Documentação de Troubleshooting

Problema: Erro de sintaxe DocumentRoot takes one argument

- **Descrição:** O comando sudo apachectl configtest retornou um erro de sintaxe na diretiva DocumentRoot, especificamente "DocumentRoot takes one argument, Root directory of the document tree".
- **Causa:** Caracteres invisíveis (como um espaço em branco no final da linha) ou um erro de digitação no caminho do DocumentRoot. O Apache é extremamente sensível a caracteres.
- **Solução:** Abrir o arquivo de configuração, apagar a linha e re-digitá-la manualmente para garantir a remoção de todos os caracteres invisíveis.

Problema: Apache falha ao iniciar com exit-code

- **Descrição:** O serviço apache2 falhou ao iniciar, conforme o sudo systemctl status apache2.service mostrou Active: failed (Result: exit-code).
- **Causa:** Erro fatal de configuração. Embora o teste de sintaxe apachectl configtest possa retornar Syntax OK, o Apache ainda pode falhar se não conseguir carregar os arquivos de certificado ou chave privada. As causas mais comuns são:
  1. **Permissões de arquivo incorretas:** O Apache (usuário www-data) não consegue ler a chave privada.
  2. **Chave e certificado não correspondem:** O openssl revela que os hashes MD5 de ambos os arquivos são diferentes.
- **Solução:**
  1. Verificar as permissões da chave privada (server.key), garantindo que ela seja legível apenas pelo usuário root (permissão 600).
  2. Verificar se a chave privada e o certificado correspondem usando openssl. Se os hashes MD5 forem diferentes, gerar um novo par de arquivos que correspondam.

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/server.key -out /etc/ssl/apache2/newreq.pem

Explicação do Comando

- `sudo openssl req`: Inicia o comando OpenSSL para criar e gerenciar pedidos de certificado.
- `-x509`: Modifica a saída do comando para gerar um certificado autoassinado em vez de um pedido de assinatura de certificado (CSR).
- `-nodes`: "No DES". Desabilita a criptografia da chave privada. Isso é útil para ambientes de desenvolvimento, pois evita que o Apache peça uma senha toda vez que

é iniciado.

- `-days 365`: Define a validade do certificado em dias. Neste caso, o certificado será válido por um ano.
- `-newkey rsa:2048`: Gera uma nova chave privada com o algoritmo RSA e um tamanho de 2048 bits. Este é um padrão de segurança amplamente aceito.
- `-keyout /etc/ssl/private/server.key`: Especifica o caminho para salvar a nova chave privada. O diretório `/etc/ssl/private/` é o local padrão e seguro para chaves privadas.
- `-out /etc/ssl/apache2/newreq.pem`: Especifica o caminho para salvar o novo certificado autoassinado.

Problema: O navegador exibe "Index of /" em vez do index.html

- **Descrição:** Ao acessar o site, o navegador mostra uma lista de diretórios e arquivos em vez do conteúdo da página inicial.
- **Causa:** O Apache não está configurado para procurar pelo arquivo index.html na raiz do site. O Virtual Host ignora a diretiva DirectoryIndex por causa de caracteres invisíveis no arquivo de configuração, ou a diretiva não está explicitamente definida.
- **Solução:**
  1. Adicionar a diretiva DirectoryIndex index.html ao Virtual Host do site.
  2. Re-digitar o arquivo de configuração inteiro, a partir do zero, para eliminar todos os caracteres invisíveis que poderiam causar o problema.

Problema: Navegador exibe aviso de "Conexão não é segura"

- **Descrição:** O navegador mostra um aviso de segurança e um cadeado riscado na barra de endereços, indicando que o site não é seguro.
- **Causa:** O site está usando um certificado autoassinado (não emitido por uma Autoridade de Certificação confiável). Navegadores como o Chrome não confiam em certificados autoassinados por padrão.
- **Solução:** Este é um comportamento normal e esperado para ambientes de desenvolvimento. Para remover o aviso, o certificado autoassinado precisa ser importado para o repositório de certificados confiáveis do sistema operacional.

Conclusão Geral: O Apache é rigoroso com a sintaxe. Erros aparentemente pequenos, como espaços em branco ou caracteres invisíveis, podem ter um grande impacto. A melhor abordagem para solucionar problemas é verificar a sintaxe, as permissões de arquivo, a correspondência entre chave e certificado, e, se tudo isso falhar, recriar o arquivo de configuração do zero.