GateManager™ server model 8250
Installation STEP 0
Preparing the LINUX installation

This guide describes the typical steps for preparing your Linux platform for installing the GateManager model 8250. This guide will depict how to install on a Linux CentOS.

Version: 1.6, November 2016

Table of Contents

Version history

- 1.6 Added new section 5 about changing local time in Linux. Previous section 5 and consecutive sections have been shifted.

.

Introduction

Related Documents

The following guides are available from the Secomea partner website – www.secomea.com

- **GateManager Server 8250 Installation STEP 0 (THIS GUIDE)**

  This guide describes preparation of the Linux platform before GateManager installation. If installing at a hosting center, the VM image with a Linux installation with preinstalled hosting center tools may be provided. This guide uses CentOS as example.

- **GateManager Server 8250 Installation STEP 1**

  This guide describes the installation of the GateManager server on the Linux platform. This step is typically done by the IT department.

- **GateManager Server Installation STEP 2**

  This guide describes the necessary steps to configure the GateManager to become operational and to setup backup. The guide is intended for the appointed GateManager Server administrator.

- **Customer and License Administration (for Secomea Distributors)**

  This guide describes common daily tasks of creating accounts and how to manage LinkManager licenses.

- **GateManager PREMIUM Domain Administration**

  This gives an overview of the daily administration tasks, such as organizing accounts and devices in domains, provide specific access to specific equipment, creates Alerts etc.

Choosing between GateManager 8250 or 9250

Secomea offers two versions of the software based GateManager:

- **Model 9250**, which is delivered as preinstalled virtual image based on a Linux platform that Secomea has adapted with the necessary services. This is the recommended version, but requires a VM platform (such as ESXi or HyperV) on which the image can be deployed. Some hosting centers do accept such customer provided images, others don’t.
- **Model 8250**, which must be installed on a Linux platform, and where the Linux environment must be adapted to the GateManager. This version is required for installation on standalone servers, and for hosting centers that do not offer installation of a customer provided VM image, but instead provides a Linux OS with preinstalled services. Such hosting centers typically offer various Linux versions, among which Debian and CentOS are typical.

The following example of Linux preparation is based on a VPS (Virtual Private Server) based on a 32bit CentOS 6.4, and fully working internet connection with an IP address accessible from the Internet and all ports forwarded to the server.

1. Preparing the Linux installation

1.1. Change the Linux password

Login to the server with your ssh client. If configuring from Windows, we recommend PuTTY.

It is recommended to change the password for the installation as the first thing.

Command:

```
# passwd
```

1.2. Install and run setuptool

You do the following steps from the command line, and with your favorite editor. To better visualize the configuration you can use a text based GUI tool will assist you in configuring the network, a simple firewall and the authentication and which system services to start up at boot.

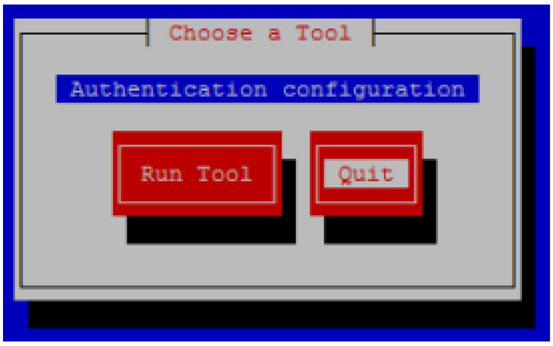
```
# yum install setuptool
```

Note the ability to install these tools, may depend on your Linux installation. If not compatible, you must perform the steps manually via standard editors.

1.3. Install needed tools

Start the setup tool, and verify what is installed

```
# setup
```

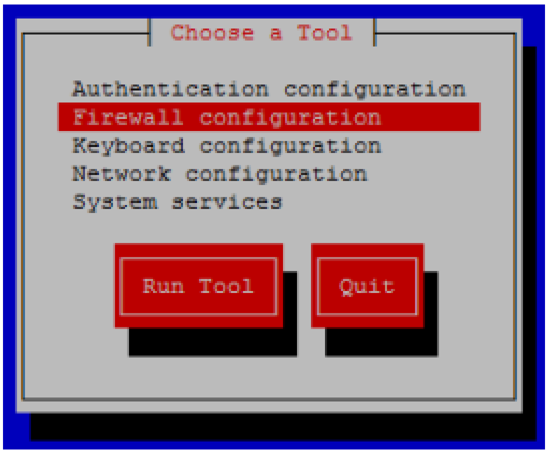


In this case, only Authentication services tool is installed, and we need to install firewall/iptables, country-keyboards and network tools:

```
# yum install system-config-securitylevel-tui
# yum install system-config-keyboard
# yum install system-config-network-tui
# yum install newt-python      (only necessary sometimes)
```

Run the setuptool again, and check that your tools are successfully installed:

```
# setup
```



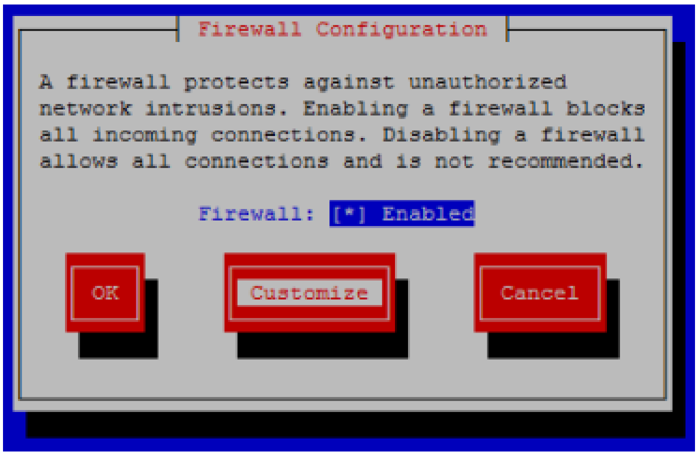
```
Choose a Tool

Authentication configuration
Firewall configuration
Keyboard configuration
Network configuration
System services
```

A good first step would be to set the Keyboard configuration to match you national keyboard layout.

2. Setup the Firewall

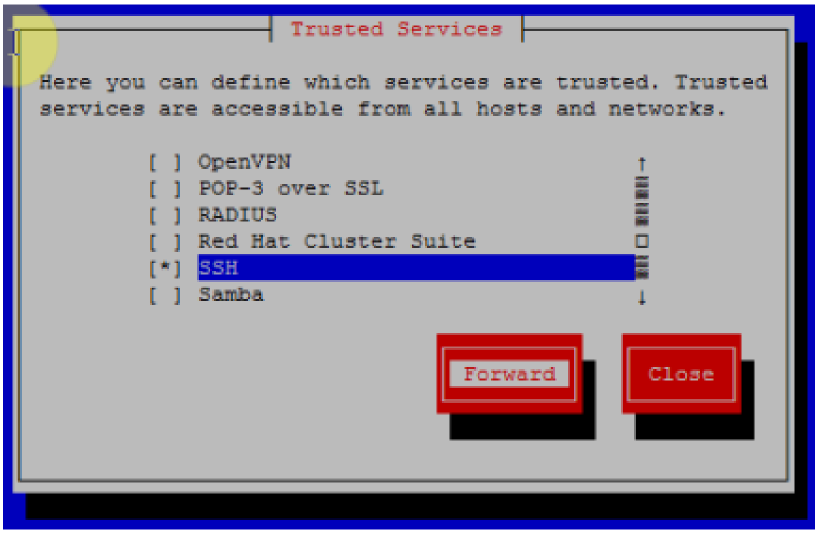
1.4. Allow incoming ports

Check that the firewall is enabled



```
Firewall Configuration

A firewall protects against unauthorized
network intrusions. Enabling a firewall blocks
all incoming connections. Disabling a firewall
allows all connections and is not recommended.

Firewall: [*] Enabled
```

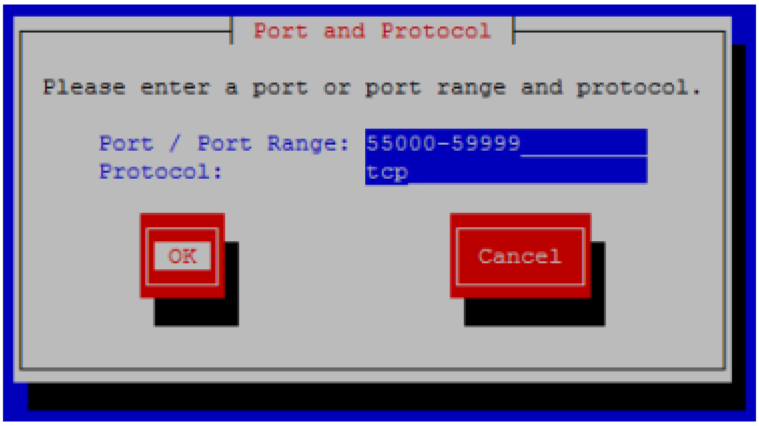
Click Customize, and scroll down the Trusted services, and check that SSH is enabled. (for VPS solutions this port would typically be open)



```
Trusted Services

Here you can define which services are trusted. Trusted
services are accessible from all hosts and networks.

[ ] OpenVPN
[ ] POP-3 over SSL
[ ] RADIUS
[ ] Red Hat Cluster Suite
[*] SSH
[ ] Samba
```

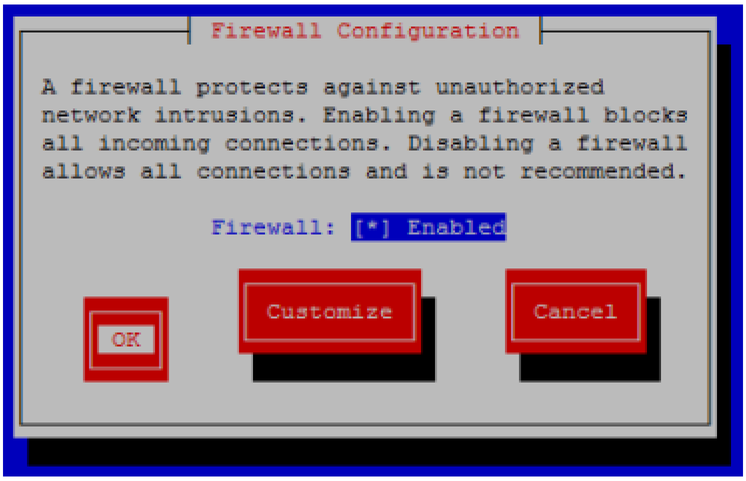
Click **Forward** and **Add** and apply following Ports and Protocols one by one:

Port	*Protocol*	*Description*
80	**tcp**	http
443	**tcp**	https
3389	**tcp**	RDP
5800	**tcp**	JVNC
5900	**tcp**	VNC
11444	**tcp**	Default Uplink
55000-59999	**tcp**	GoToAppliance



```
Please enter a port or port range and protocol.

  Port / Port Range: 55000-59999
  Protocol:          tcp
```

Make sure Firewall is enabled and select OK and Yes to override existing configuration.



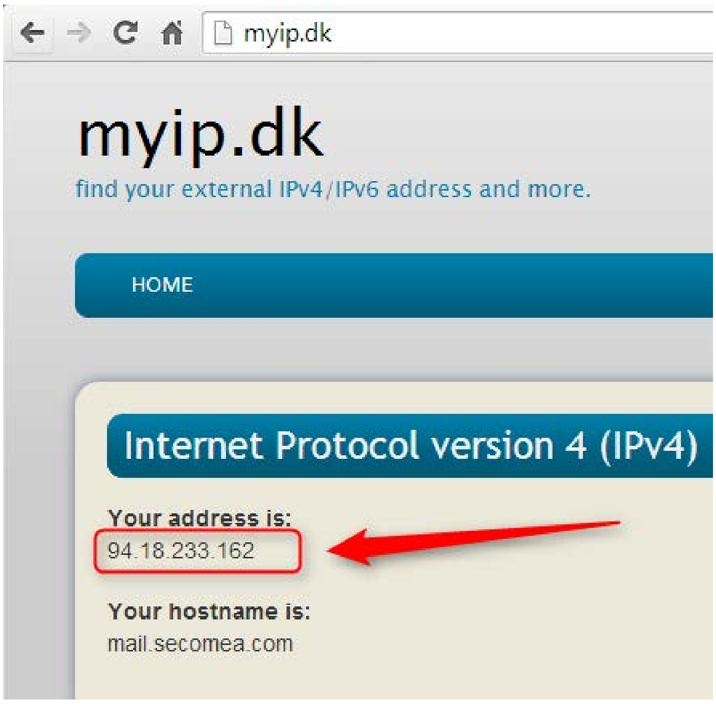
```
A firewall protects against unauthorized
network intrusions. Enabling a firewall blocks
all incoming connections. Disabling a firewall
allows all connections and is not recommended.

            Firewall: [*] Enabled
```

Exit the setup tool and

1.5. Optional: Restrict access to SSH

You may need access to SSH to make configuration of the server, but SSH is not a port you want to have open to the Internet. An interim solution is to restrict access to the public Internet address of your location. Make sure that this IP is not a dynamic address (i.e. it should be your fixed corporate address).

You can check your public address by one of the many websites providing such information, such as www.myip.dk:



myip.dk

find your external IPv4/IPv6 address and more.

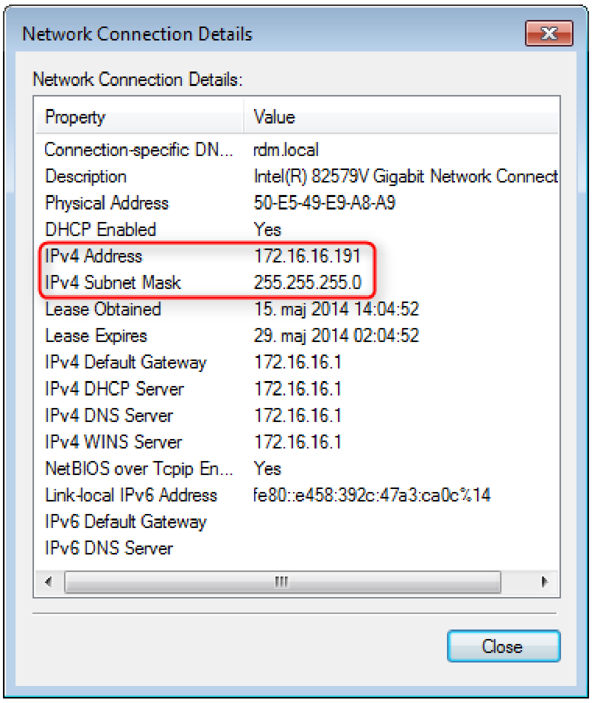
Internet Protocol version 4 (IPv4)

Your address is:
94.18.233.162

Your hostname is:
mail.secomea.com

If the server is residing behind your corporate firewall, you should also allow your local IP address, or rather your local subnet, as your IP may be DHCP assigned and could change.

On Windows, open a command prompt and type **`ipconfig`**, and check the status of your currently active network adapter in the control panel



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	rdm.local
Description	Intel(R) 82579V Gigabit Network Connect
Physical Address	50-E5-49-E9-A8-A9
DHCP Enabled	Yes
IPv4 Address	172.16.16.191
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	15. maj 2014 14:04:52
Lease Expires	29. maj 2014 02:04:52
IPv4 Default Gateway	172.16.16.1
IPv4 DHCP Server	172.16.16.1
IPv4 DNS Server	172.16.16.1
IPv4 WINS Server	172.16.16.1
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::e458:392c:47a3:ca0c%14
IPv6 Default Gateway	
IPv6 DNS Server	

The subnet represented by this IP address and subnet mask, can also be denoted as **172.16.16.0/24**.

Make sure you have an appropriate editor on the Linux server. In this case we install nano:

```
# yum install nano
```

With the editor open the firewall configuration:

```
# nano /etc/sysconfig/iptables
```

Here we see the list of ports we added using the setup tool. Locate the line with the SSH port (includes the parameter "--dport 22"), and apply your public source IP address, so the line reads as follows:

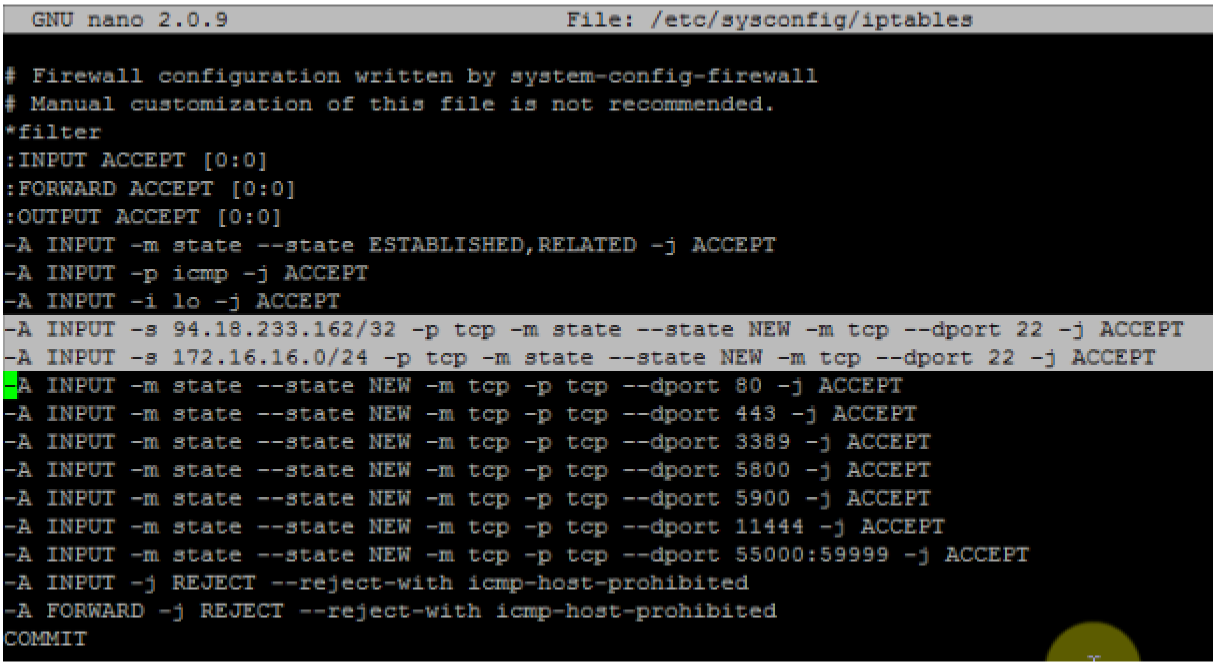
```
-A INPUT -s 94.18.233.162/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

(The subnet mask /32 will limit to this single IP, rather than a range of IPs)

If the service is inside your corporate network, you should duplicate the line, and apply your local IP address of local subnet. e.g in this case /24 indicates the entire range 172.16.16.1-254:

```
-A INPUT -s 172.16.16.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

The iptables file with the new corrected entries should look like this:



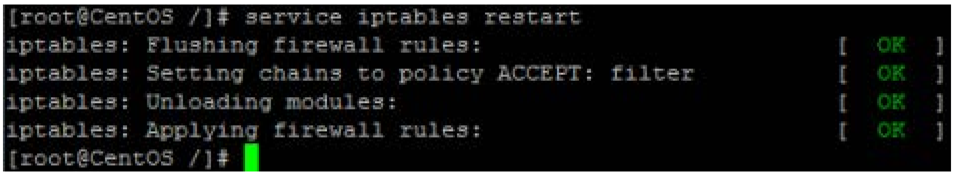
```
  GNU nano 2.0.9                         File: /etc/sysconfig/iptables

# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 94.18.233.162/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.16.16.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3389 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5800 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 11444 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 55000:59999 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

1.6. Verify firewall changes

Restart the firewall to verify changes.

```
# service iptables restart
```

Check that it all says OK:



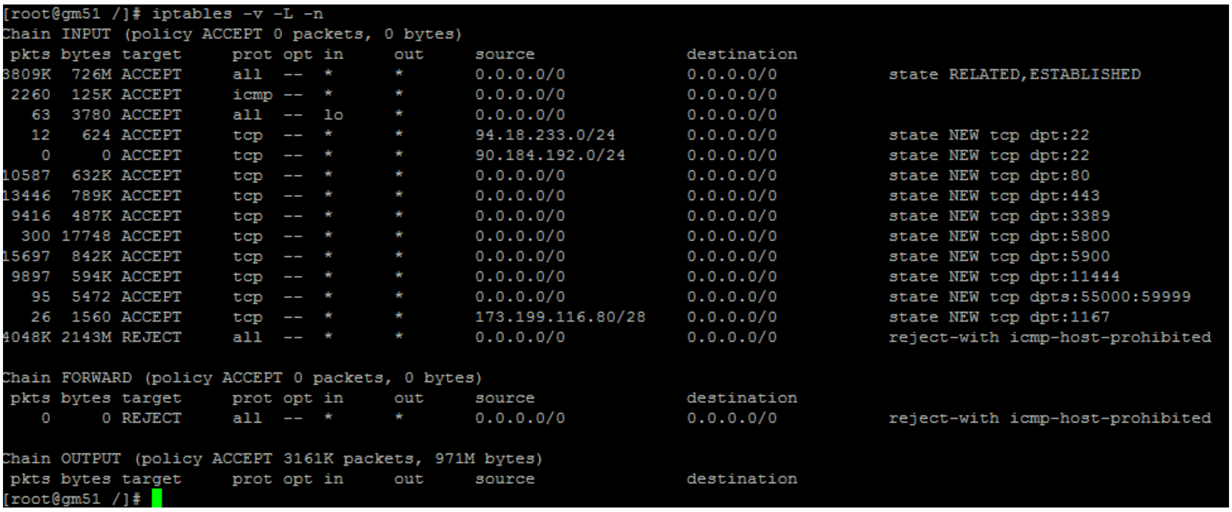
```
[root@CentOS /]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
[root@CentOS /]#
```

Now save the changes to activate them:

```
# service iptables save
```

You can always check the running configuration with the command:

```
# iptables –v –L –n
```



```
[root@gm51 /]# iptables -v -L -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
3809K  726M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
 2260  125K ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
   63  3780 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
   12   624 ACCEPT     tcp  --  *      *       94.18.233.0/24       0.0.0.0/0           state NEW tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       90.184.192.0/24      0.0.0.0/0           state NEW tcp dpt:22
10587  632K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
13446  789K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
 9416  487K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:3389
  300 17748 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:5800
15697  842K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:5900
 9897  594K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:11444
   95  5472 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpts:55000:59999
   26  1560 ACCEPT     tcp  --  *      *       173.199.116.80/28    0.0.0.0/0           state NEW tcp dpt:1167
4048K 2143M REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 3161K packets, 971M bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@gm51 /]#
```

Reboot the server to see the changes take effect and to verify that you can still connect to the server

```
# reboot
```

If you cannot connect afterwards, you may have made a configuration error in the firewall, and you may have logon locally on the server to fix, or have the VPS image reset at the hosting center. Better run into such problems now, before you have made a lot of installation on the server.

IMPORTANT! If you rerun the firewall menu from the setup tool and save the changes, then be aware the special rules for SSH will be reverted and you have to redo the steps shown above.

3. Remove unnecessary Linux services

You should disable preinstalled services that are not needed, both in order to optimize performance and to avoid potential security issues (especially those representing listen sockets)

Services that typically installed with a VPS and which should be disabled are:

cups, ip6tables, nfslock, rpsbind, rpcgssd, rpcidmapd, fcoe

Services that we should make sure are running are:

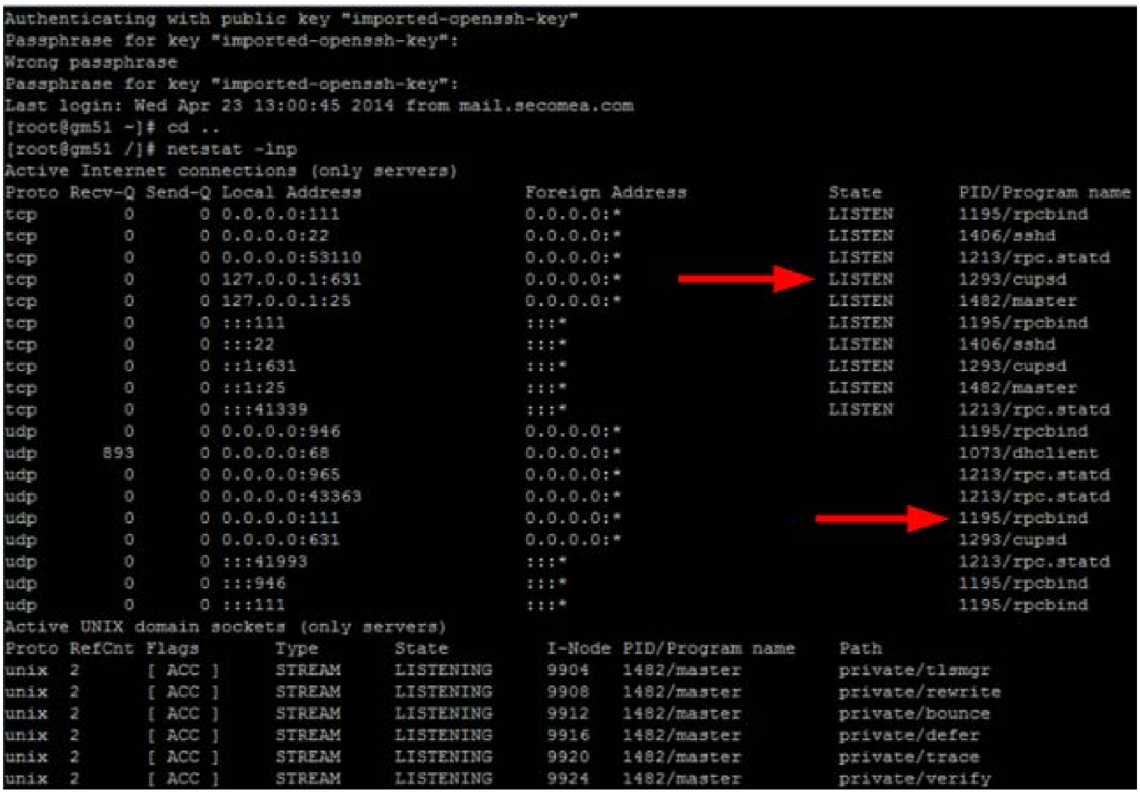
crond, gatemanager, iptables, network, ntpd, postfix*, sshd

(* Or other mail service, such as sendmail)

Use netstat to verify currently running services:

```
# netstat -lnp
```

In this example we see cups and rpsbind services being active:

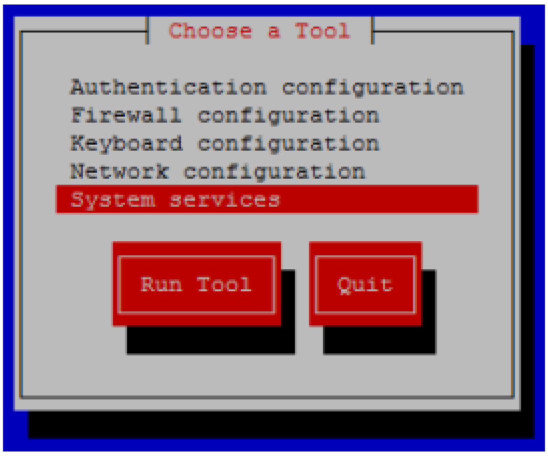


```
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Wrong passphrase
Passphrase for key "imported-openssh-key":
Last login: Wed Apr 23 13:00:45 2014 from mail.secomea.com
[root@gm51 ~]# cd ..
[root@gm51 /]# netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      1195/rpcbind
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1406/sshd
tcp        0      0 0.0.0.0:53110               0.0.0.0:*                   LISTEN      1213/rpc.statd
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      1293/cupsd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1482/master
tcp        0      0 :::111                      :::*                        LISTEN      1195/rpcbind
tcp        0      0 :::22                       :::*                        LISTEN      1406/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      1293/cupsd
tcp        0      0 ::1:25                      :::*                        LISTEN      1482/master
tcp        0      0 :::41339                    :::*                        LISTEN      1213/rpc.statd
udp        0      0 0.0.0.0:946                 0.0.0.0:*                               1195/rpcbind
udp      893      0 0.0.0.0:68                  0.0.0.0:*                               1073/dhclient
udp        0      0 0.0.0.0:965                 0.0.0.0:*                               1213/rpc.statd
udp        0      0 0.0.0.0:43363               0.0.0.0:*                               1213/rpc.statd
udp        0      0 0.0.0.0:111                 0.0.0.0:*                               1195/rpcbind
udp        0      0 0.0.0.0:631                 0.0.0.0:*                               1293/cupsd
udp        0      0 :::41993                    :::*                                    1213/rpc.statd
udp        0      0 :::946                      :::*                                    1195/rpcbind
udp        0      0 :::111                      :::*                                    1195/rpcbind
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
unix  2      [ ACC ]     STREAM     LISTENING     9904   1482/master         private/tlsmgr
unix  2      [ ACC ]     STREAM     LISTENING     9908   1482/master         private/rewrite
unix  2      [ ACC ]     STREAM     LISTENING     9912   1482/master         private/bounce
unix  2      [ ACC ]     STREAM     LISTENING     9916   1482/master         private/defer
unix  2      [ ACC ]     STREAM     LISTENING     9920   1482/master         private/trace
unix  2      [ ACC ]     STREAM     LISTENING     9924   1482/master         private/verify
```

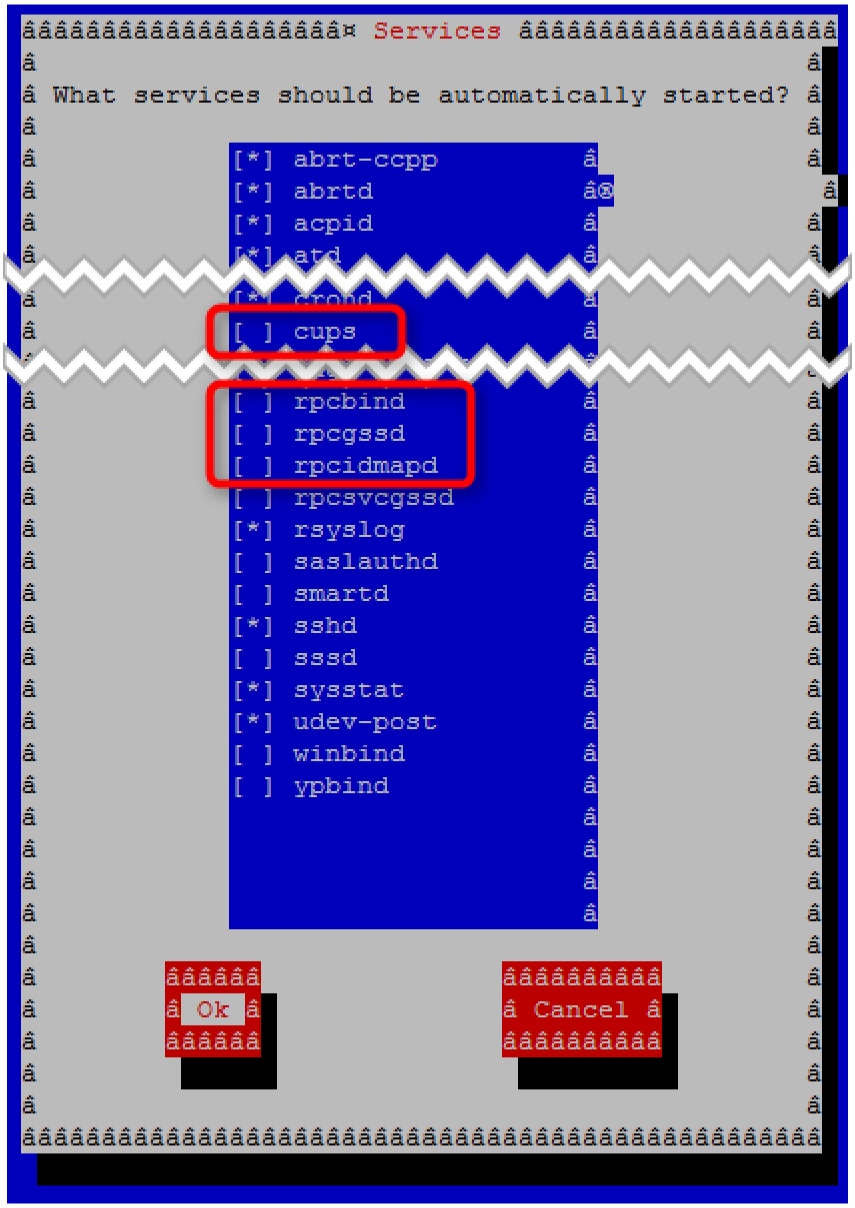
Start the setuptool

```
# setup
```

And run the System services tool



Uncheck the unnecessary services:



```
ââââââââââââââââââââ¤ Services ââââââââââââââââââââ
â                                                  â
â What services should be automatically started?   â
â                                                  â
â              [*] abrt-ccpp            â          â
â              [*] abrtd                â®          â
â              [*] acpid                â          â
â              [*] atd                  â          â
â              [*] crond                â          â
â              [ ] cups                 â          â
â              [ ] rpcbind              â          â
â              [ ] rpcgssd              â          â
â              [ ] rpcidmapd            â          â
â              [ ] rpcsvcgssd           â          â
â              [*] rsyslog              â          â
â              [ ] saslauthd            â          â
â              [ ] smartd               â          â
â              [*] sshd                 â          â
â              [ ] sssd                 â          â
â              [*] sysstat              â          â
â              [*] udev-post            â          â
â              [ ] winbind              â          â
â              [ ] ypbind               â          â
â                                       â          â
â                                       â          â
â                                       â          â
â                                       â          â
â                                                  â
â         ââââââ                ââââââââââ         â
â         â Ok â                â Cancel â         â
â         ââââââ                ââââââââââ         â
â                                                  â
â                                                  â
ââââââââââââââââââââââââââââââââââââââââââââââââââââ
```

Note: this is just an example – your CentOS installation will probably vary.

Press OK to save.

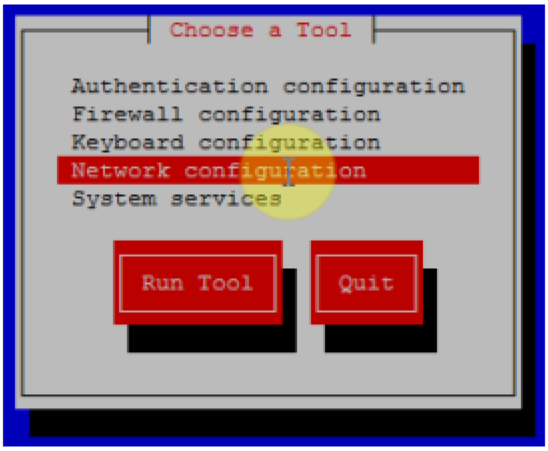
4. Setting the server host name (DNS)

The host name is displayed at the command prompt. In this case it is “CentOS”.

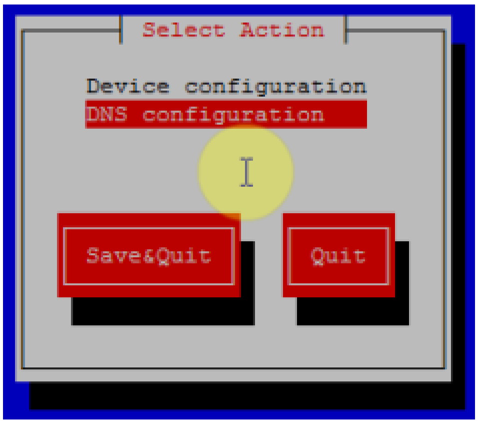
Run the setuptool.

```
# setup
```

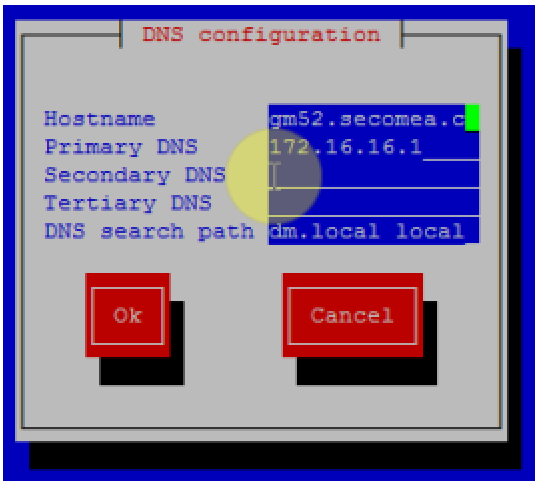
Select Network configuration



DNS configuration



Enter the DNS name (Hostname) you want your GateManager registered as



```
Hostname          gm52.secomea.c
Primary DNS       172.16.16.1
Secondary DNS
Tertiary DNS
DNS search path   dm.local local
```

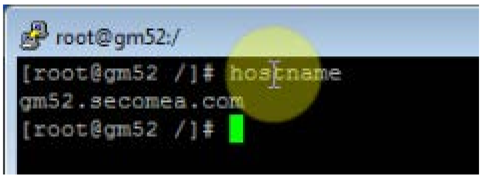
Press OK and Save.

Reboot the server to ensure the new DNS name is activated

```
# reboot
```

The command prompt will indicate first part of the hostname. Use the hostname command to check the hostname

```
# hostname
```



```
[root@gm52 /]# hostname
gm52.secomea.com
[root@gm52 /]#
```

Refer to the STEP1 guide to install the GateManager.

5. Adjusting locales on Linux

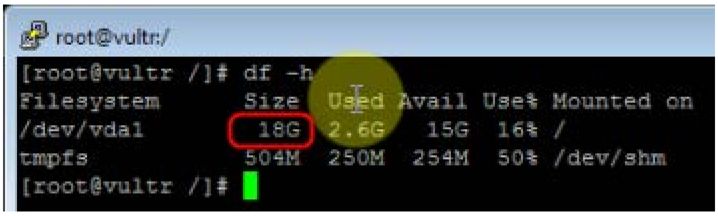
To make sure the date and time is correct, make sure the right locales are set in the Linux. On a CentOS and Debian installation, you can do the following:

1. Remove current localtime file (backup first):
   # mv /etc/localtime /etc/localtime.bck
2. Create a symbolic link from the correct localtime file:
   # ln -s /usr/share/zoneinfo/Europe/Berlin localtime
3. Adjust the time / date by running an NTP tool like “ntpdate”:
   # ntpdate -s pool.ntp.org

6. Check available disk space.

Ensure you have available disk space for the GateManager installation with the following command

#df –h



```
[root@vultr /]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        18G  2.6G   15G  16% /
tmpfs           504M  250M  254M  50% /dev/shm
[root@vultr /]#
```

In this case we have 18 GB storage. As GateManager requires only 10GB, you can continue with the STEP1 guide to install the GateManager

If you have less than 10GB, you should apply additional storage. Refer to Appendix A for an example.

7. Verifying sending emails

Sending emails is essential to the GateManager. It is used for sending alerts, account certificates and passwords and reports. You should make sure that the mail service is activated and working on the Linux server.

As default Linux mail services will send mails directly, but you can also configure that emails are send via an external mail server. Refer to **APPENDIX B, Using external mail server (Smarthost** setup)

GateManager sends emails by calling “sendmail” located in usr/lib (called with the -t option). If installing another mail program than Sendmail, such as Postfix or Exim, these will typically ensure redirection of the sendmail request to the proper service.

Check if the Sendmail service is running.

# service sendmail status

Or if using e.g. Postfix, check

```
# service postfix status
```

If no email service is installed, you can install by the command.

```
# yum install postfix
```

A quick test of the mail service is operational can be made by the following command:

```
# echo "My test email" | /usr/sbin/sendmail myemail@domain.com
```

If the mail seems be sent alright, but does not arrive, it may be because of other settings in the environment or on the Linux server blocking it, or it could be that the test mail has been blocked by a spam filter. It may be that genuine GateManager emails will not be blocked, but you should be alert about it.

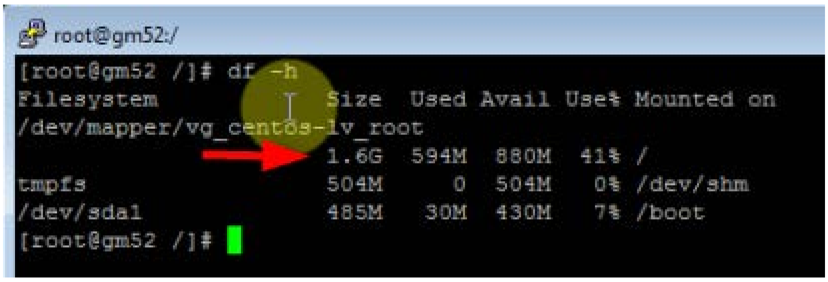
APPENDIX A, Mounting additional storage disk

In case of a VPS image, you may need to apply additional storage to the installation. In some cases, a VPS is provided with a Primary disk with the Linux OS and an additional disk for storage. It is common that the storage disk is not mounted by default. Follow these steps if you have this situation.

Check disk space with the command:

#df –h

In this example we see the primary disk to be 1.6GB



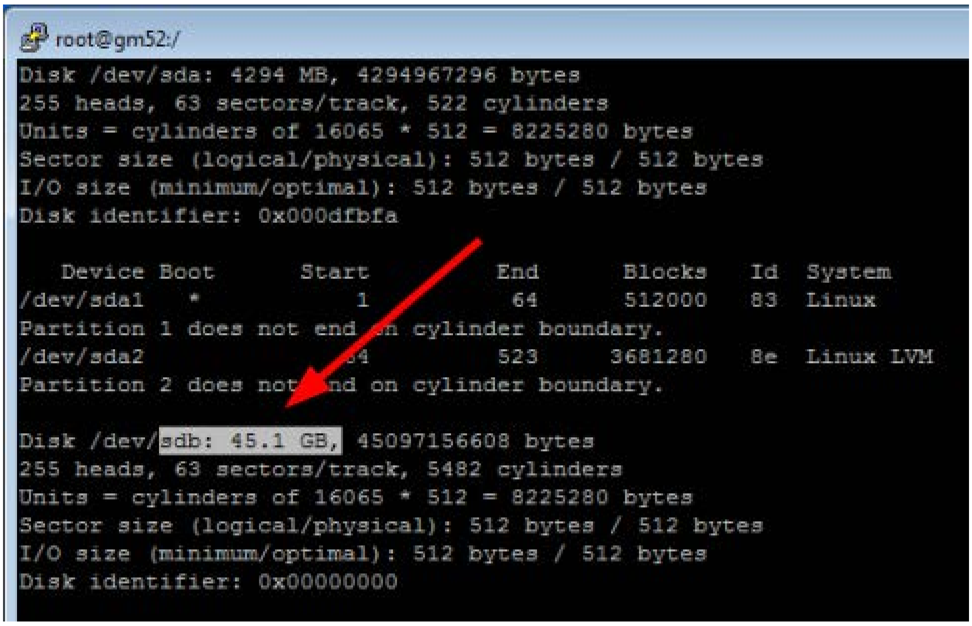
```
[root@gm52 /]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_centos-lv_root
                      1.6G  594M  880M  41% /
tmpfs                 504M     0  504M   0% /dev/shm
/dev/sda1             485M   30M  430M   7% /boot
[root@gm52 /]#
```

This is insufficient. The GateManager would need minimum 10GB disk.

Use fdisk to verify available storage

#fdisk -l

In this case we find a storage disk of 45GB

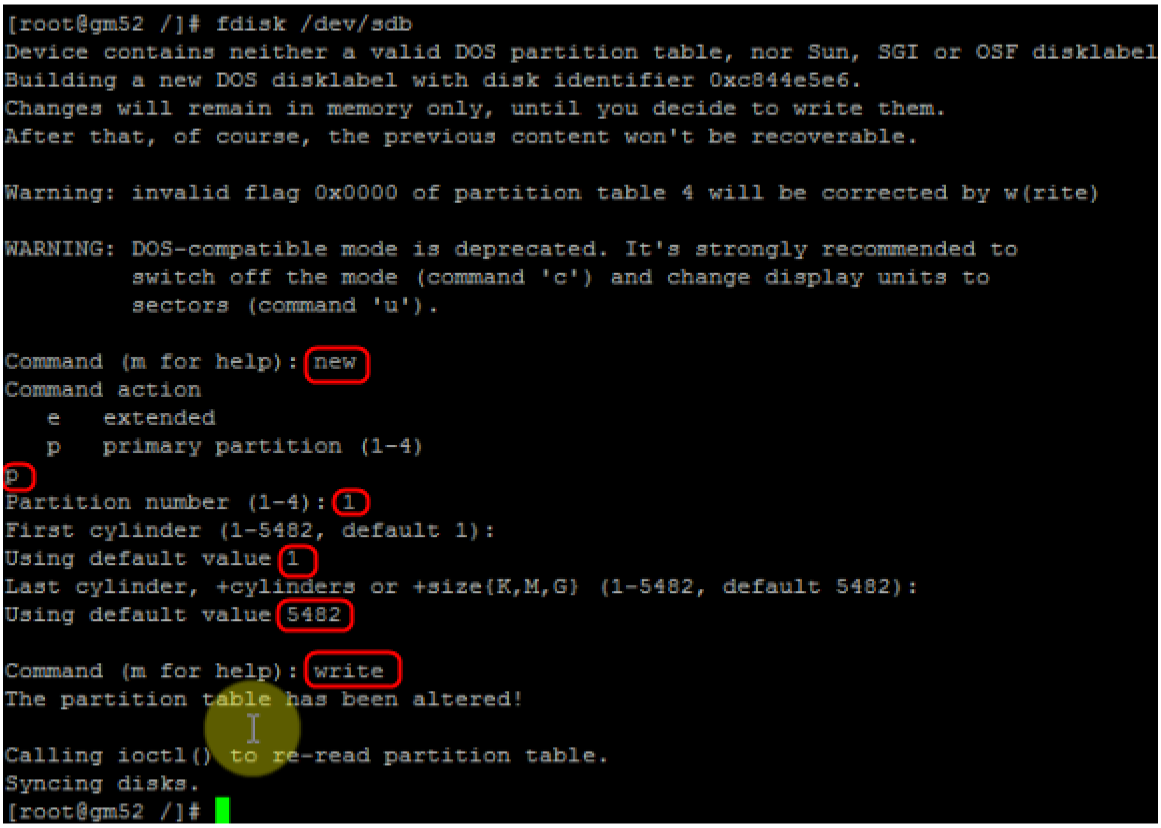


```
Disk /dev/sda: 4294 MB, 4294967296 bytes
255 heads, 63 sectors/track, 522 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000dfbfa

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          64      512000   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2              64         523     3681280   8e  Linux LVM
Partition 2 does not end on cylinder boundary.

Disk /dev/sdb: 45.1 GB, 45097156608 bytes
255 heads, 63 sectors/track, 5482 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

We want to allocate from this:

#fdisk /dev/sdb

Define the new partition



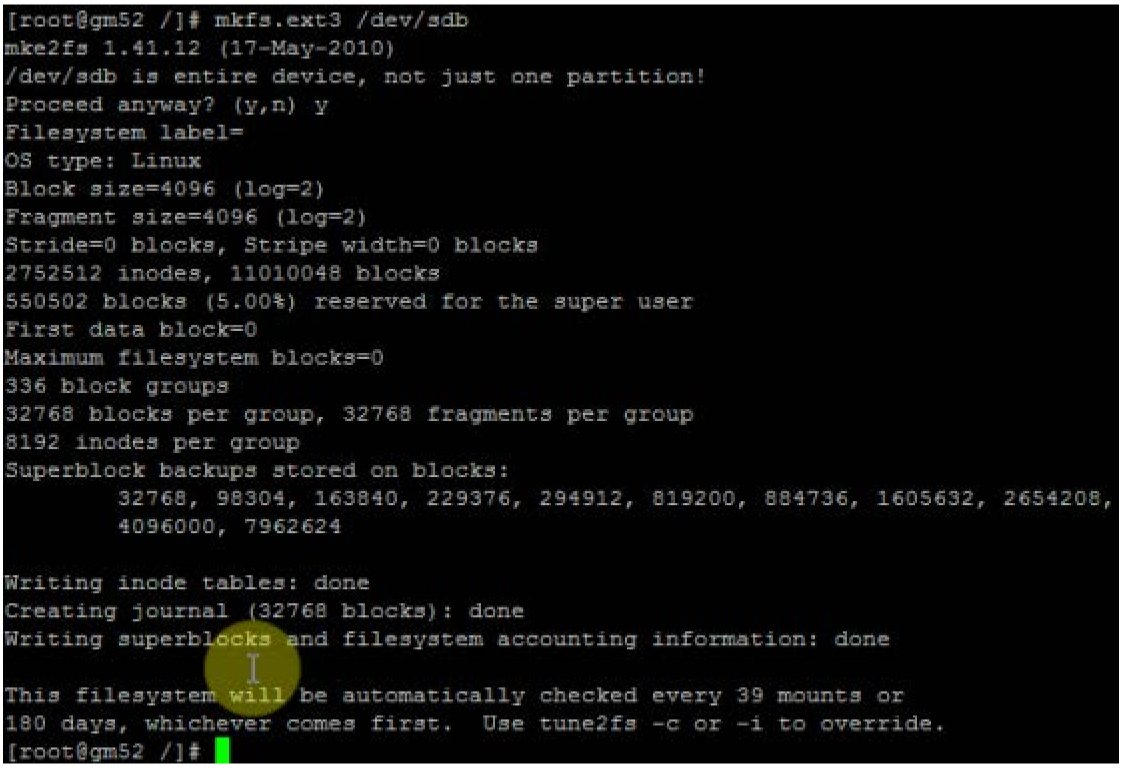
```
[root@gm52 /]# fdisk /dev/sdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xc844e5e6.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

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

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): new
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-5482, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-5482, default 5482):
Using default value 5482

Command (m for help): write
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@gm52 /]#
```

If you only want to allocate 10 GByte of the 45 GByte disk, then instead of using the default value (in this case 5482) just type the ‘last cylinder: +10GB’ – this will reduce the disk size and less backup storage may be needed.

Type

```
# mkfs.ext3 /dev/sdb
```

Type yes to proceed, and wait for the process to finalize



```
[root@gm52 /]# mkfs.ext3 /dev/sdb
mke2fs 1.41.12 (17-May-2010)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
2752512 inodes, 11010048 blocks
550502 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=0
336 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 39 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
[root@gm52 /]#
```

Make a folder for the GateManager installation.

```
# mkdir /usr/local/gatemanager
```

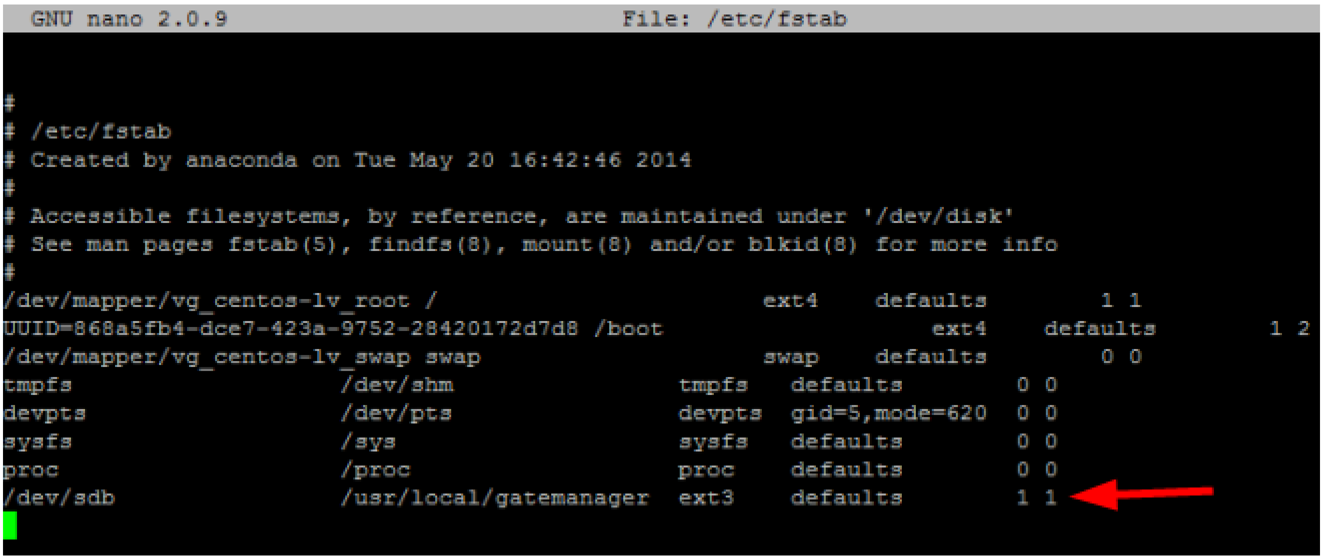
NOTE: it is important to use this exact path for the GateManager installation

Add the new map to the file system, by editing the fstab file:

```
# nano /etc/fstab
```

Add the following line:

```
/dev/vdb   /usr/local/gatemanager  ext3   defaults   1 1
```



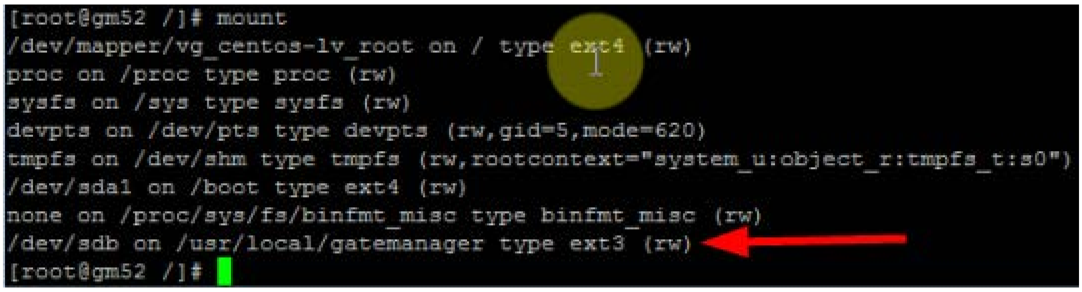
```
  GNU nano 2.0.9                          File: /etc/fstab


#
# /etc/fstab
# Created by anaconda on Tue May 20 16:42:46 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/vg_centos-lv_root /                       ext4    defaults        1 1
UUID=868a5fb4-dce7-423a-9752-28420172d7d8 /boot                   ext4    defaults        1 2
/dev/mapper/vg_centos-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
/dev/sdb                /usr/local/gatemanager  ext3    defaults        1 1
```

Save and Mount the disk

```
# mount -a
```

Check the result by typing:

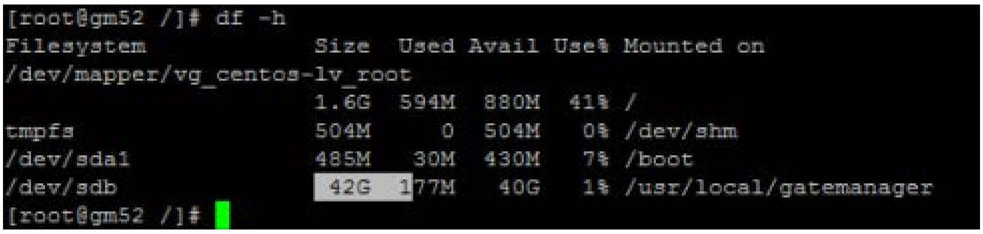
```
# mount
```



```
[root@gm52 /]# mount
/dev/mapper/vg_centos-lv_root on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext4 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
/dev/sdb on /usr/local/gatemanager type ext3 (rw)
[root@gm52 /]#
```

Verify the available storage disk for GateManager installation

```
# df -h
```



```
[root@gm52 /]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_centos-lv_root
                      1.6G  594M  880M  41% /
tmpfs                 504M     0  504M   0% /dev/shm
/dev/sda1             485M   30M  430M   7% /boot
/dev/sdb               42G  177M   40G   1% /usr/local/gatemanager
[root@gm52 /]#
```

APPENDIX B, Using external mail server (Smarthost setup)

GateManager sends emails by calling “sendmail” located in usr/lib (called with the -t option)

You may, due to corporate policy, security reasons or in order to prevent potential spam blocking of GateManager generated email, want to use an external mail server (aka ”smarthost”, which is a mail relay specialized to deal with outbound e-mail)

External mail server is optional, as the GateManager’s sendmail request can be managed on the Linux server.

The following is one method for setting up the Linux mail settings to use an external mail server. The following is exemplified using Postfix as mail service, which we have experience of providing better results than e.g. Sendmail.

Check that Postfix is installed and running:

```
# service postfix status
```

This should show .. master is running….

If this is not the case, you can install it with this command:

```
# yum install postfix
```

Follow the instructions on the screen.

In case another mail service is running, such as Sendmail, then we recommend that you remove that service before installing postfix like:

```
# yum erase sendmail
```

Follow the instructions on the screen.

Configure the external mail relay server, by adding the following line to the cf file /etc/postfix/main.cf

```
relayhost = [smtp.yourserver.com]
```

Restart the postfix service

```
# service postfix restart
```

If your mail server is not using the default port 25 but for example port 587, then apply the portnumber to the entry:

```
relayhost = [smtp.yourserver.com]:587
```

If the mail server requires credentials, you can specify login and password as follows. Edit the following file:

```
# nano /etc/postfix/relay_passwd
```

And dd the line:

```
smtp.yourserver.com USERNAME:PASSWORD
```

Set the permissions for the file:

```
# chown root:root /etc/postfix/relay_passwd
# chmod 600 /etc/postfix/relay_passwd
```

Create hash from the password file:

```
# postmap /etc/postfix/relay_passwd
```

(note: run this command every time passwd file is changed)

The following needs to be added to the main.cf file:

```
# nano /etc/postfix/main.cf
  smtp_sasl_auth_enable = yes
  smtp_sasl_password_maps = hash:/etc/postfix/relay_passwd
  smtp_sasl_security_options =
  relayhost = [smtp.yourserver.com]:587
```

Restart the service to activate changes:

```
# service postfix restart
```

Test the result:

```
# echo "GMTestmail" | mail -s "Test GM" mail email@domain
```

When you have verified that it is working you should delete the password text file:

```
# rm /etc/postfix/relay_passwd
```

If your mail relay server requires TLS1 encryption, e.g. if usingsmtp.gmail.com, you should specify this:

```
# nano /etc/postfix/main.cf
  smtp_sasl_auth_enable = yes
  smtp_sasl_password_maps = hash:/etc/postfix/relay_passwd
  smtp_sasl_security_options = noanonymous
  # Secure channel TLS with exact nexthop name match.
  smtp_tls_security_level = secure
  smtp_tls_mandatory_protocols = TLSv1
  smtp_tls_mandatory_ciphers = high
  smtp_tls_secure_cert_match = nexthop
  smtp_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt
  relayhost = [smtp.gmail.com]:587
```

Restart the service to activate changes:

```
# service postfix restart
```

If you need a backup mail relay server, you can apply this to the main.cf file

The following example adds 172.16.114.12 as primary relay server and smtp.backupSRV.com as backup server:

```
# nano /etc/postfix/main.cf
  relayhost = [172.16.114.12]:25
  smtp_fallback_relay = [smtp.backupSRV.com]:587
```

Restart the service to activate changes

```
# service postfix restart
```

Nice to know about postfix:

```
# service postfix flush      - to clear any hanging mails in the queue.
# mailq                      - show mails in the queue
# tail –f /var/log/maillog   - show the mail log.
# chkconfig postfix on       - make postfix start automatically after
                               a reboot (default on)
# mail user@domain.com       - test the mail system from command line.
```

Notices

Publication and copyright

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. The combined body of work that constitutes CentOS™ is a collective work which has been organized by the CentOS™ Project, and the CentOS Project holds the copyright in that collective work; licensing is under the GPL. www.centos.org. Other trademarks are the property of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com