

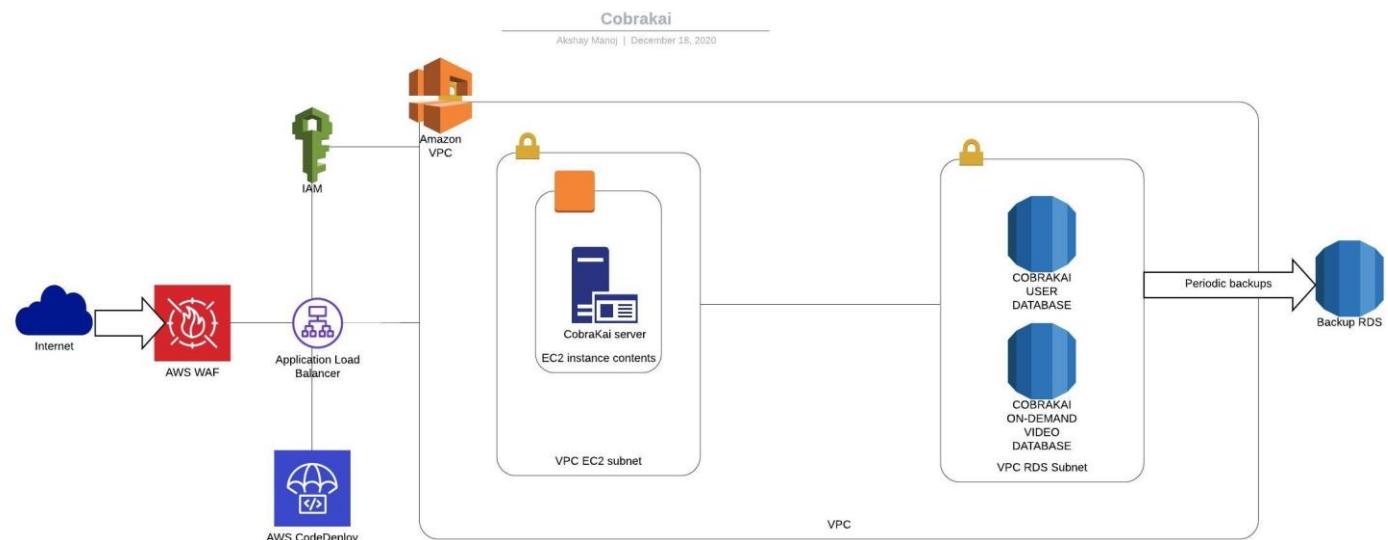
ENPM809J FINAL

CLOUD MIGRATION TECHNICAL PRESENTATION FOR COBRA KAI

AKSHAY MANOJ UID:116921169

PROPOSED ARCHITECTURE FROM LAST MEETING

- After some meetings with high level members of the company
- The following architecture has been approved for our cloud application



CONCLUSION FROM LAST PRESENTATION

- Steps we need to take:
 - Migrating a website to cloud
 - Setting up database on the cloud
 - Setting up load balancing on the cloud services
 - Setting up IAM for cloud services
 - Managing code on the cloud

BEFORE MIGRATION

- Create an AWS Root Account
- Set up a private Git repository for the application code

SETUP IAM SERVICES AND ROLES

- Types of user roles we need to create :
 - Administrator
 - Database Admin
 - Network Admin
 - Developer
 - Deployment User
 - Security auditor
 - Read only User

EXAMPLE DATABASE ADMIN USER AND ROLE CREATION

The screenshot shows the AWS IAM Management Console interface for creating a new user. The top navigation bar includes the IAM Management Console logo, a search bar, and user profile information (AkshayManoj). The main content area is titled "Set user details".

User name*: Enpm809j-Database-admin

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

- Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

- Autogenerated password
- Custom password

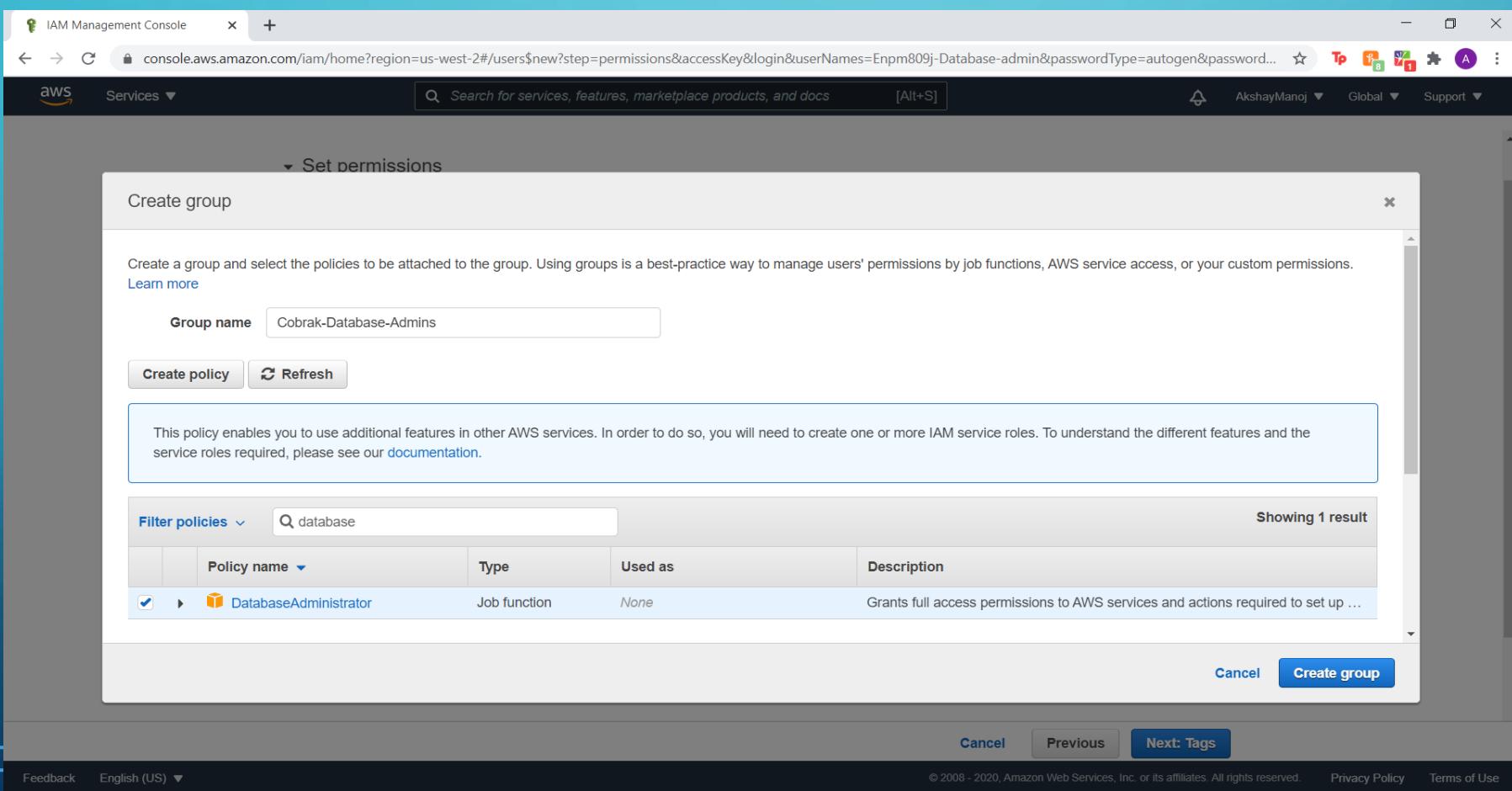
Require password reset
User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel **Next: Permissions**

Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

EXAMPLE DATABASE ADMIN USER AND ROLE CREATION



EXAMPLE DATABASE ADMIN USER AND ROLE CREATION

IAM Management Console

console.aws.amazon.com/iam/home?region=us-west-2#/users\$new?step=review&accessKey&login&userNames=Enpm809j-Database-admin&passwordType=autogen&passwordReset... AkshayManoj Global Support

User details

User name	Enpm809j-Database-admin
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	CobraKai-Database-Admins
Managed policy	IAMUserChangePassword

Tags

The new user will receive the following tag

Key	Value
Responsibilities	Manage database systems

Cancel Previous Create user

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

EXAMPLE DATABASE ADMIN USER AND ROLE CREATION

The screenshot shows the AWS IAM Management Console with the URL `console.aws.amazon.com/iam/home?region=us-west-2#/users$new?step=final&accessKey&login&userNames=Enpm809j-Database-admin&passwordType=autogen&passwordReset&...$`. The page title is "Add user". A success message box is displayed, stating: "Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." Below the message, it says "Users with AWS Management Console access can sign-in at: <https://934110205667.signin.aws.amazon.com/console>". A "Download .csv" button is present. A table lists the newly created user:

	User	Access key ID	Secret access key	Password	Email login instructions
▶	Enpm809j-...	AKIA5S7KOS3R34BEZHRZ	***** Show	***** Show	Send email

At the bottom, there are links for "Feedback", "English (US)", "Close", "Privacy Policy", and "Terms of Use".

SETTING UP AN EC2 INSTANCE

- Our current webserver is an Ubuntu server running from the basement of the office
- We can migrate our server side application onto the Cloud using an EC2 instance
- For simplicity we have decided to keep the EC2 and the Database Server instances in the same VPC network
- Next slides will demonstrate how to setup an EC2 Instance for our webserver

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS EC2 Management Console interface. The top navigation bar includes tabs for 'Instances' (selected), 'EC2 Management', and a '+' button. The URL is 'us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:'.

The left sidebar has a 'New EC2 Experience' toggle, followed by links for 'EC2 Dashboard', 'Events', 'Tags', 'Limits', and a 'Instances' section with sub-links for 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', and 'Capacity Reservations'. Below that is an 'Images' section with 'AMIs' and an 'Elastic Block Store' section with 'Volumes' and 'Snapshots'.

The main content area is titled 'Instances (1) Info' and contains a table with one row:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
-	i-071280708a6b4e81a	Stopped	t2.micro	-	No alarms +	us-west-2b	-

A message at the bottom of the table says 'Select an instance above'.

At the bottom of the page are links for 'Feedback', 'English (US)', and 'Feedback' again, along with copyright information: '© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy' and 'Terms of Use'.

SETTING UP AN EC2 WEB SERVER

Launch instance wizard | EC2 Main

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:

AWS Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Are you launching a database instance? Try Amazon RDS.

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora**, **MariaDB**, **MySQL**, **Oracle**, **PostgreSQL**, and **SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

Launch a database using RDS

AMI Name	Description	Select	64-bit (x86)	64-bit (Arm)
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-07dd19a7900a1f049 (64-bit x86) / ami-03c1b544a7566b3e5 (64-bit Arm)	Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services). Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select	<input checked="" type="radio"/> 64-bit (x86)	<input type="radio"/> 64-bit (Arm)
Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0ac73f33a1888c64a (64-bit x86) / ami-09e38cf07be65a594 (64-bit Arm)	Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services). Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select	<input checked="" type="radio"/> 64-bit (x86)	<input type="radio"/> 64-bit (Arm)
Microsoft Windows Server 2019 Base - ami-0d28bf0201017ce45	Microsoft Windows 2019 Datacenter edition. [English] Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select	<input checked="" type="radio"/> 64-bit (x86)	<input type="radio"/> 64-bit (Arm)
Deep Learning AMI (Ubuntu 18.04) Version 38.0 - ami-098555c9b343eb09c	MXNet-1.8.0 & 1.7.0, TensorFlow-2.3.1, 2.1.2 & 1.15.4, PyTorch-1.4.0 & 1.7.0, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA support. For fully managed experience, check: https://aws.amazon.com/sagemaker	Select	<input checked="" type="radio"/> 64-bit (x86)	<input type="radio"/> 64-bit (Arm)

Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS Launch Instance Wizard on the 'Choose Instance Type' step. The URL is us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard. The page displays a table of instance types across various families (t2, t3) with their respective specifications: vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, Network Performance, and IPv6 Support. The 't2.micro' instance type is highlighted as 'Free tier eligible'. The 't3.micro' instance type is selected.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input checked="" type="checkbox"/>	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes

Step 2: Choose an Instance Type

Currently selected: t3.micro (- ECUs, 2 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

Cancel Previous Review and Launch Next: Configure Instance Details

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS Launch Instance Wizard on the "Configure Instance" step. The URL in the browser is us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard. The page title is "Launch instance wizard | EC2".

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: Request Spot instances

Network: vpc-ef216897 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

CPU options: Specify CPU options

Shutdown behavior: Stop

Stop - Hibernate behavior: Enable hibernation as an additional stop behavior

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS Launch Instance Wizard interface for launching an EC2 instance. The current step is "4. Add Storage".

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0ec1b1f4a87b3b65a	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS Launch Instance Wizard at Step 6: Configure Security Group. The URL in the browser is us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:6. The page title is "Launch instance wizard | EC2 Mar". The navigation bar includes "AWS Services" and a search bar "Search for services, features, marketplace products, and docs [Alt+S]". The user is signed in as "AkshayManoj" in the Oregon region.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name: CobraKai application security group

Description: launch-wizard-2 created 2020-12-13T22:24:06.393-05:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 129.2.181.50/32	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Add Rule

At the bottom right are buttons for "Cancel", "Previous", and "Review and Launch".

SETTING UP AN EC2 WEB SERVER

The screenshot shows the AWS Launch Instance Wizard at Step 7: Review Instance Launch. The browser window title is "Launch instance wizard | EC2 Mar...". The URL is "us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#LaunchInstanceWizard:". The AWS logo is in the top left, and the user "AkshayManoj" is logged in.

The navigation bar includes "Services ▾", a search bar "Search for services, features, marketplace products, and docs [Alt+S]", and links for "1. Choose AMI", "2. Choose Instance Type", "3. Configure Instance", "4. Add Storage", "5. Add Tags", "6. Configure Security Group", and "7. Review".

The main content area is titled "Step 7: Review Instance Launch" and contains a section for "Instance Details". It lists various configuration options:

- Number of instances:** 1
- Purchasing option:** On demand
- Network:** vpc-ef216897
- Subnet:** No preference (default subnet in any Availability Zone)
- EBS-optimized:** No
- Monitoring:** No
- Termination protection:** No
- Shutdown behavior:** Stop
- Stop - Hibernate behavior:** Disabled
- Capacity Reservation:** open
- IAM role:** None
- Domain join directory:** None
- Tenancy:** default
- Credit specification:** Standard
- Host ID:** (empty)
- Host resource group name:** (empty)
- Affinity:** Off
- Kernel ID:** Use default
- RAM disk ID:** Use default
- Enclave:** false
- Metadata accessible:** Enabled
- Metadata version:** V1 and V2 (token optional)
- Metadata token response hop limit:** 1
- User data:** (empty)
- Assign Public IP:** Use subnet setting (Enable)
- Assign IPv6 IP:** Use subnet setting (Enable)

At the bottom right are buttons for "Cancel", "Previous", and "Launch".

Page footer: Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

SETUP DATABASE ON CLOUD

- We need to migrate our current on premise SQL database to the Cloud
- For this purpose we will create an instance of AWS RDS (Relational Database System)
- We can then write a migration script to just migrate our data onto this database instance

CREATING AN RDS INSTANCE ON AWS

RDS - AWS Console + us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#launch-dbinstance:gdb=false;s3-import=false

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S] AkshayManoj ▾ Oregon ▾ Support ▾

RDS > Create database

Create database

Choose a database creation method Info

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

Amazon Aurora 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CREATING AN RDS INSTANCE ON AWS

The screenshot shows the AWS RDS console interface for creating a new database instance. The URL is us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#launch-dbinstance:gdb=false;s3-import=false. The page displays a 'Templates' section with three options: 'Production' (selected), 'Dev/Test', and 'Free tier'. Below this is a 'Settings' section where the 'DB instance identifier' is set to 'CobraKai-Database-1'. Under 'Credentials Settings', the 'Master username' is 'admin' and the 'Master password' is masked. The 'Confirm password' field also contains masked text. The bottom of the screen includes standard AWS navigation links like Feedback, English (US), and footer links for Privacy Policy and Terms of Use.

RDS - AWS Console

us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#launch-dbinstance:gdb=false;s3-import=false

AWS Services Search for services, features, marketplace products, and docs [Alt+S]

AkshayManoj Oregon Support

Templates
Choose a sample template to meet your use case.

Production
Use defaults for high availability and fast, consistent performance.

Dev/Test
This instance is intended for development use outside of a production environment.

Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
[Info](#)

Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.
CobraKai-Database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Credentials Settings

Master username [Info](#)
Type a login ID for the master user of your DB instance.
admin

1 to 16 alphanumeric characters. First character must be a letter

Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm password [Info](#)

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CREATING AN RDS INSTANCE ON AWS

The screenshot shows the AWS RDS console interface for creating a new database instance. The top navigation bar includes the AWS logo, Services dropdown, search bar, and user profile (AkshayManoj). The URL in the address bar is `us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#launch-dbinstance:gdb=false;s3-import=false`.

DB instance size

DB instance class: [Info](#)
Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

Standard classes (includes m classes)
 Memory Optimized classes (includes r and x classes)
 Burstable classes (includes t classes)

db.m5.xlarge
4 vCPUs 16 GiB RAM Network: 4,750 Mbps

[Info](#) New instance classes are available for specific engine versions.

Include previous generation classes

Storage

Storage type: [Info](#)
Provisioned IOPS (SSD)

Allocated storage: 100 GiB
Minimum: 100 GiB, Maximum: 65,536 GiB

Provisioned IOPS: [Info](#)
3000 IOPS
Minimum: 1,000 IOPS, Maximum: 80,000 IOPS

[Info](#) Your actual IOPS might vary from the amount that you provisioned based on your database workload and instance type. [Learn more](#)

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CREATING AN RDS INSTANCE ON AWS

Availability & durability

Multi-AZ deployment [Info](#)

Create a standby instance (recommended for production usage)
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.

Do not create a standby instance

Connectivity

Virtual private cloud (VPC) [Info](#)
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-ef216897)

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change the VPC selection.

Subnet group [Info](#)
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default

Public access [Info](#)

Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing
Choose existing VPC security groups

Create new
Create new VPC security group

Existing VPC security groups

Choose VPC security groups

default X

► Additional configuration

CREATING AN RDS INSTANCE ON AWS

The screenshot shows the AWS RDS console interface for creating a new database instance. The URL in the browser is `us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#launch-dbinstance:gdb=false;s3-import=false`. The page is titled "Create a new DB instance".

VPC Security Groups: A dropdown menu titled "Choose VPC security groups" is open, showing "default" selected.

Database authentication: The "Password and IAM database authentication" option is selected. Other options shown are "Password authentication" and "Password and Kerberos authentication (not available for this version)".

Additional configuration: This section includes options for "Database options", "Encryption enabled", "Backup enabled", "Backtrack disabled", "Performance Insights enabled", "Enhanced Monitoring enabled", "Maintenance", "CloudWatch Logs", and "Delete protection enabled".

Estimated monthly costs:

DB instance	249.66 USD
Storage	25.00 USD
Multi-AZ standby instance	249.66 USD
Provisioned IOPS	300.00 USD
Total	824.32 USD

A note states: "This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer." Below this, there is a link to "Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)".

Subnet group: A modal window titled "Subnet group" is displayed, asking to "Choose the DB subnet group that defines which subnets and IP ranges the DB instance can use in the Virtual Private Cloud (VPC) you chose." It lists "Choose VPC security groups" and "default".

Buttons: At the bottom are "Cancel" and "Create database" buttons.

Page footer: Includes links for "Feedback", "English (US)", "Privacy Policy", and "Terms of Use".

SOME ADDITIONAL CONFIGURATIONS FOR OUR RDS

Backup
Creates a point-in-time snapshot of your database

Enable automatic backups
Enabling backups will automatically create backups of your database during a certain time window.

⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details [here](#).

Backup retention period [Info](#)
Choose the number of days that RDS should retain automatic backups for this instance.

Backup window [Info](#)
Select the period for which you want automated backups of the database to be created by Amazon RDS.
 Select window
 No preference

Copy tags to snapshots

Encryption

Enable encryption
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Master key [Info](#)

Account
934110205667

KMS key ID
alias/aws/rds

WHAT DO WE HAVE NOW?

- We have setup some IAM users and roles
- We have created an EC2 instance for our webserver
- We have created an RDS instance for our application database
- We have ensured that all these instances belong to the same VPC allowing them to communicate with each other easily

WHAT DO WE NEED TO DO NEXT?

- We need to deploy our code onto the EC2 instances.
- Our application will run on our EC2 Instances but still doesn't take advantage of the cloud scalability and load balancing
- We need to configure a load balancer between the internet and our application servers.
- We need to configure the firewall

CONFIGURE LOAD BALANCER

- We need to create an internet facing load balancer which will balance the incoming traffic between multiple EC2 instances
- A load balancer will require a listener and needs to be connected to the EC2 instances.
- The load balancer will be the entry point of our application, all incoming connections to our web application will pass through the loadbalancer

CONFIGURE LOAD BALANCER

The screenshot shows the AWS EC2 Management Console interface for configuring load balancers. The top navigation bar includes the EC2 Management Console logo, a search bar, and various AWS services like Lambda, CloudWatch Metrics, and CloudWatch Logs. The main content area displays a table titled "Load Balancers" with columns for Name, DNS name, State, VPC ID, Availability Zones, Type, Created At, and Monitoring. A message at the bottom of the table states, "You do not have any load balancers in this region." On the left side, a sidebar lists several service categories: Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts (New), Scheduled Instances, Capacity Reservations, Images (AMIs), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, New, Elastic IPs, New, Placement Groups, New, Key Pairs, New, Network Interfaces), Load Balancing (Load Balancers, Target Groups, New), and Auto Scaling (Launch Configurations, Auto Scaling Groups). The "Load Balancers" link under the Load Balancing category is highlighted in orange.

CONFIGURE LOAD BALANCER

Create Load Balancer | EC2 Manager + New

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:type=application:

AWS Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name: Scheme: internet-facing internal IP address type:

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80

Add listener

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC: Availability Zones:

Subnet	IPv4 address	Status
subnet-169f456e	Assigned by AWS	<input checked="" type="checkbox"/>
subnet-9c1cd8d6	Assigned by AWS	<input checked="" type="checkbox"/>
subnet-2caffa71	Assigned by AWS	<input checked="" type="checkbox"/>
subnet-37e2cf1c		<input type="checkbox"/>

Add-on services

Cancel Next: Configure Security Settings

Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CONFIGURE LOAD BALANCER

Create Load Balancer | EC2 Mana x +

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#CreateELBWizard:

AWS Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

AkshayManoj ▾ Oregon ▾ Support ▾

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

Assign a security group: Create a **new** security group Select an **existing** security group

Filter VPC security groups

Security Group ID	Name	Description	Actions
<input checked="" type="checkbox"/> sg-fa28c0d4	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-014faf6c87bcce3d4	launch-wizard-1	launch-wizard-1 created 2020-11-06T12:10:19.640-05:00	Copy to new

Cancel Previous Next: Configure Security Settings

Feedback English (US) ▾ © 2008 – 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CONFIGURE LOAD BALANCER

The screenshot shows the AWS Create Load Balancer wizard at Step 3: Configure Security Settings. The URL in the browser is us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#CreateELBWizard:3.

Step 3: Configure Security Settings

Select Certificate

AWS Certificate Manager (ACM) is the preferred tool to provision and store server certificates. If you previously stored a server certificate using IAM, you can deploy it to your load balancer. [Learn more](#) about HTTPS/SSL listeners and certificate management.

Certificate type: Choose a certificate from ACM (recommended)
 Choose a certificate from IAM
 Upload a certificate to IAM

Request a new certificate from ACM
AWS Certificate Manager makes it easy to provision, manage, deploy, and renew SSL Certificates on the AWS platform. ACM manages certificate renewals for you. [Learn more](#)

Certificate:

Select a Cipher

Configure SSL negotiation settings for the HTTPS/SSL listeners of your load balancer. You may select one of the Security Policies listed below, or customize your own settings. [Learn more](#) about the Security Policies and configuring SSL negotiation settings.

Predefined Security Policy: ELBSecurityPolicy-2016-08

Custom Security Policy:

SSL Protocols

Protocol-TLSv1
 Protocol-SSLv3
 Protocol-TLSv1.1
 Protocol-TLSv1.2

SSL Options

Server Order Preference

SSL Ciphers

ECDHE-ECDSA-AES128-GCM-SHA256

Buttons: Cancel, Previous, Next: Configure Health Check

Page Footer: Feedback, English (US) ▾, © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved., Privacy Policy, Terms of Use

CONFIGURE LOAD BALANCER

Create Load Balancer | EC2 Manager

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:type=application:

AWS Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

AkshayManoj ▾ Oregon ▾ Support ▾

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 4: Configure Routing
Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer; you can edit the listeners and add listeners after the load balancer is created.

Target group

Target group: New target group
Name: AppServers
Target type: Instance
Protocol: HTTP
Port: 80
Protocol version: HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
 HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
 gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol: HTTP
Path: /index.html

Advanced health check settings

Port: traffic port
 override
Healthy threshold: 5
Unhealthy threshold: 2
Timeout: 5 seconds
Interval: 30 seconds
Success codes: 200

Cancel Previous Next: Register Targets

CONFIGURE LOAD BALANCER

Create Load Balancer | EC2 Mana +

us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#V2CreateELBWizard:type=application:

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S]

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 5: Register Targets
Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets
To deregister instances, select one or more registered instances and then click Remove.

Remove

Instance	Name	Port	State	Security groups	Zone
No instances available.					

Instances
To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search Instances

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
i-071280708a6b4e81a	running	launch-wizard-1	us-west-2b	subnet-9c1cd8d6	172.31.32.0/20	

Cancel Previous Next: Review

Feedback English (US) ▾

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CONFIGURE LOAD BALANCER

The screenshot shows the AWS Create Load Balancer wizard at Step 6: Review. The page displays the configuration details for a new application load balancer named "CobraBalancer".

Load balancer:

- Name: CobraBalancer
- Scheme: internet-facing
- Listeners: Port:80 - Protocol:HTTP
- IP address type: ipv4
- VPC: vpc-e9f216897
- Subnets: subnet-169f456e, subnet-9c1cd8d6, subnet-2caf1a71, subnet-37e2cf1c
- Tags: (none)

Security groups:

- Security groups: sg-014faf6c87bcce3d4

Routing:

- Target group: New target group
- Target group name: AppServers
- Port: 80
- Target type: instance
- Protocol: HTTP
- Protocol version: HTTP1
- Health check protocol: HTTP
- Path: /index.html
- Health check port: traffic port
- Healthy threshold: 5
- Unhealthy threshold: 2
- Timeout: 5
- Interval: 30
- Success codes: 200

Targets:

- Instances: i-071280708a6b4e81a:80

Add-on services:

- AWS Global Accelerator: Disabled

At the bottom right, there are "Cancel", "Previous", and "Create" buttons.

SETUP THE AWS APPLICATION FIREWALL

- Now that we have our ALB created we can setup some WAF ACL's
- ALB would function as a firewall which blocks, allows or counts incoming requests matching a rule
- We can use preconfigured rules or can create our own rules

SETUP THE AWS APPLICATION FIREWALL

The screenshot shows a step-by-step setup process for AWS WAF. The main window is titled "Step 4: Configure metrics" and "Step 5: Review and create web ACL". A modal dialog box is open, titled "Add AWS resources". The "Resource type" section is displayed, with "Application Load Balancer" selected. Below it, a search bar says "Find AWS resources to associate" and lists "Name" and "CobraBalancer". At the bottom of the dialog are "Cancel" and "Add" buttons. The background shows other tabs like "Tutorial: Create a Classic Load Balancer" and "Instances | EC2 Management Console". The bottom of the screen includes standard AWS navigation links: Feedback, English (US), Copyright notice (© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

SETUP THE AWS APPLICATION FIREWALL

The screenshot shows the AWS WAF console interface. The top navigation bar includes tabs for "Tutorial: Create a Classic Load Balancer", "Registered instances for your CloudFront distribution", "AWS WAF", "Instances | EC2 Management Console", and "Internet-facing Classic Load Balancer". The main content area displays a table of rule groups:

Group	Count	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	<input type="checkbox"/> Add to web ACL <input type="radio"/> Set rules action to count
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	<input checked="" type="checkbox"/> Add to web ACL <input type="radio"/> Set rules action to count
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application.	50	<input checked="" type="checkbox"/> Add to web ACL <input type="radio"/> Set rules action to count
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.	700	<input type="checkbox"/> Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	<input type="checkbox"/> Add to web ACL
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.	200	<input checked="" type="checkbox"/> Add to web ACL <input type="radio"/> Set rules action to count
PHP application Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands.	100	<input type="checkbox"/> Add to web ACL
POSIX operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the POSIX operating system, including shell injection and privilege escalation.	100	<input type="checkbox"/> Add to web ACL

On the left sidebar, there are navigation steps: Step 3 (Set rule priority), Step 4 (Configure metrics), and Step 5 (Review and create web ACL). The top right corner shows the user's name "AkshayManoj" and navigation links for "Global" and "Support".

SETUP THE AWS APPLICATION FIREWALL

The screenshot shows the AWS WAF Rule configuration interface. The left sidebar is titled "WAF & Shield" and contains a "AWS WAF" section with options like "Getting started", "Web ACLs", "IP sets", "Regex pattern sets", "Rule groups", and "AWS Marketplace". It also includes links to "Switch to AWS WAF Classic", "AWS Shield", and "AWS Firewall Manager". The main content area is titled "Rule" and shows the configuration for a new rule named "Block_LaRusso". The "Type" is set to "Regular rule". The "If a request" condition is set to "matches the statement". The "Statement" section allows inspecting "Originates from a country in" and selecting "Choose country codes". A specific entry "China - CN" is selected. Below this, there is a note about determining the country of origin based on the source IP address or header. The "Then" section is titled "Action" and shows three options: "Allow", "Block", and "Count", with "Block" being selected. At the bottom right are "Cancel" and "Add rule" buttons.

Tutorial: Create a Classic Load | Registered instances for your | AWS WAF | Instances | EC2 Management | Internet-facing Classic Load | Karate Kid - Google Search | + | - | X

console.aws.amazon.com/wafv2/homev2/web-acls/new?region=us-west-2

aws Services ▾

Search for services, features, marketplace products, and docs [Alt+S]

WAF & Shield X

▼ AWS WAF

- Getting started
- Web ACLs**
- IP sets
- Regex pattern sets
- Rule groups
- AWS Marketplace

Switch to AWS WAF Classic

▶ AWS Shield

▶ AWS Firewall Manager

Rule

Name: Block_LaRusso

Type: Regular rule

If a request: matches the statement

Statement

Inspect: Originates from a country in

Country codes: Choose country codes

China - CN X

IP address to use to determine the country of origin
When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

Source IP address

IP address in header

Then

Action

Choose an action to take when a request matches the statements above.

Allow

Block

Count

Cancel Add rule

Feedback English (US) ▾

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

SETUP THE AWS APPLICATION FIREWALL

The screenshot shows the AWS WAF interface for creating a new Web ACL. The left sidebar is titled "WAF & Shield" and includes sections for "AWS WAF" (Getting started, Web ACLs, IP sets, Regex pattern sets, Rule groups, AWS Marketplace), "Switch to AWS WAF Classic", "AWS Shield", and "AWS Firewall Manager". The main content area is titled "Set rule priority" and shows a table of rules:

Name	Capacity	Action
Block_LaRusso	1	Block
AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
AWS-AWSManagedRulesSqlRuleSet	200	Use rule actions

Buttons at the bottom include "Cancel", "Previous", and "Next".

Page footer: Feedback English (US) ▾ © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

CODE DEPLOYMENT

- We can use AWS Code Deploy to setup our project on an online project management platform.
- We can connect our Git project to the AWS Code Deploy and setup the instances where the code will be deployed.
- We can also setup periodic builds to push code to the instances in versions.
- The development and devOps team will have to follow the detailed walkthrough at the link below to integrate our github repo with AWS code deploy
<https://docs.aws.amazon.com/codedeploy/latest/userguide/integrations-partners-github.html>

TIMELINE GOALS FOR THE CURRENT ROADMAP

- Aim to complete the user and role creation by Jan 12th 2021
- Aim to complete EC2 instance setup with deployed code by Feb 12th 2021
- Aim to complete RDS instance setup by Feb 12th 2021
- Aim to complete load balancer and firewall setup by Feb 20th 2021
- 2 weeks of Regression testing and Security testing to ensure no unexpected bugs
- Application should be ready for production use by March 1st 2021

REFERENCES

- <https://docs.aws.amazon.com/>