การติดตั้ง CentOS Linux เพื่อใช้งาน

คมกริช คำสวัสดิ์
วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

PDCA on your System.

- Plan
    - Requirements gathering
    - System design (Work flow, Diagram, Business Process)
    - Shopping (Hardware/Virtualization, Software, Network)

- Do
    - Secured installation
    - Secured dev.

- Check
    - System & Application audit (VA, PenTest)

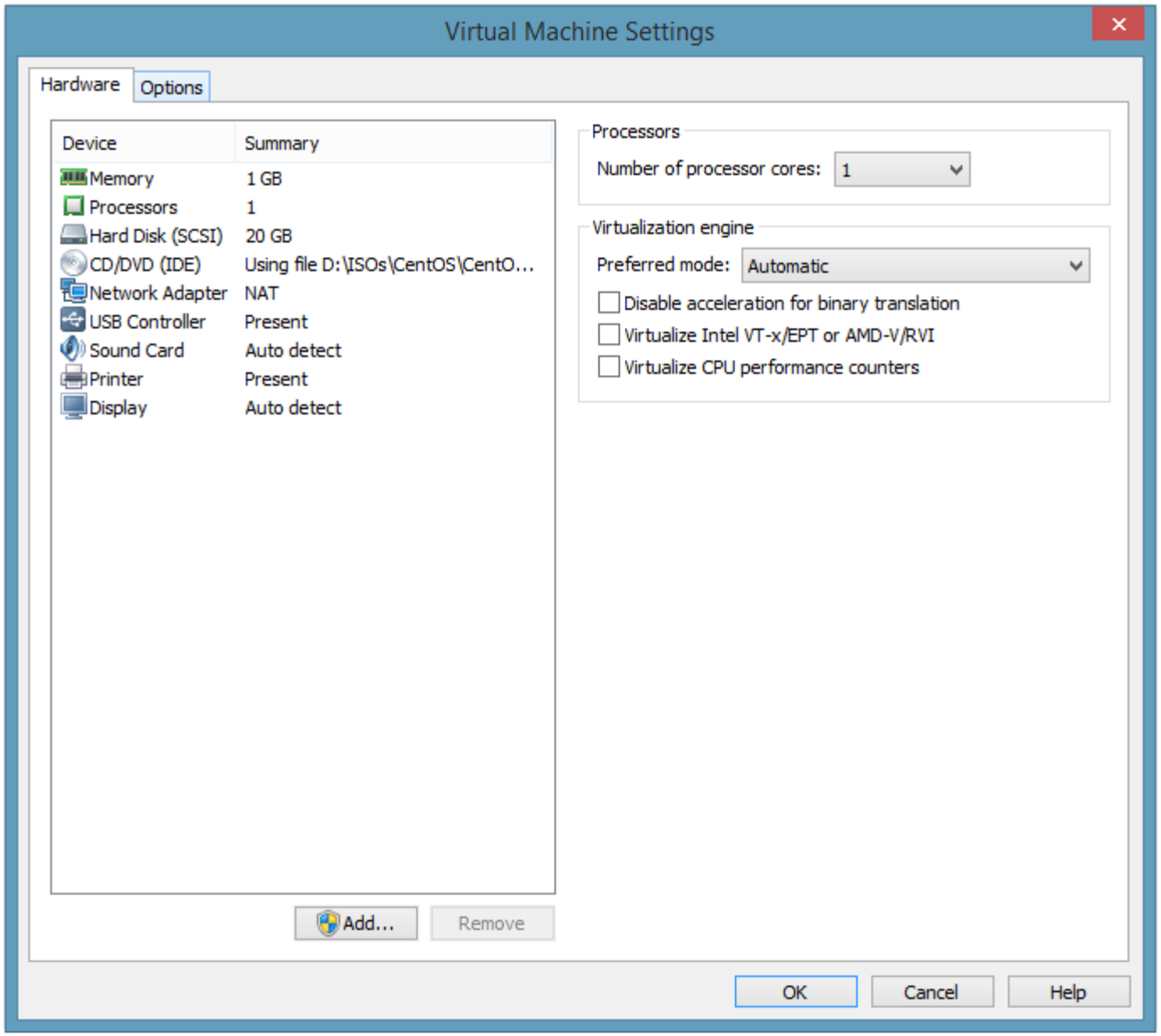
- Act
    - Hardening

Linux secured installation steps

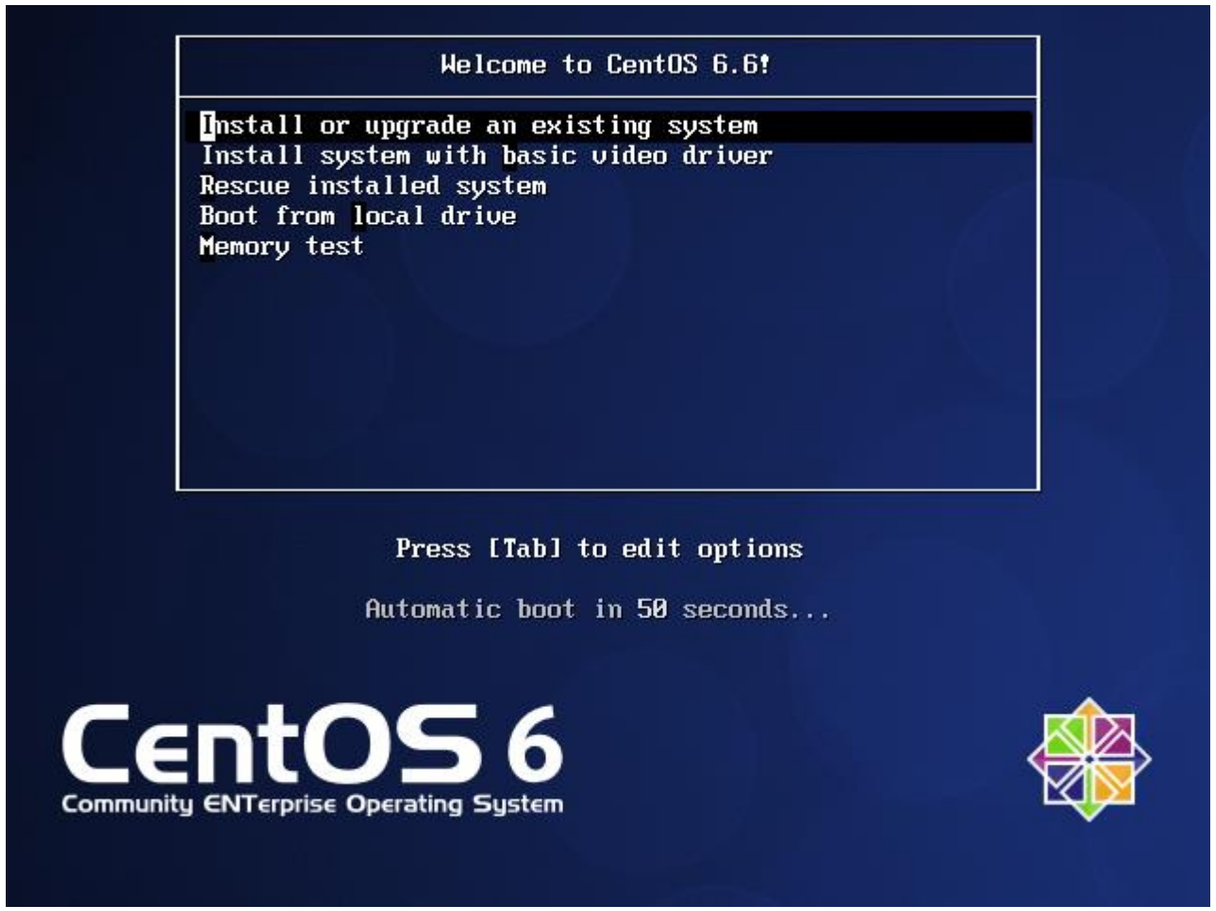
- Installation
    - Setup OS
    - Patching
    - Time sync.
    - Default services hardening (Disabled unneeded/unsecured services)
    - Secured services installation (SSH, MySQL, Apache+PHP, FTP)
    - Application installations (iTop)
- Hardening steps
    - Server management (Secure Shell: SSH)
    - Local firewall (iptables, ip6tables)
    - Logging
- System monitoring tools
- Hands-on labs

Setup a Linux server

Virtual server ที่ใช้ทดสอบ

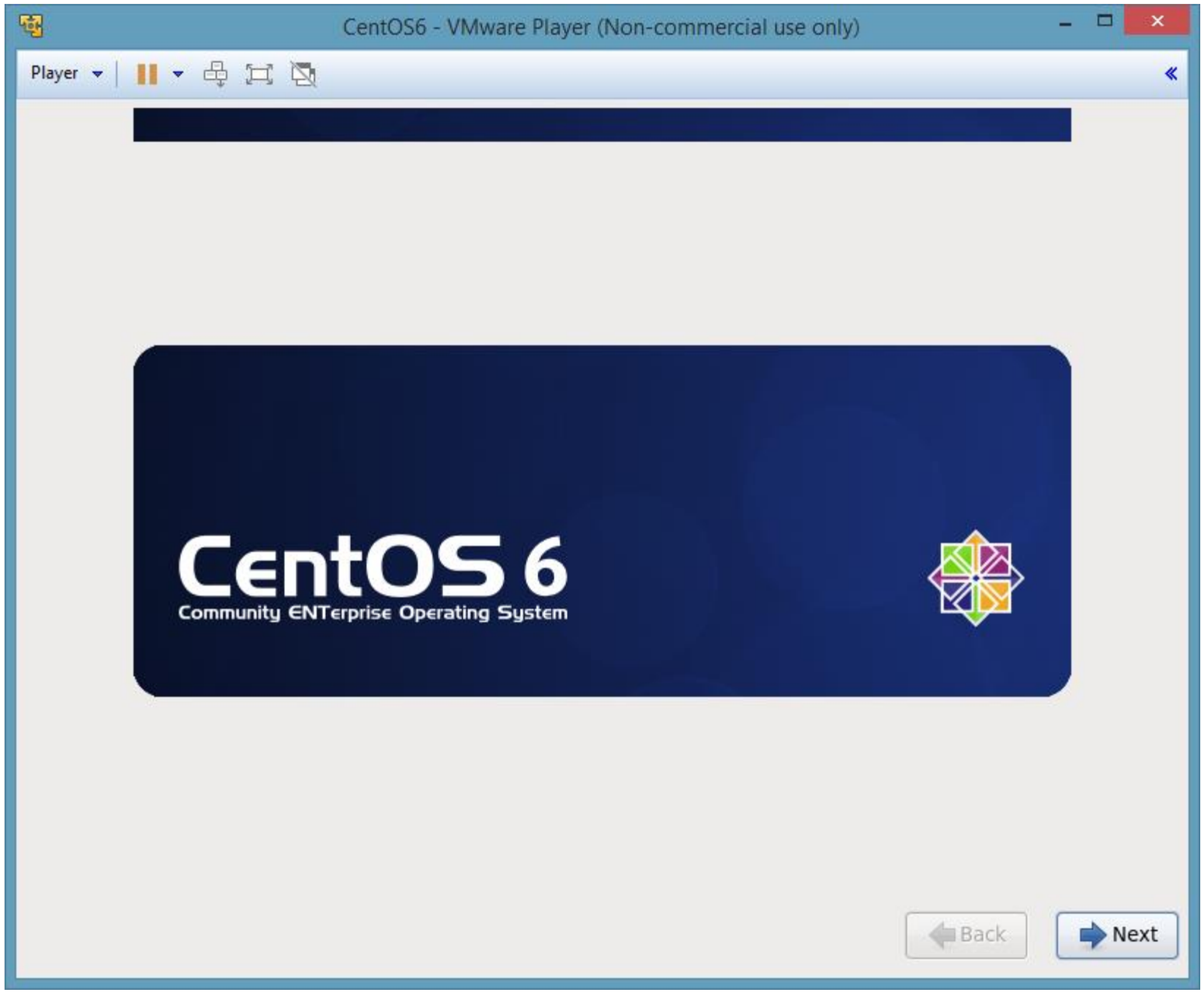


Installation

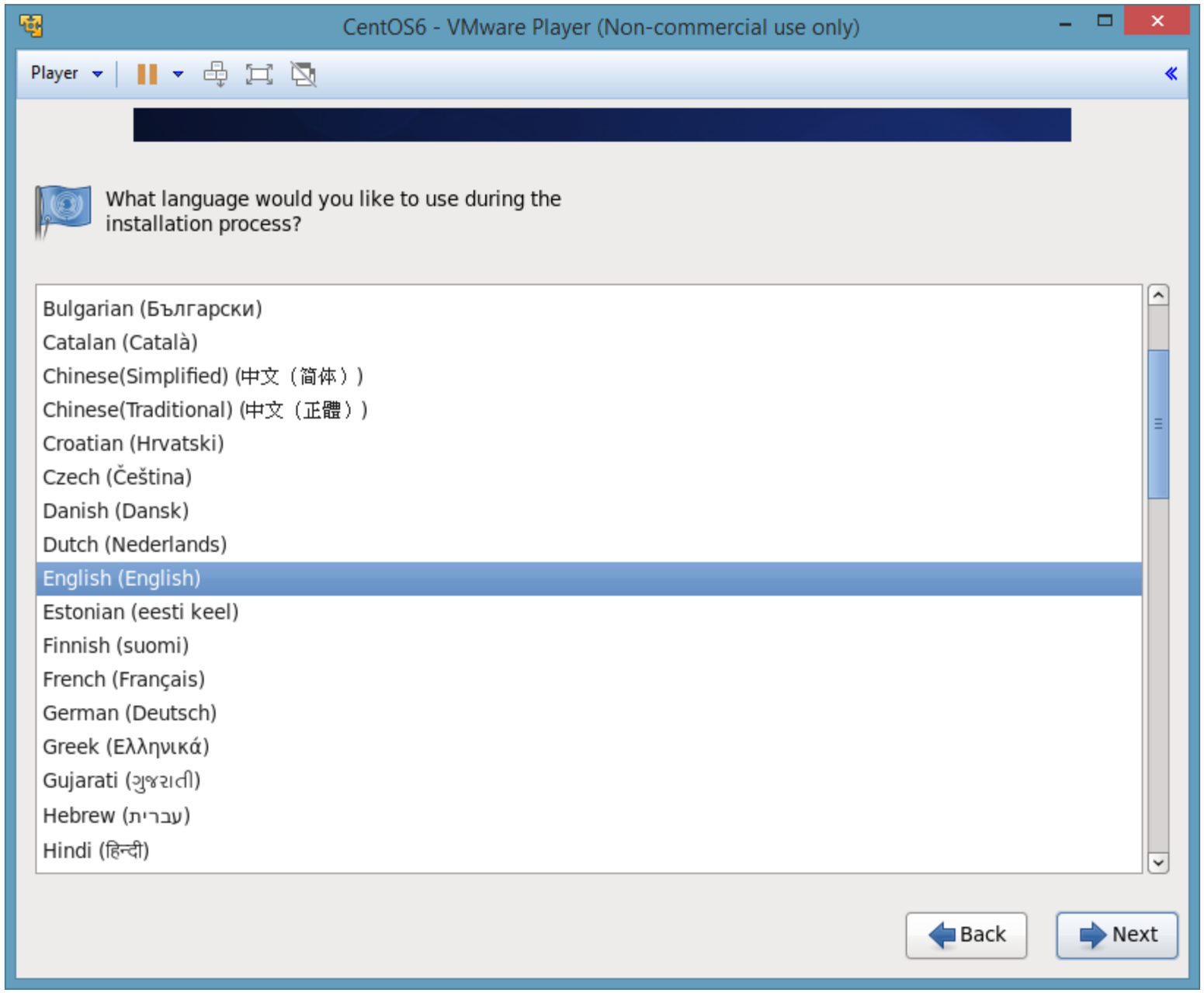


ขั้นตอนตรวจสอบ Installation media

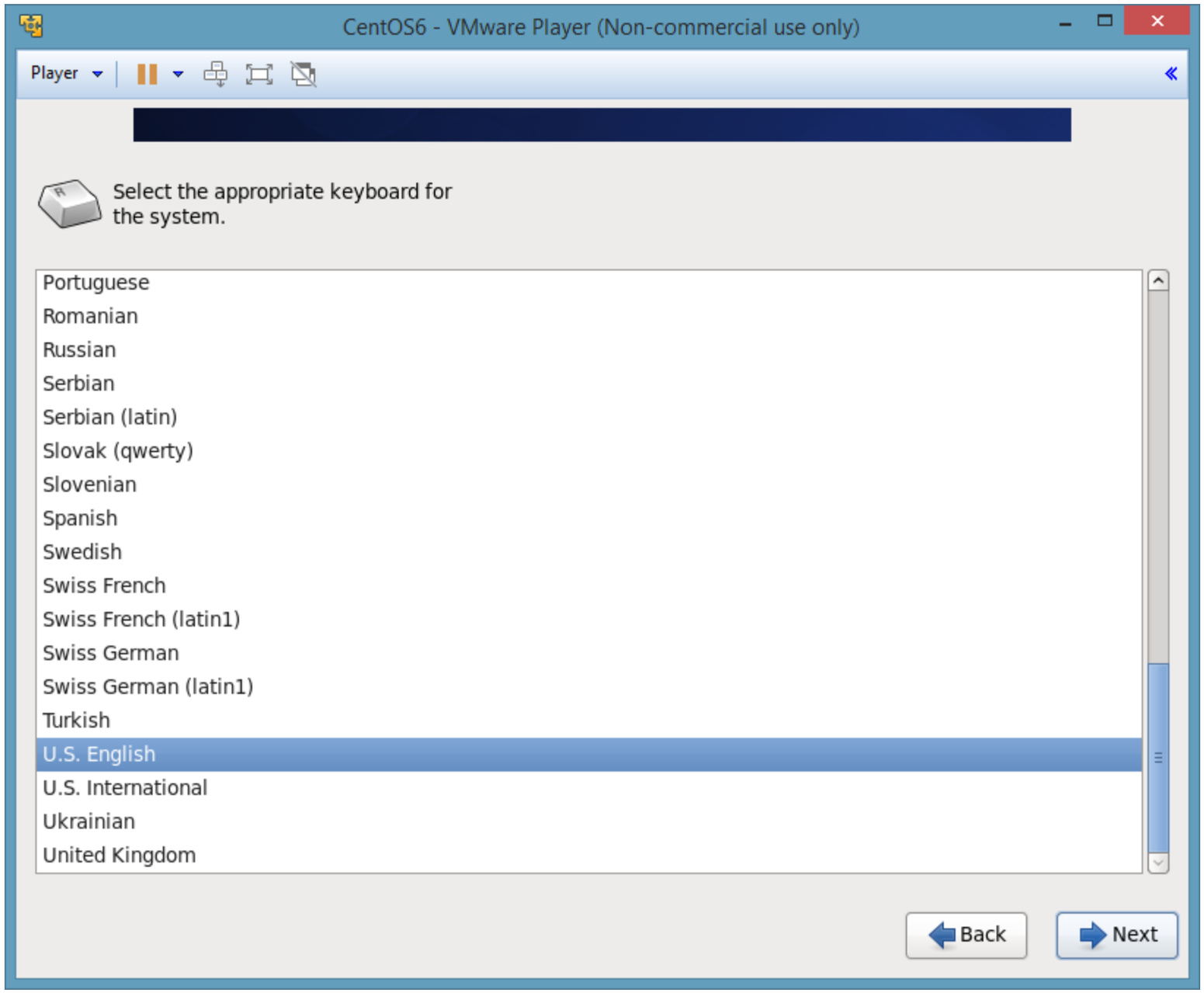
Installation



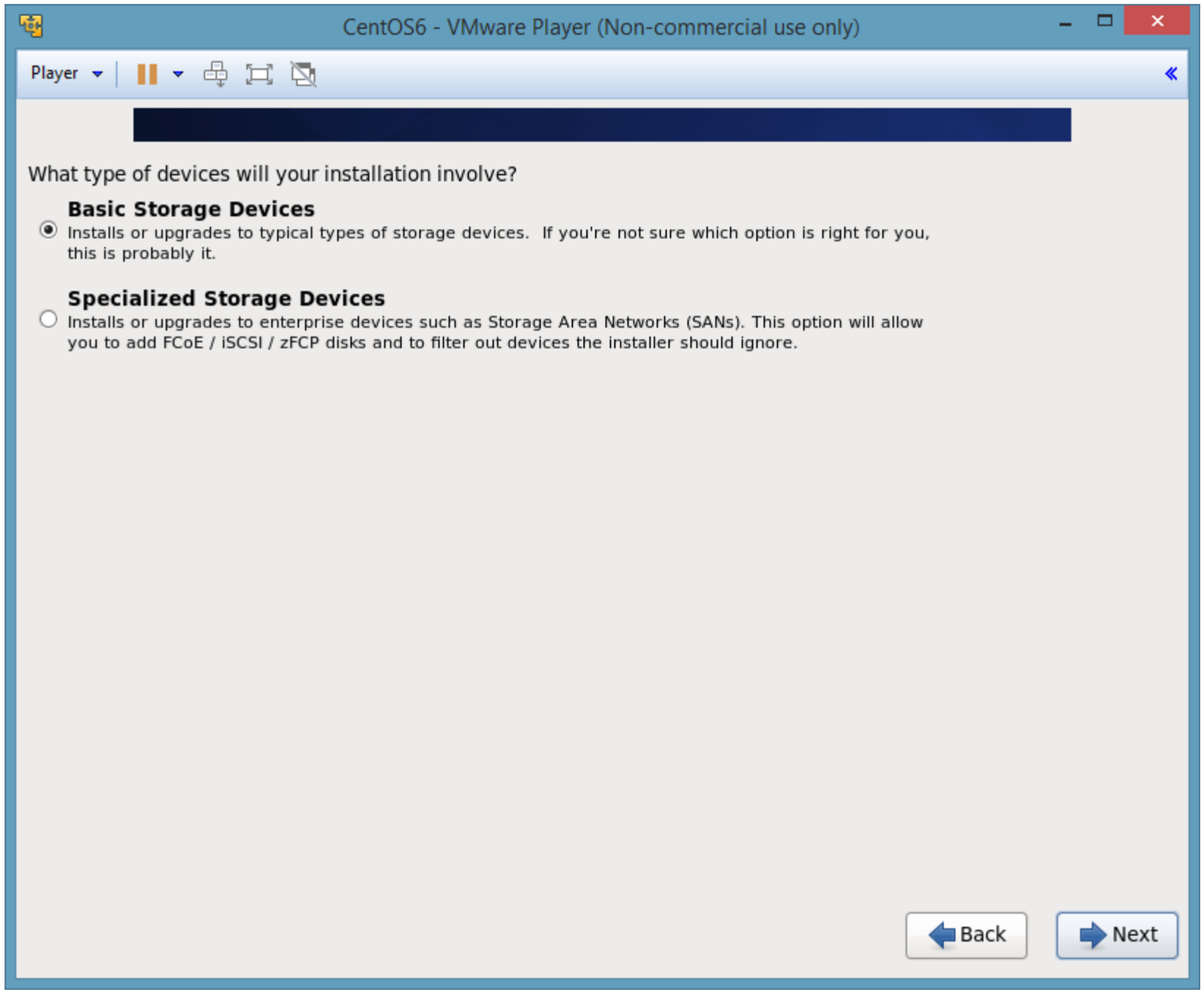
เลือกภาษาในการติดตั้ง



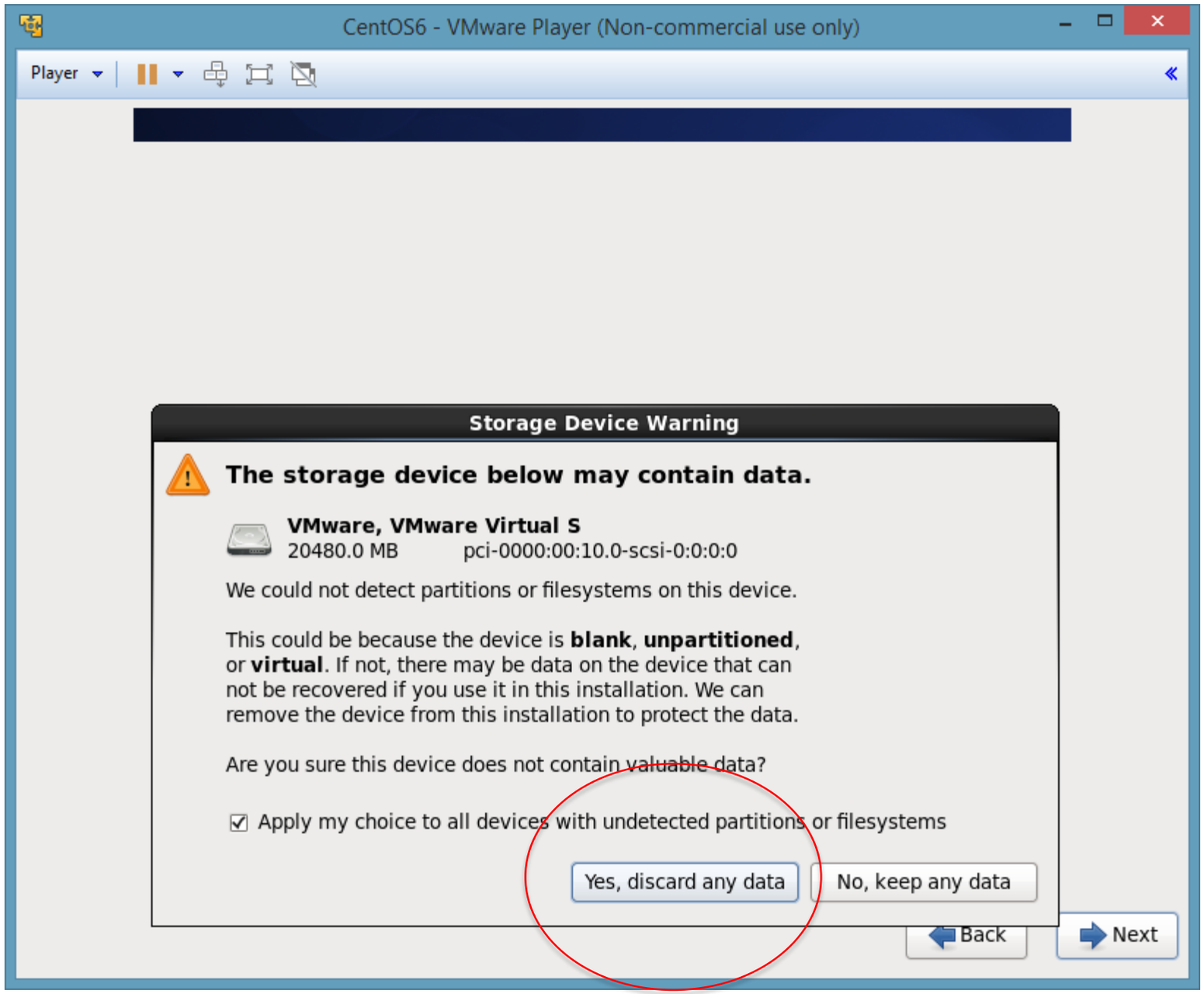
เลือกประเภท Keyboard



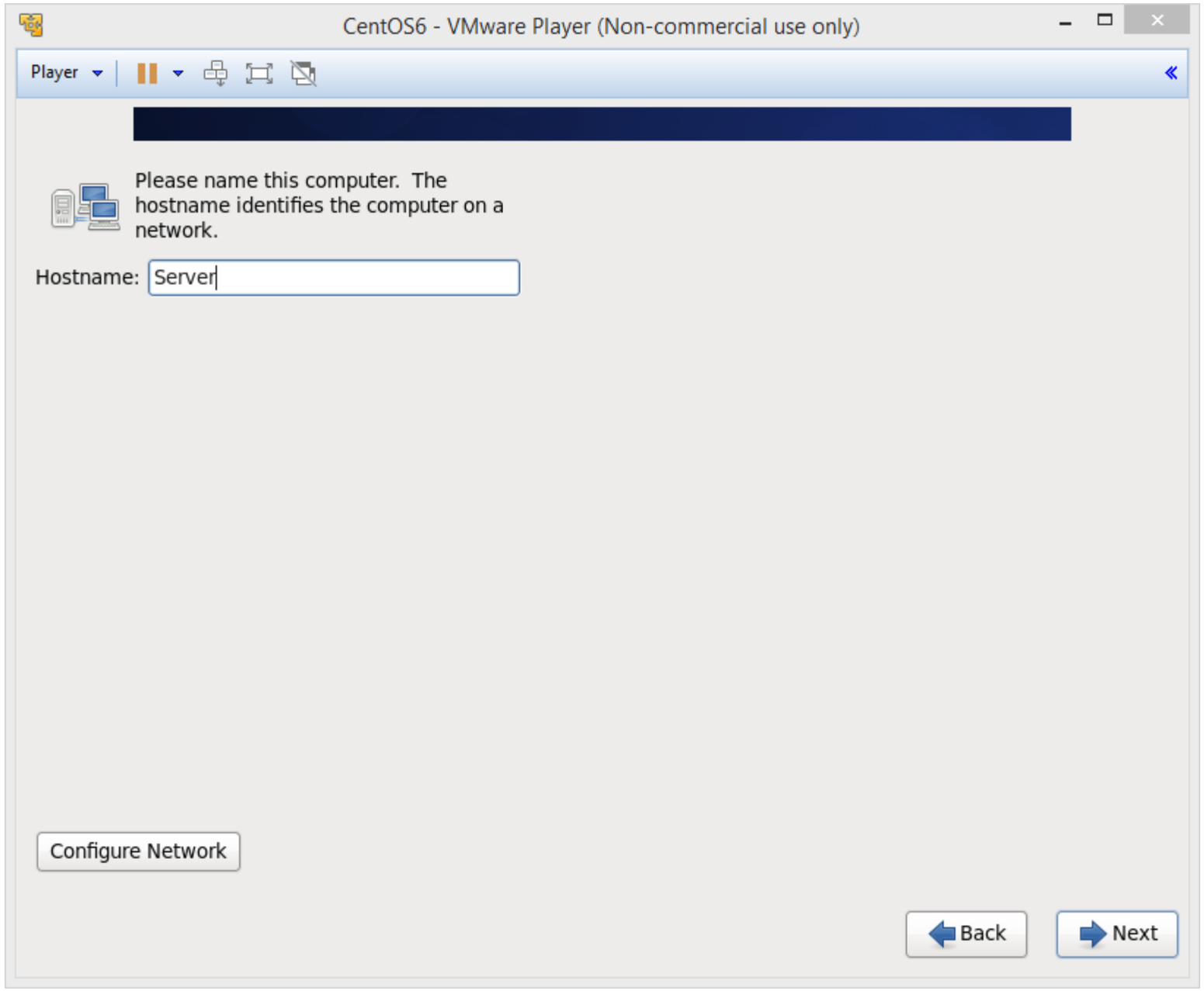
การจัดการ Disk



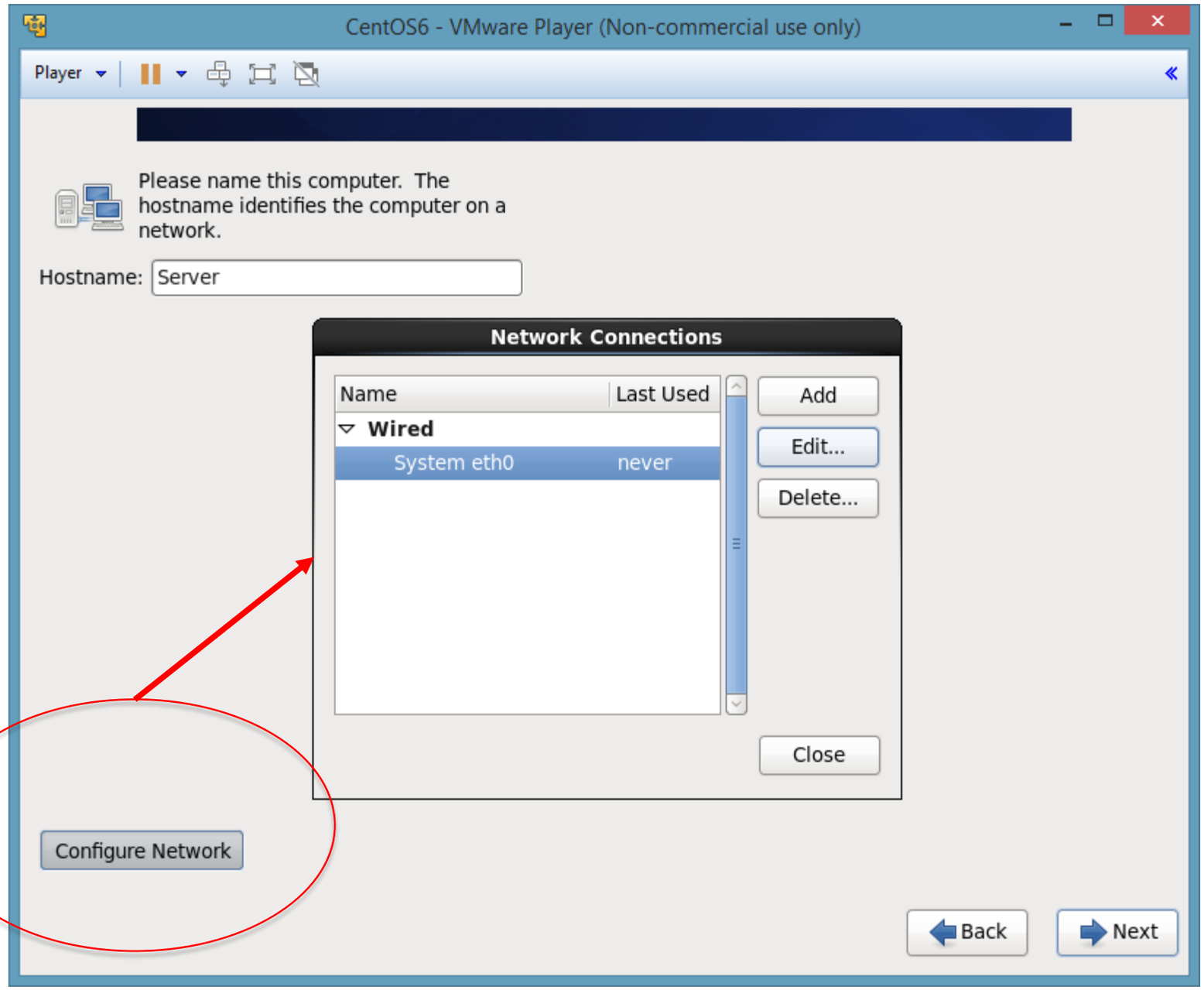
การจัดการ Disk



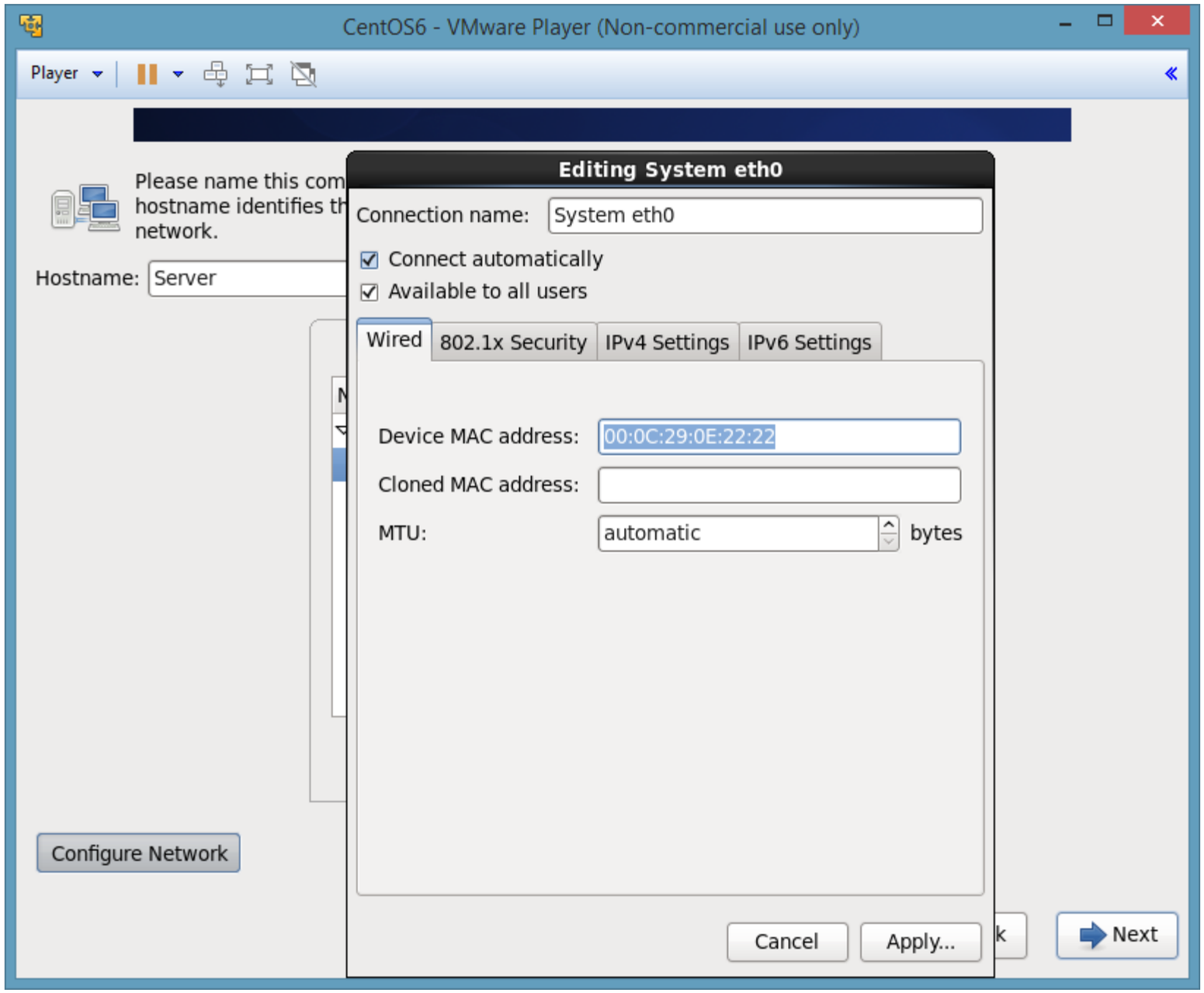
Hostname / Networking



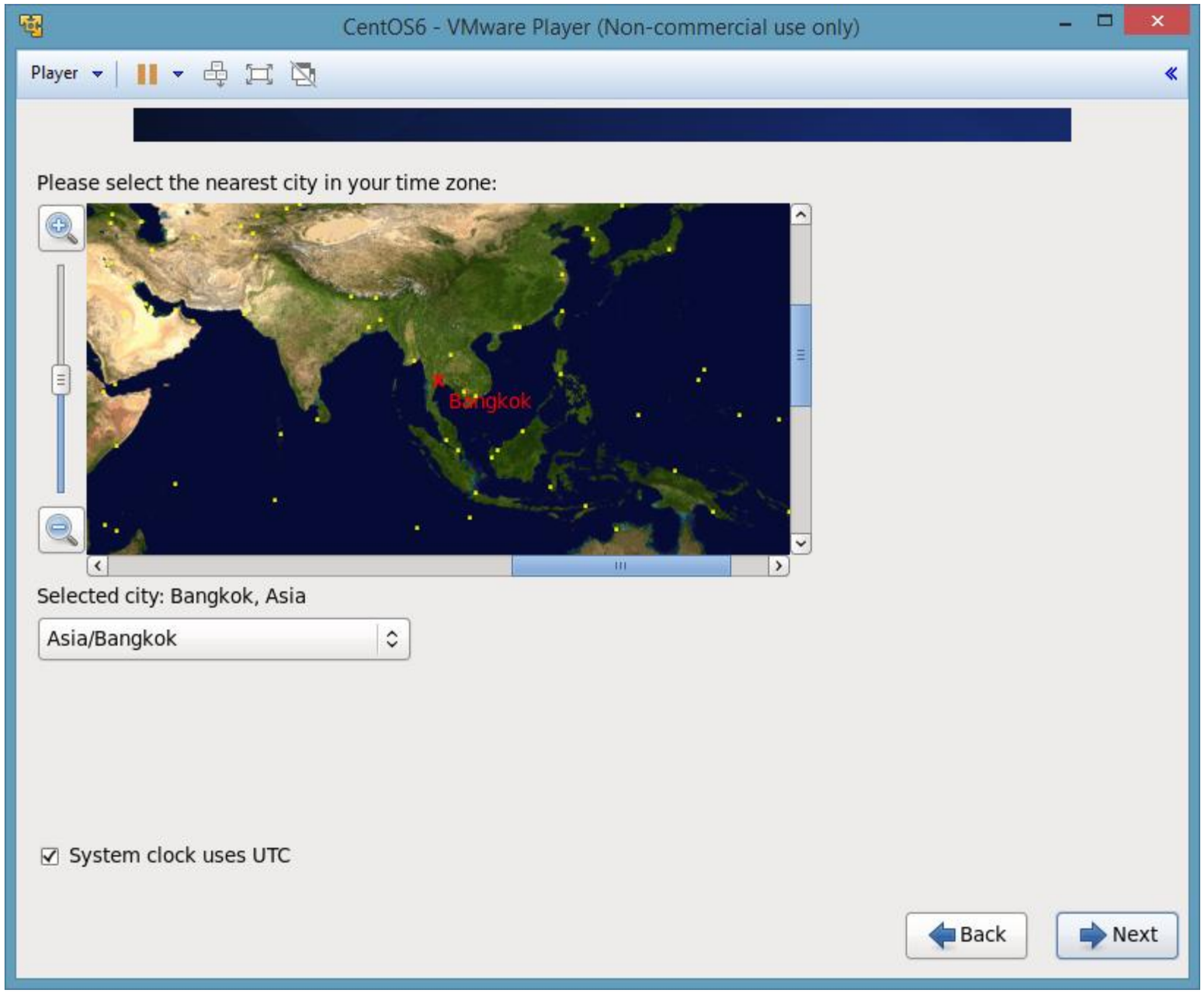
Networking


CentOS6 - VMware Player (Non-commercial use only)
Player
Please name this computer. The hostname identifies the computer on a network.
Hostname: Server
Network Connections
Name
Last Used
Wired
System eth0
never
Add
Edit...
Delete...
Close
Configure Network
Back
Next

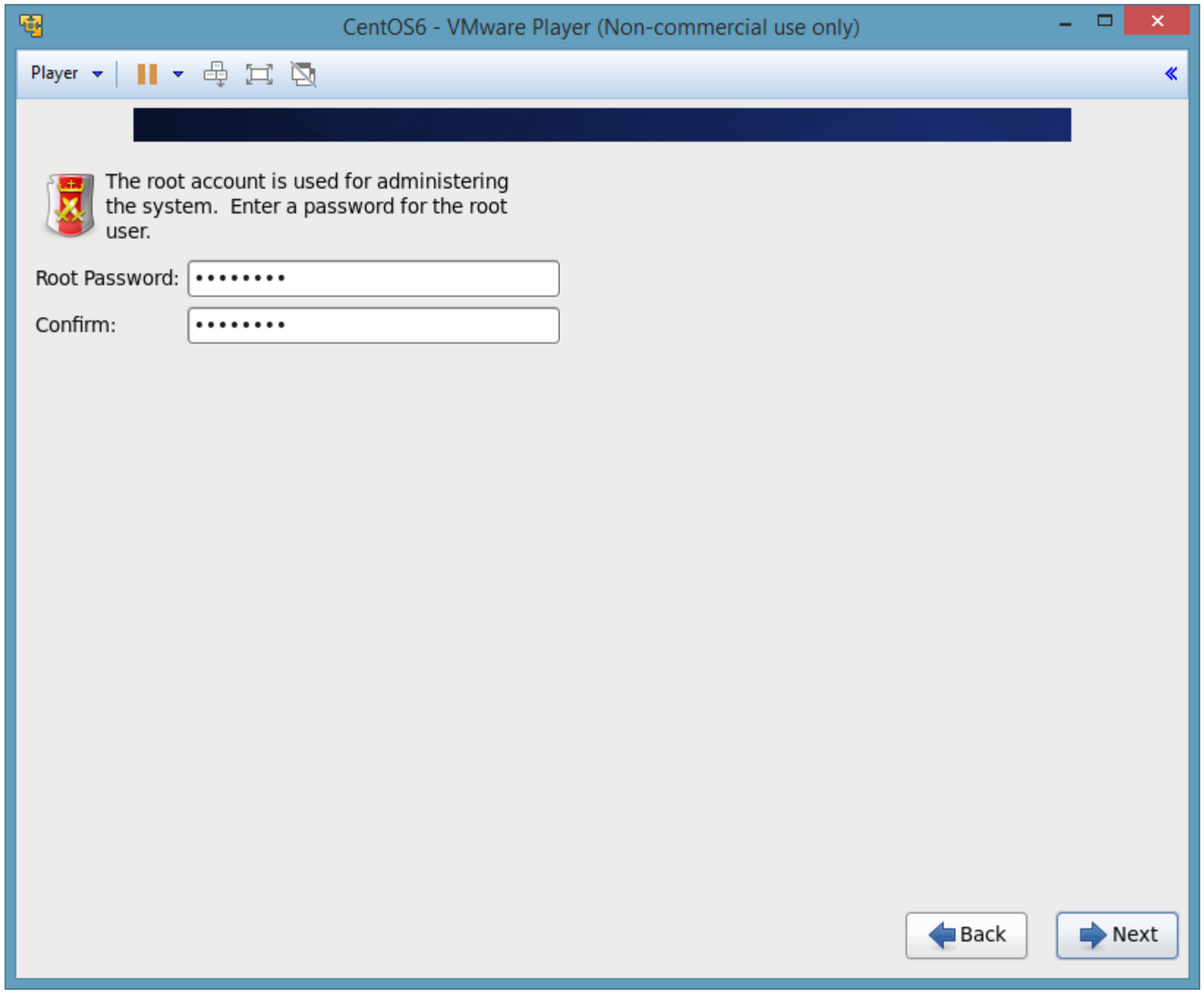
Networking


CentOS6 - VMware Player (Non-commercial use only)
Player
Please name this com
hostname identifies th
network.
Hostname:
Server
Configure Network
Editing System eth0
Connection name:
System eth0
Connect automatically
Available to all users
Wired
802.1x Security
IPv4 Settings
IPv6 Settings
Device MAC address:
00:0C:29:0E:22:22
Cloned MAC address:
MTU:
automatic
bytes
Cancel
Apply...
Next

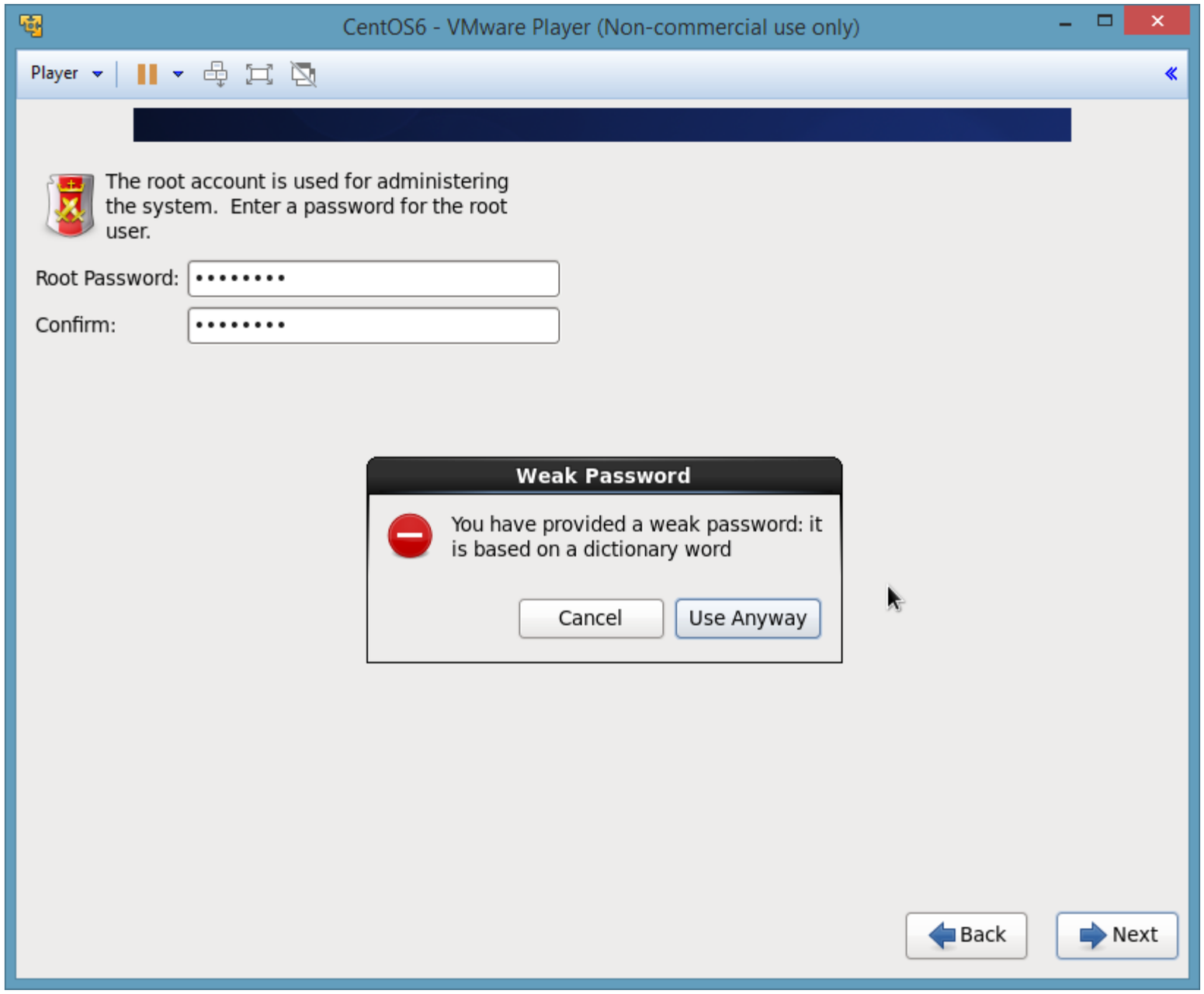
Time zone


CentOS6 - VMware Player (Non-commercial use only)
Player
Please select the nearest city in your time zone:
Bangkok
Selected city: Bangkok, Asia
Asia/Bangkok
System clock uses UTC
Back
Next

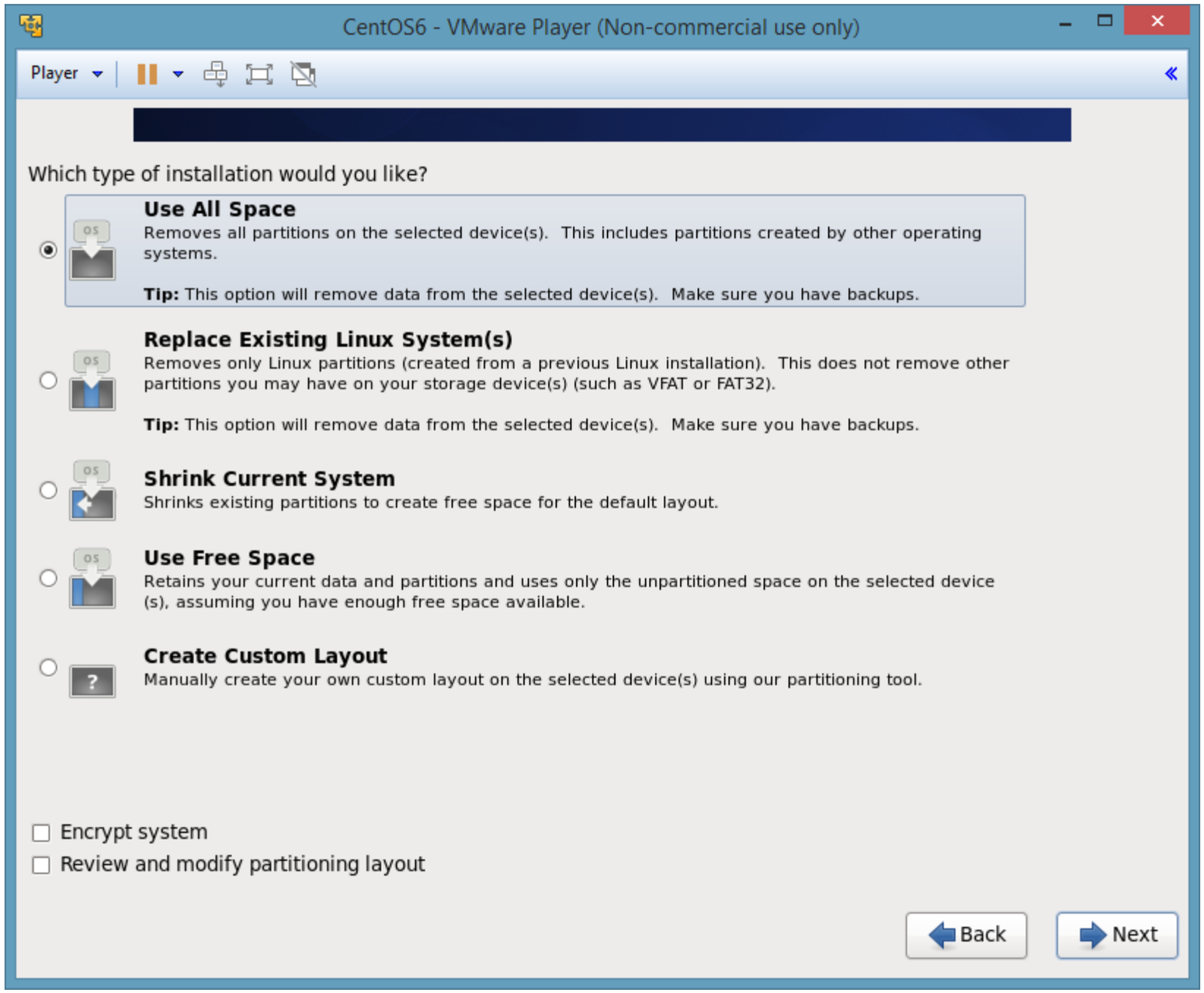
ROOT password



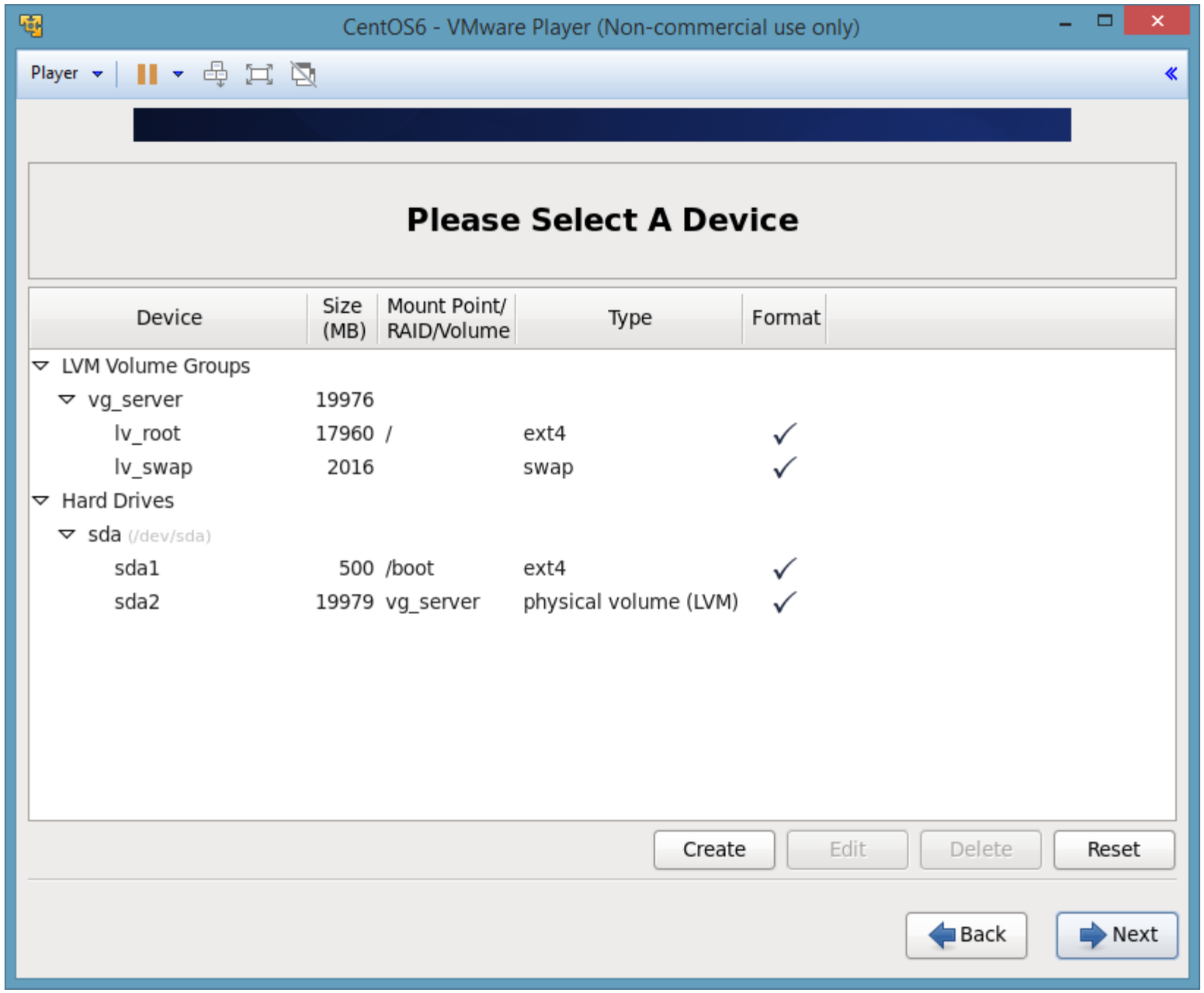
Weak Password!!!



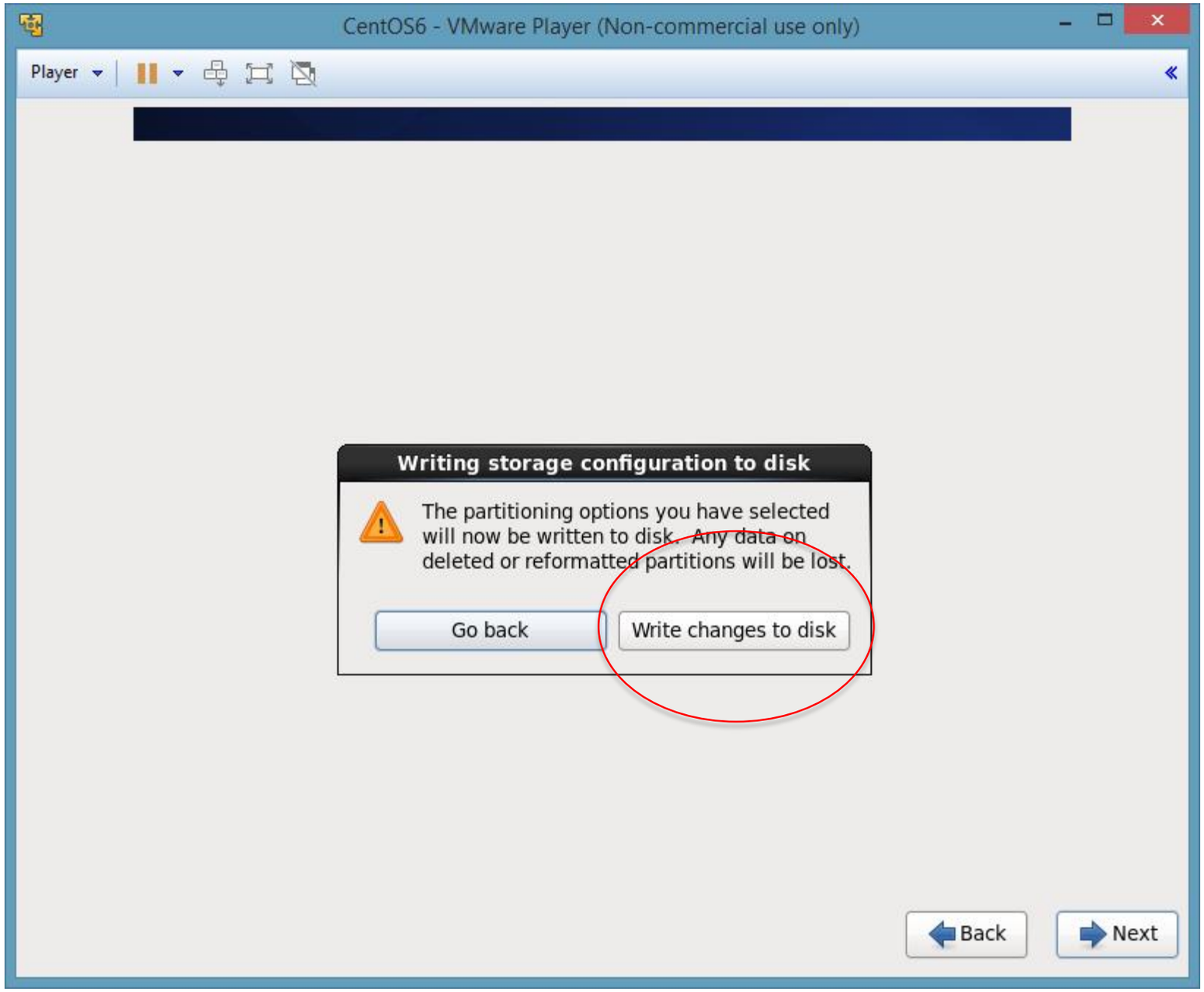
จัดการ Disk partitions



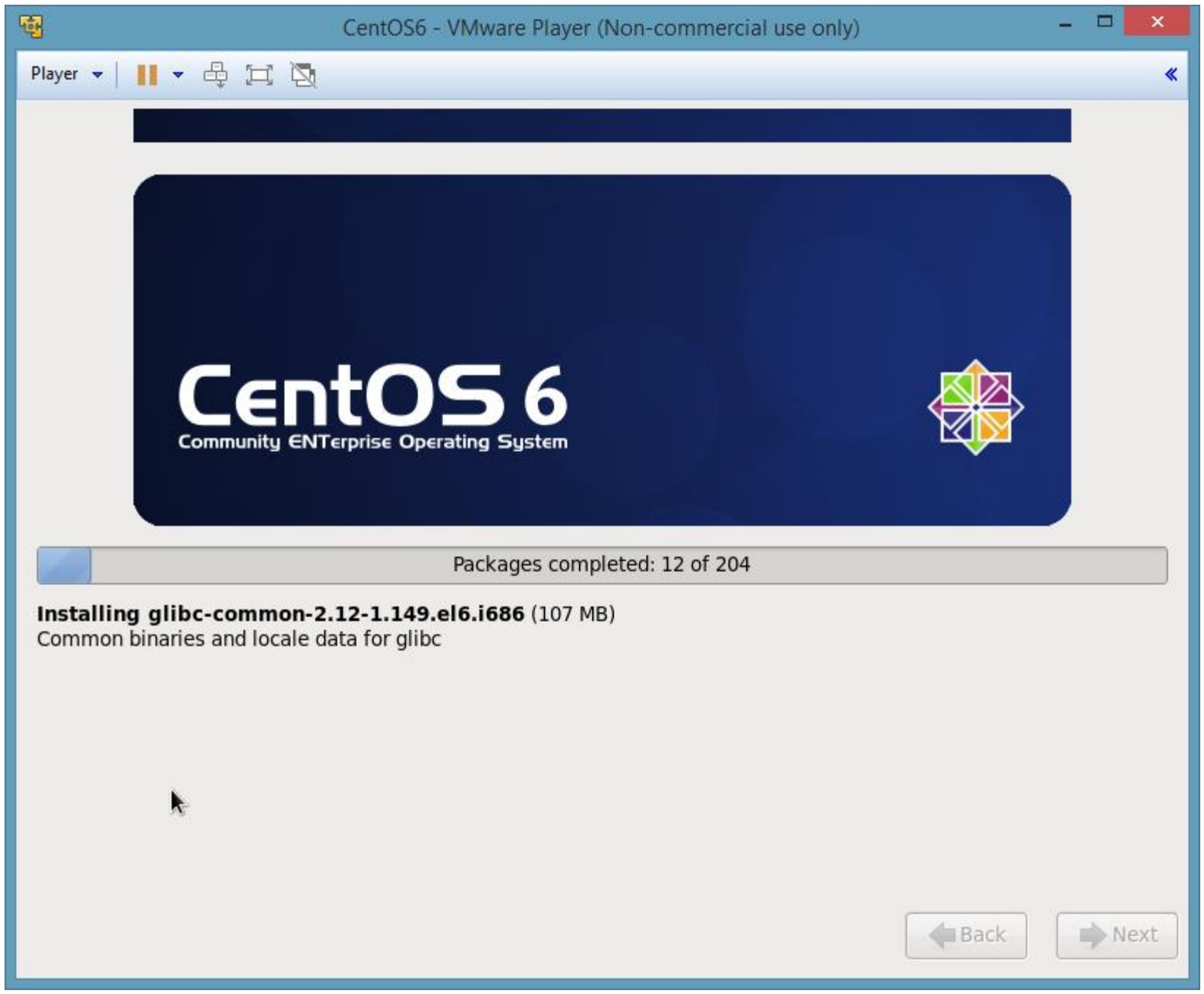
จัดการ Disk partitions



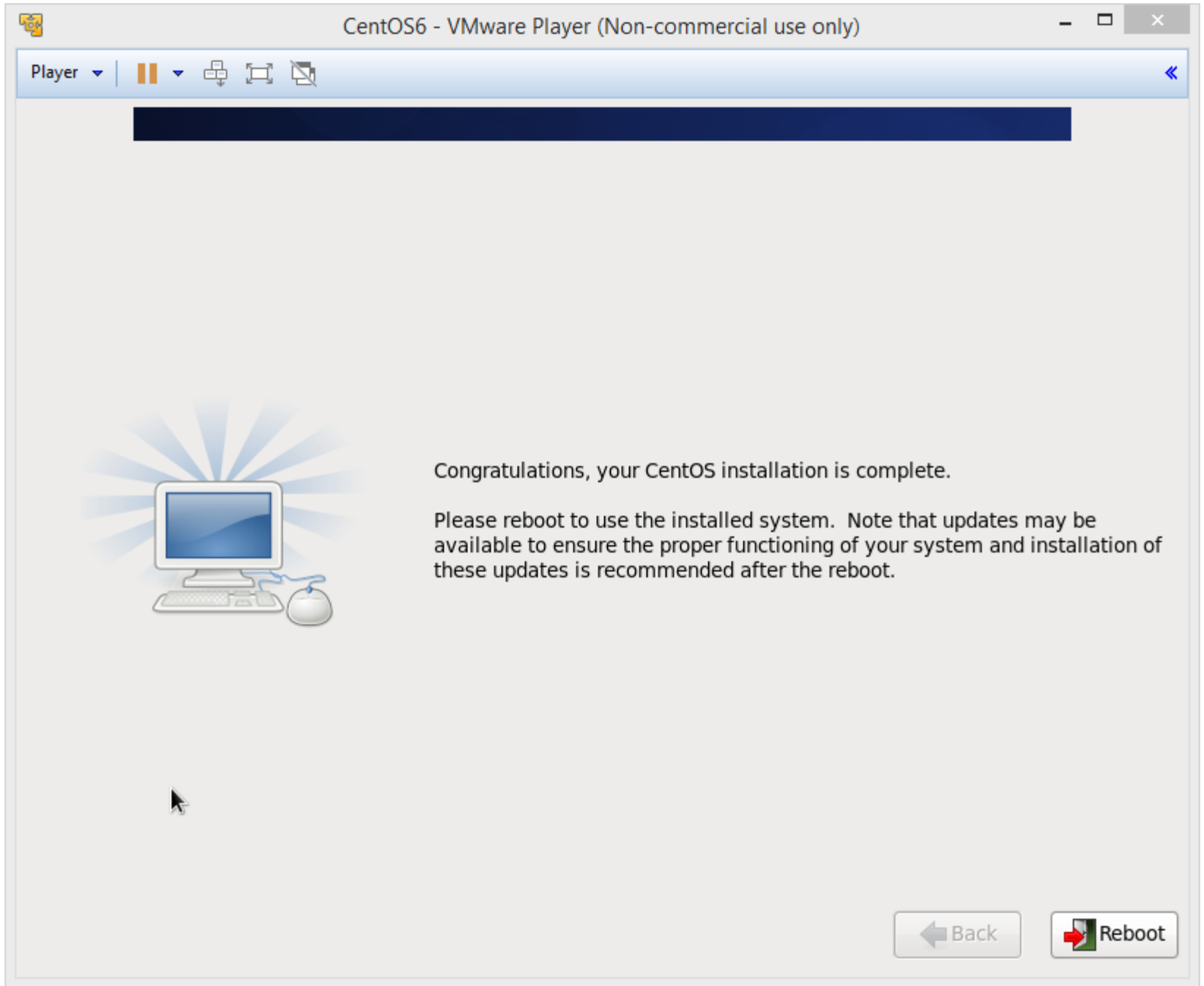
จัดการ Disk partitions



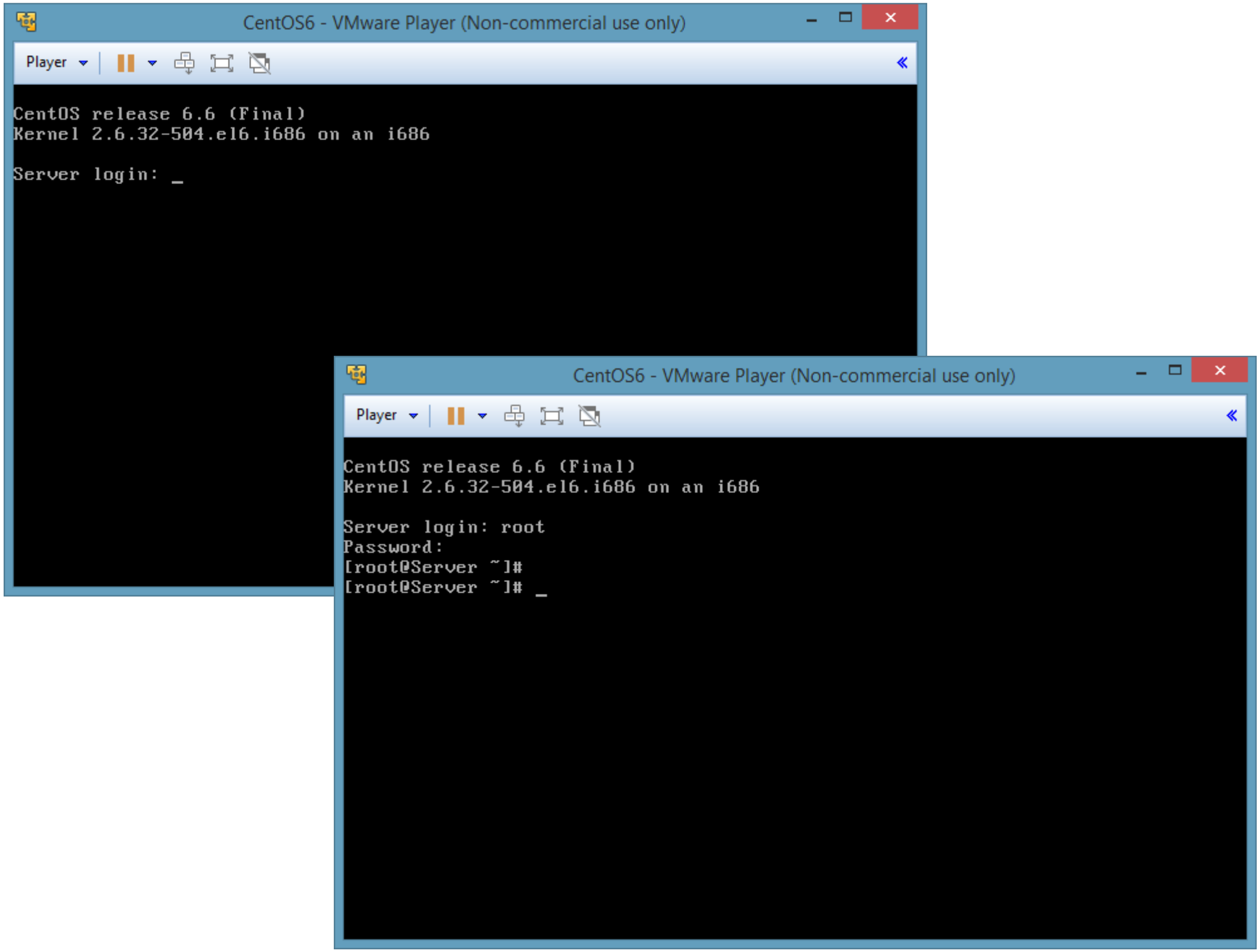
เริ่มติดตั้ง


CentOS6 - VMware Player (Non-commercial use only)
Player
CentOS 6
Community ENTerprise Operating System
Packages completed: 12 of 204
Installing glibc-common-2.12-1.149.el6.i686 (107 MB)
Common binaries and locale data for glibc
Back
Next

ติดตั้งแล้วเสร็จ



ระบบพร้อมใช้งาน



How to Disable SELINUX and IPTABLES (Just for testing system)

- การ Disable SELINUX

```
[root@Server ~]# setenforce 0
```

แก้ไขไฟล์ /etc/selinux/config โดยแก้ให้

SELINUX=disabled

- การ Disable IPTABLES

```
[root@Server ~]# chkconfig iptables off
[root@Server ~]# service iptables stop
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
```

การจัดการ User ของ Linux เบื้องต้น

- การเพิ่ม User

```
[root@Server ~]# adduser admin01
```

- การแก้ Password

```
[root@Server ~]# passwd admin01
Changing password for user admin01.
New password: <password>
Retype new password: <password>
passwd: all authentication tokens updated successfully.
```

การจัดการ User ของ Linux เบื้องต้น

- การลบ User (รวมถึง User’s Home ด้วย)

[root@Server ~]# **userdel -r admin01**

- การ Lock user

[root@Server ~]# **usermod -L admin01**

- การ Unlock user

- [root@Server ~]# **usermod -U admin01**

Default System Hardening

- Disabled unneeded/unsecured services เช่นโดยปกติแล้ว CentOS จะทำการติดตั้ง Postfix (Mail server) มาให้ด้วย ซึ่งหากไม่ใช้งานควรทำการ Disable ดังตัวอย่าง

```
[root@Server ~]# chkconfig postfix off
```

- System tuning เช่น การเปิดใช้งาน TCP syncookies เป็นต้น (/etc/sysctl.conf)

Patching your Linux

Update patch

```
[root@Server ~]# yum upgrade
Loaded plugins: fastestmirror
Setting up Upgrade Process
Base                                                    | 3.7 kB     00:00
base/primary_db                                         | 3.6 MB     00:00
Extras                                                  | 3.4 kB     00:00
extras/primary_db                                       |  29 kB     00:00
Updates                                                 | 3.4 kB     00:00
updates/primary_db                                      | 3.6 MB     00:01
Resolving Dependencies
--> Running transaction check
...
...
Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade      52 Package(s)
Total download size: 83 M
Is this ok [y/N]: y
```

Update patch

```
----------------------------------------------------------------------------------------
Total                                                    1.3 MB/s |  83 MB     01:05
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
Importing GPG key 0xC105B9DE:
 Userid : CentOS-6 Key (CentOS 6 Official Signing Key) <centos-6-key@centos.org>
 Package: centos-release-6-6.el6.centos.12.2.i686 (@anaconda-CentOS-201410241409.i386/6.6)
 From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
Is this ok [y/N]:y
...
...
Complete!
[root@Server ~]#
[root@Server ~]# reboot

Broadcast message from root@Server
        (/dev/pts/0) at 20:31 ...

The system is going down for reboot NOW!
```

Clock synchronizations

เทียบเวลากับ NTP server

- การติดตั้ง ntpdate

```
[root@Server ~]# yum -y install ntpdate
```

- เทียบเวลากับ NTP server

```
[root@Server ~]# ntpdate time.ega.or.th
13 Jul 15:28:42 ntpdate[1429]: step time server 164.115.2.132 offset -25201.355561 sec

[root@Server ~]# ntpdate time.ega.or.th time.navy.mi.th
13 Jul 15:29:33 ntpdate[1430]: adjust time server 203.185.69.60 offset 0.000215 sec
```

เทียบเวลากับ NTP server

- การติดตั้ง ntpd

```
[root@Server ~]# yum -y install ntp
```

- แก้ไข NTP servers ในไฟล์ **/etc/ntp.conf** ดังนี้

```
server time.ega.or.th iburst
server time.navy.mi.th iburst
server time1.nimt.or.th iburst
server time2.nimt.or.th iburst
```

เทียบเวลากับ NTP server

- กำหนดให้ ntpd ทำงานทุกครั้งที่ reboot

```
[root@Server ~]# chkconfig ntpd on
```

- การ Start/Stop/Restart ntpd

```
[root@Server ~]# service ntpd start
[root@Server ~]# service ntpd stop
[root@Server ~]# service ntpd restart
```

- ตรวจสอบสถานการณ์ทำงานของ ntpd

```
[root@Server ~]# ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+164.115.2.132   203.185.67.115   3 u   34   64    1    3.932    3.032   1.926
+113.53.247.3    .PPS.            1 u   31   64    3    5.531    2.460   0.769
 203.185.69.60   .STEP.          16 u    -   64    0    0.000    0.000   0.000
*203.185.69.59   .GPS.            1 u  125   64    2    5.414    2.098   0.550
```

MySQL server

การติดตั้ง MySQL server

- ติดตั้ง MySQL server

```
[root@Server ~]# yum -y install mysql-server
```

- การกำหนดให้ MySQL ทำงานทุกครั้งเมื่อมีการ boot เครื่อง

```
[root@Server ~]# chkconfig mysqld on
```

- การ Start/Stop/Restart MySQL server

```
[root@Server ~]# service mysqld start
[root@Server ~]# service mysqld stop
[root@Server ~]# service mysqld restart
```

MySQL server

- ตำแหน่งไฟล์ Configuration ของ MySQL server

/etc/my.cnf

- ตำแหน่งไฟล์ Logs ของ MySQL server

/var/log/mysqld.log

MySQL server

- ตรวจสอบสถานการณ์ทำงานของ MySQL server

```
[root@Server ~]# ps ax | grep mysqld
 1541 ?        S      0:00 /bin/sh /usr/bin/mysqld_safe --datadir=/var/lib/mysql --
socket=/var/lib/mysql/mysql.sock --pid-file=/var/run/mysqld/mysqld.pid --basedir=/usr --
user=mysql
 1643 ?        Sl     0:03 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --
user=mysql --log-error=/var/log/mysqld.log --pid-file=/var/run/mysqld/mysqld.pid --
socket=/var/lib/mysql/mysql.sock
 1915 pts/0    S+     0:00 grep mysqld


[root@Server ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address     State       PID/Program name
tcp        0      0 0.0.0.0:3306       0.0.0.0:*           LISTEN      1643/mysqld
```

MySQL server

- เข้าใช้งาน MySQL server

```
[root@Server ~]# mysql -u root -p
Enter password:<password>
Your MySQL connection id is 9
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

MySQL server

- การตั้ง Password ให้ Root ของ MySQL (ผ่าน SQL query)

```
[root@Server ~]# mysql -u root –p mysql
Enter password:

mysql> update user set password = password("MySQLPASSWORD") where user = "root";
Query OK, 3 rows affected (0.00 sec)
Rows matched: 3  Changed: 3  Warnings: 0

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

MySQL server

- การตั้ง Password ให้ Root ของ MySQL (แนะนำใช้วิธีนี้)

```
[root@Server ~]# mysql_secure_installation
...
Enter current password for root (enter for none):
OK, successfully used password, moving on...
Change the root password? [Y/n] Y
New password: <new-secure-password>
Re-enter new password: <new-secure-password>
Password updated successfully!
Reloading privilege tables..
 ... Success!
Remove anonymous users? [Y/n] Y
 ... Success!
```

MySQL server

```
Disallow root login remotely? [Y/n] Y
 ... Success!
Remove test database and access to it? [Y/n] Y
 - Dropping test database...
... Success!
 - Removing privileges on test database...
 ... Success!
Reload privilege tables now? [Y/n] Y
 ... Success!
Cleaning up...
All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.
Thanks for using MySQL!
```

MySQL server

- **Command อื่น ๆที่น่าสนใจ**

```
mysql> use mysql;
Database changed
mysql> select user,host,password from user;
+--------+-----------+-------------------------------------------+
| user   | host      | password                                  |
+--------+-----------+-------------------------------------------+
| root   | localhost | *4A07491D82231F5AA938F1670CA874A1384677B0 |
| root   | server    | *4A07491D82231F5AA938F1670CA874A1384677B0 |
| root   | 127.0.0.1 | *4A07491D82231F5AA938F1670CA874A1384677B0 |
|        | localhost |                                           |
|        | server    |                                           |
| komkit | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root   | %         | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+--------+-----------+-------------------------------------------+
7 rows in set (0.00 sec)
```

MySQL server

- **Command อื่นๆที่น่าสนใจ**

```
mysql> show processlist;
+----+------+--------------------+------+---------+------+-------+------------------+
| Id | User | Host               | db   | Command | Time | State | Info             |
+----+------+--------------------+------+---------+------+-------+------------------+
| 26 | root | localhost          | mysql | Query   |    0 | NULL  | show processlist |
| 37 | root | 192.168.38.1:54182 | NULL  | Sleep   |    4 |       | NULL             |
| 38 | root | 192.168.38.1:54183 | NULL  | Sleep   |    4 |       | NULL             |
+----+------+--------------------+------+---------+------+-------+------------------+
3 rows in set (0.00 sec)
```

MySQL server

- **การกำหนดให้ MySQL server ทำการ Listen บนเฉพาะ Localhost เท่านั้น** (ในกรณีที่ Application และ MySQL อยู่บนเครื่องเดียวกัน) โดยให้ทำการแก้ไขที่ไฟล์ **/etc/my.cnf** ดังนี้

```
[mysqld]
bind-address=127.0.0.1
```

จากนั้นทำการ restart mysqld แล้วตรวจสอบการทำงาน

```
[root@Server ~]# service mysqld restart
[root@Server ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address    Foreign Address        State       PID/Program name
tcp        0      127.0.0.1:3306    0.0.0.0:*              LISTEN      1953/mysqld
```

HTTP server

Apache server

- **การติดตั้ง Apache server**

```
[root@Server ~]# yum -y install httpd
```

- การกำหนดให้ Apache ทำงานทุกครั้งเมื่อมีการ boot เครื่อง

```
[root@Server ~]# chkconfig httpd on
```

- การ Start/Stop/Restart Apache server

```
[root@Server ~]# service httpd start
[root@Server ~]# service httpd stop
[root@Server ~]# service httpd restart
```

Apache server

- ตำแหน่งไฟล์ Configuration ของ Apache server

/etc/httpd/

- ตำแหน่งไฟล์ Logs ของ Apache server

/var/log/httpd/

- ตำแหน่งที่เก็บไฟล์ของ WWW server

/var/www/html/

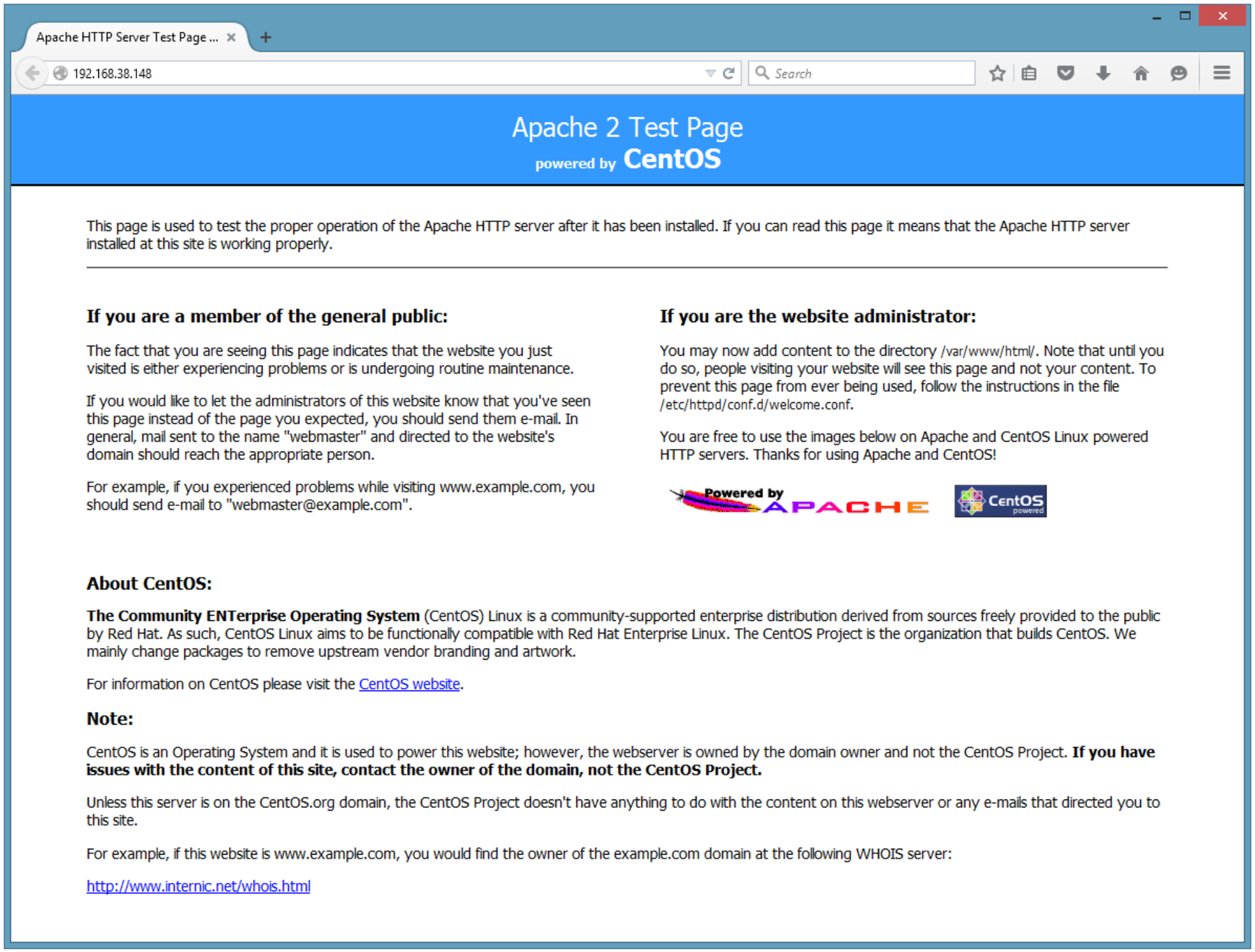
Apache server

- ตรวจสอบสถานการณ์ทำงานของ Apache server

```
[root@Server ~]# ps ax | grep httpd
 1942 ?        Ss     0:00 /usr/sbin/httpd
 1944 ?        S      0:00 /usr/sbin/httpd
 1945 ?        S      0:00 /usr/sbin/httpd
 1946 ?        S      0:00 /usr/sbin/httpd
 1947 ?        S      0:00 /usr/sbin/httpd
 1948 ?        S      0:00 /usr/sbin/httpd
 1949 ?        S      0:00 /usr/sbin/httpd
 1950 ?        S      0:00 /usr/sbin/httpd
 1951 ?        S      0:00 /usr/sbin/httpd
 1955 pts/0    S+     0:00 grep httpd
```

```
[root@Server ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address  Foreign Address      State       PID/Program name
tcp        0      0 :::80          :::*                LISTEN      1942/httpd
```

Apache server



Apache + PHP

- **ติดตั้ง PHP**

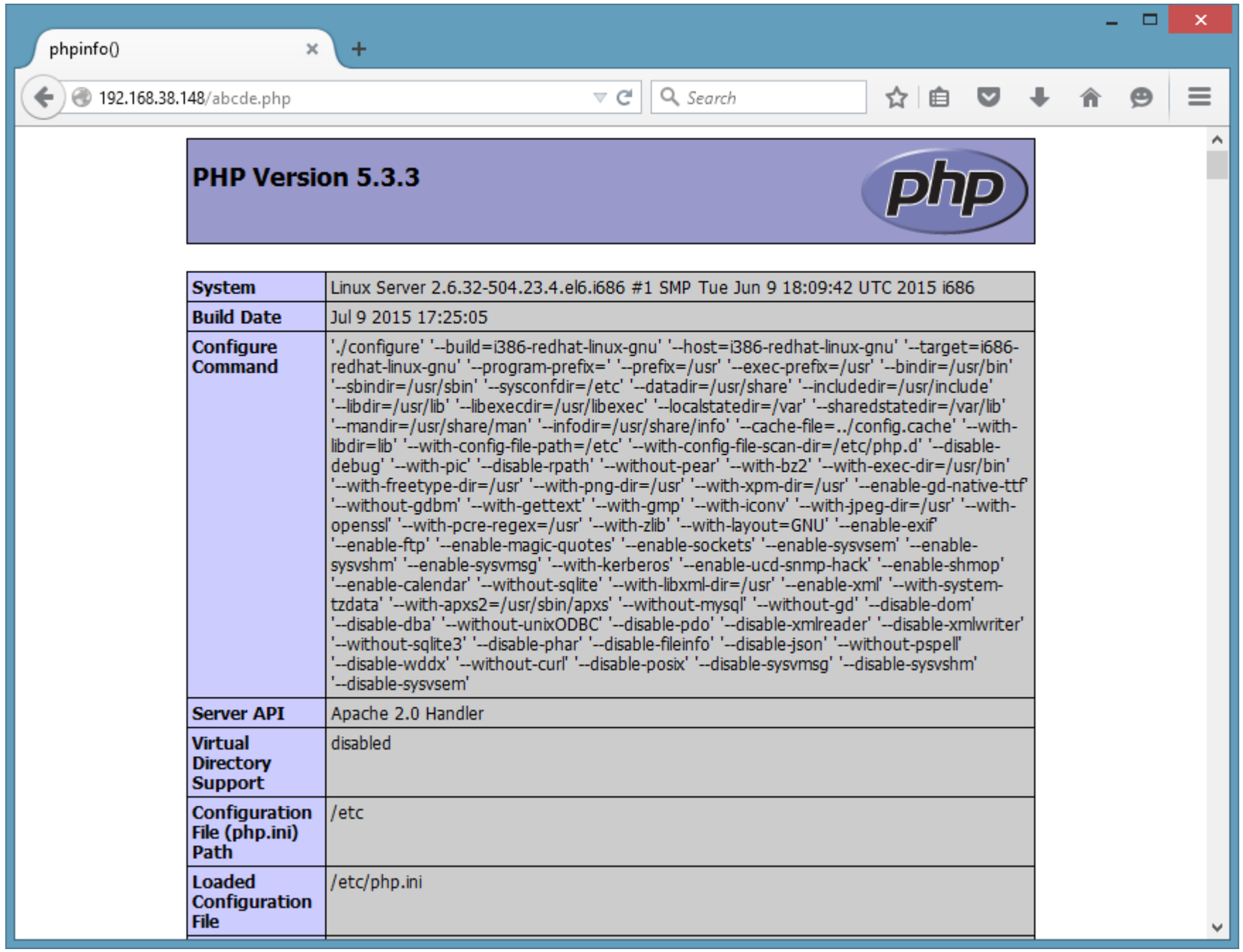
```
[root@Server ~]# yum -y install php php-mysql
[root@Server ~]# service httpd restart
```

- ทดสอบใช้งาน PHP

```
[root@Server ~]# vi /var/www/html/abcde.php
```

```
<?php phpinfo(); ?>
```

Apache + PHP

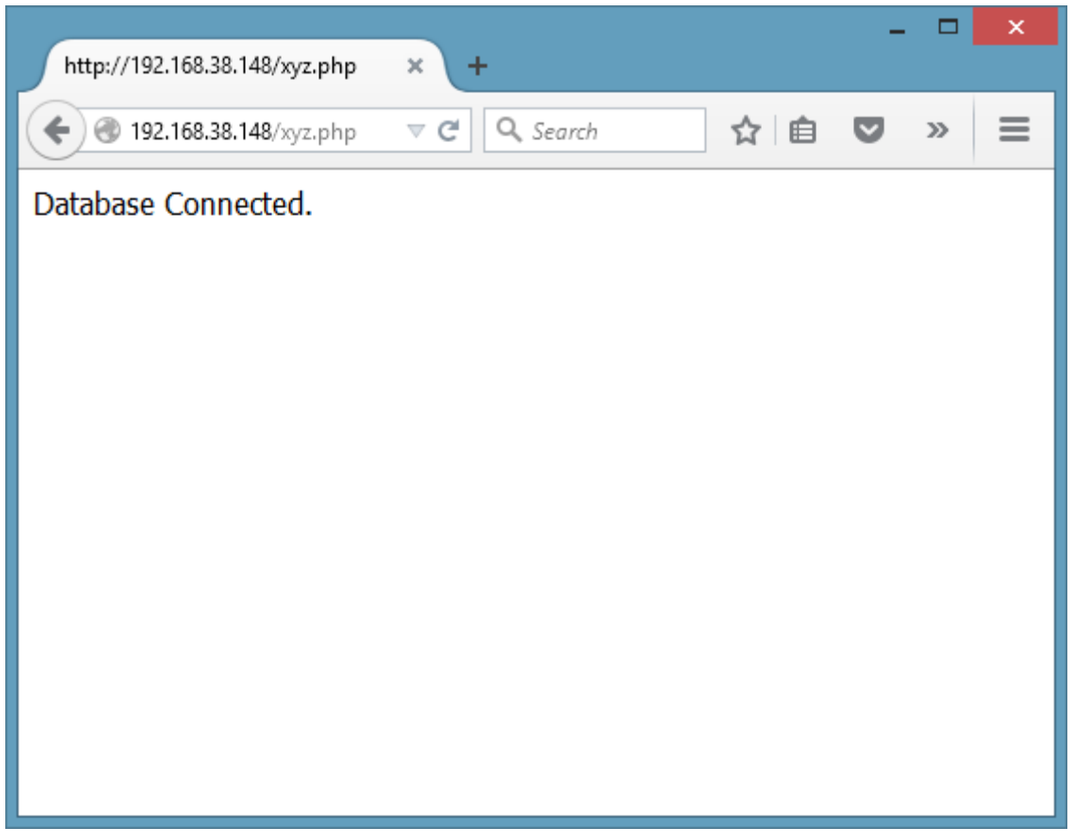

phpinfo()
192.168.38.148/abcde.php
Search
PHP Version 5.3.3
php
System
Linux Server 2.6.32-504.23.4.el6.i686 #1 SMP Tue Jun 9 18:09:42 UTC 2015 i686
Build Date
Jul 9 2015 17:25:05
Configure Command
'./configure' '--build=i386-redhat-linux-gnu' '--host=i386-redhat-linux-gnu' '--target=i686-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem'
Server API
Apache 2.0 Handler
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/etc
Loaded Configuration File
/etc/php.ini

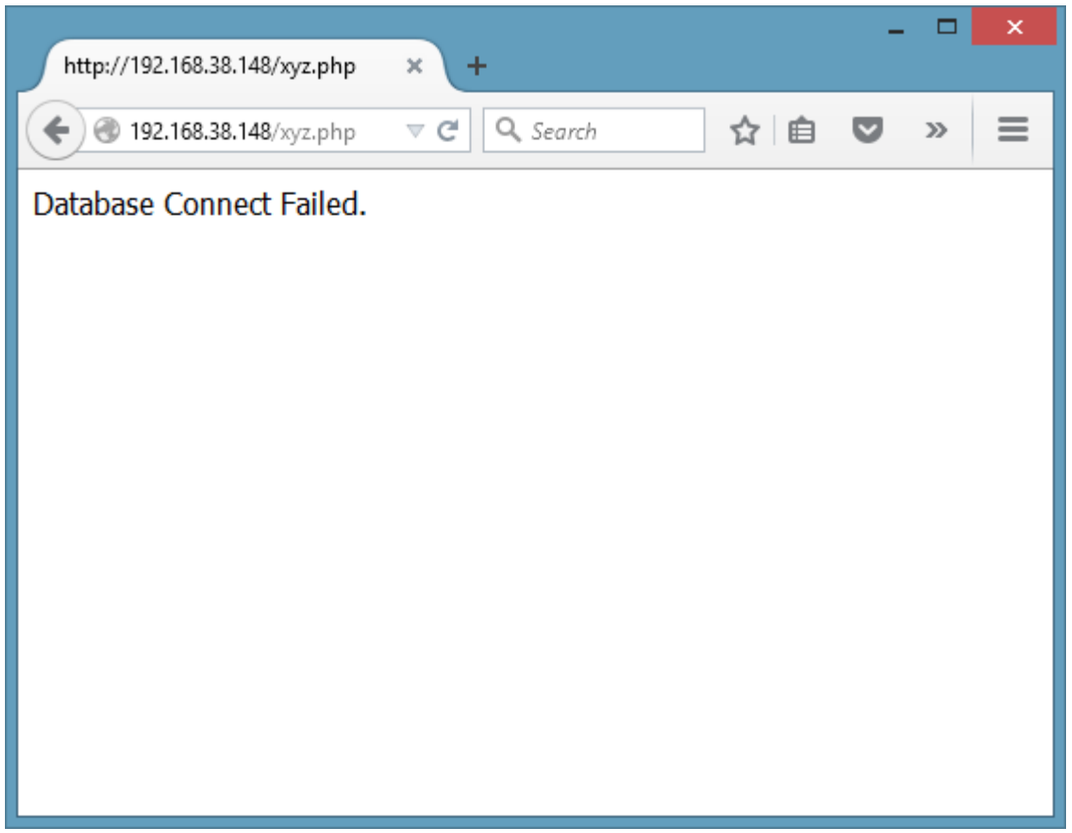
LAMP: Linux + Apache + MySQL + PHP

- ทดสอบ Connect MySQL ด้วย PHP

```
<?php

$dbConnect = mysql_connect("localhost","root","MySQLPASSWORD");

if($dbConnect)
	{
		echo "Database Connected.";
	}
	else
	{
		echo "Database Connect Failed.";
	}

mysql_close($dbConnect);

?>
```

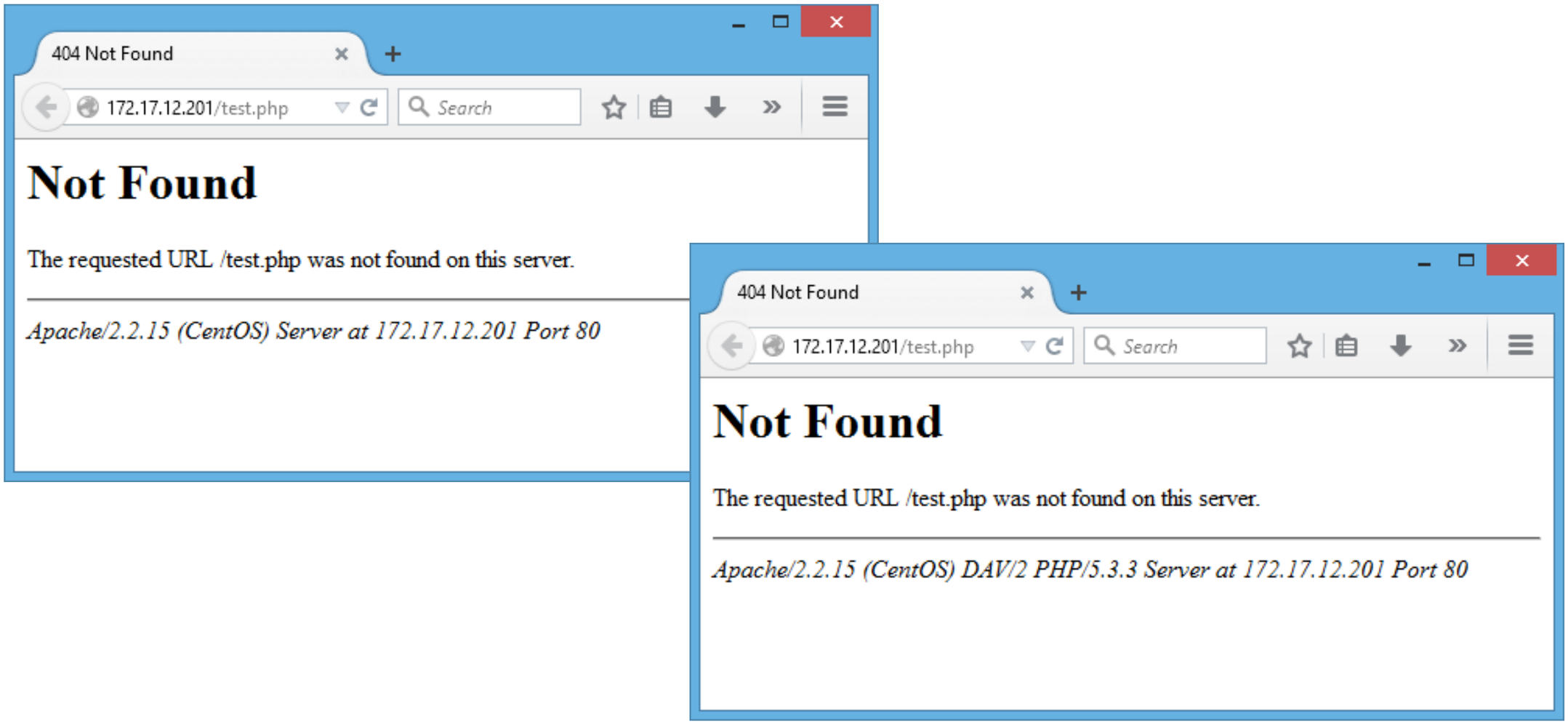
LAMP: Linux + Apache + MySQL + PHP





Apache server (Hardening)

ปิดการแสดง Apache version และ OS version



Apache server (Hardening)

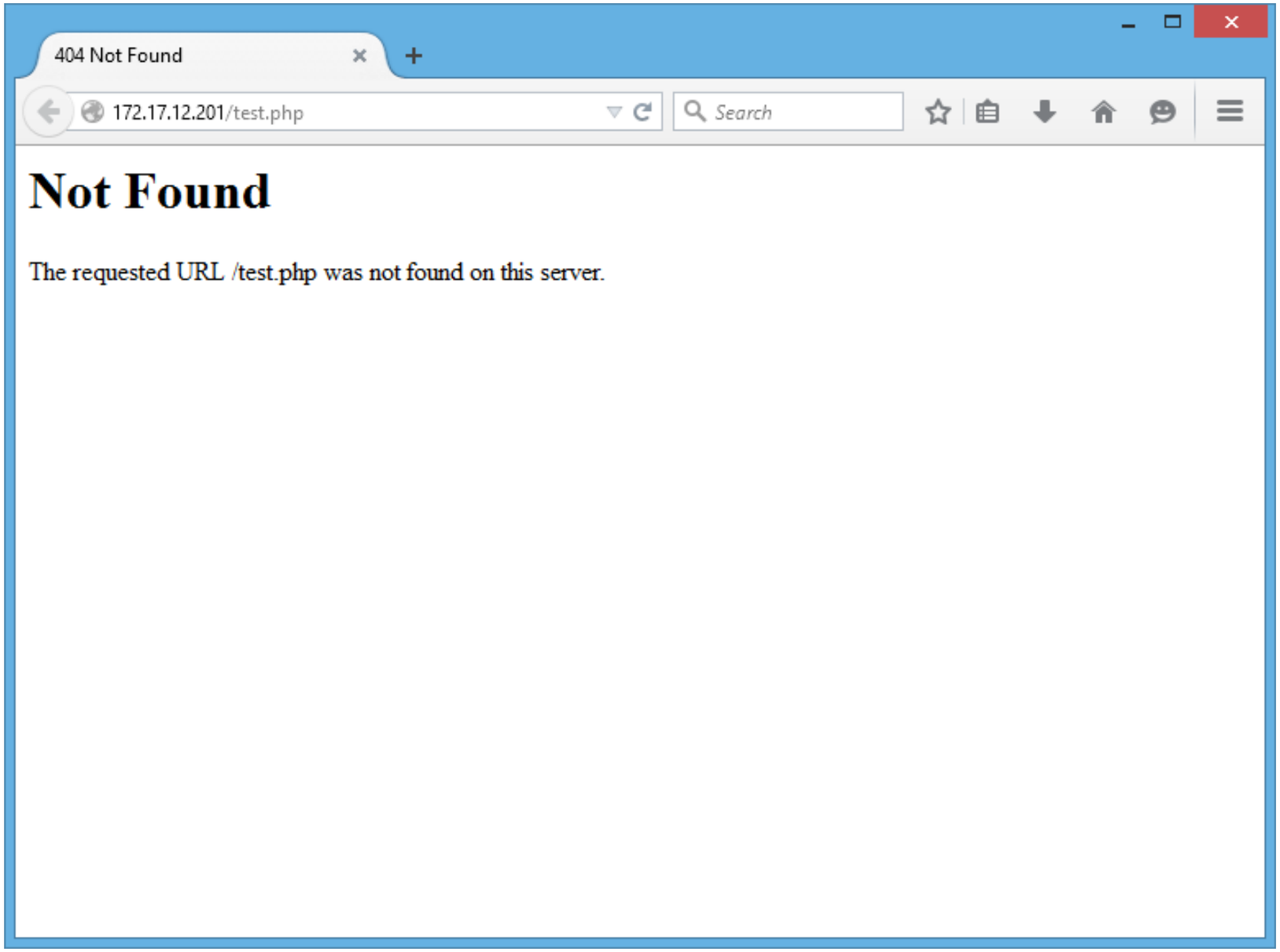
แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf**

ServerTokens Prod
ServerSignature Off

ทำการ restart httpd

```
[root@Server ~]# service httpd restart
Stopping httpd:                                    [  OK  ]
Starting httpd: httpd: apr_sockaddr_info_get() failed for Server
httpd: Could not reliably determine the server's fully qualified
domain name, using 127.0.0.1 for ServerName
                                                   [  OK  ]
```

Apache server (Hardening)



Apache server (Hardening)

ตัวอย่างเพิ่มเติมเกี่ยวกับ ServerTokens

ServerTokens Prod[uctOnly]

Server sends (*e.g.*): `Server: Apache`

ServerTokens Major

Server sends (*e.g.*): `Server: Apache/2`

ServerTokens Minor

Server sends (*e.g.*): `Server: Apache/2.0`

ServerTokens Min[imal]

Server sends (*e.g.*): `Server: Apache/2.0.41`

ServerTokens OS

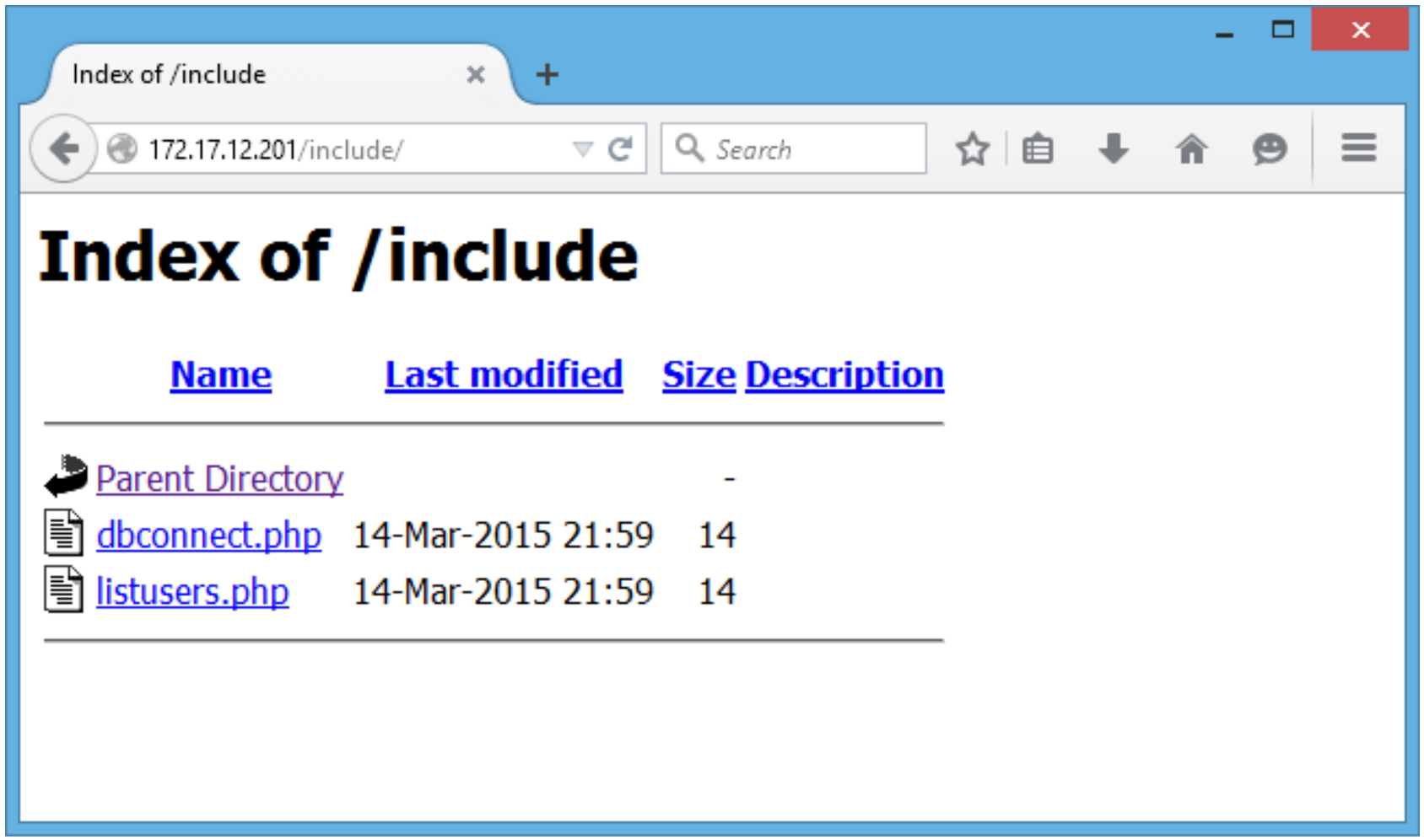
Server sends (*e.g.*): `Server: Apache/2.0.41 (Unix)`

ServerTokens Full (or not specified)

Server sends (*e.g.*): `Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2`

Apache server (Hardening)

ปิดการใช้งาน Directory Listing



Apache server (Hardening)

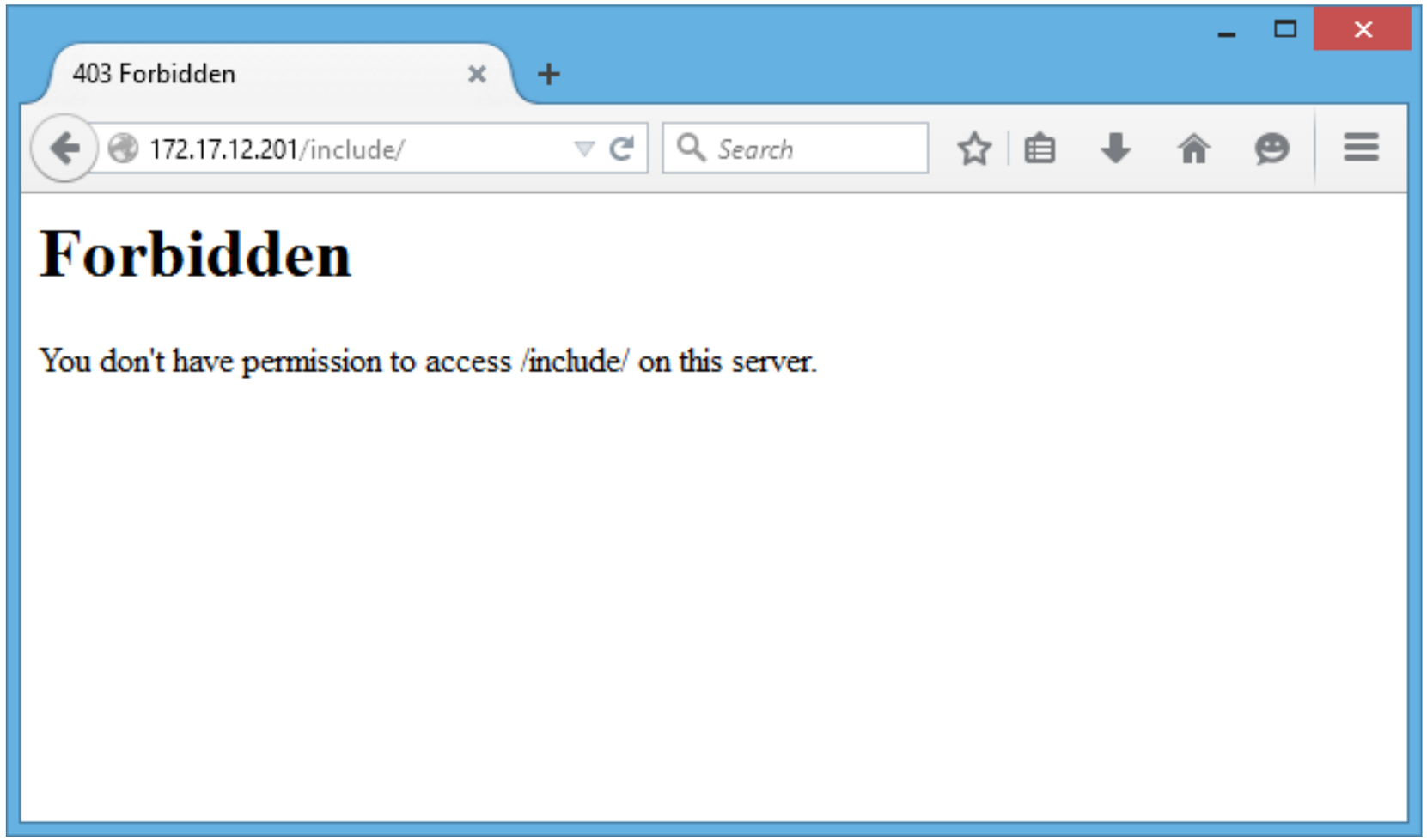
แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf** แล้วค้นหา

```
<Directory "/var/www/html">
        --- ตัด Output ---
        Options Indexes FollowSymLinks
        --- ตัด Output ---
</Directory>
```

แก้ไขเป็น

```
<Directory "/var/www/html">
        --- ตัด Output ---
        Options FollowSymLinks
        --- ตัด Output ---
</Directory>
```

Apache server (Hardening)



Apache server (Hardening)

การจำกัดให้เฉพาะบาง IP เข้าถึง Directory โดย .htaccess

การเปิดการใช้งาน .htaccess

แก้ไขไฟล์ **/etc/httpd/conf/httpd.conf แล้วค้นหา**

```
<Directory "/var/www/html">
        --- ตัด Output ---
      AllowOverride None
        --- ตัด Output ---
<Directory>
```

Apache server (Hardening)

แก้ไขเป็น

```
<Directory "/var/www/html">
        --- ตัด Output ---
      AllowOverride All
        --- ตัด Output ---
<Directory>
```

จากนั้น Restart httpd service

Apache server (Hardening)

ตัวอย่างการใช้งาน .htaccess เพื่อจำกัดให้เฉพาะ IP 192.168.0.0/24 เท่านั้นที่สามารถเข้าใช้งาน http://IP-Address/administrator ได้

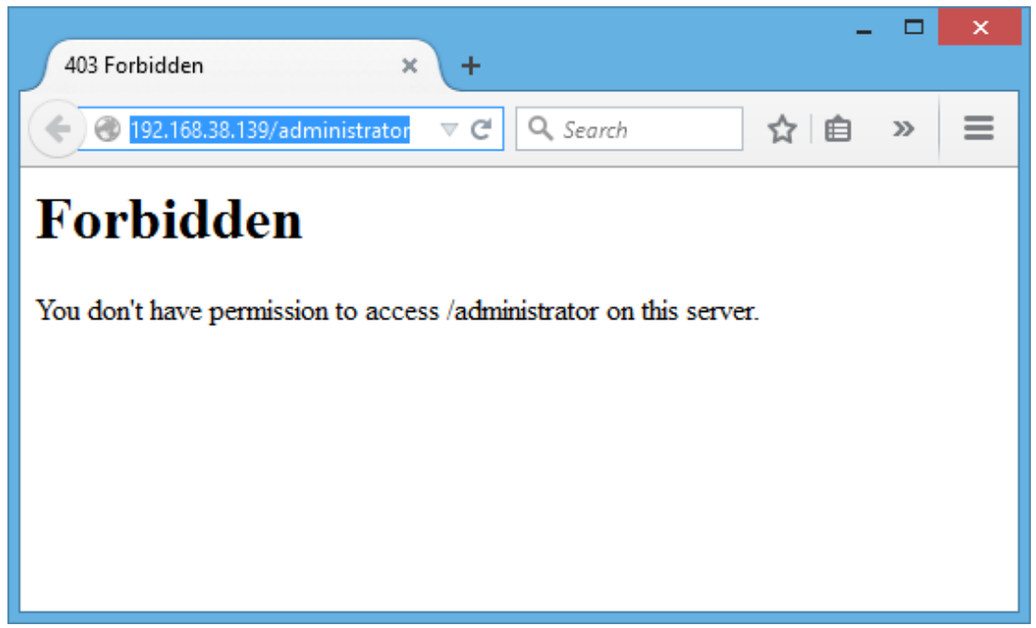
สามารถทำได้โดย สร้างไฟล์ .htaccess ภายใน Directory administrator แล้วใส่ค่า Configuration ดังนี้

```
order deny,allow
deny from all
allow from 192.168.0.0/24
```

จากนั้นทำการบันทึกไฟล์

Apache server (Hardening)

ทดสอบการใช้งานจาก IP **ที่ไม่ใช่ 192.168.0.0/24**



Log การ Deny IP ที่เข้าถึง (/var/log/httpd/error_log)

[Tue Mar 17 19:26:15 2015] [error] [client 192.168.38.1] client denied by server configuration: /var/www/html/administrator

Apache: enable HTTPS

```
[root@Server ~]# yum -y install mod_ssl
```

จากนั้นทำการ restart httpd

```
[root@Server ~]# service httpd restart
```

ตรวจสอบว่า HTTPS ถูกเปิดแล้ว

```
[root@Server ~]# netstat –antup
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 :::443                  :::*                    LISTEN      2412/httpd
```

Apache: Redirect Users to HTTPS

! ทำการสร้างไฟล์ .htaccess ใน Directory ที่ต้องการให้มีการ redirect เช่นตัวอย่างจะสร้างใน path /admin

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/admin/$1 [R,L]
```

FTP server

การติดตั้ง FTP server (vsftpd)

- การติดตั้ง FTP server

```
[root@Server httpd]# yum -y install vsftpd
```

- การกำหนดให้ FTP ทำงานทุกครั้งเมื่อมีการ boot เครื่อง

```
[root@Server ~]# chkconfig vsftpd on
```

- การ Start/Stop/Restart MySQL server

```
[root@Server ~]# service vsftpd start
[root@Server ~]# service vsftpd stop
[root@Server ~]# service vsftpd restart
```

FTP server

- ตำแหน่งไฟล์ Configuration ของ FTP server

/etc/vsftpd/

- ตำแหน่งไฟล์ Logs ของ FTP server

/var/log/xferlog

/var/log/secure

FTP server

- ตรวจสอบสถานการณ์ทำงานของ FTP server

```
[root@Server ~]# ps ax | grep vsftpd
 2289 ?        Ss     0:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
 2433 pts/0    S+     0:00 grep vsftpd
```

```
[root@Server ~]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address     State       PID/Program name
tcp        0      0 0.0.0.0:21         0.0.0.0:*           LISTEN      2289/vsftpd
```

FTP server

- ทำการ Hardening FTP service โดยแก้ไขไฟล์ **/etc/vsftpd/vsftpd.conf**

```
anonymous_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
chroot_local_user=YES
```

vsftpd with SSL

! ทำการสร้าง Certificate

openssl req -x509 -nodes -days 365 -newkey rsa:1024 –keyout /etc/vsftpd/vsftpd.pem -out /etc/vsftpd/vsftpd.pem

```
Generating a 1024 bit RSA private key
..++++++
.........................++++++
writing new private key to '/etc/vsftpd/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:TH
State or Province Name (full name) []:Bangkok
Locality Name (eg, city) [Default City]:Bangkok
Organization Name (eg, company) [Default Company Ltd]:EGA
Organizational Unit Name (eg, section) []:EGA.Security
Common Name (eg, your name or your server's hostname) []:www.ega.or.th
Email Address []:contact@ega.or.th
```

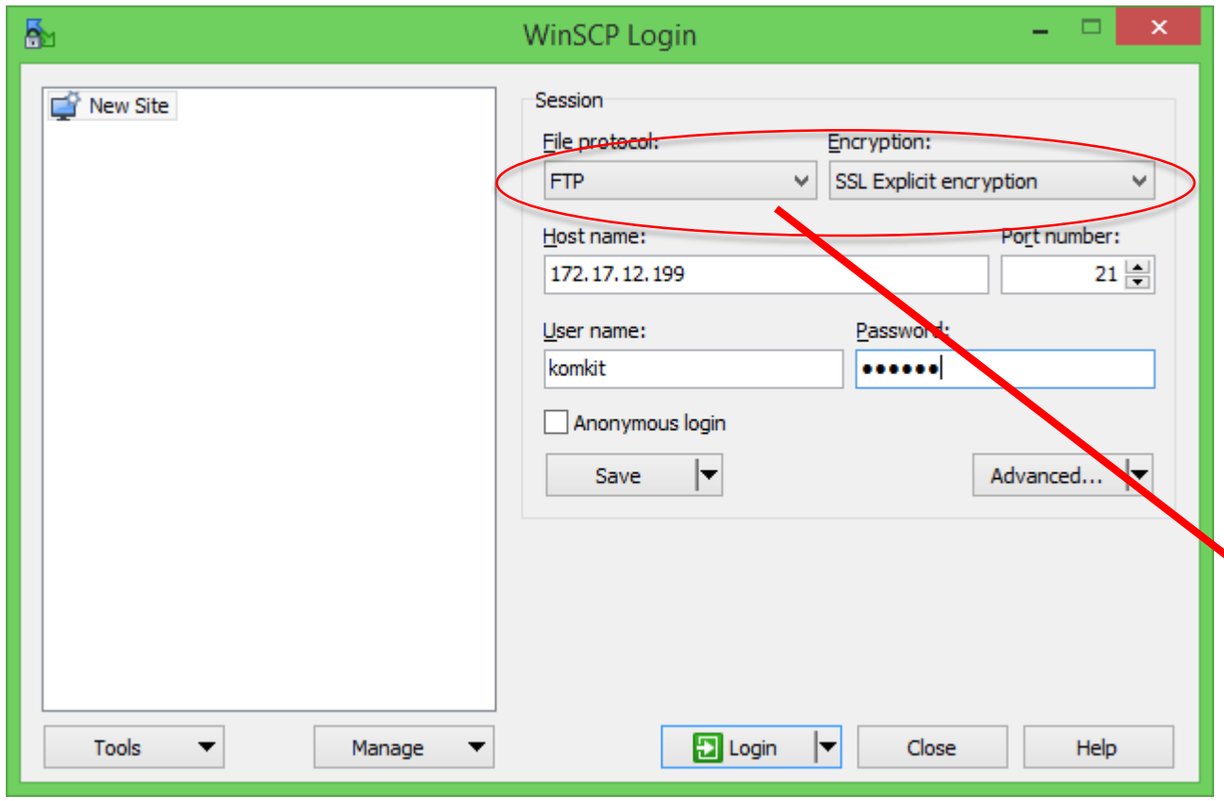
vsftpd with SSL

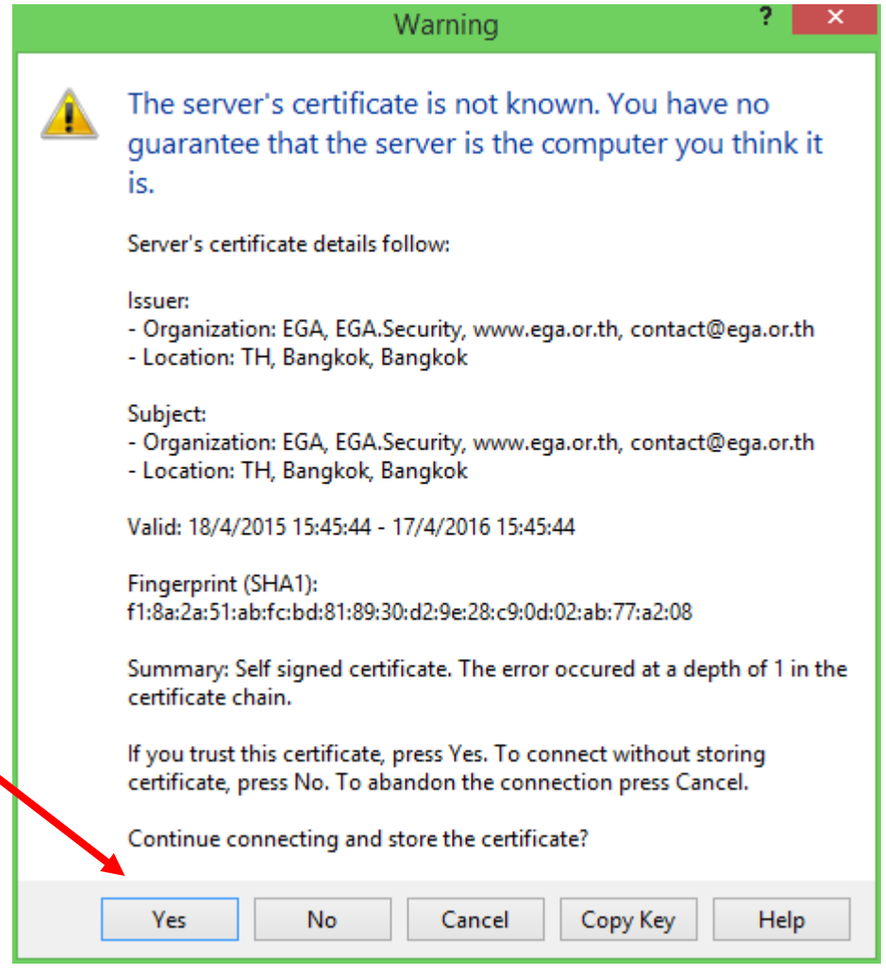
! แก้ไขไฟล์ **/etc/vsftpd/vsftpd.conf** เพิ่มแถวต่อไปนี้

```
ssl_enable=YES
rsa_cert_file=/etc/vsftpd/vsftpd.pem
rsa_private_key_file=/etc/vsftpd/vsftpd.pem
allow_anon_ssl=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=YES
ssl_sslv3=YES
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

vsftpd with SSL

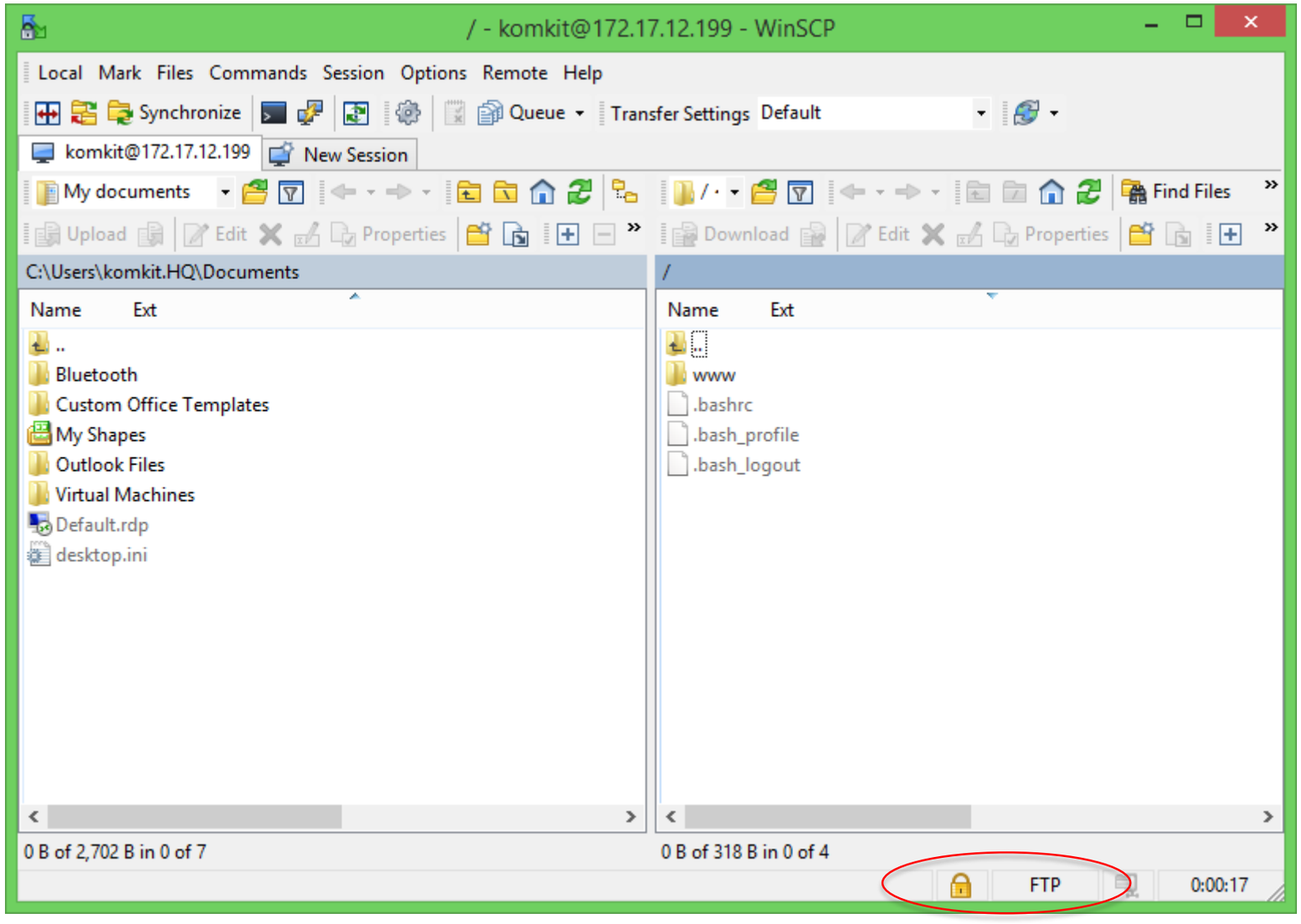
! ทดสอบการใช้งานผ่าน SSL





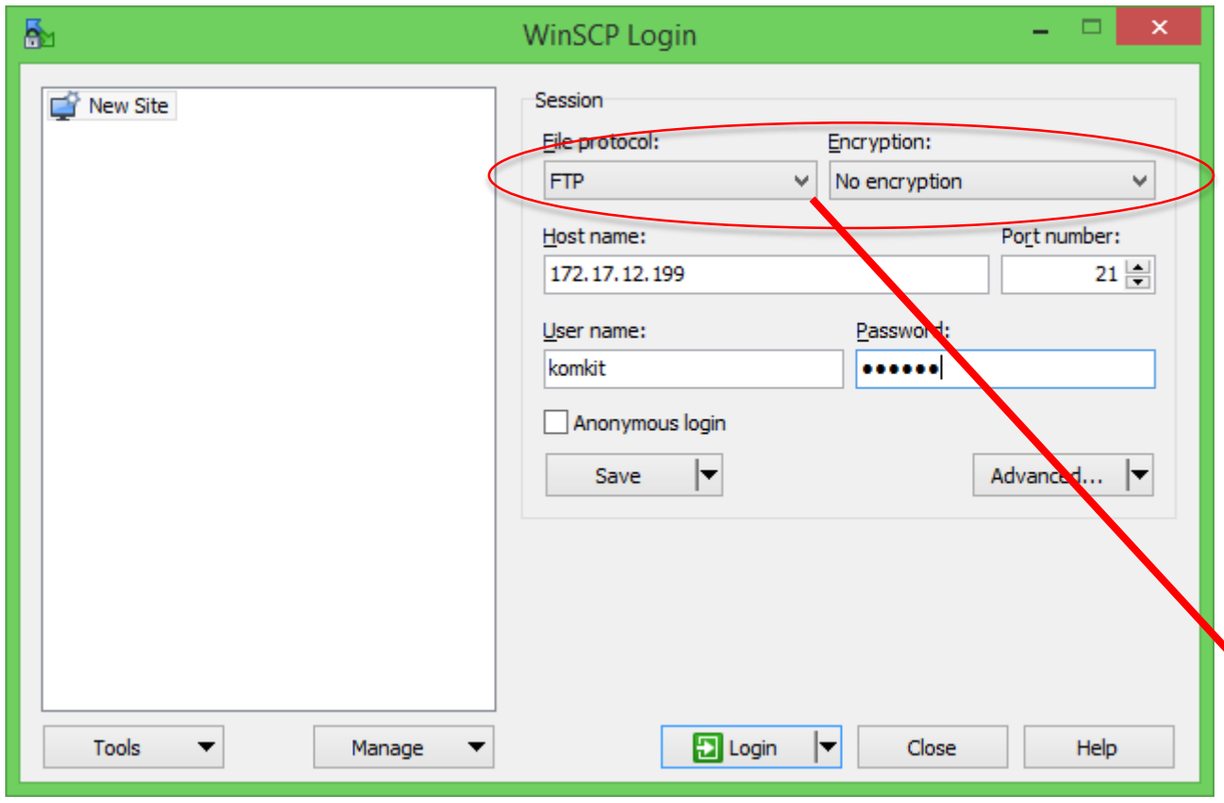
vsftpd with SSL

! ทดสอบการใช้งานผ่าน SSL

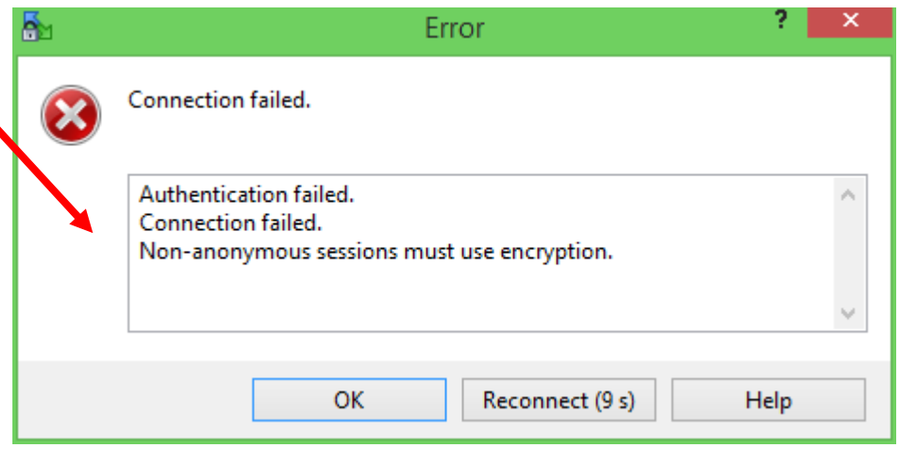


vsftpd with SSL

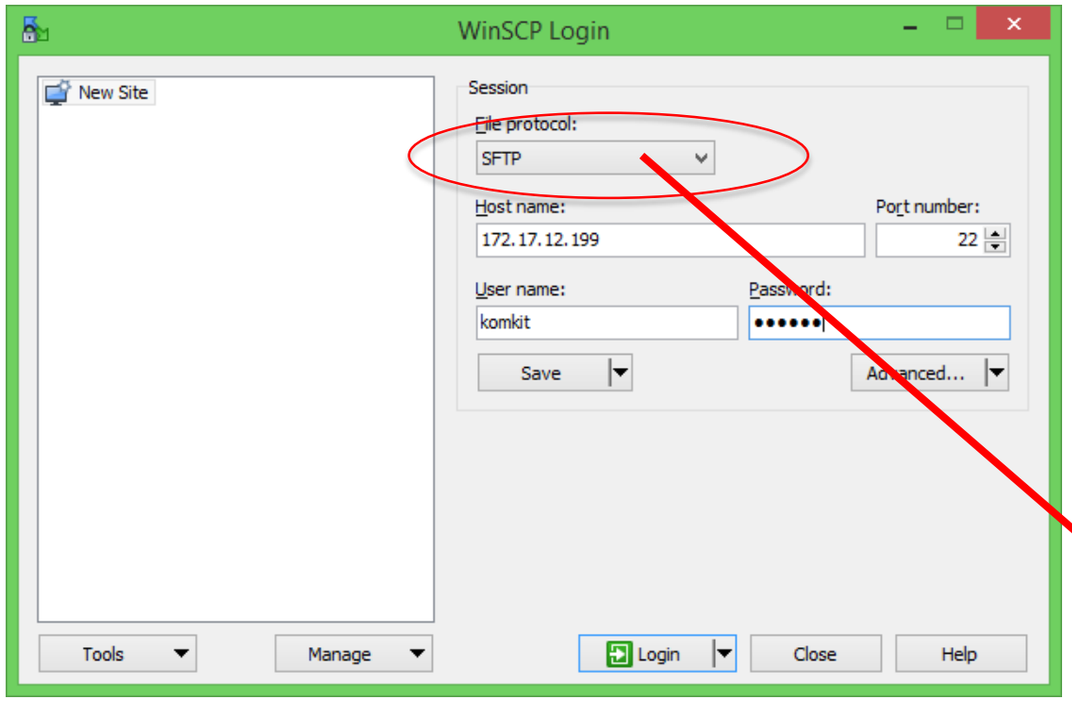
! ทดสอบใช้งานแบบไม่ผ่าน SSL

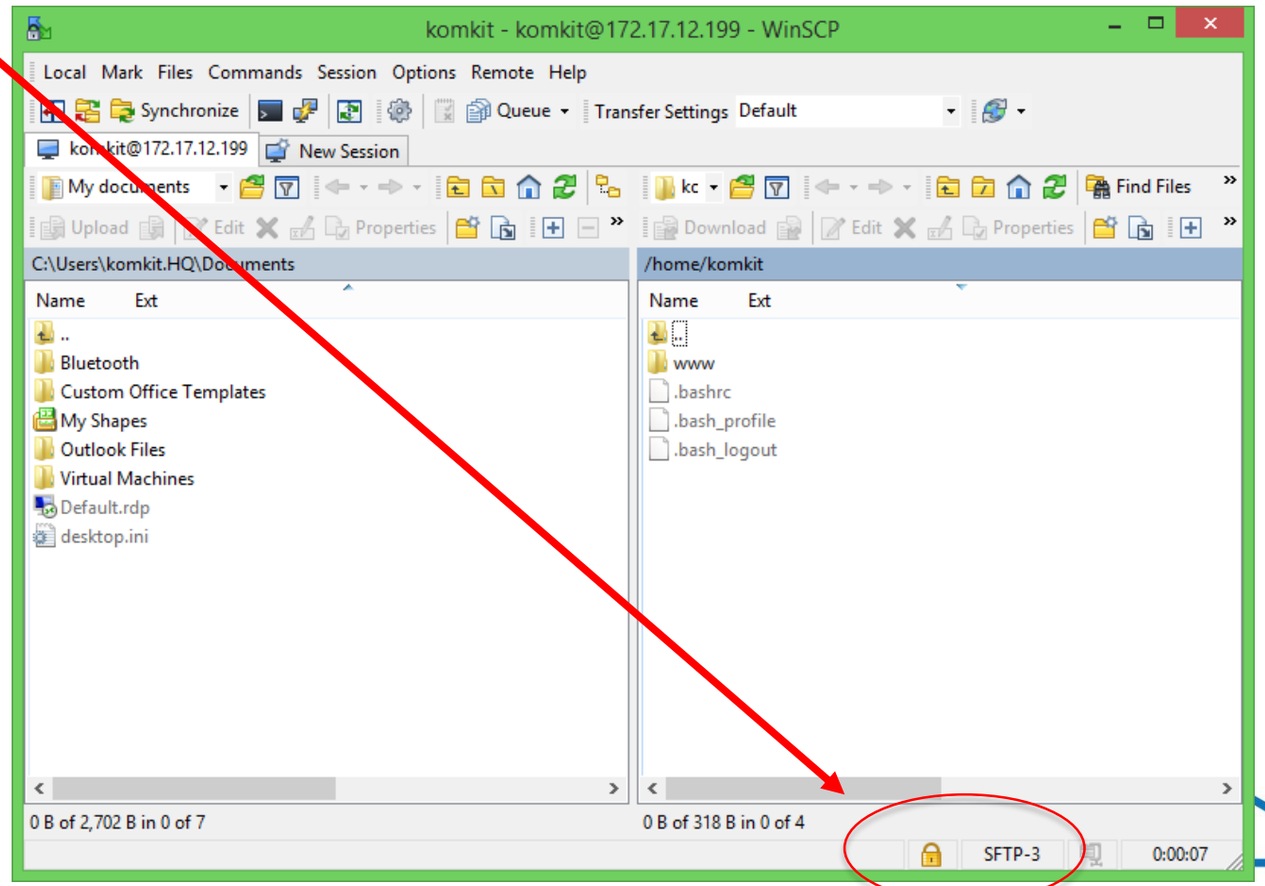



```
X:\>ftp  172.17.12.199
Connected to 172.17.12.199.
220 Authorized person only!
User (172.17.12.199:(none)): komkit
530 Non-anonymous sessions must use encryption.
Login failed.
ftp>
```

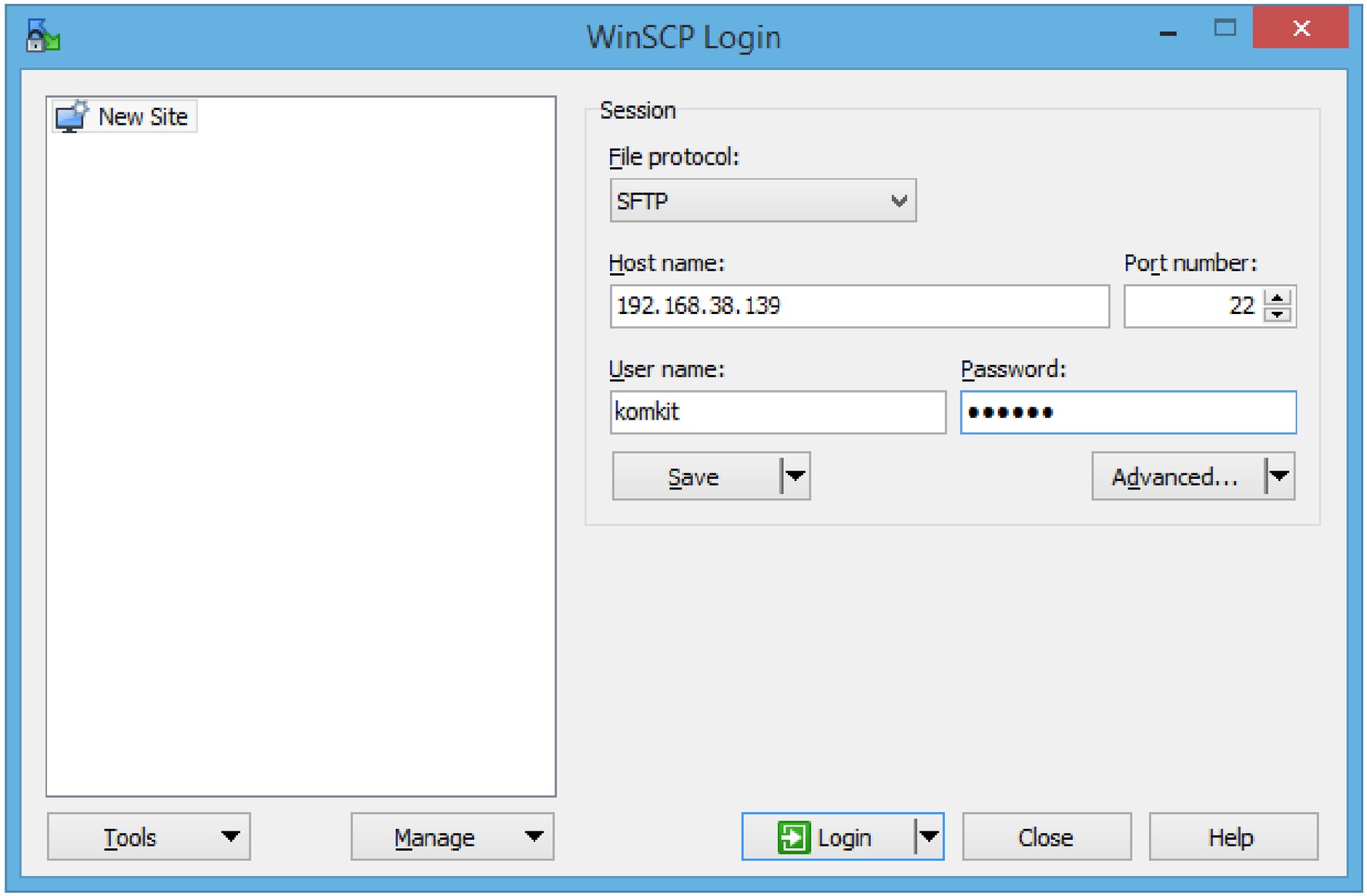


SFTP by OpenSSH

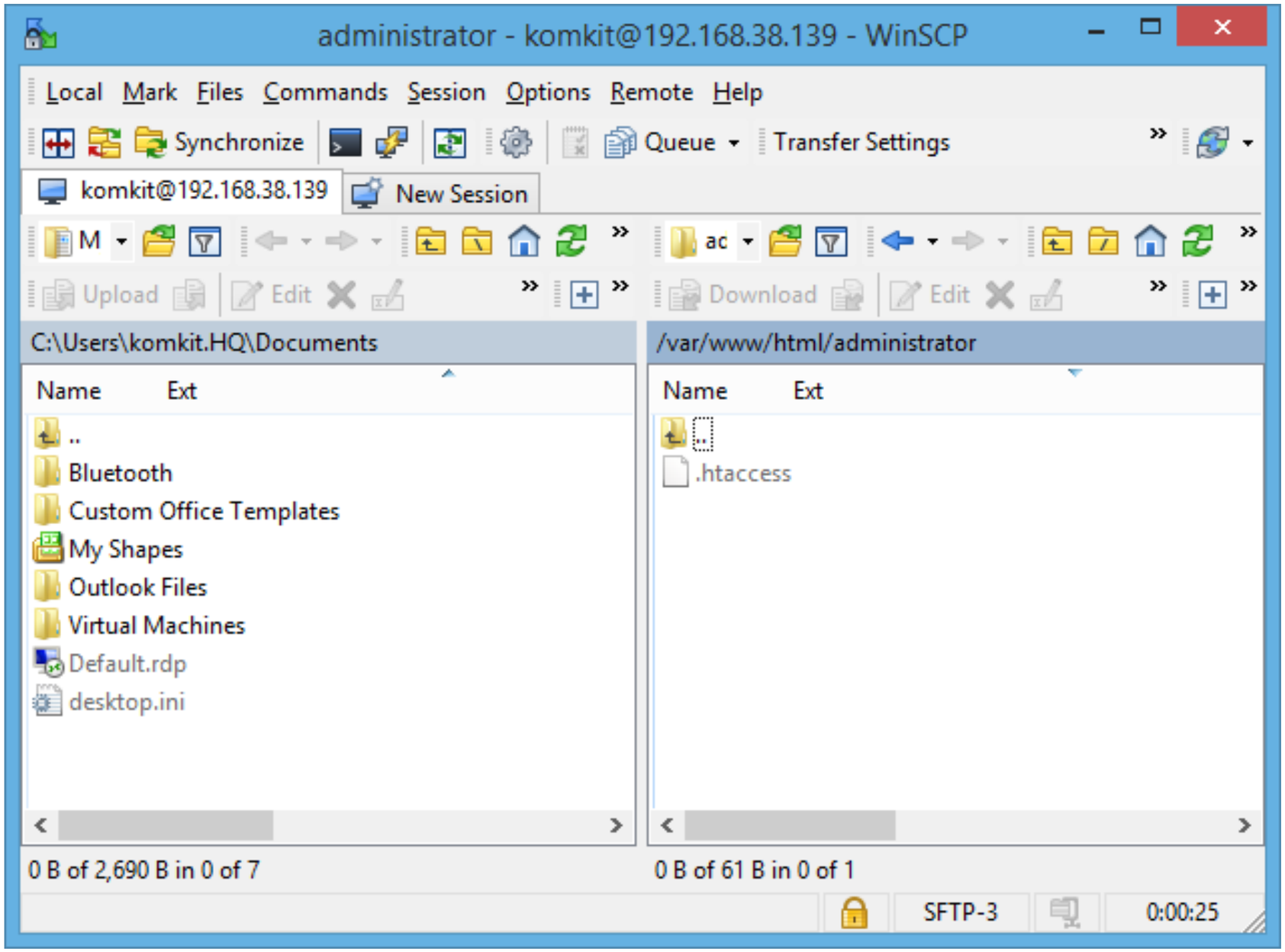




การใช้งาน SSH ในการ SFTP



การใช้งาน SSH ในการ SFTP



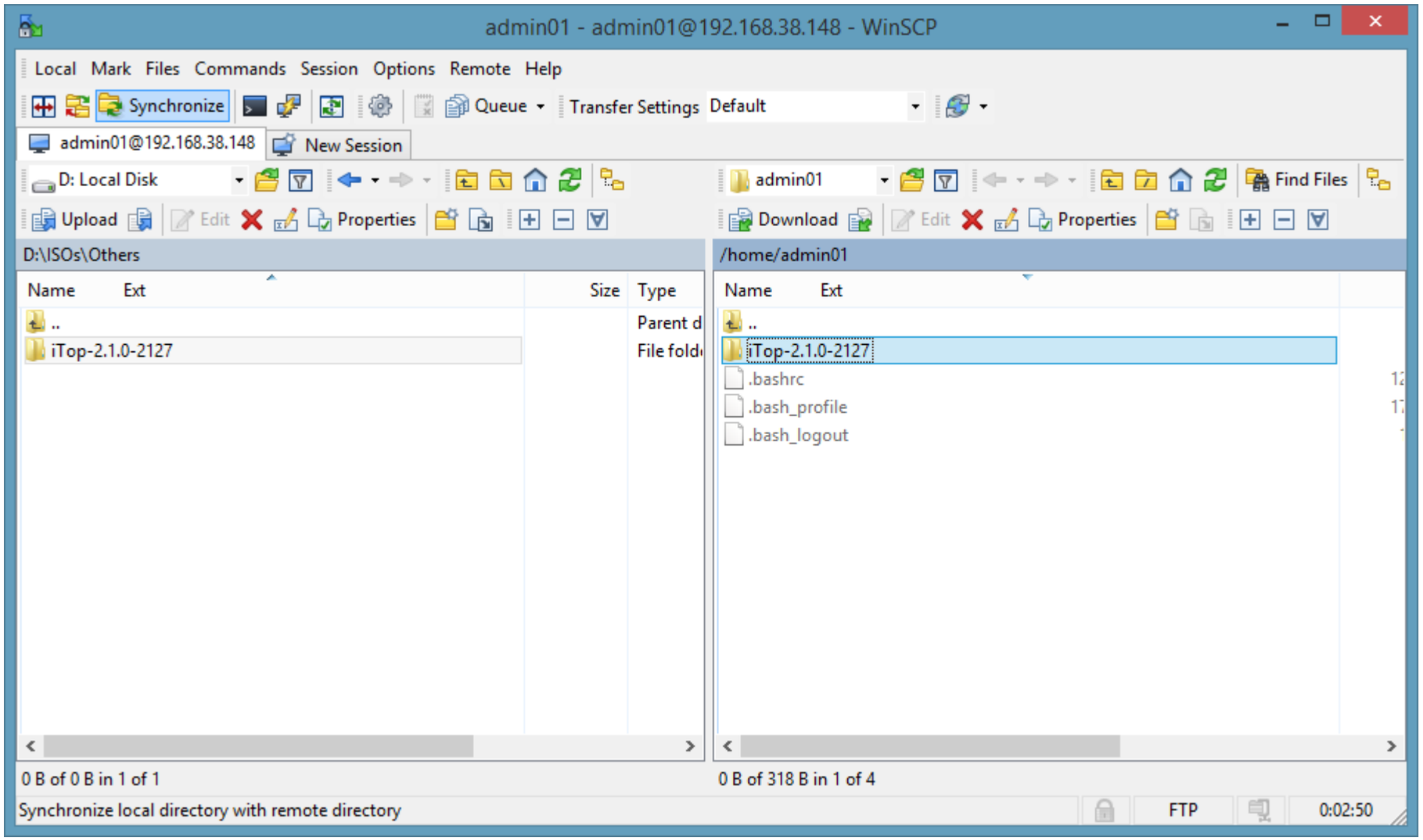
Hands-on LAB

iTop

- iTop (http://www.combodo.com/-Overview-.html)

iTop

- Upload iTop ไปยัง Web server โดย FTP



iTop

- ทำการ Copy โฟล์เดอร์ web ใน iTop ไปยัง /var/www/html/itop

```
[root@Server ~]# cp -rv /home/admin01/iTop-2.1.0-2127/web /var/www/html/itop/
```

- แก้ owner ของไฟล์ให้เป็น apache

```
[root@Server ~]# chown apache:apache -R /var/www/html/itop
```

- ติดตั้ง PHP extendtion พื้นฐานที่จำเป็น

```
[root@Server ~]# yum -y install php-dom php-soap php-ldap
```

```
[root@Server ~]# service httpd restart
```

- เพิ่ม Options ให้ MySQL server โดยแก้ไขเข้าไปที่ไฟล์ **/etc/my.cnf** ดังนี้

```
[mysqld]
max_allowed_packet=2097652
```

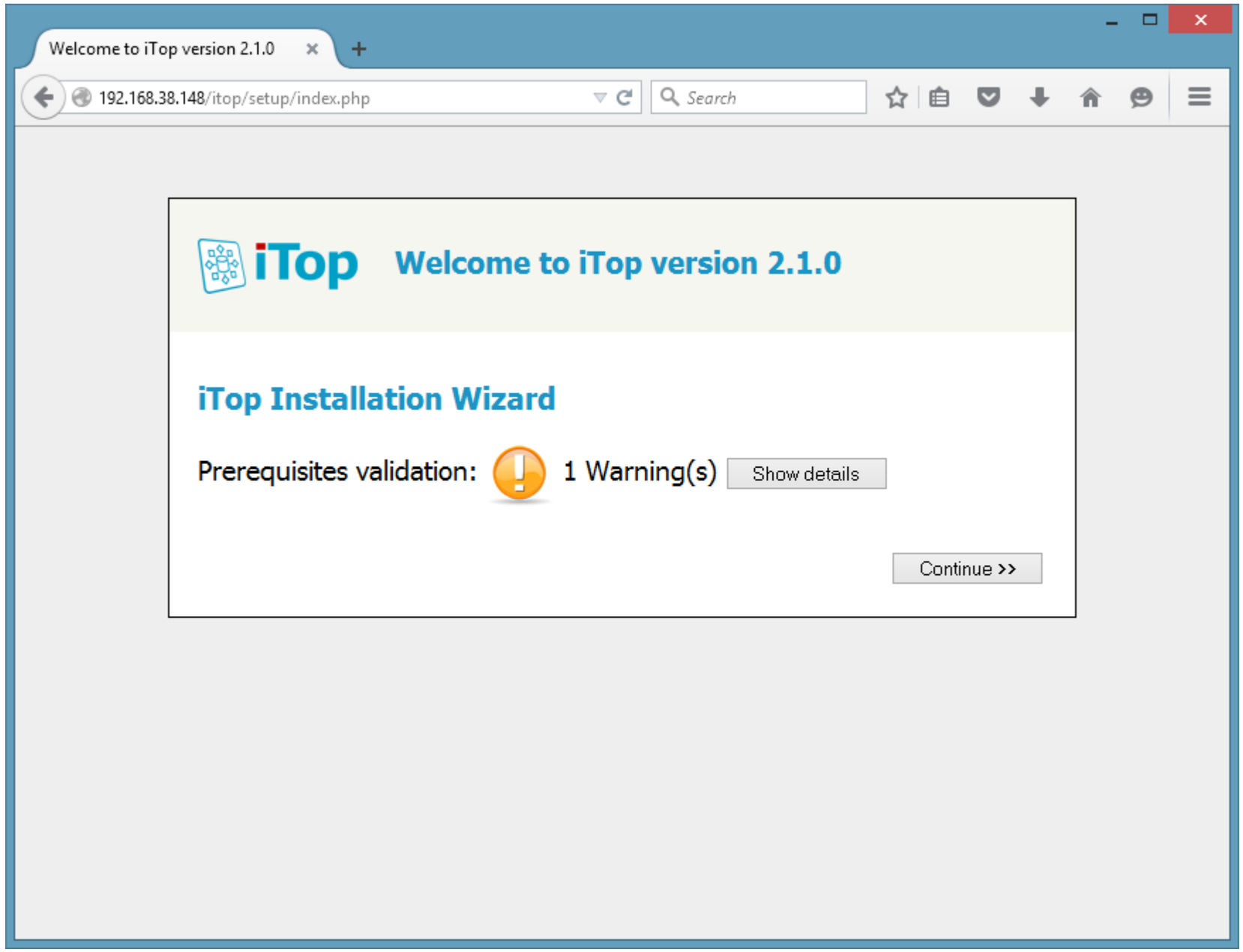
จากนั้นใช้คำสั่ง **service mysqld restart**

iTop

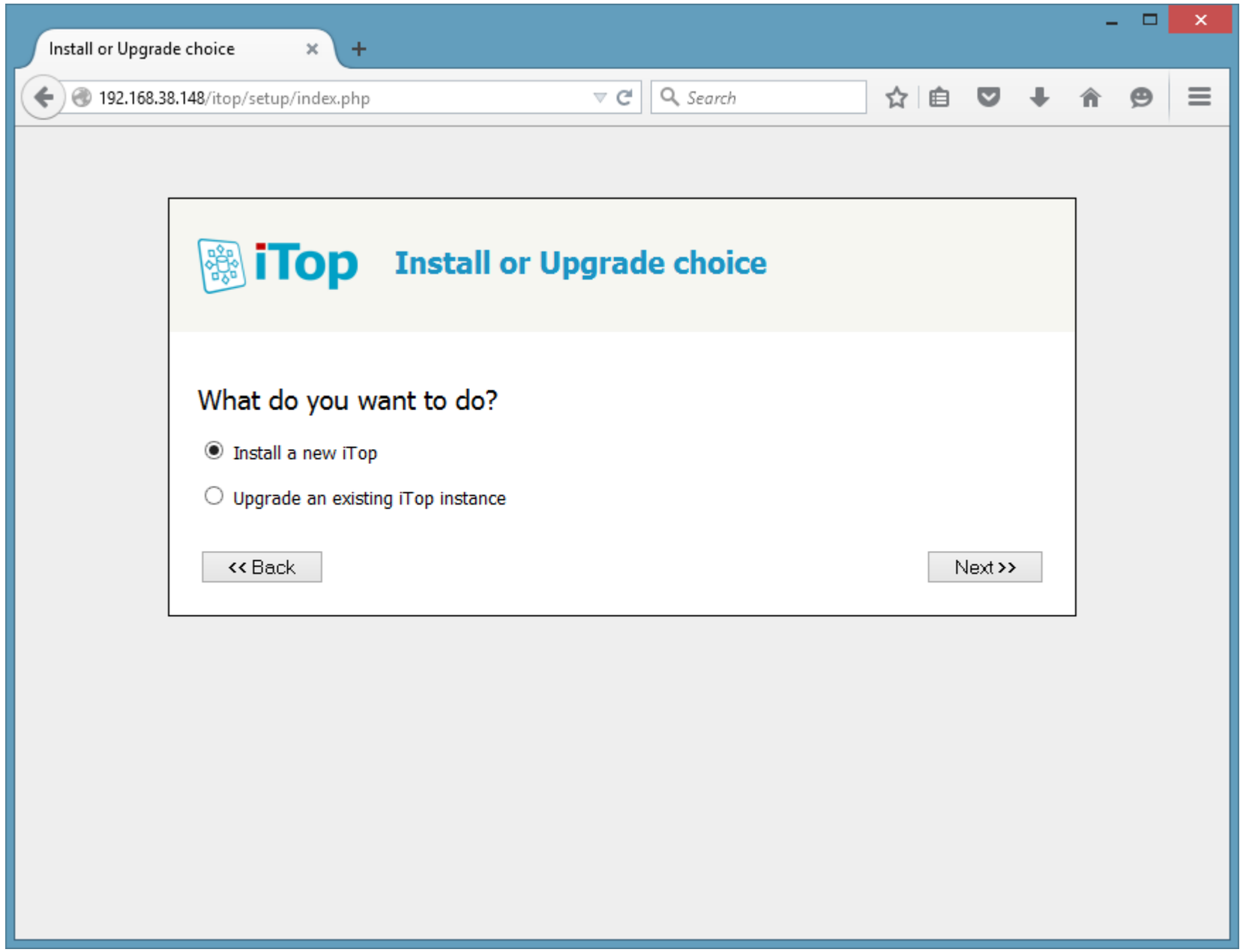
- สร้าง Database สำหรับ iTop

```
[root@Server ~]# mysql -u root -p
Enter password:
mysql>
mysql> create database itop;
Query OK, 1 row affected (0.00 sec)

mysql> grant all on itop.* to "itopuser"@"localhost" identified by "itoppassword";
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
```

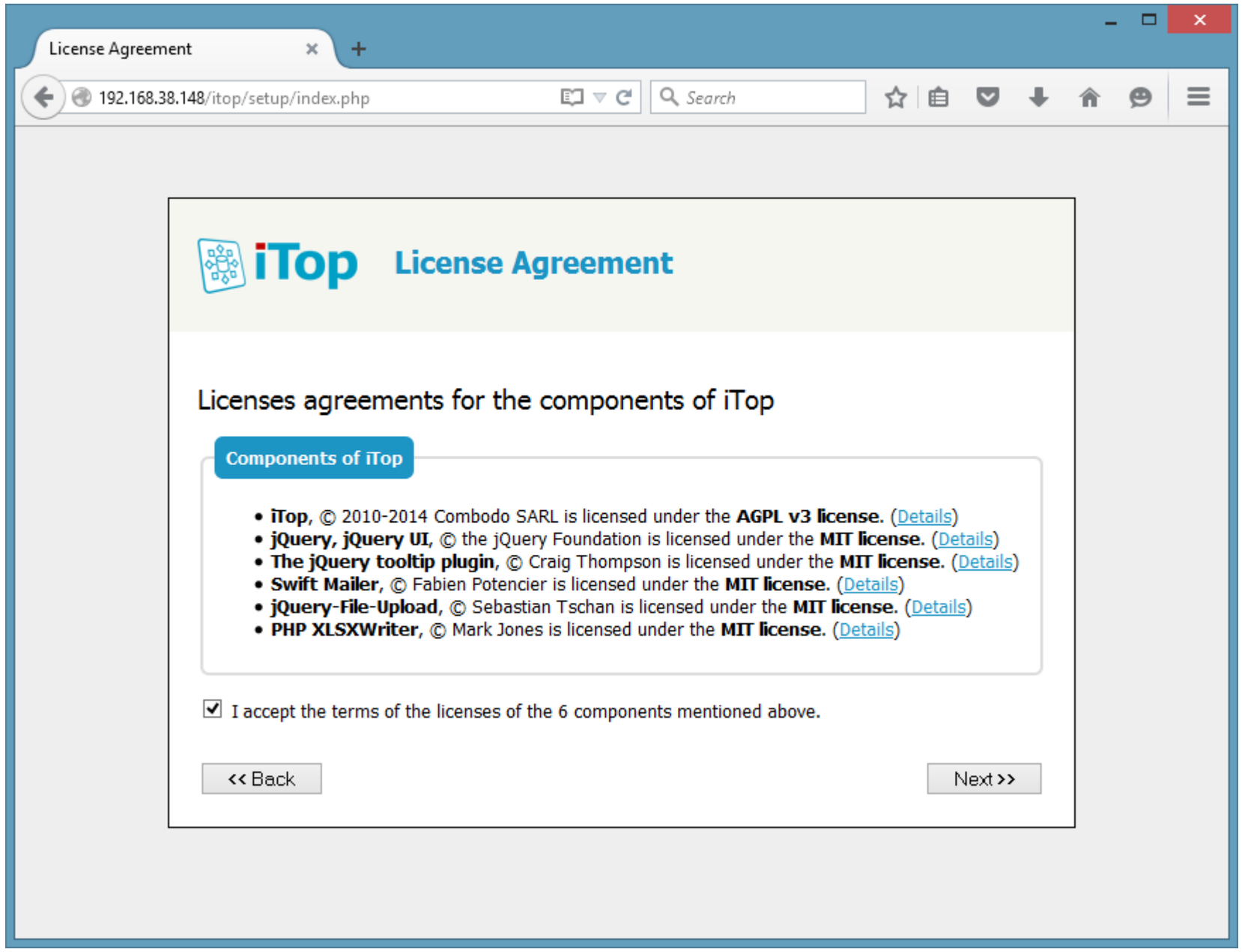
iTop


Welcome to iTop version 2.1.0
192.168.38.148/itop/setup/index.php
Search
iTop
Welcome to iTop version 2.1.0
iTop Installation Wizard
Prerequisites validation:
1 Warning(s)
Show details
Continue >>

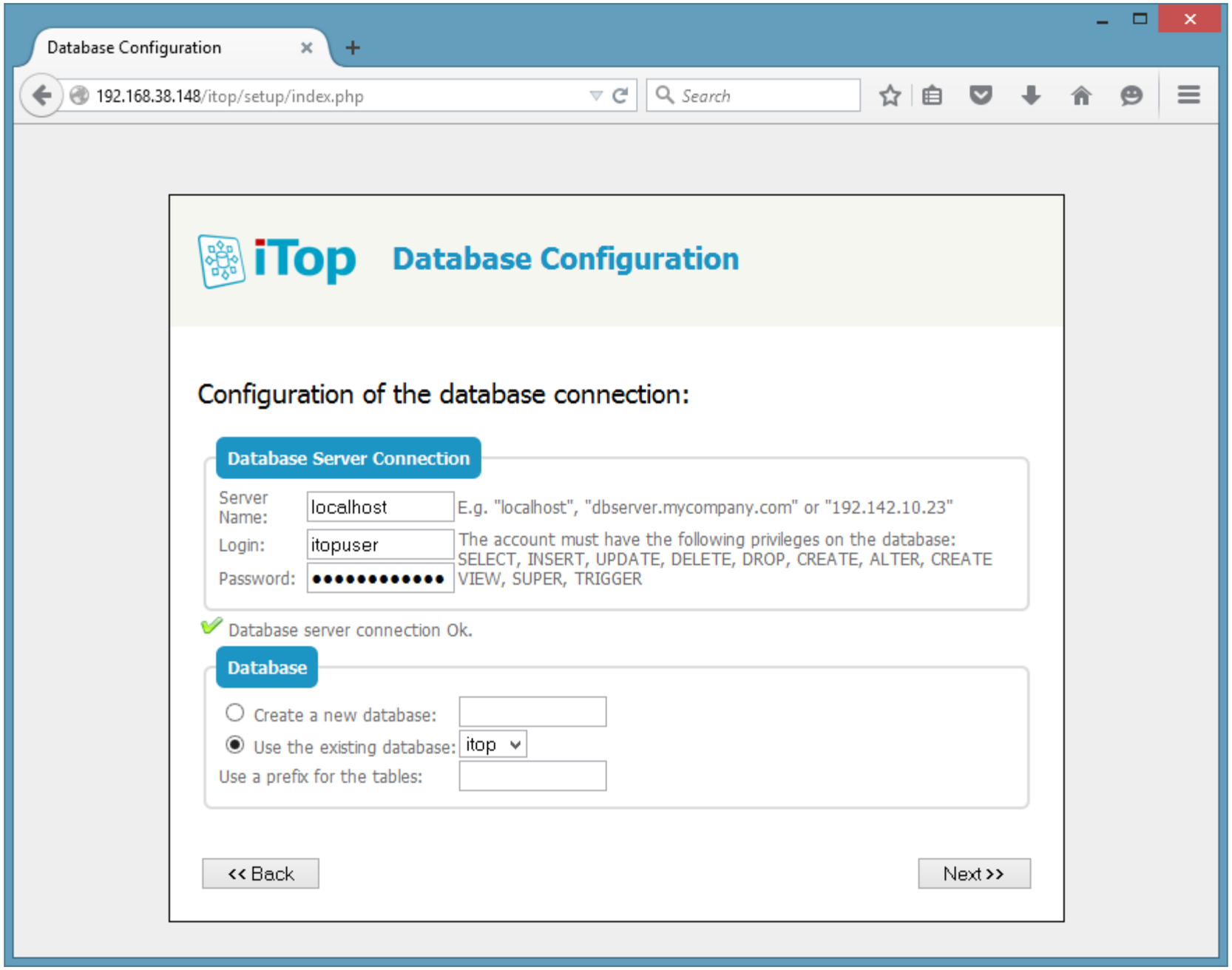
iTop


Install or Upgrade choice
192.168.38.148/itop/setup/index.php
Search
iTop
Install or Upgrade choice
What do you want to do?
Install a new iTop
Upgrade an existing iTop instance
<< Back
Next >>

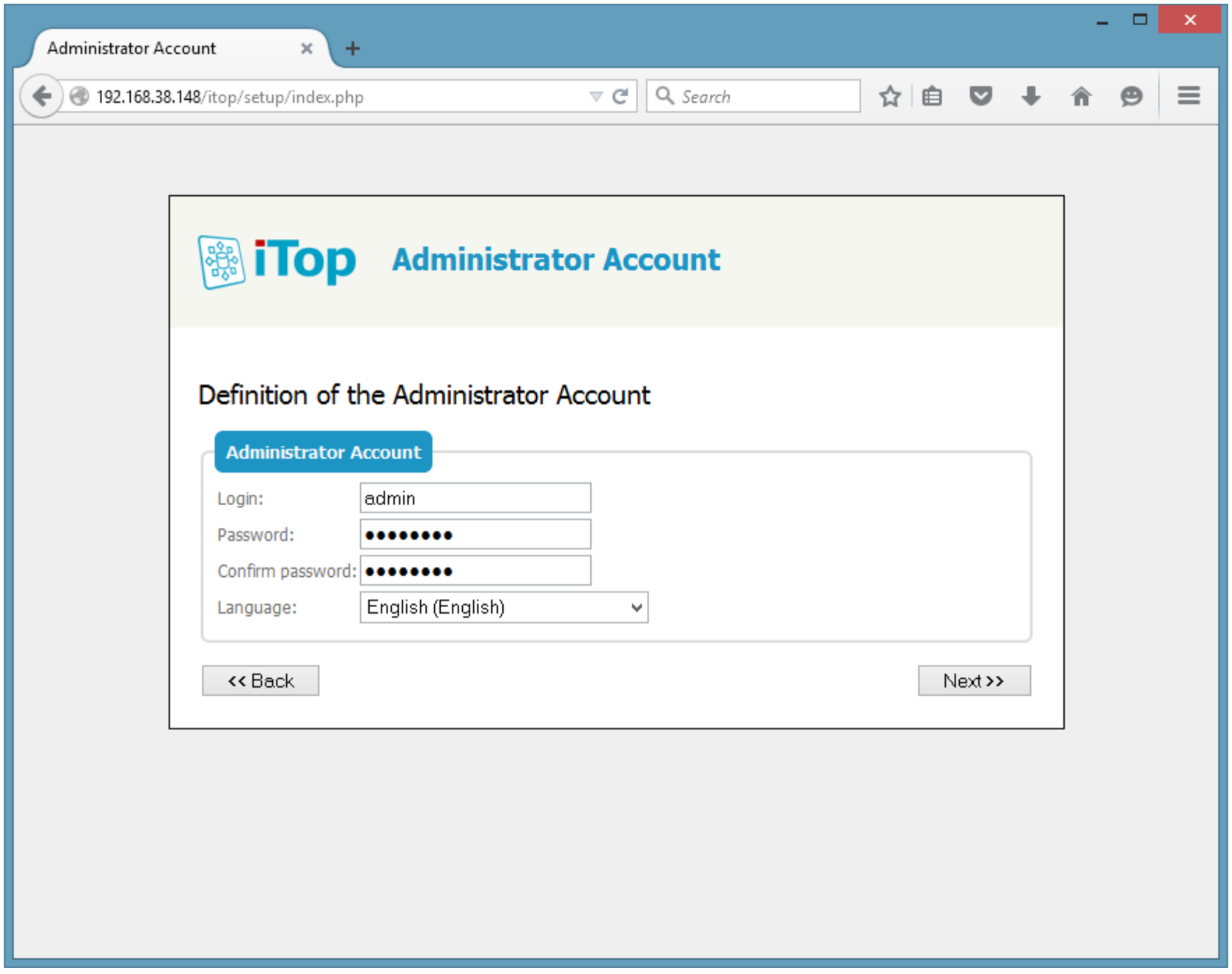
iTop


License Agreement
192.168.38.148/itop/setup/index.php
Search
iTop
License Agreement
Licenses agreements for the components of iTop
Components of iTop
• iTop, © 2010-2014 Combodo SARL is licensed under the AGPL v3 license. (Details)
• jQuery, jQuery UI, © the jQuery Foundation is licensed under the MIT license. (Details)
• The jQuery tooltip plugin, © Craig Thompson is licensed under the MIT license. (Details)
• Swift Mailer, © Fabien Potencier is licensed under the MIT license. (Details)
• jQuery-File-Upload, © Sebastian Tschan is licensed under the MIT license. (Details)
• PHP XLSXWriter, © Mark Jones is licensed under the MIT license. (Details)
I accept the terms of the licenses of the 6 components mentioned above.
<< Back
Next >>

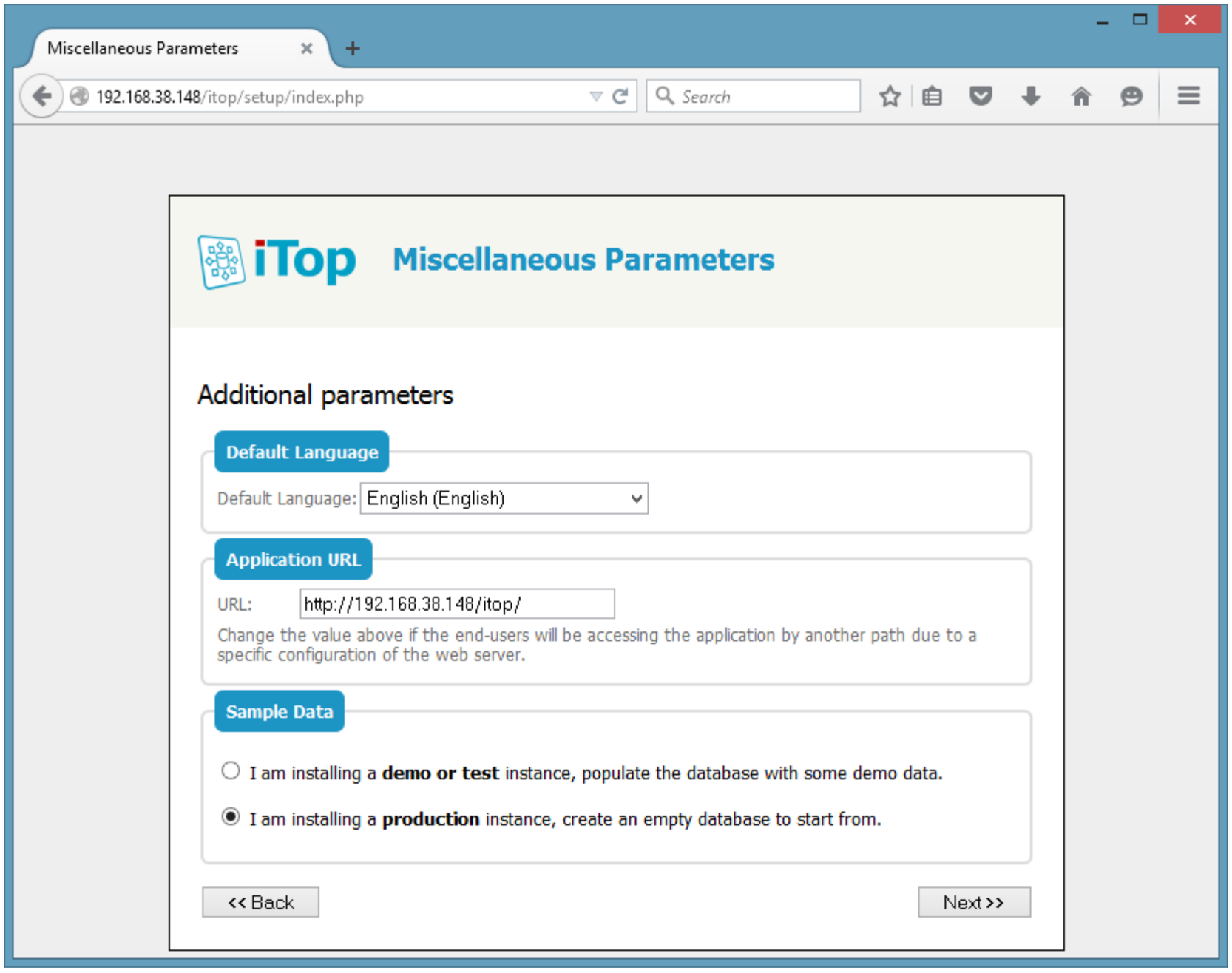
iTop


Database Configuration
192.168.38.148/itop/setup/index.php
Search
iTop
Database Configuration
Configuration of the database connection:
Database Server Connection
Server Name:
localhost
E.g. "localhost", "dbserver.mycompany.com" or "192.142.10.23"
Login:
itopuser
Password:
The account must have the following privileges on the database: SELECT, INSERT, UPDATE, DELETE, DROP, CREATE, ALTER, CREATE VIEW, SUPER, TRIGGER
Database server connection Ok.
Database
Create a new database:
Use the existing database:
itop
Use a prefix for the tables:
<< Back
Next >>

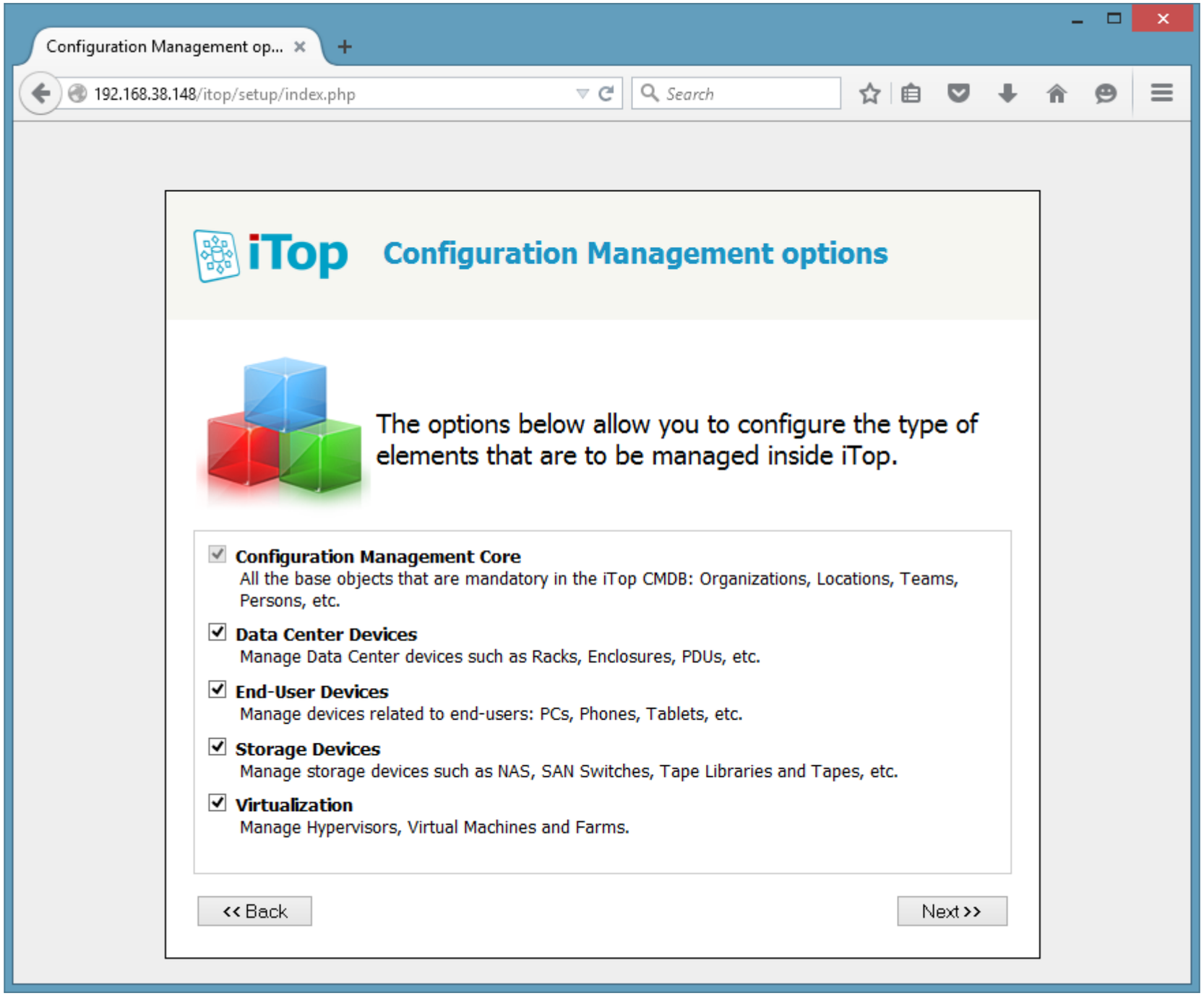
iTop


Administrator Account
192.168.38.148/itop/setup/index.php
Search
iTop
Administrator Account
Definition of the Administrator Account
Administrator Account
Login:
admin
Password:
Confirm password:
Language:
English (English)
<< Back
Next >>

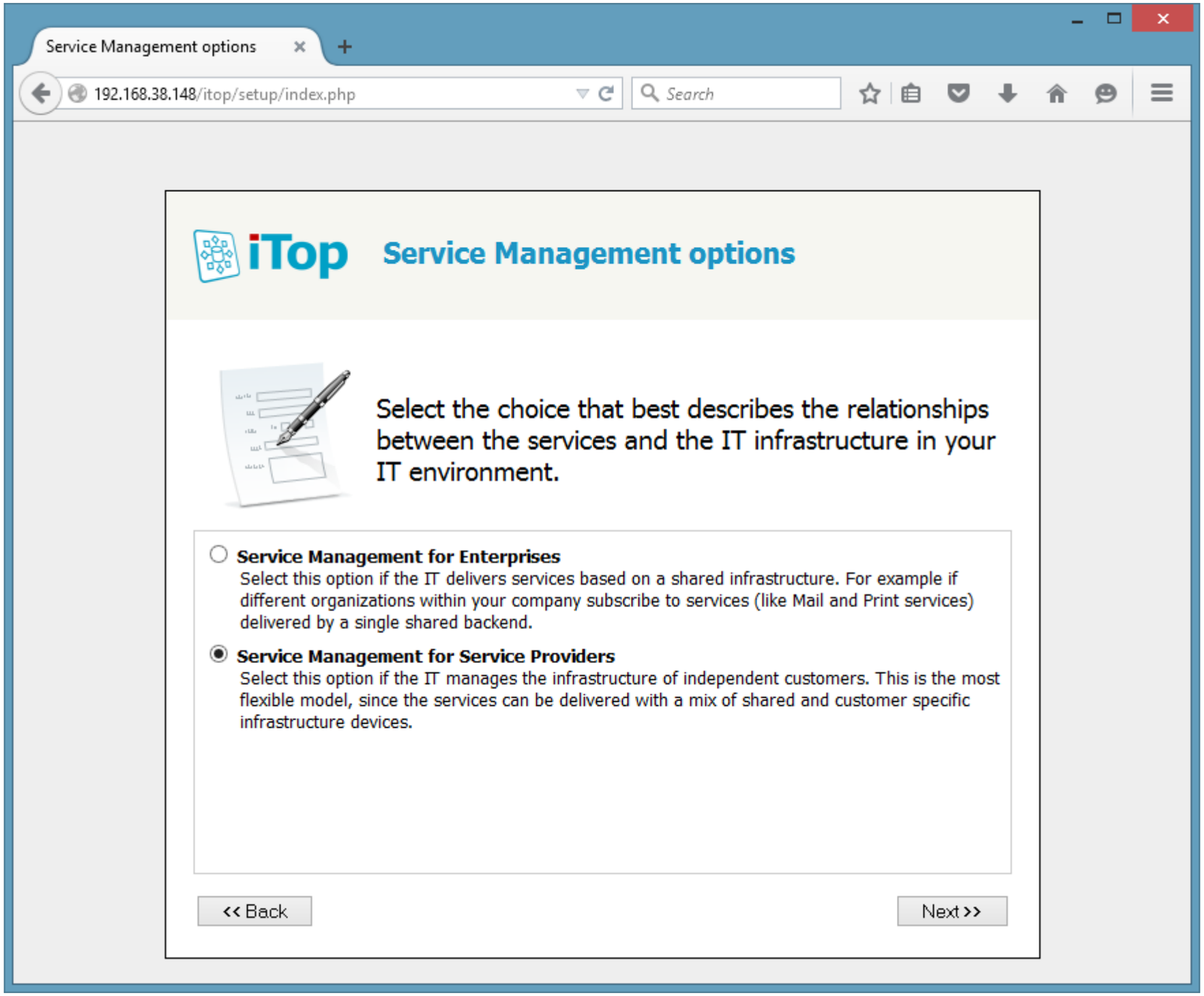
iTop


Miscellaneous Parameters
192.168.38.148/itop/setup/index.php
Search
iTop
Miscellaneous Parameters
Additional parameters
Default Language
Default Language: English (English)
Application URL
URL: http://192.168.38.148/itop/
Change the value above if the end-users will be accessing the application by another path due to a specific configuration of the web server.
Sample Data
I am installing a demo or test instance, populate the database with some demo data.
I am installing a production instance, create an empty database to start from.
<< Back
Next >>

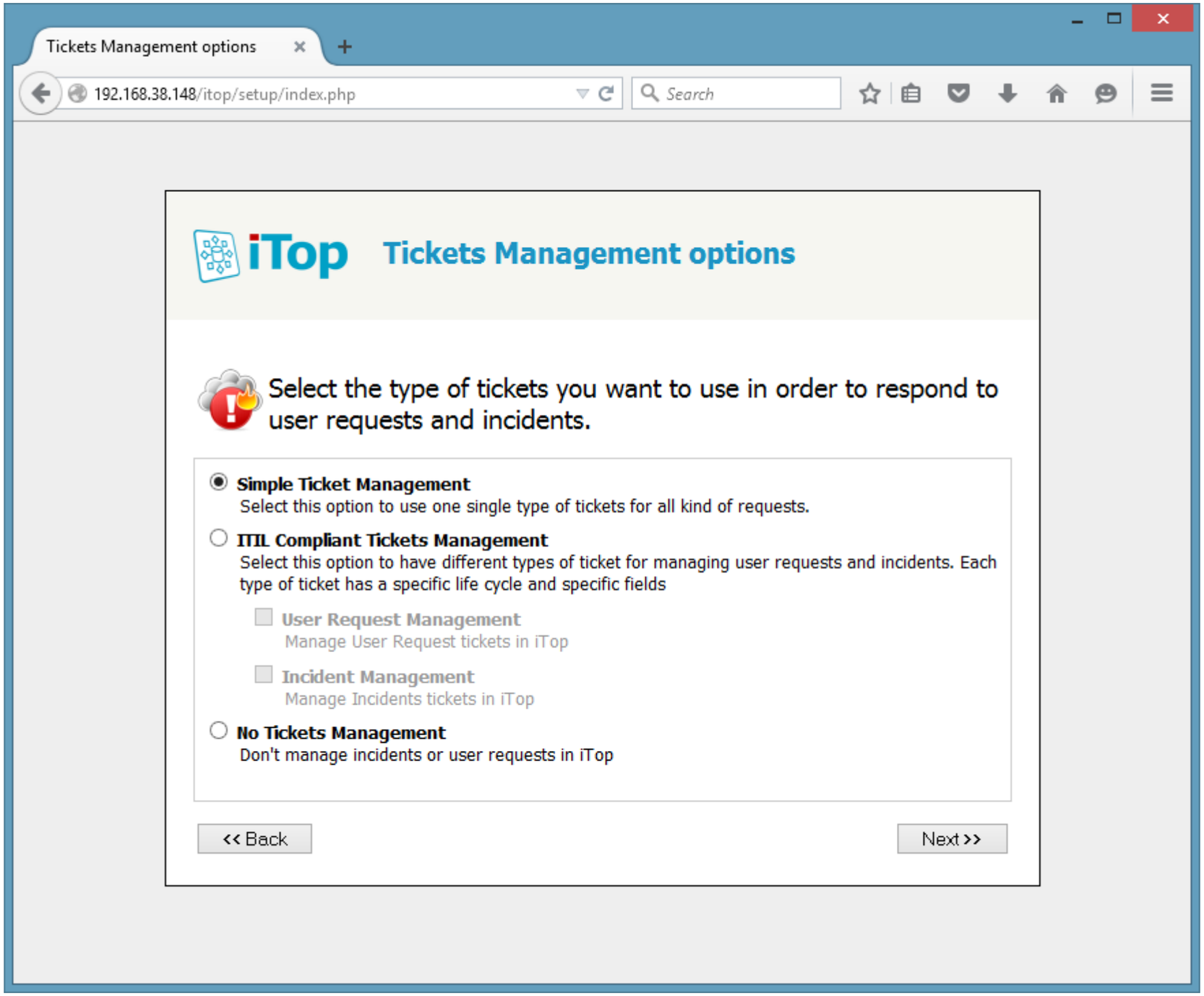
iTop


Configuration Management op...
192.168.38.148/itop/setup/index.php
Search
iTop
Configuration Management options
The options below allow you to configure the type of elements that are to be managed inside iTop.
Configuration Management Core
All the base objects that are mandatory in the iTop CMDB: Organizations, Locations, Teams, Persons, etc.
Data Center Devices
Manage Data Center devices such as Racks, Enclosures, PDUs, etc.
End-User Devices
Manage devices related to end-users: PCs, Phones, Tablets, etc.
Storage Devices
Manage storage devices such as NAS, SAN Switches, Tape Libraries and Tapes, etc.
Virtualization
Manage Hypervisors, Virtual Machines and Farms.
<< Back
Next >>

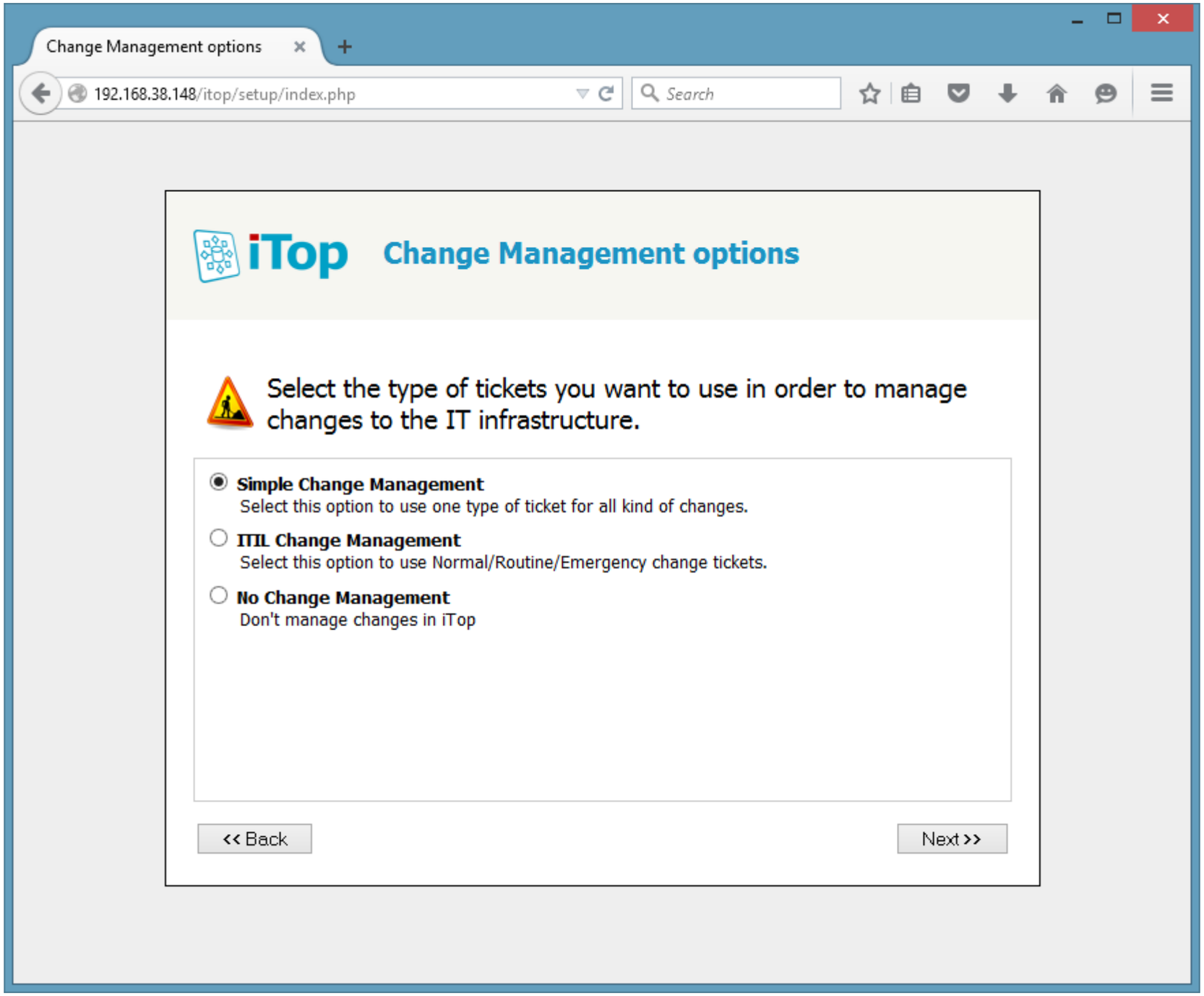
iTop


Service Management options
192.168.38.148/itop/setup/index.php
Search
iTop
Service Management options
Select the choice that best describes the relationships between the services and the IT infrastructure in your IT environment.
Service Management for Enterprises
Select this option if the IT delivers services based on a shared infrastructure. For example if different organizations within your company subscribe to services (like Mail and Print services) delivered by a single shared backend.
Service Management for Service Providers
Select this option if the IT manages the infrastructure of independent customers. This is the most flexible model, since the services can be delivered with a mix of shared and customer specific infrastructure devices.
<< Back
Next >>

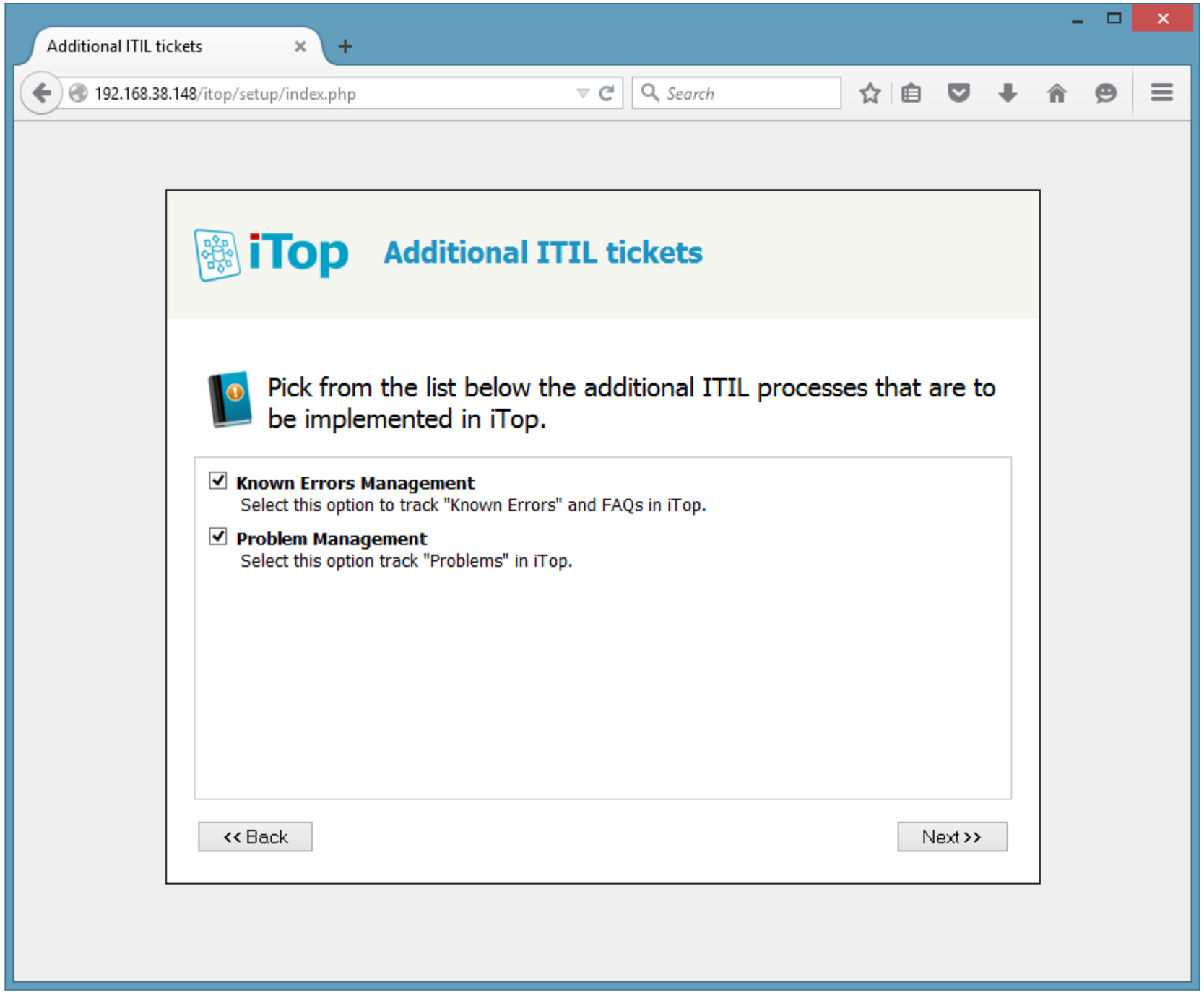
iTop


Tickets Management options
192.168.38.148/itop/setup/index.php
Search
iTop
Tickets Management options
Select the type of tickets you want to use in order to respond to user requests and incidents.
Simple Ticket Management
Select this option to use one single type of tickets for all kind of requests.
ITIL Compliant Tickets Management
Select this option to have different types of ticket for managing user requests and incidents. Each type of ticket has a specific life cycle and specific fields
User Request Management
Manage User Request tickets in iTop
Incident Management
Manage Incidents tickets in iTop
No Tickets Management
Don't manage incidents or user requests in iTop
<< Back
Next >>

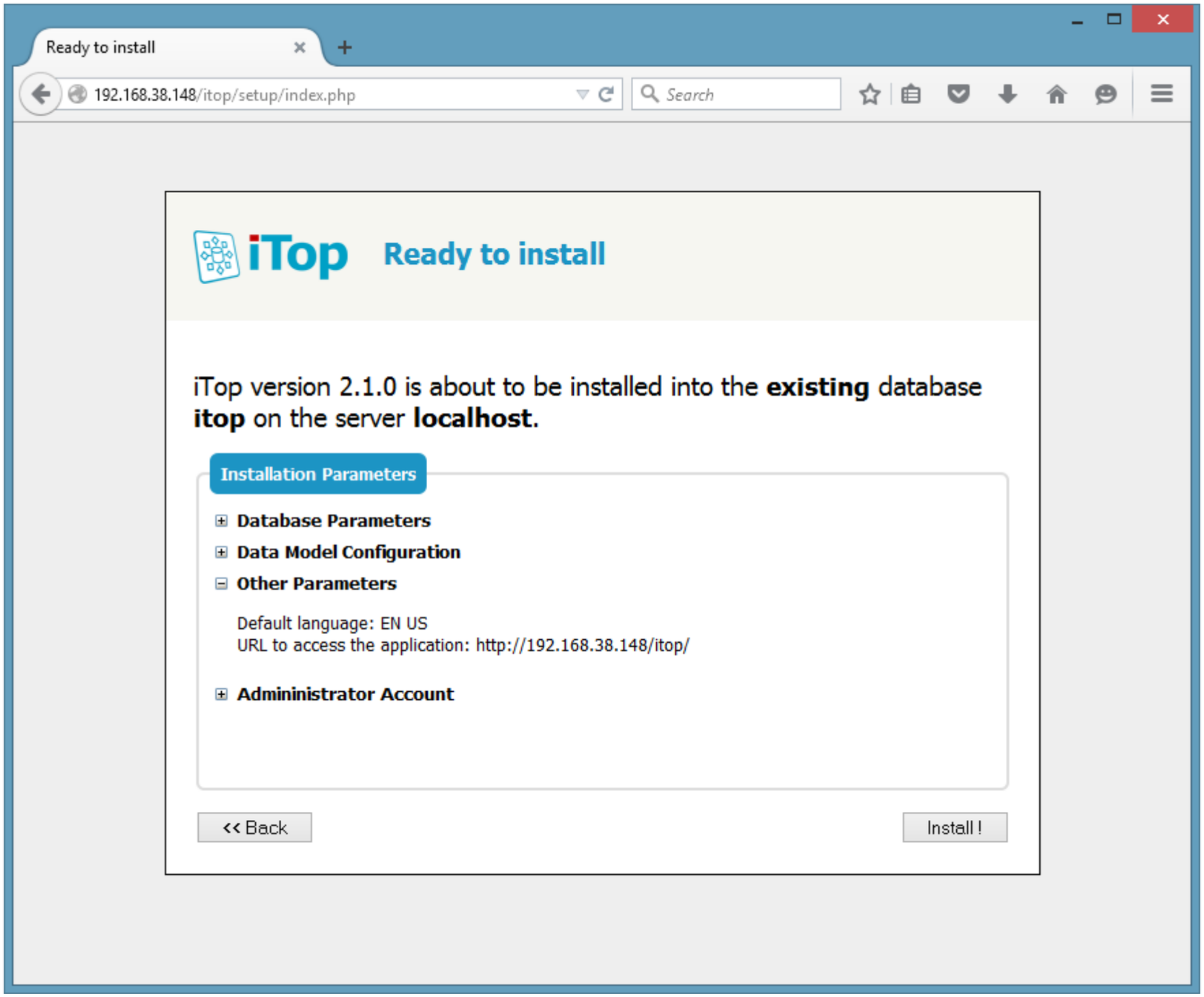
iTop


Change Management options
192.168.38.148/itop/setup/index.php
Search
iTop
Change Management options
Select the type of tickets you want to use in order to manage changes to the IT infrastructure.
Simple Change Management
Select this option to use one type of ticket for all kind of changes.
ITIL Change Management
Select this option to use Normal/Routine/Emergency change tickets.
No Change Management
Don't manage changes in iTop
<< Back
Next >>

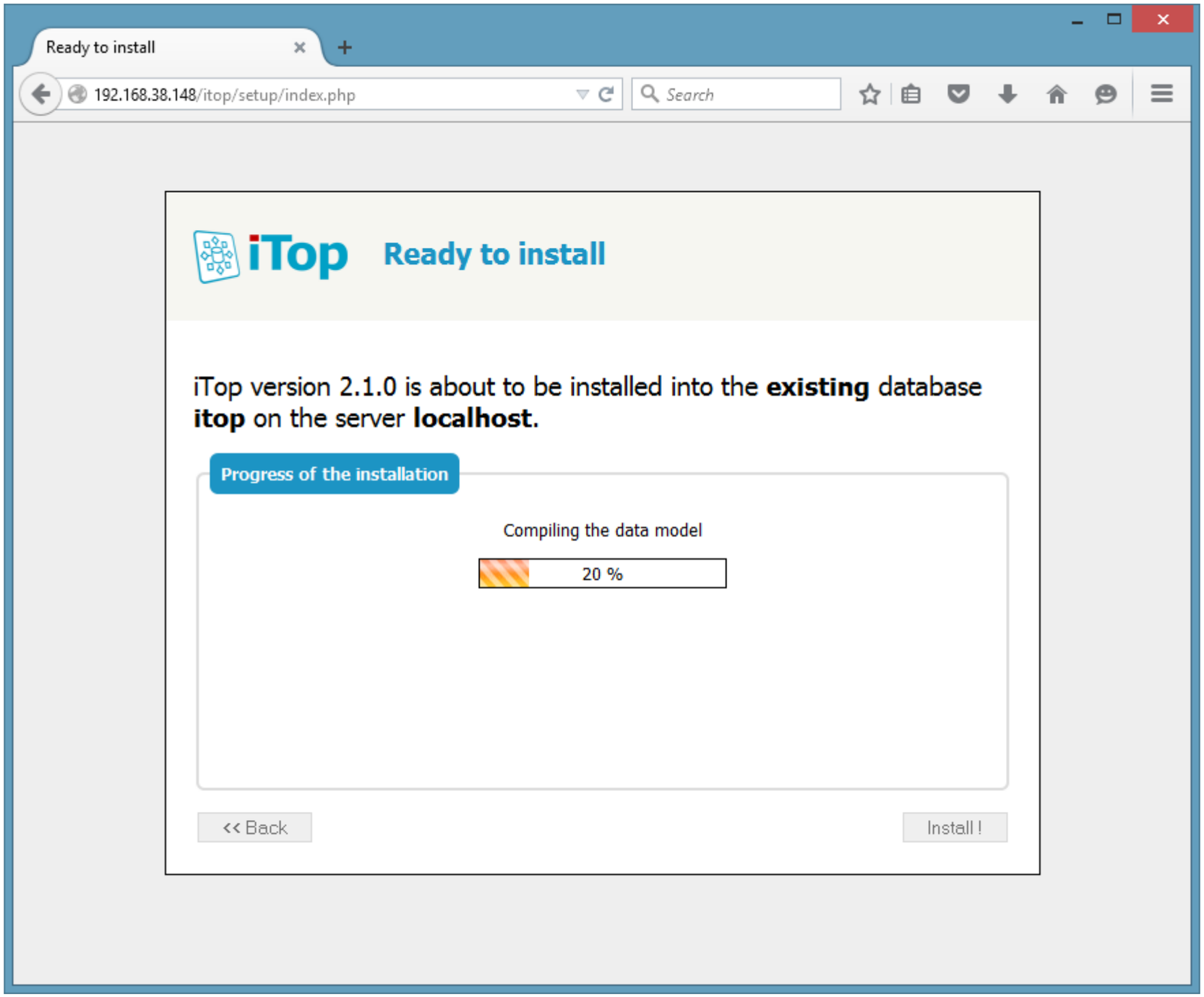
iTop


Additional ITIL tickets
192.168.38.148/itop/setup/index.php
Search
iTop
Additional ITIL tickets
Pick from the list below the additional ITIL processes that are to be implemented in iTop.
Known Errors Management
Select this option to track "Known Errors" and FAQs in iTop.
Problem Management
Select this option track "Problems" in iTop.
<< Back
Next >>

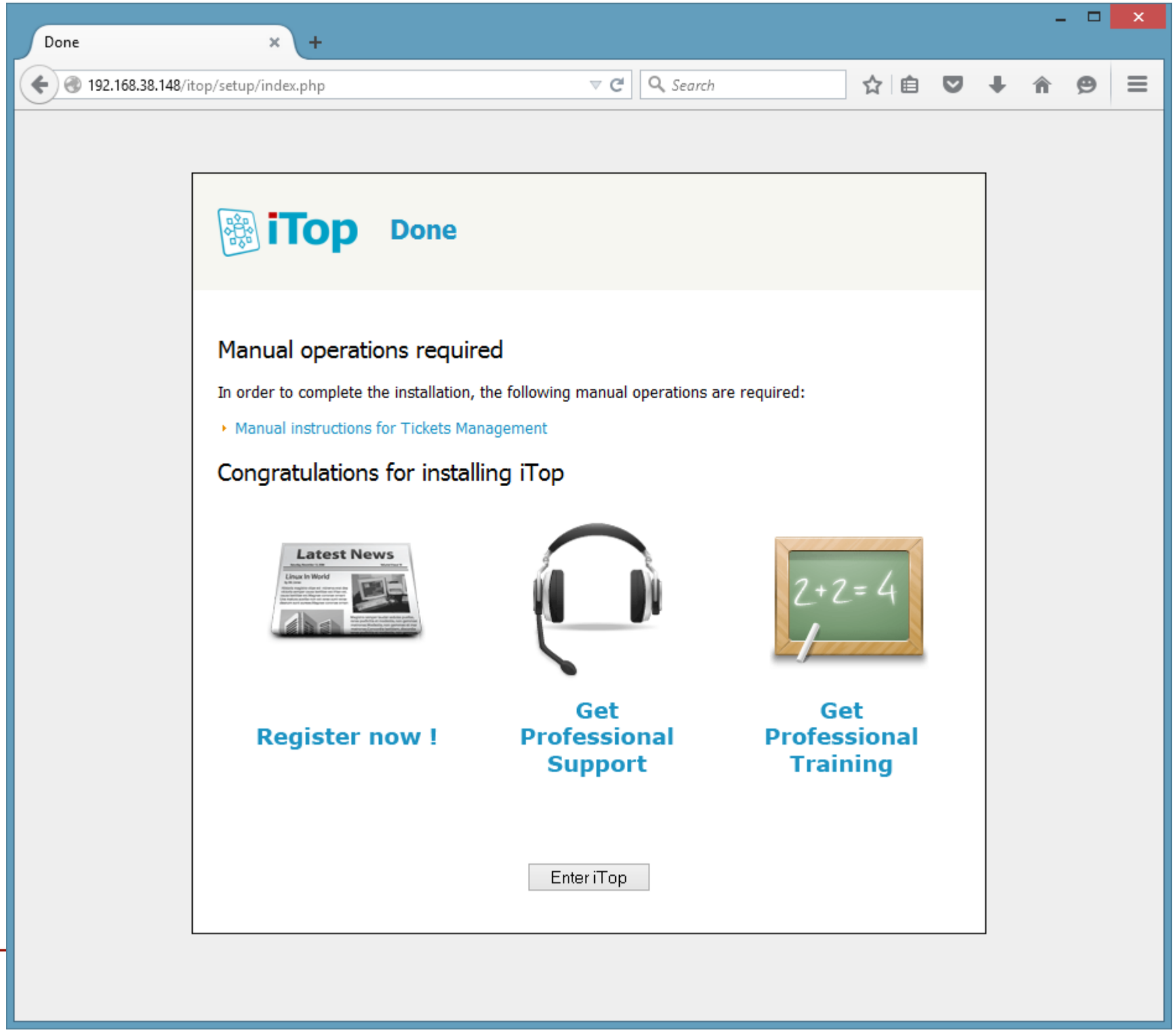
iTop


Ready to install
192.168.38.148/itop/setup/index.php
Search
iTop
Ready to install
iTop version 2.1.0 is about to be installed into the existing database itop on the server localhost.
Installation Parameters
Database Parameters
Data Model Configuration
Other Parameters
Default language: EN US
URL to access the application: http://192.168.38.148/itop/
Admininistrator Account
<< Back
Install !

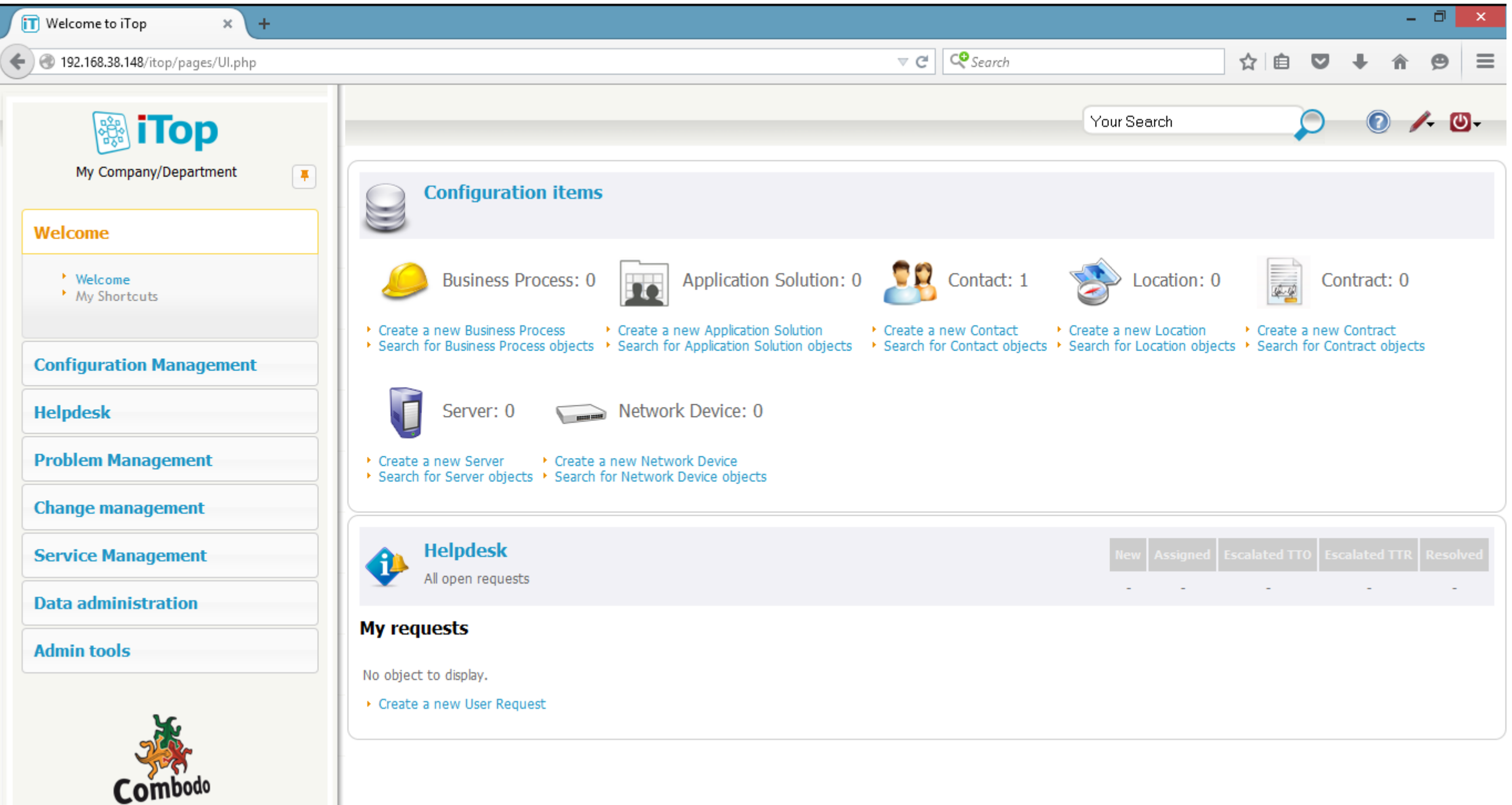
iTop


Ready to install
192.168.38.148/itop/setup/index.php
Search
iTop
Ready to install
iTop version 2.1.0 is about to be installed into the existing database itop on the server localhost.
Progress of the installation
Compiling the data model
20 %
<< Back
Install !

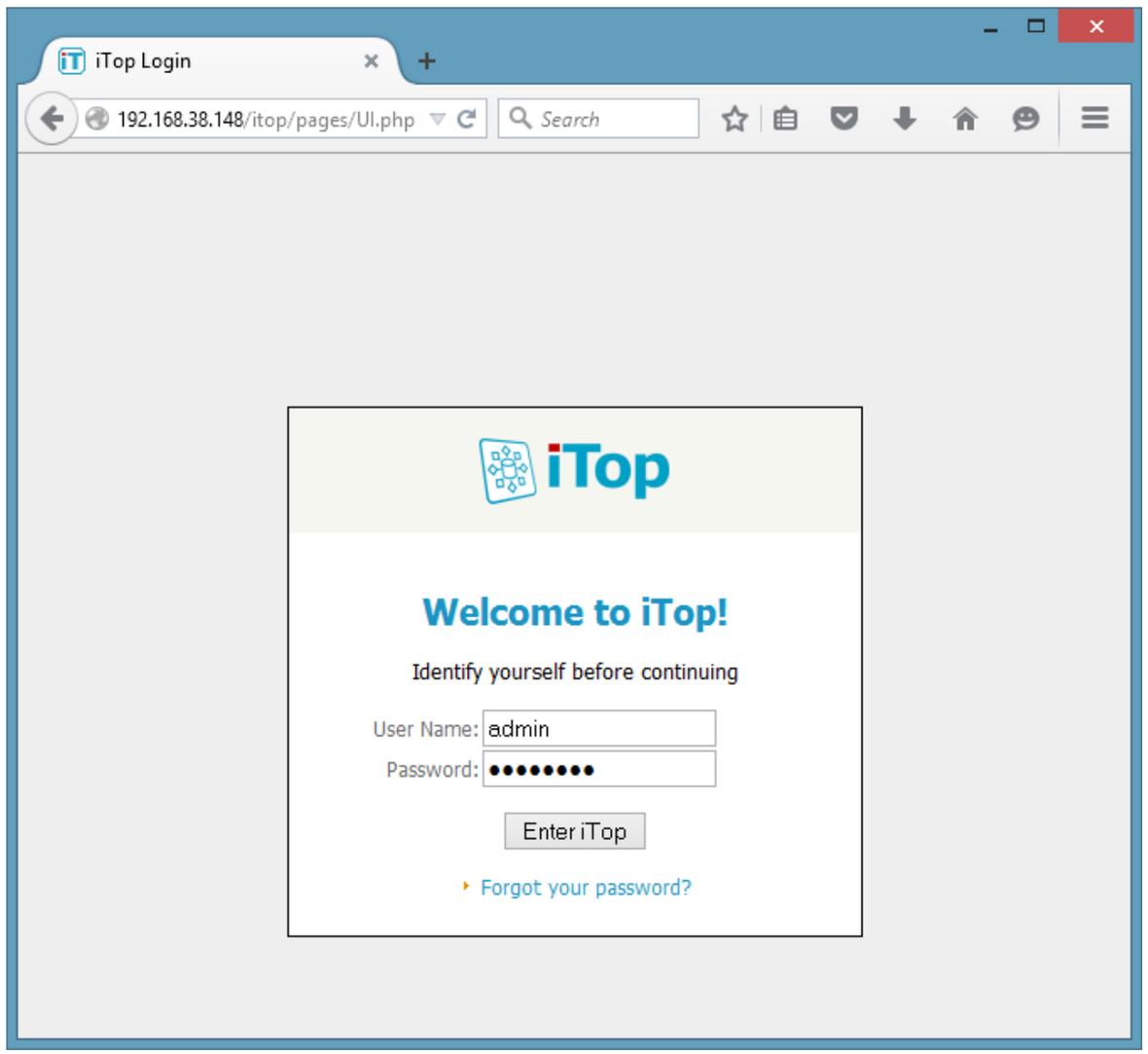
iTop

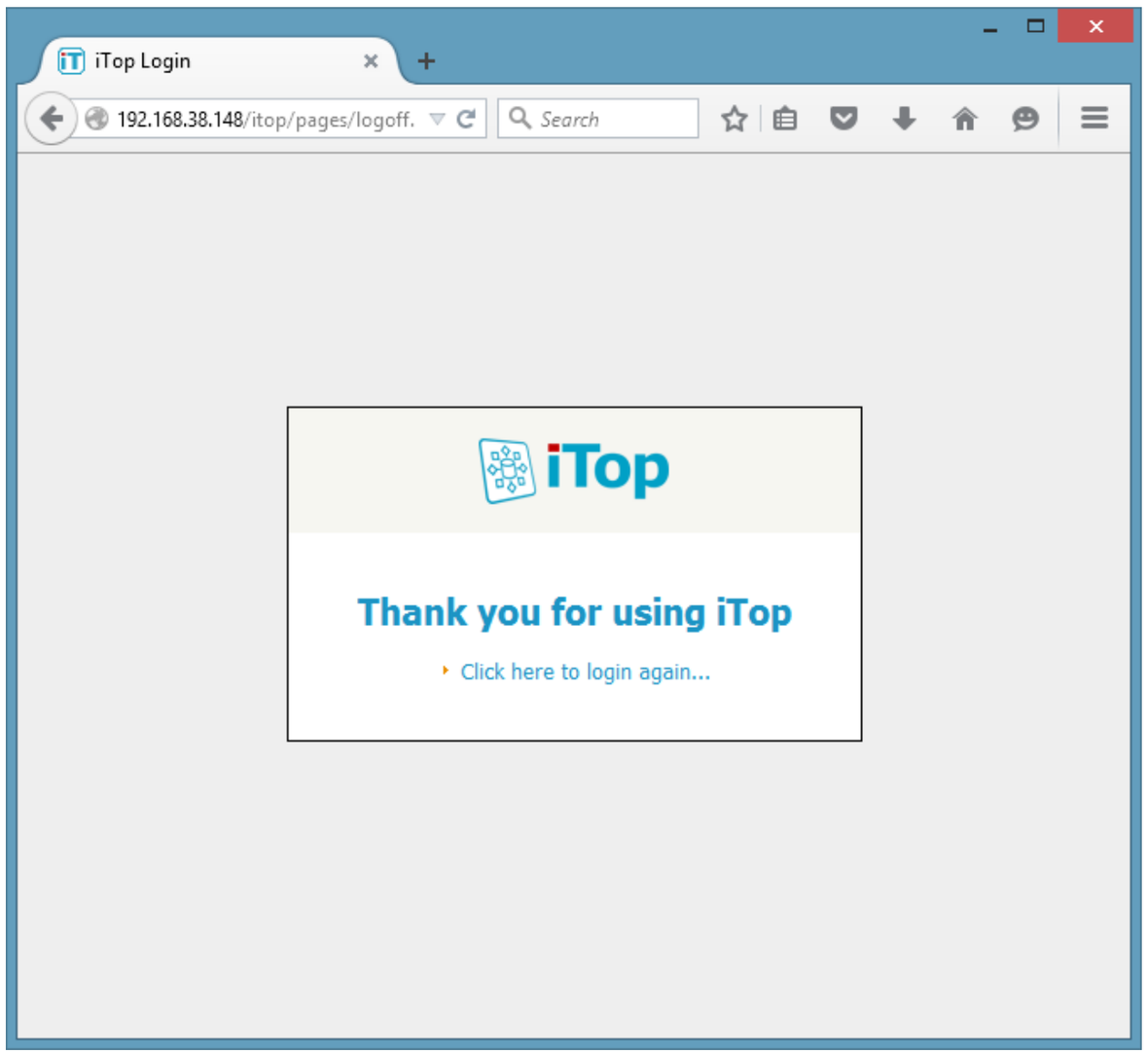

Done
192.168.38.148/itop/setup/index.php
Search
iTop
Done
Manual operations required
In order to complete the installation, the following manual operations are required:
Manual instructions for Tickets Management
Congratulations for installing iTop
Latest News
Linux in World
2+2=4
Register now !
Get Professional Support
Get Professional Training
Enter iTop

iTop


Welcome to iTop
192.168.38.148/itop/pages/UI.php
Search
iTop
My Company/Department
Welcome
Welcome
My Shortcuts
Configuration Management
Helpdesk
Problem Management
Change management
Service Management
Data administration
Admin tools
Combodo
Your Search
Configuration items
Business Process: 0
Application Solution: 0
Contact: 1
Location: 0
Contract: 0
Create a new Business Process
Search for Business Process objects
Create a new Application Solution
Search for Application Solution objects
Create a new Contact
Search for Contact objects
Create a new Location
Search for Location objects
Create a new Contract
Search for Contract objects
Server: 0
Network Device: 0
Create a new Server
Search for Server objects
Create a new Network Device
Search for Network Device objects
Helpdesk
All open requests
New
Assigned
Escalated TTO
Escalated TTR
Resolved
My requests
No object to display.
Create a new User Request

iTop


iTop Login
192.168.38.148/itop/pages/UI.php
Search
iTop
Welcome to iTop!
Identify yourself before continuing
User Name: admin
Password: ••••••••
Enter iTop
Forgot your password?


iTop Login
192.168.38.148/itop/pages/logoff.
Search
iTop
Thank you for using iTop
Click here to login again...

SSH: Secure Shell

Secure Shell (SSH)

Ref. http://linux-audit.com/auditing-hardening-ssh-configurations/

แก้ไขไฟล์ **/etc/ssh/sshd_config**

```
Protocol 2
X11Forwarding no
IgnoreRhosts yes
PermitEmptyPasswords no
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 4
```

Secure Shell (SSH)

```
[root@Server ~]#  service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
```

Secure Shell (SSH)

แก้ไขไฟล์ **/etc/ssh/sshd_config**

ในส่วนนี้ควรกำหนดให้เหมาะสม

```
AllowUsers user1 user2 user3

AllowGroup usergroup1 usergroup2

DenyUsers user1 user2 user3

DenyGroup usergroup1 usergroup2
```

Secure Shell (SSH)

ตัวอย่าง SSH log (/var/log/secure)

Mar 14 19:02:43 Server sshd[4698]: User cloudadmin01 from 172.17.12.5 not allowed because **not listed in AllowUsers**

Mar 14 19:08:11 Server sshd[4758]: User cloudadmin01 from 172.17.12.5 not allowed because **none of user's groups are listed in AllowGroups**

Mar 14 19:18:27 Server sshd[4972]: User cloudadmin01 from 172.17.12.5 not allowed because **listed in DenyUsers**

Mar 14 19:26:36 Server unix_chkpwd[9920]: password check failed for user (root)

IPTABLES / IP6TABLES

IPTABLES / IP6TABLES

- การกำหนดให้ iptables/ip6tables ทำงานทุกครั้งที่ reboot เครื่อง

```
[root@Server sysconfig]# chkconfig iptables on
[root@Server sysconfig]# chkconfig ip6tables on
```

- ไฟล์ Configuration ของ iptables และ ip6tables

```
/etc/sysconfig/iptables
/etc/sysconfig/ip6tables
```

IPTABLES / IP6TABLES

- การ Start/Stop/Restart iptables/ip6tables service

```
[root@Server sysconfig]# service iptables start
[root@Server sysconfig]# service iptables stop
[root@Server sysconfig]# service iptables retart

[root@Server sysconfig]# service ip6tables start
[root@Server sysconfig]# service ip6tables stop
[root@Server sysconfig]# service ip6tables restart
```

IPTABLES / IP6TABLES

- การตรวจสอบการทำงานของ **iptables**

```
[root@Server sysconfig]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   27  1976 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
    0     0 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 16 packets, 1872 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

IPTABLES / IP6TABLES

- การตรวจสอบการทำงานของ **iptables**

```
[root@Server sysconfig]# ip6tables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all      *      *       ::/0                 ::/0                 state RELATED,ESTABLISHED
    0     0 ACCEPT     icmpv6    *      *       ::/0                 ::/0
    0     0 ACCEPT     all      lo     *       ::/0                 ::/0
    0     0 ACCEPT     udp      *      *       ::/0                 fe80::/64            state NEW udp dpt:546
    0     0 ACCEPT     tcp      *      *       ::/0                 ::/0                 state NEW tcp dpt:22
    0     0 REJECT     all      *      *       ::/0                 ::/0                 reject-with icmp6-adm-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all      *      *       ::/0                 ::/0                 reject-with icmp6-adm-prohibited

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

IPTABLES / IP6TABLES

- ตัวอย่างการเพิ่ม Policy ให้ iptables เพื่ออนุญาตให้ใช้งาน TCP/80

```
# 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 -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

IPTABLES / IP6TABLES

- ตัวอย่างการเพิ่ม Policy ให้ iptables เพื่ออนุญาตให้ใช้งาน TCP/80 จากต้นทาง IP 192.168.1.0/24 เท่านั้น

```
# 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 -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -s 192.168.1.0/24 -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Logging

Logging

- การส่ง System log ไปเก็บที่ Syslog server ให้ทำการแก้ไขไฟล์ /etc/rsyslog.conf ดังนี้

```
*.*     @IP-Log-Server
```

- จากนั้นทำการ restart rsyslog

```
[root@Server sysconfig]# service rsyslog restart
```

System monitoring tools

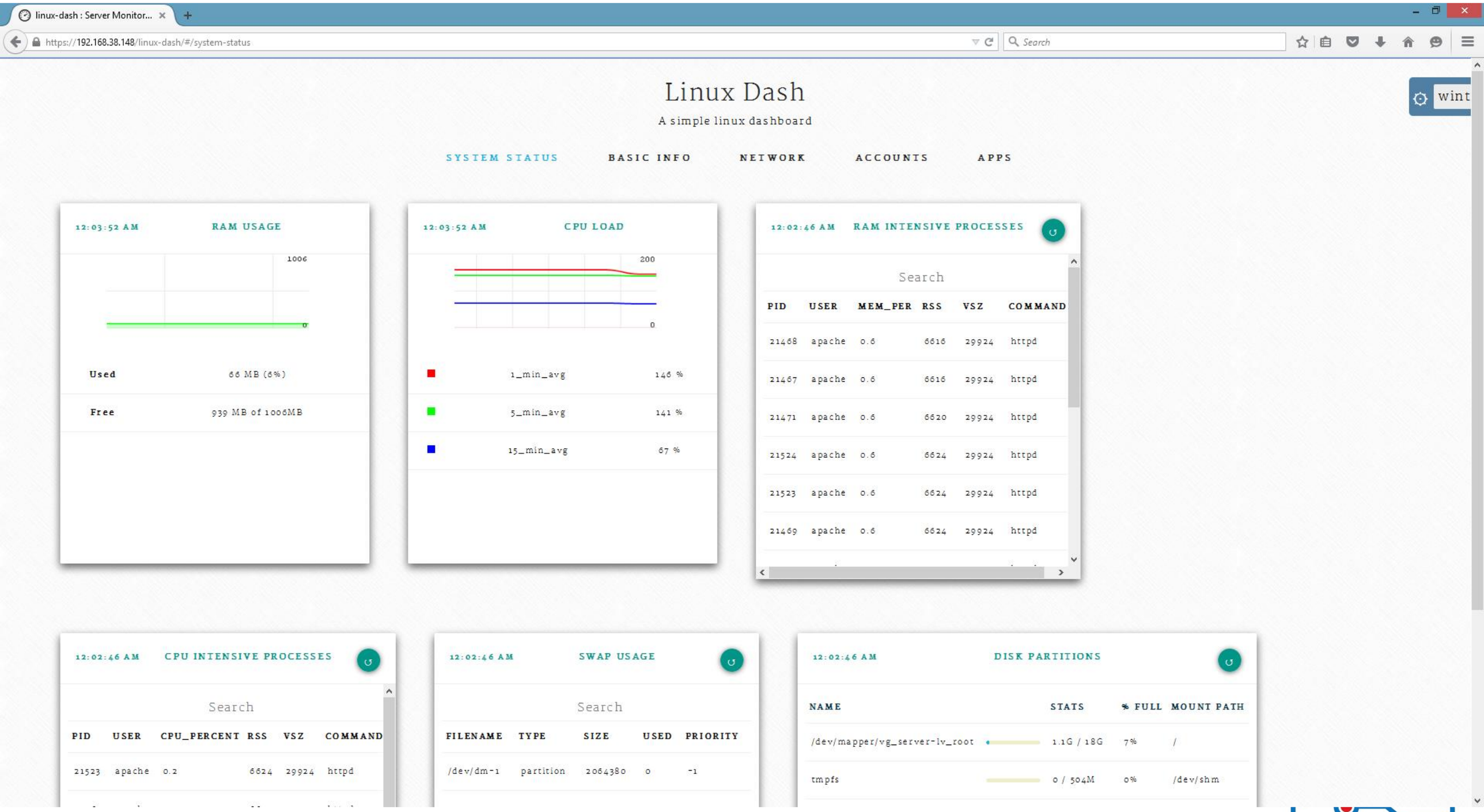
Linux-dash

- **Linux-dash (https://github.com/afaqurk/linux-dash/)**

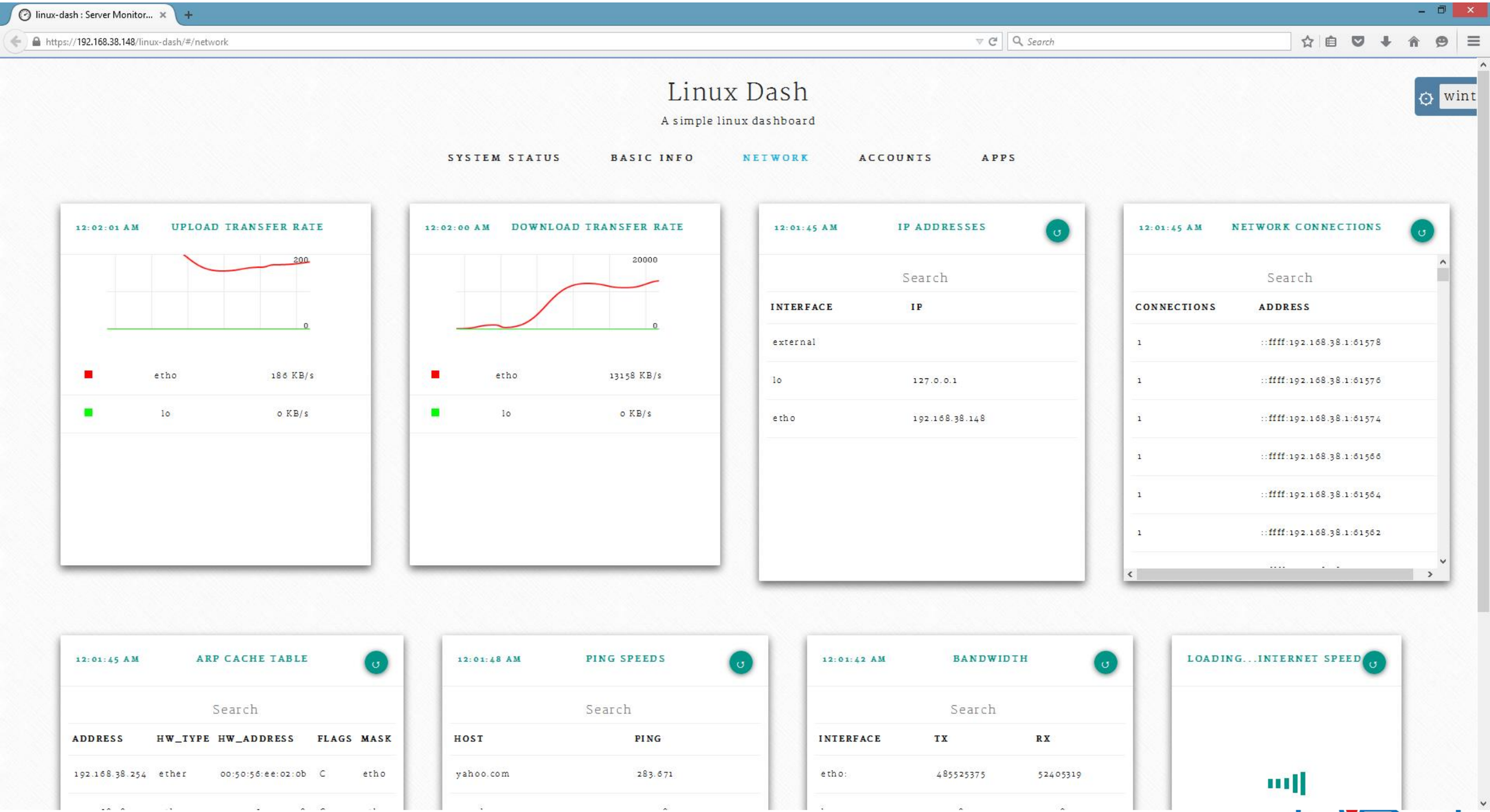
```
[root@Server ~]# yum -y install git
[root@Server ~]# cd /var/www/html/
[root@Server html]# git clone https://github.com/afaqurk/linux-dash.git
Initialized empty Git repository in /var/www/html/linux-dash/.git/
remote: Counting objects: 2888, done.
Receiving objects: 100% (2888/2888), 3.26 MiB | 25 KiB/s, done.
remote: Total 2888 (delta 0), reused 0 (delta 0), pack-reused 2888
Resolving deltas: 100% (1666/1666), done.
```

- **เข้าใช้งานที่ https://ip-address/linux-dash/**

Linux-dash


linux-dash : Server Monitor...
https://192.168.38.148/linux-dash/#/system-status
Search
Linux Dash
A simple linux dashboard
SYSTEM STATUS
BASIC INFO
NETWORK
ACCOUNTS
APPS
12:03:52 AM
RAM USAGE
1006
0
Used
66 MB (6%)
Free
939 MB of 1006MB
12:03:52 AM
CPU LOAD
200
0
1_min_avg
146 %
5_min_avg
141 %
15_min_avg
67 %
12:02:46 AM
RAM INTENSIVE PROCESSES
Search
PID USER MEM_PER RSS VSZ COMMAND
21468 apache 0.6 6616 29924 httpd
21467 apache 0.6 6616 29924 httpd
21471 apache 0.6 6620 29924 httpd
21524 apache 0.6 6624 29924 httpd
21523 apache 0.6 6624 29924 httpd
21469 apache 0.6 6624 29924 httpd
12:02:46 AM
CPU INTENSIVE PROCESSES
Search
PID USER CPU_PERCENT RSS VSZ COMMAND
21523 apache 0.2 6624 29924 httpd
12:02:46 AM
SWAP USAGE
Search
FILENAME TYPE SIZE USED PRIORITY
/dev/dm-1 partition 2064380 0 -1
12:02:46 AM
DISK PARTITIONS
NAME STATS % FULL MOUNT PATH
/dev/mapper/vg_server-lv_root 1.1G / 18G 7% /
tmpfs 0 / 504M 0% /dev/shm

Linux-dash


linux-dash : Server Monitor...
https://192.168.38.148/linux-dash/#/network
Search
Linux Dash
A simple linux dashboard
wint
SYSTEM STATUS
BASIC INFO
NETWORK
ACCOUNTS
APPS
12:02:01 AM
UPLOAD TRANSFER RATE
200
0
etho
186 KB/s
lo
0 KB/s
12:02:00 AM
DOWNLOAD TRANSFER RATE
20000
0
etho
13158 KB/s
lo
0 KB/s
12:01:45 AM
IP ADDRESSES
Search
INTERFACE
IP
external
lo
127.0.0.1
etho
192.168.38.148
12:01:45 AM
NETWORK CONNECTIONS
Search
CONNECTIONS
ADDRESS
1
::ffff:192.168.38.1:61578
1
::ffff:192.168.38.1:61576
1
::ffff:192.168.38.1:61574
1
::ffff:192.168.38.1:61566
1
::ffff:192.168.38.1:61564
1
::ffff:192.168.38.1:61562
12:01:45 AM
ARP CACHE TABLE
Search
ADDRESS
HW_TYPE
HW_ADDRESS
FLAGS
MASK
192.168.38.254
ether
00:50:56:ee:02:0b
C
etho
12:01:48 AM
PING SPEEDS
Search
HOST
PING
yahoo.com
283.671
12:01:42 AM
BANDWIDTH
Search
INTERFACE
TX
RX
etho:
485525375
52405319
LOADING...INTERNET SPEED

System monitoring tools

- Cacti (http://www.cacti.net)

- Nagios (https://www.nagios.org)

- Zabbix (http://www.zabbix.com)

Hands-on LAB