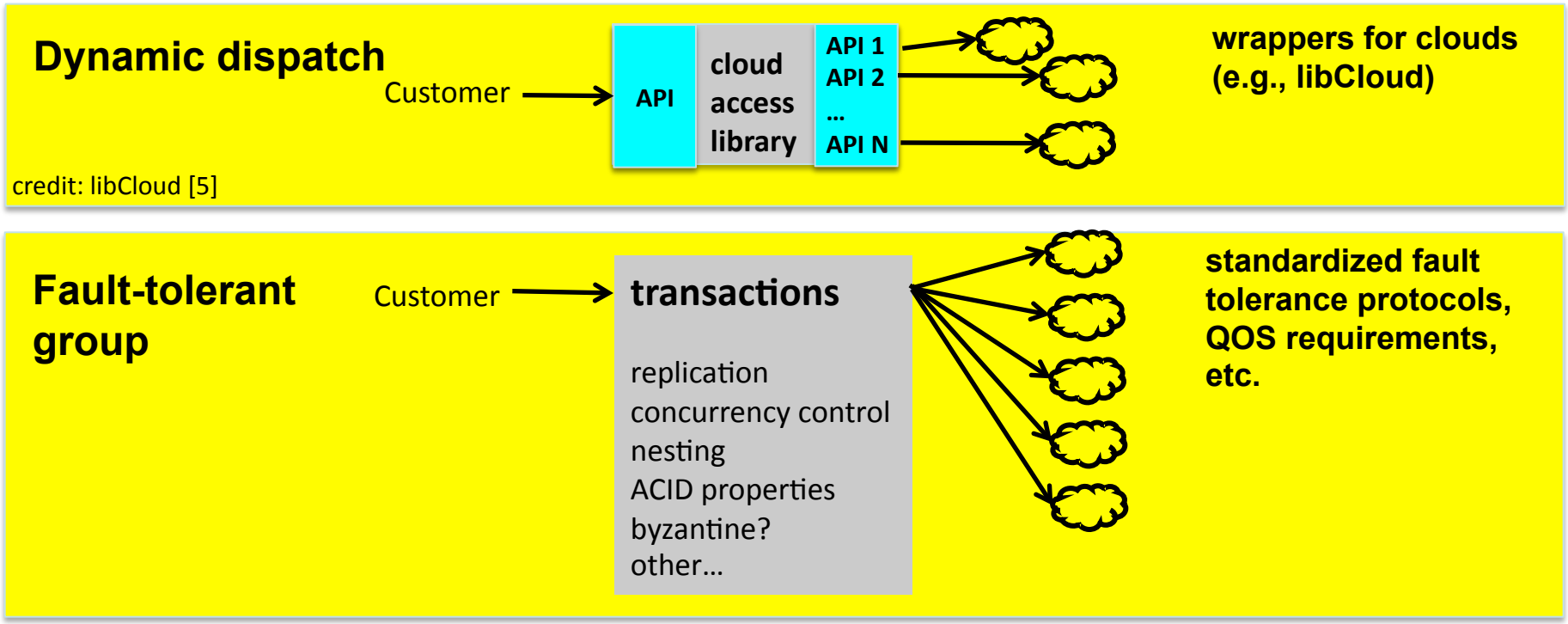
broker could provide a simple or stable interface to customers, even when providers change or have diverse APIs.

Cloud-2-Cloud (3)



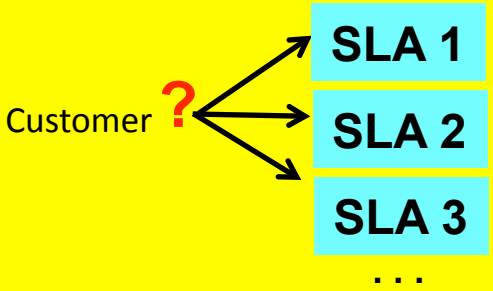


Cloud-2-Cloud (4)



Admin

SLA comparison



An SLA Template?

Cloud Provider Promises

availability
remedies for failure to perform
data preservation
legal care of customer info

Limitations

scheduled outages
force majeure events
changes to the SLA
security
service API changes

User Promises

acceptable use policies
provided software
on-time payment

perhaps as a prelude to more detailed terms that extend but do not contradict?

Info Discovery

A search service that retrieves documents subpoenaed for court.

credit: SNIA [7]

who gets notified?
who bears costs?
timeliness?

User Acct Mgmt

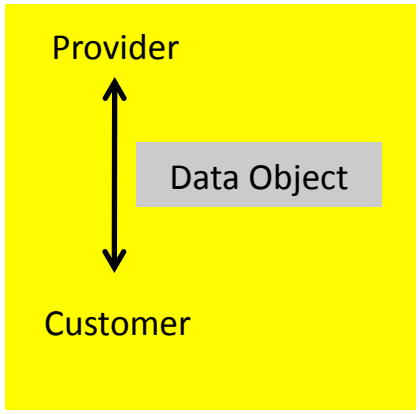
A cloud customer may have his/her own customers, and a provider sometimes provides SaaS-style customer management services.

How to prevent "jar'ing" of customer-customers when providers change?

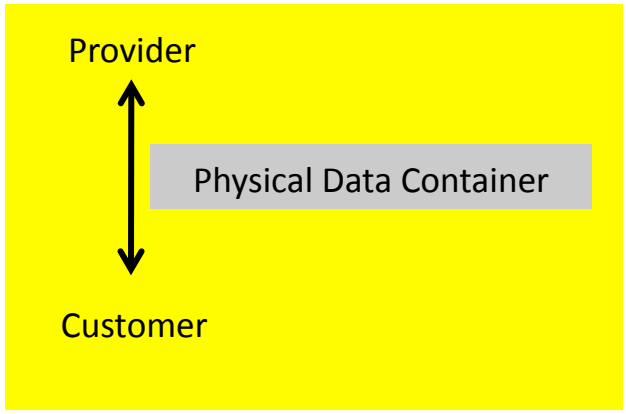
Admin (2)

Compliance credit: DMTF [4]	Providers sometimes assert compliance with (HIPPA, PCI, Sarbanes-Oxley, FISMA) requirements.	**how can customers tell?**
Special Security credit: DMTF [4]	E.g., a “mono-tenancy” requirement for a customer’s workloads.	**how can customers specify and tell?**

Data Management



Network Scenario



Physical Scenario

- transfer data in
- transfer data out
- backup to cloud
- restore from cloud
- archive/preservation to cloud

protection in transit;
verification of correct data received;
correct naming;
initialization of access rules;
…

References

[1] Amazon Web Services, aws.amazon.com.

[2] “Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems”, UCSB Computer Science Technical Report Number 2008-10.

[3] IDC Enterprise Panel, August 2008 n=244

[4] “Interoperable Clouds, A White Paper from the Open Cloud Standards Incubator”, Distributed Management Task Force, Version 1.0, DMTF Informational, Nov. 11, 2009, DSP-IS0101

[5] libcloud, http://incubator.apache.org/libcloud/

[6] “Open Virtualization Format Specification”, DMTF Document Number DSP0243, Version 1.0, Feb. 22, 2009.

[7] “Cloud Storage Use Cases”, Storage Network Industry Association, Version 0.5 rev 0, June 8, 2009.

[8] “Starting Amazon EC2 with Mac OS X”. Robert Sosinski. http://www.robertsosinski.com/2008/01/26/starting-amazon-ec2-with-mac-os-x/

[9] “The Eucalyptus Open-source Cloud-computing System”, D. Nurmi, R. Wolski, C. Grzegorcyk, G. Obertelli, S. Soman, L. Youseff, D. Zagorodnov, in Proceedings of Cloud Computing and Its Applications, Oct. 2008.

[10] “Ubuntu Enterprise Cloud Architecture”, S. Wardley, E. Goyer and N. Barcet, Technical White Paper, 2009, www.canonical.com

Questions?