ssh_config

Fichier de configuration pour ssh

ssh obtient sa configuration depuis les sources suivantes, dans l'ordre :

1. Options de ligne de commande
2. fichier de configuration utilisateur
3. Fichier de configuration du système

Pour chaque paramètre, la première valeur obtenue est utilisée. Les fichiers de configuration contiennent des sections séparés par des spécifications Host, qui ne s'appliquent qu'aux hôte qui matchent un des patterns donnés dans la spécification.

OPTIONS

Host Restreint les déclarations suivantes aux hôtes qui matchent le motif donné. '*' peut être utilisé comme section par défaut. ' !' peut être utilisé pour inverser le match.

Match Restreint les déclarations suivantes seulement quand les conditions spécifiées sont satisfaites :

canonical matche seulement quand le fichier de configuration est reparcouru après la canonisation du nom d'hôte (voir l'option CanonicalizeHostname).

exec Exécute la commande spécifié dans le shell de l'utilisateur. Si la commande retourne un code de sortie 0, la condition est vrai

host Les critères sont matchés avec le nom d'hôte de la cible, après substitution par les options Hostname ou CanonicalizeHostname

originalhost Matche avec le nom d'hôte tel que spécifié sur la ligne de comande.

user Matche le nom d'utilisateur cible dans l'hôte distante

localuser Matche e nom de l'utilisateur local qui lance ssh

all Match tout

AddKeysToAgent yes|ask|confirm|no Spécifie si le clés devraient être automatiquement ajoutés à un ssh-agent en cours de fonctionnement. Si cette option est à yes, et qu'une clé est chargée depuis un fichier, la clé et sa passphrase sont ajoutés à l'agent avec la durée de vie par défaut, comme avec ssh-add. Si cette option est à ask, ssh demande confirmation en utilisant le programme SSH_ASKPASS. à confirm, chaque utilisation de la clé doit être confirmée. à no, aucune clé n'est ajoutée

AddressFamily any|inet|inet6 Spécifie quelle famille d'adresse utiliser pour la connexion

BatchMode yes|no à yes, la demande de mot de passe est désactivée

BindAddress Utilise l'adresse spécifié dans la machine locale comme adresse sources de la connexion. Ne fonctionne pas si UsePrivilegedPort est à yes

CanonicalDomains Activé, spécifie la liste de suffixes de domaines dans lequel rechercher l'hôte de destination

CanonicalizeFallbackLocal yes|no à yes, tente de rechercher le nom d'hôte non qualifié en utilisant les règles de recherche du résolveur. à no, ssh échoue immédiatement si CanonicalizeHostname est activé et que la cible n'est pas trouvé dans les domaines spécifiés par CanonicalDomains

CanonicalizeHostname yes|no Effectue une canonicalisation de nom d'hôte. à no, laisse le résolver rechercher les noms d'hôte, à yes, pour les connexion qui n'utilisent pas ProxyCommand, ssh tente de canoniser le nom d'hôte.

CanonicalizeMaxDots Nombre de points maximum dans le nom d'hôte avant de désactiver la canonicalisation.

CertificateFile Spécifie le certificat de l'utilisateur

ChallengeResponseAuthentication yes|no Active l'authentification challenge-response

CheckHostIP yes|no à yes, effectue une vérification additionnelle de l'adresse IP dans le fichier known_hosts. Permet de détecter si une clé hôte a changé dû à un DNS spoofing

Ciphers Spécifie les chiffrements permet, dans l'ordre de préférence (ssh -Q cipher pour obtenir une liste de chiffrements disponibles)

ClearAllForwardings yes|no Spécifie que tous les ports forwarding local, distant et dynamique spécifiés sont effacés. Utile pour scp et sftp qui les définissent automatiquement.

Compression yes|no Utilise la compression

ConnectionAttempts Nombre de tentatives (1 par secondes) avant de quitter. Défaut : 1

ConnectTimeout Spécifie le timeout en secondes utilisé pour se connecter au serveur ssh, au lieu d'utiliser le timeout TCP du système. Cette valeur est utilisé quand la cible est indisponible, pas quand elle refuse la connexion

ControlMaster yes|no|ask|autoask Active le partage de plusieurs sessions dans une seule connexion réseaux. à yes, ssh écoute les connexions dans un socket de contrôle ControlPath

ControlPath Spécifie le socket contrôle utilisé pour le partage de connexion

ControlPersist yes|no Spécifie que la connexion master de rester en tâche de fond pour de future connexions client, après que la connexion cliente initiale a été fermée

DynamicForward [bind_address :] port Spécifie qu'un port TCP dans la machine locale est forwardée dans le canal sécurisé, et le protocole d'application est ainsi utilisé pour déterminer où se connecter depuis la machine distante

EnableSSHKeySign yes|no à yes, active l'utilisation de ssh-keysign durant HostbaseddAuthentication

EscapeChar Définis le caractère d'échappement (défaut : ~)

ExitOnForwardFailure yes|no Indique si ssh termine la connexion s'il ne peut pas définir les ports forwardings dynamique, local, tunnel, et distant

FingerprintHash md5|sha256 Spécifie l'algorithme de hashage utilisé pour afficher les empreintes de clé

ForwardAgent yes|no Spécifie si la connexion à l'agent d'authentification est forwardée à la machine distante.

ForwardX11 yes|no Spécifie si les connexions X11 sont automatiquement redirigés dans la canal sécurisé.

ForwardX11Timeout timeout pour le forwarding X11 utilisant le format de temps. Les connexions après ce délai sont refusés

ForwardX11Trusted yes|no à yes, les clients X11 distants ont un accès complet à l'affichage X11 original. à no, les clients sont considérés comme non-sûres et bloqués pour éviter le vol ou la falsification des données des clients X11 de confiance.

GatewayPorts yes|no Spécifie si les hôtes distant sont autorisés à se connecter aux ports forwardés locaux. par défaut, ces ports sont liés à l'adresse de bouclage. Cela empêche d'autres hôtes de se connecter aux ports forwardés. Cette option peut être utilisée pour spécifier que ssh lie le port forwarding à l'adresse wildcard.

GlobalKnownHostsFile Spécifie un ou plusieurs fichiers à utiliser pour la base de clé hôte globale, séparé par ' '. Défaut : /etc/ssh/ssh_known_hosts, /etc/ssh/ssh_known_hosts2

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

GSSAPIDelegateCredentials yes|no Forward les accréditifs au serveur

HashKnownHosts yes|no Indique que ssh doit hasher les noms d'hôte et les adresses quand elles sont ajoutées à ~/.ssh/known_hosts.

HostbasedAuthentication yes|no Spécifie si l'authentification à clé publique basée sur l'hôte est permise

HostbasedKeyTypes Spécifie la liste des types de clé qui sont utilisé pour l'authentification basé sur l'hôte.

HostKeyAlgorithms Spécifie les algorithmes de clé hôte à utiliser par le client, dans l'ordre de préférence.

HostKeyAlias Spécifie un alias qui doit être utilisé à la place du vrai nom d'hôte en recherchant ou en sauvegardant la clé hôte dans les fichiers de base de clé hôte.

HostName Spécifie le nom d'hôte réel de connexion. Défaut : le nom spécifié sur la ligne de commande

IdentitiesOnly yes|no Spécifie que ssh devrait seulement utiliser l'identité d'authentification et les fichiers de certificat explicitement configurés dans ssh_config ou passés sur la ligne de commande, même si ssh-agent ou un PKCS11Provider offfre plus d'identitiés.

IdentityAgent Spécifie le socket unix utilisé pour communiquer avec l'agent d'authentification

IdentityFile Spécifie un fichier depuis lequel l'identité d'authentification DSA, ECDSA, Ed25519, ou RSA de l'utilisation est lu. Défaut : ~/.ssh/id_dsa, ~/.ssh/id_ecdsa, ~/.ssh/id_ed25519, ~/.sdsh/id_rsa.

IgnoreUnknown Spécifie une liste de motifs d'options inconnue à ignorer s'ils sont rencontrés dans la configuration

Include Inclus les fichiers de configuration spécifiés. Plusieurs fichiers peuvent être spécifié et peuvent contenir un wildcard

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.

KbdInteractiveDevices Spécifie la liste des méthodes à utiliser dans l'authentification interactive.

KexAlgorithms Spécifie les algorithmes d'échange de clé permis

LocalCommand Spécifie une commande à exécuter dans la machine locale après s'être connecté au serveur.

LocalForward [bind_address :]port Spécifie qu'un port TCP dans la machine local est forwardé via le canal sécurisé vers l'hôte :port distant. Seul root peut forwarder des ports privilégiés Par défaut, le port local est lié en accord avec GatewayPorts, si bind_address n'est pas spécifié

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

NoHostAuthenticationForLocalhost yes|no Peut être utilisé si le répertoire hôte est partagé. Dans ce cas localhost réfère à une machine différente dans chaque machine et l'utilisateur a des alerts sur les clés d'hôte changés. Cette option désactive l'authentification pour localhost.

NumberOfPasswordPrompts Spécifie le nombre de demande de mot de passe maximume. Défaut : 3

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

PermitLocalCommand yes|no Autorise l'exécution de commande locale via l'option LocalCommand

PKCS11Provider Spécifie le fournisseur PKCS#11 à utiliser.

Port Spécifie le port de connexion. Défaut : 22

PreferredAuthentications Spécifie l'ordre des méthodes d'authentification

ProxyCommand Spécifie la commande à utiliser pour se connecter au serveur. La chaîne s'étend à la fin de la ligne et est exécuté en utiisant exec

ProxyJump Spécifie un ou plusieurs sauts proxy. Plusieurs proxy peuvent être spécifié, et sont visités séquentiellement. Noter que cette option est en concurrence avec ProxyCommand, c'est le premier spécifié qui est utilisé

ProxyUseFdpass yes|no Spécifie que ProxyCommand passe un descripteur de fichier connecté à ssh au lieu de continuer à exécuter et passe des données.

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

PubkeyAuthentication yes|no Indique si l'authentification à clé publique est permise

RekeyLimit Spécifie la quantité maximum de données qui peuvent être transmis avant que la clé de session soit renégociée, optionnellement suivant par un délay. La taille peut être préfixé(K, M, G), le délay utilise le format de temps.

RemoteCommand Spécifie une commande à exécuter dans la machine distante une foi connecté au serveur. La chaîne s'étend à la fin de la ligne, et est exécuté avec le shell de l'utilisateur.

RemoteForward [bind_address :]port Spécifie qu'un port TCP dans la machine distante est forwardée dans le canal sécurisé à l'hôte :port dans la machine locale.

RequestTTY yes|auto|force|no Demande un pseudo-tty pour la session.

RevokedHostKeys Spécifie le clés publiques révoquées. Les clés listées dans ce fichier seront refusés pour l'authentification de l'hôte. Ce fichier peut être un fichier texte listant une clé publique par ligne, ou comme une liste de révocation de clé OpenSSH, tel que généré pa ssh-keygen.

SendEnv Spécifie quelles variables de l'environnement local sont envoyés au serveur. Le serveur doit également le supporter et doit les accepter Noter que TERM est toujours envoyé. Voir AcceptEnv dans sshd_config

ServerAliveCountMax Définis le nombre de message alive serveur qui peuvent être envoyés sans que ssh ne reçoive de réponse du serveur, terminant la session. Il est important de noter que ces messages sont différents de TCPKeepAlive, qui est spoofable. Défaut : 3

ServerAliveInterval Intervalle en secondes sans avoir reçu de données avant d'envoyer une requête au serveur. Défaut : 0 (désactivé)

StreamLocalBindMask umask utilisé en créant le socket unix. Utilisé uniquement pour le port forwarding vers un socket unix. Défaut : 0177

StreamLocalBindUnlink yes|no Spécifie si le socket unix est supprimé avant d'en créer un nouveaux.

StrictHostKeyChecking yes|ask|no à yes, ssh n'ajoute jamais automatiquement les clés hôte dans ~/.ssh/known_hosts, et refuse de se connecter si la clé hôte a changé.

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

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

Tunnel yes|point-to-point|ethernet|no Demande un périphérique tun entre le client et le serveur.

TunnelDevice local_tun[:remote_tun] Spécifie le périphérique tun à ouvrir. Les périphériques peuvent être spécifiés par ID ou le mot clé any qui utiliser le premier périphérique disponible

UpdateHostKeys yes|no|ask Spécifie si ssh accepte les notification de clé hôtes additionnels du serveur une fois l'authentification réussie et le ajoute à UserKnownHostsFile.

UsePrivilegedPort yes|no Spécifie l'utilisation d'un port privilégié pour les connexions sortantes. ssh doit être setuid root

User Spécifie l'utilisateur pour la connexion

UserKnownHostsFile Spécifie un ou plusieurs fichiers à utiliser pour la base de clé d'hôte utilisateur. Défaut : "~/.ssh/known_hosts ~/.ssh/known_hosts2"

VerifyHostKeyDNS yes|no|ask Indique si la clé distante est vérifié en utilisant DNS et les enregistrement SSHFP.

VisualHostKey yes|no À yes, une réprésentation ASCII de l'empreinte de la clé distante est affichée au login pour les clés hôte inconnues.

XAuthLocation Chemin du programme xauth. Défaut : /usr/X11R6/bin/xauth

Motifs

Un pattern consiste de 0 ou plusieurs caractères non-blanc '*' ou ' ?'. Par exemple, pour spécifier un jeu de déclarations pour un hôte dans le domaine .co.uk :

Host *.co.uk

Pour matcher un hôte dans le réseau 192.168.0.[0-9] :

Host 192.168.0.?

Un pattern-list est une liste de patterns. les patterns peuvent être inversé avec ' !'. Par exemple, pour autoriser une clé excepté depuis le pool dialup, l'entrée suivante dans authorized_keys :

from="!*.dialup.example.com,*.example.com"

Jetons

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

%% le caractère %

%C Raccourcis pour %I%h%p%r

%d home de l'utilisateur

%h Nom de l'hôte distant

%I UID local

%L Nom de l'hôte local

%I FQDN de l'hôte local

%n Nom de l'hôte distant, tel que donné sur la ligne de commande

%p Le port distant

%r Nom de l'utilisateur distant

%u Nom de l'utilisateur local

Les mots clés qui accèptent les jetons sont :

jetons permis

Match exec %%, %h, %L, %l, %n, %p, %r, %u.

CertificateFile %%, %d, %h, %l, %r, %u.

ControlPath %%, %C, %h, %i, %L, %l, %n, %p, %r, %u.

HostName %%, %h.

IdentityAgent

IdentityFile %%, %d, %h, %l, %r, %u.

LocalCommand %%, %C, %d, %h, %l, %n, %p, %r, %u.

ProxyCommand %%, %h, %p, %r.

RemoteCommand %%, %C, %d, %h, %l, %n, %p, %r, %u.

fichiers

~/.ssh/config Fichier de configuration de l'utilisateur. Ce fichier doit avoir les permissions suivantes : rw pour l'utilisateur, aucun pour les autres.

/etc/ssh/ssh_config Fichier de configuration système.