AWS CERTIFIED SOLUTION ARCHITECT

ASSOCIATE

AMAZON WEB SERVICES

ELASTIC COMPUTE CLOUD - EC3

- Points To Remember

Basics about launching EC2 instance

Launching Amazon EC2 instance involves choosing AMI (must know what are the sources for AMI), choosing instance type (must know what a instance type control) and configuring user data.

Understand the pricing model for EC2

Three difference pricing models are available: reserved, spot and on-demand. Understand under what circumstances you will choose which pricing model.

EC2 Instance metadata and how to find it

Metadata is the data about your instance that you can use to configure or manage the running instance. Metadata includes AMI-id, public IP address and any roles assigned to the EC2 instance and hostname. Metadata can be access by logging into the instance and using **http://169.254.169.254/latest/meta-data**

EC2 Instance "user data" and how to find it

User data is loaded on the initial boot of the EC2 instance, and it can be loaded in subsequent boots. Includes specifying parameters for configuring your instance, downloading patches, installing software or attaching some scripts. User data size is limited to 16 KB. Can be accessed by logging into the instance and using **http://169.254.169.254/latest/user-data**

EC2 Instance metadata and how to find it

Metadata is the data about your instance that you can use to configure or manage the running instance. Metadata includes AMI-id, public IP address and any roles assigned to the EC2 instance and hostname. Metadata can be access by logging into the instance and using **http://169.254.169.254/latest/meta-data**

EC2 Instance "user data" and how to find it

User data is loaded on the initial boot of the EC2 instance, and it can be loaded in subsequent boots. Includes specifying parameters for configuring your instance, downloading patches, installing software or attaching some scripts. User data size is limited to 16 KB. Can be accessed by logging into the instance and using **http://169.254.169.254/latest/user-data**

Secure Network Architecture

Network devices, including firewall and other boundary devices are in place to monitor and control communications at the external boundary of the network and at key internal boundaries in the network.

Secure Access Points

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic.

Network Monitoring & Protection

AWS network provides significant protection against traditional network security issues.

1. Distributed Denial of Service (DDoS) attacks
2. Man in the Middle (MITM) attacks - new SSH host certificates on first boot
3. IP Spoofing - instance is not allowed to send traffic with a source IP or MAC other than its own
4. Port Scanning - by default all inbound ports on EC2 instances are closed
5. Packet Sniffing - hypervisor (xen) will not deliver any traffic to them, which is not addressed to them. Even two instances by the same customer cannot listen each other traffic