Certified Solution Architect – Professional

Contents

[**Section 3: Designing Solutions for High Availability and BusinessContinuity** 1](#_Toc28708567)

**12/31/2019**

# **Section 3: Designing Solutions for High Availability and Business Continuity**

* Business continuity and Disaster Recovery
* Resiliency and Fault Tolerant
* Redundancy and high availability
* Cost optimization
* Performance
* Security
* Monitoring
* Saleable and Elasticity
* Ease of deployment
* Migration and Hybrid architectures

Fault Tolerant: Ability of a system/application/infrastructure to be operational even if one or more system fails is call fault tolerant. A fault tolerant system should be the one which can recover/failover with minimal or no human interventions on a even of any failure.

AWS recommended to create a library of own AMI, with own standard & best practice. Ensure the AMI is up to date and stable for production usages.

Floating IP (elastic IP) = the IP that can be shift from the primary instance to secondary on an event of any failure.

Create regular EBS snapshots – EBS are region specific, to be used in another region we need to copy the snapshot to the desired region before creating the EBS volume from that snapshot. EBS are region specific and EBS volume are AZ specific.

Multiple site architecture: In this approach the goal is to have two or more independent copy of each application stack into two or more availability zone (site). Every application tier need to have redundant copy , in case of failure the traffic can be route to the alternative availability zone (site) – this can further be made more effective by introducing elastic load balance which can automatically route traffic between AZ, OR having a route53 health check created to route traffic between different region, alternatively one can also use elastic ip for routing traffic, so that when the instance fails the elastic ip can be remapped to another running instance in same/different AZ. Implement Autoscaling to address flatulating production load.

**01/01/2020**

Disaster Recover – Recovery plan from a system failure to resume business continuity without impacting business operation.

|  |  |
| --- | --- |
| **Benefit of having AWS as alternative site** | **Counter Argument** |
| Don’t need to negotiate contract with other provide in another region. | Avoiding vendor locking – have a multi-vendor/multi-cloud landscape. |
| One can use the same underline AWS technology across region | Need to have trained staff in more than one cloud technology – will be cost intensive to maintain multi talent pool. |
| One can use same tool/AWS build artifacts/API across region | One need to maintain different tool/build artifacts/APIs for different cloud. |

**Recovery Time Objective (RTO) –** Time taken after a disruption to restore a business process to its service level agreement as define by the operational level argument (OLA).

**Recovery Point Objective (RPO)** – Acceptable amount of data loss measure in time. For example, If the disruption occurs at 12 Noon and RPO is 15 minutes, the system should be successfully able to restore all its transactions which have occur till 11:45AM.

Note: RPO and RTO is defined by the financial impact to the business when systems are unavailable.

* Disaster Recovery Plan for Commute from AMI backup aspect:
* AMIs can help in restoring failed instance quickly.
* AMIs can be used within the context of the autoscaling to scale out DR site on an event of primary site failure.
* AWS recommended to maintain a library of preconfigure AMIs, including the application stack, so that on an event of a disaster these can be used to create new (EC2) instances to replace the old/failed once.
* Keep the AMIs available on DR sites.
* Disaster Recovery Plan for Storage from S3 Fault tolerance aspect [FOR OBJECT STORAGE]:
* Can be used as primary object storage.
* Highly redundant, with 99.99999999999 (11 9’s) redundancy rate. Objects stored within S3 buckets are automatically backed up in multiple facilities within the region.
* Additional security can be provided within S3 bucket for ensure high degree of data retention through MFA for delete operation, versioning, cross region replication – for auto backup in DR site, bucket level policies & object level policies.
* One can also use S3 Glacier storage class for archiving/storing data at very LOW COST, however RTO needs to be set to meet the recovery time as object archive in S3 Glacier takes longer time (usually 3-5 hours).
* Disaster Recovery Plan for Storage from EBS Fault tolerance aspect [FOR BLOCK STORAGE]:
* Point-in-Time snapshot can be created to backed up EBS content into S3 bucket.
* Snapshot created can be use to create a new EBS volume & then connect it the EC2 instance to replace failed EBS volume.
* EBS volume data are stored in different system within the Availability Zone (AZ), this provide protection from single system failure within AZ.
* Disaster Recovery Plan for Storage from Storage Gateway prospective
* Storage gateway provides an easy means to backup/store on-premises data on to AWS cloud. Customer can download VMware image from AWS console, and install a VM instance from the same on premises which will provide NFS/iSCSI interface for backup/storage.
* Storage Gateway – File Gateway: files are asynchronously backed up into S3 bucket, there is a one-to-one mapping between on premises files and S3 objects. User can ALSO access the S3 objects(files) from the S3 bucket. S3 sub resources like lifecycle policy, versioning etc. can be implemented on the uploaded file(objects).
* Storage Gateway – Volume Gateway (Cached | Storage Mode): Unlike File gateway, in case of the volume gateway, on premises files are stored into S3 bucket as BLOCK store. There are two possible operating modes – *Cached Mode* where frequently use files are cached on-premises while its asynchronously backed up on S3 bucket as volume store, in *Storage Mode* there is NO local file store everything is backed up on S3 as EBS snapshot. One can’t access the files stored in S3 directly – to access the files one need to create EBS volume from form the snapshot (*in case of cache mode, first snapshot needs to create from the volume store prior to creating EBS volume*).
* Storage Gateway – Tape Gateway: it provides an iSCSI VTL (Virtual Tape Library) interface to backed up on premises files into virtual tape data store within S3 bucket or can be achieve into S3 Glacier. It consists of virtual media changer, virtual tape drive, and virtual tapes.
* Disaster Recovery Plan for Storage from AWS Import/Export prospective:
* If large amount of data needs to migrate (backed up) quickly into AWS one can use AWS import/export feature – solution like snowball, snowball edge and snowmobile can be leverage for the same.
* Rule of thumb – “*if the data takes more than week to transfer over the available connection (VPN/Direct Connection/Open internet), then better use AWS import export instead*”.
* Disaster Recovery Plan for Storage from VM Import/Export prospective:
* Ease means to transfer VM image from/to AWS.
* This can be helpful in creating DR site at AWS or on premises.
* NOTE: VM Export is ONLY AVAILABLE to those instances which are initially brought in using VM import feature. AMI based EC2 instance cannot be exported using AWS Export feature.
* Disaster Recovery Plan for Storage from RDS Fault Tolerance aspect:
* RDS Multi-AZ: Primary-to-Secondary synchronous data replication within a region. On an event of any failure the primary db instance DNS entry will be automatically swapped with secondary db instance. Help in archiving zero downtime during system patching/upgrade.
* Read Replicas: For read intensive applications, a read-only db instance can be provide with asynchronous data replication from the primary instance. On an event of any failure read replicas can be promoted
* Automated Backup: Automated backup in conjunctions with transaction logs to help recover failed db instance with RPO upto 5 min.
* Manual Snapshot: this are necessary for backing up a db instance OR restoring a db instance in another region.