Introduction to Amazon Cloud & EC2 Overview

Milty Brizan, AWS Solutions Architect WWPS SLG

March 27, 2018
Agenda

• Introduction to AWS Cloud
• Overview of AWS most used service: EC2
• EC2 Security Details
What is AWS?

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.

Benefits

- Low Cost
- Elasticity & Agility
- Open & Flexible
- Secure
- Global Reach
What sets AWS apart?

- **Experience**: Building and managing cloud since 2006
- **Service Breadth & Depth**: 90+ services to support any cloud workload
- **Pace of Innovation**: History of rapid, customer-driven releases
- **Global Footprint**: 16 regions, 44 availability zones, 100 edge locations
- **Pricing Philosophy**: 62 proactive price reductions to date
- **Ecosystem**: Thousands of consulting/system integrator & technology partners

*as of July 31, 2014*
Experience with Operational Reliability

We are driven to remove any all causes of failure. Our goal is to make our operational performance indistinguishable from perfect.

- We have spent over a decade building the world’s most reliable, secure, scalable, and cost-effective infrastructure.

- Service SLAs between 99.9% and 100% availability. Amazon S3 is designed for 99.999999999% durability.

- Availability Zones exist on isolated fault lines, flood plains, and electrical grids to substantially reduce the chance of simultaneous failure.

- The AWS Service Health Dashboard provides 24/7 visibility in the real-time operational status of all services around the globe.
Pricing Philosophy

High volume / low margin businesses are in our core DNA

- Trade CapEx for variable expense
- Our economies of scale provide us with lower costs
- Pricing model choice to support variable and stable workloads
- Save more money as you grow bigger

- 62 price reductions since 2006
- On-demand
- Reserved Instances
- Spot
- Tiered pricing
- Volume discounts
- Custom pricing
AWS Positioned as a Leader in the Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide*

AWS is positioned highest in execution and furthest in vision within the Leaders Quadrant

*Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Leong, Lydia, Petri, Gregor, Gill, Bob, Dorosh, Mike, August 2016

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS: http://www.gartner.com/doc/reprints?id=1-2G205FC&ct=150519&st=sb

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Introduction to AWS
AWS Global Infrastructure

18 Regions
54 Availability Zones
114 Points of Presence (103 Edge Locations, 11 Regional Caches)
Service Breadth & Depth

TECHNICAL & BUSINESS SUPPORT

AWS MARKETPLACE
- Support
- Professional Services
- Partner Ecosystem
- Training & Certification
- Account Management
- Solutions Architects
- Security & Pricing Reports

MANAGEMENT TOOLS
- Big Data & HPC
- Business Apps
- Security
- Development
- Backup
- Databases
- Industry Solutions
- Queuing
- Notifications
- Search
- Orchestration
- Email

PLATFORM SERVICES
- Analytics
- Mobile
- Development
- App
- Data Warehousing
- Sync
- Containers
- Mobile & Web Front-end
- Hadoop
- Identity
- Source Code
- Functions
- Streaming
- Push Notifications
- Build Tools
- Identity
- Orchestration
- Data Pipelines
- Mobile Analytics
- Deployments
- Data Store
- Machine Learning
- Mobile Backend
- DevOps
- Real-time

ENTERPRISE APPS
- Virtual Desktops
- Sharing & Collaboration
- Email & Calendaring
- Direct Connect
- Directories
- Identity Federation
- Backups
- Storage Gateway
- Integrated Management

SECURITY & MANAGEMENT
- Network
- Identity & Access
- Encryption Keys
- Configuration
- Monitoring
- Dedicated

INFRASTRUCTURE SERVICES
- Regions
- Availability Zones
- Compute
- Storage Objects, Blocks, Files
- Databases
- SQL, NoSQL, Caching
- Networking
- CDN

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
Any Questions?
EC2 Overview
EC2 Terminology

AMI

Virtual Machine Configuration

Instance

Running or Stopped VM

VPC

AZ

Availability Zone

EBS

Snapshots

Amazon S3

S3 Buckets

Region

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
EC2 Network Environment

Virtual Private Cloud
Bring your own network
Customer-managed subnets and routing
Additional network controls (Security Groups, NACLs, routing)
Hardware VPN options between corporate networks
Instances have Security Group–controlled private IPs (dynamic public IPs or EIPs optional)

Default VPC
Automatically assigned network and subnets (can now include NAT)
Broad Set of Compute Instance Types

General purpose

Compute optimized

Storage and IO optimized

GPU enabled

Memory optimized

M4

C4

I3

D2

P3

X1

M3

C3

P2

R4

R3

M3

C3

P2

R4

R3

M4

C4

I3

D2

P3

X1

T2

M3

C3

P2

R4

R3

M4

C4

I3

D2

P3

X1

T2
### Purchasing options at a glance

<table>
<thead>
<tr>
<th>On-Demand Instances</th>
<th>Reserved Instances</th>
<th>Spot Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay as you go</td>
<td>Pay a low upfront price</td>
<td>Bid what you like—your Spot instances run while your bid &gt; the Spot price</td>
</tr>
<tr>
<td>Flat hourly rate</td>
<td>Reserve an instance slot</td>
<td>Save up to 90% off of On-Demand</td>
</tr>
<tr>
<td>No commitment</td>
<td>Secure a low hourly rate</td>
<td>Run 1,000s of instances</td>
</tr>
</tbody>
</table>

- **On-Demand Instances**
  - Pay as you go
  - Flat hourly rate
  - No commitment

- **Reserved Instances**
  - Pay a low upfront price
  - Reserve an instance slot
  - Secure a low hourly rate
  - Sell & modify reservations if your needs change

- **Spot Instances**
  - Bid what you like—your Spot instances run while your bid > the Spot price
  - Save up to 90% off of On-Demand
  - Run 1,000s of instances
EC2 Operating Systems Supported

Amazon Linux
Debian
Suse
CentOS
Red Hat Enterprise Linux
Ubuntu
Layer your options
EC2 Security and Design
Details of a Virtual Machine

VM Workspace

Hypervisor

One or more ephemeral (temporary) drives

Network I/O

EBS

One or more EBS (persistent) drives

Amazon S3

EBS

EBS Snapshot

EBS Snapshot

EBS Snapshot
EBS AMI First Time Boot

VM Workspace

Hypervisor

Drive attaches to hypervisor & boots

Network I/O

EBS

Amazon S3

EBS

EBS Snapshot
EBS AMI Restart

VM Workspace

EBS

Hypervisor

Drive reattached

Network I/O

Amazon S3

EBS

EBS Snapshot

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
EBS AMI Terminate (Default behavior)

Default behavior: Drive deleted
EC2 Security Groups

Security Group Rules

- Name
- Description
- Protocol
- Port range
- IP address, IP range, Security Group name
Hierarchical Security Group Rules

- Dynamically created rules
- Based on Security Group membership
- Create tiered network architectures

**“Web” Security Group:**
- TCP 80 0.0.0.0/0
- TCP 22 “Mgmt”

**“App” Security Group:**
- TCP 8080 “Web”
- TCP 22 “Mgmt”

**“DB” Security Group:**
- TCP 3306 “App”
- TCP 22 “Mgmt”

**“Mgmt” Security Group:**
- TCP 22 163.128.25.32/32
## EC2 IP Addressing

<table>
<thead>
<tr>
<th>Default VPC</th>
<th>Virtual Private Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Private IP</td>
<td>Dynamic or Static Private IP Address</td>
</tr>
<tr>
<td>Dynamic Public IP</td>
<td>None by default (can be created with publicIP=true)</td>
</tr>
<tr>
<td>Optional Static Public IP (EIP)</td>
<td>Optional Static Public IP (EIP)</td>
</tr>
<tr>
<td>AWS-provided DNS names</td>
<td>AWS-provided public DNS lookup</td>
</tr>
<tr>
<td>• Private DNS name</td>
<td>AWS-provided private DNS names</td>
</tr>
<tr>
<td>• Public DNS name</td>
<td>Customer-controlled DNS options</td>
</tr>
</tbody>
</table>
EC2-Specific Credentials

EC2 key pairs
- Linux – SSH key pair for first-time host login
- Windows – Retrieve Administrator password

Standard SSH RSA key pair
- Public/Private Keys
- Private keys are not stored by AWS

AWS approach for providing initial access to a generic OS
- Secure
- Personalized
- Non-generic (NIST, PCI DSS)

“Public Half” inserted by Amazon into each EC2 instance that you launch

“Private Half” downloaded to your desktop
EC2 Instance access and Key Pairs

Linux launch (first boot)

- **Public key** made available through metadata
- Public key inserted into ~/.ssh/authorized_keys
- User connects with SSH using their **private key**
EC2 Instance access and Key Pairs

Linux launch (first boot)
- Public key made available through metadata
- Public key inserted into ~/.ssh/authorized_keys
- User connects with SSH using their private key

Windows launch (first boot sequence)
- Public key made available through metadata
- Sysprep
- Random Administrator password
- Password encrypted with public key
- User decrypts password with their private key
Instance Metadata


- ami-id
- ami-launch-index
- ami-manifest-path
- block-device-mapping/
- hostname
- instance-action
- instance-id
- instance-type
- kernel-id
- local-hostname
- local-ipv4
- mac
- network/
- placement/availability-zone
- profile
- public-hostname
- public-ipv4
- public-keys/
Any Questions?