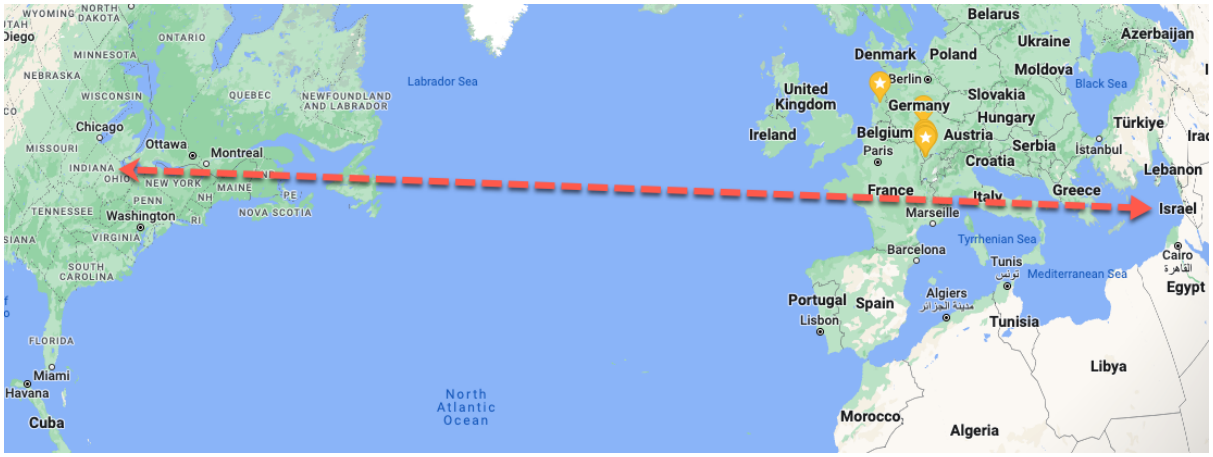
AWS-Architect- Final Project

Lovely company is a dating startup community platform for all ages. The company has local on premises site in Tel-Aviv & USA based on VMware architecture platform.

Currently there are 2 major sites in Israel & Indiana based on S2S VPN.



The company has the following challenges for migrating several services to the cloud based on AWS services and working as a hybrid platform, as followed by sections:

Physical & virtual environments

1. Lovely has 50 employees based on organizational units as follows:
    - **R&D** – 20 employees
    - **IT** – 10employees
    - **DevOps** – 10 employees
2. **Management** – Act as your central management account with no employee assignment except you.
3. R&D resources are based on Linux platform only
4. R&D & IT employees are divided between Indiana & Israel assets.
5. For simple deployment create max 5 employees for each account.

Account & billing architecture demands

1. Each OU needs its own AWS account according to its budget.
2. They need to get an alarm based on notification when the costs are greater than $5.
3. The relevant solutions need a management platform to manage all the relevant accounts in a single management platform, for business expense monitoring with relevant security policies for each OU.
4. R&D accounts have AWS services in the Europe and USA.
5. IT & DevOps have also used AWS services in the Europe and USA regions.

IT architecture demands

1. The identity provider for the company is Azure AD.
2. The CISO of the company is instructed to create an SSO solution based on MFA with Azure AD and AWS accounts.
    - **The current task is based on user provisioning & not a group based because it's not supporting in Azure free tier account.**
3. Only IT has root account access for all Lovely AWS accounts.
4. IAM local users are allowed only for auditing and monitoring by IT employees.
5. For cost savings, at the end of the date, automatically terminate all the unused instances or services.

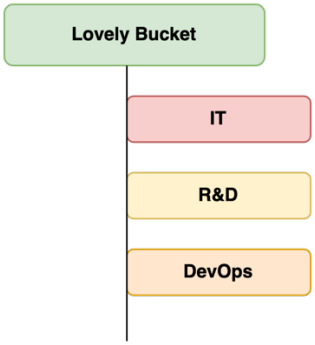
Network architecture demands

1. Lovely site in Israel needs to be connected securely to R&D based asset services in USA via S2SVPN Bidirectional.
    a. You can create a dedicated account or use one of the current to create S2S based on AWS services, instead of local VMware assets.
2. The network architecture needs to be based on public & private solutions.
3. Each account needs its own network segments for routing challenges.
4. Each region must have one or more VPCs for managing the network.
5. The R&D teams need a dedicated segment with up to 1,000 instances for test deployments.
6. The IT teams need a dedicated segment for up to 500 instances.

7. Only IT and DevOps accounts have granular access to manage all the network services in all AWS accounts.
8. Employees from R&D in USA must have route access to R&D in Europe network assets only – If you are not applying S2S (for external guest students).
9. The company's security policy for managing EC2 instances is to minimize the exposure of public addresses and to connect directly to private subnets.
10. All private networks need access to the internet for regular patching.
11. Access to AWS service is only allowed from Lovely on-premises assets & your home IP only.

IT architecture demands for resource sharing

All shared documents need to be in the S3 bucket with the current tree folders as follows:



1. According to permissions, each OU has only access to its own folder based on Entra-ID account.
2. All the files must be encrypted with dedicated symmetric key managed by you.
3. The storage must have redundancy with 3 copy's highly available and durable solution that preserves how users currently access the files.
4. For disaster recovery the CISO instruct to create another copy of the current bucket with minimal costs.
5. All the files must have a dedicated policy for 10 days safe before they are deleted – **the current challenge isn't supported by AWS with replication features, you can create a granular bucket to enable this feature** .
6. All the files can be restored to their previous state at any time.

7. The current bucket needs to be **shared** and **automatically** replicated for multiple regions, including the USA & Europe regions, while each side adds a file its automate the replica to other regions – **challenged**.
8. EC2 instance from the IT private subnet account must have a dedicated permissions for managing the bucket with minimal costs.

CISO architecture demands

1. Each account must have a role separation for a granular dedicated task.
2. You can use RBAC or ABAC based policy for applying the roles.
3. The administrator role is forbidden for day-to-day use.
4. Hardening & limiting network protocols as much as you can.
5. Encryption is a must implement for any service or protocol according to data in transit and data at rest.
6. HA solution must take consideration for any solutions.
7. The connection to EC2 based on port 22 must be enforced with a different key pair for each OU.
8. Only EC2 instances that run in the private subnets can have access for each AWS services.
9. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.
10. All the assets & services access are based on FQDN only.
11. All the images will be updated & managed only by IT OU. The images must contain the Lovely company logo, and shared for all accounts as base line infrastructure images.

R&D architecture demands

1. The main product of Lovely is the social meeting web site that based on WordPress architecture.
2. A company is developing a two-tier web application on AWS.
3. The company's developers will deploy the application on an Amazon EC2 instance that connects directly to a backend database and save the relevant page data on external shared file system.
4. The database engine must be relational & highly available.

5. To improve database performance, create a solution for offloading the primary server of the database engine - **challange**.
6. The application also must be highly available & scale up or down base on the usage time & available.
    - The CISO enforced to implement at least 2 instances in a different zone.
    - The CISO also enforces implement the web application solutions based on HTTPS protocol
7. **For disaster recovery if AWS regions fail, deploy at least a static web site or equivalent of the same web application on a different region.**
8. For the best user experience, the application latancy needs to be accessed and localized in the user's country - **challenge**.
9. The company must not hardcode database credentials in the application - **challenge**.
10. The company must also implement a solution to automatically rotate the database credentials on a regular basis – **challenge**.

Management architecture demands

1. **The whole project architecture needs to be drafted using in high-level design(HLD).**
2. **The R&D implantation needs to be drafted using low level design (LLD).**
3. **Make a summarize presentation for all your solution architect project.**
4. Use AWS services with cost management as part of your design.
5. As much as you can, try to automate your coding-based solution.

Instructor architecture demands

- Read several times the whole project before you start to implement
- Start your design by simple draft until you finalize the whole solution
- Try to simplify the process much as you can.
- The main clue for this project is: **God in details**.