نظام الملفات File System



نظام الملفات File System

1-1 المقدمة

ما هو نظام الملفات ؟

مفهوم نظام الملفات ينقسم إلى قسمين:

- بنية المجلد: Directory Structure البنية الهيكلية لإنشاء وتخزين الملفات والمجلدات ضمن القرص الصلب.وهي متشابهة في معظم أنظمة لينكس (الفقرة 1-5 مجلدات البنية الشجرية)
- التنظيم الأولي Low Level Organization المستخدم في القرص الصلب لتخزين البيانات (أصفار ووحدات) وهي تختلف من نظام ملفات لآخر.

ويتميز نظام ملفات عن آخر بكيفية إصلاح الأخطاء والزمن الذي يحتاجه للإصلاح وإمكانية استخدام الأسماء الطويلة أو القصيرة وحجم الملفات القادر على تخزينها. فمثلا أنظمة ملفات مثل يونكس أو لينكس تسمح بتخزين ملفات يصل حجم الملف الواحد إلى 16TB.

تختلف أسماء أنظمة الملفات من نظام تشغيل لآخر، فمثلاً:

نظام يونكس ufs- لينكس ريدهات ext - دوس fat - نظام win/NT fat32,NTFS .

2-1 عناصر نظام الملفات [1]

يتألف نظام الملفات من مجموعة من العناصر وهي:

- [1] System Administrator's Guide

1-2-1 قطاع الإقلاع: *boot block*

وهو القطاع رقم 0 ضمن القسم من القرص الذي يحوي نظام الملفات ويحوي معلومات عن مكان وجود برنامج الإقلاع.

1-2-2 *super block*

القطاع الذي يلي قطاع الإقلاع ورقمه 1 يحتوي معلومات عن نظام الملفات الموجود ضمن هذا القسم من القرص الصلب مثل رقم قطاع البداية وعدد القطاعات الموجودة ورقم قطاع النهاية وعدد العقد i-node المتوفرة و عدد قطاعات العقد الفارغة.

1-2-3 عقد الفهرسة *i-node*

عبارة عن مؤشر إلى كل عنصر من عناصر نظام الملفات (أي الملفات والمجلدات)، يحوي معلومات عن الملف مثل اسمه –اسم المالك– الحجم– السماحيات–تاريخ الإنشاء أو التعديل وتاريخ آخر وصول–حجم الملف – عدد الارتباطات. يختلف عدد قطاعات عقد الفهرسة تبعا لحجم نظام الملفات المحدد.

ملاحظة :

عند تنفيذ فحص القرص بواسطة الأمر fsck فإن النظام يقارن بين معلومات عقد الفهرسة للملفات وبين ما هو موجود على القرص الصلب وهذا مشابه لنظام ويندوز ودوس حيث يقوم جدول fat بتخزين أسماء الملفات والمجلدات ومواقعها وأماكن وجودها على القرص الصلب وعند تنفيذ وإجراء scandisk يقوم بمقارنة محتويات جدول fat مع محتويات القرص الصلب.

1-2-4 منطقة التخزين *storage blocks*

تمثل المنطقة المتبقية من حجم نظام الملفات والتي تستخدم لتخزين البيانات.

1-2-5 الارتباطات *Links*

يؤمن نظام لينكس نوعين من الارتباطات:

الارتباط الصلب hard link

يضيف مسار إضافي لملف وحيد ضمن نفس نظام الملفات، كل مرجع لمجلد له نفس رقم عقدة الفهرسة.

خصائصه:

- لا يتم بين نظامي ملفات مختلفين.
- رقم العقدة يتناقص بعملية الحذف بواسطة الأمر rm ، الملف موجود طالما هناك ارتباطات صلبة به.
- يحذف الملف عندما يصبح عدد الارتباطات 0.
- رقم عقدة الفهرسة للملف الأصلي هو نفس رقم العنصر المرتبط به.
- يمكن مشاهدة رقم عقدة الفهرسة بالأمر (ls -i) .

```
[root@mail ~]# ln ex2.cpp new-ex2
[root@mail ~]# ls -i new-ex2
1245662 new-ex2
[root@mail ~]# ls -i ex2.cpp
1245662 ex2.cpp
```

الشكل 1-1 إنشاء الارتباط الصلب

- يظهر في خرج الأمر (ls -l) لأي مجلد ضمن الحقل الثاني رقم يشير إلى عدد العناصر المرتبطة بهذا المجلد من آباء وأبناء وعند حذف أي ملف من هذا المجلد نجد أن هذا الرقم يتناقص إلى أن يشير للرقم الصفر.
- إنشاء ارتباط صلب:

ln filename linkname

الارتباط المرن symbolic link

يسمى أيضا الاختصار shortcut، أي إنشاء رمز يحوي مسار الوصول للعنصر الأصلي.

خصائصه:

- يظهر نوع الملف (l) عند تنفيذ أمر (ls -l).
- لكلا منهما رقم عقدة فهرسة مختلف. كما في الشكل التالي:

```
1180163 lrwxrwxrwx 1 root root 11 Jun 24 02:28 S99local -> ../rc.local
[root@mail ~]# ls -i /etc/rc.d/rc.local
1180155 /etc/rc.d/rc.local
```

الشكل 1-2 إنشاء الارتباط المرن

- يمكن أن تتم بين نظامي ملفات مختلفين.
- إنشاء ارتباط مرن:

ln -s filename linkname

يظهر الشكل التالي إنشاء الارتباط المرن، ورقم العقد الخاص بكل منهما والنوع.

```
root@mail ~]# ln -s ex1.c Desktop/
root@mail ~]# ls -i Desktop/
98849 ex1.c      98684 lab-handout-S10.ppt   98587 Squid.pdf            205449 Xen
98558 IPtables   98689 S5-S6 Lab Files       98609 vmware-tools-distrib
root@mail ~]# ls -i ex1.c
245656 ex1.c
root@mail ~]# ls -il Desktop/ex1.c
8849 lrwxrwxrwx 1 root root 5 Oct 22 17:10 Desktop/ex1.c -> ex1.c
root@mail ~]# ls -il ex1.c
245656 -rw-r--r-- 1 root root 79 Sep 25 06:57 ex1.c
```

الشكل 1-3 إنشاء الارتباط المرن

1-2-6 ملفات الأجهزة *device file*

يتميز نظام يونكس و لينكس بأنه يتعامل مع كافة الأجهزة المادية المتوفرة ضمنه وكأنها ملفات لتمكين البرامج من الاتصال بالمكونات المادية

للحاسب، فعند إنشاء النواة يتم ربطها مع هذه الملفات والتي تحوي تفاصيل إدارة الأجهزة والتعامل معها، فهي وسيلة اتصال بالأجهزة وليس الأجهزة ذاتها.

تصنف هذه الأجهزة المادية إلى نوعين :

الأجهزة المحرفية character devices

وهي الأجهزة التي يتم تخزينها وتعاملها مع البيانات محرف محرف ولا تحتاج إلى ذواكر buffer لتخزين البيانات قبل تخزينها مثل الشاشات و الطابعات و أجهزة النسخ الاحتياطي tape، تظهر هذه الملفات عند استعراض محتويات المجلد dev/:

ls -l /dev

إذ تظهر أنواعها مبتدئة بالحرف c ليشير أنها ملفات أجهزة تتعامل مع المحارف.

الأجهزة الكتلية block devices

الأجهزة التي تستخدم طريقة تخزين عشوائية ، وتتعامل مع مقاطع دخل وخرج كبيرة وتحتاج إلى أن تقوم النواة بعملية التخزين المؤقتة لهذه المقاطع عوضا عنها، مثل الأقراص الصلبة والمرنة والليزرية.

تظهر كملفات ضمن مجلد dev/ وبنوع b قبل السماحيات، وهذا مناسب للأجهزة المصممة لتخزين البيانات(الأقراص الصلبة) بسبب توفر إمكانية ترتيب المعلومات قبل كتابتها على القرص مما يعطي كتابتها وتنظيمها فعالية أكثر.

لا تتم عملية الكتابة ضمن هذه الملفات وإنما تستخدم لتحديد كيفية التعامل مع الأجهزة المرتبطة بها لإجراء عمليات الدخل والخرج إليها.

```
brw-r----- 1 root disk     1,    7 Oct 16 05:50 ram7
brw-r----- 1 root disk     1,    8 Oct 16 05:50 ram8
brw-r----- 1 root disk     1,    9 Oct 16 05:50 ram9
lrwxrwxrwx 1 root root           4 Oct 16 05:52 ramdisk -> ram0
crw-rw-rw- 1 root root     1,    8 Oct 16 05:52 random
crw------- 1 root root   162,    0 Oct 16 05:52 rawctl
brw------- 1 root root   253,    0 Oct 16 05:50 root
crw-r--r-- 1 root root    10,  135 Oct 16 05:50 rtc
brw-r----- 1 root disk     8,    0 Oct 16 05:50 sda
brw-r----- 1 root disk     8,    1 Oct 16 05:52 sda1
brw-r----- 1 root disk     8,    2 Oct 16 05:50 sda2
brw-r----- 1 root disk     8,   16 Oct 16 05:50 sdb
crw------- 1 root root    14,    1 Oct 16 05:52 sequencer
crw------- 1 root root    14,    8 Oct 16 05:52 sequencer2
crw------- 1 root root    21,    0 Oct 16 05:52 sg0
crw------- 1 root root    21,    1 Oct 16 05:52 sg1
drwxrwxrwt 2 root root          40 Oct 16 05:52 shm
crw------- 1 root root    10,  231 Oct 16 05:52 snapshot
drwxr-xr-x 2 root root         180 Oct 16 05:52 snd
lrwxrwxrwx 1 root root          15 Oct 16 05:52 stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root          15 Oct 16 05:52 stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root          15 Oct 16 05:52 stdout -> /proc/self/fd/1
crw------- 1 root root     4,    0 Oct 16 05:50 systty
crw-rw-rw- 1 root tty      5,    0 Oct 16 05:52 tty
crw-rw---- 1 root root     4,    0 Oct 16 05:50 tty0
crw------- 1 root root     4,    1 Oct 16 05:54 tty1
crw-rw---- 1 root tty      4,   10 Oct 16 05:50 tty10
crw-rw---- 1 root tty      4,   11 Oct 16 05:50 tty11
crw-rw---- 1 root tty      4,   12 Oct 16 05:50 tty12
crw-rw---- 1 root tty      4,   13 Oct 16 05:52 tty13
crw-rw---- 1 root tty      4,   14 Oct 16 05:52 tty14
crw-rw---- 1 root tty      4,   15 Oct 16 05:52 tty15
```

الشكل 1-4 محتوى مجلد dev

تتميز هذه الملفات بوجود رقمين يظهران عند تنفيذ الأمر (ls -l /dev) وذلك في عمود الحجم (كما يظهر الشكل السابق 1-4) وهذان الرقمان هما:

الرقم الأساسي major number

ويشير هذا الرقم إلى إحدى الجدولين للأجهزة الكتلية أو المحرفية (أي هل سيبعث محرف أم كتل وهل هو قرص صلب أم مرن أم شاشة ....) لتحديد نوع هذا الجهاز. كافة الأجهزة التي لها ذات الرقم major تتبع نفس التعريف ضمن نظام التشغيل. فكافة الأقراص الصلبة sda لها رقم 8.

الرقم الثاني minor number

يستخدم هذا الرقم لتحديد أي الأجهزة من النوع الذي تم تحديده من خلال رقم major سيتم استعمالها، كافة الأجهزة التي تتبع نوع معين لها رقم major وحيد متشابه وتختلف ب minor.

1-2-7 مجلد التحميل *mount point*

في الأنظمة المفتوحة open source يعتبر مجلد التحميل هو المجلد الذي سيتم إسناد نظام الملفات إليه. وباعتبار أن أنظمة الملفات موجودة على أقسام مستقلة partitions ضمن القرص الصلب فسيكون لها مجلد تحميل أو جذر ملفات، ولكن كافة هذه الأنظمة وكافة هذه الأقسام ستسند إلى جذر شجرة الملفات الأصلي / وهو root وستظهر هذه الأقسام وكأنها مجلدات تتبع الجذر.

ترتبط هذه الأنظمة مع مجلداتها مع المجلد الجذر / عند الإقلاع من خلال قراءة الملف /etc/fstab والذي يحتوي معلومات عن الأقسام الموجودة على القرص الصلب وأنواعها والخيارات المتعلقة بها وأنظمة الملفات المعرفة ضمنها.

أما في ويندوز فيبقى كل قرص أو قسم من القرص الصلب له دليل جذر رئيسي خاص به (E:\ , D:\ , c:\ وهكذا) ، وتظهر كأقراص صلبة مستقلة ضمن My Computer.

1-3 الملف /etc/fstab [2]

ملف نصي يمكن فتحه وتعديله من قبل المشرف فقط، كل سطر ضمنه يشير إلى نظام ملفات معرف ضمن نظام التشغيل. يتم قراءة fstab عند كل إقلاع ويربط مجلدات تحميل هذه الأنظمة مع المجلد الجذر /، علماً أن الترتيب في تسلسل تحميل هذه الأنظمة مهم إذ لا يمكن أن يحمل نظام ملفات /proc قبل تحميل المجلد الجذر الأساسي /.

محتوى السطر الواحد:

Device file mount point file system type options sync seq

- [2] Red Hat Enterprise Linux 5 Deployment Guide

```
[root@localhost root]# cat /etc/fstab
LABEL=/                 /                       ext3    defaults        1 1
none                    /dev/pts                devpts  gid=5,mode=620  0 0
none                    /proc                   proc    defaults        0 0
none                    /dev/shm                tmpfs   defaults        0 0
/dev/hda2               swap                    swap    defaults        0 0
/dev/cdrom              /mnt/cdrom              iso9660 auto,user,kudzu,ro 0 0
/dev/fd0                /mnt/floppy             auto    auto,user,kudzu 0 0
/dev/hda5               /win                    vfat    auto
/dev/hdb1               /win3                   vfat    auto
/dev/hda4               /win2                   vfat    auto
```

الشكل 1-5 الملف fstab

كل سطر مؤلف من:

- اسم ملف الجهاز device file.
- مجلد التحميل mount point.
- نوع نظام الملفات file system type.
- الخيارات: تحدد كيفية تحميل نظام الملفات:

Auto: تحميل نظام الملفات تلقائياً عند إقلاع النظام.

noauto: إجراء تحميل يدوي لنظام الملفات عند الحاجة من قبل المشرف وليس تلقائياً عند الإقلاع.

nouser: منع تحميل نظام الملفات من قبل المستخدم العادي.

user: السماح للمستخدم العادي بإجراء تحميل لنظام الملفات وإلغاء تحميله, مثل السواقة الليزرية والفلاش usb.

users: السماح للمستخدم العادي بإلغاء تحميل نظام ملفات قام بتحميله مستخدم آخر.

kudzu: للكشف عن نظام الملفات تلقائياً عند إقلاع نظام لينكس.

ro: تحميل نظام الملفات بصفة للقراءة فقط.

rw: تحميل نظام الملفات بصفة للقراءة والكتابة.

defaults: يحوي الخيارات الافتراضية لنظام الملفات وهي rw,nouser,auto,dev,suid.

suid: يصبح أي مستخدم لنظام الملفات مالكا له.

dev: للسماح باستخدام ملفات الأجهزة المعرفة ضمن نظام الملفات.

Owner: تمكين مالك الجهاز المادي من إجراء تحميل لنظام الملفات.

- حقل sync ويأخذ قيمة 1 اذا اردنا الكتابة مباشرة على الجهاز المادي مثل القرص المرن و usb فلاش وغير مجدية مع الأقراص الصلبة وتأخذ صفر اذا لا نريد الكتابة مباشرة.
- حقل seq يشير لترتيب إجراء fsck فحص أنظمة الملفات الواردة في الملف fstab وإذا وضعت صفر فلا يهم الترتيب.

1-4 أنواع أنظمة الملفات [3]

Second Extended Filesystem:*Ext2*

يعتبر نظام الملفات القياسي لنظام لينكس وسيئته هي الوقت المستخدم لمحاولة إصلاح النظام عند الإقلاع، يستطيع التعامل مع ملفات ذات أسماء طويلة أو قصيرة.

third Extended Filesystem:*Ext3*

أنشئ مع نسخة ريدهات 7.2، مبني على نظام الملفات ext2.

خصائصه:

[3] Red_Hat_Enterprise_Linux-5-Deployment_Guide-en-US.pdf
https://www.tldp.org/LDP/sag/html/filesystems.html

- دعم ميزة journaling التصفح التي تمكن نظام الملفات من متابعة حركة رأس القرص الصلب ومعرفة ما يحدث لنظام الملفات والبيانات بشكل مستمر وتلقائي ويسجل عناوين القطاعات التي تم تعديلها على القرص. في حال حدوث خطأ في نظام الملفات لا يضطر النظام لفحص كامل نظام الملفات وإنما يفحص محتوى المتصفح أي فقط ما تم تعديله من أخر عملية فحص، ويقارنها مع محتويات القرص الصلب مما يقلل من الوقت اللازم لفحص نظام الملفات عند حدوث خطأ ما وهذا الزمن يقارب ثانية وأقل.
- دعم حجم نظام ملفات أعظمي 16TB.
- حجم ملف أعظمي 2 TB.
- يمكن أن يصل عدد المجلدات الفرعية في مجلد إلى 32000.

Fourth Extended File system:Ext4

ظهر مع نواة Linux 2.6.28 و يشكل تطورا كبيرا نسبة ل ext3 فهو يعدل في بنية بيانات نظام الملفات، مما يحسن التصميم والأداء و الوثوقية. خصائصه:

- يدعم حجم نظام ملفات أعظمي (exabytes) 1EB(1EB=1,048,576TB).
- حجم ملف أعظمي 16 TB بسبب إضافته بلوك 48 بت للعنونة (وليس 64 بت وهو يحتاج لبعض التعديلات للانتقال).
- عدد المجلدات الفرعية غير محدد.
- الملفات الكبيرة تجزأ في عدة أقسام (القسم هو عدة بلوكات فيزيائية متجاورة) مما يحسن الأداء ويقلل التجزئة.
- يستخدم آلية multiblocking وضع عدة بلوكات معا واستدعائها بطلب واحد عوضا عن كل بلوك بطلب، مما يحسن الأداء والسرعة.

- Journal Checksumming: افتراضيا غير مؤهلة، تتأكد أن البيانات المصنفة سليمة أو معطوبة، مع الفرق أنها تنجزه بمرحلة واحدة وليس مرحلتين كما في ext3.

- **الانتقال:**

يمكن الانتقال من نظام ملفات إلى ext4 وبالتالي ستأخذ البيانات الجديدة التصميم الجديد بدون التعديل في بنية البيانات القديمة مع الإبقاء على إمكانية التعديل والقراءة لها. علماً أنه بعد الانتقال لا يمكن العودة لنظام الملفات السابق. وللانتقال نستخدم الأمر:

tune2fs -O extents,uninit_bg,dir_index /dev/yourfilesystem

بعد ذلك، يجب تنفيذ الأمر fsck ثم إعادة تحميل نظام الملفات.

XFS [4]

نظام الملفات الجديد الافتراضي مع نسخة ريدهات 7 ، صمم في مختبرات Silicon Graphics, Inc.

خصائصه:

- حجم نظام الملفات أكبر من 16EB (exabytes) .
- حجم الملف الواحد 8EB.
- 10 مليون مستوى للمجلدات المعشعشة.
- يتميز بالأداء العالي.
- قابلية التعديل.
- تسريع خاصية journaling لإصلاح أخطاء القرص.
- إمكانية إلغاء التجزئة وتكبير الحجم أثناء تحميل وعمل نظام الملفات.
- توفر أداة النسخ الاحتياطي والاستعادة الخاصة به.

4 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux /7 /html /storage_administration_guide/ch-xfs

NFS (network file system) نظام ملفات الشبكة

يمكن نظام ملفات nfs من تصدير نظام ملفات أو قسم من القرص الصلب أو مجلد ما إلى أجهزة أخرى عبر الشبكة. مما يسهل مركزية تخزين البيانات على مخدم وحيد ويتميز بأنه لا داعي لإجراء تهيئة لهذا النوع من أنظمة الملفات عند تعريفها وإنما يستخدم لدعم عمليات الدخل والخرج للقرص المحلي وذلك بشكل مغاير لباقي أنظمة الملفات والتي تتطلب وجود قرص صلب محلي. هذا يمكن من مشاركة ملفات عبر عدد من الحواسب.

msdos

نظام ملفات fat لكن بأسماء ملفات صغيرة 8 أحرف ،بدون تغير صفات الملف مثل السماحيات والملكية.

vfat

نظام ملفات ويندوز fat32 و لكن بأسماء ملفات طويلة 255 حرف، وأيضا بدون تغيير السماحيات والملكية.

ISO9660

نظام ملفات السواقة الليزرية وقد وضع هذا المقياس من قبل منظمة المقاييس العالمية لتوضيح كيفية تواجد الملفات ضمن القرص الليزري ويدعم أقراص CD-ROM و CD-RW .وقد طور هذا النظام إلى:

Joliet الجزء الموسع من ISO9660 والمطور من قبل مايكروسوفت لوضع ملفات بأسماء طويلة 64 محرف ضمن القرص الليزري واستخدام مجموعة محارف Unicode.

يستخدم مقياس Rock Ridge بعض الحقول الغير معرفة في ISO لدعم حالة الأحرف المختلطة والارتباطات المرنة والمجلدات المعشعشة.

(universal disk format)Udf

مخصص لأجهزة DVD-Rom.

5-1 مجلدات البنية الشجرية لنظام لينكس [5]

تصنف الملفات ضمن نظام التشغيل لينكس إلى أربع أنواع هي:

1-الملفات المشاركة shareable: التي يمكننا الدخول إليها من مخدمات بعيدة.

2-الملفات غير المشاركة unshareable:الملفات التي يتم التعامل معها ضمن المخدم المحلي.

3-الملفات الثابتة static: الملفات التي لا يمكن تعديلها إلا بتدخل من المشرف.

4- الملفات المتغيرة variable: الملفات التي تعدل تلقائياً بدون أي تتدخل.

	Sharable	Unsharable
static	/usr /opt	/etc /boot
variable	/var/mail /var/spool/news	/var/lock

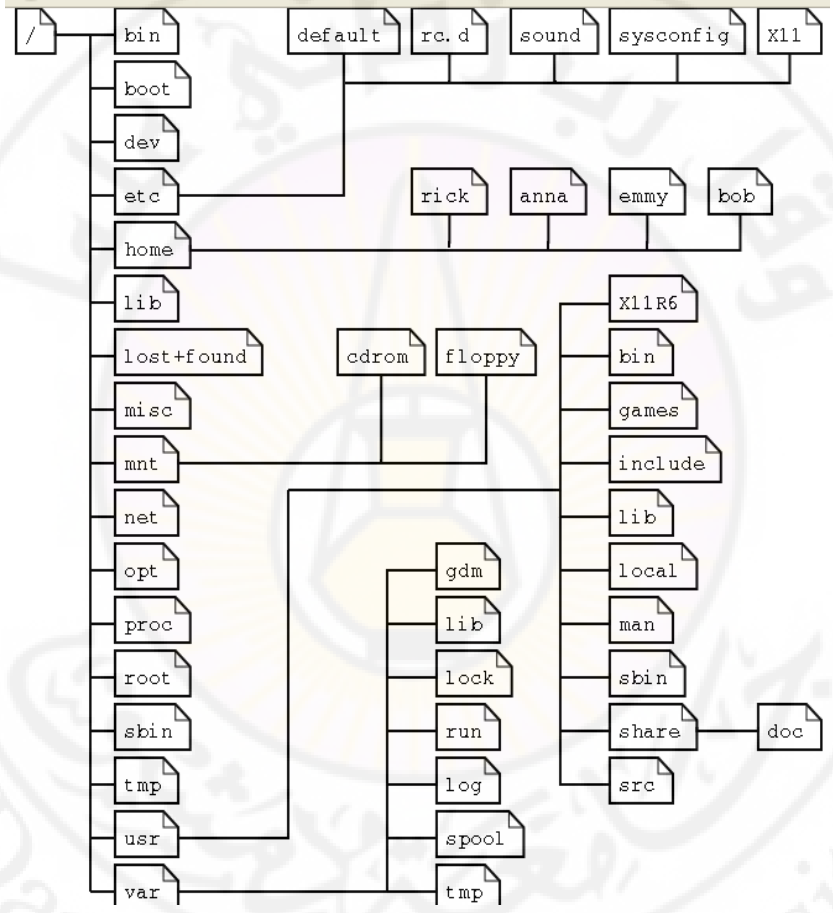
فمثلاً:

/boot: المجلد الذي يحتوي ملفات الإقلاع والنواة والقرص الابتدائي للذاكرة وبالتالي لا يمكن أن يكون إلا على الحاسب المحلي ولا تعدل ملفاته إلا بتدخل من المشرف.

5 https://access.redhat.com/documentation/en-us/ red_hat_enterprise_linux/5 /html/deployment_guide/s1-filesystem-fhs

/var/lock: لا يمكن مشاركتها مع أحد ولكنها متغيرة وتتعلق بإقفال بعض البرامج أثناء عملها.

البنية الشجرية لجذر شجرة الملفات ضمن لينكس:



الشكل 1-6 البنية الشجرية لنظام لينكس

/boot: يحتوي الملفات التي تعمل عند الإقلاع مثل النواة والقرص الذاكرة الابتدائي initrd (وكما ذكرنا سابقاً يمكن وجوده على نفس القرص الصلب الذي يحتوي جذر شجرة الملفات أو على قسم مستقل).

/etc: يحتوي كافة الملفات اللازمة لتعريف إعداد النظام والخدمات و الملفات والشبكة. تستخدم عند الإقلاع مثل: /etc/passwd, /etc/fstab,

/etc/inittab ويحتوي مجلدات فرعية مثل skel و rc.d ولا يحتوي ملفات ثنائية.

/sbin : يحتوي الملفات الثنائية system binaries أي الملفات التنفيذية المتعلقة بأوامر النظام الخاصة بالمشرف مثل /sbin/lilo.

/bin : يحتوي الملفات الثنائية أي ملفات الأوامر الخاصة بالمستخدم العادي، ls، cp، who .

/dev: يحتوي ملفات تعريف الأجهزة والمكونات المادية للحاسب. مثل /dev/cdrom ملف السواقة الليزرية، /dev/cua ملف المنفذ التسلسلي، /dev/sda ملف القرص الصلب.

/opt: يؤمن مساحة كبيرة من القرص الصلب لتخزين البرامج والألعاب ذات الحجوم الكبيرة ولتجنب وضعها ضمن نظام الملفات بحيث نجد لكل برنامج مجلد مستقل به وله بنية تنظيمية، ليعطي للمشرف إمكانية إدارة هذه البرامج.

بفرض لدينا برنامج يدعى sample فإن كافة الملفات التي تتبع هذا البرنامج ستكون ضمن مجلدات المجلد /opt/sample وسيقوم النظام تلقائيا بإنشاء مجلد لوضع الملفات التنفيذية لهذا البرنامج /opt/sample/bin ضمنه و مجلد فرعي لوضع ملفات المساعدة ضمنه /opt/sample/man وهكذا.

/lib: library يحتوي المكتبات اللازمة لتشغيل الملفات الثنائية الموجودة في /bin و /sbin. المكتبات نوعين:

- مكتبات ديناميكية dynamic object بلاحقة so (shared object) لأن كافة البرامج التي ترتبط بهذه المكتبة تستخدم نفس الملف وليس نسخة عنه.
- مكتبات ستاتيكية بلاحقة a (archive) لأنها ملفات أرشيفية للملفات الأصلية.
- ملفات نصية تستخدم من قبل الحزمة البرمجية libtools الخاصة بمنظمة GNU لشرح الملفات التي تبني المكتبات.

/Proc: virtual file system يضم عدد من الملفات الخاصة والتي تعطي معلومات آنية عن موارد الحاسب والنواة والإجرائيات العاملة، وباستعراض محتويات هذا المجلد سنجد أن حجوم هذه الملفات تساوي الصفر إذ أن أي ملف عند فتحه سيستدعي المعلومات من النظام.

cat /proc/mounts

```
[root@localhost ~]# cat /proc/mounts
rootfs / rootfs rw 0 0
/dev/root / ext3 rw,data=ordered 0 0
/dev /dev tmpfs rw 0 0
/proc /proc proc rw 0 0
/sys /sys sysfs rw 0 0
/proc/bus/usb /proc/bus/usb usbfs rw 0 0
devpts /dev/pts devpts rw 0 0
/dev/sda1 /boot ext3 rw,data=ordered 0 0
tmpfs /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
none /proc/fs/vmblock/mountPoint vmblock rw 0 0
sunrpc /var/lib/nfs/rpc_pipefs rpc_pipefs rw 0 0
/etc/auto.misc /misc autofs rw,fd=6,pgrp=2458,timeout=300,minproto=5,maxproto=5,indirect 0 0
-hosts /net autofs rw,fd=11,pgrp=2458,timeout=300,minproto=5,maxproto=5,indirect 0 0
```

الشكل 1-7 محتوى الملف mounts

يعرض أسماء أنظمة الملفات المحملة الآن.

ضمن ملف etc/fstab/ سنجد سطر لتحميله عند إقلاع النظام ولكنه غير مرتبط بجهاز مادي ما أو بقسم من القرص الصلب.

/usr: يحتوي البرامج التي يمكن مشاركتها ضمن الشبكة، ويمكن أن يكون له قسم من القرص الصلب مستقل ويجب تحميله للقراءة فقط. يضم العديد من المجلدات مثل usr/local/ الذي يحوي برمجيات محلية، /usr/include الملفات الرأسية الخاصة ببرامج لغة C.

كما يمكن أن يضم البرامج والبيانات التي نريد مشاركتها بين عدة مخدمات.

/home: يضم مجلدات المستخدمين ضمن النظام ويفضل وضع هذا المجلد على قسم مستقل من القرص الصلب لمنع تخزين المستخدمين لملفاتهم في قسم نظام الملفات.

/var: تحتوي كافة الملفات المتغيرة مثل مجلدات news, print, mail, log .

/mnt: يضم مجلدات أنظمة الملفات المؤقتة مثل /mnt/floppy و /mnt/cdrom.

6-1 إنشاء نظام ملفات [6]

تستخدم عدة أوامر ضمن النظام لإجراء عملية إنشاء لنظام الملفات أي **التهيئة**، مثل mkfs، mke2fs, mkdosfs mkfs. وهي من صلاحيات المشرف فقط .

شكل التعليمة:

/ sbin/mkfs options device-file

/sbin/mkfs -t type device-file

device: اسم الملف الذي يحدد نوع الجهاز الجديد.

الخيارات:

v-: إعطاء رسائل توضح ما يحدث أثناء تنفيذ الأمر.

l name-: وضع اسم لنظام الملفات.

t type-: تحديد نوع نظام الملفات الجديد (msdos، vfat، nfs، ntfs، proc، ufs ،..).

b size-: تحديد حجم البلوك عند إنشاء نظام الملفات.

لإنشاء نظام ملفات ext3 على قسم القرص الصلب من نوع سكازي أو ساتا sda1، نكتب:

/sbin/mkfs -t ext3 /dev/sda1

[6] Red_Hat_Enterprise_Linux-5-Deployment_Guide-en-US.pdf

7-1 تحميل نظام الملفات [7]

لا يكفي إنشاء نظام الملفات لنتمكن من التعامل معه وإنما يجب إجراء تحميل له أي ربطه بمجلد نستطيع من خلاله التعامل مع نظام الملفات الجديد.

نستعمل التعليمة mount لإجراء التحميل كما يلي:

/sbin/mount -t type options device dir

dir: مجلد التحميل الذي سيحمل ضمنه نظام الملفات.

device هو ملف الجهاز المعني (دوما موجودً في المجلد /dev).

الخيارات الممكنة هي:

-s تتجاهل الخيارات التي كتبتها اذا كانت تتعارض مع نوع نظام الملفات المراد تحميله.

-f إجبار على التحميل.

-r تحميله بصفة للقراءة فقط.

-w تحميله بصفة قراءة/كتابة.

-L لوضع اسم لنظام الملفات.

-t لتحديد نوع نظام الملفات (msdos أو vfat أو ext3).

-a تحميل كافة الأنظمة المعرفة في ملف fstab.

وكما ذكرنا سابقا فأنه لجعل المستخدم العادي قادراً على تحميل نظام ملفات ما؟ نضع الخيار user لهذا النظام ضمن ملف fstab ، وسيستطيع المستخدم من التحميل ولكن وفق الخيارات ومجلد التحميل المحدد فقط في ملف fstab ،وهي غالبا ما توضع في سطر أنظمة الملفات التي تعرف الأقراص المتحركة (المرنة والليزرية).

لتحميل القرص الليزري، نكتب:

mount /dev/cdrom

[7] Red_Hat_Enterprise_Linux-5-Deployment_Guide-en-US.pdf

أو

mount -t iso9660 /dev/cdrom /mnt/cdrom

1-8 إلغاء تحميل نظام الملفات

لإيقاف العمل بنظام ملفات ما (دون حذفه نهائياً)، نقوم بإلغاء تحميله، أي تفريغ المجلد المحمل به بدون حذف المجلد بحيث يظهر فارغ عند استعمال أمر ls.

لكن لا يمكننا إلغاء تحميل نظام ملفات مشغول ومستخدم، أي يجب عدم وجود أي ملف أو مجلد مفتوح، ولا نستطيع تشغيل برنامج موجود ضمن نظام الملفات المراد إلغاء تحميله.

نقوم بذلك باستعمال التعليمة umount كما يلي:

/sbin/umount dir

dir: هو اسم المجلد الذي نتعامل من خلاله مع نظام الملفات.

كما أن المستخدم الذي يحمل النظام هو الذي يلغي التحميل ؟؟؟ إلا إذا تم إضافة خيار users في ملف fstab لنظام الملفات، أو عند تنفيذ أمر mount.

1-8-1 الأمر *fuser* [8]

عند القيام بإلغاء تحميل نظام ملفات وكان مشغول سيتم إعطاء رسالة بذلك، لمعرفة السبب.

fuser -mv mount-point

mount-point مجلد التحميل.

-mv لإيجاد عمليات الدخول إلى نظام الملفات.

تشير رموز الخرج في العمود Access (الشكل 1-8) ما يفعله كل إجراء للتعامل مع طلب إلغاء التحميل.

- [8] دليل مدير النظام Linux – إصدار دار شعاع – د. خليل جورج عجمي

```
[root@server Thread]# mount -t ext3 /dev/grp1/project  /project/
[root@server Thread]# cd /project
[root@server project]# touch f1
[root@server project]# umount /project/
umount: /project: device is busy
umount: /project: device is busy
[root@server project]# fuser -mv /project

                     USER        PID ACCESS COMMAND
/project:            root      25089 ..c.. bash
```

الشكل 1-8 الأمر fuser

رموز التعامل لعمود Access:

c: يتوضع المجلد الحالي في نظام الملفات. (كما في الشكل 1-8).

f: ملف مفتوح من نظام الملفات.

e: توضع برنامج مفتوح في نظام الملفات.

r: توضع الدليل الجذر في نظام الملفات.

m: وجود ملف أو مكتبة برمجية مشتركة.

1-9 فحص نظام الملفات File System maintenance [9]

يقوم النص البرمجي rc.sysinit عند إقلاع الحاسب بتنفيذ أمر fsck لفحص أنظمة الملفات المحددة في ملف /etc/fstab ، فإذا وجد أحداها محدد ك dirty أو يحوي بيانات ضمن journal ، فسيتم إصلاحها من خلال fsck ، وإذا أصلح الخطأ سيتم تحميل نظام الملفات ويستمر الإقلاع، وإذا فشل سيقوم rc.sysinit بتشغيل sulogin لتشغيل fsck يدويا من قبل المشرف.

1-9-1 أوامر الفحص

e2fsck، fsck: تكشف وتصلح الأخطاء في بنية نظام الملفات بما فيها قطاعات البيانات الغير مرتبطة، وعند الإصلاح لا يدمرها وإنما يجعلها غير مرئية ضمن البنية الشجرية وستظهر في مجلد /lost+found.

يمكن تحديد نوع نظام الملفات عند الفحص والا سيعتبرها ext2.

[9] Red_Hat_Enterprise_Linux-5-Deployment_Guide-en-US.pdf

خيار **f–** للأمر يجبره على الفحص حتى وأن كان نظيفا. شكل الأمر:

fsck -t ext2 -f /
e2fsck -f /

tune2fs: تغير خصائص نظام ملفات، مثل تغيير النسبة المئوية المستخدمة من القطاعات، أو تغيير العدد الأعظمي قبل استخدام e2fsck، العدد الافتراضي هو 20 (وهو يتبع بنية نظام الملفات)

dumpe2fs: تطبع معلومات superblock ومجموعة البلوكات لنظام الملفات الموجودة على الجهاز المادي.

debugfs: أداة تفاعلية لفحص نظام الملفات ext2، و فحص سلامة العقد وتقوم باسترجاع البيانات.

resize2fs: يستخدم لتغيير حجم ext2, ext3، ولكن يجب استخدام الأمر fdisk أو أي أداة أخرى لتكبير الحجم أولا. أما لتصغير الحجم نستخدم الأمر أولا ثم الأمر fdisk أو غيره (هذه العملية حرجة ومدمرة للبيانات اذا لم تنفذ بالترتيب الوارد).

1-9-2 معلومات عن القرص الصلب

من الأمور المهمة للمشرف هي معرفة نسبة استخدام القرص والمساحات المستخدمة و المتوفرة، ويتم ذلك من خلال الأمرين:

Disk Free df

يعطي معلومات عن القرص تبعا لمعلومات أنظمة الملفات المسجلة في ملف /etc/mtab.

df –i mount point| directory

تعطي العقد i-node المستخدمة والمتوفرة.

df -h mount point| directory

تعطي الحجوم بالكيلوبايت أو الميغابايت.

Disk Usage du

إظهار معلومات عن حجوم المجلدات.

du -b bytes -B block-size -c -a directory

c- إعطاء قيم إجمالية للحجم لكل الملفات.

a- إظهار الحجوم لكافة الملفات والمجلدات.

10-1 تبادل الملفات بين نظامي ويندوز ولينكس

عند توفّر أكثر من نظام تشغيل ضمن قرص صلب واحد أو قرصين في حاسب واحد، فإننا سنحتاج حتماً إلى التنقل وتبادل الملفات فيما بينهما. يمكن الدخول إلى جزء القرص الصلب الذي يحوي نظام التشغيل ويندوز من لينكس بالشكل التالي:

بفرض أن ويندوز ضمن القرص صلب IDE ضمن القسم الخامس (أي /dev/hda5)، ندخل كمدير نظام root (أو ننفذ التعليمة su) وننفذ ما يلي:

1-ننشئ المجلد الذي سيتم تحميل نظام ملفات ضمنه:

mkdir /win

2-تحميل هذا النظام لنتمكن من الدخول إليه:

mount -t vfat /dev/hda5 /win

3-تعديل ملف /etc/fstab وإضافة السطر الذي يعرف نظام ملفات ويندوز. ليتم التعرف عليه تلقائيا عند الإقلاع، وبوضع الخيار auto ليتم تحميله تلقائيا عند الإقلاع وربطه بمجلد /win.

```
/dev/hda5          /win            vfat    auto
```

ثم نخزن الملف ونخرج منه. للتعامل مع النظام الجديد ومشاهدة الملفات والمجلدات يكفي الدخول إلى المجلد /win بعد إعادة الإقلاع.

ملاحظة: لا يجوز مطلقا إجراء تهيئة بواسطة mkfs أو أي أمر أخر، لأن النظام مهيئ ويحوي بيانات، وإلا أدى ذلك إلى ضياع البيانات.

11-1 إضافة قرص صلب جديد أو تعريف قسم جديد

عرض الأقراص أو الأقسام الموجودة ضمن الحاسب، نستخدم الأمر:

fdisk -l

عند الحاجة إلى تركيب قرص صلب جديد ؟ نتبع الخطوات التالية:

1. تعريف القرص ضمن نظام BIOS.
2. إجراء تقسيم للقرص باستخدام الأمر fdisk، مع تحديد اسم ملف القرص المراد تقسيمه:

fdisk /dev/sdb

11-1-1 مراحل عمل *fdisk*

```
Command (m for help): p
Disk /dev/had 64heads, 32Sector,1030 Cylinders
Units=Cylinder of 2048*512 byte
DeviceBoot Begin Start End Block Id system
/dev/sda1 1 1 100 102384 6 Dos-
(6bit)=32
```

(هذه الأرقام خاصة بحاسب ما وقد تشاهد أرقام مختلفة لديك تبعاً للقرص الصلب وحجم أقسامه).

أوامر fdisk:

يتم كتابة أوامر fdisk عند سطر المحث.

command(m for help):

p: عرض الأقراص والأقسام المتوفرة في القرص الصلب.

d : لحذف الأقسام الموجودة مسبقاً حتى نبدأ من قرص فارغ ونظيف.

n: إضافة قسم جديد ضمن القرص الصلب.

```
Command(m for help):n
Command action
E extended
P primary partition(1-4)
```

نكتب P لتحديد نوعه primary:

```
p
Partition number(1-4): 1
```

نحدد رقم القسم الجديد 1:

```
1
First Cylinder(1-100): 1
Last cylinder or +size or+sizeM or+sizeK(1-100): +50M
Command (m for help):P
Disk /dev/sdb:64heads,32sectors,100 Cylinders
Units=cylinders of 2048*512bytes
Device Boot    Begin   start    End    Block    ID    System
/dev/sdb1        1       1      51     52208    83    Liner
native
command(m for help) :n
command action
E  extended
P  Primary Partition(1-4)
P
Partition number(1-4):2
First Cylinder(1-100):52
Last cylinder or +Size or +SizeM or +SizeK([52]-100): 100
Command(m for help):
```

يمكن وضع الحجم بعد كلمة size+ كعدد أسطوانات cylinder أو حجوم مع الوحدة بالميغا أو الكيلو بايت،

النوع الافتراضي لكل قسم جديد هو Linux native، وهو نظام الملفات من نوع ext3. ولتغيير نوع نظام الملفات (لتحديد قسم swap مثلاً) نكتب:

```
Command(m for help): t
Partition number(1-4): 1
Hex Code (type L to list code): 82
Chang system type of partition 1 to 82 (Linux swap).
```

l: عرض أنواع وترميز أنظمة الملفات الممكن تعريفها.

t: تغيير نوع نظام الملفات.

w: حفظ التعديلات والخروج.

3. ننشئ نظام الملفات بتشغيل الأمر mke2fs أو mkfs:

```
mke2fs      /dev/sda1
```

4. تحميل نظام الملفات الجديد على القسم الجديد:

mount /dev/sda1 /tmp2

5. لتحميله آلياً عند الإقلاع، نعدل ملف /etc/fstab/ ونضيف له السطر التالي:

device mountpoint filesystemtype options dump fsckorder
/dev/sda2 /tmp2 ext2 default 1 2

Damascus University

إدارة الأقسام المنطقية

Logical Volume Administration

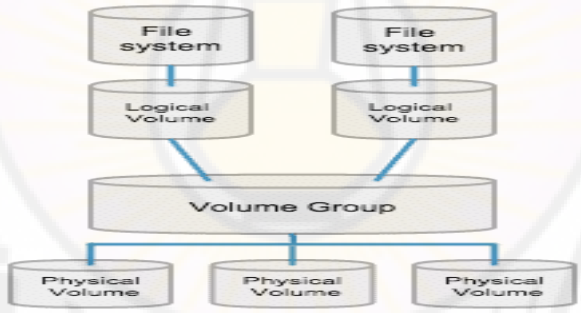
إدارة الأقسام (Logical Volume Management) LVM المنطقية

2-1 المقدمة

مفهوم الأقسام المنطقية [1]

بالنسبة لأنظمة Windows القسم المنطقي هو جزء موجود ضمن القسم الموسع (Extended) من القرص الصلب الواحد، و يمكن أن توجد عدة أقسام منطقية.

بالنسبة للأنظمة المفتوحة مثل لينكس ،القسم المنطقي هو قسم يمكن تشكيله من عدة أقسام من عدة أقراص صلبة، أي من أكثر من حيز فيزيائي.



الشكل 2-1 آلية عمل الأقسام المنطقية

يتلخص إنشاء الأقسام المنطقية بالخطوات التالية (كما في الشكل 2-1):

1. إنشاء حيز فيزيائي physical vloume واحد مؤلف من عدة أقسام من عدة أقراص.
2. إنشاء مجموعة حجوم volume group من الحيز الفيزيائي الجديد وبأسماء مختلفة.
3. إنشاء الحجوم المنطقية logical volume من مجموعات الحجوم التي أنشئت سابقا.

[1] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Cluster_Logical_Volume_Manager/LVM_CLI.html

4. تهيئة الأقسام الجديدة المنطقية mkfs وتنزيل أنظمة الملفات ضمنها.

5. تحميل الأنظمة الجديدة mount وربطها بمجلدات.

يمكن استعراض الحجوم الفيزيائية ومجموعات الحجوم والأقسام المنطقية المتوفرة ضمن النظام ، باستخدام الأوامر التالية:

pvs
vgs
lvs

```
root@localhost ~]# pvs
  PV         VG          Fmt  Attr PSize    PFree
  /dev/sda2  VolGroup00 lvm2 a-       9.88G    0
  /dev/sdb1  grp1       lvm2 a-    1016.00M    0
  /dev/sdc1  grp1       lvm2 a-    1016.00M 4.00M
root@localhost ~]# vgs
  VG          #PV #LV #SN Attr   VSize VFree
  VolGroup00    1   2   0 wz--n- 9.88G    0
  grp1          2   1   0 wz--n- 1.98G 4.00M
root@localhost ~]# lvs
  LV       VG          Attr   LSize Origin Snap%  Move Log Copy%
  LogVol00 VolGroup00 -wi-ao 8.88G
  LogVol01 VolGroup00 -wi-ao 1.00G
  project  grp1       -wi-ao 1.98G
```

الشكل 2-2 إظهار معلومات عن الأقسام المنطقية

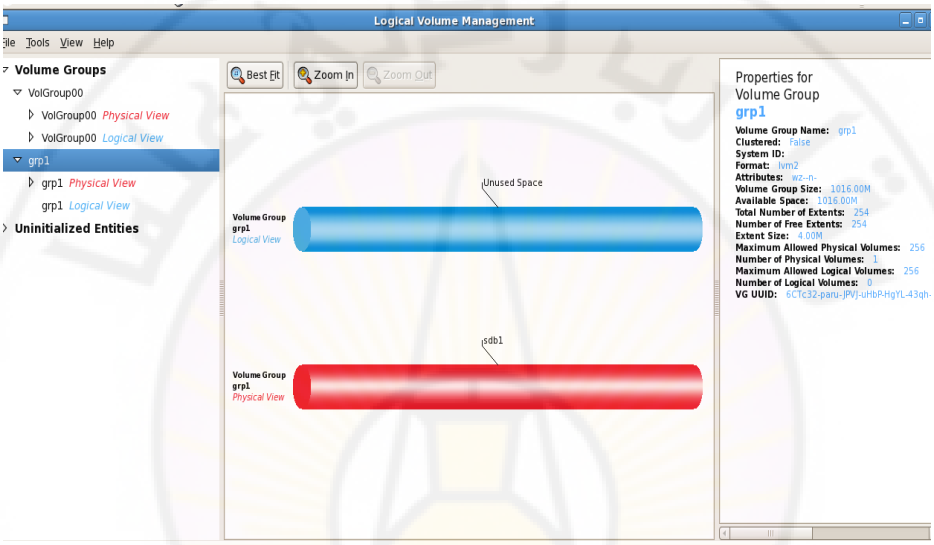
2-2 مزايا LVM [2]

1. إنشاء أقسام جديدة من أقراص أو أقسام موجودة وبالتالي تجميع المساحات الفارغة من عدة أقراص في قرص جديد.
2. تغليف القسم الفيزيائي مهما كان نوعه (IDE, SATA, SCSI, ...).
3. تؤمن عملية تخزين للبيانات باستخدام بنية شجرية هي الأقسام الفيزيائية ثم مجموعة الأقسام ثم مجموعة الأقسام المنطقية.
4. الأقسام الفيزيائية قد تكون بأي حجم.

[2] https://access.redhat.com/documentation/

3-2 إنشاء الأقسام المنطقية Logical Volume [3]

- أثناء تنصيب النظام
- باستخدام الأوامر
- باستخدام واجهة رسومية نصل إليها بالأمر system-config-lvm



الشكل 2-3 الواجهة الرسومية لإنشاء الأقسام المنطقية

2-3-1 مراحل إنشاء *Logical Volume* باستخدام الأوامر

لنفترض لدينا قرصيين صلبين sdb و sdc نريد تقسيم كل منهما إلى قسم وحيد ثم دمجهما معا لنشكل حجم منطقي جديد واحد.

1. إنشاء Partion بواسطة الأمر fdisk وتغيير نظام الملفات إلى LVM باستخدام الخيار t. وذلك لكل قرص صلب نريد إنشاء أقسام منطقية منه.

بالأمر:

```
fdisk   /dev/sdb
fdisk   /dev/sdc
```

[3] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Cluster_Logical_Volume_Manager/LVM_CLI.html

ملاحظة:

لا يمكن تغيير نظام الملفات إلى LVM إذا كان القسم Partion من النوعExtended ، يمكن تحويل أي Primary Partion وليس بالضرورة أن يتم إنشاء Partion جديد.

```
[root@localhost ~]# fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI
 or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previo
us
content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be correct
ed by w(rite)

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-130, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-130, default 130):
Using default value 130

Command (m for help): t
Selected partition 1
Hex code (type L to list codes): 8e
Changed system type of partition 1 to 8e (Linux LVM)
```

الشكل 2-4 تعديل نوع نظام الملفات إلى lvm ضمن امر fdisk

نستخدم الأمر fdisk -l بعد الانتهاء للتأكد من صحة الإنشاء وتحديد نوع نظام الملفات.

```
[root@localhost ~]# fdisk  -l

Disk /dev/sda: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          13      104391   83  Linux
/dev/sda2              14        1305    10377990   8e  Linux LVM

Disk /dev/sdb: 1073 MB, 1073741824 bytes
255 heads, 63 sectors/track, 130 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         130     1044193+  8e  Linux LVM

Disk /dev/sdc: 1073 MB, 1073741824 bytes
255 heads, 63 sectors/track, 130 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1         130     1044193+  8e  Linux LVM
[root@localhost ~]#
```

الشكل 2-5 خرج الأمر fdisk -l

2. إنشاء حجوم فيزيائية بواسطة الأمر:

pvcreate partations-device-files
pvcreate /dev/sdb1 /dev/sdc1

ويمكن مشاهدة الحجوم الفيزيائية بعد الإنشاء للتأكد باستخدام الأمر pvdisplay أو pvs.

```
[root@localhost ~]# pvcreate /dev/sdb1  /dev/sdc1
  Physical volume "/dev/sdb1" successfully created
  Physical volume "/dev/sdc1" successfully created
[root@localhost ~]# pvdisplay
  --- Physical volume ---
  PV Name               /dev/sda2
  VG Name               VolGroup00
  PV Size               9.90 GB / not usable 22.76 MB
  Allocatable           yes (but full)
  PE Size (KByte)       32768
  Total PE              316
  Free PE               0
  Allocated PE          316
  PV UUID               NI0dTW-RCzd-JSwS-Qivn-paD5-PwXD-vANH6c

  --- NEW Physical volume ---
  PV Name               /dev/sdb1
  VG Name
  PV Size               1019.72 MB
  Allocatable           NO
  PE Size (KByte)       0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               BxTiSW-yW94-uTxl-lF0J-V1KH-kI1d-8BVutn

  --- NEW Physical volume ---
  PV Name               /dev/sdc1
  VG Name
```

الشكل 2-6 الأمر pvcreate و pvdisplay

3. إنشاء مجموعة حجوم فيزيائية بواسطة الأمر:

vgcreate group-name device-files-names

يمكن أن ننشئ مجموعة واحدة ضمن الحيز الفيزيائي من كافة الأقسام، أو ننشئ عدة مجموعات مع تحديد الأقسام الفيزيائية المشكلة للمجموعة من مجموعة الأقسام الفيزيائية المشكلة للحجم الفيزيائي.

سنفترض في مثالنا اننا أنشئنا مجموعة واحدة من كافة الأقسام.

vgcreate grp1 /dev/sdb1 /dev/sdc1
vgdisplay

نفترض اسم المجموعة grp1.

للتأكد vgs أو vgdisple.

```
root@localhost ~]# vgcreate  grp1  /dev/sdb1  /dev/sdc1
 Volume group "grp1" successfully created
root@localhost ~]# vgdisplay
 --- Volume group ---
 VG Name               grp1
 System ID
 Format                lvm2
 Metadata Areas        2
 Metadata Sequence No  1
 VG Access             read/write
 VG Status             resizable
 MAX LV                0
 Cur LV                0
 Open LV               0
 Max PV                0
 Cur PV                2
 Act PV                2
 VG Size               1.98 GB
 PE Size               4.00 MB
 Total PE              508
 Alloc PE / Size       0 / 0
 Free  PE / Size       508 / 1.98 GB
 VG UUID               qnGTsh-mt0L-uYLB-U7e8-eNrS-k5qM-2XBk0p

 --- Volume group ---
```

الشكل 2-7 إنشاء مجموعة حجوم

4. إنشاء حجوم منطقية بواسطة الأمر:

Lvcreate -L size -n logic-name group-name

نحدد الحجم من خرج vgdisplay الذي يظهر حجم المجموعة الكلي VG Size، ونقرر إذا أردنا أن ننشئ قسم وحيد بكامل المساحة أو نجزئ المجموعة إلى أقسام بحجوم أخرى.

lvcreate -L 1.98G -n lv1 grp1

```
root@localhost ~]# lvcreate  -L 1.986  -n lv1  grp1
 Rounding up size to full physical extent 1.98 GB
 Logical volume "lv1" created
root@localhost ~]# lvdisplay
 --- Logical volume ---
 LV Name                /dev/grp1/lv1
 VG Name                grp1
 LV UUID                wspg3Q-B2qc-z0Tr-6DId-5awM-EoTa-SQK1IF
 LV Write Access        read/write
 LV Status              available
 # open                 0
 LV Size                1.98 GB
 Current LE             507
 Segments               2
 Allocation             inherit
 Read ahead sectors     0
 Block device           253:2
```

الشكل 2-8 إنشاء الحجم المنطقي

وللتأكد lvdisplay أو lvs.

نلاحظ من الشكل أن ملف الحجم المنطقي الجديد الذي تشكل هو **/dev/grp1/lv1** وضمن مجلد dev .

5. إنشاء نظام ملفات في الحجوم المنطقية بواسطة الأمر mkfs

نحتاج بعد إنشاء القسم المنطقي الجديد إلى عملية تنزيل نظام الملفات أي التهيئة بواسطة الأمر mkfs.

mkfs -t fs-type device-file-name
mkfs -t ext3 /dev/grp1/lv1

```
root@localhost ~]# mkfs  -t ext3  /dev/grp1/lv1
ke2fs 1.39 (29-May-2006)
ilesystem label=
S type: Linux
lock size=4096 (log=2)
ragment size=4096 (log=2)
59584 inodes, 519168 blocks
5958 blocks (5.00%) reserved for the super user
irst data block=0
laximum filesystem blocks=532676608
6 block groups
2768 blocks per group, 32768 fragments per group
6224 inodes per group
uperblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

riting inode tables: done
reating journal (8192 blocks): done
riting superblocks and filesystem accounting information: done

his filesystem will be automatically checked every 23 mounts or
80 days, whichever comes first.  Use tune2fs -c or -i to override.
```

الشكل 2-9 تهيئة قسم منطقي

6. تحميل نظام ملفات الحجوم المنطقية الجديدة بواسطة الأمر mount

نقوم بربط ملف القسم المنطقي الجديد بمجلد ضمن البنية الشجرية كي نستطيع التعامل معه.

mount -t fs-type device-file mount point
mkdir /hard2
mount –t ext3 /dev/grp1/lv1 /hard2

```
[root@localhost ~]# mkdir  /hard2
[root@localhost ~]# mount   -t   ext3  /dev/grp1/lv1   /hard2
[root@localhost ~]# ls -l  /hard2
total 16
drwx------ 2 root root 16384 Dec 14 21:59 lost+found
[root@localhost ~]# ls -ld  /hard2
drwxr-xr-x 3 root root 4096 Dec 14 21:59 /hard2
[root@localhost ~]#
```

الشكل 2-10 تحميل القسم المنطقي الجديد

2-3-2 تغير اسم القسم المنطقي

يمكن تغير اسم القسم المنطقي بواسطة الأمر lvrename

lvrename old-name new-name

لو أردنا تغيير الاسم من lv1 إلى project.

lvrename /dev/grp1/lv1 /dev/grp1/project

```
root@localhost ~]# lvrename  /dev/grp1/lv1 /dev/grp1/project
 Renamed "lv1" to "project" in volume group "grp1"
root@localhost ~]# lvdisplay
 --- Logical volume ---
 LV Name                /dev/grp1/project
 VG Name                grp1
 LV UUID                wspg3Q-B2qc-z0Tr-6DId-5awM-EoTa-SQK1IF
 LV Write Access        read/write
 LV Status              available
 # open                 1
 LV Size                1.98 GB
```

الشكل 2-11 إعادة تسمية قسم منطقي

2-3-3 تغيير حجم قسم منطقي

نستطيع بعد إنشاء مجموعة الحجوم أن نغير حجمها زيادة أو انقاص بشرط وجود مساحة فارغة عند التكبير الحجم ضمن مجموعة الحجوم المنطقية التي أنشئ منها القسم المنطقي.

vgextend volumegroup-name device-file

ولمعرفة الأقسام الفيزيائية المشكلة لمجموعة حجوم ، بالأمر :

pvscan

```
root@localhost ~]# pvscan
 PV /dev/sdb1   VG grp1         lvm2 [1016.00 MB / 0    free]
 PV /dev/sdc1   VG grp1         lvm2 [1016.00 MB / 4.00 MB free]
 PV /dev/sda2   VG VolGroup00   lvm2 [9.88 GB / 0    free]
 Total: 3 [11.86 GB] / in use: 3 [11.86 GB] / in no VG: 0 [0   ]
```

الشكل 2-12 عرض الأقسام الفيزيائية

تكبير الحجم: يشترط وجود مساحة فارغة ضمن مجموعة الحجوم volume group حرة وذلك بواسطة الأمر vgdisplay (الشكل 2-7 إنشاء مجموعة حجوم).

وفق الخطوات التالية:

1. تكبير الحجم المنطقي.

lvresize -l -+size logic-volume-name
lvresize -l +2G /dev/grp1/project

2. تكبير نظام الملفات ولا داعي لإجراء إعادة تحميل لنظام الملفات

resize2fs logic-volume-name
resize2fs /dev/grp1/lv1

تصغير الحجم: نقوم بالخطوات التالية:

1. إلغاء تحميل نظام الملفات.

umount mount-point
umount /hard2

2. تصغير حجم نظام الملفات، ولنفترض 300 ميغابايت ليصبح 1500 ميغابايت.

resize2fs device-file size[M|G]
resize2fs /dev/grp1/project 1500M

3. إجراء فحص له.

e2fsck device-file
e2fsck /dev/grp1/project

4. تصغير حجم القسم المنطقي.

lvreduce -L -size[M|G] device-file
lvreduce -L -300M /dev/grp1/project

5. فحص نظام الملفات بعد تصغير الحجم.

e2fsck device-file
e2fsck /dev/grp1/project

6. إعادة تحميل نظام الملفات من جديد.

mount mount-point
mount /hard2

يوضح الشكل التالي الأوامر السابقة و تنفيذها.

```
[root@localhost ~]# lvs
  LV       VG         Attr   LSize Origin Snap%  Move Log Copy%
  LogVol00 VolGroup00 -wi-ao 8.88G
  LogVol01 VolGroup00 -wi-ao 1.00G
  project  grp1       -wi-ao 1.90G
[root@localhost ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      8.6G  5.2G  3.0G  64% /
/dev/sda1              99M   14M   81M  15% /boot
tmpfs                 125M     0  125M   0% /dev/shm
/dev/mapper/grp1-project
                      1.9G  2.9M  1.8G   1% /hard2
[root@localhost ~]# umount /hard2/
[root@localhost ~]# e2fsck -f /dev/grp1/project
e2fsck 1.39 (29-May-2006)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/grp1/project: 11/249344 files (9.1% non-contiguous), 8568/498688 blocks
[root@localhost ~]# resize2fs /dev/grp1/project  1500M
resize2fs 1.39 (29-May-2006)
Resizing the filesystem on /dev/grp1/project to 384000 (4k) blocks.
The filesystem on /dev/grp1/project is now 384000 blocks long.

[root@localhost ~]# lvreduce  -L -300M /dev/grp1/project
  WARNING: Reducing active logical volume to 1.61 GB
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce project? [y/n]: y
  Reducing logical volume project to 1.61 GB
  Logical volume project successfully resized
[root@localhost ~]#
```

الشكل 2-13 تصغير حجم قسم منطقي

نستخدم الأمر lvdisplay أو lvs لمشاهدة الحجم بعد التصغير.

```
[root@localhost ~]# resize2fs /dev/grp1/project  1500M
resize2fs 1.39 (29-May-2006)
Resizing the filesystem on /dev/grp1/project to 384000 (4k) blocks.
The filesystem on /dev/grp1/project is now 384000 blocks long.

[root@localhost ~]# lvreduce  -L -300M /dev/grp1/project
  WARNING: Reducing active logical volume to 1.61 GB
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce project? [y/n]: y
  Reducing logical volume project to 1.61 GB
  Logical volume project successfully resized
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Name                /dev/grp1/project
  VG Name                grp1
  LV UUID                CLlVUo-dvTs-C2q0-IzxF-btEG-nh8F-Ha0xEs
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                1.61 GB
  Current LE             412
  Segments               2
  Allocation             inherit
  Read ahead sectors     0
  Block device           253:2
```

الشكل 2-14 إظهار حجم القسم المنطقي بعد التصغير

بروتوكولات الاتصال عن بعد

Remote Access

م. ماجدة محمد أسعد

بروتوكولات الاتصال عن بعد

Remote Access

6-1 المقدمة

يسمح نموذج مخدّم/زبون بالسماح للمستخدم بإنشاء جلسة عمل على الجهاز البعيد وتشغيل تطبيقاته. تعرف هذه الآلية باسم الدخول عن بعد، ويمكن القيام بذلك عن طريق تنفيذ تطبيق (بروتوكول) على المخدّم والزبون معاً.

من أنواع البروتوكولات التي تستخدم للدخول عن بعد:
TELNET- RSH-RLOGIN-FTP-SSH

6-2 البروتوكول telnet

يُعدُّ telnet (terminal network) من أوامر الشبكة وبروتوكولات الدخول عن بعد (Remote Access)، ومن معيار TCP/IP لإنشاء اتصال عن بعد. يسمح بإنشاء اتصال والدخول إلى جهاز بعيد عبر شبكة الإنترنت أو ضمن شبكة محلية من خلال اسم حساب وكلمة سر، أي بدء جلسة Shell عن بعد. تصبح شاشة المستخدم ولوحة مفاتيحه بعد إجراء الاتصال متصلة مباشرة بالمخدّم البعيد.

6-2-1 خصائص *Telnet*

- يتم بناء برنامج الزبون لاستخدام واجهات المخدّم / الزبون القياسية من دون معرفة تفاصيل برامج المخدّم.
- يتم التفاوض بين المخدّم والزبون على خيارات تنسيق البيانات.
- يتم التعامل بشكل متناظر بين طرفي الاتصال بمجرد إنشاء الاتصال من خلال telnet.
- يعمل على البوابة (Port) 23.

6-2-2 آلية العمل

يقوم برنامج تشغيل المحطة الطرفية للزبون باستقبال ضربات المفاتيح، وتفسر له كأحرف من خلال نظام التشغيل عندما يقوم المستخدم بتسجيل الدخول إلى المخدّم البعيد.

تتحول الأحرف عادة إلى مجموعة أحرف عالمية تسمى الشبكة الظاهرية الطرفية (Network Virtual Terminal-NVT) والذي يستخدم التمثيل 7-بت USASCII للبيانات. ثم ينشئ الزبون اتصال TCP بالمخدّم ليتم إرسال النصوص في نسق NVT باستخدام TCP ويتم تسليمها إلى نظام تشغيل المخدّم البعيد. يقوم المخدّم بتحويل الأحرف مرة أخرى من NVT إلى تنسيق الجهاز الزبون المحلي.

يُعدُّ Telnet إحدى خدمات xinetd (الخدمة المسؤولة عن إدارة عمليات الشبكة كافة)، فهي مدمجة ضمنها، وليست خدمة مستقلة بحد ذاتها؛ لذلك لا يمكن تعديل حالتها باستخدام الأمر service.

لـ Telnet ملف إدارة خاص بها /etc/xinetd.d/telnet، من أجل تفعيل خدمة Telnet:

1. نعدل الخيار disable الموجود في الملف إلى disable = no

```
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
```

الشكل 6-1 ملف telnet

2. نقوم بإيقاف جدار الحماية:

service iptables stop

3. نقوم بإنشاء مستخدم جديد له كلمة سر:

useradd tcc -p 12345

4. نعيد تشغيل خدمة xinetd:

service xinetd restart

5. نفعِّل الخدمة بواسطة الأمر chkconfig:

Chkconfig telnet on

6. نفعِّل خدمة بروتوكول krb5 الذي يقوم بتوثيق زبائن Telnet:

chkconfig krb5-telnet on

```
[root@server ~]# service iptables stop
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
[root@server ~]# service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
[root@server ~]# chkconfig telnet on
[root@server ~]# chkconfig krb5-telnet on
[root@server ~]# chkconfig --list|grep telnet
        ekrb5-telnet:   off
        krb5-telnet:    on
        telnet:         on
[root@server ~]#
```

الشكل 6-2 تشغيل خدمة Xinetd وتفعيل telnet.

استخدام Telnet

شكل الأمر:

telnet [host name/ip] [port #]

لو أردنا الدخول من جهاز ويندوز إلى مخدّم لينكس لخدمة telnet.



الشكل 6-2 دخول مستخدم ويندوز لخدمة telnet.

مثال:

telnet 192.168.1.10 80 80

Login: TCC

Paswword: *****
[TCC@localhost ~]$

ملاحظة: رقم البوابة افتراضياً هو 23، ولكن يمكن استعمال رقم بوابة آخر.

يمكن بتنفيذ الأمر **w** معرفة المستخدمين العاملين الآن على النظام ومن أي طرفية.

3-6 SSH Secure Shell

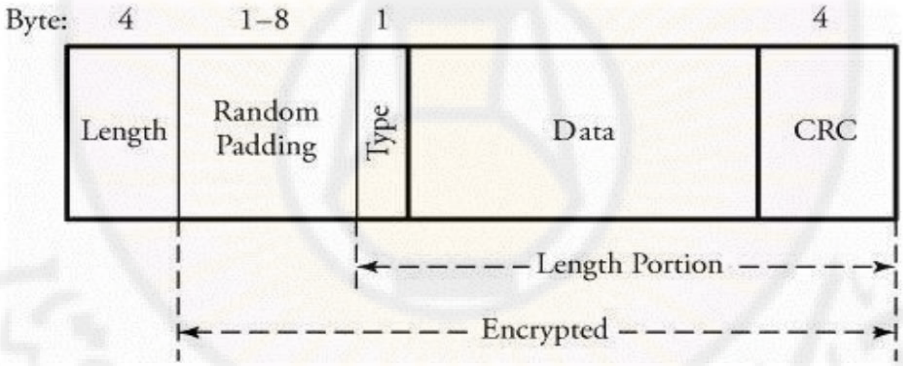
بروتوكول دخول عن بعد آخر، يستخدم بروتوكول TCP للاتصال، ولكن بشكل أكثر فاعلية ومرونة من telnet بحيث تمكن المستخدم من تنفيذ أوامر النظام على طرفية بعيدة.

6-3-1 مزايا *SSH*

1. تؤمن اتصالاً آمناً من خلال تشفير الرسائل والتوثيق.
2. تؤمن إرسال بيانات متعددة بالاتصال نفسه من خلال استخدام عدة أقنية للدخول عن بعد.
3. SSH2 هي نسخة مطورة عنSSH1 تدعم طرق تبادل مفاتيح KEYS وطرق تشفير أقوى أكثر، لجعل النظام يعمل على النسخة الثانية ندخل لملف الإعداد الخاص بالخدمة /etc/ssh/sshd_config ، ونكتب :

 # protocol 2

4. تنسيق طرد خدمة :SSH



الشكل 6-3 تنسيق حزمة ssh.

Length: حجم رزمة البيانات.

Random Padding: تجعل التسلل أكثر صعوبة.

Type: نوع الرسالة.

Data: البيانات المرسلة.

CRC: cyclic redundancy checks حقل كشف الخطأ.

5. يعمل على المنفذ port رقم 22، نستطيع تغيير رقم المنفذ port من ملف الإعداد الخاص بالخدمة.

6-3-2 آلية العمل

1. تحقق ssh الأمن من خلال استخدام تشفير المفتاح العام والخاص بين المستخدم والمخدّم البعيد.
2. عند إقامة الاتصال مع المخدّم، فإن البيانات المرسلة تبقى مشفرة (حتى لو قام متسلل ما بالحصول عبر الشبكة على نسخة منها)، يقوم المخدّم عند وصولها بعملية المصادقة على الرسائل للتعرف إلى المرسل.
3. عادة يحتاج المستخدم إلى كلمة سر خاصة للدخول واستخدام هذه الخدمة.

6-3-3 إعداد المخدّم/ الزبون

المخدّم:

ملف الخدمة هو /etc/ssh/sshd_config

خدمة SSH تدعم طريقتي توثيق Authenticationهي:

1. اسم المستخدم وكلمة السر. ويتم تفعيلها ضمن المخدّم من خلال ملف إعداد الخدمة sshd_config وإسناد قيمة للمتحول الخاص بالشكل:

PasswordAuthentication yes

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
GSSAPICleanupCredentials yes
```

الشكل 6-4 ملف sshd_config.

2. استخدام زوج مفاتيح Public-key Authentication عام وخاص public وprivate. يتم وضع المفتاح العام على مخدّم ssh ويحتفظ المستخدم بالمفتاح الخاص لديه. عندما يريد المستخدم الدخول للمخدّم واستخدام خدمة ssh سيقوم المخدّم بتشفير رقم عشوائي بوساطة المفتاح العام للمستخدم

وسيطلب منه أن يفك تشفيره بوساطة مفتاحه الخاص وبهذا سيتم التأكد من أن المستخدم موثوق وهو صاحب المفتاح العام ومن يقوم بإرسال البيانات.

vi /etc/ssh/sshd_config
PasswordAuthentication no

نعمل إعادة تشغيل للخدمة

[root@localhost ~]# /etc/init.d/sshd restart

```
[root@server ~]# service sshd start
Starting sshd:                                [  OK  ]
```

الزبون

1- في حال تم اختيار طريقة التوثيق بكلمة سر، فلا نحتاج لإجراء أي إعداد عند الزبون.

الدخول:

ssh [ip-server-ssh]

2- طريقة استخدام المفاتيح:

a. توليد المفاتيح:

[tcc@localhost ~]$ ssh-keygen –t rsa

RSA: هي خوارزمية تشفير وإنشاء مفاتيح بطول 2048 bit.

سيقوم بطلب قيمة عشوائية لإنشاء المفاتيح. سيتم تخزين المفتاحين الخاص والعام في مجلد المستخدم tcc، بالأسماء:

/home/tcc/.ssh/id_rsa
/home/tcc/.ssh/id_rsa.pub

```
[majeda@server ~]$ ssh-keygen  -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/majeda/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/majeda/.ssh/id_rsa.
Your public key has been saved in /home/majeda/.ssh/id_rsa.pub.
The key fingerprint is:
17:bd:f6:64:e9:cc:2b:67:dc:82:07:5b:11:3e:10:39 majeda@server
[majeda@server ~]$ ls -a
.   .bash_history  .bash_profile  .emacs  f4    .ssh  test1.doc
..  .bash_logout   .bashrc        f1     .kde  test  .zshrc
[majeda@server ~]$ ls -a ./.ssh/
.  ..  id_rsa  id_rsa.pub
```

الشكل 6-6 إنشاء زوج مفاتيح لمستخدم ssh.

b. نسخ المفتاح العام الخاص بالمستخدم إلى السيرفر نكتب:

scp ~/.ssh/id_rsa.pub tcc@ IP server:.ssh/authorized_keys

ينسخ إلى ملف authorized_keys الموجود في المجلد المخفي ssh.

```
[majeda@server ~]$ scp ./.ssh/id_rsa.pub majeda@192.168.0.2:.ssh/authorized_keys
The authenticity of host '192.168.0.2 (192.168.0.2)' can't be established.
RSA key fingerprint is 5f:8d:c0:10:39:20:28:37:ff:2e:2c:a4:11:8b:a9:d5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.2' (RSA) to the list of known hosts.
majeda@192.168.0.2's password:
id_rsa.pub                                    100%  395     0.4KB/s   00:00
[majeda@server ~]$ ls .ssh/
authorized_keys  id_rsa  id_rsa.pub  known_hosts
```

الشكل 6-7 نسخ المفتاح العام لزبون ssh.

c. ثم نغير سماحية ملف المفتاح الخاص وملف المفتاح العام، لمنع أي شخص غير المستخدم المحدد من قراءة الملفين:

chmod 600 /home/tcc/.ssh/id_rsa.pub
chmod 400 /home/tcc/.ssh/id_rsa

d. يقوم المستخدم بالدخول إلى مخدّم ssh، بالأمر الآتي:

ssh ssh-server-ip

يتم طلب passphrase للتأكد من أن المستخدم هو من قام بتوليد المفاتيح وهو مالك الحساب.

```
[majeda@server .ssh]$ chmod 600 id_rsa.pub
[majeda@server .ssh]$ chmod 400 id_rsa
[majeda@server .ssh]$ ssh 192.168.0.2
Enter passphrase for key '/home/majeda/.ssh/id_rsa':
Last login: Fri Feb 23 00:55:57 2018
[majeda@server ~]$ w
 23:18:11 up 1 day,  4:34,  5 users,  load average: 0.13, 0.16, 0.10
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
majeda   tty4     -                 Fri00    4days  0.05s  0.05s -bash
tcc      tty5     -                 Fri00    4days  0.03s  0.03s -bash
root     pts/1    :0.0              19Feb18  0.00s  2.81s  0.06s ssh 192.168.0.2
root     pts/2    :0.0              23:14    4:01   0.05s  0.05s bash
majeda   pts/3    server.tcc.com    23:18    0.00s  0.07s  0.02s w
[majeda@server ~]$
```

الشكل 6- 5 دخول مستخدم ssh.

وبعد الدخول لمخدّم ssh وفتح جلسة عن بعد يمكن التأكد من ذلك بتنفيذ الأمر w الذي يظهر عنوان IP المخدّم الذي قمت بالدخول منه (كما في الشكل السابق).

التأكد من عدم وجود مشاكل في ملف الإعدادات

نقوم بتنفيذ الآتي:

`which sshd` -t

سيقوم بفحص الإعدادات عند وجود مشاكل في ملف الإعداد؛ وإن لم يكن هناك أي أخطاء لن يظهر شيء.

4-6 البروتوكول FTP

من بروتوكولات الاتصال عن بعد لنقل الملفات، ومن أكثر البروتوكولات استخداماً في الإنترنت الآن، وذلك للنقل الآمن للملفات بين المخدّمات والزبائن دون الحاجة لدخولها مباشرة لهذه المخدّمات. والسماح المباشر لها بالولوج للملفات من خلال أوامر بسيطة.

لا يشبه FTP باقي البروتوكولات؛ لأنه يستخدم عدة منافذ port من الشبكة ليعمل بشكل صحيح، يستخدم المنفذ Port 21 (يدعى منفذ الأوامر command port) ليقومَ الزبون الاتصال مع المخدّم.

ويستخدم المنفذ Port 20 (منفذ الاتصال data port) لنقل البيانات من المخدّم.

يختلف رقم المنفذ الخاص بنقل البيانات والطريقة التي تتم بها تهيئة نقل البيانات، وفقًا للزبون في طلب البيانات في الوضع النشط active أو الكامن passive.

الوضع النشط active mode

الطريقة الأساسية المستخدمة من قبل بروتوكول FTP لنقل البيانات إلى تطبيق الزبون. يفتح المخدّم اتصالاً من المنفذ 20 على المخدّم عند بدء نقل البيانات إلى عنوان IP ومنفذ عشوائي غير مميز (أكبر من 1024) يحدده الزبون.

أي يجب السماح لجهاز الزبون بقبول الاتصالات عبر أي منفذ رقمه فوق 1024.

ولكن مع استخدام جدران النار لحماية أجهزة الزبائن سيتم رفض الاتصالات الواردة من مخدّمات FTP ذات الوضع النشط، لذلك ينصح بالوضع الكامن.

الوضع الكامن passive mode

يتم بدء الوضع الكامن، مثل الوضع النشط، من خلال تطبيق زبون FTPعند طلب بيانات من المخدّم؛ مشيراً إلى أنه يريد الوصول إلى البيانات في الوضع الكامن؛ ويوفر المخدّم عنوان IP ومنفذاً عشوائياً غير مميز (أكبر من 1024) على المخدّم. ليتصل الزبون بهذا المنفذ ويبدأ تنزيل الملفات المطلوبة.

يحل هذا الوضع مشكلات تداخل منافذ جدار النار عند الزبون مع اتصالات البيانات، مما يعقد إدارة جدار النار عند المخدّم.

ويمكن حل المشكلة بتقليل عدد المنافذ المفتوحة على المخدّم بتحديد مجال من أرقام المنافذ غير الموثوقة على مخدّم .FTP.

6-4-1 مخدّم *VSFTPD*

يتوفر أنواع عدة من بروتوكول FTP مثل GFTP، TFTP، FTPS، ولكن أكثرها أمناً هو VSFTP (Very Secure File Transfer Protocol) يتم تنصيبه تلقائياً مع توزيعة ريدهات.

خصائص *VSFTPD*

- FTP لا نحتاج إلى دخول مباشر للمخدّم؛ أي فتح جلسة shell.
- FTP تنقل البيانات إلى المخدّم من دون تشفير.
- يمكن منع الانتقال إلى حسابات المستخدمين المحليين.
- vsftpd سريع وآمن وثابت.
- vsftpd يستخدم بروتوكول tcp في طبقة النقل.
- Vsftpd يسمح بعدد كبير من الاتصالات الآمنة.
- يستخدم من قبل المستخدم المجهول (Anonymous) أو المحلي local user.
- يجب استخدام SFTP عوضا عن FTP عند نقل البيانات من خلال شبكة عامة كالإنترنت.
- ملف الإعداد الخاص به /etc/vsftpd/vsftpd.conf.

6-4-2 إعداد بروتوكول *VSFTPD*

تعتمد آلية عمل هذا البروتوكول على وجود مخدّم وزبون.

المخدّم

1. نتأكد من وجود الحزمة الخاصة بـ FTP

rpm -qa | grep vsftp

```
[root@localhost ~]# rpm -qa vsftpd
vsftpd-2.0.5-10.el5
[root@localhost ~]# rpm -qa ftp
ftp-0.17-33.fc6
```

الشكل 6-9 استعلام وجود خدمة ftp.

2. يستخدم مخدّم ftp البوابة 21، لذلك يجب التأكد من فتحها وخاصة في حال وجود جدار النار، لذلك نضيف القاعدة الآتية لفتح البوابة:

iptables -A INPUT -m state --state NEW -m tcp –p tcp --dport 21 -j ACCEPT

3. في حال عمل خدمة SELinux، يجب السماح للمستخدم المحلي بإجراء رفع وتنزيل إلى مجلده الخاص، نكتب القاعدة الآتية:

setsebool ftp_home_dir 1

4. نعيد تشغيل خدمة vsftpd.

Service vsftpd restart

5. نعدل ملف إعداد الخدمة /etc/vsftpd/vsftpd.conf

من الخيارات التي يمكن تعديلها في الملف:

- السماح للمستخدم المجهول بالدخول إلى مخدّم ftp

anonymous_enable = YES

- السماح للمستخدمين المحليين بالدخول إلى مخدّم ftp

local_enable = YES

- عدم السماح للمستخدم المحلي بالانتقال خارج مجلده الخاص

chroot_local_user = YES

- السماح بعملية الكتابة على مخدّم ftp

Write_enable=YES

- السماح للمستخدم المجهول بإجراء upload

anon_upload_enable = YES | NO

- السماح للمستخدم المجهول بإنشاء مجلدات

anon_mkdir_write_enable = YES | NO

- تغيير المالك لعملية الـ Upload

chown_uploads = YES | NO

- تحديد اسم مالك عملية الـ Upload الجديد

chown_username = [user name]

- تفعيل عمل ملف user_list لمنع مستخدمين محددين من استخدام ftp

Userlist_enable=YES

- تحديد الـ Port 20 ليتم الاتصال من خلاله

connect_from_port_20 = YES | NO

الزبون

لا يوجد إعدادات خاصة عند الزبون؛ وإنما فقط مايلي:

م. ماجدة محمد أسعد

1. تشغيل خدمة FTP

Service vsftpd start

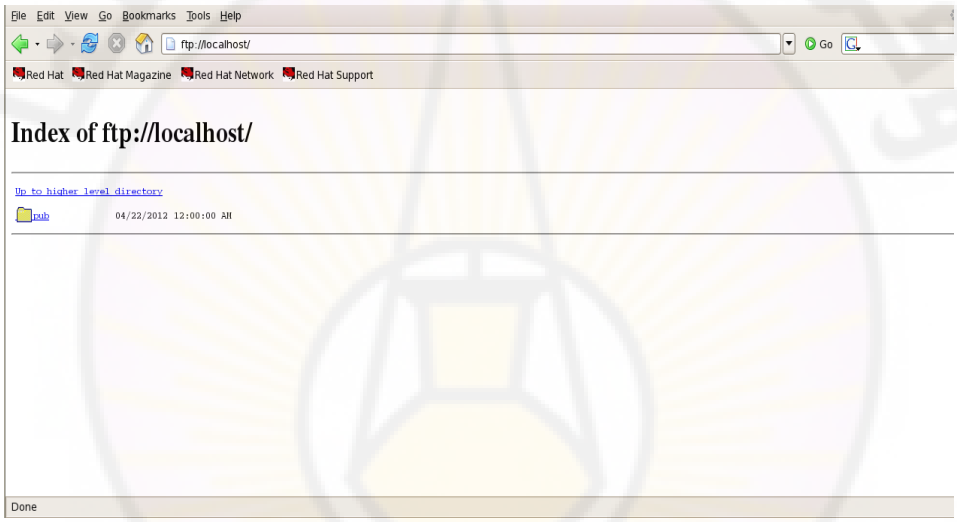
2. إيقاف الـ Firewall، مالم يتم إضافة قاعدة خاصة بالخدمة vsftpd ضمن جدار النار (وهذا ما سيتم تناوله في فصل الآمن – جدار النار)

Service iptables stop

3. الاتصال

يمكن الدخول كمستخدم مجهول مباشرة باستخدام متصفح الإنترنت عن طريق الكتابة في شريط العنوان:

ftp:// [ftp ip/name]



الشكل 6-10 الدخول كمستخدم مجهول بواسطة ftp.

أو الدخول من خلال شاشة نصية، بالشكل:

ftp [ip \ name]

```
[root@localhost ~]# ftp 192.186.0.2
Connected to 192.186.0.2.


[1]+  Stopped                 ftp 192.186.0.2
[root@localhost ~]# ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.0.2:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

الشكل 6-11 الدخول كمستخدم مجهول لمخدّم ftp.

يمكن الدخول كمستخدم محلي بعد تفعيل الخيار اللازم له في ملف vsftpd.conf والخيار هو:

local_enable=yes

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
"/etc/vsftpd/vsftpd.conf" 116L, 4395C
```

الشكل 6-12 تعديل ملف إعداد vsftpd.conf لتفعيل المستخدم المحلي.

يستطيع مستخدم محلي بالدخول بعد تعديل هذا الخيار.

```
[root@localhost ~]# gedit /etc/vsftpd/vsftpd.conf
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
[root@localhost ~]# ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.0.2:root): tcc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/tcc"
ftp> ls
227 Entering Passive Mode (192,168,0,2,91,174)
150 Here comes the directory listing.
-rw-rw-r--    1 500      500             0 Nov 23 16:52 gg
-rw-rw-r--    1 501      0               0 Nov 20 22:46 test
226 Directory send OK.
ftp>
```

الشكل 6-6 الدخول كمستخدم محلي.

يبدأ عمل برنامج ftp، فنقوم بتنفيذ الأوامر الخاصة به، وهي:

- معرفة الدليل الحالي pwd
- استعراض محتوى المجلد الحالي لدى المخدّم، (في حال كان الدخول كمستخدم محلي، سيكون المجلد الحالي هو مجلد المستخدم، أما إذا كان الدخول كمستخدم مجهولاً سيكون المجلد الحالي لدى المخدّم /var/ftp

ftp> ls

بعد الاتصال بـ FTP Server جميع الأوامر التي تُكتب تنفذ على مخدّم FTP، من أجل تنفيذ الأوامر على الجهاز الحالي (المتصل بـ FTP) يسبق الأمر بإشارة (!)، مثال:

ftp> ! ls

```
ftp> pwd
257 "/"
ftp> !ls
anaconda-ks.cfg  install.log         test
Desktop          install.log.syslog  test1
home             old.home            vmware-tools-distrib
infile.c         old.tar
infile.c~        scsrun.log
ftp> !pwd
/root
ftp> ls
227 Entering Passive Mode (192,168,0,2,152,131)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Apr 22  2012 pub
-rw-r--r--    1 0        0             139 Jan 03 18:29 test
226 Directory send OK.
ftp>
```

الشكل 6-7 أوامر ftp على حاسب الزبون والمخدّم.

- التحميل من مخدّم FTP كمستخدم مجهول إلى المجلد المحلي الحالي.

ftp > get [path/filename]

كما يظهر بالشكل (6–15) تحميل ملف test من المخدّم (مجلد var/ftp/) إلى حاسب الزبون المجهول بالدليل الحالي.

```
ftp> pwd
257 "/"
ftp> !ls
anaconda-ks.cfg  install.log         test
Desktop          install.log.syslog  test1
home             old.home            vmware-tools-distrib
infile.c         old.tar
infile.c~        scsrun.log
ftp> !pwd
/root
ftp> ls
227 Entering Passive Mode (192,168,0,2,152,131)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Apr 22  2012 pub
-rw-r--r--    1 0        0             139 Jan 03 18:29 test
226 Directory send OK.
ftp> get test
local: test remote: test
227 Entering Passive Mode (192,168,0,2,83,162)
150 Opening BINARY mode data connection for test (139 bytes).
226 File send OK.
139 bytes received in 0.00034 seconds (4e+02 Kbytes/s)
ftp> !ls
anaconda-ks.cfg  home      infile.c~    install.log.syslog  old.tar    test  vmware-tools-distrib
Desktop          infile.c  install.log  old.home            scsrun.log  test1
ftp>
```

الشكل 6-15 التحميل downloadكمستخدم مجهول.

في الشكل (6–16) عملية تحميل لملف new من المخدّم (مجلد المستخدم المحلي) إلى مجلد الزبون.

```
ftp> ls
227 Entering Passive Mode (192,168,0,2,239,127)
150 Here comes the directory listing.
-rw-rw-r--    1 500      500           0 Nov 23 16:52 gg
-rw-r--r--    1 0        0           139 Jan 03 19:22 new
-rw-rw-r--    1 501      0             0 Nov 20 22:46 test
226 Directory send OK.
ftp> !ls
anaconda-ks.cfg  home     infile.c~   install.log.syslog  old.tar    test   vmware-tools-distrib
Desktop          infile.c  install.log  old.home          scsrun.log  test1
ftp> get new
local: new remote: new
227 Entering Passive Mode (192,168,0,2,145,251)
150 Opening BINARY mode data connection for new (139 bytes).
226 File send OK.
139 bytes received in 0.00039 seconds (3.5e+02 Kbytes/s)
ftp> !ls
anaconda-ks.cfg  home     infile.c~   install.log.syslog  old.home  scsrun.log  test1
Desktop          infile.c  install.log  new               old.tar   test        vmware-tools-distrib
ftp>
```

الشكل 6-8 التحميل download كمستخدم محلي.

- الرفع إلى المجلد الخاص بالمستخدم المحلي على FTP

ftp > mput path/filename

ترفع ملفات المستخدمين المجهولين إلى var/ftp/، في حال المستخدم المحلي ترفع الملفات إلى مجلده الخاص.

```
ftp> !ls
anaconda-ks.cfg  home      infile.c~    install.log.syslog  old.home
Desktop          infile.c  install.log  new                 old.tar
ftp> mput infile.c
mput infile.c? yes
227 Entering Passive Mode (192,168,0,2,180,118)
150 Ok to send data.
226 File receive OK.
80 bytes sent in 0.051 seconds (1.5 Kbytes/s)
ftp> ls
227 Entering Passive Mode (192,168,0,2,192,207)
150 Here comes the directory listing.
-rw-rw-r--    1 500      500             0 Nov 23 16:52 gg
-rw-------    1 500      500            80 Jan 03 19:27 infile.c
-rw-r--r--    1 0        0             139 Jan 03 19:22 new
-rw-rw-r--    1 501      0               0 Nov 20 22:46 test
226 Directory send OK.
ftp>
```

الشكل 6-17 الرفع upload إلى مخدّم ftp كمستخدم محلي.

- إنهاء جلسة FTP

ftp > quit

6-4-3 منع مستخدم محدد

تأهيل خيار local_enable في ملف إعداد الخدمة يسمح للمستخدمين كافة باستخدام ftp. يمكن منع مستخدم محدد من استخدام خدمة ftp من خلال تعديل الملف /etc/vsftpd/user_list.

بفرض لدينا مستخدم net نريد منعه، نقوم بالآتي:

```
[root@localhost ~]# ls /home
net  tcc
[root@localhost ~]# cat /etc/vsftpd/user_list
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@localhost ~]# cat>>/etc/vsftpd/user_list
net
[root@localhost ~]#
```

الشكل 6-9 منع مستخدم من خدمة ftp.

سيتم إعطاء رسالة عند قيام المستخدم المحجوب بالدخول إلى مخدّم ftp.

```
[root@localhost ~]# ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.0.2:root): net
530 Permission denied.
Login failed.
ftp>
```

الشكل 6-10 دخول مستخدم ممنوع.

6-4-4 إعداد خدمة *SELinux* لاستخدام *FTP*

- السماح باستخدام ftp ضمن SELinux من دون قيود

setsebool allow_ftpd_full_access 1

- السماح بالكتابة ضمن المجلدات المعدة ضمن إعدادات SELinux

setsebool allow_ftpd_anon_write 1

- السماح باستخدام الملفات التي تم مشاركتها من خلال NFS

setsebool aloow_ftpd_use_nfs 1

- السماح للمستخدم المحلي بالدخول إلى مجلده الخاص

setsebool ftp_home_directory 1

إعداد الشبكة

Network Configurations

إعداد الشبكة Network Configurations

5-1 المقدمة

يتم إقلاع نظام التشغيل لينكس بحالة عمل متعددة المستخدمين multiuser أي تفعيل خدمة الشبكة وذلك بحالة العمل 2 و3 و 5.

نقوم باستعراض الملف /etc/modprobe للتأكد من تحميل الوحدة النمطية الخاصة بالشبكة ضمن النواة conf.

يقرر نظام لينكس عنوان كرت الشبكة إما بشكل أوتوماتيكي من خلال dhcp أو يتم إعطاءه عنوان ثابت static.

يدعم لينكس بروتوكول IPV4, IPV6.

5-2 ملفات إعداد الشبكة

5-2-1 ملف */etc/hosts*

يعدل يدويا من قبل المشرف، يستخدم في حال عدم وجود DNS وبالتالي نضع عنوان ip و name اسم للمخدم .

```
[root@mail ~]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain   localhost
::1     localhost6.localdomain6 localhost6
192.168.1.3     mail.tcc.com    mail
192.168.1.3     www.mysite.com
192.168.1.3     www.ERH153.com
[root@mail ~]#
```

الشكل 5-1 ملف hosts

5-2-2 ملف */etc/host.conf*

يحتوي ترتيب البحث من عناوين مخدمات الأسماء DNS، اذا تم التعامل مع الأسماء:

ملف host السابق أو خدمة مجال الأسماء bind ومحتوى الملف فقط سطر وحيد ونستطيع تغيير الترتيب بين كلا الآليتين :

```
[root@mail ~]# cat /etc/host.conf
order hosts,bind
[root@mail ~]#
```

الشكل 5-2 ملف host.conf

5-2-3 ملف */etc/services*

يظهر رقم بوابات التطبيقات أي الخدمات العاملة ضمن النظام مع اسم البروتوكول، ويمكن إيقاف عمل بوابة ما، بوضع تعليق في بداية السطر أو حذفه:

```
# Each line describes one service, and is of the form:
#
# service-name  port/protocol  [aliases ...]   [# comment]

tcpmux          1/tcp                           # TCP port service multiplexer
tcpmux          1/udp                           # TCP port service multiplexer
rje             5/tcp                           # Remote Job Entry
rje             5/udp                           # Remote Job Entry
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
systat          11/udp          users
daytime         13/tcp
daytime         13/udp
qotd            17/tcp          quote
qotd            17/udp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp-data        20/udp
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
```

الشكل 5-3 ملف services

5-2-4 ملف */etc/nsswitch.conf*

يحتوي ترتيب البحث عن أداة توثيق المستخدمين و تكون بإحدى الطرق:

File: استخدام ملف etc/passwd/ للتوثيق.

Nis:استخدام خدمة NIS (Network Information System) للتوثيق.

DNS: استخدام مخدم الأسماء للبحث عن مخدم توثيق آخر.

محتوى الملف ونجد في البداية أسطر تعليق تشرح كل مدخل ضمنه:

```
# Legal entries are:
#
#       nisplus or nis+         Use NIS+ (NIS version 3)
#       nis or yp               Use NIS (NIS version 2), also called YP
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the local database (.db) files
#       compat                  Use NIS on compat mode
#       hesiod                  Use Hesiod for user lookups
#       [NOTFOUND=return]       Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files
shadow:     files
group:      files

#hosts:     db files nisplus nis dns
hosts:      files dns
```

الشكل 5-4 ملف nsswitch.conf

5-2-5 ملف */etc/resolve.conf*

يحتوي أسماء و عناوين مخدمات الأسماء المرتبطة بالشبكة.

```
[root@mail ~]# cat /etc/resolv.conf
# Generated by NetworkManager


# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
#
# DNS1=xxx.xxx.xxx.xxx
# DNS2=xxx.xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
```

الشكل 5-5 ملف resolv.conf

5-2-6 ملف */etc/sysconfig/network/*

تفعيل الشبكة عند اقلاع النظام وتعديل اسم المخدم و تفعيل كرت الشبكة أم لا و تفعيل IPV6 ، ووضع اسم مخدم NIS في حال استخدامه.

```
[root@mail ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=mail.tcc.com
NISDOMAIN="tcc-server"
IPV6_AUTOCONF=yes
[root@mail ~]#
```

الشكل 5-6 ملف network

5-2-7 مجلد */etc/sysconfig/network.scripts/*

يحتوي على:

1-ملفات نصية تمثل خصائص كل نوع من أنواع بطاقات الشبكة المتوفرة في النظام، فمثلاً: /etc/sysconfig/Network.script/ifcfg-eth0 الملف الخاص بكرت الشبكة إيثرنت الأول.

محتوى الملف:

- اسم الاختصار الخاص بالبطاقة.
- نوع بروتوكول الإقلاع (none (static) or dhcp) لتحديد عنوان ip للحاسب.
- تفعيل البطاقة عند الإقلاع أم لا(onboot) .

- عنوان البطاقة التسلسلي MAC (HWADDR).
- عنوان ip وقناع الشبكة الفرعية للحاسب (IPADRR).
- البوابة الافتراضية Default Gateway.

```
[root@mail ~]# ls /etc/sysconfig/network-scripts/
ifcfg-eth0      ifdown-post     ifup-ippp     ifup-sl
ifcfg-eth0~     ifdown-ppp      ifup-ipsec    ifup-tunnel
ifcfg-eth0.bak  ifdown-routes   ifup-ipv6     ifup-wireless
ifcfg-lo        ifdown-sit      ifup-ipx      init.ipv6-global
ifdown          ifdown-sl       ifup-isdn     net.hotplug
ifdown-bnep     ifdown-tunnel   ifup-plip     network-functions
ifdown-eth      ifup            ifup-plusb    network-functions-ipv6
ifdown-ippp     ifup-aliases    ifup-post     route-eth0
ifdown-ipsec    ifup-bnep       ifup-ppp
ifdown-ipv6     ifup-eth        ifup-routes
ifdown-isdn     ifup-ib         ifup-sit
[root@mail ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
HWADDR=00:0c:29:c6:70:ba
[root@mail ~]#
```

الشكل 5-7 مجلد network-scripts وملف ifcfg-eth0

2-مجموعة من الملفات التنفيذية scripts لتفعيل البطاقات أو إيقافها والتأكد من تنفيذ السكريبت الخاص بالبطاقة ، فمثلا ifup eth0 و ifdown eth0 لكرت الشبكة إيثرنت.

الخدمة الأساسية للشبكة موجودة في مجلد /etc/init.d/network فهي تحمل التوابع اللازمة لعمل الشبكة والتحقق من ملف network ومن نوع البطاقة .

التحقق من إعداد البطاقة وتأهيله يتم باستخدام الأمر :

service network status

في الشكل التالي نبين عمل أمر التحقق و أمر التأهيل وإلغاء التأهيل.

```
[root@mail ~]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
[root@mail ~]# service network status
Configured devices:
lo eth0
Currently active devices:
lo eth0
[root@mail ~]# ifdown eth0
[root@mail ~]# service network status
Configured devices:
lo eth0
Currently active devices:
lo
[root@mail ~]# ifup eth0
[root@mail ~]# service network status
Configured devices:
lo eth0
Currently active devices:
lo eth0
[root@mail ~]#
```

الشكل 5-8 الأمر service للشبكة

3–ملف /etc/sysconfig/network-scripts/network-functions

ملف التوابع اللازمة لتأهيل وإلغاء تأهيل بطاقات كافة أنواع الشبكات والتي تستخدمها الملفات التنفيذية في مجلد network-scripts.

5–3 إعداد كرت الشبكة

لارتباط عدة حواسب معا؟ نحتاج إلى بطاقة شبكة ونظام تشغيل يتعامل مع بطاقة الشبكة (مثل إيثرنت ، مودم ISDN ، Token ring) وتعريف البطاقة بشكل صحيح للاتصال.

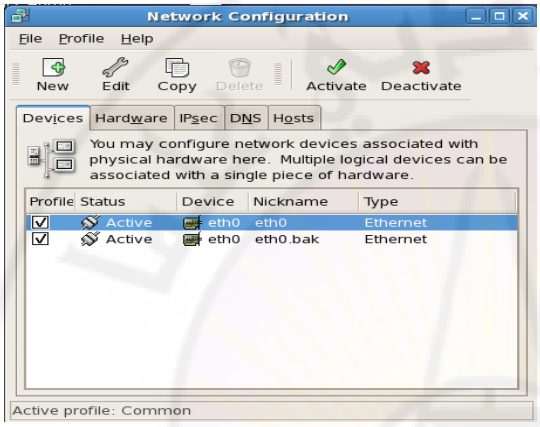
يمكن تعريف بطاقات الشبكة من أي نوع: Ethernet – ISDN – modem

wireless – token ring –– xDSL

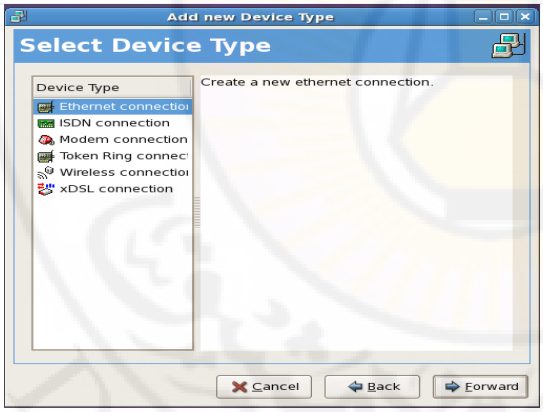
نستطيع التعريف بواسطة واجهة رسومية أو نصياً.

5-3-1 رسوميا

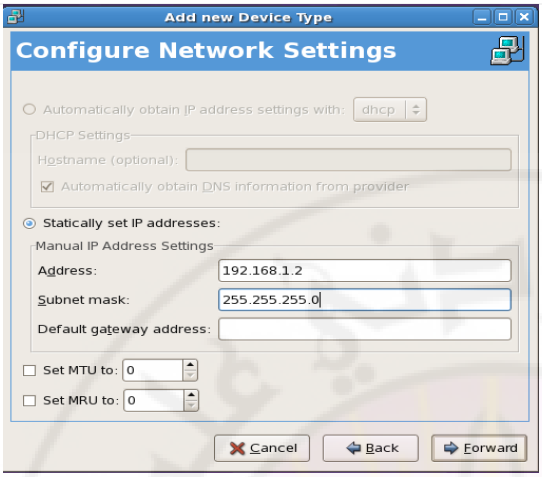
1. قائمة system --- administration --- network
2. تنفيذ الأمر system-config-network



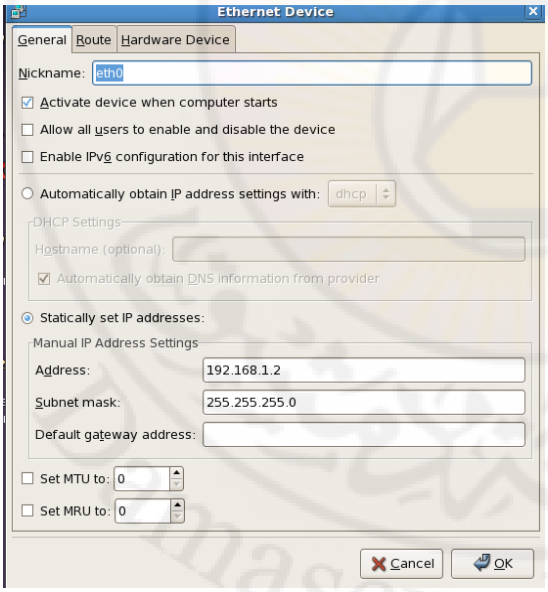
نختار إضافة بطاقة شبكة new :



نختار نوع بطاقة الشبكة المراد إضافته وليكن Ethernet



نكتب عنوان ip والشبكة الفرعية، أو نختار dhcp تلقائياً.



أو نختار كرت الشبكة ثم زر edit لتعديل خصائصه وإضافة الموجه و البوابة الافتراضية واسم المخدم. بالإضافة لعدة خيارات ،هي:

تفعيل تلقائي عند الإقلاع.

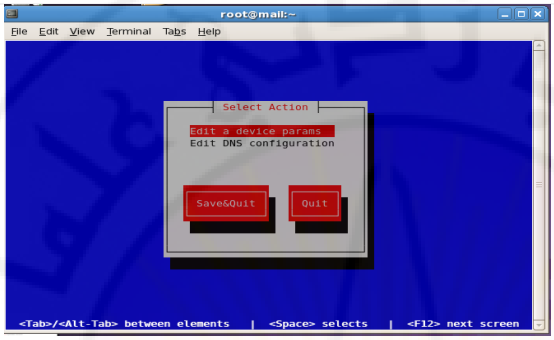
تمكين المستخدمين من تفعيل وإلغاء تفعيل البطاقة.

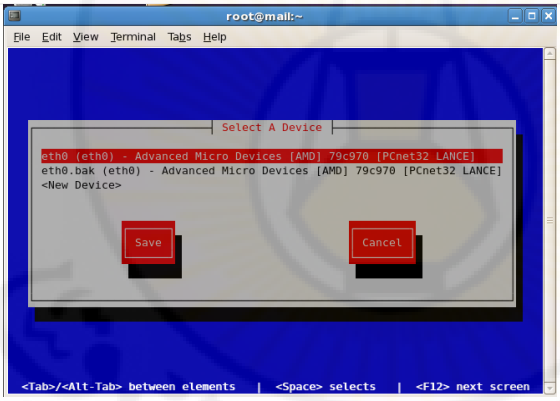
تفعيل بروتوكول IPv6 لهذه البطاقة.

5-3-2 نصيا

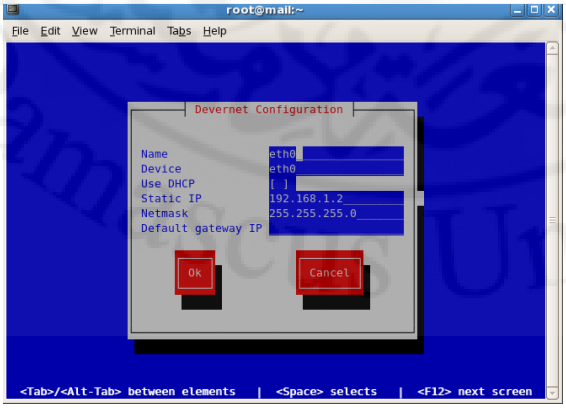
1- استخدام الأداة **system-config-network-tui**

تستخدم في حال عدم وجود واجهة رسومية.





نختار بطاقة شبكة الإيثرنت eth0



نحدد رقم ip وقناع الشبكة الفرعية أو اختيار dhcp عنوان البوابة الافتراضية

2- استخدام سطر الأمر:

ifconfig eth0 192.168.1.2 netmask 255.255.255.0

أو

ip addr add 192.168.1.2 dev eth0

```
[root@mail ~]# ifconfig   eth0 192.168.1.2   netmask 255.255.255.0
[root@mail ~]# ip   addr add 192.168.1.2  dev  eth0
```

الشكل 5-9 تعريف بطاقة شبكة جديدة

ملاحظة:

- هذا الأمر سيعدل مباشرة ضمن النواة.
- عند استخدام الأمر netconfig أو أي أداة إعداد أخرى، فهي ستعدل ملف الكرت مباشرة /etc/sysconfig/network-scripts/ifcfg-eth0 لذلك يجب إعادة تشغيل خدمة الشبكة

/etc/init.d/network restart

5-3-3 التعديل اليدوي للملفات

1. نعدل الملفات الخاصة بإعداد بطاقة الشبكة:

/etc/sysconfig/network-scripts/ifcfg-eth0 لتحديد بروتوكول الإقلاع ،عنوان ip ، قناع الشبكة الفرعية.

/etc/sysconfig/network لتحديد تفعيل الشبكة واسم المخدم وعنوان البوابة الافتراضية.

2. نعيد تشغيل الشبكة

Service network restart

3. ملف /etc/resolv.conf لإدخال عنوان مخدم الأسماء DNS ، بالشكل:

```
Nameserver      10.0.80.11
Nameserver      192.168.1.1
```

5-3-4 إنشاء كرت افتراضي *aliases*

استخدام نفس بطاقة الشبكة وإعطاءها عنوان ip مختلف. وهذا يتم بشكل ثابت وليس ديناميكي لأنه لا يعمل مع dhcp.

1. نعطي اسم وعنوان جديد

```
ifconfig  eth0:1  192.168.1.3
```

2. ننسخ الملف الخاص ببطاقة الشبكة الأساسي /etc/sysconfig/network-scripts/ifcfg-eth0

```
cp –v /etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-eth0:1
```

3. نعدل ضمن الملف عنوان ip للاختصار الجديد

5-3-5 حذف بطاقة شبكة افتراضية

ننفذ الأمر التالي:

```
Ifconfig  eth0:1  del  192.168.1.3
```

5-4 أوامر الشبكة Common Network Utilities

تستخدم لفحص الشبكة واكتشاف الأخطاء.

5-4-1 *Ping*

للاتصال مع حواسب أخرى باستخدام بروتوكول ICMP لإرسال رسالة echo-requests و استقبال ech-replies.

شكل الأمر:

ping -c 3 -I 3 host-ip

c تحديد عدد رسائل ICMP المراد إرسالها.

i تحديد التأخير الزمني بين رسالة وأخرى، افتراضيا 1 ثانية.

host-ip وضع عنوان أو اسم حاسب، ويستخدم هذا الأمر محتوى ملف /etc/hosts للحصول على عناوين الحواسب في حال استخدم الاسم.

ملاحظة: يوقف جدار النار عمل ICMP.

NETSTAT 2-4-5

إعطاء معلومات عن اتصالات الشبكة وكافة البروتوكولات، من ملف /proc/net ، ويستخدم الملف /etc/services ليحول رقم البوابة إلى اسم الخدمة.

شكل الأمر:

Netstat	
netstat -a	يظهر كافة protocols/sockets
netstat -ntlp	يظهر كافة البوابات التي يستمع لها TCP
netstat –nulp	يظهر كافة البوابات التي يستمع لها UDP
netstat -ntp	تظهر الاتصالات الفعالة
netstat -rn	تظهر جدول التوجيه

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:login                     *:*                         LISTEN
tcp        0      0 *:shell                     *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:telnet                    *:*                         LISTEN
tcp        0      0 localhost.localdomain:smtp  *:*                         LISTEN
tcp        0      0 *:imaps                     *:*                         LISTEN
tcp        0      0 *:pop3s                     *:*                         LISTEN
tcp        0      0 *:pop3                      *:*                         LISTEN
tcp        0      0 *:imap                      *:*                         LISTEN
udp        0      0 *:syslog                    *:*
udp        0      0 *:tftp                      *:*
udp        0      0 *:49256                     *:*
udp        0      0 *:mdns                      *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:53944                     *:*
udp        0      0 *:mdns                      *:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     5306   @ISCSIADM_ABSTRACT_NAMESPACE
unix  14     [ ]         DGRAM                    5638   /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     9549   @/tmp/fam-root-
--More--
```

الشكل 5-10 خرج الأمر netstat

```
[root@mail ~]# netstat -ntlp|more
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name

tcp        0      0 0.0.0.0:513                 0.0.0.0:*                   LISTEN      2262/xinetd

tcp        0      0 0.0.0.0:514                 0.0.0.0:*                   LISTEN      2262/xinetd

tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      2027/portmap

tcp        0      0 0.0.0.0:23                  0.0.0.0:*                   LISTEN      2262/xinetd

tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      2300/sendmail: a
cce
tcp        0      0 :::993                      :::*                        LISTEN      2273/dovecot

tcp        0      0 :::995                      :::*                        LISTEN      2273/dovecot

tcp        0      0 :::110                      :::*                        LISTEN      2273/dovecot

tcp        0      0 :::143                      :::*                        LISTEN      2273/dovecot

[root@mail ~]# netstat -nulp|more
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
udp        0      0 0.0.0.0:514                 0.0.0.0:*                               1989/syslogd
udp        0      0 0.0.0.0:69                  0.0.0.0:*                               2262/xinetd
udp        0      0 0.0.0.0:49256               0.0.0.0:*                               2357/avahi-daemon:
udp        0      0 0.0.0.0:5353                0.0.0.0:*                               2357/avahi-daemon:
udp        0      0 0.0.0.0:111                 0.0.0.0:*                               2027/portmap
udp        0      0 :::53944                    :::*                                    2357/avahi-daemon:
udp        0      0 :::5353                     :::*                                    2357/avahi-daemon:
```

الشكل 5-11 خرج الأمر netstat –ntlp

ملاحظة :0.0.0.0:514 أي خدمة syslog ستقبل كافة طرود عناوين ومنافذ IP المعرفة ضمن النظام.

ARP 3-4-5

يحول من عنوان فيزيائي من الطبقة الثانية (OSI model) إلى عنوان ip في الطبقة 3 ، وعند اتصال حاسبين معا سيحول من عنوان ip إلى عنوان فيزيائي.

لمعرفة العنوان الفيزيائي	***ifconfig***
ليعطي عنوان IP والعنوان الفيزيائي	***arp -a***

4-4-5 *Ifconfig*

إعطاء معلومات عن البطاقات المعرفة.

```
[root@mail ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:3C:71:F1
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3c:71f1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13395 (13.0 KiB)  TX bytes:8306 (8.1 KiB)
          Interrupt:169 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1904 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1904 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2644008 (2.5 MiB)  TX bytes:2644008 (2.5 MiB)
```

الشكل 5-12 خرج الأمر ifconfig

5-4-5 *route*

إظهار جدول التوجيه

```
[root@mail ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     255.255.255.0   UG    0      0        0 eth0
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
```

الشكل 5-13 الأمر route

تستخدم أيضا لتعريف موجه route جديد للشبكة أو بوابة افتراضية.

```
[root@mail ~]# route add -host 192.168.1.1 dev eth0
[root@mail ~]# route add default gw 192.168.1.1
[root@mail ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.1     *               255.255.255.255 UH    0      0        0 eth0
default         192.168.1.1     255.255.255.0   UG    0      0        0 eth0
192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
default         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
[root@mail ~]#
```

الشكل 5-14 إضافة موجه جديد للشبكة المحلية