AWS RDS: Complete Deployment Guide

Interview Preparation - RDS Creation, Public vs Private Subnet, Multi-AZ & Security

1. What is Amazon RDS (Relational Database Service)?

Definition: Amazon RDS is a fully managed relational database service that makes it easy to set up, operate, and scale databases in the cloud. AWS handles routine database tasks like provisioning, patching, backup, recovery, and failure detection.

Supported Database Engines:

Database Engine	Version	Use Case	License
Amazon Aurora (MySQL)	Aurora 3.x (MySQL 8.0)	High performance, scalability	Open Source
Amazon Aurora (PostgreSQL)	Aurora 15.x (PG 15)	Advanced features, JSON support	Open Source
MySQL	8.0	Web applications, Popular open-source	GPL
PostgreSQL	15.x	Advanced SQL, JSON, geospatial	PostgreSQL License
MariaDB	10.11	MySQL fork, better performance	GPL
Oracle	19c, 21c	Enterprise apps, legacy systems	BYOL or Included
SQL Server	2019, 2022	Microsoft stack, .NET apps	License Included

Key RDS Benefits:

- **Managed Service:** AWS handles patching, backups, and maintenance automatically
- **Multi-AZ Deployment:** Automatic failover for high availability
- **Automated Backups:** Point-in-time recovery up to 35 days
- **Read Replicas:** Scale read workloads across multiple regions
- **Encryption:** At-rest (KMS) and in-transit (SSL/TLS) encryption
- **Monitoring:** CloudWatch metrics and Performance Insights included

2. RDS Instance Types and Sizing

Choose the right instance type based on workload requirements:

Instance Class	Use Case	vCPU	Memory	Example
General Purpose (db.t3, db.t4g)	Dev/Test, small prod DBs	2-8	1-32 GB	db.t3.medium (2 vCPU, 4 GB)
Memory Optimized (db.r6, db.x2)	Large databases, in-memory processing	2-128	16 GB-4 TB	db.r6i.xlarge (4 vCPU, 32 GB)
Burstable Performance (db.t3, db.t4g)	Variable workload, low baseline	2-8	0.5-32 GB	db.t3.micro (2 vCPU, 1 GB)

Storage Types:

Storage Type	IOPS	Throughput	Use Case	Cost
General Purpose SSD (gp3)	3K-16K (baseline 3K)	Up to 1,000 MB/s	Most workloads, balanced price-performance	Low
Provisioned IOPS SSD (io1/io2)	Up to 256K (guaranteed)	Up to 4,000 MB/s	I/O-intensive, latency-sensitive apps	High
Magnetic (standard)	Best effort	Limited	Legacy support only (deprecated)	Lowest

3. RDS Creation Process - Step-by-Step Guide

Follow these steps to create an RDS instance in AWS Console:

#	Action	Details / Options
1	Navigate to RDS Console	AWS Console → Services → RDS Click "Create database" button
2	Choose DB Creation Method	Standard Create: Full control Easy Create: AWS best practices
3	Select Engine Type	Aurora, MySQL, PostgreSQL, MariaDB, Oracle, SQL Server Choose engine version
4	Choose Templates	Production: Multi-AZ, auto backups Dev/Test: Single instance Free Tier: db.t3.micro (750 hrs/mo)
5	DB Instance Settings	DB Instance ID: myapp-prod-db Master username: admin Master password: Strong password Confirm password: Re-enter
6	Instance Configuration	Instance class: db.t3.medium Storage type: gp3 (General Purpose) Allocated storage: 100 GB Auto-scaling: Enable (max 1000 GB)
7	Connectivity Settings	VPC: Select VPC (10.0.0.0/16) Subnet group: Default or custom Public access: Yes or No (critical!) VPC Security group: Select/create AZ: No preference or specific AZ
8	Database Authentication	Password auth: Standard IAM database auth: Optional Kerberos auth: For SQL Server
9	Additional Configuration	Initial DB name: myappdb Backup retention: 7 days (1-35) Backup window: Preferred time Enable encryption: Yes (KMS key) Monitoring: Enable Enhanced Maintenance: Preferred time
10	Review and Create	Review all settings Estimated monthly cost: Displayed Click "Create database" Wait 5-15 min for provisioning

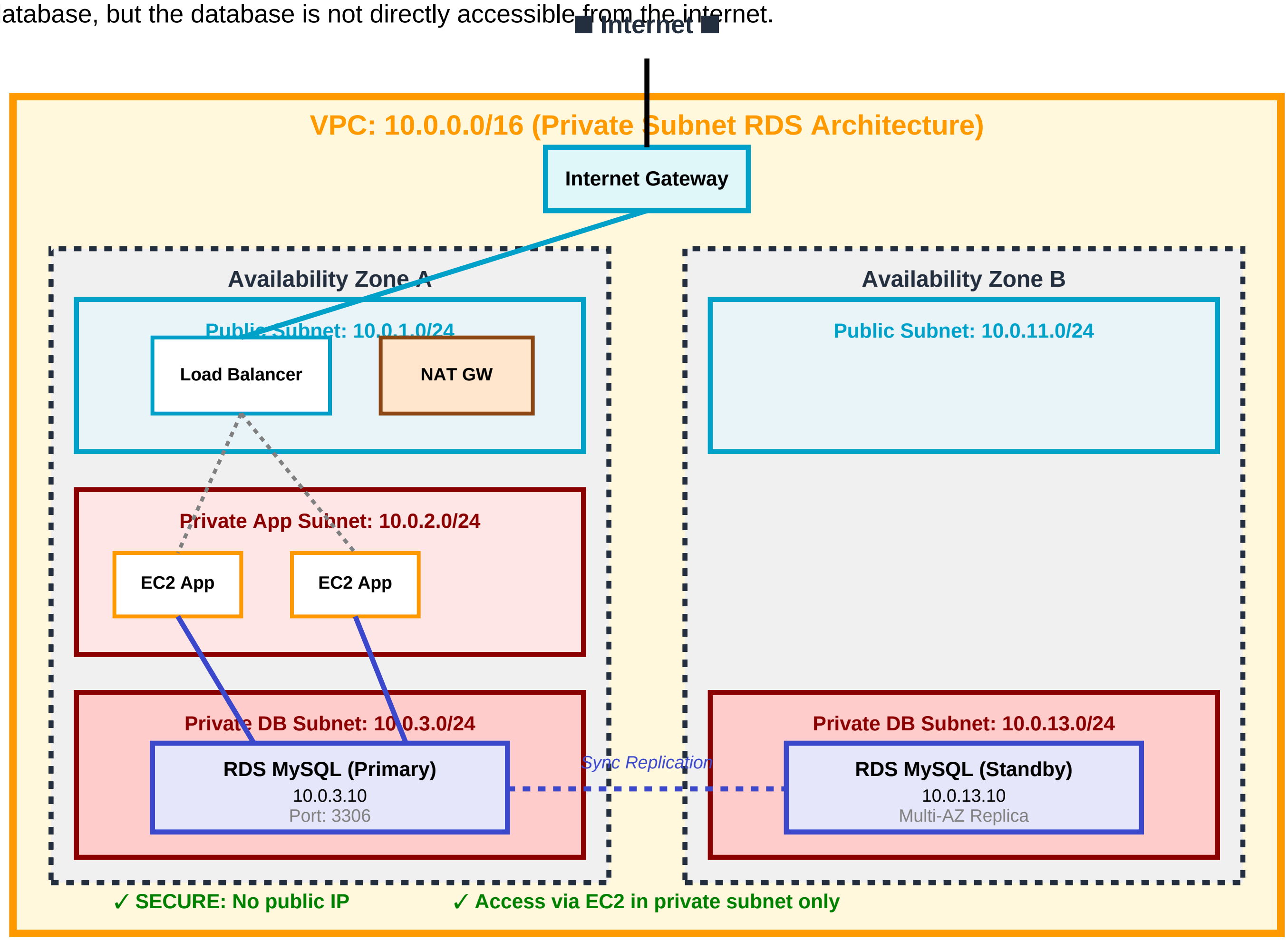
Important Notes on RDS Creation:

- **Cannot change VPC:** VPC selection is permanent, choose carefully

- **Security groups:** Must allow inbound traffic on database port (3306 for MySQL)
- **Subnet group:** Must have subnets in at least 2 AZs for Multi-AZ deployment
- **Public accessibility:** Think carefully - exposing DB to internet is risky

4. RDS in Private Subnet - Recommended Architecture

Best Practice: Deploy RDS in private subnets for security. Application servers in private subnets can access the database, but the database is not directly accessible from the internet.


■ Internet ■
VPC: 10.0.0.0/16 (Private Subnet RDS Architecture)
Internet Gateway
Availability Zone A
Public Subnet: 10.0.1.0/24
Load Balancer
NAT GW
Private App Subnet: 10.0.2.0/24
EC2 App
EC2 App
Private DB Subnet: 10.0.3.0/24
RDS MySQL (Primary)
10.0.3.10
Port: 3306
Sync Replication
Availability Zone B
Public Subnet: 10.0.11.0/24
Private DB Subnet: 10.0.13.0/24
RDS MySQL (Standby)
10.0.13.10
Multi-AZ Replica
✓ SECURE: No public IP
✓ Access via EC2 in private subnet only

Best Practice: RDS in private subnet with Multi-AZ for HA

Private Subnet Configuration Steps:

Configuration	Setting	Explanation
Public Access	No	RDS not accessible from internet
VPC	10.0.0.0/16	Your custom VPC
Subnet Group	db-subnet-group	Private subnets in 2+ AZs: • 10.0.3.0/24 (AZ-A) • 10.0.13.0/24 (AZ-B)
Security Group	rds-private-sg	Inbound: Port 3306 from 10.0.2.0/24 (app subnet)
Multi-AZ	Yes	Standby in different AZ for failover

Access Method	Via EC2 Bastion or App Server	No direct internet connection

Advantages of Private Subnet Deployment:

✓ **Security:** Database not exposed to internet, reduced attack surface

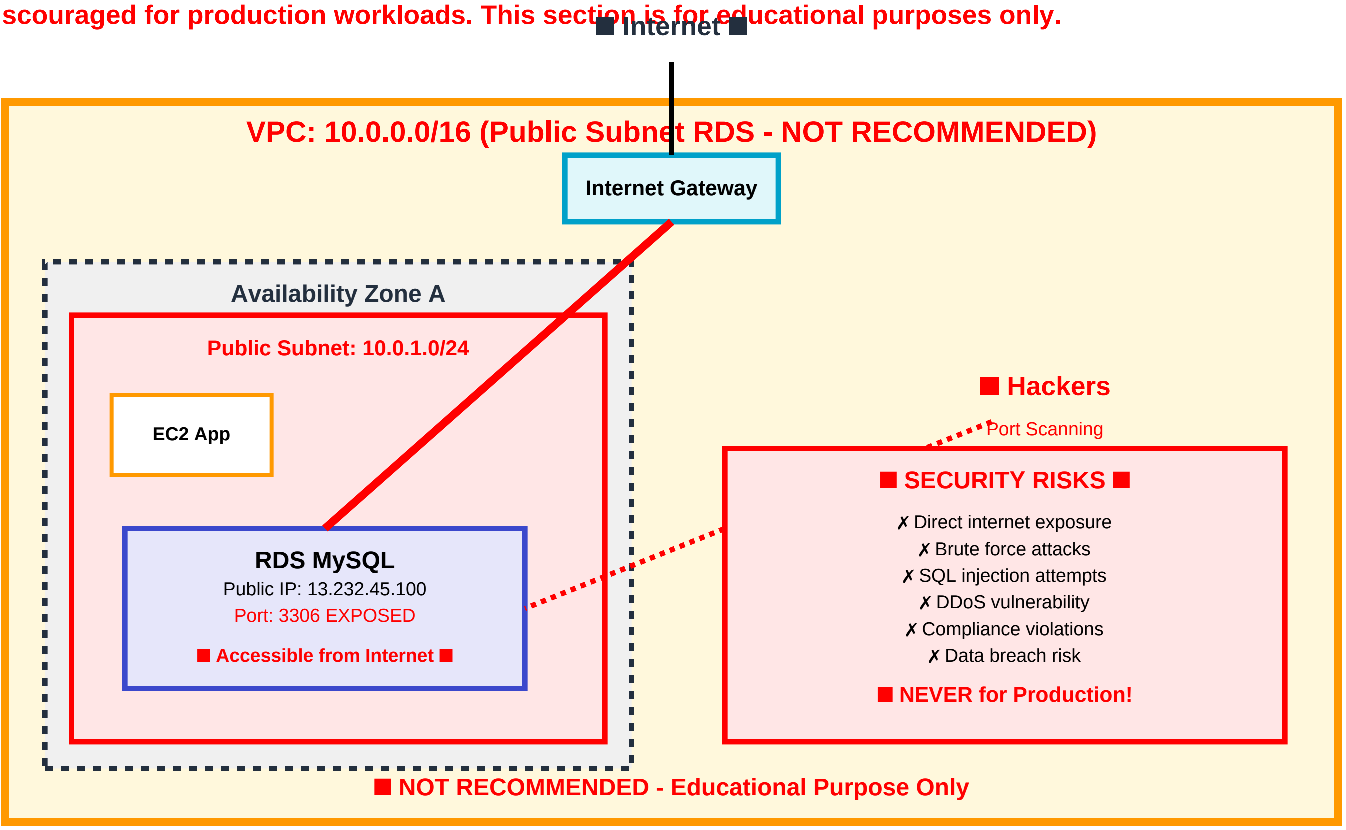
✓ **Compliance:** Meets security standards (PCI-DSS, HIPAA) requiring DB isolation

✓ **Network Control:** Precise control over which resources can access database

✓ **No Public IP Cost:** No need for Elastic IP

5. RDS in Public Subnet - NOT Recommended (Educational Only)

■ Warning: Deploying RDS in a public subnet exposes your database directly to the internet. This is highly discouraged for production workloads. This section is for educational purposes only.



If you must use public access for testing: Use strong passwords, restrict IPs, enable encryption

Public Subnet Configuration (NOT Recommended):

Configuration	Setting	Risk / Impact
Public Access	Yes	■ Database accessible from internet
Public IP	Assigned (EIP)	■ Endpoint exposed to attackers
Security Group	rds-public-sg	Must restrict to specific IPs (still vulnerable)
Subnet Route	0.0.0.0/0 → IGW	Direct internet routing
Multi-AZ	Optional	Standby also gets public IP
Encryption	Mandatory	At-rest and in-transit required

Why Public RDS is Dangerous:

- **Attack Surface:** Exposed to millions of internet attackers
- **Brute Force:** Automated scripts constantly try default credentials
- **Compliance Failure:** Violates PCI-DSS, HIPAA, SOC2 requirements
- **DDoS Risk:** Database can be overwhelmed with connection attempts
- **Data Breach:** One misconfigured security group = complete data exposure

When (if ever) to use Public RDS: Only for temporary development/testing with non-sensitive data, strong passwords, IP whitelisting, and immediate deletion after use. NEVER for production.

6. Private vs Public Subnet RDS - Complete Comparison

Aspect	Private Subnet (Recommended)	Public Subnet (NOT Recommended)
Internet Accessibility	No direct access from internet	Directly accessible from internet (dangerous)
Public IP	No public IP assigned	Public IP or Elastic IP assigned
Security Posture	Highly secure, isolated	High risk, exposed to attacks
Access Method	Via EC2 in private subnet, Bastion host, or VPN	Direct connection from anywhere (risky)
Security Group Rules	Allow only from app subnet CIDR (e.g., 10.0.2.0/24)	Must restrict to specific IPs (still vulnerable)
Route Table	No route to IGW (0.0.0.0/0 → NAT for EC2)	Has route to IGW (0.0.0.0/0 → IGW)
Compliance	✓ Meets PCI-DSS, HIPAA, SOC2 standards	■ Fails most compliance requirements
Use Case	✓ Production DBs ✓ Enterprise apps ✓ Sensitive data	■ Quick testing only ■ Never for production
Cost	No extra cost	May incur Elastic IP costs
Multi-AZ Impact	Standby also in private subnet (secure)	Standby also gets public IP (double exposure)

7. RDS Security Best Practices

#	Best Practice	Implementation	Why It Matters
1	Deploy in Private Subnet	Use DB subnet group with private subnets Disable public access	Eliminates direct internet exposure
2	Enable Encryption	At-rest: AWS KMS In-transit: SSL/TLS Certificate validation	Protects data from unauthorized access

3	Strong Passwords	Min 16 characters Mix letters, numbers, symbols Rotate every 90 days	Prevents brute force attacks
4	Security Group Restrictions	Allow only app subnet CIDR Never 0.0.0.0/0 Specific port only	Limits attack surface
5	IAM Database Authentication	Use IAM roles instead of passwords Temporary credentials	Eliminates password management
6	Enable Multi-AZ	Automatic failover Synchronous replication < 2 min recovery	High availability and disaster recovery
7	Automated Backups	Retention: 7-35 days Point-in-time recovery Test restores	Protects against data loss
8	Enhanced Monitoring	CloudWatch metrics Performance Insights Slow query logs	Detect anomalies and performance issues
9	Parameter Groups	Custom DB parameters Disable unused features Enforce SSL	Harden database configuration
10	VPC Flow Logs	Log network traffic Send to CloudWatch or S3 Set up alerts	Audit and detect suspicious activity

8. Multi-AZ Deployment vs Read Replicas

Understanding the difference between Multi-AZ and Read Replicas is crucial for interviews:

Feature	Multi-AZ Deployment	Read Replicas
Primary Purpose	High Availability (HA) and Disaster Recovery	Read Scalability and Performance
Replication	Synchronous replication to standby	Asynchronous replication to replica
Failover	Automatic failover (< 2 minutes)	Manual promotion to master if needed
Number Allowed	1 standby instance (same region)	Up to 5 read replicas (cross-region OK)
Endpoint	Single DNS endpoint (automatic redirect)	Separate endpoint for each replica
Data Lag	No lag (synchronous)	Typically seconds (asynchronous)
Cost	Double instance cost (2x compute + storage)	Additional instance cost per replica
Use Case	Production DBs requiring HA Meet SLA uptime Automatic recovery	Scale read workloads Reporting queries Analytics dashboards Reduce primary load
Region	Same region, different AZ	Same or different region
Can Write?	Standby cannot be accessed directly	Read replicas are read-only

Can You Use Both?

✓ **Yes!** You can enable Multi-AZ for high availability AND create Read Replicas for read scalability. This is common for large production workloads.

9. RDS Pricing Breakdown

Understanding RDS costs for interview discussions:

Cost Component	Pricing Model	Example (MySQL)	Notes
Instance Hours	Per hour based on instance type	db.t3.medium: $0.068/hour ($50/month)	Charged per second, 1-min minimum

Storage (gp3)	Per GB-month	$0.115/GB (100 GB = $11.50)	First 20 GB free tier eligible
IOPS (io1/io2)	Per provisioned IOPS	$0.10 per IOPS-month (10K IOPS = $100)	Only for Provisioned IOPS storage
Backup Storage	Per GB-month	Free up to 100% of DB storage Extra: $0.095/GB	Backups beyond DB size charged
Snapshot Export	Per GB	$0.010/GB exported to S3	For data analysis outside RDS
Data Transfer	Out to internet	First 1 GB/mo free Then $0.09/GB	In-region transfer free
Multi-AZ	Double instance cost	2x compute + storage = ~$100/month	Standby costs same as primary
Read Replicas	Per replica instance	Same as primary instance cost	Each replica charged separately

Sample Monthly Cost Calculation:

Component	Configuration	Monthly Cost
Instance	db.t3.medium (Multi-AZ)	$100 (2 instances × $50)
Storage	200 GB gp3	$23
Backups	150 GB (50 GB extra)	$5
Data Transfer	10 GB out	$1
		<b>$129/month</b>

10. Interview Key Points to Remember

When explaining RDS:

- RDS = Fully managed relational database service (AWS handles maintenance)
- Supports 7 engines: Aurora, MySQL, PostgreSQL, MariaDB, Oracle, SQL Server
- Benefits: Automated backups, patching, Multi-AZ, encryption, monitoring

When explaining Private Subnet deployment:

- **Always recommend private subnet** for production databases
- No public IP, not accessible from internet
- Access via EC2 in private subnet, bastion host, or VPN
- Security group allows only app subnet CIDR (e.g., 10.0.2.0/24)

When discussing Public Subnet:

- **NOT RECOMMENDED** - mention this immediately
- Database exposed to internet = major security risk
- Violates compliance (PCI-DSS, HIPAA)
- Only acceptable for temporary testing with non-sensitive data

When explaining Multi-AZ:

- Multi-AZ = High Availability with automatic failover
- Synchronous replication to standby in different AZ
- Failover < 2 minutes, single DNS endpoint
- Standby cannot be accessed (not for read scaling)

When explaining Read Replicas:

- Read Replicas = Scale read workloads, reduce primary load
- Asynchronous replication (seconds lag)
- Up to 5 replicas, can be cross-region
- Each replica has separate endpoint, read-only

11. Common RDS Interview Questions & Answers

Question	Answer
Why deploy RDS in private subnet?	Security: Database not exposed to internet, reduces attack surface, meets compliance
What is Multi-AZ?	HA solution with synchronous replication to standby in different AZ. Auto failover < 2 min

Multi-AZ vs Read Replicas?	Multi-AZ: HA, sync replication, auto failover Read Replicas: Scalability, async, manual promotion
Can RDS be in public subnet?	Technically yes, but NOT recommended. Exposes DB to internet attacks, fails compliance
How to connect to RDS in private subnet?	Via EC2 instance in private subnet, bastion host in public subnet, or VPN/Direct Connect
What is DB subnet group?	Collection of subnets (in 2+ AZs) where RDS can place instances. Required for Multi-AZ
How does RDS failover work?	Multi-AZ: DNS switches to standby (~2 min). App reconnects automatically to same endpoint
What encryption options?	At-rest: KMS encryption of storage/backups In-transit: SSL/TLS connections enforced

AWS RDS Complete Guide | Interview Success | Remember: ALWAYS Private Subnet for Production!