- **User Permissions:**
    - Define different user roles (admin, editor, viewer) with granular access levels (read, write, delete) to specific tables or data sets.
    - Implement the principle of least privilege - grant only the minimum permissions required for a user to perform their tasks.
    - Use strong passwords and enforce regular password changes.
- **Network Access:**
    - Restrict database access to authorized IP addresses or networks. This prevents unauthorized attempts from outside your trusted environment.
    - Configure firewalls to block access to database ports from untrusted sources.
- **Security Settings:**
    - Enable encryption for data at rest and in transit. This scrambles sensitive information making it unreadable in case of a breach.
    - Regularly review and update database security patches to address vulnerabilities.
    - Implement audit logging to track user activity and identify any suspicious access patterns.
- **Performance Optimization:**
    - Properly configure database schema to minimize redundant data storage and optimize query execution.
    - Monitor database performance metrics like query response times and resource utilization to identify bottlenecks.
    - Consider database tuning techniques like indexing frequently accessed columns to improve query speed.
- **Backups and Recovery:**
    - Establish a regular database backup schedule and store backups securely off-site. This ensures data recovery in case of hardware failure, software errors, or accidental data deletion.
    - Implement a disaster recovery plan outlining steps to restore database functionality in case of a major outage.