Dragos Madarasan

Solutions Architect
Amazon Web Services

Running Microsoft SQL on AWS

Sponsors

Global SQL Saturday Partners

Microsoft Azure

PASS

Sponsors and Partners

Microsoft

Domino's

UBISOFT

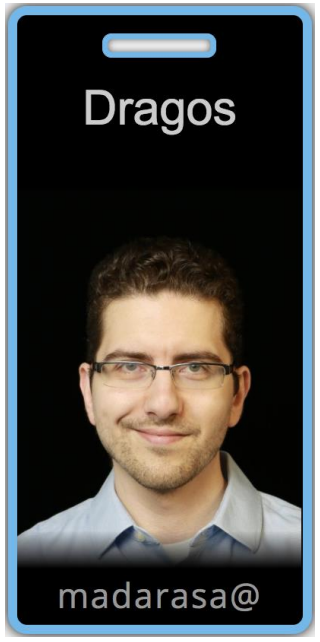
Esential Training

GENOS

About me

Dragos Madarasan – https://dragos.madarasan.com

- Solutions Architect @ AWS, covering Romania and Hungary
- Work with and support clients, partners, NGOs, Public Sector
- Based in Munich, Germany, often in Romania
- Previously Support Engineer and ProServe Consultant @ AWS



Agenda

- Introduction
- Availability
- Storage
- Security
- Backup and monitoring
- Data migration

AWS by Category: Core Services

Compute


Amazon EC2


AWS Elastic Beanstalk


Auto Scaling


AWS Lambda


Amazon Elastic Container Registry


Amazon Elastic Container Service


Amazon Lightsail


AWS Batch

Networking


Amazon VPC


Amazon Route 53


AWS Direct Connect


Elastic Load Balancing

Storage


Amazon S3


Amazon EBS


Amazon CloudFront


Amazon Glacier


Amazon Elastic File System


AWS Snowball


Storage Gateway


AWS Snowmobile

Database


Amazon RDS


Amazon DynamoDB


Amazon Redshift

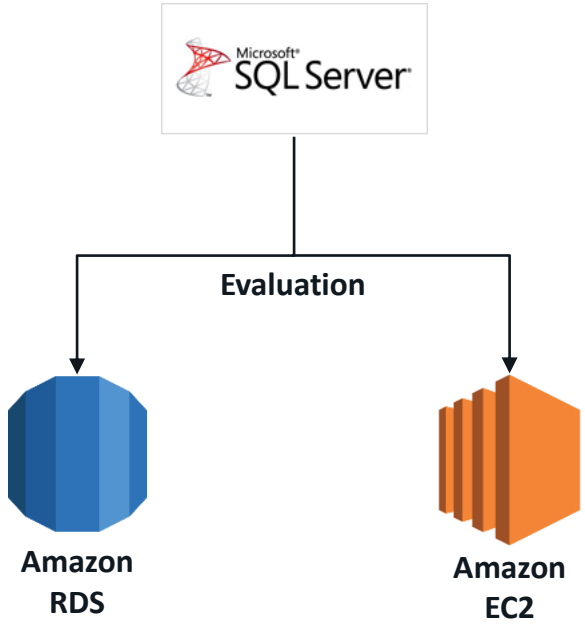

AWS Database Migration Service


Amazon ElastiCache

Choose the best service for your needs

Amazon RDS SQL Server

- Managed physical infrastructure
- Managed DB Install and backups
- Managed OS and patching
- Managed high availability and scaling



SQL Server on Amazon EC2

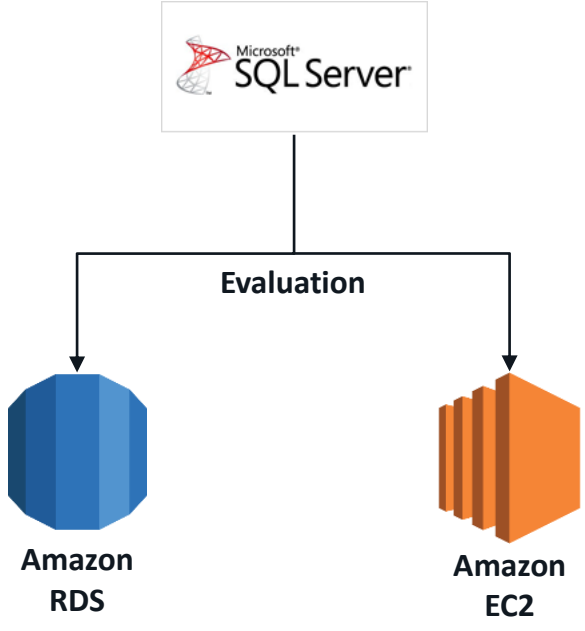
- Managed physical infrastructure
- Managed OS installation
- Managed scaling
- OS-level control

Choose the best service for your needs

Amazon RDS SQL Server

Your responsibility:

- App optimization and tuning
- Deployment Orchestration



SQL Server on Amazon EC2

Your responsibility:

- App optimization and tuning
- Deployment orchestration
- Monitoring and recovery
- High availability
- Backups
- DB & OS patching

SQL Server features at a glance

	Amazon RDS	Amazon EC2
Versions supported:	2012, 2014, 2016, 2017	All
Editions supported:	Express, Web, Standard, Enterprise**	All
High availability:	AWS-managed	Self-managed; AlwaysOn, Mirror, Log Ship
Encryption:	Encrypted Storage using AWS KMS (all editions); TDE Support	
Authentication:	Windows & SQL authentication	
Backups:	Managed automated backups	Maintenance plans & 3rd party tools
Maintenance:	Automatic software patching	Self-managed

SQL Server EC2 vs. RDS

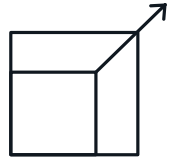
	EC2	RDS
License included	✓	✓
BYOL	✓	
Full control over the instance	✓	
Automated backups		✓
Self-managed AlwaysOn availability groups	✓	
AWS-managed Multi-AZ deployment		✓

Amazon Relational Database Service (Amazon RDS)

Amazon Aurora · MySQL · PostgreSQL · MariaDB · Microsoft SQL Server · ORACLE

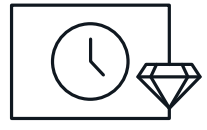
Easy to administer

Easily deploy and maintain hardware, OS and DB software; built-in monitoring



Performant & scalable

Scale compute and storage with a few clicks; minimal downtime for your application



Available & durable

Automatic Multi-AZ data replication; automated backup, snapshots, and failover

Secure & compliant

Data encryption at rest and in transit; industry compliance and assurance programs

Amazon RDS - Managed Service

What does Amazon RDS Manage?

- Provisioning
- Installation and Patching
- Automated Backups
- Restores: Snapshot and point-in-time
- High Availability
- Monitoring

Amazon RDS - Configuration

What can you configure?

- Instance type/Class
- Engine version/Edition
- Storage
- Network Connectivity
- Time Zone
- Backup Retention
- Encryption
- High Availability
- Monitoring

SQL Server as a managed service

AMAZON RDS

- Same SQL Server DB engine as with Amazon Elastic Compute Cloud (Amazon EC2)
- Management, monitoring, and automation layer around the DB engine
- Automated full DB instance backups, with point-in-time restore
- Automated high availability (HA)
- Automated provisioning, patching, monitoring, directory integration

LIMITATIONS

- Cannot run SSRS, SSIS, SSAS on the DB instance (works as data source)
- Maximum ~~30~~ 100 databases per instance
- No sysadmin role, server administrator, or direct file system access
  https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.MasterAccounts.html
- Not supported: MSDTC, maintenance plans, database mail

Amazon RDS for SQL Server

Continuously improved

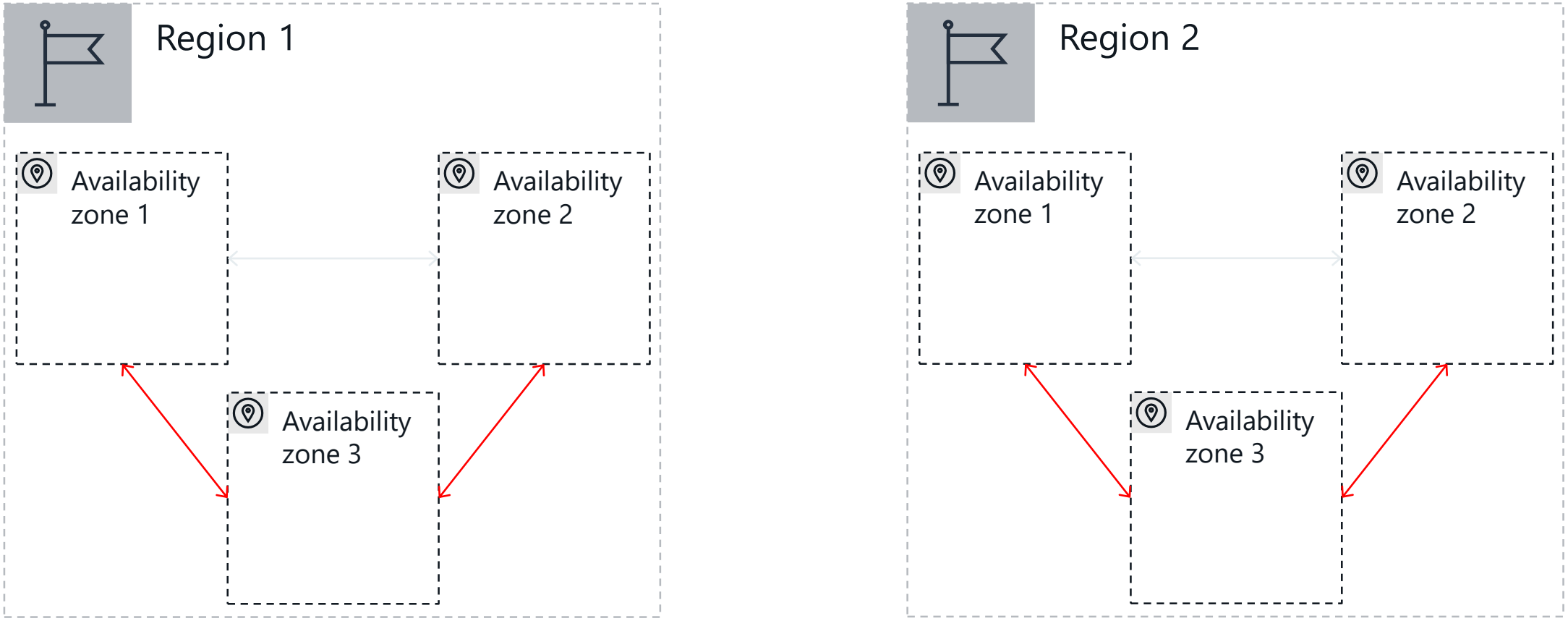
- Change server-level collation – August 6, 2019
- Multi-File native restores – June 5, 2019
- SQL Server Auditing – May 24, 2019
- Always On Availability Groups for SQL Server 2017 – May 23, 2019
- Increased database limit per database instance – May 22, 2019
- Performance insights – March 4, 2019

Agenda

- Introduction ✓
- (High) Availability
- Storage
- Security
- Backup and monitoring
- Data migration

Availability - concepts

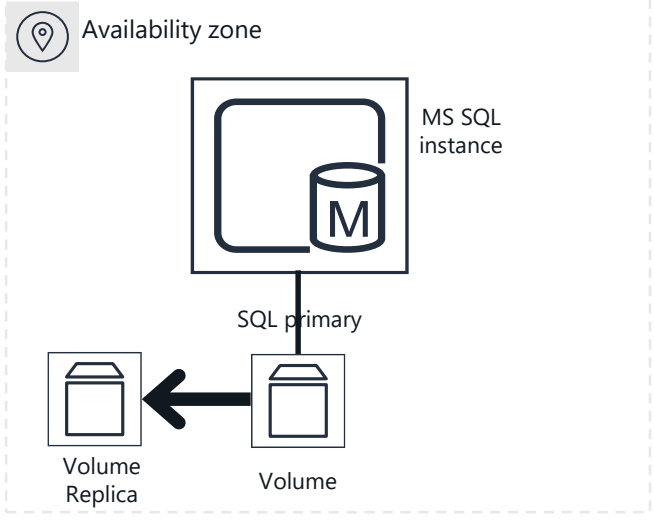
Regions and Availability Zones (AZs)



Availability - concepts

Single-AZ

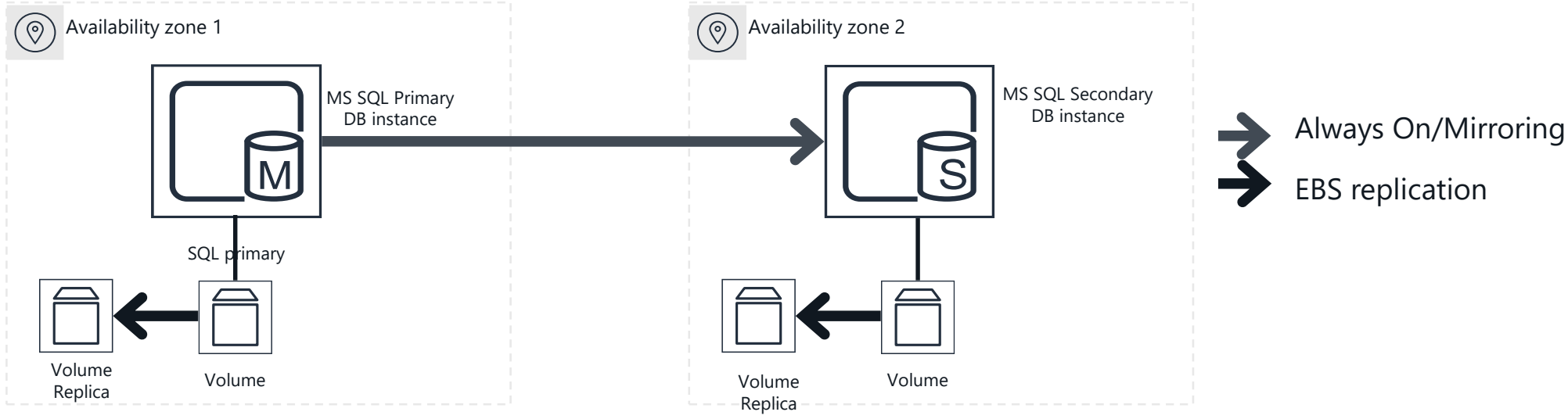
- Synchronous volume replication within AZ
- Recovery time varies from mins to several hours for AZ outages



Availability - concepts

Multi-AZ

- Synchronous volume replication within AZ and synchronous data replication across AZs
- Recovery time typically ~ 1 minute
- Uses Always On for 2016/2017 Enterprise Edition and DB Mirroring for other versions/editions
- Failover triggered by SQL Server



Availability - mirroring

AMAZON RDS FOR SQL SERVER MULTI-AZ DEPLOYMENT

- Fully managed and automated HA solution in an AWS region
- Principal and secondary DB nodes in different AZs
- Witness in a third AZ
- Leverages SQL Server DB mirroring
- Works with standard and enterprise editions
- DNS endpoint provided for app connectivity

CONSIDERATIONS

- Mirroring impact on change-heavy workloads

Availability - AlwaysOn

AMAZON RDS FOR SQL SERVER MULTI-AZ DEPLOYMENT

- SQL Server 2016 and 2017 Only
- Fully managed and automated HA solution in an AWS region
- Principal and secondary DB nodes in different AZs
- Leverages AlwaysOn (non-domain joined)
- Enterprise edition only
- Secondary node is completely passive
- DNS endpoint provided for app connectivity
  - AlwaysOn AG listener

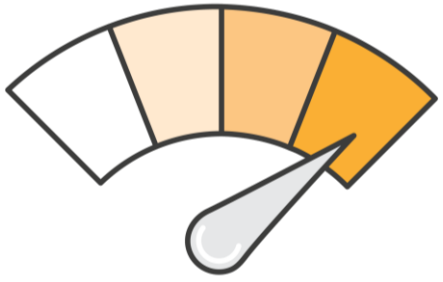
Agenda

- Introduction ✓
- Availability ✓
- Storage
- Security
- Backup and monitoring
- Data migration

Storage

AMAZON RDS STORAGE

- Low latency, persistent, network-attached block storage
- Easy to change after initial selection
- Maximum storage: **16 TB**
- Maximum IOPS: **32,000**
- Maximum throughput: **500** MiB/sec
- Amazon RDS **storage throughput** depends on DB instance class (see equivalent Amazon EC2 EBS optimized instance type)
- Keep in mind this includes TempDB



MONITORING I/O EFFICIENCY

- Amazon CloudWatch metric **average queue depth**
  - I/O requests waiting to be serviced

Agenda

- Introduction ✓
- Availability ✓
- Storage ✓
- Security
- Backup and monitoring
- Data migration

Security– tenets

1. **Restrict Access**
   Security Groups. Network ACLs. Subnets.
2. **Audit Access**
   SQL Server Audit. SQL Server trace.
3. **Encrypt Data**
   TDE. KMS. SSL.

Security

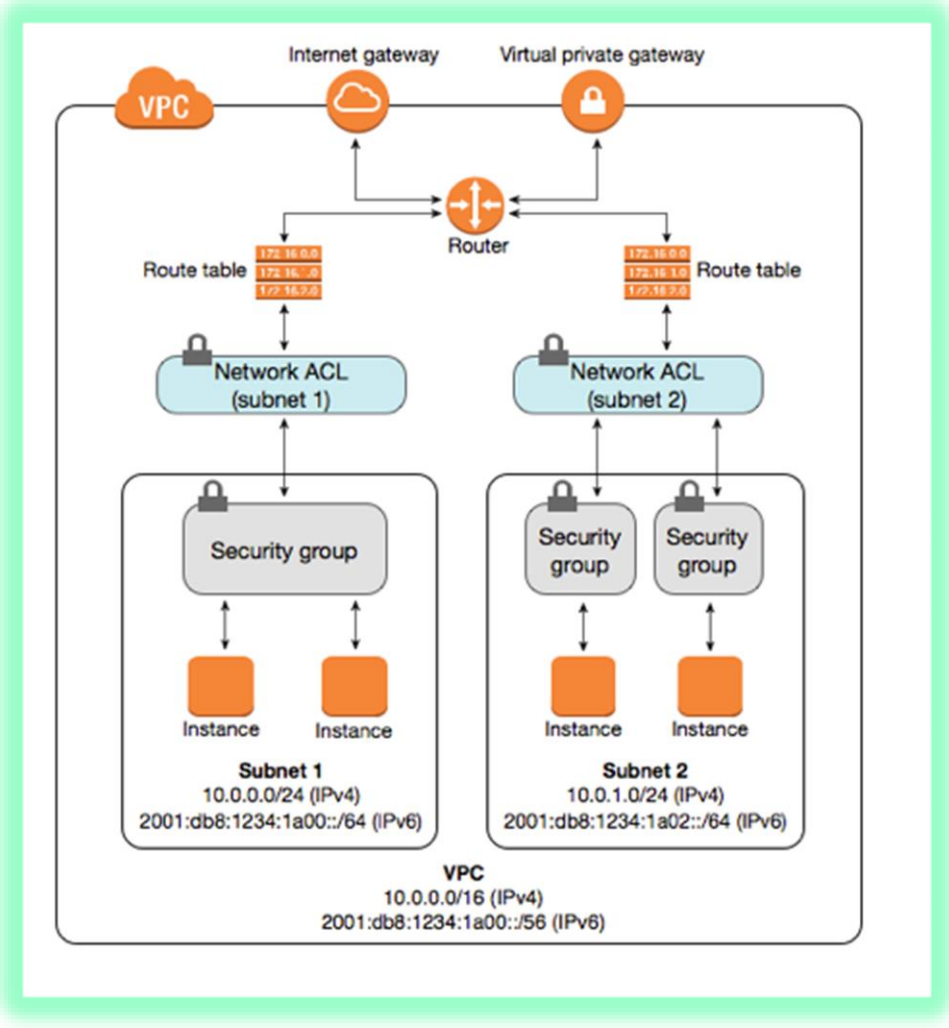
Restrict Access :

Use AWS Identity and Access Management (IAM) accounts to control access to Amazon RDS API actions

Restrict database accessibility

Avoid enabling public access

Avoid using port 1433



Security – auditing

Audit Access:

Enable rds.sqlserver_audit in the parameter group

Audit Action Groups enabled

SERVER_PERMISSION_CHANGE_GROUP
SERVER_PRINCIPAL_CHANGE_GROUP
SERVER_PRINCIPAL_IMPERSONATION_GROUP
SERVER_ROLE_MEMBER_CHANGE_GROUP
BACKUP_RESTORE_GROUP
DBCC_GROUP
SERVER_OPERATION_GROUP
SERVER_STATE_CHANGE_GROUP
SERVER_OBJECT_CHANGE_GROUP
SUCCESSFUL_LOGIN_GROUP
FAILED_LOGIN_GROUP
LOGOUT_GROUP
AUDIT_CHANGE_GROUP

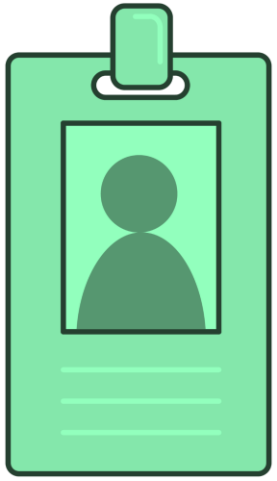
DATABASE_PERMISSION_CHANGE_GROUP
DATABASE_PRINCIPAL_CHANGE_GROUP
DATABASE_OWNERSHIP_CHANGE_GROUP
DATABASE_PRINCIPAL_IMPERSONATION_GROUP
DATABASE_ROLE_MEMBER_CHANGE_GROUP
DATABASE_OBJECT_ACCESS_GROUP
DATABASE_OBJECT_CHANGE_GROUP
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
FAILED_DATABASE_AUTHENTICATION_GROUP

Security – auditing contd.

Audit Access :

Enable SQL Server Auditing

- Compression by default : up to 80% compression
- Retain audit files on the server for quick access



Edition \ Version	2012/2014	2016/2017
Enterprise	Server and DB level	Server and DB level
Standard/Web/Express	Server level	Server and DB level

SQL Server 2008 R2 trace example

```
-- Create a trace file max size of 50MB called LogionTraceTest:
DECLARE @file_name NVARCHAR(245) = 'D:\RDSDBDATA\Log\LoginTraceTest';
DECLARE @max_file_size BIGINT = 50;
DECLARE @on BIT = 1;
DECLARE @rc INT;
DECLARE @traceid INT;
EXEC @rc = sp_trace_create @traceid OUTPUT, 2, @file_name, @max_file_size

-- Set Audit events as needed. 14 --> Successful login ; 20 --> Failed login:
IF (@rc = 0) BEGIN
   EXEC sp_trace_setevent @traceid, 14, 6, @on --NTUserName
   EXEC sp_trace_setevent @traceid, 14, 7, @on --NTDomainName
   EXEC sp_trace_setevent @traceid, 14, 8, @on --Hostname
   EXEC sp_trace_setevent @traceid, 14, 9, @on --ClientProcessID
   EXEC sp_trace_setevent @traceid, 14, 10, @on --ApplicationName
   EXEC sp_trace_setevent @traceid, 14, 11, @on --LoginName
   EXEC sp_trace_setevent @traceid, 14, 12, @on --SPID
   EXEC sp_trace_setevent @traceid, 14, 14, @on --StartTime
   EXEC sp_trace_setevent @traceid, 14, 15, @on --EndTime
   EXEC sp_trace_setevent @traceid, 14, 23, @on --Success
   EXEC sp_trace_setstatus @traceid, 1
END
```

SQL Server 2008 R2 trace example contd.

```
-- Reading the created trace file
select
StartTime,EndTime,Success,ClientProcessID,LoginName,SPID,Hostname,ApplicationName,NTUse
rName,NTDomainName FROM fn_trace_gettable('D:\rdsdbdata\Log\LoginTraceTest.trc',
default)where LoginName != 'NT AUTHORITY\SYSTEM';

-- Recording the trace file data to a table.
create database auditdb

select * into auditdb.dbo.logindata from
fn_trace_gettable('D:\rdsdbdata\Log\LoginTraceTest.trc', default) where LoginName !=
'NT AUTHORITY\SYSTEM';

insert into auditdb.dbo.logindata select * FROM
fn_trace_gettable('D:\rdsdbdata\Log\LoginTraceTest.trc', default) where LoginName !=
'NT AUTHORITY\SYSTEM';
```

Security

Encrypt Data: At rest

Enable storage encryption – AWS Key Management Service (AWS KMS)

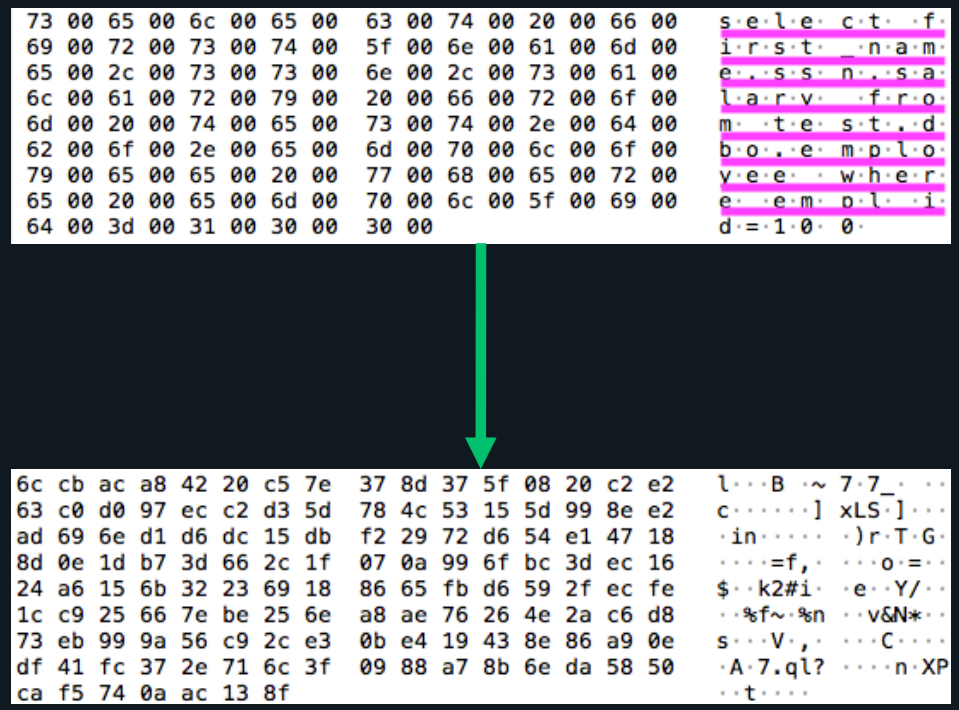
- Transparent to application
- No additional cost
- Minimal performance impact
- Log backups are also encrypted
- Supported across all editions

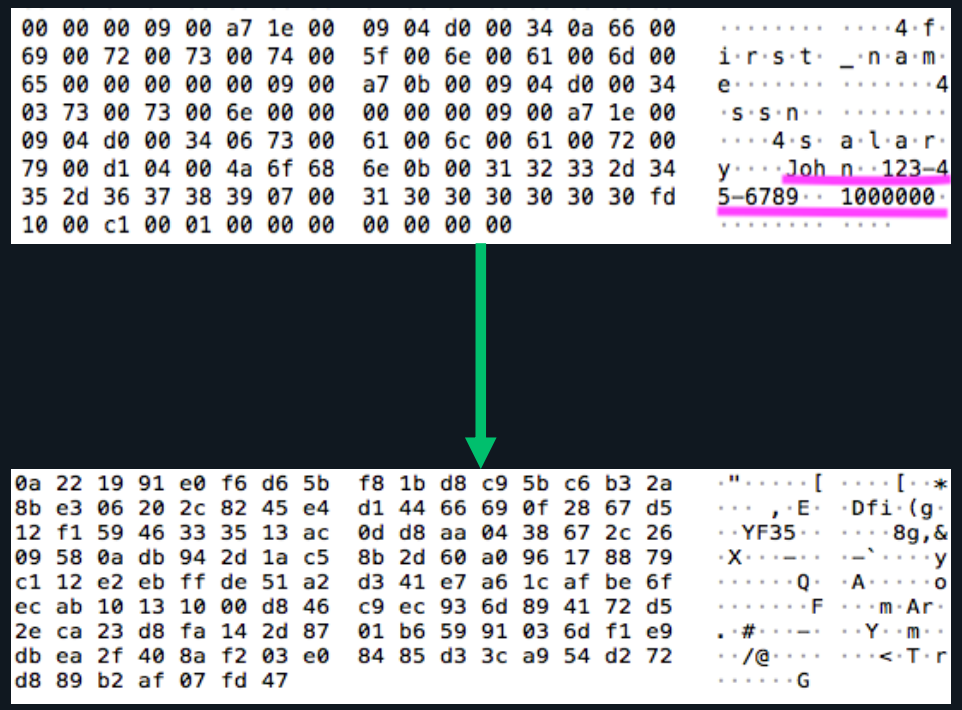
Transparent Data Encryption for Enterprise Edition

Security – encryption contd.

Encrypt Data: in-transit

Set rds.force_ssl : Forces all client connections to be encrypted





Agenda

- Introduction ✓
- Availability ✓
- Storage ✓
- Security ✓
- Backup and monitoring
- Data migration

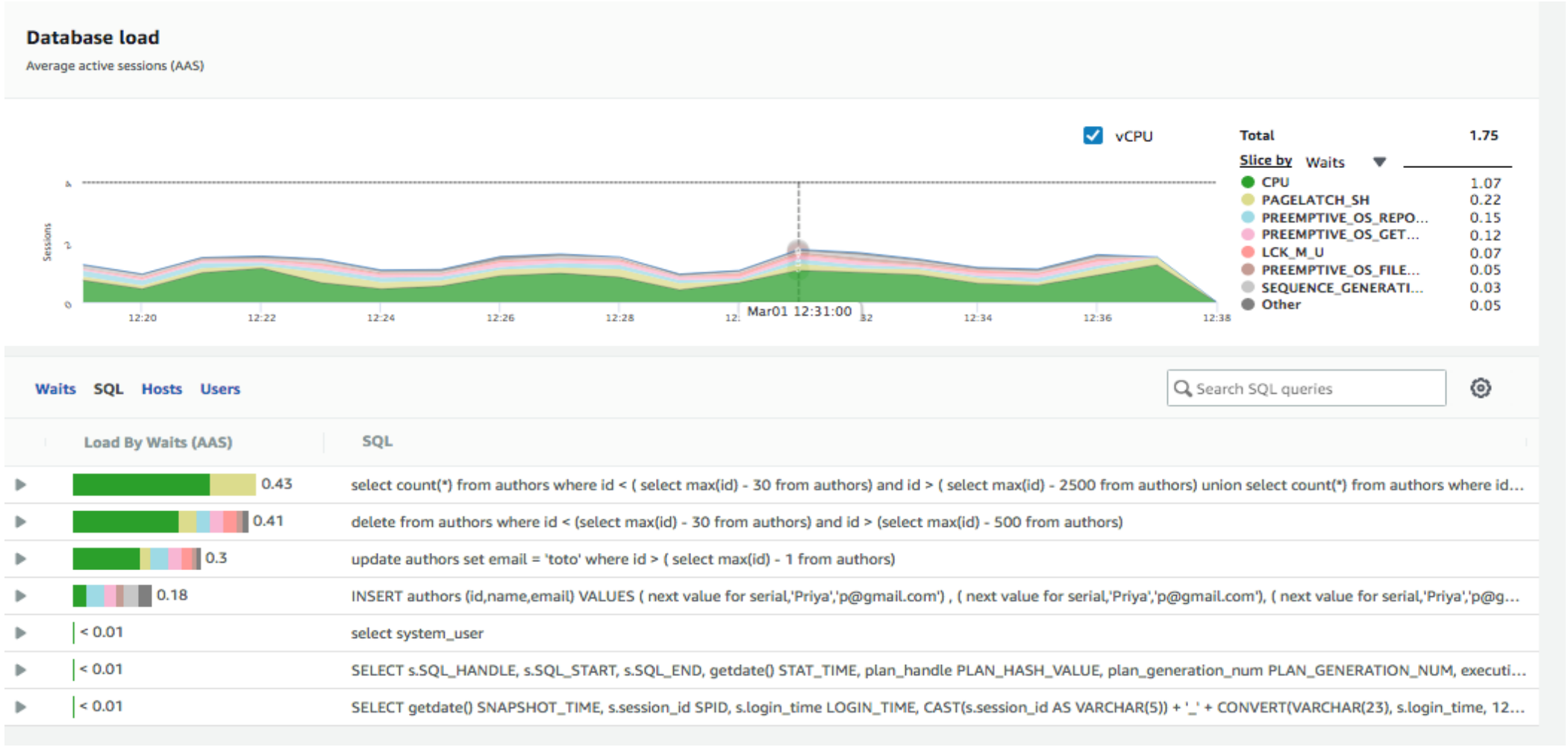
Backup - concepts

- Automatic snapshots taken daily
  - Transaction log backups every five minutes are streamed directly to Amazon S3
  - Snapshots and logs retained for the configured interval
  - Restore of a snapshot *always* creates a new instance
  - You can take manual snapshots (they are retained forever)
  - Reminder: This is a snapshot of *all* databases
- Native backup/restore
  - Native backups are always *copy only* to not break transaction log chain
  - Native restore will always be to the point of the backup, not point in time
- Practice restoring!
  - Understand the performance profile in particular after a restore
  - How long will it take? How long before the Amazon Elastic Block Store (Amazon EBS) volumes fully restored from S3?

Monitoring

- SQL Server agent
  - Job scheduling (rebuild index, DBCC checks etc.)
  - Some alerting
  - No DB mail
- CloudWatch
  - Enhanced monitoring available
  - Job scheduler available
  - Strategic direction of RDS is to integrate for monitoring
- Performance insights
  - Common RDS management interface
  - Monitors slow queries, etc.
- Third parties: AppDynamics, SQL Sentry, etc.

Performance insights



Agenda

- Introduction ✓
- Availability ✓
- Storage ✓
- Security ✓
- Backup and monitoring ✓
- Data migration

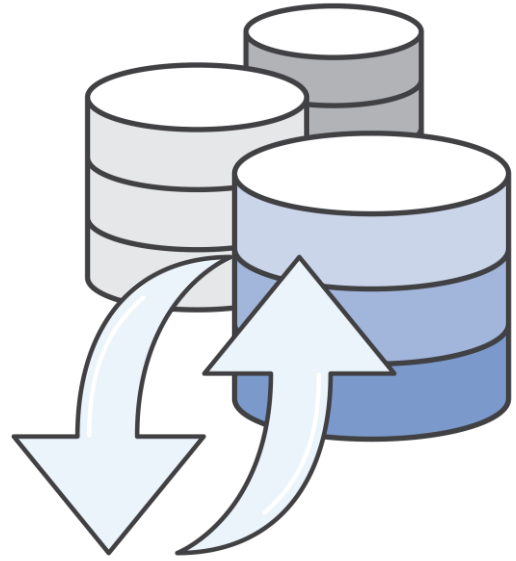
RDS SQL Server data movement

1. .BAK file import and export
   Leverages SQL Server's native backup functionality

2. Database publishing wizard, import/export, bulk copy
   Use **bcp**; export to T-SQL files & load using **sqlcmd**

3. AWS Database Migration Service (AWS DMS)
   Supports heterogeneous migrations in and out (CDC)

4. AWS Marketplace
   Third-party data import and export tools and solutions



AWS Popup Loft Bucharest

Date: November 11-15, 2019

Time: 9:00 – 5:30

Location: Impact Hub Timpuri Noi, Bucharest

Thank you! Multumesc!

Q&A and contact info

- madarasa@amazon.com
- https://dragos.madarasan.com
- @dragospm

Sponsors

Global SQL Saturday Partners

Microsoft Azure

PASS

Sponsors and Partners

Microsoft

Domino's

UBISOFT

Esential Training

GENOS

Please evaluate THIS event!

- Overall event
  https://www.sqlsaturday.com/915/EventEval.aspx
- The sessions
  https://www.sqlsaturday.com/915/Sessions/SessionEvaluation.aspx

PASS SQLSATURDAY BUCURESTI | 05 OCT 2019