Question 1 Answer:

1. **Debugging steps:**
   1. Check the application monitoring dashboard for any issues that may direct troubleshooting.
      1. Are all configuration items (CIs) responding to health checks (ex: ping)?
      2. Are all services health checks ‘green’?
         1. Example: CPU, Disk, system services, web services, synthetic logins.
      3. Check that DNS resolution for the application returns the expected results.
   2. Via the bastion host, attempt to login to the server(s).
      1. Is the server responsive to commands?
      2. Are there any errors being printed to the console?
      3. Are there any other apparent errors?
      4. Are all expected services running?
   3. Were any changes scheduled for deployment prior to the incident?
   4. Check ALB target group health status.
   5. Check ALB target group configuration to confirm configuration as expected.
2. **The following tools and processes should be available to check system working fine or not**.
   1. **Systems monitoring.**
      1. Up/Down monitoring for the operating systems (ex: ping and response time)
      2. CPU, disk, and network usage monitoring.
      3. Services monitoring for baseline services expected to be running.
      4. Application services monitoring for customized application services (ex: web server, database server, custom services)
   2. **Application and database monitoring**
      1. Performance and availability monitoring for high-level application entry points
         1. HTTP 200 response codes to the front page
         2. Synthetic user logins to ensure higher level functionality and responsiveness.
      2. Database monitoring
         1. Database locks
         2. Long running or runaway queries
   3. **Centralized logging**
      1. A collection of logs from:
         1. Operating system (application, security, and system)
         2. Application logs (web server, tomcat, wordpress)
         3. Load balancers
         4. Firewalls
         5. Cloudwatch and Cloudtrail logs
         6. VPC flow logs
   4. **Information Technology Services Management tools**
      1. Change requests
      2. Prior issues with matching incident descriptions
3. **Improvements suggested**
   1. Based on the diagram and the assumptions the server, wpserver2, is not in the load balancer’s target group. If wpserver1 fails, the application will cease to function as the load balancer won’t know to send new requests to wpserver2.
   2. Update the target group for the application load balancer to include both servers.
   3. It is not clear, but RDS 1 may not be configured for multi-AZ redundancy. Confirm this configuration and investigate the costs and benefits of implementing this redundancy.
   4. Depending on the criticality of the application, a disaster recovery environment may be necessary to handle complete outages.