Kirish

Ubuntu Server qo'llanmasining ushbu bo'limida OpenSSH deb nomlangan tarmoqli kompyuterlar bilan masofadan boshqarish va ma'lumotlar almashinuvi uchun kuchli vositalar to'plami mavjud. Bundan tashqari, OpenSSH server ilovasi uchun mavjud konfiguratsion sozlamalarni va ularni Ubuntu tizimingizda qanday o'zgartirishni bilib olasiz.

OpenSSH - bu kompyuterlarning masofadan boshqarish vositalari va Secure Shell (SSH) protokoli yordamida fayllarni uzatish vositalarining oilaviy bepul versiyasi. Telnet va rcp kabi ushbu maqsadlar uchun ishlatiladigan an'anaviy uskunalar xavfsiz emas va foydalanuvchi parolini aniq matnga yuboradi. OpenSSH, xavfsizlik operatsiyalarini, shifrlangan masofadan boshqarish va fayl uzatishlarni osonlashtiradigan va eskirgan vositalarni samarali tarzda almashtirish uchun server protseduralari va mijoz ilovalarini taqdim etadi.

OpenSSH, sshd server komponenti doimiy mijoz dasturlarini istalgan dastur dasturidan kutadi. Aloqa so'rovi kelganda, sshd bog'langan mijoz turiga qarab, to'g'ri ulanish turini belgilaydi. Misol uchun, agar masofali kompyuter ssh-mijoz yordamida bog'lansa, OpenSSH-server autentifikatsiya qilinganidan keyin masofaviy boshqarish sessiyasini boshlaydi. Agar masofali foydalanuvchi scp orqali ulansa, OpenSSH serverining haqiqiyligi autentifikatsiya qilinganidan keyin server va mijoz o'rtasidagi fayllarni xavfsiz nusxalashni tashkil qiladi. OpenSSH muntazam parol, ochiq kalitni ishlatish va Kerberos sertifikatlarini o'z ichiga olgan turli autentifikatsiya usullarini qo'llashi mumkin.

OpenSSH mijozi va serverini o'rnatish oddiy. OpenSSH dasturini Ubuntu tizimiga o'rnatish uchun terminalda quyidagicha buyruqni bajaring:

sudo apt install openssh-client

OpenSSH serverini va barcha kerakli fayllarni o'rnatish uchun ushbu buyruqni terminalda bajaring:

sudo apt install openssh-server

Konfiguratsiya  
  
Sshd, / etc / ssh / sshd\_config faylini tahrirlash orqali OpenSSH server dasturining standart xatti-harakatlarini sozlashingiz mumkin. Ushbu faylda ishlatiladigan konfiguratsiya ko'rsatmalari haqida ma'lumot olish uchun tegishli buyruqni terminalda buyruq qatorida quyidagi buyruq bilan ko'rishingiz mumkin:

man sshd\_config

Aloqa sozlamalari va autentifikatsiya usullari kabi narsalarni boshqaradigan sshd konfiguratsiya faylida bir qancha ko'rsatmalar mavjud. / Etc / ssh / sshd\_config faylini tahrirlash orqali o'zgartirish mumkin bo'lgan konfiguratsiya ko'rsatmalariga misollar quyida keltirilgan.

Sozlamalar faylida o'zgarishlar qilishdan oldin asl faylning nusxasini olishingiz va uni yozishdan saqlanishingiz kerak. Buning yordamida original sozlamalarni ko'rishingiz mumkin va agar kerak bo'lsa, ushbu sozlamalarga qaytasiz.  
  
/ Etc / ssh / sshd\_config faylining nusxasini yarating va terminalda quyidagi buyruqlarni yozish orqali uni yozilishdan saqlang:

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.original

sudo chmod a-w /etc/ssh/sshd\_config.original

Quyida siz o'zgartirishingiz mumkin bo'lgan konfiguratsiya ko'rsatmalari misollari keltirilgan:

OpenSSH xizmatining TCP portini 2222 standart TCP porti o'rniga tinglashini sozlash uchun Port direktivini quyidagi kabi o'zgartiring:

Port 2222

Sshd-ga umumiy kalitlarga asoslangan ma'lumotlar bilan foydalanuvchi autentifikatsiya qilish protsedurasidan foydalanishga ruxsat berish uchun quyidagi qatorlarni qo'shing yoki o'zgartiring:

PubkeyAuthentication yes

Agar chiziq allaqachon mavjud bo'lsa, unda sharhlanmaganligiga ishonch hosil qiling.

OpenSSH serveringiz /etc/issue.net faylining mazmunini login qilishdan oldin xabar sifatida ko'rsatish uchun quyidagi qatorlarni qo'shing yoki o'zgartiring:

Banner /etc/issue.net

В файле /etc/ssh/sshd\_config.

/etc/ssh/sshd\_config faylga o'zgarishlar kiritganingizdan so'ng uni saqlang va o'zgarishlarni amalga oshirish uchun terminalda quyidagi buyruqni ishga tushirib, sshd server dasturini qayta ishga tushiring:

sudo systemctl restart sshd.service

Server dasturining xatti-harakatlarini sizning ehtiyojlaringizga o'zgartirish uchun boshqa sshd konfiguratsiya ko'rsatmalari mavjud. Biroq, serverga kirishning yagona usuli ssh bo'lsa va siz / etc / ssh / sshd\_config faylida sshd bilan tuzilma xatoligini yaratgan bo'lsangiz, serveringiz qayta ishga tushirilgunga qadar qulflangan bo'lishi mumkin. Bunga qo'shimcha ravishda, noto'g'ri konfiguratsiya direktifi ko'rsatilgan bo'lsa, sshd server yuklashni rad qilishi mumkin, shuning uchun ushbu faylni uzoq serverga tahrirlashda juda ehtiyot bo'ling.

SSH kalitlari  
SSH tugmachalari foydalanuvchilarga parol kiritish kerak bo'lmasdan ikkita asosiy kompyuter o'rtasida autentifikatsiya qilish imkonini beradi. Ssh kalitlari uchun haqiqiylik ikki kalitdan iborat: maxfiy va ommaviy.  
  
Klaviatura yaratish uchun terminalda so'rovni kiriting:

ssh-keygen -t rsa

Bu RSA algoritmidan foydalanib kalitlarni ishlab chiqaradi. Jarayon davomida sizga parol so'raladi. Kalitni yaratish talab qilingan vaqtda, "Enter" tugmasini bosing.  
  
Odatiy bo'lib, umumiy kalit ~ / .ssh / id\_rsa.pub faylida saqlanadi, ~ / .ssh / id\_rsa esa xususiy kalit hisoblanadi. Endi id\_rsa.pub faylini uzoqdan xostga nusxa oling va uni ~ / .ssh / authorized\_keys-ga kirib, unga qo'shing:

ssh-copy-id username@remotehost

So'ngra, authorized\_keys faylining ruxsatini ikki marta tekshiring. Faqat autentifikatsiya qilingan foydalanuvchi ushbu faylga o'qish va yozish uchun ruxsat berishi kerak. Agar huquqlar noto'g'ri o'rnatilgan bo'lsa, ularni o'zgartiring:

chmod 600 .ssh/authorized\_keys

Endi bu parolni kiritmasdan SSH-ga ulanish imkoniyati mavjud.