

CTI - GLPI

Manual de instalação, atualização e configuração do sistema GLPI

- [Considerações Gerais](#)
- [Instalação](#)
- [Backup e Restauração do Banco de Dados](#)
- [Atualização](#)
- [Configuração](#)

Considerações Gerais

Na Instalação realizada em 17/03/2025 foi utilizado o Sistema Operacional Ubuntu 24.04 LTS e a versão do GLPI 10.18

A opção pelo S.O Ubuntu Server se deu devido ao seu longo suporte, até 2029, e pela característica da Canonical de manter seus pacotes em versões mais recentes, comparado ao Debian. O GLPI passa por constantes atualizações de segurança sendo ideal que o S.O ofereça os pacotes mais recentes dos recursos necessários para sua execução como php, apache, mysql ou mariadb etc.

No Virtualizado Proxmox PVEP foi criado uma VM (136) chamada GLPI com as configurações da imagem abaixo:

Virtual Machine 136 (GLPI) on node 'pvep' No Tags  

	Add	Remove	Edit	Disk Action	Revert
Summary					
Console					
Hardware					
Cloud-Init					
Options					
Task History					
Monitor					
Backup					
Replication					
Snapshots					

Memory	8.00 GiB
Processors	8 (2 sockets, 4 cores) [host] [numa=1] [cpulimit=4]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/ubuntu-24.04.2-live-server-amd64.iso,media=cdrom,size=3137758K
Hard Disk (scsi0)	local-lvm:vm-136-disk-1,discard=on,iothread=1,size=60G,ssd=1
Network Device (net0)	virtio=BC:24:11:6A:4E:81,bridge=vbr0,firewall=1,tag=50
Unused Disk 0	local-lvm:vm-136-disk-0

Também foi adicionado no processo de backup e redundância de backup em disco USB.

O IP de acesso da VM é 10.116.50.10 e nome da maquina passou a ser GLPI com acesso tambem podendo ser realizado por glpi.ti.srt.ifsp.edu.br

Portanto, em 17/03/2025, foi feita uma nova instalação do GLPI e os passos para um futura nova instalação ou atualização podem ser consultados nas paginas desse livro.

Instalação

Abaixo segue o passo a passo a ser executado para concluir a instalação do GLPI. Foram seguidas orientações do portal oficial do GLPI que pode ser acessado no link: <https://glpi-install.readthedocs.io/pt/latest/>

1. Atualizar o Sistema Operacional

```
sudo apt update && sudo apt dist-upgrade -y
```

2. Reconfigurar o timezone

```
sudo dpkg-reconfigure tzdata
```

3. Reiniciar para aplicar as configurações

```
sudo shutdown -r now
```

4. Instalar Apache, PHP e MySQL e dependências necessárias

```
apt install -y \  
apache2 \  
mariadb-server \  
mariadb-client \  
libapache2-mod-php \  
php-dom \  
php-fileinfo \  
php-json \  
php-simplexml \  
php-xmlreader \  
php-xmlwriter \  
php-curl \  
php-gd \  
php-intl \  
php-mysqli \  
php-bz2 \  
php-zip \  
php-exif \  
php-ldap \  
php-opcache \  
php-mbstring
```

5. Criar banco de dados do glpi

```
mysql -e "CREATE DATABASE glpi"  
mysql -e "GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' IDENTIFIED BY 'senha'"  
mysql -e "GRANT SELECT ON mysql.time_zone_name TO 'glpi'@'localhost'"  
mysql -e "FLUSH PRIVILEGES"
```

6. Carregar timezones no MySQL

```
mysql_tzinfo_to_sql /usr/share/zoneinfo | sudo mysql -u root mysql
```

7. Desabilitar o site padrão do apache2

```
a2dissite 000-default.conf
```

8. Criar o virtualhost do glpi

```
cat << EOF | sudo tee /etc/apache2/sites-available/suporte.conf
<VirtualHost *:80>
ServerName suporte.ti.srt.ifsp.edu.br
DocumentRoot /var/www/glpi/public
<Directory /var/www/glpi/public>
Require all granted
RewriteEngine On
# Ensure authorization headers are passed to PHP.
# Some Apache configurations may filter them and break usage of API, CalDAV, ...
RewriteCond %{HTTP:Authorization} ^(.+)$
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

# Redirect all requests to GLPI router, unless file exists.
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>
EOF
```

9. Configuração de segurança para sessões

Para aumentar a segurança, é recomendável configurar sessões PHP com as seguintes configurações:

session.cookie_secure: deve ser definido on quando o GLPI puder ser acessado somente no protocolo HTTPS;

session.cookie_httponly: deve ser definido on para impedir que scripts do lado do cliente acessem valores de cookies;

session.cookie_samesite: deve ser definido, pelo menos, como Lax, para evitar que cookies sejam enviados em solicitações POST de origem cruzada (entre domínios).

Acesso o arquivo /etc/php/8.3/apache2/php.ini, procure os parâmetros acima e altere conforme orientação.

10. Habilitar o virtualhost

```
sudo a2ensite glpi.conf
```

11. Habilitar módulos do Apache necessários

```
sudo a2enmod rewrite
```

12. Reinicia o apache para entrar em vigor

```
sudo systemctl restart apache2
```

13. Download do glpi

```
wget -q https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz
```

ou ultima versão disponível no github

14. Descompactar a pasta do GLPI

```
tar -zxf glpi-*
```

15. Mover a pasta do GLPI para a pasta htdocs

```
sudo mv glpi /var/www/glpi
```

16. Configurar a permissão na pasta www/glpi

```
sudo chown -R www-data:www-data /var/www/glpi/
```

17. Finalizar setup do glpi pela linha de comando

```
sudo php /var/www/glpi/bin/console db:install \  
--default-language=pt_BR \  
--db-host=localhost \  
--db-port=3306 \  
--db-name=glpi \  
--db-user=glpi \  
--db-password=senha
```

18. Remover o arquivo de instalação

```
sudo rm /var/www/glpi/install/install.php
```

19. Mover pastas do GLPI de forma segura

O GLPI armazena alguns dados no filesdiretório, a configuração de acesso ao banco de dados é armazenada no configdiretório, etc. Mesmo que o GLPI forneça algumas maneiras de impedir que os arquivos sejam acessados diretamente pelo servidor web, a prática recomendada é armazenar os dados fora da raiz web. Dessa forma, arquivos confidenciais não podem ser acessados diretamente do servidor web.

```
mv /var/www/glpi/files /var/lib/glpi  
mv /var/www/glpi/config /etc/glpi  
mkdir /var/log/glpi  
chown -R www-data:www-data /var/lib/glpi  
chown -R www-data:www-data /etc/glpi  
chown -R www-data:www-data /var/log/glpi
```

20. Mover pastas do GLPI de forma segura | conf-dir

```
cat << EOF | sudo tee /var/www/glpi/inc/downstream.php  
<?php  
define('GLPI_CONFIG_DIR', '/etc/glpi/');  
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
```

```
require_once GLPI_CONFIG_DIR . '/local_define.php';
}
EOF
```

21. Mover pastas do GLPI de forma segura | data dir

```
cat << EOF | sudo tee /etc/glpi/local_define.php
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
EOF
```

22. Pós-instalação

Depois que o GLPI estiver instalado, você estará quase pronto.

Uma etapa extra seria proteger o diretório de instalação. Como exemplo, você pode considerar adicionar o seguinte à configuração do seu host virtual Apache (ou ao glpi/install/.htaccessarquivo):

```
<IfModule mod_authz_core.c>
Require local
</IfModule>
<IfModule !mod_authz_core.c>
order deny, allow
deny from all
allow from 127.0.0.1
allow from ::1
</IfModule>
ErrorDocument 403 "<p><b>Restricted area.</b><br />Only local access allowed.<br />Check your configuration or contact your administrator.</p>"
```

Neste exemplo, o acesso ao diretório de instalação será limitado apenas ao host local e exibirá uma mensagem de erro caso contrário

23. Primeiros Passos

4.1. Acessar o GLPI via web browser

4.2. Criar um novo usuário com perfil super-admin

4.3. Remover os usuários glpi, normal, post-only, tech.

4.3.1. Enviar os usuários para a lixeira

4.3.2. Remover permanentemente

4.3.4. Configurar a url de acesso ao sistema em: Configurar -> Geral -> Configuração Geral -> URL da aplicação.

Após a conclusão o acesso ao GLPI deve estar concluído.

Backup e Restauração do Banco de Dados

Em dado momento, devido a atualização ou problema como servidor, pode ser necessário a realização de um backup e restauração do banco de dados.

1 - Dump do banco de dados

cd /var/www/glpi/files/_dumps (para acessar a pasta de dump do glpi e poder salvar o banco de dados nela)

mysql -u root -p "show databases" (para visualizar os bancos de dados existentes no mysql)

mysqldump -u root -p glpi > glpi_bkp.sql (para fazer um backup do banco de dados).

tail -1 glpi_bkp.sql (para verificar se o backup foi realizado com sucesso).

2 - Criar uma base de dados limpa para restauração

```
mysql -e "CREATE DATABASE glpi"
```

```
mysql -e "GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' IDENTIFIED BY 'senha"
```

```
mysql -e "GRANT SELECT ON mysql.time_zone_name TO 'glpi'@'localhost'"
```

```
mysql -e "FLUSH PRIVILEGES"
```

3 - Importar o banco de dados

```
mysql -u glpi -p glpi < glpi_bkp.sql
```

Atualização

Importante Realizar um backup ou snapshot no gerenciador de virtualização antes de realizar atualização.

Foram seguidas as orientações oficiais do portal do glpi.

<https://glpi-install.readthedocs.io/pt/latest/update.html>

<https://www.youtube.com/watch?v=lwVLAJWflcA>

Abaixo estão os passos a seguir para realizar a atualização do GLPI.

1 - Fazer update e upgrade do SO.

```
apt install && dist-upgrade
```

2 - Realiza backup do banco de dados.

Seguir passo do manual contido no portal

3 - Realizar backup do diretório config e das chaves config/glpi.key e config/glpicrypt.key;

Realizar copia das pastas e dos arquivos

4 - Backup do diretório files e marketplace.

Realizar copias das pastas

5 - Acesse a pasta do glpi /var/www

```
cd /var/www/glpi
```

6 - Altere o nome da pasta completa

```
mv glpi glpi_old
```

7 - Faça o download a versão nova

```
wget -q https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz
```

ou ultima versão disponível no github

8 - Extrair a versão nova

```
tar -zxvf nome do arquivo.
```

9 - Restaure os diretórios e arquivos que foram realizados backup.

Copie de volta os arquivos e pastas do passo 3 e 4

10 - Abra o navegador e acesso o site do GLPI

Siga as orientações para finalizar a atualização.

Configuração

Apos a instalação concluída algumas configurações deve ser realizadas para que o GLPI possa capturar e-mails em uma caixa de entrada e gerar chamados automaticamente, configurações para que ao realizar tratativas no chamado aberto o solicitante seja notificado e editar o crontab do sistema operacional para forçar a execução das ações automáticas afim de manter o sistema sempre em operação.

1 - Configuração do Crontab

Como usuário root no linux execute o comando

```
# contrab -e
```

Adicione a linha abaixo para que seja executado o arquivo cron.php do glpi a cada 1 minuto

```
* * * * * php /var/www/glpi/front/cron.php
```

2 - Configuração das Notificações

2.1 Modelos de Notificação

O GLPI traz modelos de notificações pré-configurados que podem ser modificados conforme necessidade. A notificação referente ao chamado pode ser customizada alterando o item Tickets.

2.2 Notificações

É possível editar quais notificações serão enviadas para os requisitantes.

2.3 Configuração de acompanhamentos por e-mail

Nessa opção é realizado a configuração da conta de e-mail que realizará o envio das notificações.

Notificação por e-mail

Endereço de e-mail do administrador: suporte.cti.srt@ifsp.edu.br

Nome do administrador: Suporte CTI IFSP Sertãozinho

Mode de envio de e-mails: SMTP+SSL

Servidor de E-mail

Verificar Certificado: Sim

Servidor do SMTP: smtp.gmail.com

Porta: 465

Login do SMTP: suporte.cti.srt@ifsp.edu.br

Senha do SMTP: senha do e-mail

3 - Configuração dos Destinatários

Nesta etapa é configurado a conta de e-mail que irá realizar a coleta dos mensagens para abertura e atualização dos chamados.

Clique em adicionar e insira as informações abaixo.

Nome: suporte.cti.srt@ifsp.edu.br

Ativo: Sim

Servidor: imap.gmail.com

Opções de Conexão: IMAP - SSL

Usuário: suporte.cti.srt@ifsp.edu.br

Senha: senha

Adicionar usuários CC como observador: Não

Coletar apenas e-mails não lidos: Sim

Conforme orientação da reitoria, não é possível adicionar um grupo de e-mails dentro de outro grupo de e-mails. Sendo assim, para que o grupo suporte.cti.srt@ifsp.edu.br seja responsável por coletar e enviar mensagens dos também grupos de e-mails cti.srt@ifsp.edu.br e portal.srt@ifsp.edu.br foi necessário a utilização de um e-mail comum do gmail, o cti.srt.ifsp@gmail.com.

Nessa solução o e-mail comum do gmail está adicionado nos grupos cti.srt@ifsp.edu.br e portal.srt@ifsp.edu.br de modo que ele receba os e-mails desses grupos e encaminhe para o suporte.cti.srt@ifsp.edu.br mantendo os remetentes originais. Essa alternativa permite que o GLPI, por meio do suporte.cti.srt capture também as mensagens enviadas para os grupos cti.srt e portal.srt.

Configurações

Geral Marcadores Caixa de entrada Contas e importação Filtros e endereços bloqueados Encaminhamento e POP/IMAP Complementos

Chat e Meet Avançado Off-line Temas

Encaminhamento:

[Saiba mais](#)

- Desativar encaminhamento
- Encaminhar uma cópia do e-mail de entrada para e

Dica: Você também pode encaminhar apenas alguns dos seus e-mails [criando um filtro!](#)

O E-mail comum suporte.cti.srt@gmail.com atua de forma transparente para os requisitante e para a o GLPI. Ele possui 15 GB de espaço, conforme contas comuns da Google, e na data de 24/04/2025 estava com 37% utilizado. Verificar com periodicidade de 1 ano e fazer uma limpeza para que a caixa de mensagem não fique cheia e possíveis problemas ocorram.

As senhas de acesso a esses grupos e e-mail comum estão guardadas no arquivo de senhas.

4 - Administração das Regras

Algumas regras ja vem disponibilizadas por padrão ao instalar o sistema. Dentre elas, a utilizada atualmente é a Regra de Negócios para Chamados.

Nessa regra é possível definir um grupo de usuários que terão acesso aos e-mails coletados por um dos Destinatários configurados.

A regra CTI encaminha para o grupo CTI todas as mensagens coletadas pelo e-mail suporte.cti.srt@ifsp.edu.br

Regra - CTI

Adicionar novo critério

Critério	Condição	Motivo
<input type="checkbox"/> Destinatário de e-mail	é	suporte.cti.srt@ifsp.edu.br

5 - Grupos de Usuários

O Grupo de usuários é configurado para permitir que regras seja aplicadas. No caso de uso da CTI, um grupo de usuários CTI é criado com todos os integrantes do setor. Assim, quando um e-mail é coletado e aberto um chamado, a regra adiciona automaticamente o grupo CTI e todos os seus integrantes passam a ter acesso ao chamado.

Caso o GLPI seja utilizado por mais de um setor, é possível configurar regras para que a coleta de e-mails direcione o chamado para outros Grupos. Como por exemplo, a configuração de um

destinatário do Patrimônio, com e-mail cap.srt@ifsp.edu.br, e um grupo CAP, pode receber todos os chamados enviados para o seu destinatário e os demais grupos não teria acesso.

6 - Categorias dos Chamados

Foi criada algumas Categorias de Chamados com a finalidade de mapear os atendimentos realizados na CTI. Dessa forma é possível extrair relatórios para análise e melhor distribuição de tarefas.

7 - Aplicação de mecanismos de segurança sugeridos pela ETIR

A ETIR elaborou um documento com boas praticas de segurança para os Servidores Apache

<https://manuais.ifsp.edu.br/books/apache-web-server-hardening-e-boas-praticas-de-seguranca-para-diminuicao-da-superficie-de-ataque-dos-ativos>

Seguindo o manual da ETIR foram aplicadas as configurações abaixo:

7.1 - Habilitando configurações de segurança nos cabeçalhos do servidor Apache

<https://manuais.ifsp.edu.br/books/apache-web-server-hardening-e-boas-praticas-de-seguranca-para-diminuicao-da-superficie-de-ataque-dos-ativos/page/habilitando-configuracoes-de-seguranca-nos-cabecalhos-do-servidor-apache>

Alteração do arquivo `/etc/apache2/conf-enabled/security.conf`

```
# Oculta versão do servidor (exibe apenas "Apache")
```

```
ServerTokens Prod
```

```
# Remove assinatura do Apache nas páginas de erro e diretórios
```

```
ServerSignature Off
```

```
#Ocultar o nome real do servidor apache2
```

```
SecServerSignature "nginx"
```

```
# Proteção contra Cross-site Scripting (XSS)
```

```
Header set X-XSS-Protection "1; mode=block"
```

```
# Impede carregamento de políticas cross-domain (Flash, etc)
```

```
Header set X-Permitted-Cross-Domain-Policies "none"
```

```
# Força o valor do cabeçalho "Host" (protege contra Host header injection)
```

```
RequestHeader set Host "meudominio.com.br"
```

```
# ATENÇÃO: Substitua por seu domínio ou IP público válido!
```

```
# Remove cabeçalhos suspeitos que podem ser usados para spoofing ou fingerprinting
```

```
RequestHeader unset X-Forwarded-Host
```

```
Header always unset X-Powered-By
```

```
Header unset X-Powered-By
```

```
Header unset X-CF-Powered-By
```

Header unset X-Mod-Pagespeed

Header unset X-Pingback

Aplica HSTS: obriga conexões via HTTPS (por 6 meses)

Header always set Strict-Transport-Security "max-age=15768000; includeSubDomains; preload"

⚠ ATENÇÃO: Ative somente se HTTPS já estiver funcionando corretamente!

Impede que o site seja carregado em iframes externos (protege contra clickjacking)

Header set X-Frame-Options "SAMEORIGIN"

Impede que o navegador tente adivinhar o tipo de conteúdo

Header set X-Content-Type-Options "nosniff"

7.2 - Desativar a listagem ou a indexação de diretórios do servidor Apache

<https://manuais.ifsp.edu.br/books/apache-web-server-hardening-e-boas-praticas-de-seguranca-para-diminuicao-da-superficie-de-ataque-dos-ativos/page/desativar-a-listagem-ou-a-indexacao-de-diretorios-do-servidor-apache>

Edite o arquivo `/etc/apache2/apache2.conf`

mude este bloco

```
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

para

```
<Directory /var/www/>
    Options FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

7-3 - Desabilitando o `/server-status` do modo público

O que é o `/status-server`?

É um módulo Apache que ajuda a monitorar a carga do servidor web e as conexões httpd atuais através de uma interface HTML que pode ser acessada através de um navegador web. Esta interface exibe configurações estritamente técnicas e por isso sensíveis do host. Por este motivo não deve estar publicada.

Por que o `/status-server` está público?

As últimas versões dos servidores web Apache, trazem por padrão uma restrição de acesso a esta página, através da configuração do `mod_status`, retornando o erro 403 Forbidden (restrito) em caso de tentativa de acesso. Porém, há casos em que esta página se encontra pública por algum

erro na configuração do servidor, expondo estas informações. Voltamos a reforçar, quem nem mesmo para fins de monitoramento estas informações devem ficar desprotegidas e públicas, pois são extremamente sensíveis e aumentam consideravelmente a superfície de ataque a este host.

Como posso tratar essa configuração?

A forma mais eficaz e geral para a solução desta falha de configuração, é informar ao servidor que ele não deve mais exibir estas informações para IPs ou ranges de IPs não autorizados, com isso, ele passará a exibir o código 403 - Forbidden (restrito) em casos de tentativas de acesso à URL. Esta configuração não tem impacto negativo para as aplicações hospedadas por este servidor, além de ser uma boa prática de segurança.

O seguinte procedimento deve ser realizado: Bloquear o acesso de IPs não autorizados à URL /server-status no servidor através de parâmetro na configuração no Apache;

Edite o arquivo `/etc/apache2/mods-enabled/status.conf`

Procure pelo bloco "`<Location /server-status>`" Mantenha a linha "`SetHandler server-status`" como está, descomentada.

Caso queira deixar acessível apenas ao localhost, deixe descomentada a linha "`Require local`".

Caso queira ampliar o acesso a algum outro ip ou faixa de IPs da sua rede, descomente a linha "`Require ip`" e defina o IP ou Range. Reinicie o serviço do apache após a alteração e veja qual a mensagem exibida quando você tentar acessar a URL.

O retorno esperado é o erro 403 (Forbidden), não exibindo mais as informações sobre o host.

Também pode-se optar pela remoção do módulo `mod_status` do Apache, caso não faça uso da funcionalidade:

Para efetuar a remoção do módulo você deve executar o comando "`sudo a2dismod status`".

Reinicie o serviço do apache após a alteração e veja qual a mensagem exibida quando você tentar acessar a URL.

O retorno esperado é o erro 404 (Not Found), não exibindo mais as informações sobre o host.

7.4 Eliminando protocolos SSL e TLS antigos do servidor Apache

Faça o teste inicial dos protocolos do seu servidor, a partir de um computador remoto:

```
openssl s_client -connect SEU_HOST:443 -tls1 (protocolo inseguro - conexão deve falhar)
```

```
openssl s_client -connect SEU_HOST:443 -tls1_1 (protocolo inseguro - conexão deve falhar)
```

```
openssl s_client -connect SEU_HOST:443 -no_tls1_1 -no_tls1_2 -no_tls1_3 -no_tls1 (teste do sslv3 - protocolo inseguro - conexão deve falhar)
```

```
openssl s_client -connect SEU_HOST:443 -tls1_2 (protocolo seguro - conexão ter sucesso)
```

```
openssl s_client -connect SEU_HOST:443 -tls1_3 (protocolo seguro - conexão ter sucesso)
```

Edite o arquivo `/etc/apache2/mods-available/ssl.conf`

Modifique estes parâmetros de

```
SSLCipherSuite HIGH:!aNULL
```

```
SSLProtocol all -SSLv3
```

para

```
SSLCipherSuite "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384"
```

```
SSLProtocol +all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

Se você usa Let's Encrypt, VERIFIQUE ESTES PARÂMETROS ADICIONAIS:

Edite o arquivo `/etc/letsencrypt/options-ssl-apache.conf`

Compare individualmente os parâmetros abaixo com os mesmo parâmetros do arquivo de configuração, e modifique-os de acordo com o exemplo abaixo:

SSL Engine on

```
# Intermediate configuration, tweak to your needs
#SSLProtocol          all -SSLv2 -SSLv3
SSLProtocol +all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite          ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
SSLHonorCipherOrder    on
SSLCompression         off
```

```
sudo systemctl restart apache2.service
```

Refaça o teste inicial dos protocolos do seu servidor, a partir de um computador local remoto:

Quando fizer a alteração em produção, faça o antes e depois com este testador:

<https://www.ssllabs.com/ssltest>

7.5 - Diretórios e Arquivos Sensíveis que não devem ter acesso público

Alguns arquivos e diretórios podem fornecer informações sensíveis a terceiros, portanto, o recomendado é que os acessos a eles sejam impedidos ou limitados.

Abaixo listaremos e atualizaremos constantemente, mediante testes, a lista de arquivos sensíveis que devem ser limitados ou bloqueados:

Edite o arquivo `/etc/apache2/apache2.conf`

Procure pela seção que tenha a tag "FilesMatch" e adicione o código ao fim desta seção:

```
<Location /server-status>  
    Deny from all  
</Location>
```

Depois reinicie o serviço do apache.

```
sudo systemctl restart apache2
```