

Müəllim – Fəxri Niftalizadə

Tələbə - Samir Eldarov

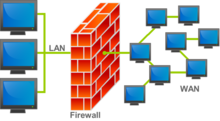
Qrup – 651.20

Fənn – Big Data

Mövzu – Firewall,SSH,Hadoop

# Firewall

Hesablamada firewall əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydaları əsasında daxil olan və gedən şəbəkə trafikinə nəzarət edən və nəzarət edən şəbəkə təhlükəsizlik sistemidir. Firewall adətən etibarlı şəbəkə ilə İnternet kimi etibarsız şəbəkə arasında maneə yaradır. Firewalllar şəbəkə əsaslı və ya host əsaslı sistem kimi təsnif edilir. Şəbəkəyə əsaslanan firewalllar iki və ya daha çox şəbəkə arasında, adətən yerli şəbəkə (LAN) və geniş ərazi şəbəkəsi (WAN) arasında yerləşdirilir. Onlar ya ümumi təyinatlı aparatda işləyən proqram təminatı, ya da xüsusi təyinatlı avadanlıqla işləyən aparat cihazıdır. avadanlıq və ya hipervizor tərəfindən idarə olunan virtual hostda işləyən virtual cihaz. Firewall cihazları həmçinin DHCPor VPN xidmətləri kimi firewall olmayan funksionallıq təklif edə bilər. Şəbəkə trafikinə və ya digər hesablama resurslarına nəzarət etmək üçün host əsaslı firewalllar birbaşa hostun özündə yerləşdirilir. Bu, əməliyyat sisteminin bir hissəsi kimi bir demon və ya xidmət və ya qorunmaq üçün agent tətbiqi ola bilər.



**SSH**

Secure Shell və ya Secure Socket Shell kimi də tanınan SSH, istifadəçilərə, xüsusən də sistem administratorlarına təhlükəsiz olmayan şəbəkə üzərindən kompüterə daxil olmaq üçün təhlükəsiz yol verən şəbəkə protokoludur.

SSH həmçinin SSH protokolunu həyata keçirən kommunal proqramlar dəstinə aiddir. Secure Shell güclü parol identifikasiyası və açıq açarın autentifikasiyası, həmçinin internet kimi açıq şəbəkə üzərindən qoşulan iki kompüter arasında şifrələnmiş məlumat rabitəsini təmin edir.

Güclü şifrələməni təmin etməklə yanaşı, SSH şəbəkə administratorları tərəfindən sistemləri və proqramları uzaqdan idarə etmək üçün geniş şəkildə istifadə olunur ki, bu da onlara şəbəkə üzərindən başqa kompüterə daxil olmaq, əmrləri yerinə yetirmək və faylları bir kompüterdən digərinə köçürmək imkanı verir.SSH həm kriptoqrafik şəbəkə protokoluna, həm də həmin protokolu həyata keçirən kommunal proqramlar dəstinə aiddir. SSH, seansın göstərildiyi son olan Secure Shell müştəri tətbiqini sessiyanın bitdiyi son olan SSH serveri ilə birləşdirən müştəri-server modelindən istifadə edir. SSH tətbiqləri tez-tez terminal emulyasiyası və ya fayl köçürmələri üçün istifadə olunan proqram protokollarına dəstək daxildir.

SSH digər proqram protokolları üçün təhlükəsiz tunellər yaratmaq üçün də istifadə edilə bilər, məsələn, X Window System qrafik sessiyalarını uzaqdan təhlükəsiz şəkildə idarə etmək üçün. SSH serveri, standart olaraq, standart Transmission Control Protocol (TCP) 22 portunu dinləyir.

SSH necə işləyir?

Secure Shell, Telnet, rlogin (uzaqdan giriş) və rsh (uzaq qabıq) kimi etibarlı olmayan terminal emulyasiyasını və ya giriş proqramlarını əvəz etmək üçün yaradılmışdır. SSH eyni funksiyaları -- uzaq sistemlərdə terminal seanslarına daxil olmaq və işləmək imkanı verir. SSH həmçinin Fayl Transfer Protokolu (FTP) və rcp (uzaqdan nüsxə) kimi fayl ötürmə proqramlarını əvəz edir.

**Hadoop setup in ubuntu**

Addım 1: Java Quraşdırması.

Addım 2: Hadoop İstifadəçisi Yaradın (Könüllü) .

Addım 3: Parolsuz SSH-ni konfiqurasiya edin.

Addım 4: Hadoop istifadəçisində Apache Hadoop-u quraşdırın və konfiqurasiya edin.

Addım 5: Java Ətraf dəyişənlərini konfiqurasiya edin.

Addım 6: Əsas saytı redaktə edin.

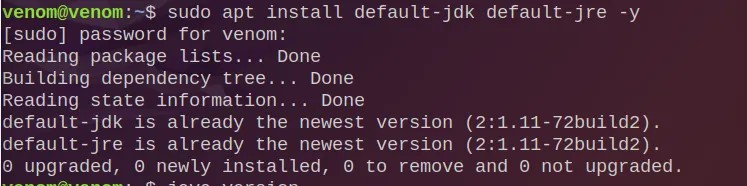
Addım 7: Hdfs-saytını redaktə edin.

**Giriş**

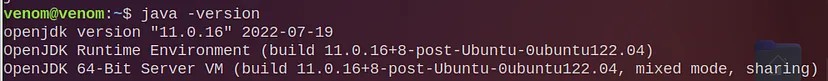
Apache Hadoop proqram kitabxanası kompüter klasterləri arasında böyük məlumat həcmlərinin paylanmış emalı üçün çərçivə təmin edir. Tək serverdən tutmuş minlərlə cihaza qədər, hər biri yerli hesablama və saxlama təmin edir, onun miqyasını genişləndirmək nəzərdə tutulur. Kitabxananın özü yüksək əlçatanlığı təmin etmək üçün avadanlığa etibar etməkdənsə, tətbiq səviyyəsindəki problemləri müəyyən etmək və idarə etmək üçün nəzərdə tutulmuşdur. Nəticə etibarı ilə, hər biri nasazlıqlara məruz qala bilən kompüterlər klasterinin üzərinə yüksək əlçatan xidmət təqdim olunur.

**Addım 1: Java Quraşdırması**

* 1. Ən son və ya istədiyiniz java versiyasını quraşdırın



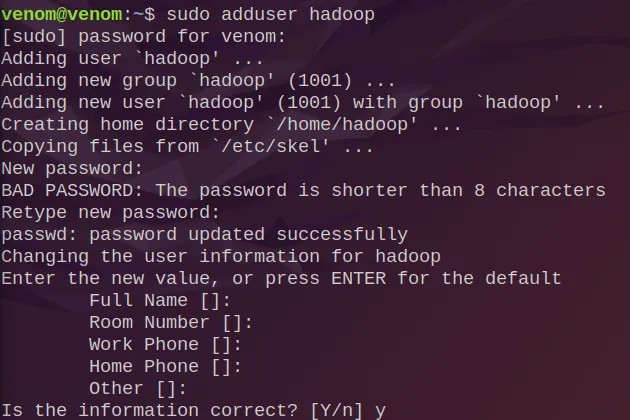
1.2 Java versiyasını yoxlayın



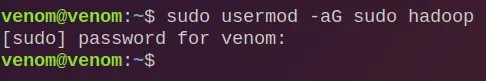
**Addım 2: Hadoop İstifadəçisi Yaradın (Könüllü)**

Hadoop fayllarını müstəqil idarə etmək istəyirsinizsə, fərqli bir istifadəçi (Hadoop istifadəçisi) yaradın.

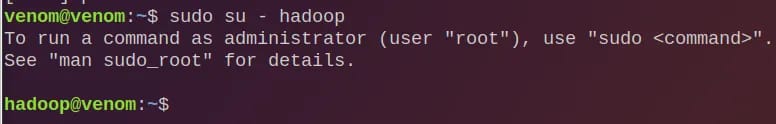
2.1 Hadoop adlı yeni istifadəçi yaradın .



2.2 Hadoop istifadəçisini sudo qrupunun üzvü edin.

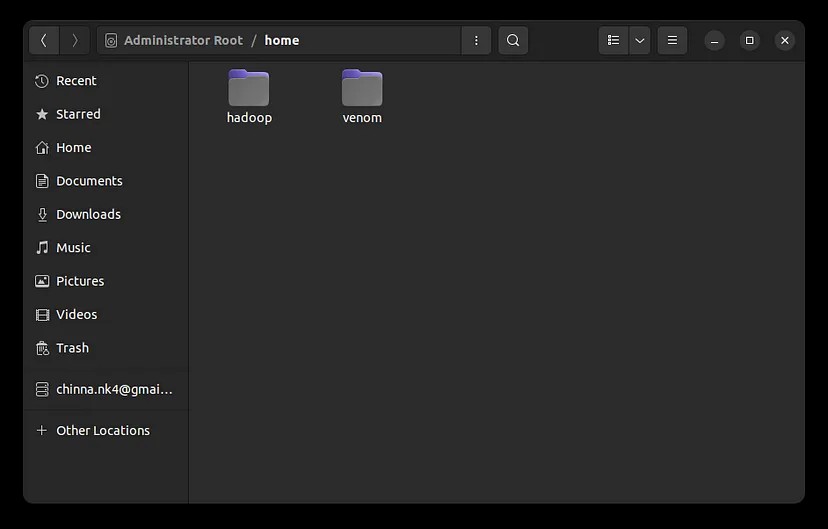


2.3 İndi Hadoop istifadəçisinə keçin.



İndi əməliyyat sisteminizdə iki istifadəçi görə bilərsiniz.

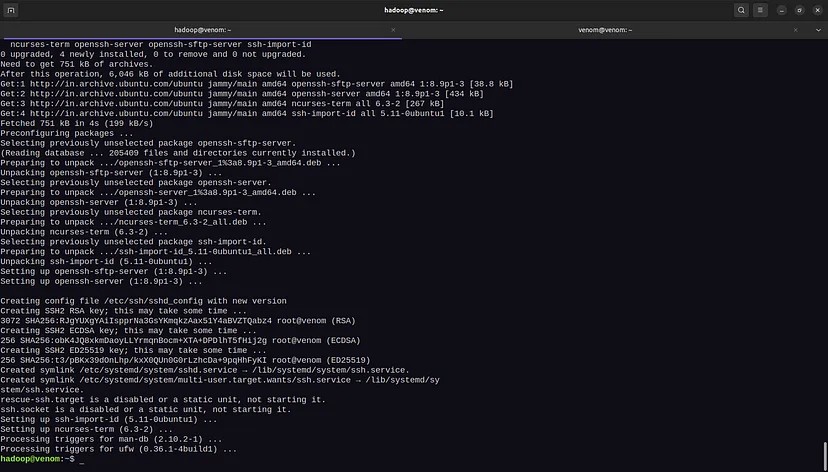
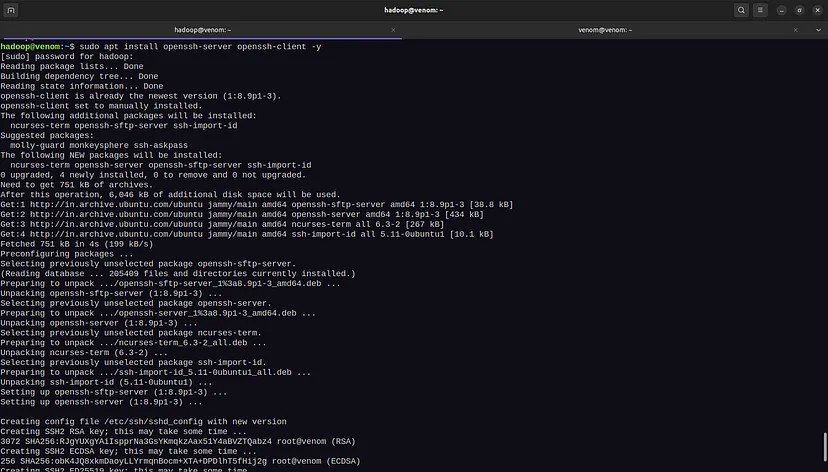
Faylları açın > Digər yerlər > Kompüter > ev



**Addım 3: Parolsuz SSH-ni konfiqurasiya edin**

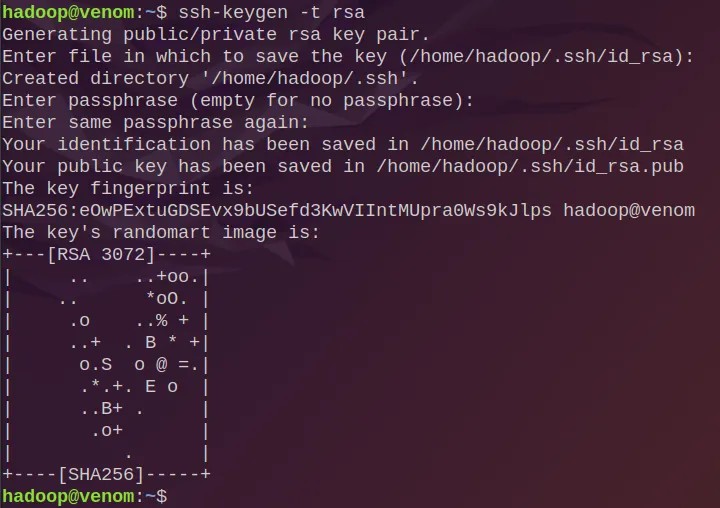
Qeyd : Əgər 2-ci addımı tamamladınızsa, hadoop istifadəçisinə keçdikdən sonra 3-cü addıma keçin ( sudo su — hadoop ).

3.1 OpenSSH server və müştəri quraşdırın



SSH-keygen yeni SSH autentifikasiya açar cütlərini yaratmaq üçün bir vasitədir. Belə açar cütləri girişləri avtomatlaşdırmaq, tək girişi aktivləşdirmək və hostların autentifikasiyası üçün istifadə olunur.

3.2 Açıq və gizli açar cütlərini yaradın.

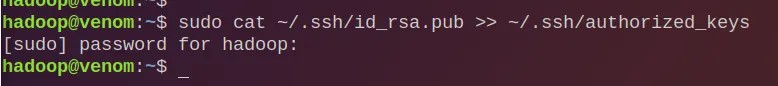


SSH protokolu açıq açar kriptoqrafiyasından istifadə edərək hostları və istifadəçiləri autentifikasiya edir. Keygen proqramı SSH açarları kimi tanınan autentifikasiya açarlarını yaratmaq üçün istifadə olunur.

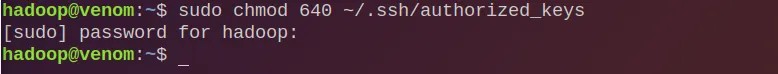
Older.rhosts autentifikasiyasına daha təhlükəsiz alternativ olaraq SSH açıq açar autentifikasiyasını təqdim etdi. O, parolların fayllarda saxlanmasına olan ehtiyacı aradan qaldıraraq təhlükəsizliyi artırıb, eləcə də istifadəçinin parolunu oğurlayan serverin oğurlanması ehtimalını aradan qaldırıb.

SSH açarları, parollar kimi, autentifikasiya etimadnaməsidir. Nəticədə, onlar istifadəçi adları və parollara bənzər şəkildə idarə edilməlidir. Onların lazımi xitam prosesi olmalıdır ki, açarlar artıq tələb olunmayanda çıxarılsın.

3.3 Yaradılmış açıq açarı id\_rsa.pub - dan avtorizasiya\_açarlarına əlavə edin



3.4 Autized\_keys üçün fayl icazələrini dəyişdirin .



Yuxarıdakı əmrdə chmod dəyişdirmə rejimidir

3.5 Parolsuz SSH-nin işlədiyini yoxlayın.

