Amazon RDS for Oracle New Features

Amit Grover
Senior Database Engineer
Amazon Web Services

Dallas Willet
Principal Database Engineer
Amazon Web Services

February 13th, 2020

NoCOUG 2020 Winter Conference: Amazon RDS for Oracle Boot Camp

Agenda

Features launched in 2019

Managed High Availability

Managed Scalability

Managed Disaster Recovery

Managed Backups and Recovery

Security: Authentication with Kerberos and Active Directory

Q & A

Features Launched in 2019

Value Proposition	Q4-2018	Q1-2019	Q2-2019	Q3-2019	Q4-2019
Compatibility	• 2018 October PSU • Oracle Database 12.2	• 2019 January PSU/RU	• 2019 April PSU/RU	• 2019 July PSU/RU • Support for Oracle Database 18c	• 2019 October PSU/RU • Support for Oracle Database 19c
Instance launches and deprecations	• Support for M5, R5 instance families	• T3 instance type	• Z1d instance type - faster clock speeds	• Deprecation of M3 and R3 instance types (in progress) • Extended regional support for X1/X1e	• Deprecation of T2 instance type (Stopped new Creates) • Extended regional support for Z1d
Feature launches	• JVM Support • Support for extended data types • SQLT Version 12.2.180331	• SQLT 12.2.180725 • APEX 18.1, 18.2	• APEX 19.1	• OEM Agent 13cR3	• OEM Agent emctl commands • OEM Agent using SSL
Manageability and security	• Performance Insights • Stop and Start of Multi-AZ DB Instances	• Data Ingress/Egress with Amazon S3 integration	• PI Counter metrics • Storage autoscaling	• Kerberos/Active Directory	• PI SQL-level metrics
Performance, scalability, & availability	• Increased the Maximum storage from 16 TiB to 32TiB	• Data Guard In-Region Read Replicas	• 80K PIOPS & 64 TiB max storage size		• Data Guard X-Region Read Replicas

aws

Agenda

Features launched in 2019

Managed High Availability

Managed Scalability

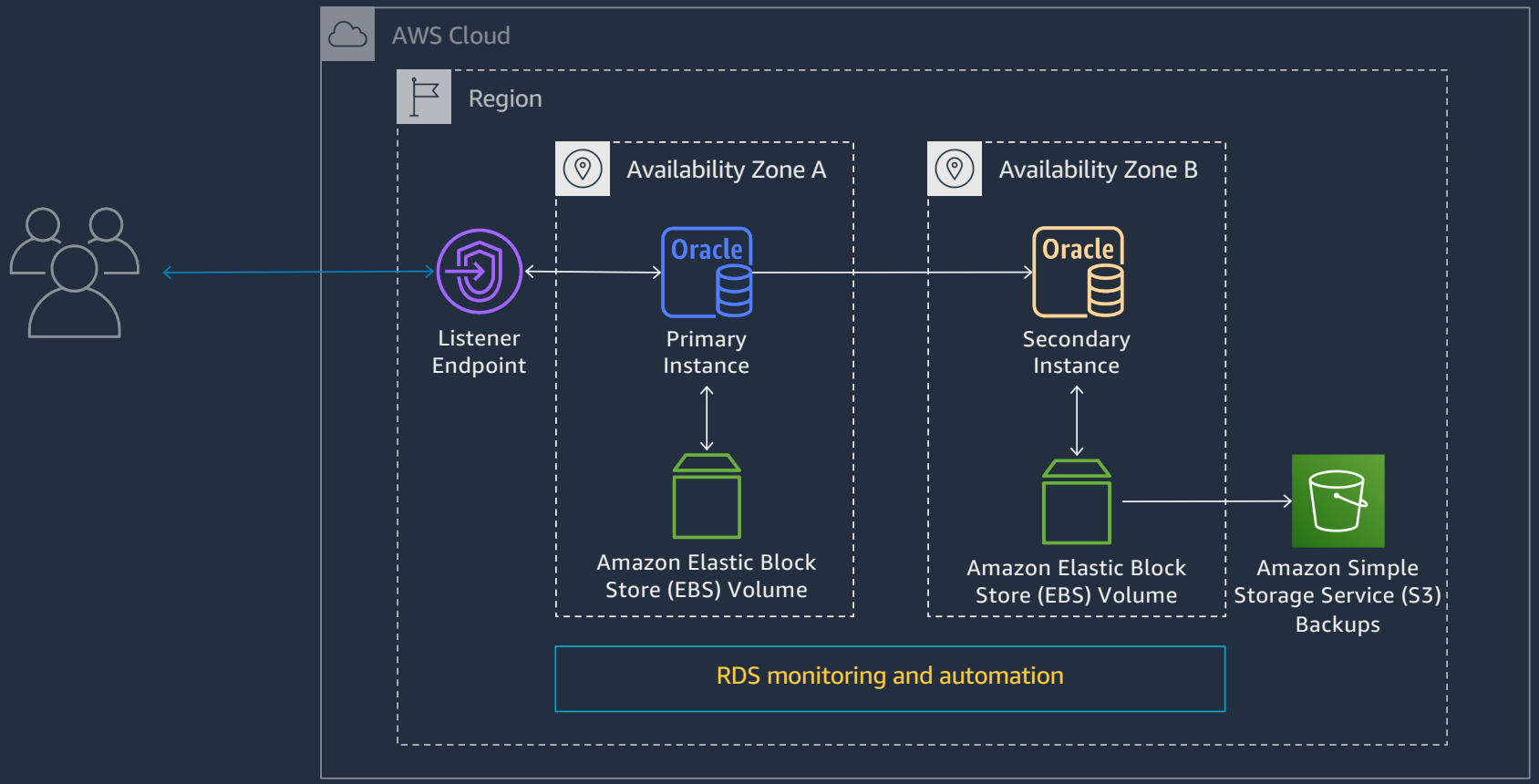
Managed Disaster Recovery

Managed Backups and Recovery

Security: Authentication with Kerberos and Active Directory

Q & A

Managed High Availability with Amazon RDS Multi-AZ



aws

Managed High Availability with Amazon RDS Multi-AZ

Best Practices

- Use Multi-AZ for mission critical workloads
- Deploy symmetric application configuration across AZs
  - No “fail back” double-outage
- Connection pools need to reconnect
  - Make sure connection pools do not cache Domain Name System (DNS)
- Test performance
  - Synchronous replication will add latency to writes
- Test application resilience → RebootDBInstance + ForceFailover

aws

Agenda

Features launched in 2019

Managed High Availability

Managed Scalability

Managed Disaster Recovery

Managed Backups and Recovery

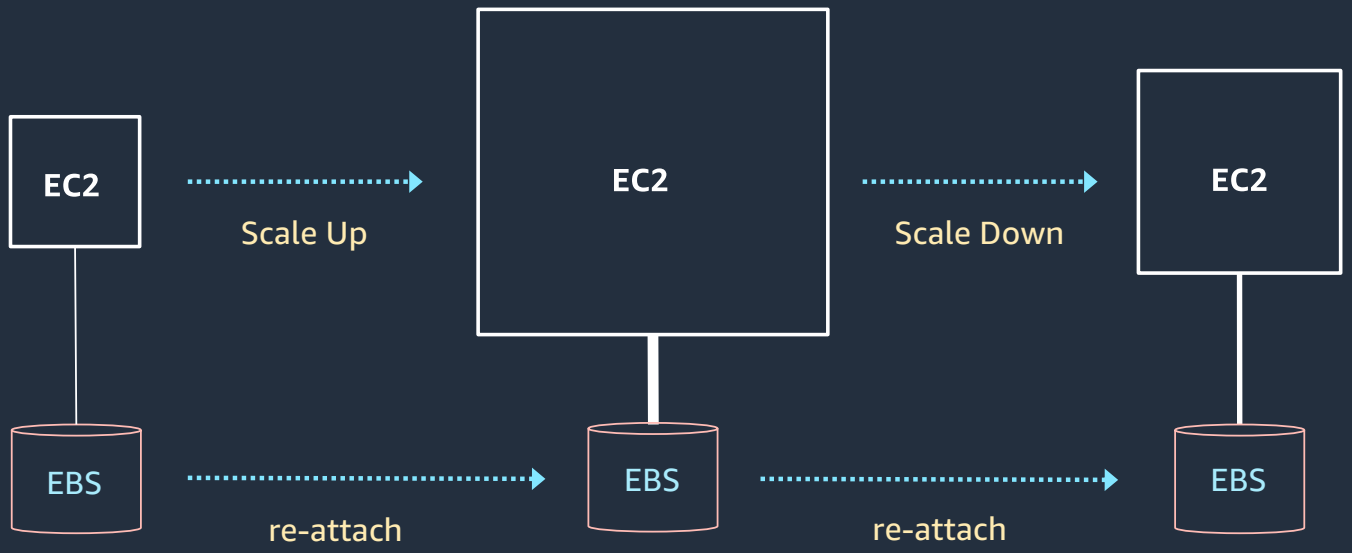
Security: Authentication with Kerberos and Active Directory

Q & A

aws

Managed Scalability - Compute

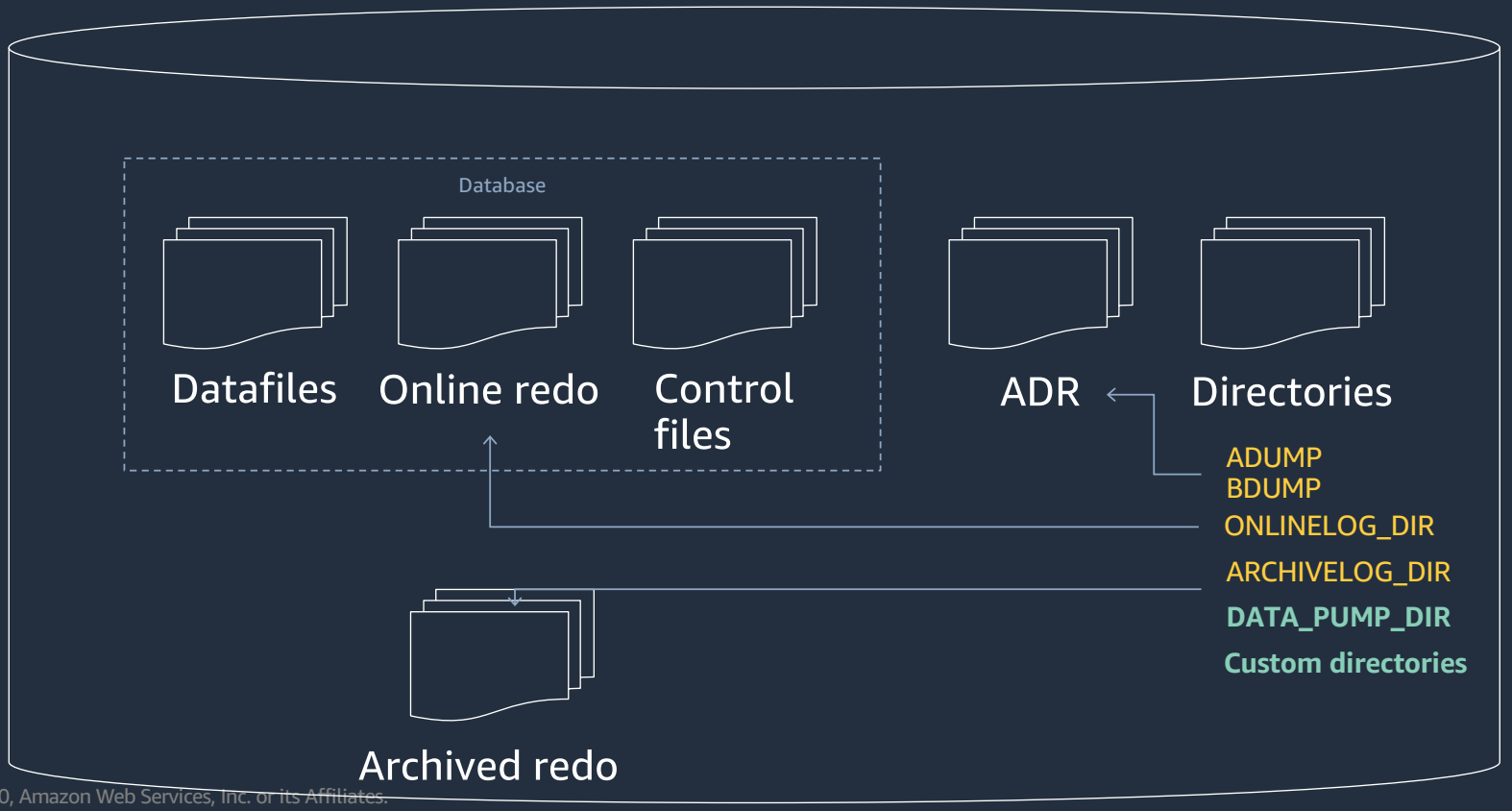
- Scale compute & memory vertically up or down



aws

Managed Scalability - Storage

- Online scaling of storage size, changing storage type (gp2, io1) or IOPS (io1), and auto-scaling



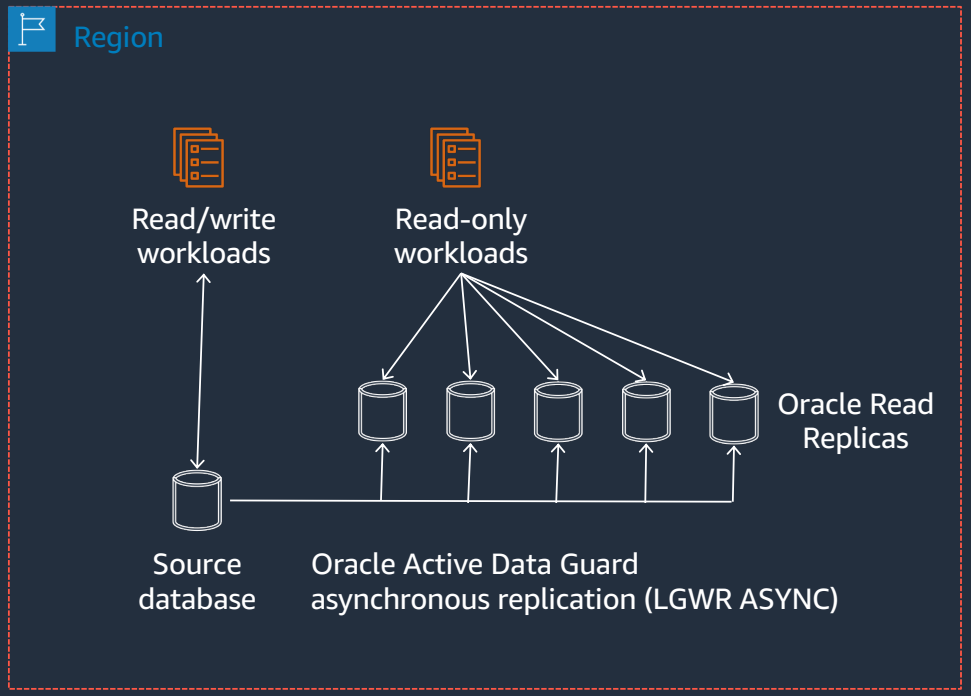
MAZ Secondary

EBS Snapshot

aws

Managed Scalability: In-Region Read Replicas

- Benefits
  - Relieve pressure on source database with additional read capacity
  - Scale your read workload
  - Promote a replica to a new stand-alone database
- Create up to 5 replicas per source database
- Managed Active Data Guard, requires bring your own license (BYOL)
- Database upgrades occur on replicas after source
- Replicas can be Multi-AZ



aws

Agenda

Features launched in 2019

Managed High Availability

Managed Scalability

Managed Disaster Recovery

Managed Backups and Recovery

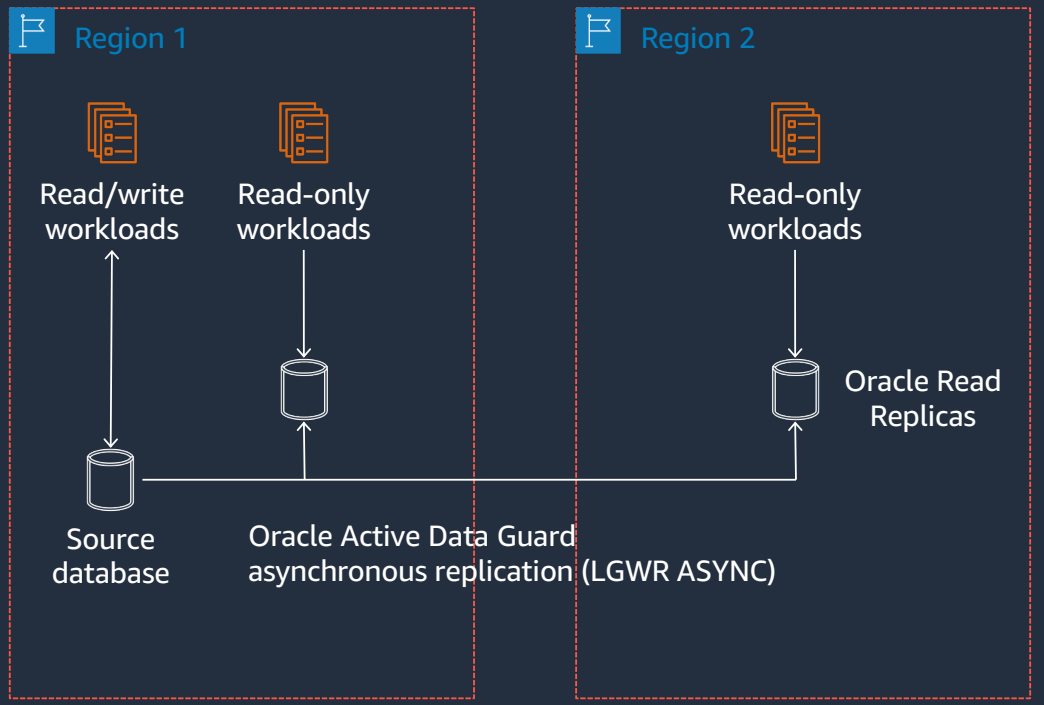
Security: Authentication with Kerberos and Active Directory

Q & A

aws

Managed Disaster Recovery: Cross-Region Read Replicas

- Benefits
  - To bring data closer to the users
  - A standby database in the event of disaster
- Create up to 5 replicas per source database
- Managed Active Data Guard, requires BYOL
- Database upgrades occur on replicas after source
- Replicas can be Multi-AZ



aws

Agenda

Features launched in 2019

Managed High Availability

Managed Scalability

Managed Disaster Recovery

Managed Backups and Recovery

Security: Authentication with Kerberos and Active Directory

Q & A

Backups, Snapshots, and Point-in-time restore

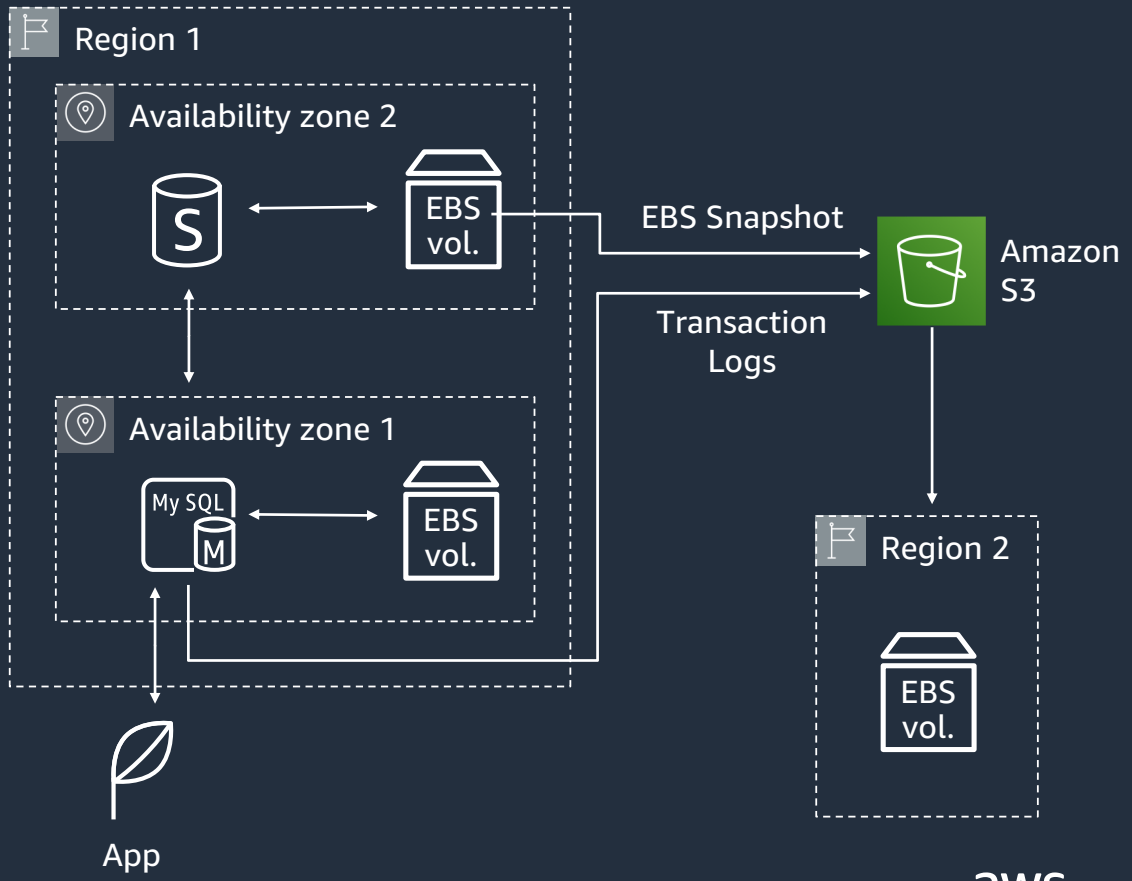
Two options—automated backups and manual snapshots

Amazon EBS snapshots stored in Amazon S3

Transaction logs stored every 5 minutes in Amazon S3 to support Point-in-time restore

No performance penalty for backups

Snapshots can be copied across regions or shared with other accounts



Agenda

Features launched in 2019

Managed High Availability

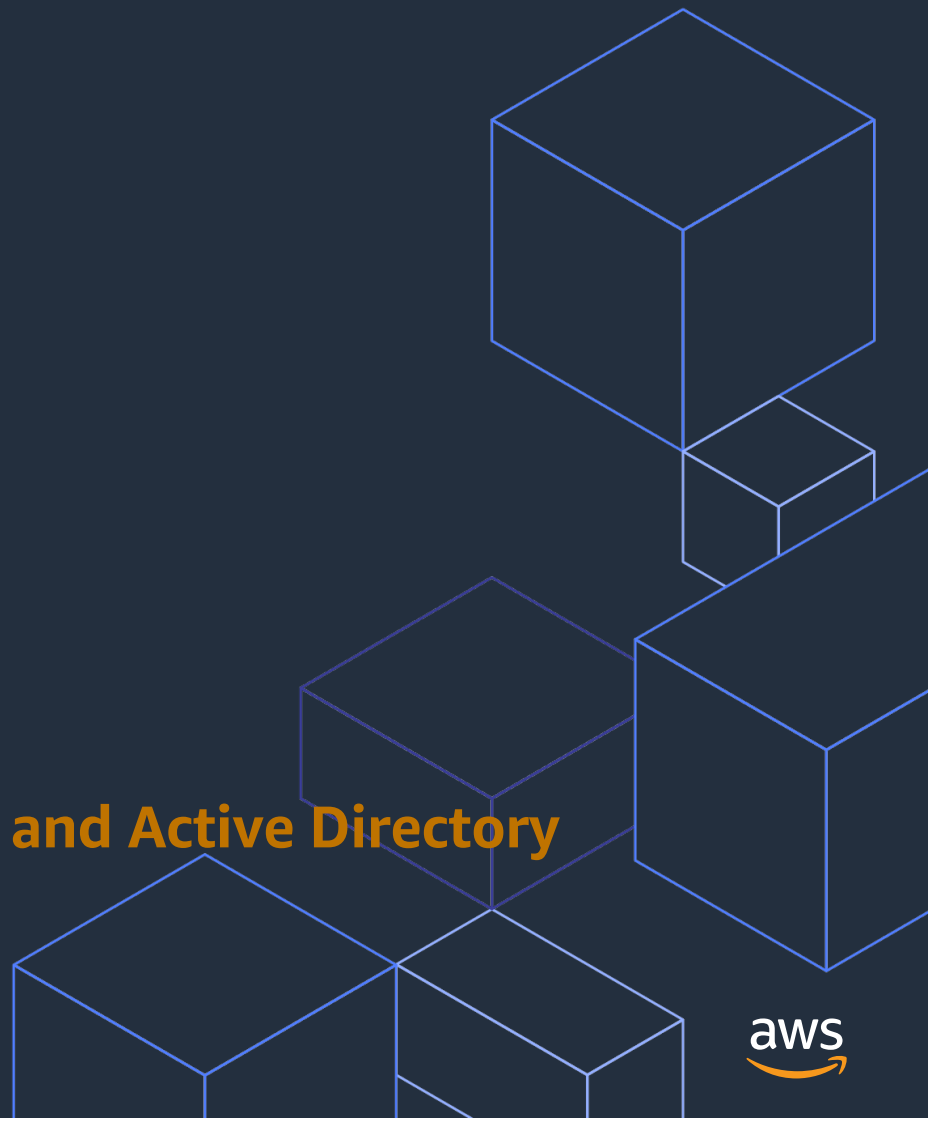
Managed Scalability

Managed Disaster Recovery

Managed Backups and Recovery

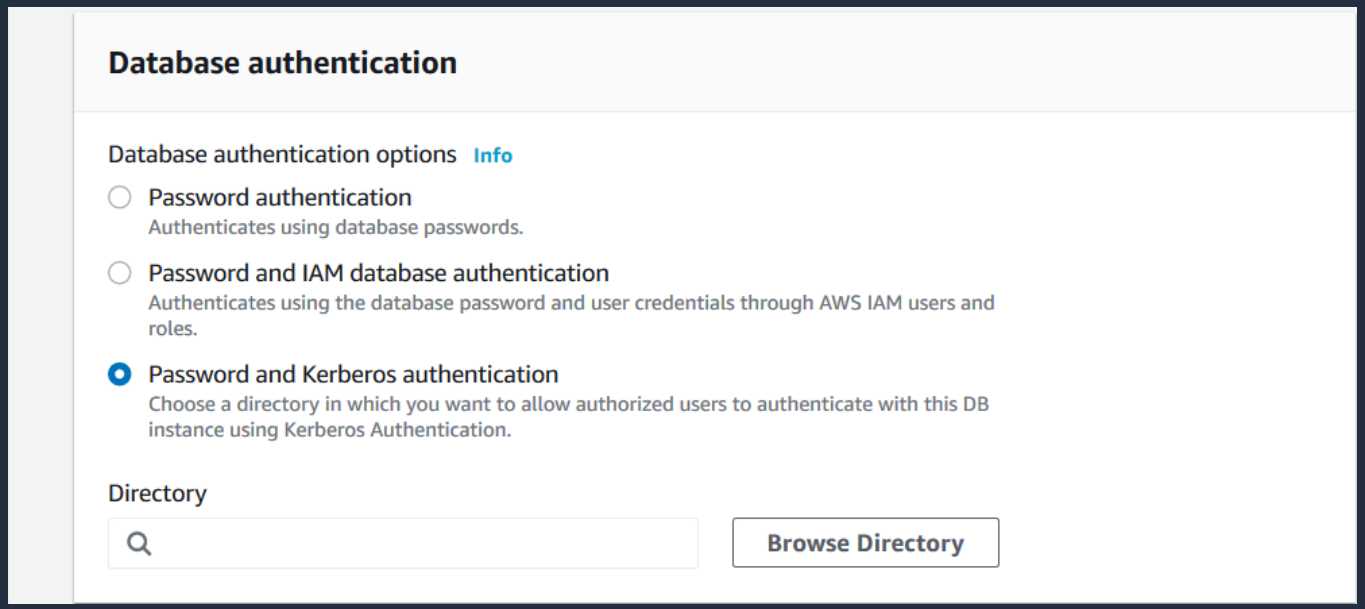
Security: Authentication with Kerberos and Active Directory

Q & A



aws

Authentication with Kerberos and Active Directory



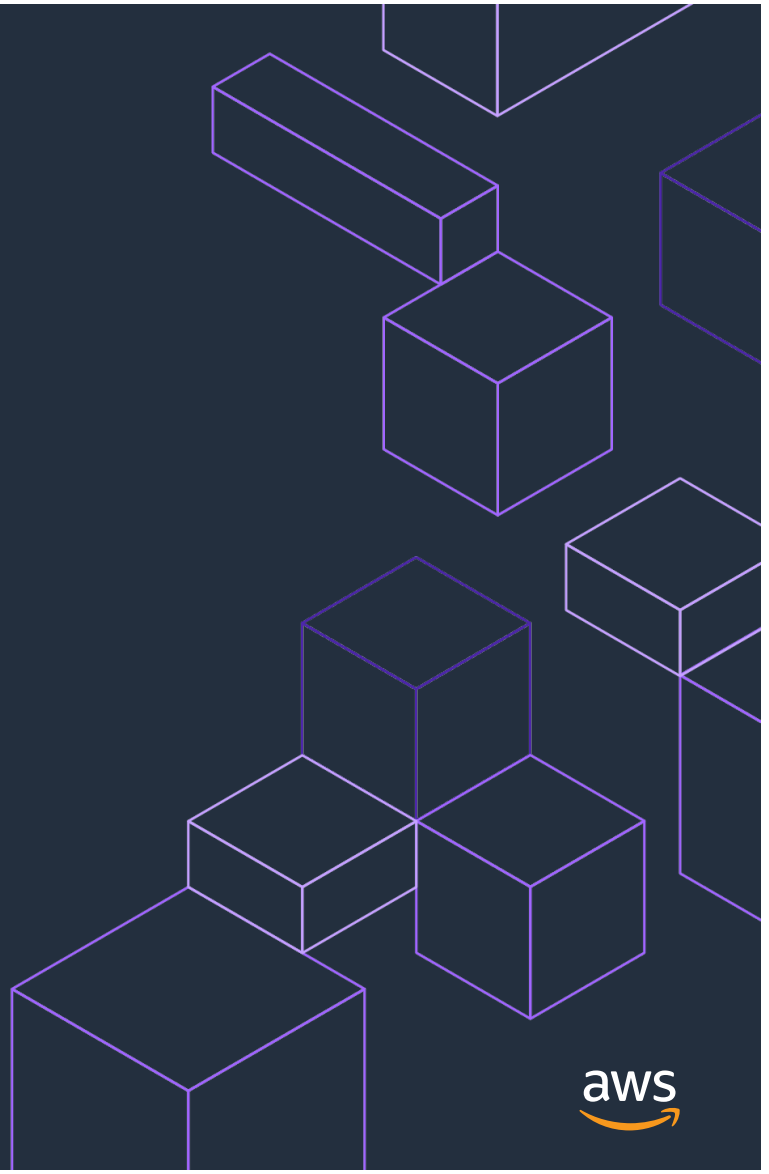
- Single Sign-on for your database
- Centrally managed authentication
- Credentials stored in AWS Directory Service for AD or on-premises AD

- Easy to manage, saves time and effort
- Use the same AD for Different VPC
- Allows instances to join AD owned by different accounts

aws

Q&A

Dallas Willet and Amit Grover



aws