



# Spacewalk

Installation Guide for CentOS 6.4

## Contents

Spacewalk Overview .....	3
Spacewalk Project Architecture .....	3
System Prerequisites.....	3
Installation .....	4
Spacewalk Components.....	4
Prerequisites Install for Spacewalk server installation .....	4
Install the Spacewalk repository .....	4
Install the priority plugin for yum .....	4
Install the following required additional repositories .....	4
Edit Configuration files.....	4
Clean Repo .....	5
Installing the PostgreSQL Database for Spacewalk.....	5
Install PostgreSQL Database Server .....	5
Enable PostgreSQL and initialize.....	5
Create the SpaceWalk database and user .....	5
Setup PostgreSQL configuration files.....	5
Testing the PostgreSQL user .....	6
Installing GPG keys.....	6
Installing the Spacewalk Server .....	7
Begin the SpaceWalk server installation.....	7
Initialize SpaceWalk server .....	7
GPG Key Import.....	8
Configuring the IPTables firewall.....	8
IPTables firewall logging .....	8
IPTables firewall rules for the Spacewalk server .....	9
Creating Repositories and Channels .....	10
Create Repositories.....	10
Create Channels .....	11
Adding Repository to Channel .....	12
Adding Packages to Repository.....	13
Connecting a CentOS 6 System.....	14
Configuring the IPTables firewall.....	14

Creating a Activation Key.....	14
Installing Spacewalk Client.....	14
System Kickstart.....	16
Installing the PXE Boot Server components .....	16
Configuring Kickstart in Spacewalk .....	18

### Spacewalk Overview

Spacewalk is an open source (GPLv2) Linux systems management solution. It is the upstream community project from which the Red Hat Network Satellite product is derived. Spacewalk provides you with the following functions:

- Inventory your systems (hardware and software information)
- Install and update software on your systems
- Collect and distribute your custom software packages into manageable groups
- Provision (kickstart) your systems
- Manage and deploy configuration files to your systems
- Monitor your systems
- Provision and start/stop/configure virtual guests
- Distribute content across multiple geographical sites in an efficient manner.

Spacewalk manages software content updates for Red Hat derived distributions such as Fedora, CentOS, and Scientific Linux, within your firewall. You can stage software content through different environments, managing the deployment of updates to systems and allowing you to view at which update level any given system is at across your deployment. A clean central web interface allows viewing of systems and their software update status, and initiating update actions.

The following link provides the differences between Spacewalk and the Red Hat Network Satellite product: <http://spacewalk.redhat.com/faq.html#compare>

### Spacewalk Project Architecture

Architecture information is directly from the Spacewalk Wiki and can be found at <https://fedorahosted.org/spacewalk/wiki/Architecture>

### System Prerequisites

- Outbound open ports 80, 443, 4545 (only if you want to enable monitoring)
- Inbound open ports 80, 443, 5222 (only if you want to push actions to client machines) and 5269 (only for push actions to a Spacewalk Proxy), 69 udp if you want to use tftp
- Storage for database: 250 KiB per client system + 500 KiB per channel + 230 KiB per package in channel (i.e. 1.1GiB for channel with 5000 packages)
- Storage for packages (default /var/satellite): Depends on what you're storing; Red Hat recommend 6GB per channel for their channels
- 2GB RAM minimum, 4GB recommended
- Make sure your underlying OS up-to-date.
- If you use LDAP as a central identity service and wish to pull user and group information from it, see SpacewalkWithLDAP
- Make sure your operating system is fully up-to-date.
- In the following steps we assume you have a default, vanilla installation of your operating system, without any customized setup of yum repositories, user management, security, etc.

# Installation

## Spacewalk Components

The main components we will be installing in this document are the Spacewalk server and it's Database (PostgreSQL) and the Spacewalk Client. This document does not cover the installation of the Spacewalk Proxy.

## Prerequisites Install for Spacewalk server installation

### Install the Spacewalk repository

```
# rpm -Uvh http://spacewalk.redhat.com/yum/latest/RHEL/6/x86\_64/spacewalk-repo-2.0-3.el6.noarch.rpm
```

### Install the priority plugin for yum

```
# yum install yum-plugin-priorities
```

### Install the following required additional repositories

Install jpackage Repository

```
# rpm -Uvh http://mirrors.dotsrc.org/jpackage/5.0/generic/free/RPMS/jpackage-release-5-4.jpp5.noarch.rpm
```

Install EPEL Repository

```
# rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86\_64/epel-release-6-8.noarch.rpm
```

Install Spacewalk Client Repository

```
# rpm -Uvh http://spacewalk.redhat.com/yum/2.0-client/RHEL/6/x86\_64/spacewalk-client-repo-2.0-3.el6.noarch.rpm
```

### Edit Configuration files

Edit `/etc/yum.repos.d/spacewalk.repo` and add the following lines

```
[spacewalk-latest]
name=Spacewalk-latest
baseurl=http://spacewalk.redhat.com/yum/latest/RHEL/6/x86\_64/
gpgkey=http://yum.spacewalkproject.org/RPM-GPG-KEY-spacewalk-2012
enabled=1
gpgcheck=1
priority=1
```

Change the following line in `/etc/yum.repos.d/jpackage.repo` under `[jpackage-distro]` heading

From:

```
mirrorlist=http://www.jpackage.org/mirrorlist.php?dist=redhat-el-  
$releasever&type=free&release=5.0
```

To:

```
mirrorlist=http://www.jpackage.org/mirrorlist.php?dist=redhat-el-5.0&type=free&release=5.0
```

### Clean Repo

```
# yum clean all
```

### Installing the PostgreSQL Database for Spacewalk

There are 2 database choices for installing Spacewalk, Oracle or PostgreSQL. In this document we are only showing the installation and configuration for the PostgreSQL database.

### Install PostgreSQL Database Server

```
# yum install postgresql postgresql-contrib postgresql-devel postgresql-server  
# yum install -y postgresql-server  
# yum install -y postgresql-pltcl
```

### Enable PostgreSQL and initialize

```
# chkconfig postgresql on  
# service postgresql initdb  
# service postgresql start
```

### Create the SpaceWalk database and user

```
# su - postgres -c 'PGPASSWORD=spacepw; createdb -E UTF8 spaceschema ; createlang plpgsql  
spaceschema ; createlang pltclu spaceschema ; yes $PGPASSWORD | createuser -P -sDR  
spaceuser'
```

### Setup PostgreSQL configuration files

Edit the `/var/lib/pgsql/data/pg_hba.conf` and add the following lines so it look like this:

NOTE: Make sure you put them *\*before\** those existing lines that are for all..

```
# TYPE DATABASE  USER    CIDR-ADDRESS   METHOD
# local spacewalk info
local spaceschema spaceuser md5
host spaceschema spaceuser 127.0.0.1/8 md5
host spaceschema spaceuser ::1/128 md5
local spaceschema postgres ident
```

Edit `/var/lib/pgsql/data/postgresql.conf` file. Add or edit the following line.

```
listen_addresses = 'localhost'
```

If you have a PostgreSQL server that is on a different system than the Spacewalk server you will need to change this to the IP Address of the network IP Address or IP Address of the Spacewalk server.

```
# service postgresql reload
```

### Testing the PostgreSQL user

```
# PGPASSWORD=spacepw psql -a -U spaceuser spaceschema
# PGPASSWORD=spacepw psql -h localhost -a -U spaceuser spaceschema
```

### Installing GPG keys

This section covers the installation of the necessary GPG keys that need to be installed on the system prior to the installation of Spacewalk.

```
# wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
http://www.redhat.com/security/37017186.txt
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
# wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL
http://download.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL
# wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
http://download.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-6
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
```

```
# wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-spacewalk-2012
http://spacewalk.redhat.com/yum/RPM-GPG-KEY-spacewalk-2012

# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-spacewalk

# wget -O /etc/pki/rpm-gpg/RPM-GPG-KEY-dag http://dag.wieers.com/packages/RPM-GPG-
KEY.dag.txt

# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-dag
```

### Installing the Spacewalk Server

This section will go through the installation and configuration of the Spacewalk server component.

Begin the SpaceWalk server installation

```
# yum install spacewalk-postgresql
```

Initialize SpaceWalk server

```
# spacewalk-setup --disconnected --external-db
```

**NOTE:** If you get receive a 'could not populate database' error here look in `/var/log/rhn/populate_db.log` to find the error.

- choose for local db (just enter)
- database is: spaceschema
- username is: spaceuser
- password is: spacepw
- Admin Email Address: <your email>
- Should setup configure apache's default ssl server for you: y
- CA certificate password: <some password>
- Re-enter CA certificate password: <same password>
- Organization: <Enter your Organization's name>
- Organization Unit: <Enter the system hostname>
- Email Address: <Enter your Email Address>
- City: <Enter your city>
- State: <Enter your State>
- Country code: <Enter your country's code>

Now the system will generate the SSL Certificate.

- Cobbler requires tftp and xinetd services be turned on for the PXE provisioning functionality. Enable these services: <If you are going to provision new systems answer



y, if not n. If you answer no, these service can be enabled later. This is explained later in this document.

After reboot you will have to adjust your firewall to allow access to ports 443 and 5222.

Your SpaceWalk server should now be available on: [https://\[box-ip-address or FQDN\]](https://[box-ip-address or FQDN])

At first access you'll be asked to create a new user.

### GPG Key Import

To import the GPG needed by the Spacewalk system follow the procedure below.

CentOS 6 and Spacewalk GPG Keys

```
# cd /etc/pki/rpm-gpg
```

```
# gpg --import RPM-GPG-KEY-CentOS-6
```

```
# gpg --import RPM-GPG-KEY-spacewalk-2012
```

```
# gpg --import RPM-GPG-KEY-EPEL-6
```

```
# gpg --list-keys This will get the key ID
```

```
# gpg --list-keys --fingerprint <8 digit Key ID> This will display the GPG key fingerprint for you to enter into the channel you create. You will need to perform this for both the CentOS and Spacewalk keys.
```

Record both the ID and fingerprint for both to be used later in the Channel Creation.

### Configuring the IPTables firewall

The following are the rules needed on the Spacewalk server for clients to connect to the server and also to connect to the Web interface.

#### IPTables firewall logging

If you desire to have firewall logging you can implement logging for IPTables by following these steps.

These steps will Log the rest of the incoming messages (all of which are dropped)with a maximum of 15 log entries per minute.

```
# iptables -A INPUT -m limit --limit 15/minute -j LOG --log-level 7 --log-prefix "Dropped by firewall: "
```

```
# iptables -A OUTPUT -m limit --limit 15/minute -j LOG --log-level 7 --log-prefix "Dropped by firewall: "
```

Reject any packets that do not meet the specified criteria

```
# iptables -A INPUT -p tcp -j REJECT --reject-with tcp-reset
```

```
# iptables -A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
```

Save the changes that you have made.

```
# service iptables save
# service iptables restart
```

Edit the rsyslog.conf file to send messages to the /etc/firewall.log file

```
# vi /etc/rsyslog.conf
```

```
Uncomment out or add this line to send logging to the firewall.log file
kern.debug          /var/log/firewall.log
```

Edit the Logrotate for the firewall log so that you do not get one big firewall logfile.

```
# vi /etc/logrotate.d/syslog
```

```
/var/log/firewall.log  # add to the list of the log names and save file
```

```
# service rsyslog restart
```

### IPtables firewall rules for the Spacewalk server

The follow rules are required for the Spacewalk server to function normally with the IPtables firewall enabled.

- Outbound open ports 80, 443, 4545 (only if you want to enable monitoring)
- Inbound open ports 80, 443, 5222 (only if you want to push actions to client machines) and 5269 (only for push actions to a Spacewalk Proxy), 69 udp if you want to use tftp

```
# iptables -I INPUT <Line #> -p tcp -s 0/0 --sport 1024:65535 -d <SPACEWALK-SERVER-IP> --dport 80 -
m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I INPUT <Line #> -p tcp -s 0/0 --sport 1024:65535 -d <SPACEWALK-SERVER-IP> --dport 443
-m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I INPUT <Line #> -p tcp -s 0/0 --sport 1024:65535 -d <SPACEWALK-SERVER-IP> --dport
5222 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I INPUT <Line #> -p tcp -s <SPACEWALK-SERVER-IP> --sport 5222 -d <CLIENT-IP> --dport
1024:65535 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I OUTPUT <Line #> -p tcp -s <SPACEWALK-SERVER-IP> --sport 80 -d 0/0 --dport
1024:65535 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I OUTPUT <Line #> -p tcp -s <SPACEWALK-SERVER-IP> --sport 443 -d 0/0 --dport
1024:65535 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# iptables -I OUPUT <Line #> -p tcp -s <CLIENT-IP> --sport 1024:65535 -d <SPACEWALK-SERVER-IP> --dport 5222 -m state --state ESTABLISHED -j ACCEPT
```

```
# iptables -I OUPUT <Line #> -p tcp -s <CLIENT-IP> --sport 1024:65535 -d <SPACEWALK-SERVER-IP> --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Postgresql Database Server when running local DB for Spacewalk.

```
# iptables -I INPUT 5 -p tcp -s 127.0.0.1 --sport 1024:65535 -d 127.0.0.1 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCPEPT
```

```
# iptables -I INPUT 5 -p tcp -s 127.0.0.1 --sport 5432 -d 127.0.0.1 --dport 1024:65535 -m state --state NEW,ESTABLISHED -j ACCPEPT
```

### Creating Repositories and Channels

In this section will create a basic repository and Channel for CentOS. The repositories and Channel you create will depend on the systems that you are supporting.

#### Create Repositories

Click on **Channels**

Click on **Manage Software Channels**

Click on **Manage Repositories**

Click on **Create New Repository**

CentOS 6.4 x86\_64

Repository Label - **CentOS6.4-x86\_64-Base**

Repository URL - [http://mirror.centos.org/centos/6.4/os/x86\\_64/](http://mirror.centos.org/centos/6.4/os/x86_64/)

Then click on **Create Repository**

Repository Label - **CentOS6.4-x86\_64-Updates**

Repository URL - [http://mirror.centos.org/centos/6.4/updates/x86\\_64/](http://mirror.centos.org/centos/6.4/updates/x86_64/)

Then click on **Create Repository**

Repository Label - **spacewalk-client-rhel6-x86\_64**

Repository URL - [http://spacewalk.redhat.com/yum/2.0/RHEL/6/x86\\_64/](http://spacewalk.redhat.com/yum/2.0/RHEL/6/x86_64/)

Then click on **Create Repository**

Repository Label – **rhn-rhel6-x86\_64**

Repository URL - [http://spacewalk.redhat.com/yum/latest-client/RHEL/6/x86\\_64/](http://spacewalk.redhat.com/yum/latest-client/RHEL/6/x86_64/)

Then click on **Create Repository**

Repository Label - **EPEL**

Repository URL – [http://dl.fedoraproject.org/pub/epel/6/x86\\_64/](http://dl.fedoraproject.org/pub/epel/6/x86_64/)

Then click on **Create Repository**

## Create Channels

Click on **Channels**  
Click on **Manage Software Channels**  
Click on **Create New Channel**

Channel Name - **CentOS 6.4 x86\_64 Base**  
Channel Label - **centos-6.4-x86\_64-base**  
Parent Channel - **none**  
Parent Channel Architecture - **x86\_64**  
Yum Repository Checksum Type - **sha256**  
Channel Summary - **CentOS 6.4 Base Software Channel**  
Under Channel Access Control Select:  
All users within your organization may subscribe to this channel.  
This channel is public and may be accessed by any of the trusted organizations trusted by this organization.  
GPG key URL - <http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-6>  
GPG key ID - Recorded from above  
GPG key Fingerprint - Recorded from above  
Click on **Create Channel**

Assign Repository  
Click **Repositories**  
Assign both **CentOS6.4-x86\_64-Base** and **CentOS6.4-x86\_64-Updates**  
Click **Update Repositories**

Click on **Channels**  
Click on **Manage Software Channels**  
Click on **Create New Channel**

Channel Name - **Spacewalk Client 2.0 64bit RHEL6**  
Channel Label - **spacewalk-client-2.0-rhel6-x86\_64**  
Parent Channel - **CentOS 6.4 x86\_64 Base**  
Parent Channel Architecture - **x86\_64**  
Yum Repository Checksum Type - **sha256**  
Channel Summary - **Spacewalk Client 64bit for RHEL6**  
Under Channel Access Control Select:  
All users within your organization may subscribe to this channel.  
This channel is public and may be accessed by any of the trusted organizations trusted by this organization.  
GPG key URL - <http://spacewalk.redhat.com/yum/RPM-GPG-KEY-spacewalk-2012>  
GPG key ID - Recorded from above  
GPG key Fingerprint - Recorded from above  
Assign the repository spacewalk-client-rhel6-x86\_64 to the channel and set a sync schedule

Click on **Channels**  
Click on **Manage Software Channels**  
Click on **Create New Channel**

Channel Name – **EPEL RHEL 6 x86\_64**  
Channel Label – **epel\_rhel-6-x86\_64**  
Parent Channel - **CentOS 6.4 x86\_64 Base**  
Parent Channel Architecture - **x86\_64**  
Yum Repository Checksum Type - **sha256**  
Channel Summary – **EPEL RHEL 6 x86\_64**  
Under Channel Access Control Select:  
All users within your organization may subscribe to this channel.  
This channel is public and may be accessed by any of the trusted organizations trusted by this organization.  
GPG key URL - <http://download.fedoraproject.org/pub/epel/RPM-GPG-KEY-EPEL-6>  
GPG key ID - Recorded from above  
GPG key Fingerprint - Recorded from above  
Assign the repository spacewalk-client-rhel6-x86\_64 to the channel and set a sync schedule

Click on **Channels**  
Click on **Manage Software Channels**  
Click on **Create New Channel**

Channel Name – **RHN RHEL 6 x86\_64**  
Channel Label – **rhn-rhel-6-x86\_64**  
Parent Channel - **CentOS 6.4 x86\_64 Base**  
Parent Channel Architecture - **x86\_64**  
Yum Repository Checksum Type - **sha256**  
Channel Summary – **RHN RHEL 6 x86\_64**  
Under Channel Access Control Select:  
All users within your organization may subscribe to this channel.  
This channel is public and may be accessed by any of the trusted organizations trusted by this organization.  
GPG key URL - <http://spacewalk.redhat.com/yum/RPM-GPG-KEY-spacewalk-2012>  
GPG key ID - Recorded from above  
GPG key Fingerprint - Recorded from above  
Assign the repository spacewalk-client-rhel6-x86\_64 to the channel and set a sync schedule

### Adding Repository to Channel

Below is the procedure for adding a Repository to a given channel. Once this is complete and the Repository has sync'd you can proceed to Adding Packages to your Repository.

Click on **Channels**

Click on **Manage Software Channels**

Click on the Channel that you want to add a Repository.

Click on **Repositories**

Select your Repository that you want to add

Click on **Update Repositories**

Click on **Sync Now** to retrieve package from the repo

To update your Repo on a scheduled basis you will need to setup a schedule for the repo. At the bottom of the **Repository → Sync** page you would select the schedule that you would like to have the Update Repo run at, then click on the **Schedule** button.

### Adding Packages to Repository

To add packages to a giving repository you will need to sync with URL you provided for the repository. Once this has completed then you will be able to select all or some of the packages download to add to your repository.

Click on **Channels**

Click on **Manage Software Channels**

Click on the Channel that you want to add a Repository.

Click on **Packages**

Click on **Add Packages**

Select the Packages that you would like to add to the Repository and then click on **Confirm Addition**

## Connecting a CentOS 6 System

### Configuring the IPtables firewall

```
# iptables -I INPUT <Line #> -p tcp -s <SPACEWALK-SERVER-IP> --sport 5222 -d <CLIENT-IP> --  
dport 1024:65535 -m state --state NEW,ESTABLISHED -j ACCEPT  
  
# iptables -I OUPUT <Line #> -p tcp -s <CLIENT-IP> --sport 1024:65535 -d <SPACEWALK-SERVER-  
IP> --dport 5222 -m state --state ESTABLISHED -j ACCEPT  
  
# iptables -I OUPUT <Line #> -p tcp -s <CLIENT-IP> --sport 1024:65535 -d <SPACEWALK-SERVER-  
IP> --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

### Creating a Activation Key

Before connecting to a CentOS 6 System you need to create an activation key to use for registering the systems and assign a software channel to it. To create an Activation Key we do the following:

- Click on **Systems**
- Click on **Activation Keys**
- Click on **Create New Key**
- Enter the Following Information
- Description – **centosver64systems**
- key system generated
- Base Channels – **Spacewalk Default**  
Add-On Entitlements - Select Monitoring and Provisioning (You can also choose the Virtualization Entitlements if you wish to use them)
- Click on **Create Activation Key**

The key is now ready to use in the Client installation below.

### Installing Spacewalk Client

This section will cover the installation of the Spacewalk client.

```
# rpm -Uvh http://spacewalk.redhat.com/yum/2.0/RHEL/6/x86\_64/spacewalk-client-repo-2.0-3.el6.noarch.rpm  
  
# BASEARCH=$(uname -i)  
  
# rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/\$BASEARCH/epel-release-6-8.noarch.rpm  
  
# yum install rhn-client-tools rhn-check rhn-setup rhnsd m2crypto yum-rhn-plugin
```

Register your CentOS or Red Hat Enterprise Linux system to Spacewalk using the activation key you created earlier

```
# rhnreg_ks --serverUrl=http://YourSpacewalk.example.org/XMLRPC --activationkey=<key-with-rhel-custom-channel>
```

rhnreg\_ks is used for registration of clients to Spacewalk. If you need to re-register a client to your Spacewalk server or change registration from one environment or server to another Spacewalk server then use the “--force” flag with rhnreg\_ks, otherwise there is no need to use “--force”.

Install packages to enable Configuration File Management

```
# yum -y install osad rhncfg rhncfg-actions rhncfg-client rhncfg-managemen
```

Install the Spacewalk Organization Cert on the Client

```
# wget -O /usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT http://<Insert FQDN for your Spacewalk Server>/pub/RHN-ORG-TRUSTED-SSL-CERT
```

Allow remote actions:

```
# rhn-actions-control --enable-all
# rhn-actions-control --report
  deploy is enabled
  diff is enabled
  upload is enabled
  mtime_upload is enabled
```

Start osad service so that remote actions are executed quickly rather than waiting for the systems to check in:

```
# service osad start
# chkconfig osad on
```



## System Kickstart

In this section we will go over the installation of the components required for Kickstart booting and installation of new systems. Once the procedures in this section have been complete you should be able to Kickstart a system via the PXE Boot method.

### Installing the PXE Boot Server components

In this section we will go over the installation of the services required to support the PXE boot and installation of a new Linux system. This installation will support both the installation of physical or virtual systems.

NOTE: The following service can be installed on any server. For this document we are going to be installing these services on the Spacewalk Server.

1. Install the necessary supporting services.

```
# yum install tftp dhcp syslinux
```

2. Create directories to support the PXE boot

```
# mkdir /var/lib/tftpboot/pxelinux.cfg  
# mkdir /var/lib/tftpboot/centos-x86_64-6.4
```

3. Locate the pxelinux.0 on the server and copy to the tftpboot directory

```
# rpm -ql syslinux | grep pxelinux.0  
# cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/  
# cp /usr/share/menu.c32 /var/lib/tftpboot/
```

4. Create PXE configuration file for client OS

```
# vi /var/lib/tftpboot/pxelinux.cfg/default
```

```
DEFAULT menu  
PROMPT 0  
MENU TITLE Select a boot option  
TIMEOUT 200  
TOTALTIMEOUT 6000  
ONTIMEOUT local
```

```
LABEL local  
MENU LABEL (local)  
MENU DEFAULT  
LOCALBOOT 0
```

```
LABEL centos-x86_64-6.4  
kernel /centos-x86_64-6.4/vmlinuz  
MENU LABEL centos-x86_64-6.4  
append initrd=centos-x86_64-6.4/initrd.img ks=http://172.16.1.10/pxe/centos.ks  
ksdevice=link
```

MENU end

5. Setup the tftp server to start on boot

```
# /sbin/chkconfig --level 345 xinetd on
# /sbin/chkconfig --level 345 tftp on
```

6. Setup DHCP Server

Editing the dhcpd config file and enter in the Ethernet interface that you want to DHCP server to answer to clients on.

```
# vi /etc/sysconfig/dhcpd

DHCPARGS=eth0

# vi /etc/dhcp/dhcpd.conf

# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;
subnet <your-IP-Subnet> netmask <your-IP-Subnet-Mask> {
# --- default gateway
option routers          <your-IP-Gateway>;
option subnet-mask     <your-IP-Subnet-Mask>;
option domain-name     "<your-Doamin-Name>";
option domain-name-servers <your-Name-Server-IP>;
range dynamic-bootp   <start-IP-for-DHCP> <end-IPfor-DHCP>;
#time unit is 1 sec
default-lease-time 21600;
max-lease-time 43200;
next-server <IP-Address>;
filename "pxelinux.0";
```

7. Start the DHCP Server and set to start on boot

```
# service dhcpd start

# chkconfig dhcpd on
```

8. Restart your server

```
# reboot
```

### Configuring Kickstart in Spacewalk

There are two main steps in setup for the Kickstart in Spacewalk, creating the distribution tree and Kickstart Profile.

1. Creating the Distribution Tree

Create a path where you will be storing the different distributions.

```
# mkdir -p /var/distro-trees/centos-x86_64-6.4
```

2. Copy installation media with the exception of the rpm files to the directory above.
3. Create Kickstart Distribution.

Click on Systems  
Click on Kickstrat  
Click on Distributions  
Click on Create new distribution

Distribution Label: centos-6.4-x86\_64-dist  
Tree Path: /var/distro-trees/centos-x86\_64-6.4/  
Base Channel: CentOS 6.4 x86\_64 Base  
Installer Generation: Red Hat Enterprise Linux 6

Click on Create Kickstart Distribution