

AWS
re:Invent

JPL

Bringing Governance to an Existing Cloud at NASA's Jet Propulsion Laboratory

Jonathan Chiang, Matt Derenski – NASA/JPL

November 12-15



Introductions

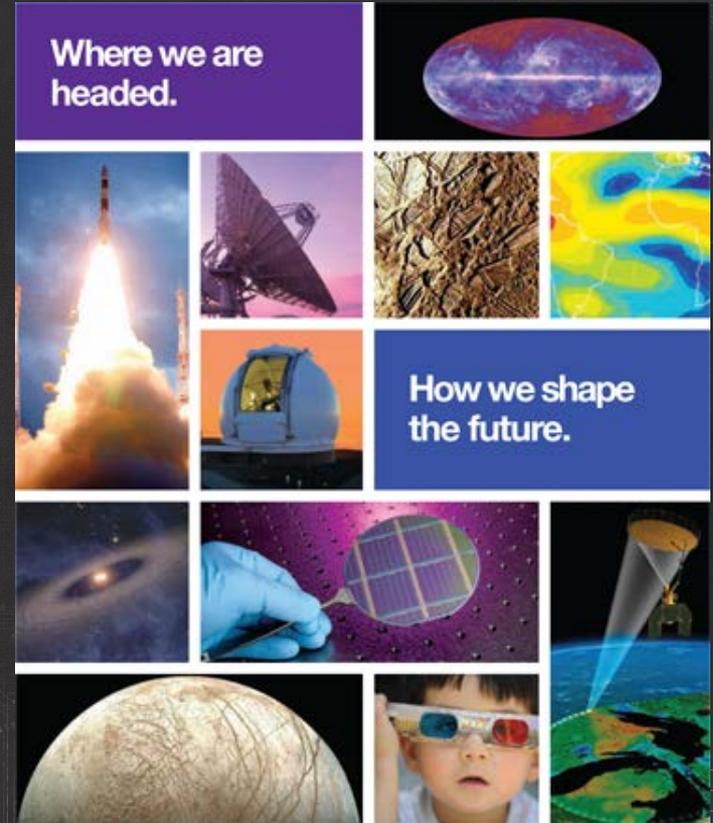
- Jonathan Chiang – IT Chief Engineer
- Matthew Derenski – Cyber Security Engineer

Agenda

- Provide a brief background of JPL
- Understand JPL use cases for AWS
- Describe JPL's early engagement with AWS
- Review JPL's implementation of its governance plan
- Utilizing governance to achieve organizational efficiency
- Measure the value

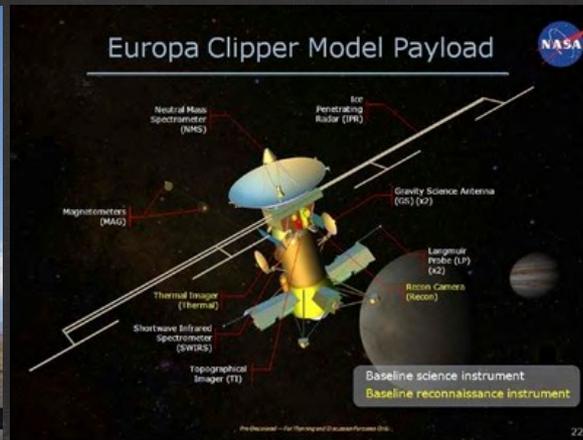
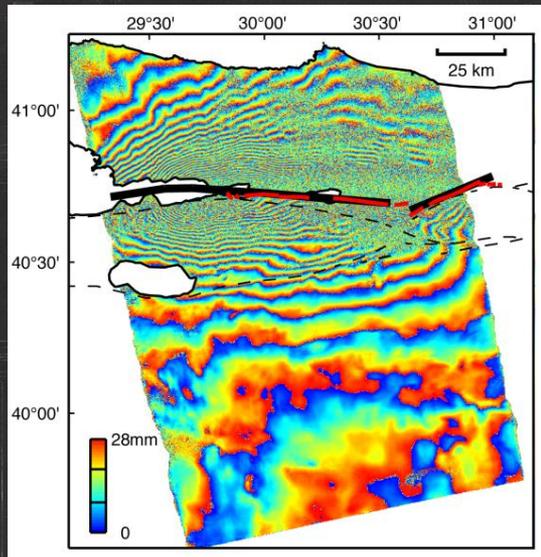
What is JPL?

- We are a Federally Funded Research and Development Center (FFRDC) managed by Caltech
- We have 21 spacecraft and 9 instruments conducting active missions
- We manage NASA's Deep Space Network (DSN)
- We “dare mighty things”



How JPL uses AWS

HPC/Data Processing



CARVE
Carbon in Arctic Reservoirs Vulnerability Experiment

How JPL uses AWS

Public Outreach

EYES ON THE SOLAR SYSTEM

"Eyes on the Solar System" is a 3-D environment full of real NASA mission data. Explore the cosmos from your computer. Hop on an asteroid, fly with NASA's Voyager spacecraft. See the entire solar system moving in real time. It's up to you. You control space and time.

Explore the Solar System **Launch**

- Voyager Interstellar
- Curiosity Landing
- Radioisotope Power
- Mission Juno

Watch the intro to get started and the video tutorials to become an expert at using "Eyes..."

Intro Tutorials

credits • feedback • follow @eyes_eye •
Thanks with love! To a great download session at "Eyes..."

Mars Exploration Program

Mars.jpl.nasa.gov

Eyes on the Solar System

Eyes.jpl.nasa.gov

Night Sky Network

Nightsky.jpl.nasa.gov

Jet Propulsion Laboratory
California Institute of Technology

Night Sky Network
Astronomy Clubs bringing the wonders of the universe to the public

Network Home Find Events Find Clubs Astronomy Activities Night Sky Planner Amateur Resources Join the Network FAQ About the Network

Event Held Since 2004: **25251** People Reached: **2640772**

LADEE Launch Day: September 6
(Updated with footage of the launch) LADEE is about to start its voyage to the moon-and there are many events to check out to celebrate. Read More...

Go Starazing! Astronomy Activities Night Sky Planner See the Stars in the Network

Shywatcher's Guide to the Moon
Use this Moon Map Guide to identify features on the Moon and find out where the astronauts landed!

Your one-stop planning resource for astronomy events.

- Look up sunset and moonrise times
- Find out what's up on the Celestial Calendar

See ALL the Stars!

- Island County Astronomical Society
- Central Florida Astronomical Society, Inc.
- Southern Maine Astronomers

Mars Exploration Program

HOME PROGRAM & MISSIONS ALL ABOUT MARS NEWS MULTIMEDIA PARTICIPATE SEARCH

Science Team Outlines Goals For NASA's 2020 Mars Rover - 07/09/2013

The rover NASA will send to Mars in 2020 should look for signs of past life, collect samples for possible future return to Earth, and demonstrate technology for future human exploration of the Red Planet, according to a report provided to the agency.

What's New?

Click to see highlights

FAVORITES

- Mars Odyssey
- Mars Exploration Rovers
- Mars Curiosity
- Mars Science Laboratory MAVEN

SEND YOUR NAME AND MESSAGE TO MARS CAMPAIGN

335 20 : 48 : 8
Time on Mars

How JPL uses AWS

Storage, Backup, and Disaster Recovery

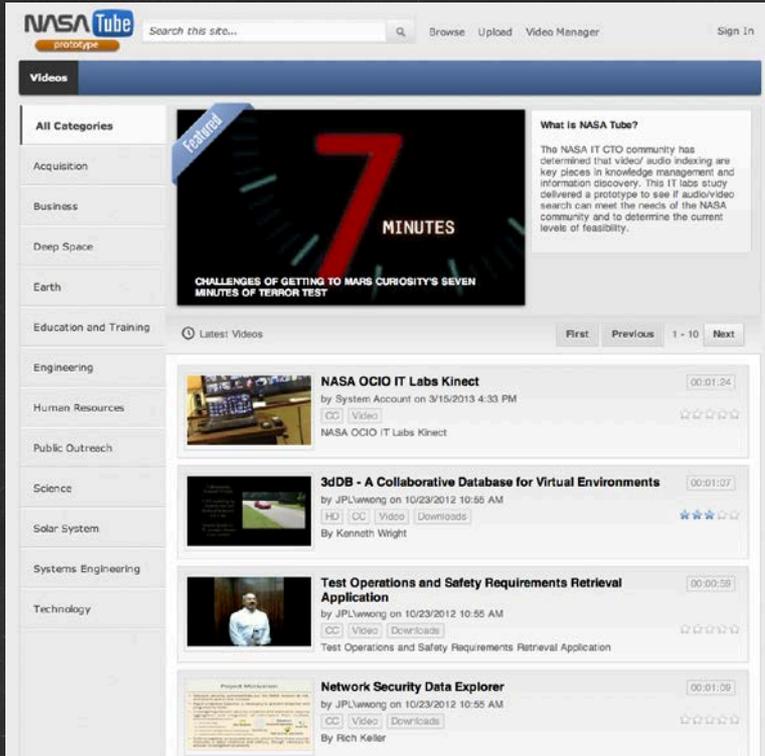


Mars Exploration Rovers

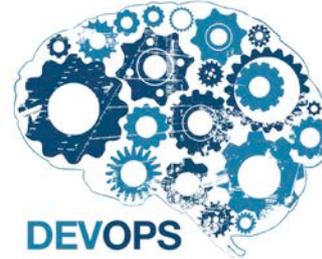


Station Fires

How JPL uses AWS Collaboration



Rapid Development



Enterprise Applications



Early AWS Engagement

- Issued 60+ root level AWS accounts to various project teams
- Added all accounts to consolidated billing
- Associated a single project/task number for chargeback and bill back

The Problem



Dear Amazon EC2 Customer,

We've received a report that your instance(s) has been port scanned.

Instance Id: [REDACTED]

IP Address: [REDACTED]

has been port scanned.

This is specifically forbidden in our User Agreement: <http://aws.amazon.com/agreement/>

Please immediately restrict the flow of traffic from your instances(s) to cease disruption to other networks and reply this email to send your reply of action to the original abuse reporter. This will activate a flag in our ticketing system, letting us know that you have acknowledged receipt of this email.

It's possible that your environment has been compromised by an external attacker. It remains your responsibility to ensure that your instances and all applications are secured. The link <http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1233> provides some suggestions for securing your instances.

Case number: [REDACTED]

Additional abuse report information provided by original abuse reporter:

* Destination IPs:

* Destination Ports:

* Destination URLs:

* Abuse Time: Fri Mar 23 23:36:00 UTC 2012

* Log Extract:

<<<

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*



Dear Amazon EC2 Customer,

We've received a report that your instance(s) has been port scanned.

Instance Id: [REDACTED]

IP Address: [REDACTED]

has been port scanned.

This is specifically forbidden in our User Agreement: <http://aws.amazon.com/agreement/>

Please immediately restrict the flow of traffic from your instances(s) to cease disruption to other networks and reply this email to send your reply of action to the original abuse reporter. This will activate a flag in our ticketing system, letting us know that you have acknowledged receipt of this email.

It's possible that your environment has been compromised by an external attacker. It remains your responsibility to ensure that your instances and all applications are secured. The link <http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1233> provides some suggestions for securing your instances.

Case number: [REDACTED]

Additional abuse report information provided by original abuse reporter:

* Destination IPs:

* Destination Ports:

* Destination URLs:

* Abuse Time: Fri Mar 23 23:36:00 UTC 2012

* Log Extract:

<<<

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*



Dear Amazon EC2 Customer,

We've received a report that your instance(s) has been port scanned.

Instance Id: [REDACTED]

IP Address: [REDACTED]

has been port scanned.

This is specifically forbidden in our User Agreement: <http://aws.amazon.com/agreement/>

Please immediately restrict the flow of traffic from your instances(s) to cease disruption to other networks and reply this email to send your reply of action to the original abuse reporter. This will activate a flag in our ticketing system, letting us know that you have acknowledged receipt of this email.

It's possible that your environment has been compromised by an external attacker. It remains your responsibility to ensure that your instances and all applications are secured. The link <http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1233> provides some suggestions for securing your instances.

Case number: [REDACTED]

Additional abuse report information provided by original abuse reporter:

* Destination IPs:

* Destination Ports:

* Destination URLs:

* Abuse Time: Fri Mar 23 23:36:00 UTC 2012

* Log Extract:

<<<

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.105:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.122:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.140:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.21:25 SYN *****S*

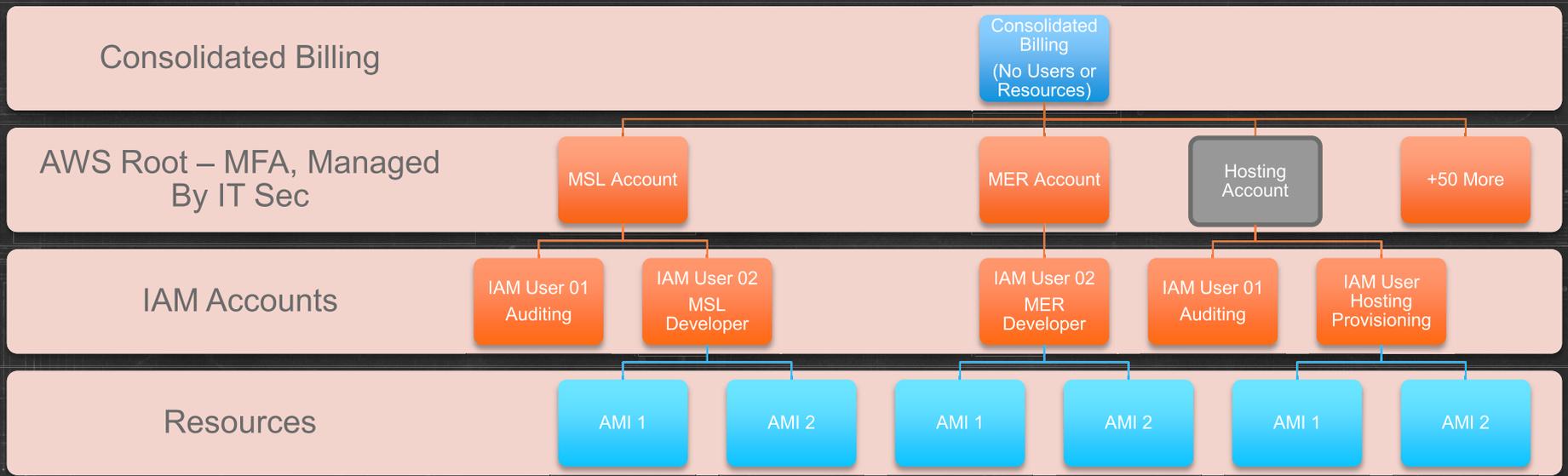
Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.240:25 SYN *****S*

Mar 23 19:36:59 50.18.0.41:17332 -> 128.173.10.44:25 SYN *****S*

Key Principles of JPL's Governance Model

- ✧ Understand your users and their use cases
- ✧ Apply policy and accountability
- ✧ Provide auditing and traceability

Account Management



Organizational Efficiency (DevOps)

- Automated Configuration Management
- Monitoring, Notification, Escalation
- Networking
- Verification and Validation



Measure the Value

- Calculate the cost of implementing governance along with the cost of cloud resources
- Consider the benefits of organizational efficiencies gained by cloud and governance

AWS re:Invent

We are sincerely eager to hear your **feedback** on this presentation and on re:Invent.

Please fill out an evaluation form when you have a chance.

Thank You

