

# Knowledgebase (KB)



### All Categories

- HR Policies (40)
- Employee Performance Management System (0)
- Training (16)
- Utilities (2)
- Knowledge Sharing (15)
  - Mobile (0)
  - Others / Misc (6)
  - Web (3)
    - Database Guidelines
    - Hardware - Software Performance Guidelines
    - Hosting Guidelines
    - HTML-CSS-JS Guidelines
    - Neosoft Secure Coding Practices
    - Security Guidelines

There are no categories to display in knowledge base.

### Recently Viewed

- Hardware - Software Performance Guidelines
- Database Guidelines
- Business Conduct And Ethics
- Working Hours
- Workplace Policies

Home » Group Categories » Knowledge Sharing

## Hosting Guidelines

Article Number: 120 | Rating: 2/5 from 1 votes | Last Updated: Wed, Mar 30, 2016 at 1:05 PM

### Architecture

- 3 Tier Architecture is recommended, minimally implement 2 tier architecture
- Development Environment
  - Set up one more more environments for application. We recommend:
    - Development
    - Test
    - Staging/UAT
    - Production
  - Use separate instances of each component in the stack. e.g. Separate databases

### Shared

### Dedicated / VPS

- Except for HTTP & HTTPS (Port 80, 443). All ports should be closed.
- Use SFTP over FTP.
- Disable passphrase based SSH access, use Private / Public keys for authentication.
- Use Fail 2 Ban to block: IP, Port, Path, User on repeated failed authentication
- Firewall
  - Every machine should have firewall activated: Such as IPTables, FirewallD
  - SELinux must be activated
- Folder access
  - User should have limited access to file system
- Email
  - Use authenticated SMTP instead of mail()
- SSH should have idle session timeouts
- IP & User whitelisting: Whitelist specific IPs allowed to log-in the server as well as user
- Disk
  - Use different mount points for
    - /
    - /boot
    - /tmp
    - /webroot
- Automated Updates
  - Setup automated security updates
  - Avoid setting up automated software updates as it may cause backward incompatibility problems

### General

- Only Application layer should be exposed through public IP, rest of the architecture should be connected via intranet.
- Database should be accessible only through Application servers. Make sure IP restrictions for both public and private IPs are in place. Example: Only local IPs of Application servers should be able to access DB server

Posted by: PHP - Administrator - Wed, Mar 30, 2016 at 1:05 PM This article has been viewed 249 times.

Filed Under: Knowledge Sharing

### Article Rating (1 Votes)



You've Already Voted.

Bookmark Article (CTRL-D)

### Attachments

There are no attachments for this article.

### Related Articles

- Database Guidelines  
Viewed 448 times since Wed, Mar 30, 2016
- Security Guidelines  
Viewed 620 times since Wed, Mar 30, 2016
- Hardware - Software Performance Guidelines  
Viewed 317 times since Wed, Mar 30, 2016
- Neosoft Secure Coding Practices  
Viewed 908 times since Wed, Mar 30, 2016
- HTML-CSS-JS Guidelines

