FTP

1 VSFTPD

1.1 Pre instalação

1.1.1 Verificar a disponibilidade da porta 21 (ou da porta que o cliente preferir utilizar na conexão FTP).

```
netstat -pln | grep 21
```

1.2.1 Caso precise liberar as portas no firewall

```
ufw allow 20/tcp
```

```
ufw allow 21/tcp
```

1.3.1 Preparar para instalar.

```
sudo apt-get update
```

1.2 INSTALAÇÃO

1.2.1 Instale com o comando

```
apt-get install vsftpd -y
```

1.2.2 Inicia o serviço

```
systemctl start vsftpd
```

1.2.3 Habilita a inicializar com o sistema

```
systemctl enable vsftpd
```

1.3 CONFIGURAÇÃO

1.3.1 O arquivo de configuração vsftpd.conf deve estar em /etc (/etc/vsftpd.conf). Realize um backup do arquivo de configuração.

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.bckp
```

1.3.2 Abrir o arquivo para a configuração e inclua (se já não houver) os parâmetros:

```
userlist_enable=YES
userlist_deny=NO
vim /etc/vsftpd.conf
```

1.3.3 Userlist

Caso não exista, crie o arquivo /etc/vsftpd.userlist. Ele abrigará os usuários que tem acesso permitido ao ftp (somente eles).

```
sudo vim /etc/vsftpd.userlist
```

Nele liste os usuários no arquivo - em formato de lista (somente o usuário sem nenhum outro parâmetro).

Exemplo:

```
usuario1
usuario2
usuario3
```

1.2 Operação do Daemon

1.2.1 Verifica o status do serviço.

```
systemctl status vsftpd
```

1.2.2 Inicia o serviço.

```
systemctl start vsftpd
```

1.2.3 Reinicia o serviço.

```
systemctl restart vsftpd
```

1.2.4 Para o serviço.

```
systemctl stop vsftpd
```

1.2.5 Torna o serviço inicializavel com o sistema.

```
systemctl enable vsftpd
```

1.3 Opções de configuração.

1.3.1 Impede o login anônimo. Se seu servidor de FTP for público, o valor deve ser YES

```
anonymous_enable=NO
```

1.3.2 Isto permite que os usuários locais efetuem o login. Útil para um servidor privado (nosso caso) como o de um ISP.

```
local_enable=YES
```

1.3.3 Permite que esses usuários escrevam em suas pastas por FTP.

```
write_enable=YES
```

1.3.4 Define as permissões dos arquivos depois do upload. O padrão é 077 (octal), escrita e leitura somente pelo dono.

```
local_umask=022
```

1.3.5 Ativa o upload anônimo. Este valor deve ser YES se o servidor de FTP for público.

```
anon_upload_enable=NO
```

1.3.6 Ativa a criação de pastas por usuários anônimos.

```
anon_mkdir_write_enable=NO
```

1.3.7 Permite que o conteúdo do arquivos .message seja exibido caso exita no diretório atual. Um bom uso deste recuso é criar o arquivo .message (o conteúdo deve ser texto puro) e colocar informações sobre a pasta atual.

```
dirmessage_enable=YES
```

1.3.8 Ativa o log detablhado, que inclui log de upload e download.

```
xferlog_enable=YES
```

1.3.9 Permite conexões na porta 20 (ftp-dados).

```
connect_from_port_20=YES
```

1.3.10 Se esta opção estiver habilitada, cada upload de arquivo executado pelo usuário anônimo terá automaticamente, como dono do arquivo, o usuário especificado na opção chown_username. Não é recomendado que seja feito upload com o usuário root

```
chown_uploads=YES
```

1.3.11 Permite especificar qual usuário será o dono dos arquivos que forem enviados para o servidor (upload) pelo usuários anônimo.

```
chown_username=whoever
```

1.3.12 Pode ser especificado em qual arquivo serão registrados os logs do serviço vsftpd. O padrão é /var/log/vsftpd.log.

```
xferlog_file=/var/log/vsftpd.log
```

1.3.13 Se estiver habilitado, o arquivo de log será gerado no formato padrão do ftpd xferlog.

```
xferlog_std_format=YES
```

1.3.14 Define o tempo de desconxão automática por inatividade.

```
idle_session_timeout=1800
```

1.3.15 Tempo permitido de ociosidade (em segundos) em uma conexão antes que o cliente remoto seja desconectado.

```
data_connection_timeout=120
```

1.3.16 Esta opção é recomendada para definir um usuário único do sistema, o qual será utilizado pelo servidor FTP que seja totalmente isolado e sem privilégios. Geralmente escolhe-se o usuário nobody.

```
nopriv_user=ftpsecure
```

1.3.17 Com esta opção ativada, o vsftpd irá carregar uma lista de nome de usuários a partir do arquivo especificado em userlist_file. Se o usuário tentar conectar usando um nome da lista, ele será PROIBIDO de fazer o login. Mesmo digitando a senha corretamente, terá um retorno de erro de acesso.

```
userlist_enable=YES
```

1.3.18 Esta opção só será examinada userlist_enable esteja ativada. Ela faz com que os usuários da lista userlist_file sejam negados antes mesmo de solictar a senha. Isso serve para impedir login com senhas nulas, chamadas de cleartext (texto puro).

```
userlist_deny=YES
```

1.3.19 Nesta opção pode ser especificado um arquivo, o qual conterá o nome dos usuários a serem negados pela opção userlist_enable.

```
userlist_file=/etc/vsftpd.user_list
```

1.3.20 Quando esta opção é habilitada, um comando do FTP conhecido como async ABOR é ativado. Alguns clientes de FTP mais antigos podem apresentar problemas se esta opção não estiver habilitada, porém ela representa um furo na segurança.

```
async_abor_enable=YES
```

1.3.21 Quando habilitada, o modo ASCII de transferência de dados é ativado para uploads.

```
ascii_upload_enable=YES
```

1.3.22 Quando habilitada, o modo ASCII de transferência de dados é ativado para downloads.

```
ascii_download_enable=YES
```

1.3.23 O banner de boas vindas, quando é feito login no servidor FTP, pode ser personalizado.

```
fptd_banner=Bem Vindo ao FTP
```

1.3.24 Endereços de e-mails anônimos podem ser desabilitados, ou seja, isso proibirá o login de usuários que possuem esse endereços. Prático para combater ataques do tipo DOS.

```
deny_email_enable=YES
```

1.3.25 Esta opção anda em conjunto com a deny_email_enable. Pode-se especificar um arquivo onde estarão listados os endereços de e-mails que serão banidos.

```
banned_email_file=/etc/vsftpd.banned_emails
```

1.3.26 Define que o usuário conectado deve ficar preso num diretório raiz. Esta opção é útil em servidores de hospedagem.

```
chroot_local_user=YES
```

1.3.27 Habilita uma lista de usuários que estarão presos em um diretório raiz.

```
chroot_list_enable=YES
```

1.3.28 Esta opção define qual é o arquivo que irá conter a lista de usuários para chroot.

```
chroot_list_file=/etc/vsftpd.chroot_list
```

1.3.29 Define a execução do vsftpd em modo standalone. Se definido como YES, requer background=YES. Se for iniciado pelo xinetd, deve ficar no NO.

```
listen=YES
```

1.3.30 Ativa a exibição dos nomes de usuários e grupos nas listagens de arquivos e diretório. Se definido como NO serão exibidos do IDs.

```
text_userdb_names=YES
```

1.3.31 Determina a exibição das datas em local time zone.

```
use_localtime=YES
```

1.3.31 Esta opção habilita a utilização do comando ls -R. Não é muito útil já que isso, em grandes diretórios, pode consumir muito recurso.

```
ls_recurse_enable=YES
```

1.3.32 Segurança: por questões de segurança, pode-se evitar que determinados usuários conectem via FTP. Se esta opção for ativada o vsftpd lerá uma lista de nomes que está na opção do userlist_file(/etc/vsftpd/ftpdusers). Se o usuário tenta acessar o sistema tiver o nome nesse arquivo, terá seu acesso negado antes que sua senha seja perguntada.

```
userlist_enable=YES
```

1.4 Opções Booleanas

Abaixo está uma lista de opções booleanas. O valor de uma opção booleana pode ser definido como YES ou NO . allow_anon_ssl Aplica-se apenas se ssl_enable estiver ativo. Se definido como SIM, os usuários anônimos poderão usar conexões SSL seguras. Padrão: NÃO

anon_mkdir_write_enable Se definido como SIM, os usuários anônimos poderão criar novos diretórios sob certas condições. Para que isso funcione, a opção write_enable deve estar ativada e o usuário de ftp anônimo deve ter permissão de gravação no diretório pai. Padrão: NÃO

anon_other_write_enable Se definido como YES, os usuários anônimos terão permissão para executar operações de gravação diferentes de upload e criação de diretório, como exclusão e renomeação. Isso geralmente não é recomendado, mas incluído para completar. Padrão: NÃO

anon_upload_enable Se definido como SIM, usuários anônimos poderão fazer upload de arquivos sob certas condições. Para que isso funcione, a opção write_enable deve estar ativada e o usuário de ftp anônimo deve ter permissão de gravação nos locais de upload desejados. Essa configuração também é necessária para o upload de usuários virtuais; por padrão, os usuários virtuais são tratados com privilégios anônimos (ou seja, com restrição máxima). Padrão: NÃO

anon_world_readable_only Quando ativado, os usuários anônimos só poderão baixar arquivos que sejam legíveis pelo mundo. Isso é reconhecer que o usuário de ftp pode possuir arquivos, especialmente na presença de uploads. Padrão: SIM

anônimo_enable Controla se logins anônimos são permitidos ou não. Se ativado, os nomes de usuário ftp e anônimo são reconhecidos como logins anônimos. Padrão: SIM

ascii_download_enable Quando ativado, as transferências de dados no modo ASCII serão respeitadas nos downloads. Padrão: NÃO

ascii_upload_enable Quando ativado, as transferências de dados no modo ASCII serão honradas nos uploads. Padrão: NÃO

async_abor_enable Quando habilitado, um comando especial de FTP conhecido como "async ABOR" será habilitado. Apenas clientes FTP mal aconselhados usarão esse recurso. Além disso, esse recurso é difícil de manusear, por isso está desabilitado por padrão. Infelizmente, alguns clientes FTP travam ao cancelar uma transferência, a menos que esse recurso esteja disponível, portanto, você pode habilitá-lo. Padrão: NÃO

fundo Quando ativado, e o vsftpd é iniciado no modo "ouvir", o vsftpd irá em segundo plano o processo do ouvinte. ou seja, o controle será imediatamente devolvido ao shell que lançou o vsftpd. Padrão: SIM

check_shell Observação! Esta opção só tem efeito para compilações não-PAM do vsftpd. Se desabilitado, o vsftpd não verificará em /etc/shells um shell de usuário válido para logins locais. Padrão: SIM

chmod_enable Quando habilitado, permite o uso do comando SITE CHMOD. NOTA! Isso se aplica apenas a usuários locais. Usuários anônimos nunca conseguem usar o SITE CHMOD. Padrão: SIM

chown_uploads Se ativado, todos os arquivos enviados anonimamente terão a propriedade alterada para o usuário especificado na configuração chown_username . Isso é útil do ponto de vista administrativo e talvez de segurança. Padrão: NÃO

chroot_list_enable Se ativado, você pode fornecer uma lista de usuários locais que são colocados em uma jaula chroot() em seu diretório inicial no login. O significado é ligeiramente diferente se chroot_local_user estiver definido como YES. Neste caso, a lista se torna uma lista de usuários que NÃO devem ser colocados em uma jaula chroot(). Por padrão, o arquivo que contém essa lista é /etc/vsftpd/chroot_list, mas você pode substituir isso pela configuração chroot_list_file . Padrão: NÃO

chroot_local_user Se definido como YES, os usuários locais serão (por padrão) colocados em uma jaula chroot() em seu diretório inicial após o login. Aviso: esta opção tem implicações de segurança, especialmente se os usuários tiverem permissão de upload ou acesso ao shell. Ative apenas se você souber o que está fazendo. Observe que essas implicações de segurança não são específicas do vsftpd. Eles se aplicam a todos os daemons FTP que oferecem colocar usuários locais em jaulas chroot(). Padrão: NÃO

connect_from_port_20 Isso controla se as conexões de dados do estilo PORT usam a porta 20 (ftp-data) na máquina do servidor. Por razões de segurança, alguns clientes podem insistir que este é o caso. Por outro lado, desabilitar esta opção permite que o vsftpd seja executado com um pouco menos de privilégio. Padrão: NÃO (mas o arquivo de configuração de amostra o habilita)

debug_ssl Se true, os diagnósticos de conexão OpenSSL são despejados no arquivo de log vsftpd. (Adicionado na v2.0.6). Padrão: NÃO

delete_failed_uploads Se true, todos os arquivos de upload com falha serão excluídos. (Adicionado na v2.0.7). Padrão: NÃO

deny_email_enable Se ativado, você pode fornecer uma lista de respostas de e-mail de senha anônima que fazem com que o login seja negado. Por padrão, o arquivo que contém esta lista é /etc/vsftpd/banned_emails, mas você pode sobrescrever isso com a configuração de arquivo_email_banido . Padrão: NÃO

dirlist_enable Se definido como NO, todos os comandos da lista de diretórios darão permissão negada. Padrão: SIM

dirmessage_enable Se ativado, os usuários do servidor FTP podem receber mensagens quando entrarem em um novo diretório pela primeira vez. Por padrão, um diretório é verificado em busca do arquivo .message, mas isso pode ser substituído pela definição de

configuração message_file . Padrão: NÃO (mas o arquivo de configuração de amostra o habilita)

download_enable Se definido como NÃO, todas as solicitações de download darão permissão negada. Padrão: SIM

dual_log_enable Se habilitado, dois arquivos de log são gerados em paralelo, indo por padrão para /var/log/xferlog e /var/log/vsftpd.log . O primeiro é um log de transferência no estilo wu-ftpd, analisável por ferramentas padrão. O último é o log de estilo do próprio vsftpd. Padrão: NÃO

force_dot_files Se ativado, os arquivos e diretórios que começam com . será mostrado nas listagens de diretórios mesmo que o sinalizador "a" não tenha sido usado pelo cliente. Esta substituição exclui o "." e entradas "..". Padrão: NÃO

force_anon_data_ssl Aplica-se apenas se ssl_enable estiver ativado. Se ativado, todos os logins anônimos são forçados a usar uma conexão SSL segura para enviar e receber dados em conexões de dados. Padrão: NÃO

force_anon_logins_ssl Aplica-se apenas se ssl_enable estiver ativado. Se ativado, todos os logins anônimos são forçados a usar uma conexão SSL segura para enviar a senha. Padrão: NÃO

force_local_data_ssl Aplica-se apenas se ssl_enable estiver ativado. Se ativado, todos os logins não anônimos são forçados a usar uma conexão SSL segura para enviar e receber dados em conexões de dados. Padrão: SIM

force_local_logins_ssl Aplica-se apenas se ssl_enable estiver ativado. Se ativado, todos os logins não anônimos são forçados a usar uma conexão SSL segura para enviar a senha. Padrão: SIM

guest_enable Se ativado, todos os logins não anônimos são classificados como logins de "convidado". Um login de convidado é remapeado para o usuário especificado na configuração guest_username . Padrão: NÃO

hide_ids Se ativado, todas as informações de usuários e grupos nas listagens de diretórios serão exibidas como "ftp". Padrão: NÃO

implícito_ssl Se ativado, um handshake SSL é a primeira coisa que se espera em todas as conexões (o protocolo FTPS). Para suportar SSL explícito e/ou texto simples também, um processo de listener vsftpd separado deve ser executado. Padrão: NÃO

ouvir Se ativado, o vsftpd será executado no modo autônomo. Isso significa que o vsftpd não deve ser executado a partir de algum tipo de inetd. Em vez disso, o executável vsftpd é executado uma vez diretamente. O próprio vsftpd cuidará de ouvir e lidar com conexões de entrada. Padrão: NÃO

listen_ipv6 Como o parâmetro listen, exceto que o vsftpd escutará em um soquete IPv6 em vez de um IPv4. Este parâmetro e o parâmetro listen são mutuamente exclusivos. Padrão: NÃO

local_enable Controla se os logins locais são permitidos ou não. Se habilitado, contas de usuário normais em /etc/passwd (ou onde quer que suas referências de configuração do

PAM) possam ser usadas para fazer login. Isso deve ser habilitado para que qualquer login não anônimo funcione, incluindo usuários virtuais. Padrão: NÃO

lock_upload_files Quando ativado, todos os uploads prosseguem com um bloqueio de gravação no arquivo de upload. Todos os downloads prosseguem com um bloqueio de leitura compartilhado no arquivo de download. AVISO! Antes de habilitar isso, esteja ciente de que leitores mal-intencionados podem matar um escritor que deseja, por exemplo, anexar um arquivo. Padrão: SIM

log_ftp_protocol Quando habilitada, todas as solicitações e respostas de FTP são registradas, desde que a opção xferlog_std_format não esteja habilitada. Útil para depuração. Padrão: NÃO

ls_recurse_enable Quando habilitada, esta configuração permitirá o uso de "ls -R". Este é um risco de segurança menor, porque um ls -R no nível superior de um site grande pode consumir muitos recursos. Padrão: NÃO

mdtm_write Quando habilitada, esta configuração permitirá que o MDTM defina os tempos de modificação do arquivo (sujeito às verificações de acesso usuais). Padrão: SIM

no_anon_password Quando ativado, isso impede que o vsftpd solicite uma senha anônima - o usuário anônimo fará login diretamente. Padrão: NÃO

no_log_lock Quando ativado, isso impede que o vsftpd bloqueie um arquivo ao gravar em arquivos de log. Esta opção geralmente não deve ser habilitada. Ele existe para solucionar bugs do sistema operacional, como a combinação de sistema de arquivos Solaris / Veritas, que às vezes exibe travamentos ao tentar bloquear arquivos de log. Padrão: NÃO

one_process_model Se você tem um kernel Linux 2.4, é possível usar um modelo de segurança diferente que usa apenas um processo por conexão. É um modelo de segurança menos puro, mas aumenta o desempenho. Você realmente não deseja habilitar isso a menos que saiba o que está fazendo, e seu site suporta um grande número de usuários conectados simultaneamente. Padrão: NÃO

passwd_chroot_enable Se ativado, junto com chroot_local_user , um local de prisão chroot() pode ser especificado por usuário. A jail de cada usuário é derivada de sua string de diretório inicial em /etc/passwd. A ocorrência de /./ na string do diretório inicial indica que a jaula está naquele local específico no caminho. Padrão: NÃO

pasv_addr_resolve Defina como YES se desejar usar um nome de host (em oposição ao endereço IP) na opção pasv_address . Padrão: NÃO

pasv_enable Defina como NÃO se desejar desabilitar o método PASV de obter uma conexão de dados. Padrão: SIM

pasv_promiscuous Defina como SIM se desejar desabilitar a verificação de segurança PASV que garante que a conexão de dados seja originada do mesmo endereço IP que a conexão de controle. Ative apenas se você souber o que está fazendo! O único uso legítimo para isso é em alguma forma de esquema de encapsulamento seguro, ou talvez para facilitar o suporte FXP. Padrão: NÃO

port_enable Defina como NO se desejar desabilitar o método PORT para obter uma conexão de dados. Padrão: SIM

port_promiscuous Defina como YES se desejar desativar a verificação de segurança PORT que garante que as conexões de dados de saída possam se conectar apenas ao cliente. Ative apenas se você souber o que está fazendo! Padrão: NÃO

exigir_cert Se definido como sim, todas as conexões do cliente SSL devem apresentar um certificado de cliente. O grau de validação aplicado a este certificado é controlado por validate_cert (Adicionado na v2.0.6). Padrão: NÃO

require_ssl_reuse Se definido como sim, todas as conexões de dados SSL devem exibir a reutilização da sessão SSL (o que prova que eles conhecem o mesmo segredo mestre que o canal de controle). Embora este seja um padrão seguro, ele pode quebrar muitos clientes FTP, então você pode desativá-lo. Para uma discussão sobre as consequências, consulte http://scarybeastsecurity.blogspot.com/2009/02/vsftpd-210-released.html (Adicionado na v2.1.0). Padrão: SIM

reverse_lookup_enable Defina como YES se desejar que o vsftpd transforme o endereço IP no nome do host, antes da autenticação pam. Isso é útil se você usar pam_access incluindo o nome do host. Se você quiser que o vsftpd seja executado no ambiente em que a pesquisa inversa para algum nome de host estiver disponível e o servidor de nomes não responder por um tempo, você deve definir isso como NÃO para evitar um problema de desempenho. Padrão: SIM

run_as_launching_user Defina como YES se desejar que o vsftpd seja executado como o usuário que iniciou o vsftpd. Isso é útil quando o acesso root não está disponível. AVISO MASSIVO! NÃO habilite esta opção a menos que você saiba totalmente o que está fazendo, pois o uso ingênuo desta opção pode criar grandes problemas de segurança. Especificamente, o vsftpd não usa/não pode usar a tecnologia chroot para restringir o acesso ao arquivo quando esta opção está definida (mesmo se iniciada pelo root). Um substituto ruim pode ser usar um deny_file configuração como {/,..*}, mas a confiabilidade disso não pode ser comparada ao chroot e não deve ser confiável. Se estiver usando esta opção, muitas restrições em outras opções se aplicam. Por exemplo, as opções que exigem privilégios, como logins não anônimos, alteração de propriedade de upload, conexão da porta 20 e portas de escuta inferiores a 1024, não devem funcionar. Outras opções podem ser afetadas. Padrão: NÃO

secure_email_list_enable Defina como SIM se desejar que apenas uma lista especificada de senhas de e-mail para logins anônimos seja aceita. Isso é útil como uma maneira simples de restringir o acesso a conteúdo de baixa segurança sem a necessidade de usuários virtuais. Quando ativado, os logins anônimos são impedidos, a menos que a senha fornecida esteja listada no arquivo especificado pela configuração email_password_file . O formato do arquivo é uma senha por linha, sem espaço em branco extra. O nome de arquivo padrão é /etc/vsftpd/email_passwords. Padrão: NÃO

session_support Isso controla se o vsftpd tenta manter sessões para logins. Se o vsftpd estiver mantendo sessões, ele tentará atualizar o utmp e o wtmp. Ele também abrirá uma pam_session se estiver usando o PAM para autenticar e fechará apenas após o logout. Você pode desabilitar isso se não precisar de log de sessão e desejar dar ao vsftpd mais oportunidade de executar com menos processos e/ou menos privilégios. OBSERVAÇÃO - o suporte a utmp e wtmp é fornecido apenas com compilações habilitadas para PAM. Padrão: NÃO

setproctitle_enable Se ativado, o vsftpd tentará mostrar as informações de status da sessão na lista de processos do sistema. Em outras palavras, o nome relatado do processo será alterado para refletir o que uma sessão vsftpd está fazendo (inativa, baixando, etc.). Você provavelmente deseja deixar isso desmarcado por motivos de segurança. Padrão: NÃO

ssl_enable Se ativado, e o vsftpd foi compilado no OpenSSL, o vsftpd suportará conexões seguras via SSL. Isso se aplica à conexão de controle (incluindo login) e também às conexões de dados. Você também precisará de um cliente com suporte a SSL. NOTA!! Cuidado ao habilitar esta opção. Habilite-o apenas se precisar. vsftpd não pode garantir a segurança das bibliotecas OpenSSL. Ao habilitar esta opção, você declara que confia na segurança de sua biblioteca OpenSSL instalada. Padrão: NÃO

ssl_request_cert Se ativado, o vsftpd solicitará (mas não necessariamente exigirá; consulte require_cert) um certificado nas conexões SSL de entrada . Normalmente , isso não deve causar nenhum problema, mas o IBM zOS parece ter problemas. (Novo na v2.0.7). Padrão: SIM

ssl_sslv2 Aplica-se apenas se ssl_enable estiver ativado. Se habilitada, esta opção permitirá conexões de protocolo SSL v2. As conexões TLS v1 são preferidas. Padrão: NÃO

ssl_sslv3 Aplica-se apenas se ssl_enable estiver ativado. Se habilitada, esta opção permitirá conexões de protocolo SSL v3. As conexões TLS v1 são preferidas. Padrão: NÃO

ssl_tlsv1 Aplica-se apenas se ssl_enable estiver ativado. Se habilitada, esta opção permitirá conexões de protocolo TLS v1. As conexões TLS v1 são preferidas. Padrão: SIM

strict_ssl_read_eof Se ativado, os uploads de dados SSL devem terminar via SSL, não um EOF no soquete. Essa opção é necessária para garantir que um invasor não encerre um upload prematuramente com um TCP FIN falsificado. Infelizmente, ele não está habilitado por padrão porque poucos clientes acertam. (Novo na v2.0.7). Padrão: NÃO

strict_ssl_write_shutdown Se ativado, os downloads de dados SSL são necessários para terminar via SSL, não um EOF no soquete. Isso está desativado por padrão, pois não consegui encontrar um único cliente FTP que faça isso. É menor. Tudo o que afeta é nossa capacidade de saber se o cliente confirmou o recebimento completo do arquivo. Mesmo sem esta opção, o cliente consegue verificar a integridade do download. (Novo na v2.0.7). Padrão: NÃO

syslog_enable Se habilitado, qualquer saída de log que teria ido para /var/log/vsftpd.log vai para o log do sistema. O registro é feito sob o recurso FTPD. Padrão: NÃO

tcp_wrappers Se habilitado, e vsftpd foi compilado com suporte a tcp_wrappers, as conexões de entrada serão alimentadas através do controle de acesso tcp_wrappers. Além disso, existe um mecanismo para configuração baseada em IP. Se tcp_wrappers definir a variável de ambiente VSFTPD_LOAD_CONF, a sessão vsftpd tentará carregar o arquivo de configuração vsftpd especificado nesta variável. Padrão: NÃO

text_userdb_names Por padrão, os IDs numéricos são mostrados nos campos de usuário e grupo das listagens de diretório. Você pode obter nomes textuais ativando este parâmetro. Ele está desativado por padrão por motivos de desempenho. Padrão: NÃO

til_user_enable Se ativado, o vsftpd tentará resolver nomes de caminho como ~chris/pics, ou seja, um til seguido por um nome de usuário. Observe que o vsftpd sempre resolverá os nomes de caminho ~ e ~/alguma coisa (neste caso, ~ resolve para o diretório de login inicial).

Observe que os caminhos do ~user serão resolvidos apenas se o arquivo /etc/passwd puder ser encontrado na jaula _current_chroot(). Padrão: NÃO

use_localtime Se ativado, o vsftpd exibirá listagens de diretórios com a hora em seu fuso horário local. O padrão é exibir GMT. Os tempos retornados pelo comando MDTM FTP também são afetados por esta opção. Padrão: NÃO

use_sendfile Uma configuração interna usada para testar o benefício relativo de usar a chamada de sistema sendfile() em sua plataforma. Padrão: SIM

userlist_deny Esta opção é examinada se userlist_enable estiver ativado. Se você definir essa configuração como NO, os usuários terão o login negado, a menos que estejam explicitamente listados no arquivo especificado por userlist_file . Quando o login é negado, a negação é emitida antes que o usuário seja solicitado a fornecer uma senha. Padrão: SIM

userlist_enable Se ativado, o vsftpd carregará uma lista de nomes de usuário, a partir do nome do arquivo fornecido por userlist_file . Se um usuário tentar fazer login usando um nome neste arquivo, ele será negado antes que seja solicitada uma senha. Isso pode ser útil para evitar que as senhas de texto não criptografado sejam transmitidas. Veja também userlist_deny . Padrão: NÃO

valid_cert Se definido como sim, todos os certificados de cliente SSL recebidos devem validar OK. Os certificados autoassinados não constituem validação OK. (Novo na v2.0.6). Padrão: NÃO

userlist_log Esta opção é examinada se userlist_enable estiver ativado. Se ativado, cada negação de login com base na lista de usuários será registrada. Padrão: NÃO

virtual_use_local_privs Se ativado, os usuários virtuais usarão os mesmos privilégios dos usuários locais. Por padrão, os usuários virtuais usarão os mesmos privilégios dos usuários anônimos, o que tende a ser mais restritivo (especialmente em termos de acesso de gravação). Padrão: NÃO

write_enable Isso controla se quaisquer comandos FTP que alteram o sistema de arquivos são permitidos ou não. Esses comandos são: STOR, DELE, RNFR, RNTO, MKD, RMD, APPE e SITE. Padrão: NÃO

xferlog_enable Se habilitado, um arquivo de log será mantido detalhando uploads e downloads. Por padrão, esse arquivo será colocado em /var/log/vsftpd.log, mas esse local pode ser substituído usando a configuração vsftpd_log_file . Padrão: NÃO (mas o arquivo de configuração de amostra o habilita)

xferlog_std_format Se ativado, o arquivo de log de transferência será gravado no formato xferlog padrão, conforme usado pelo wu-ftpd. Isso é útil porque você pode reutilizar os geradores de estatísticas de transferência existentes. O formato padrão é mais legível, no entanto. O local padrão para este estilo de arquivo de log é /var/log/xferlog, mas você pode alterá-lo com a configuração xferlog_file . Padrão: NÃO

isolar_rede Se habilitado, use CLONE_NEWNET para isolar os processos não confiáveis para que eles não possam fazer connect() arbitrários e, em vez disso, precisem solicitar soquetes ao processo privilegiado (port_promiscuous deve ser desabilitado). Padrão: SIM

isolar Se habilitado, use CLONE_NEWPID e CLONE_NEWIPC para isolar processos em seus namespaces ipc e pid. Portanto, processos separados não podem interagir uns com os outros. Padrão: SIM

Opções numéricas Abaixo está uma lista de opções numéricas. Uma opção numérica deve ser definida como um número inteiro não negativo. Números octais são suportados, para conveniência das opções de umask. Para especificar um número octal, use 0 como o primeiro dígito do número. accept_timeout O tempo limite, em segundos, para um cliente remoto estabelecer conexão com uma conexão de dados estilo PASV. Padrão: 60

anon_max_rate A taxa máxima de transferência de dados permitida, em bytes por segundo, para clientes anônimos. Padrão: 0 (ilimitado)

anon_umask O valor para o qual o umask para criação de arquivo está configurado para usuários anônimos. NOTA! Se você quiser especificar valores octais, lembre-se do prefixo "0", caso contrário o valor será tratado como um inteiro de base 10! Padrão: 077

chown_upload_mode O modo de arquivo a ser forçado para uploads anônimos chown()ed. (Adicionado na v2.0.6). Padrão: 0600

connect_timeout O tempo limite, em segundos, para um cliente remoto responder à nossa conexão de dados estilo PORT. Padrão: 60

data_connection_timeout O tempo limite, em segundos, que é aproximadamente o tempo máximo que permitimos que as transferências de dados parem sem progresso. Se o tempo limite for acionado, o cliente remoto será iniciado. Padrão: 300

delay_failed_login O número de segundos para pausar antes de relatar um login com falha. Padrão: 1

delay_successful_login O número de segundos para pausar antes de permitir um login bem-sucedido. Padrão: 0

arquivo_open_mode As permissões com as quais os arquivos carregados são criados. Umasks são aplicados em cima desse valor. Você pode querer mudar para 0777 se quiser que os arquivos carregados sejam executáveis. Padrão: 0666

ftp_data_port A porta da qual as conexões do estilo PORT se originam (desde que o mal nomeado connect_from_port_20 esteja habilitado). Padrão: 20

idle_session_timeout O tempo limite, em segundos, que é o tempo máximo que um cliente remoto pode gastar entre os comandos de FTP. Se o tempo limite for acionado, o cliente remoto será iniciado. Padrão: 300

porta_escuta Se o vsftpd estiver no modo autônomo, esta é a porta em que ele escutará as conexões FTP de entrada. Padrão: 21

local_max_rate A taxa máxima de transferência de dados permitida, em bytes por segundo, para usuários locais autenticados. Padrão: 0 (ilimitado)

local_umask O valor para o qual o umask para criação de arquivo está configurado para usuários locais. NOTA! Se você quiser especificar valores octais, lembre-se do prefixo "0", caso contrário o valor será tratado como um inteiro de base 10! Padrão: 077

max_clients Se o vsftpd estiver no modo autônomo, este é o número máximo de clientes que podem ser conectados. Quaisquer clientes adicionais que se conectem receberão uma mensagem de erro. O valor 0 desliga o limite. Padrão: 2000

max_login_fails Após tantas falhas de login, a sessão é encerrada. Padrão: 3

max_per_ip Se o vsftpd estiver no modo autônomo, este é o número máximo de clientes que podem ser conectados a partir do mesmo endereço de internet de origem. Um cliente receberá uma mensagem de erro se ultrapassar esse limite. O valor 0 desliga o limite. Padrão: 50

pasv_max_port A porta máxima a ser alocada para conexões de dados de estilo PASV. Pode ser usado para especificar um intervalo de portas estreito para auxiliar no firewall. Padrão: 0 (use qualquer porta)

pasv_min_port A porta mínima a ser alocada para conexões de dados de estilo PASV. Pode ser usado para especificar um intervalo de portas estreito para auxiliar no firewall. Padrão: 0 (use qualquer porta)

trans_chunk_size Você provavelmente não quer mudar isso, mas tente configurá-lo para algo como 8192 para um limitador de largura de banda muito mais suave. Padrão: 0 (deixe o vsftpd escolher uma configuração sensata)

Opções de sequência Abaixo está uma lista de opções de string. anon_root Esta opção representa um diretório para o qual o vsftpd tentará mudar após um login anônimo. A falha é ignorada silenciosamente. Padrão: (nenhum)

arquivo_email_banido Esta opção é o nome de um arquivo que contém uma lista de senhas de e-mail anônimas que não são permitidas. Este arquivo é consultado se a opção deny_email_enable estiver habilitada. Padrão: /etc/vsftpd/banned_emails

arquivo_banner Esta opção é o nome de um arquivo contendo texto a ser exibido quando alguém se conecta ao servidor. Se definido, ele substitui a string do banner fornecida pela opção ftpd_banner . Padrão: (nenhum)

ca_certs_file Esta opção é o nome de um arquivo para carregar os certificados da Autoridade de Certificação, com a finalidade de validar os certificados do cliente. Os certificados carregados também são anunciados ao cliente, para atender a clientes TLSv1.0, como o cliente FTP do z/OS. Lamentavelmente, os caminhos de certificado SSL CA padrão não são usados, devido ao uso de espaços restritos do sistema de arquivos (chroot) pelo vsftpd. (Adicionado na v2.0.6). Padrão: (nenhum)

chown_username Este é o nome do usuário que recebe a propriedade dos arquivos enviados anonimamente. Esta opção só é relevante se outra opção, chown_uploads , estiver definida. Padrão: raiz

chroot_list_file A opção é o nome de um arquivo contendo uma lista de usuários locais que serão colocados em uma jaula chroot() em seu diretório inicial. Esta opção só é relevante se a opção chroot_list_enable estiver habilitada. Se a opção chroot_local_user estiver habilitada, então o arquivo de lista se torna uma lista de usuários para NÃO colocar em uma jaula chroot(). Padrão: /etvsftpd.confc/vsftpd.chroot_list

cmds_allowed Esta opção especifica uma lista separada por vírgulas de comandos FTP permitidos (pós-login. USER, PASS e QUIT e outros são sempre permitidos pré-login). Outros comandos são rejeitados. Este é um método poderoso de realmente bloquear um servidor FTP. Exemplo: cmds_allowed=PASV,RETR,QUIT Padrão: (nenhum)

cmds_denied Esta opção especifica uma lista separada por vírgulas de comandos FTP negados (pós-login. USER, PASS, QUIT e outros são sempre permitidos pré-login). Se um comando aparecer em ambos this e cmds_allowed , a negação terá precedência. (Adicionado na v2.1.0). Padrão: (nenhum)

deny_file Esta opção pode ser usada para definir um padrão para nomes de arquivos (e nomes de diretórios, etc.) que não devem ser acessíveis de forma alguma. Os itens afetados não estão ocultos, mas qualquer tentativa de fazer algo com eles (baixar, mudar para o diretório, afetar algo dentro do diretório etc.) será negada. Esta opção é muito simples e não deve ser usada para controle de acesso sério - as permissões do sistema de arquivos devem ser usadas preferencialmente. No entanto, essa opção pode ser útil em determinadas configurações de usuário virtual. Em particular, ciente de que, se um nome de arquivo for acessível por uma variedade de nomes (talvez devido a links simbólicos ou links físicos), deve-se tomar cuidado para negar o acesso a todos os nomes. O acesso será negado aos itens se seus nomes contiverem a string fornecida por hide_file ou se corresponderem à expressão regular especificada por hide_file. Observe que vsftpd' O código de correspondência de expressão regular de s é uma implementação simples que é um subconjunto da funcionalidade completa de expressão regular. Por isso, você precisará testar cuidadosa e exaustivamente qualquer aplicação dessa opção. E é recomendável usar as permissões do sistema de arquivos para quaisquer políticas de segurança importantes devido à sua maior confiabilidade. A sintaxe de regex com suporte é qualquer número de , *? e operadores {,} não aninhados. A correspondência Regex é suportada apenas no último componente de um caminho, por exemplo, a/b/? é suportado, mas a/?/c não é. Exemplo: deny_file={*.mp3,*.mov,.private} E é recomendável usar as permissões do sistema de arquivos para quaisquer políticas de segurança importantes devido à sua maior confiabilidade. A sintaxe de regex com suporte é qualquer número de , ? e operadores {,} não aninhados. A correspondência Regex é suportada apenas no último componente de um caminho, por exemplo, a/b/? é suportado, mas a/?/c não é. Exemplo: deny_file={.mp3,*.mov,.private} E é recomendável usar as permissões do sistema de arquivos para quaisquer políticas de segurança importantes devido à sua maior confiabilidade. A sintaxe de regex com suporte é qualquer número de , ? e operadores {,} não aninhados. A correspondência Regex é suportada apenas no último componente de um caminho, por exemplo, a/b/? é suportado, mas a/?/c não é. Exemplo: deny_file={*.mp3,*.mov,.private} Padrão: (nenhum)

dsa_cert_file Esta opção especifica o local do certificado DSA a ser usado para conexões criptografadas SSL. Padrão: (nenhum - um certificado RSA é suficiente)

dsa_private_key_file Esta opção especifica o local da chave privada DSA a ser usada para conexões criptografadas SSL. Se esta opção não estiver definida, espera-se que a chave privada esteja no mesmo arquivo que o certificado. Padrão: (nenhum)

email_password_file Esta opção pode ser usada para fornecer um arquivo alternativo para uso pela configuração secure_email_list_enable . Padrão: /etc/vsftpd/email_passwords

ftp_username Este é o nome do usuário que usamos para lidar com FTP anônimo. O diretório inicial deste usuário é a raiz da área de FTP anônima. Padrão: ftp

ftpd_banner Esta opção de string permite que você substitua o banner de saudação exibido pelo vsftpd quando uma conexão for iniciada. Padrão: (nenhum - o banner vsftpd padrão é exibido)

guest_username Consulte a configuração booleana guest_enable para obter uma descrição do que constitui um login de convidado. Essa configuração é o nome de usuário real para o qual os usuários convidados são mapeados. Padrão: ftp

hide_file Esta opção pode ser usada para definir um padrão para nomes de arquivos (e nomes de diretórios, etc.) que devem ser ocultados das listagens de diretórios. Apesar de estarem ocultos, os arquivos/diretórios etc. são totalmente acessíveis aos clientes que sabem quais nomes realmente usar. Os itens ficarão ocultos se seus nomes contiverem a string fornecida por hide_file ou se corresponderem à expressão regular especificada por hide_file. Observe que o código de correspondência de expressão regular do vsftpd é uma implementação simples que é um subconjunto da funcionalidade completa de expressão regular. Consulte deny_file para obter detalhes sobre exatamente qual sintaxe regex é suportada. Exemplo: hide_file={*.mp3,.hidden,hide*,h?} Padrão: (nenhum)

listen_address Se o vsftpd estiver no modo autônomo, o endereço de escuta padrão (de todas as interfaces locais) pode ser substituído por essa configuração. Forneça um endereço IP numérico. Padrão: (nenhum)

listen_address6 Como listen_address, mas especifica um endereço de escuta padrão para o listener IPv6 (que é usado se listen_ipv6 estiver definido). Formato é o formato de endereço IPv6 padrão. Padrão: (nenhum)

local_root Esta opção representa um diretório para o qual o vsftpd tentará mudar após um login local (ou seja, não anônimo). A falha é ignorada silenciosamente. Padrão: (nenhum)

arquivo_mensagem Esta opção é o nome do arquivo que procuramos quando um novo diretório é inserido. O conteúdo é exibido para o usuário remoto. Esta opção só é relevante se a opção dirmessage_enable estiver habilitada. Padrão: .message

nopriv_user Este é o nome do usuário que é usado pelo vsftpd quando ele quer ser totalmente desprivilegiado. Observe que este deve ser um usuário dedicado, e não ninguém. O usuário none tende a ser usado para muitas coisas importantes na maioria das máquinas. Padrão: ninguém

pam_service_name Essa string é o nome do serviço PAM que o vsftpd usará. Padrão: ftp

pasv_address Use esta opção para substituir o endereço IP que o vsftpd anunciará em resposta ao comando PASV. Forneça um endereço IP numérico, a menos que pasv_addr_resolve esteja habilitado; nesse caso, você pode fornecer um nome de host que será o DNS resolvido para você na inicialização. Padrão: (nenhum - o endereço é obtido do soquete conectado de entrada)

rsa_cert_file Esta opção especifica o local do certificado RSA a ser usado para conexões criptografadas SSL. Padrão: /usr/share/ssl/certs/vsftpd.pem

rsa_private_key_file Esta opção especifica o local da chave privada RSA a ser usada para conexões criptografadas SSL. Se esta opção não estiver definida, espera-se que a chave privada esteja no mesmo arquivo que o certificado. Padrão: (nenhum)

secure_chroot_dir Esta opção deve ser o nome de um diretório que está vazio. Além disso, o diretório não deve ser gravável pelo usuário ftp. Este diretório é usado como uma prisão chroot() segura às vezes o vsftpd não requer acesso ao sistema de arquivos. Padrão: /usr/share/empty

ssl_ciphers Esta opção pode ser usada para selecionar quais cifras SSL vsftpd permitirão conexões SSL criptografadas. Consulte a página de manual de cifras para obter mais detalhes. Observe que restringir as cifras pode ser uma precaução de segurança útil, pois evita que partes remotas maliciosas forcem uma cifra com a qual encontraram problemas. Padrão: DES-CBC3-SHA

user_config_dir Esta opção poderosa permite a substituição de qualquer opção de configuração especificada na página de manual, por usuário. O uso é simples e é melhor ilustrado com um exemplo. Se você definir user_config_dir como /etc/vsftpd/user_conf e, em seguida, efetuar logon como o usuário "chris", o vsftpd aplicará as configurações no arquivo /etc/vsftpd/user_conf/chris durante a sessão. O formato deste arquivo é conforme detalhado nesta página de manual! OBSERVE que nem todas as configurações são efetivas por usuário. Por exemplo, muitas configurações apenas antes do início da sessão do usuário. Exemplos de configurações que não afetarão nenhum comportamento por usuário incluem listen_address, banner_file, max_per_ip, max_clients, xferlog_file, etc. Padrão: (nenhum)

user_sub_token Esta opção é útil em conjunto com usuários virtuais. Ele é usado para gerar automaticamente um diretório inicial para cada usuário virtual, com base em um modelo. Por exemplo, se o diretório inicial do usuário real especificado via guest_username for /home/virtual/$USER , e user_sub_token estiver definido como $USER , quando o usuário virtual fred fizer login, ele terminará (geralmente chroot()'ed) no diretório /home/virtual/fred . Esta opção também terá efeito se local_root contiver user_sub_token . Padrão: (nenhum)

userlist_file Esta opção é o nome do arquivo carregado quando a opção userlist_enable está ativa. Padrão: /etc/vsftpd/user_list

vsftpd_log_file Esta opção é o nome do arquivo no qual gravamos o arquivo de log do estilo vsftpd. Este log só é gravado se a opção xferlog_enable estiver configurada e xferlog_std_format NÃO estiver configurada. Alternativamente, é escrito se você definiu a opção dual_log_enable . Mais uma complicação - se você configurou syslog_enable , esse arquivo não será gravado e a saída será enviada para o log do sistema. Padrão: /var/log/vsftpd.log

xferlog_file Esta opção é o nome do arquivo no qual gravamos o log de transferência do estilo wu-ftpd. O log de transferência só é gravado se a opção xferlog_enable estiver configurada, junto com xferlog_std_format . Alternativamente, é escrito se você definiu a opção dual_log_enable . Padrão: /var/log/xferlog

1.5 Arquivo de configuração

´´´ listen=YES

- YES = Coloca o servidor em estado de prontidao e iniciando com o sistema
- NO = Obriga a inicializacao manual.

listen_ipv6=NO

- YES = Utiliza IPV6.

- NO = Utiliza somente IPV4

Permissão de acesso anônimo.

- local_enable=NO
- local_enable=YES

userlist_enable=YES

- Aponta o arquivo que consta a lista dos usuários com permissao.

userlist_file=/etc/vsftpd.userlist

- Aponta o caminho do arquivo contendo a lista dos usuarios permitidos.

Libera o acesso aos usuarios de vsftpd.userlist.

#userlist_deny=NO userlist_deny=NO

YES = Habilita o acesso anônimo.

NO = Desabilita o acesso anônimo.

---

anonymous_enable=NO

Exibe uma mensagem ao entrarem em um novo diretório pela primeira vez.

#dirmessage_enable=NO dirmessage_enable=YES

Habilita comandos para mudar o Sistema de Arquivos.

#write_enable=NO write_enable=YES

Permissoes para criacao de arquivos na pasta.

local_umask=077

Exibe listagens de diretórios com a hora em seu fuso horário local.

#use_localtime=NO use_localtime=YES

Gera um arquivo de log detalhando uploads e downloads. Por padrão, esse arquivo será colocado em /var/log/vsftpd.log

#xferlog_enable=NO xferlog_enable=YES

Direciona as conexões para a porta 20.

#connect_from_port_20=NO connect_from_port_20=YES

Determina se os usuários locais serão colocados em chrootjail.

#chroot_local_user=NO chroot_local_user=YES

Torna gravável o diretório chrootjail.

#allow_writeable_chroot=NO allow_writeable_chroot=YES

Aponta o arquivo de logs.

xferlog_file=/var/log/vsftpd.log xferlog_std_format=YES

Customizar o banner de acesso.

---

ftpd_banner=Bem vindo ao Servidor ftp VSFTPD.

---

secure_chroot_dir=/var/run/vsftpd/empty Diretório é usado como uma prisão chroot.

pam_service_name=srvftppam

- Nome do serviço PAM que o vsftpd usará.

> Há relatos na internet atribuindo uma série de falhas quando esse valor é "vsftpd".

Habilita SSL na autenticação.

- ssl_enable=NO
- rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
- rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

utf8_filesystem=YES

- Deixe descomentado se for usar um sistema UTF-8.

```
Fonte
```

```
------------------------------------------------------------

* <https://sempreupdate.com.br/como-instalar-um-servidor-ftp-ubuntu/>

* <https://www.youtube.com/watch?v=1WVBC0KBOeE>
```