Project Design Phase-**||**

**CLOUD DEPLOYMENT**

|  |  |
| --- | --- |
| NAME | T.SURESH KUMAR |
| NM ID | EA32343CFBC1AD09D4E465F983490A2F |
| PROJECT | HOW TO CREATE A GOOGLE ADS COMPAIGN FOR YOUR BRAND |

1. Select a Cloud Service Provider:

- Choose a cloud service provider, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure, based on your preferences, familiarity, and specific requirements.

2. Infrastructure Planning:

- Determine the type of infrastructure you need, including virtual machines, databases, and storage solutions.

- Set up virtual servers to host your web application, database, and other components.

3. Containerization and Orchestration:

- Consider using containerization technologies like Docker to package your application and its dependencies.

- Utilize container orchestration platforms such as Kubernetes to manage and scale containers efficiently.

4. Database Setup:

- Choose a database service provided by the cloud platform (e.g., Amazon RDS, Azure SQL Database, Google Cloud SQL) or set up your database server.

- Ensure that data storage and databases are secure and properly configured.

5. Network Configuration:

- Configure virtual networks and security groups to control traffic to and from your cloud resources.

- Ensure proper firewall rules and security measures are in place.

6. Web Application Deployment:

- Deploy your web application to the cloud servers.

- Use a web server (e.g., Nginx, Apache) to serve your application.

- Enable SSL/TLS for secure data transmission.

7. Google Ads API Integration:

- Securely configure the integration with the Google Ads API, ensuring that API credentials are stored safely.

- Implement authentication mechanisms for API access.

8. Data Storage and Backup:

- Implement data storage solutions such as cloud-based object storage (e.g., Amazon S3, Google Cloud Storage) for storing campaign data.

- Set up regular automated backups to prevent data loss.

9. Security Measures:

- Utilize cloud platform security features such as Identity and Access Management (IAM) to control user access and permissions.

- Implement firewall rules and security groups to protect your cloud resources.

- Employ encryption for data at rest and data in transit.

10. Monitoring and Logging:

- Set up monitoring tools provided by the cloud platform (e.g., AWS CloudWatch, GCP Stackdriver) to monitor system health and performance.

- Configure logging to capture system activities and application logs for debugging and auditing.

11. Scalability and Load Balancing:

- Consider using auto-scaling groups to automatically adjust resources based on demand.

- Implement load balancing to distribute traffic across multiple instances for improved availability and performance.

12. Disaster Recovery:

- Develop a disaster recovery plan to ensure data integrity and service availability in case of system failures.

- Regularly test the recovery plan to validate its effectiveness.

13. Documentation:

- Create comprehensive documentation that covers the cloud architecture, configurations, and procedures for maintaining and managing the system.

14. Continuous Optimization:

- Continuously monitor cloud resources and adjust configurations as needed for cost optimization and performance improvement.

15. Compliance:

- Ensure that your cloud deployment complies with relevant data protection and compliance standards.

16. Budget Management:

- Keep a close eye on cloud usage and associated costs to avoid unexpected expenses.