sshd_config

Fichier de configuration pour sshd

AcceptEnv Spécifie quelles variables d'environnement envoyées par le client sont copiées dans l'environnement de la session. Voir SendEnv dans ssh_config

AddressFamily any|inet|inet6 Spécifie quelles familles d'adresse sont utilisés par sshd

AllowAgentForwarding yes|no Spécifie si le forwarding ssh-agent est permis. Noter que le désactiver n'améliore pas la sécurité sauf si les utilisateur se voient refuser un accès shell, vu qu'ils peuvent installer leur propre forwarders.

AllowGroups Liste de pattern de nom de groupe autorisé à se connecter

AllowStreamLocalForwardings yes|all|no|local|remote Spécifie si le forwarding StreamLocal (socket Unix) est permis

AllowTcpForwarding yes|all|no|local|remote Spécifie si le forwarding TCP est permis

AlowUsers Liste de noms d'utilisateurs autorisés à se connecter

AuthenticationMethods Spécifie les méthodes d'authentification qui doit être complétée pour autoriser l'accès à un utilisateur. 'any' indique toutes les méthodes.

AuthorizedKeysCommand Spécifie un programme à utiliser pour rechercher les clés publique de l'utilisateur. Le programme doit être possédé par root, pas en écriture pour le groupe et les autres. Le programme doit sortir 0 ou plusieurs ligne au format authorized_keys.

AuthorizedKeysCommandUser Spécifie l'utilisateur sous lequel AuthorizedKeysCommand est lancé.

AuthorizedKeysFile Spécifie le fichier qui contient les clés publique utilisées pour l'authentification utilisateur.

AuthorizedPrincipalsCommand Spécifie un programe à utiliser pour générer une liste de principaux.

AuthorizedPrincipalsCommandUser Spécifie l'utilisateur sous lequel la commande AuthorizedPrincipalsCommand est lancée

AuthorizedPrincipalsFile Spécifie un fichier qui liste les noms principaux qui sont acceptés pour l'authentification par certificat.

Banner Le contenu de ce fichier est affiché à l'utilisateur avant l'authentification.

ChallengeResponseAuthentication yes|no Spécifie si l'authentification par challenge/réponse est authorisée

ChrootDirectory Spécifie le chemin d'un répertoire pour chroot après l'authentification.

Ciphers Liste des chiffrements permis.

ClientAliveCountMax Définis le nombre de messages alive client qui peuvent être envoyés sans reçevoir de réponse du client. Si ce seuil est atteint, le client est déconnecté.

ClientAliveInterval timeout en secondes après lequel si aucune données n'a été reçue du client, sshd envoie un message alive. 0 = désactivé

Compression yes|no Spécifie si la compression est autorisé une fois l'authentification réussie.

DenyGroups Liste de groupes autorisés à se connecter

DenyUsers Liste d'utilisateurs non autorisés à se connecter

DisableForwarding Désactive toutes les fonctionnalités de forwarding

FingerprintHash md5|sha1256 Spécifie l'algorithme de hashage utilisé pour les empreintes de clé le login

ForceCommand Force l'exécution de la commande spécifié, ignorant toute commande fournie par le client et ~/.ssh/rc.

GatewayPorts yes|no|clientspecified Spécifie si les hôte distant sont autorisés à se connecter aux port forwardés pour le client.

GSSAPIAuthentication yes|no Spécifie si l'authentification basée sur GSSAPI est permis

GSSAPICleanupCredentials yes|no Spécifie si le cache d'accréditifs utilisateurs est automatiquement détruit à la déconnexion

GSSAPIStrictAcceptorCheck yes|no Détermine si l'acceptation de l'identité GSSAPI est stricte.

HostbasedAcceptedKeyTypes Spcifie les types de clé acceptés pour l'authentification basé sur l'hôte.

HostbasedAuthentication yes|no Spécifie si l'authentification rhosts ou /etc/hosts.equiv avec la clé publique cliente est permise

HostbasedUsesNameFromPacketOnly Spéifie si le serveur tente d'effectuer une recherche inversée en matchant les noms dans ~/.shosts, ~/.rhosts et /etc/hosts.equiv.

HostCertificate Spécifie un fichier contenant un certificat hôte publique.

HostKey Spécifie un fichier contenant une clé privée hôte.

HostKeyAgent Identifie le socket Unix utilisé pour communiquer avec un agent que a accès aux clés privées

HostKeyAlgorithms Spécifie les algorithmes de clé hôte que le serveur offre.

IgnoreRhosts yes|no Spécifie que les fichiers .rhosts, et .shosts ne sont pas utilisé dans HostbasedAuthentication

IgnoreUserKnownHosts yes|no Spécifie si sshd doit ignorer le fichier ~/.ssh/known_hosts de l'utilisateur durant HostbasedAuthentication.

IPQoS Spécifie le type de service IPv4 ou la classe DSCP pour les connexions. aff11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef, lowdelay, throughput, reliability, ou une valeur numérique.

KbdInteractiveAuthentication yes|no Utilise l'authentification interactive au clavier.

KerberosAuthentication yes|no Spécifie si le mot de passe fournis par l'utilisateur pour PasswordAuthentication est validé auprès du KDC.

KerberosGetAFTToken yes|no Si AFS est actif et l'utilisateur a un TGT, tente d'acquérir un jeton AFS avant d'accéder au répertoire home.

KerberosOrLocalPasswd yes|no Si l'authentification kerberos échoue, le mot de passe est validé avec un mécanisme local.

KerberosTicketCleanup yes|no Spécifie si le cache de ticket de l'utilisateur est automatiquement détruit à la déconnexion.

KeyAlgorithms Spécifie les algorithmes d'échange de clé permis.

ListenAddress Spécifie les adresses locales d'écoute

LoginGraceTime Délay au delà duquel le serveur déconnecte si l'utilisateur n'a pas réussi la connexion. 0 = pas de limite.

LogLevel Niveau de verbosité des logs. QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, DEBUG3.

MACs Spécifie les algorithmes MAC dans l'ordre de préférence

Match Introdui un block conditionnel. Si tous les critères sont satisfaut, les mots clés suivant remplacent la section globale. Les critèrse sont User, Group, Host, LocalAddress, LocalPort, et Address. Les mots clés suivants sont permis après un match : AcceptEnv, AllowAgentForwarding, AllowGroups, AllowStreamLocalForwarding, AllowTcpForwarding, AllowUsers, AuthenticationMethods, AuthorizedKeysCommand, AuthorizedKeysCommandUser, AuthorizedKeysFile, AuthorizedPrincipalsCommand, AuthorizedPrincipalsCommandUser, AuthorizedPrincipalsFile, Banner, ChrootDirectory, ClientAliveCountMax, ClientAliveInterval, DenyGroups, DenyUsers, ForceCommand, GatewayPorts, GSSAPIAuthentication, HostbasedAcceptedKeyTypes, HostbasedAuthentication, HostbasedUsesNameFromPacketOnly, IPQoS, KbdInteractiveAuthentication, KerberosAuthentication, LogLevel, MaxAuthTries, MaxSessions, PasswordAuthentication, PermitEmptyPasswords, PermitOpen, PermitRootLogin, PermitTTY, PermitTunnel, PermitUserRC, PubkeyAcceptedKeyTypes, PubkeyAuthentication, RekeyLimit, RevokedKeys, StreamLocalBindMask, StreamLocalBindUnlink, TrustedUserCAKeys, X11DisplayOffset, X11Forwarding et X11UseLocalHost.

MaxAuthTries Spécifie le nombre maximum de tentatives d'authentification permise par connexion. Une fois ce nombre atteint, des erreurs additionnels sont loggés.

MaxSessions Nombre de shell, login, ou de sessions sous-système (ex sftp) par connexion réseaux Plusieurs sessions peuvent être établies par les clients qui supportent le multiplexage de connexion. 1 = désactive le multiplexage, 0 = empêche toute session.

MaxStartups Nombre de connexions non-authentifiée concurrentes permises. Alternativement, un format "start :rate :full" va refuser les tentatives de connexion avec un aux de rate/100, s'il y a start connections non-authentifiées concurrentes. La probabilité augmente de manière linéaire et toutes les tentatives de connexion sont refusés si le nombre de connexions non-authentifiées atteint 'full' (Défaut : 10 :30 :100)

PasswordAuthentication yes|no Spécifie si l'authentification par mot de passe est permise

PermitEmptyPasswords yes|no Quand l'authentification par mot de passe est permis, spécifie si le serveur autorise le login aux comptes sans mot de passe.

PermitOpen [hostname|IP] :port [...] Spécifie les destinations pour lesquels le port forwarding TCP est permis. 'any' supprime toute restriction.

PermitRootLogin yes|prohibit-password|without-password|forced-commands-only|no prohibit-password ou without-password, l'authentification par mot de passe et au clavier sont désactivés. À forced-commands-only, la connexion root avec clé publique est autorisées mais seulement si l'option command a été spécifiée.

PermitTTH yes|no Spécifie si l'allocation pty est permise

PermitTunnel yes|point-to-point|ethernet|no Spécifie si le forwarding de périphérique tun est permis

PermitUserEnvironment yes|no Spécifie si ~/.ssh/environment dans dans le fichier ~/.ssh/authorized_keys sont traités par sshd.

PermitUserRC yes|no Spécifie si le fichier ~/.ssh/rc est exécuté

PidFile Fichier pid du service, on 'none' pour désactiver l'écriture de ce fichier

Port Spécifie le numéro de port d'écoute de sshd. Défaut : 22. Peut être spécifié plusieurs fois

PrintLastLog yes|no Spécifi si sshd affiche la date de dernière connexion de l'utilisateur

PrintMotd yes|no Spécifie si sshd doit afficher /etc/motd quand l'utilisateur se log.

PubkeyAcceptedKeyTypes Spécifie les types de clé acceptés pour l'authentification à clé publique

PubkeyAuthentication Spécifie si l'authentification par clé publique est permise

RekeyLimit Quantité maximum d-e données transmises avant que la clé de session soit renégociée, optionnellement avec un suffix 'K', 'M', ou 'G'.

RevokedKeys Spécifie le fichier de clés révoquées

StreamLocalBindMask umask de création de fichier utilisé en créant le socket unix. Défaut : 0177.

StreamLocalBindUnlink yes|no Spécifie si un fichier socket unix existant doit être supprimé avant d'en créer un nouveau.

StrictModes yes|no Vérifie les permissions et propriétaire des fichiers utilisateur et répertoire home avant d'accepter la connexion

Subsystem Configure un sous-système externe (ex : sftp)

SyslogFacility DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

TCPKeepAlive yes|no Spécifie si le système envoie des messages TCP keepalive.

TrustedUserCAKeys Spécifie un fichier contenant les clé publiques d'autorité de certification utilisés pour signer les certificats utilisateurs

UseDNS yes|no Recherche les noms d'hôte distants via DNS.

VersionAddendum Spécifie un texte additionnel à ajouter au protocole Banner envoyé par le serveur.

X11DisplayOffset Spécifie le premier affichage disponible pour le forwarding X11.

X11Forwarding yes|no Autorise le forwarding X11

X11UseLocalHost yes|no Spécifie si sshd lie le forwarding X11 à l'adresse de boucle locale ou l'adresse wildcard.

XAuthLocation Chemin complet du programme xauth

Formats de temps

Les options qui s'expriment sous la forme 'time[qualifier], ou time est un entier positif, et qualifier est :

(none) secondes

s|S secondes

m|M minutes

h|H Heures

d|D jours

w|W Semaines

Jetons

Les arguments de certains mots clé peuvent utilise des jetons, étendus comme suit :

%% le caractère %

%F l'enpreinte de la clé CA

%f l'empreinte de la clé ou du certificat

%h Répertoire personnel de l'utilisateur

%I ID de clé dans le certificat

%K Clé CA base64

%k clé ou certificat base64 pour l'authentification

%s Numéro de série du certificat

%T Type de clé CA

%t Type de clé ou certifiat

%u Nom de l'utilisateur

Les mots clés qui accèptent les jetons sont :

AuthorizedKeysCommand %%, %f, %h, %k, %t, %u

AuthorizedKeysFile %%, %h, %u.

AuthorizedPrincipalsCommand %%, %F, %f, %h, %i, %K, %k, %s, %T, %t, %u.

AuthorizedPrincipalsFile %%, %h, %u.

ChrootDirectory %%, %h, %u.