**Project’s Requirements - Coverage**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| C | # | Task | Domain | How | Status | Resp |
| 1. **Physical & virtual environments** | | | | | | |
| A | 1 | Lovely has 50 employees based on organizational units as follows:   * + **R&D** – 20 emp.   + **IT** – 10 emp.   + **DevOps** – 10 emp. | Users |  | V |  |
| A | 2 | **Management** – Act as your central management account with no employee assignment except you. | Users |  | V |  |
| A | 3 | **R&D** resources are based on **Linux** platform only | Infrast. | Manually | - |  |
| A | 4 | **R&D** & **IT** employees are divided between **US** & **EU** assets. | Infrast.  Users | Policy – Private Subnet Access for each OU  >> NACL | Open |  |
| A | 5 | For simple deployment create max 5 employees for each account. | Users |  | V |  |
|  |  |  |  |  |  |  |
| 1. **Account & billing architecture demands** | | | | | | |
| B | 1 | Each **OU** needs its own AWS account according to its **budget** | Users | Coded. | V |  |
| B | 2 | They need to get an alarm based on notification when the costs are greater than $5. | Users | Coded. | V |  |
| B | 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** | Users | ->>  Security Policy for each OU | V  Open |  |
| B | 4 | **R&D** accounts have AWS services in the **Europe** and **USA** | Users  Network | Security Policy for each OU | Open |  |
| B | 5 | **IT** & **DevOps** have also used AWS services in the **Europe** and **USA** regions. | Users  Network | Security Policy for each OU | Open |  |
|  |  |  |  |  |  |  |
| 1. **IT architecture demands** | | | | | | |
| C | 1 | The **Identity Provider** for the company is **Entra ID.** | Infrast. |  | V |  |
| C | 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. | Infrast. | MFA not completed | V  Open |  |
| C | 3 | Only **IT** has **root account access** for all Lovely AWS accounts. | Users | Security Group | Open |  |
| C | 4 | **IAM** local users are allowed only for auditing and monitoring by IT employees. | Users | Security Group (Not required) | Open |  |
| C | 5 | For cost savings, at the end of the date, automatically terminate all the unused instances or services. | Infrast. |  | V |  |
|  |  |  |  |  |  |  |
| 1. **Network architecture demands** | | | | | | |
| D | 1 | Lovely site in EU needs to be connected securely to **R&D** based asset services in **USA** via **S2S VPN 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. | Infrast. | Irrelevant to Fargate solution. | V |  |
| D | 2 | The network architecture needs to be based on **public** & **private** solutions. | Infrast. |  | V |  |
| D | 3 | Each account needs its own network segments for routing challenges. | Users  Network | Policy required | Open |  |
| D | 4 | Each **region** must have one or more **VPCs** for managing the network. | Infrast. |  | V |  |
| D | 5 | The **R&D** teams need a dedicated segment with up to **1,000 instances** for test deployments. | Infrast. |  | V |  |
| D | 6 | The **IT** teams need a dedicated segment for up to **500** instances. | Infrast. |  | V |  |
| D | 7 | Only **IT** and **DevOps** accounts have granular access to manage all the network services in all AWS accounts. | Users | Policy | Open |  |
| D | 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). | --- | --- | --- | --- |
| D | 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. | Security  Network | Add NAT on EU  Add NAT to US AZ 1b | Open | Ron |
| D | 10 | All private networks need access to the internet for regular patching. | Network | After NAT addition and configuration | Open |  |
| D | 11 | Access to AWS service is only allowed from Lovely on-premises assets & your home IP only. | Security  Network | Route53 | V |  |
|  |  |  |  |  |  |  |
| 1. **IT architecture demands for resource sharing** | | | | | | |
| E | 1 | According to permissions, each **OU** has only access to its own folder based on Entra-ID account. | Users  Resourc |  | Open |  |
| E | 2 | All the files must be encrypted with dedicated symmetric key managed by you. | Resourc | Check if set | Open |  |
| E | 3 | The storage must have redundancy with 3 copy’s highly available and durable solution that preserves how users currently access the files. | Resourc | Not implemented |  |  |
| E | 4 | For disaster recovery the CISO instruct to create another copy of the current bucket with minimal costs. | Resourc | Glacier | Open |  |
| E | 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. | Resourc |  | Open |  |
| E | 6 | All the files can be restored to their previous state at any time. | Resourc | Versioning | Check |  |
| E | 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**. | Resourc  Network |  | --- |  |
| E | 8 | EC2 instance from the IT private subnet account must have a dedicated permissions for managing the bucket with minimal costs. |  | Policy | Open | Y |
|  |  |  |  |  |  |  |
| 1. **CISO architecture demands** | | | | | | |
| F | 1 | Each account must have a role separation for a granular dedicated task. | Users |  | Open | Y |
| F | 2 | You can use RBAC or ABAC based policy for applying the roles. | Resour. |  | Open |  |
| F | 3 | The administrator role is forbidden for day-to-day use. | Users |  | V |  |
| F | 4 | Hardening & limiting network protocols as much as you can. | Security | Security Policy | Open |  |
| F | 5 | Encryption is a must implement for any service or protocol according to data in transit and data at rest. | Security |  | V |  |
| F | 6 | HA solution must take consideration for any solutions. | Infrast |  | V |  |
| F | 7 | The connection to **EC2** based on port 22 must be enforced with a different key pair for each OU. | Security | Lambda ? – to establish EC2 – AMI preparation | Open |  |
| F | 8 | Only EC2 instances that run in the private subnets can have access for each AWS services. | Network | Policy | Open | Y |
| F | 9 | The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload. | Infrast |  | V |  |
| F | 10 | All the assets & services access are based on FQDN only. | Network |  | V |  |
| F | 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. | Users  Infrast | Not implemented. | -- |  |
|  |  |  |  |  |  |  |
| 1. **R&D architecture demands** | | | | | | |
| G | 1 | The main product of Lovely is the social meeting web site that based on WordPress architecture. | Infrast. | Flask | VxV |  |
| G | 2 | A company is developing a two-tier web application on AWS. | Infrast |  |  |  |
| G | 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. | Infrast | No no no | xV |  |
| G | 4 | The database engine must be relational & highly available. | Infrast | We used DynamoDB – non relational, fast replication. | V |  |
| G | 5 | To improve database performance, create a solution for offloading the primary server of the database engine – challenge. | Infrast | - | - |  |
| G | 6 | The application also must be highly available & scale up or down base on the usage time & available.  o The **CISO** enforced to implement at least 2 instances in a different zone.  o The **CISO** also enforces implement the web application solutions based on HTTPS protocol | Infrast  Security |  | V  V |  |
| G | 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. | Infrast | Implemented by TerraForm | V |  |
| G | 8 | For the best user experience, the application latancy needs to be accessed and localized in the user's country – challenge. | Infrast | - | - |  |
| G | 9 | The company must not hardcode database credentials in the application – challenge. | Infrast | - | - |  |
| G | 10 | The company must also implement a solution to automatically rotate the database credentials on a regular basis – challenge. | Infrast | - | - |  |
|  |  |  |  |  |  |  |
| 1. **Management architecture demands** | | | | | | |
| H | 1 | The whole project architecture needs to be drafted using in high-level design(HLD). | Design |  |  | Yuval |
| H | 2 | The **R&D** implantation needs to be drafted using low level design (LLD). | Design |  |  | Yuval |
| H | 3 | Make a summarize presentation for all your solution architect project. | Design |  |  | Yuval |
| H | 4 | Use AWS services with cost management as part of your design. | Design |  |  |  |
| H | 5 | As much as you can, try to automate your coding-based solution. | Infrast | Ahushiling | V |  |