**1.1 List all of the networking requirements for Daydreams Travel Agency based on the business needs in the case study. List the cloud resources needed to meet these requirements.**

| **Business Needs** | **Cloud Resource** | **Comments** |
| --- | --- | --- |
| Increased Storage | Amazon S3 | S3 standard single bucket in the local AWS region |
| Support for remote workers | AWS WorkSpaces | A managed, secure Desktop-as-a-Service (DaaS) solution |
| Scalable Computing Power | AWS EC2 | Virtual servers to handle increasing workloads |
| Database Services | Amazon RDS | Managed relational database service for ease of management |
| Network Security | AWS Security Group & Network ACLs | For controlling inbound and outbound traffic |
| Reliable Email Service | Amazon WorkMail | To provide reliable email services |
| Secure Remote Access | AWS VPN | For secure access to AWS resources |
| Networking | AWS VPC | Virtual private cloud for secure and isolated network setup |
| Network Traffic Monitoring | Amazon CloudWatch and VPC Flow Logs | For network monitoring and traffic analysis |
| Reliable Backup Service | AWS Backup | To automate backup processes and maintain data redundancy |

**1.2 Identify business and industry requirements**

The industry standards and guidelines include privacy laws, data protection laws, GDPR (if dealing with EU clients), and travel industry-specific regulations. You would also need to comply with Australian Privacy Principles under the Privacy Act 1988, Anti-Money Laundering and Counter-Terrorism Financing Act 2006, and the standards set by Australian Federation of Travel Agents for ethical practice and customer service.

**1.3 Identify security options for the virtual network based on AWS tools**

| **Security Tool** | **Applied To...** | **Comments** |
| --- | --- | --- |
| Amazon IAM | All components | Control and monitor access and identity; identify users and roles before configuring IAM |
| AWS Security Groups | EC2 instances | Control inbound and outbound traffic at instance level |
| Network Access Control Lists | Subnets | Control inbound and outbound traffic at subnet level |
| AWS Shield | Protection against DDoS attacks | Automated DDoS protection |
| AWS WAF (Web Application Firewall) | Web applications | Protect web applications from common web exploits |
| AWS Key Management Service (KMS) | Encryption keys for data security | Manage and control cryptographic keys |
| AWS Certificate Manager | Secure connections to AWS services and websites | Provision, manage, and deploy public and private SSL/TLS certificates for network communications |
| Amazon Macie | Data protection | Uses machine learning to recognize sensitive data such as PII |

Australian Privacy Principles under the Privacy Act 1988:

The Privacy Act 1988 is a federal law which regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information, and access to and correction of that information. The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act, outline how most Australian and Norfolk Island Government agencies, all private sector, and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information.

You can find more information on the official Office of the Australian Information Commissioner (OAIC) website: Australian Privacy Principles

Anti-Money Laundering and Counter-Terrorism Financing Act 2006:

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 is an Australian law to deter money laundering and financing of terrorism. It imposes a number of obligations on the financial sector, gambling sector, remittance (money transfer) services, bullion dealers and other professionals or businesses that provide services covered by the Act.

More information is available from the Australian Government's official AUSTRAC website: Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Standards set by Australian Federation of Travel Agents for ethical practice and customer service:

The Australian Federation of Travel Agents (AFTA) is a representative body which upholds professional standards within Australia's travel industry. Their ATAS - AFTA Travel Accreditation Scheme - provides criteria for ethical conduct, professional competency, and a process for handling complaints and disputes.

You can find more information and the AFTA Code of Ethics on the AFTA official website: ATAS - AFTA Travel Accreditation Scheme

Please note that this is a general guide and it is crucial that you review these legislations and standards thoroughly to ensure compliance. Additionally, consider seeking professional legal advice as needed.

|  |  |  |
| --- | --- | --- |
| Amazon S3 | Will provide storage for all DTA operations in the local geographical area | Via the AWS management console or AWS CLI, create a new S3 bucket in the selected region |
| Amazon EC2 | To host applications and provide scalable compute capacity | Deploy EC2 instances using the AWS management console, configure as per application requirements |
| AWS VPC | To create an isolated network for DTA's resources | Create a new VPC in AWS, configure subnets, route tables, and internet gateways |
| AWS IAM | Manage user access and permissions | Create IAM roles/policies for specific users or services to control access to AWS resources |
| Amazon RDS | Database service for managing relational databases | Setup RDS instances for application database requirements, ensuring proper security group settings |
| AWS VPN | To securely access DTA's network resources | Set up a Site-to-Site VPN connection between the on-premises network and AWS VPC |
| AWS Direct Connect | To establish a dedicated network connection from on-premises to AWS | Setup Direct Connect for consistent network performance |
| AWS Route 53 | To manage DNS and direct end-user requests to the application | Configure Route 53 to route users to application hosted on EC2 instances |
| Amazon CloudFront | To deliver content securely and with low latency | Set up CloudFront distribution for application to speed up distribution of files and secure applications |
| AWS CloudTrail | For governance, compliance, and auditing of AWS environment | Enable CloudTrail to log and retain account activity related to actions across AWS infrastructure |
| AWS CloudWatch | For monitoring resources and applications on AWS | Set up CloudWatch alarms and metrics to monitor EC2 instances and RDS databases |
| Amazon EBS | Provides persistent block storage for EC2 instances | Attach EBS volumes to EC2 instances for application data storage |
| AWS Lambda | To run code without provisioning or managing servers | Use Lambda to automate tasks such as image processing or log file analysis |
| Amazon S3 Transfer Acceleration | Speed up transfer of files over long distances | Enable S3 Transfer Acceleration for the S3 bucket to speed up uploads to the bucket |