

การใช้งาน CentOS 7 เบื้องต้น

คมกริช คำสวัสดิ์

วิศวกรอาวุโส

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

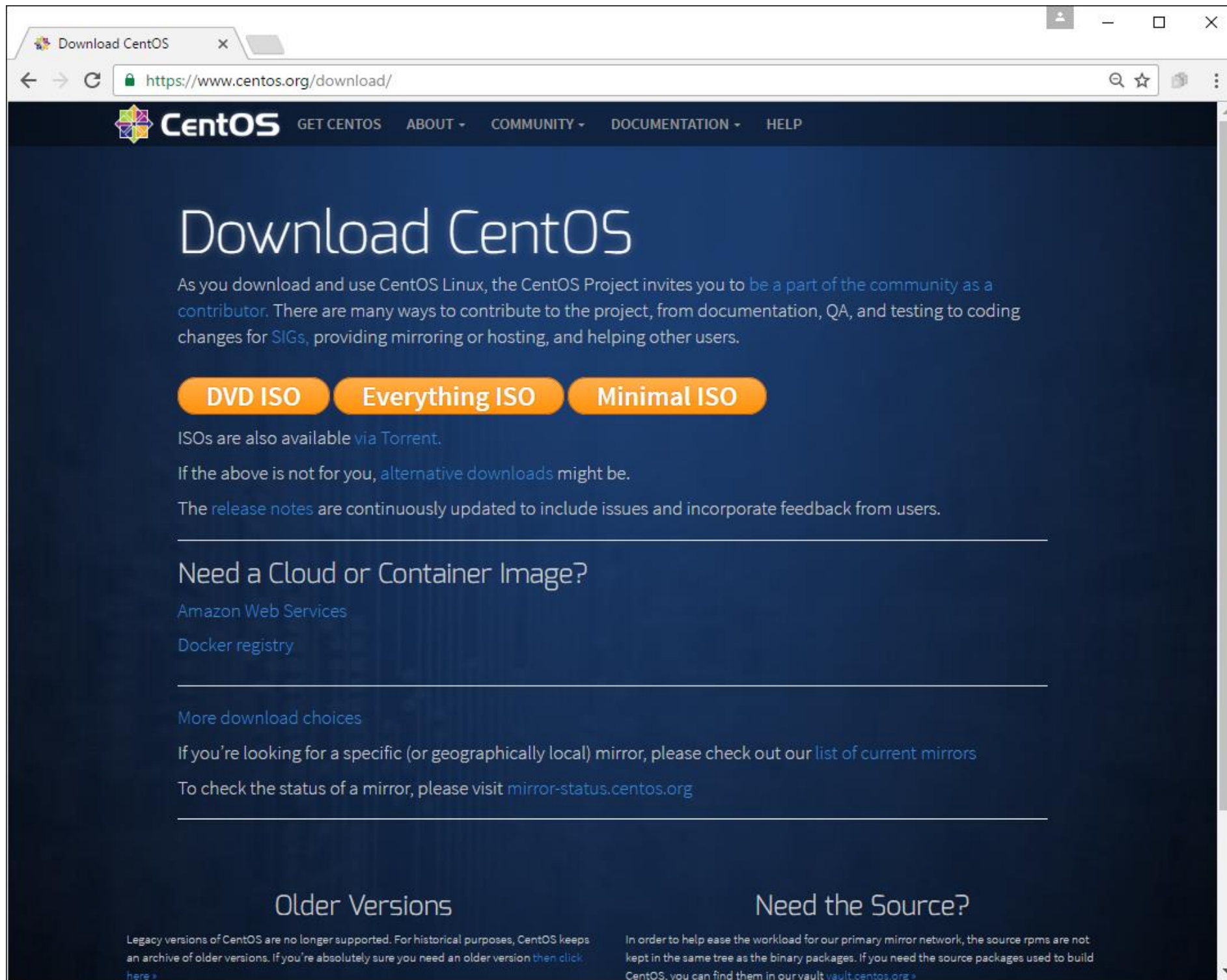
การใช้งาน CentOS 7 เบื้องต้น

- Installation
- Sync system time with NTP server
- Install additional packages
- Update/Upgrade
- Local Firewall by iptables
- SSH basic Hardening
- Send system log to Syslog server
- NTP service
- MariaDB
- MySQL
- Web server (HTTPD)
- FTP server (VSFTPD)

www.centos.org



www.centos.org



The screenshot shows a web browser window with the address bar displaying <https://www.centos.org/download/>. The page features the CentOS logo and navigation links: GET CENTOS, ABOUT, COMMUNITY, DOCUMENTATION, and HELP. The main heading is "Download CentOS". Below it, a paragraph states: "As you download and use CentOS Linux, the CentOS Project invites you to be a part of the community as a contributor. There are many ways to contribute to the project, from documentation, QA, and testing to coding changes for SIGs, providing mirroring or hosting, and helping other users." Three orange buttons are displayed: "DVD ISO", "Everything ISO", and "Minimal ISO". Below these buttons, text indicates "ISOs are also available via Torrent." and "If the above is not for you, alternative downloads might be." It also mentions "The release notes are continuously updated to include issues and incorporate feedback from users." A section titled "Need a Cloud or Container Image?" includes links for "Amazon Web Services" and "Docker registry". Another link, "More download choices", is provided. A paragraph states: "If you're looking for a specific (or geographically local) mirror, please check out our list of current mirrors" and "To check the status of a mirror, please visit mirror-status.centos.org". At the bottom, there are two sections: "Older Versions" with a note that legacy versions are no longer supported and a link to an archive, and "Need the Source?" with a note about source rpms and a link to the vault.

Download CentOS

As you download and use CentOS Linux, the CentOS Project invites you to be a part of the community as a contributor. There are many ways to contribute to the project, from documentation, QA, and testing to coding changes for SIGs, providing mirroring or hosting, and helping other users.

DVD ISO **Everything ISO** **Minimal ISO**

ISOs are also available via Torrent.

If the above is not for you, alternative downloads might be.

The release notes are continuously updated to include issues and incorporate feedback from users.

Need a Cloud or Container Image?

[Amazon Web Services](#)

[Docker registry](#)

[More download choices](#)

If you're looking for a specific (or geographically local) mirror, please check out our [list of current mirrors](#)

To check the status of a mirror, please visit [mirror-status.centos.org](#)

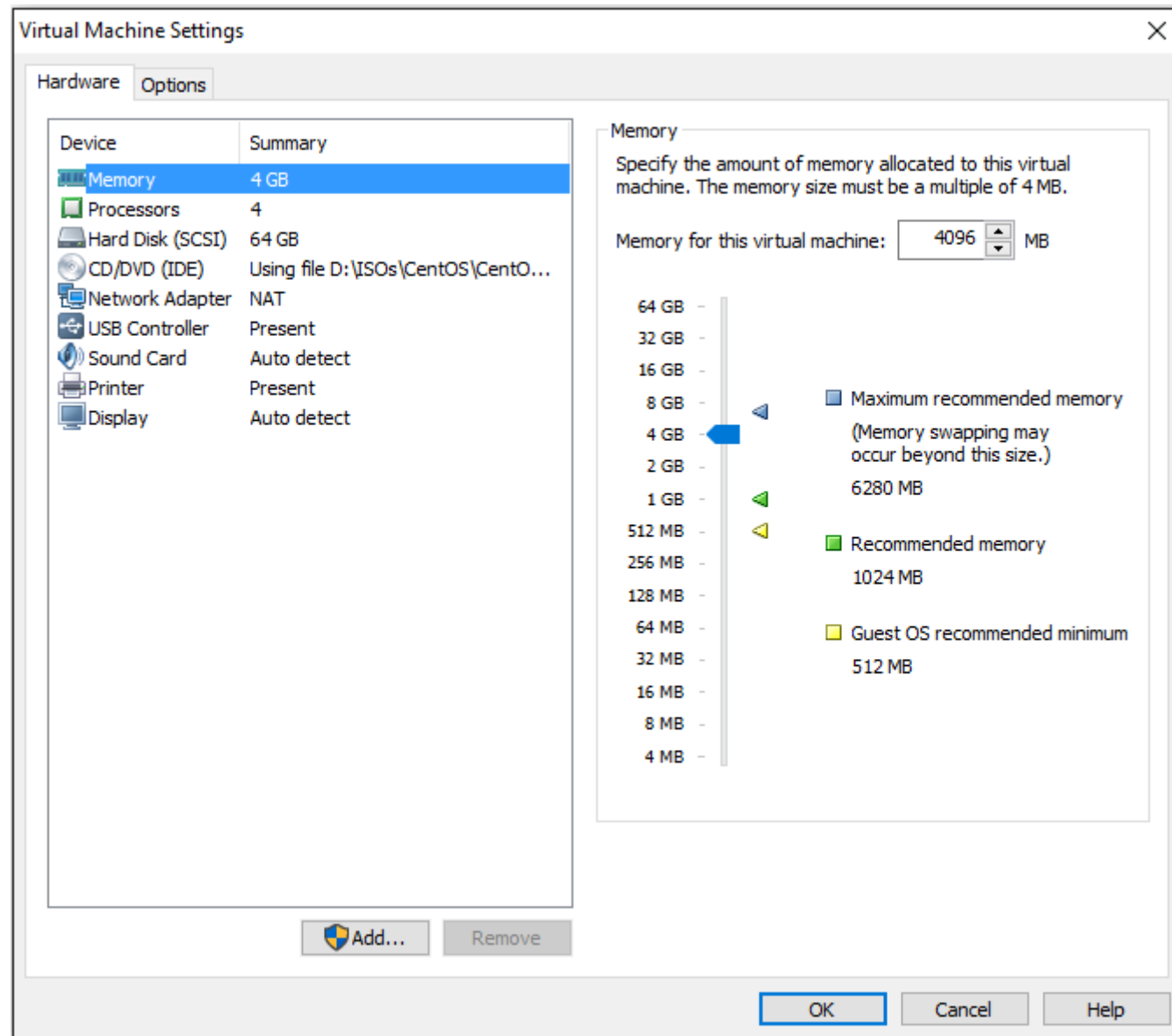
Older Versions

Legacy versions of CentOS are no longer supported. For historical purposes, CentOS keeps an archive of older versions. If you're absolutely sure you need an older version [then click here](#)

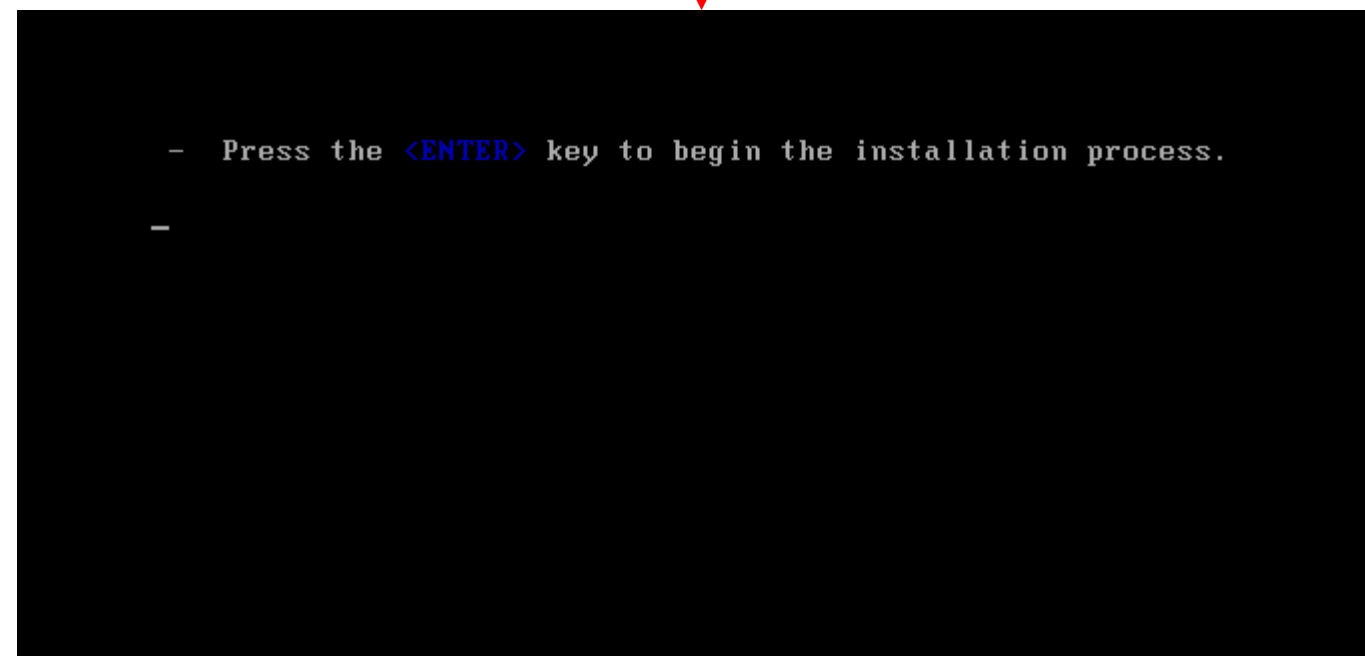
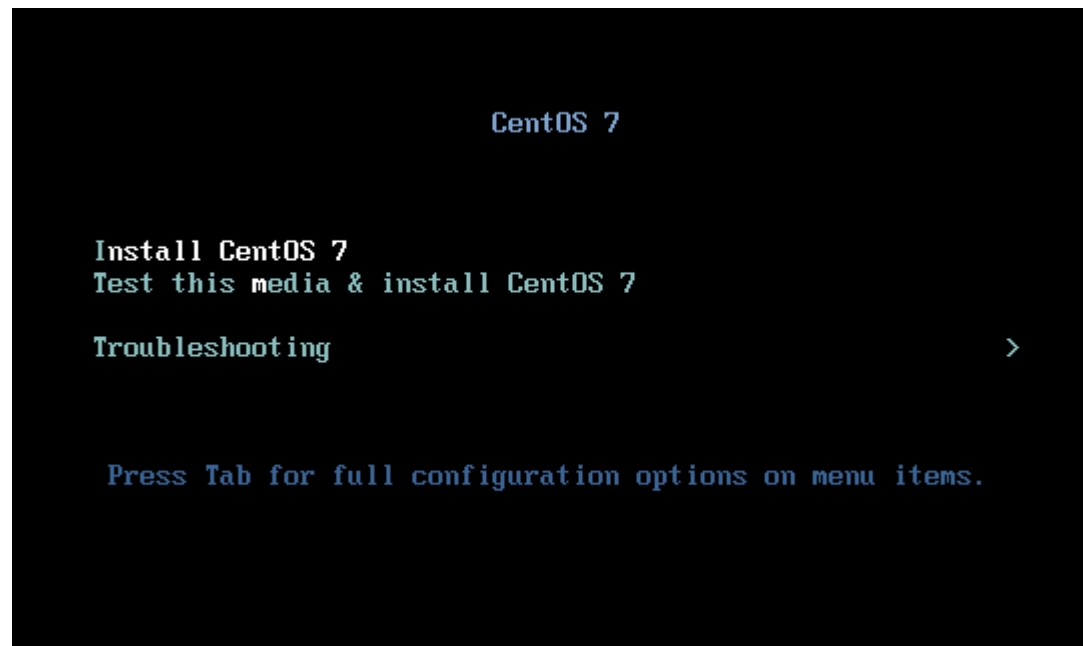
Need the Source?

In order to help ease the workload for our primary mirror network, the source rpms are not kept in the same tree as the binary packages. If you need the source packages used to build CentOS, you can find them in our vault [vault.centos.org](#)

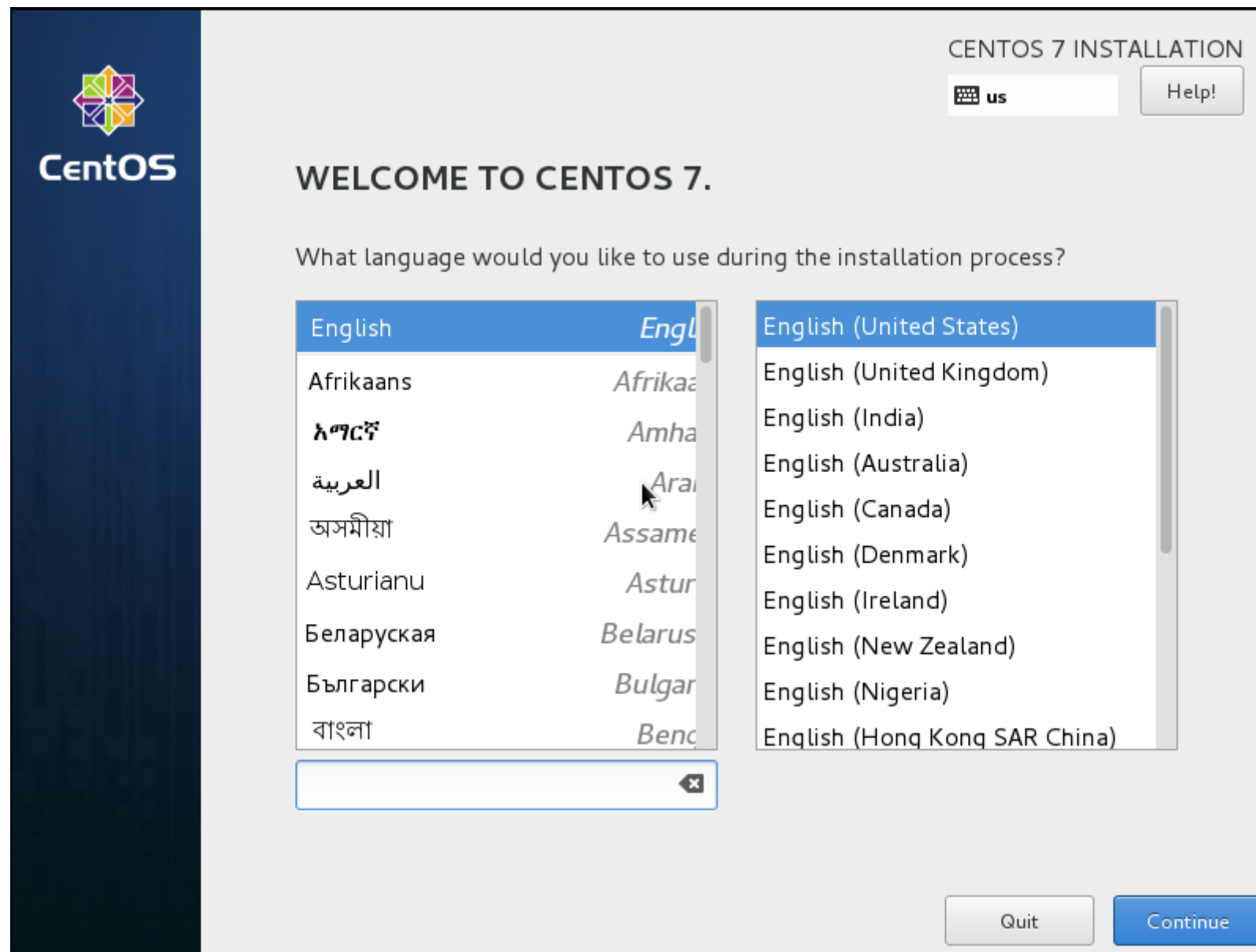
การติดตั้ง CentOS 7



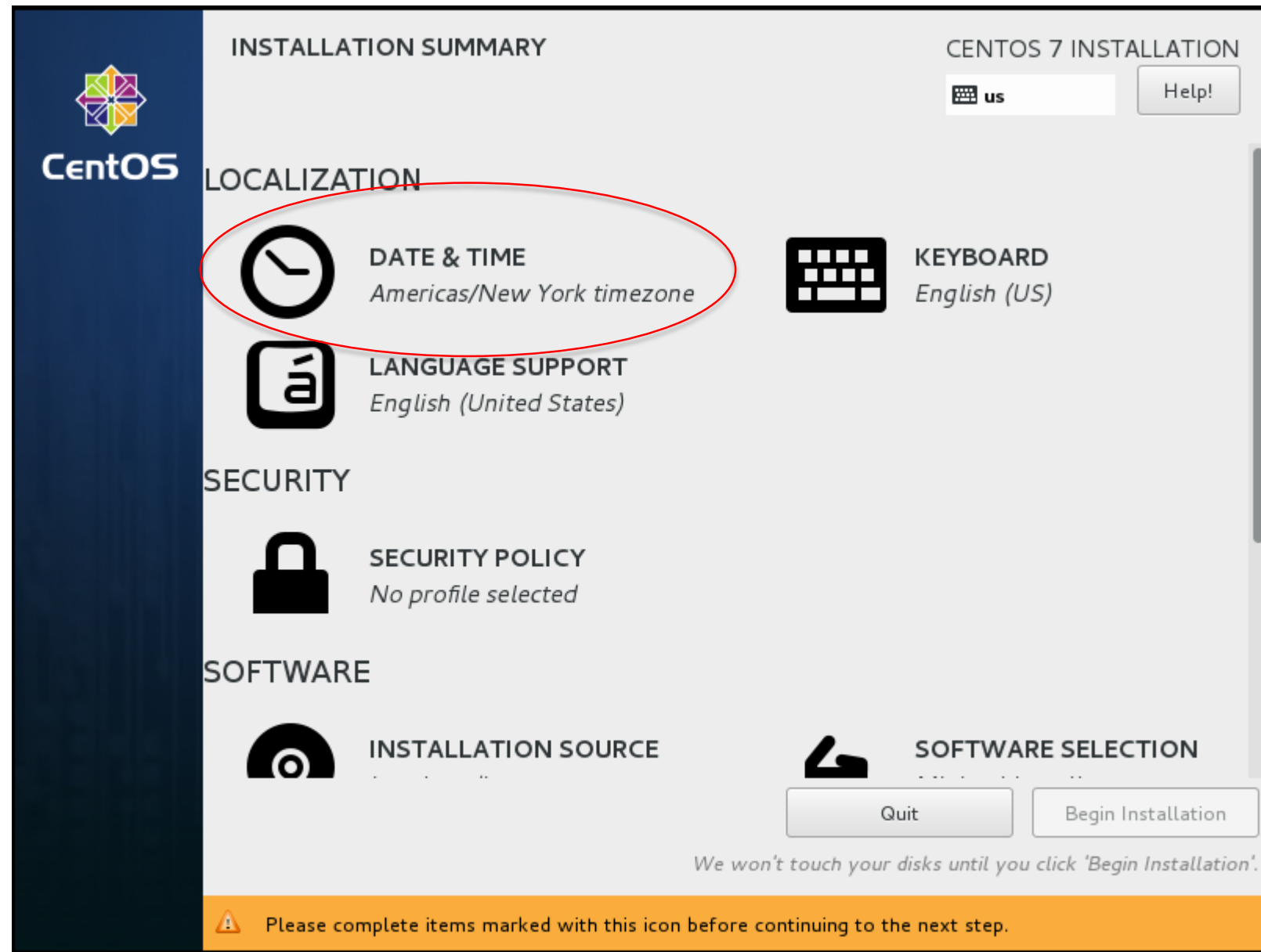
การติดตั้ง CentOS 7: Boot from CD



การติดตั้ง CentOS 7 : เลือกภาษา



การติดตั้ง CentOS 7 : ส่วนกำหนดค่าพื้นฐานของระบบ



การติดตั้ง CentOS 7 : Time Zone

DATE & TIME Done CENTOS 7 INSTALLATION us Help!

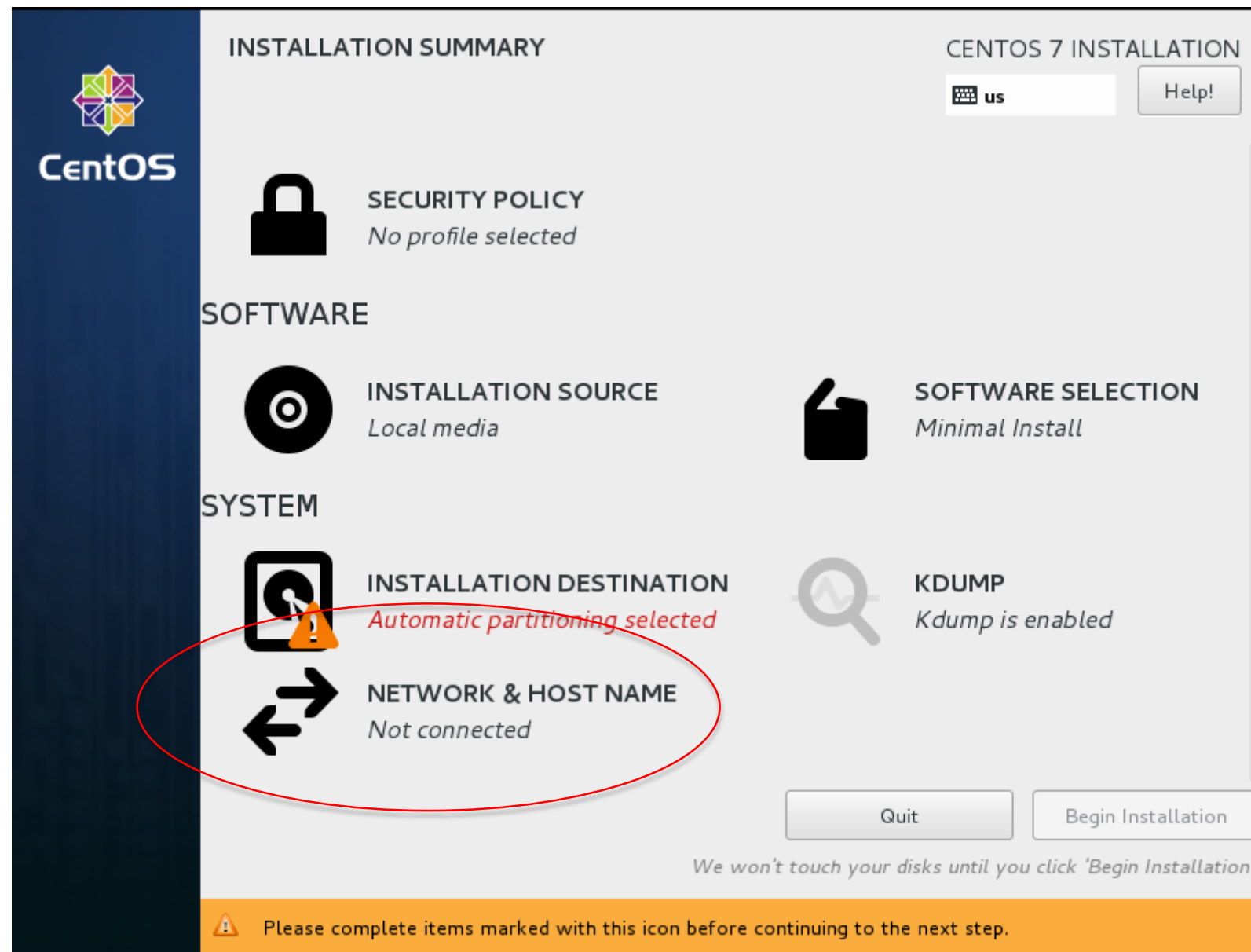
Region: Asia City: Bangkok Network Time OFF



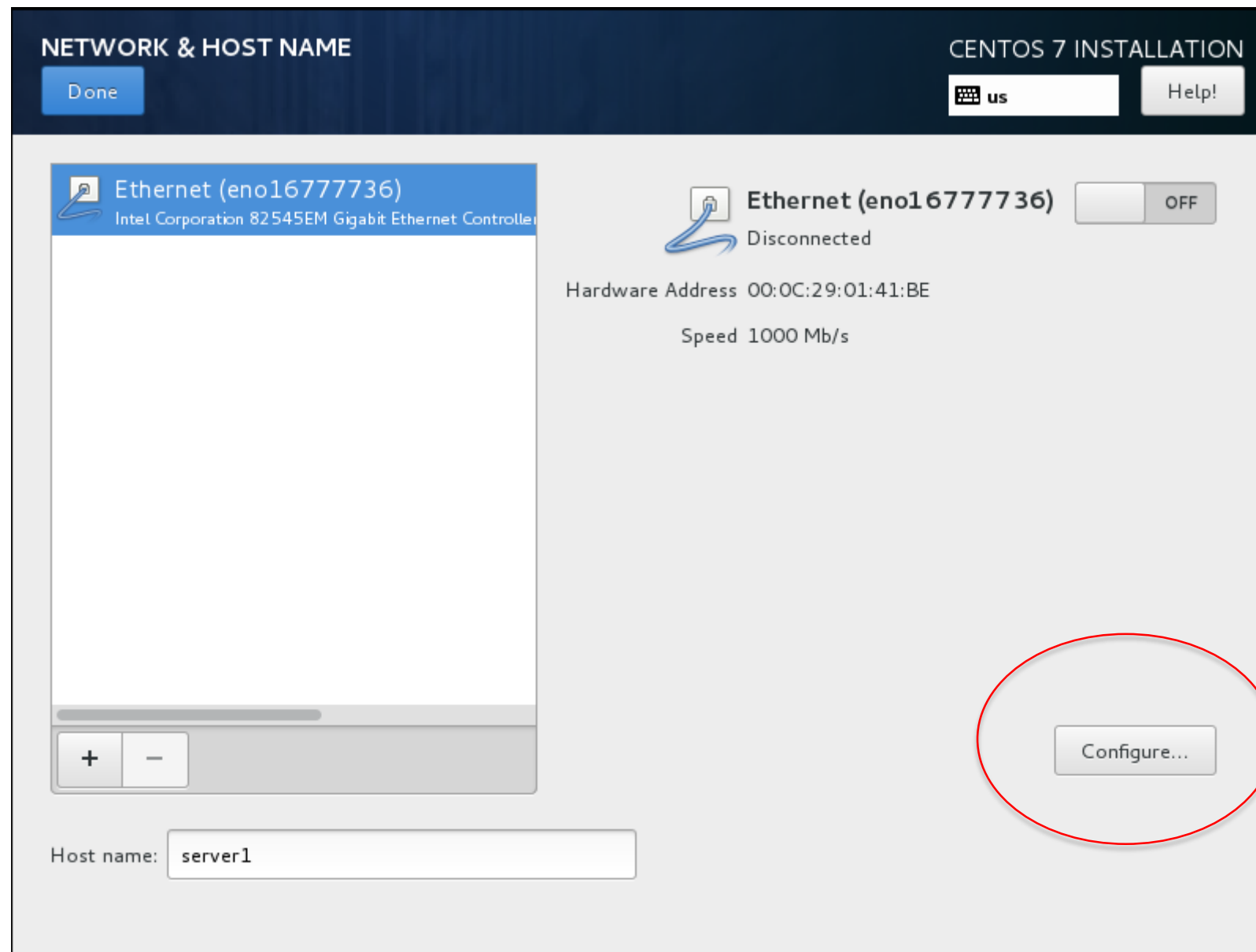
18:05 PM 24-hour AM/PM 07 / 26 / 2016

 You need to set up networking first if you want to use NTP

การติดตั้ง CentOS 7 : Network



การติดตั้ง CentOS 7 : Network



การติดตั้ง CentOS 7 : Network

NETWORK & HOST NAME CENTOS 7 INSTALLATION

Done us Help!

Editing eno16777736

Connection name:

General Ethernet 802.1x Security DCB IPv4 Settings IPv6 Settings

☒ Automatically connect to this network when it is available

☒ All users may connect to this network

☐ Automatically connect to VPN when using this connection

Firewall zone:

Cancel Save

การติดตั้ง CentOS 7 : Network

NETWORK & HOST NAME CENTOS 7 INSTALLATION

Done us Help!

Editing eno16777736

Connection name:

General **Ethernet** **802.1x Security** **DCB** **IPv4 Settings** **IPv6 Settings**

Method:

Addresses

Address	Netmask	Gateway
192.168.146.146	255.255.255.0	192.168.146.2

Add Delete

DNS servers:

Search domains:

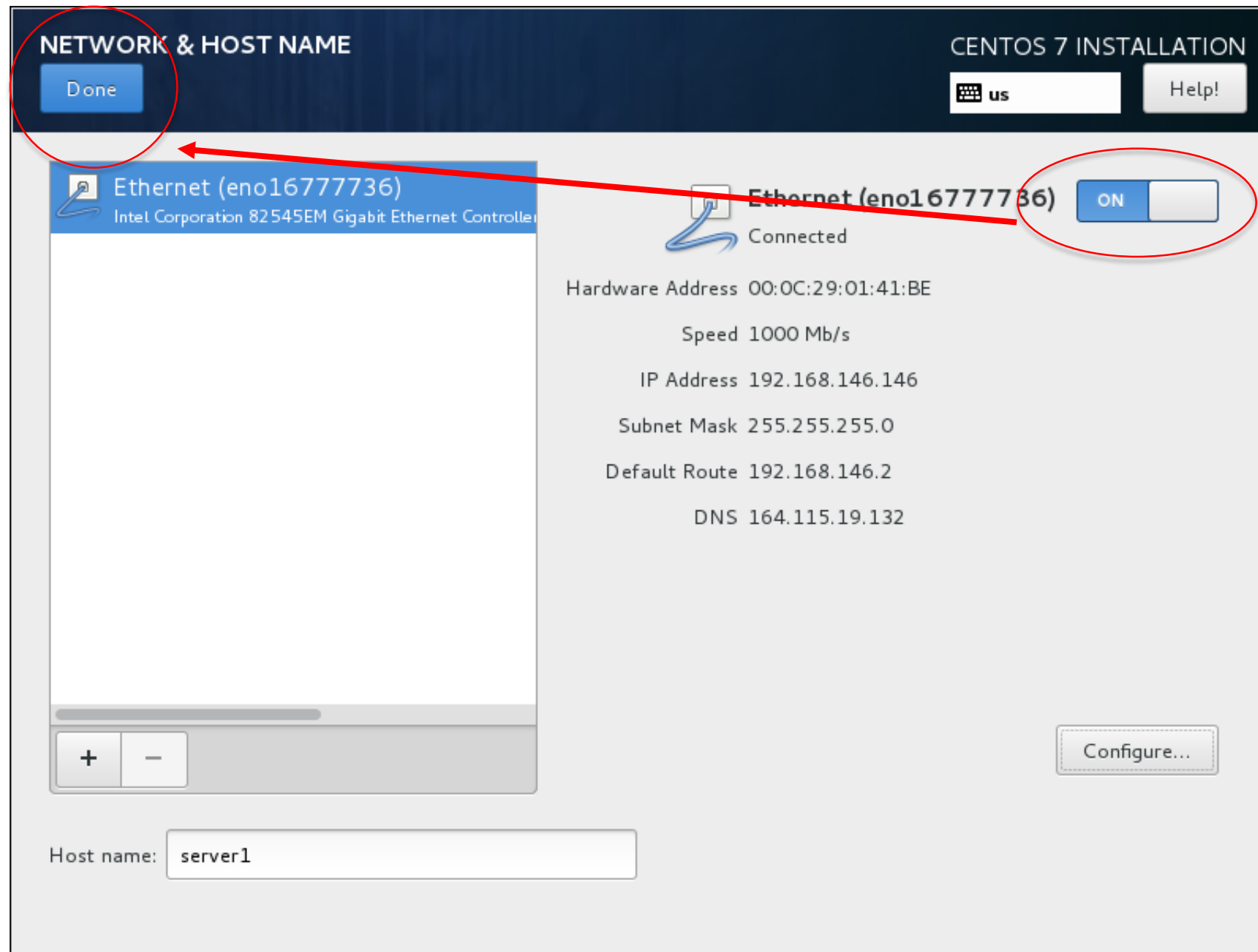
DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

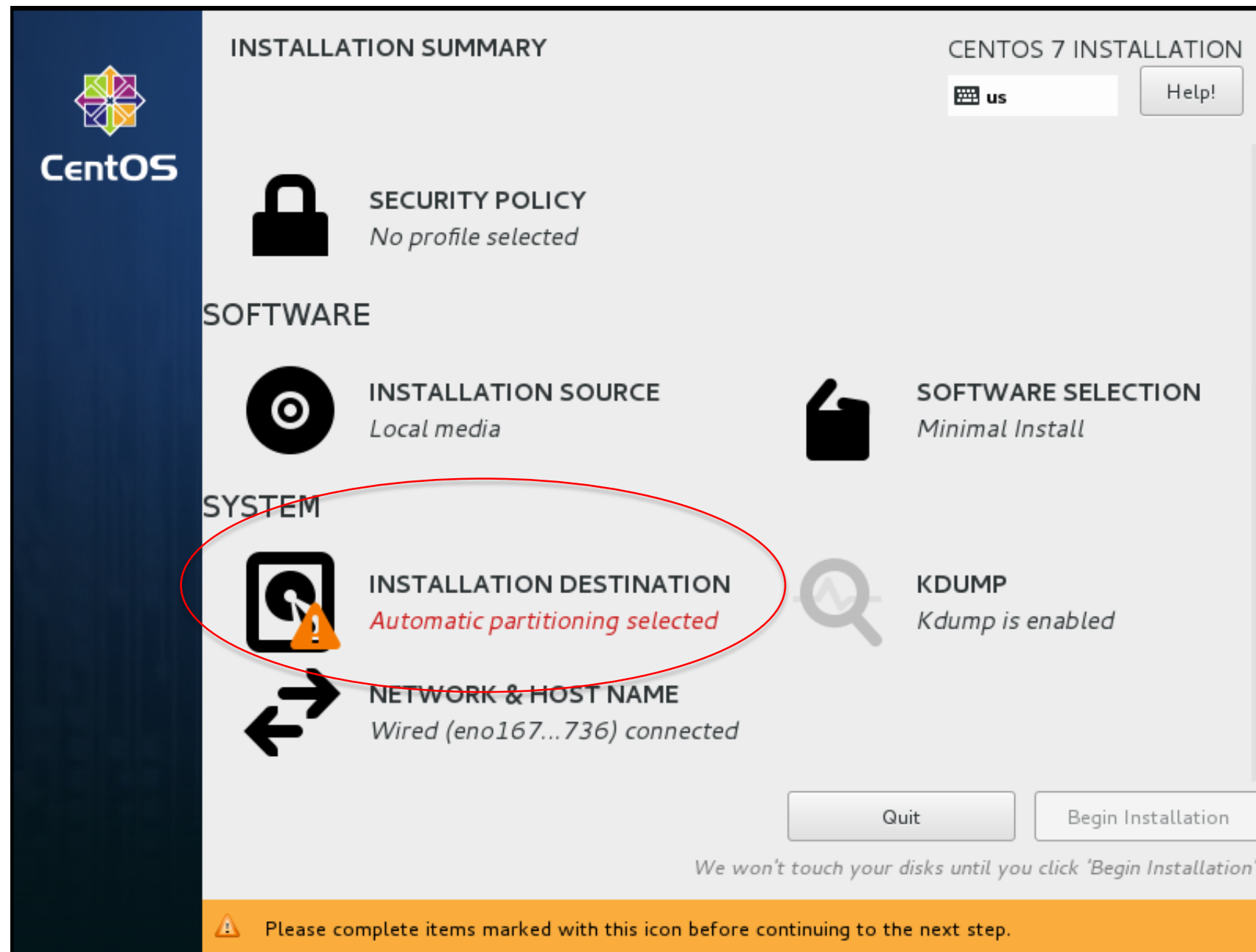
Routes...

Cancel Save

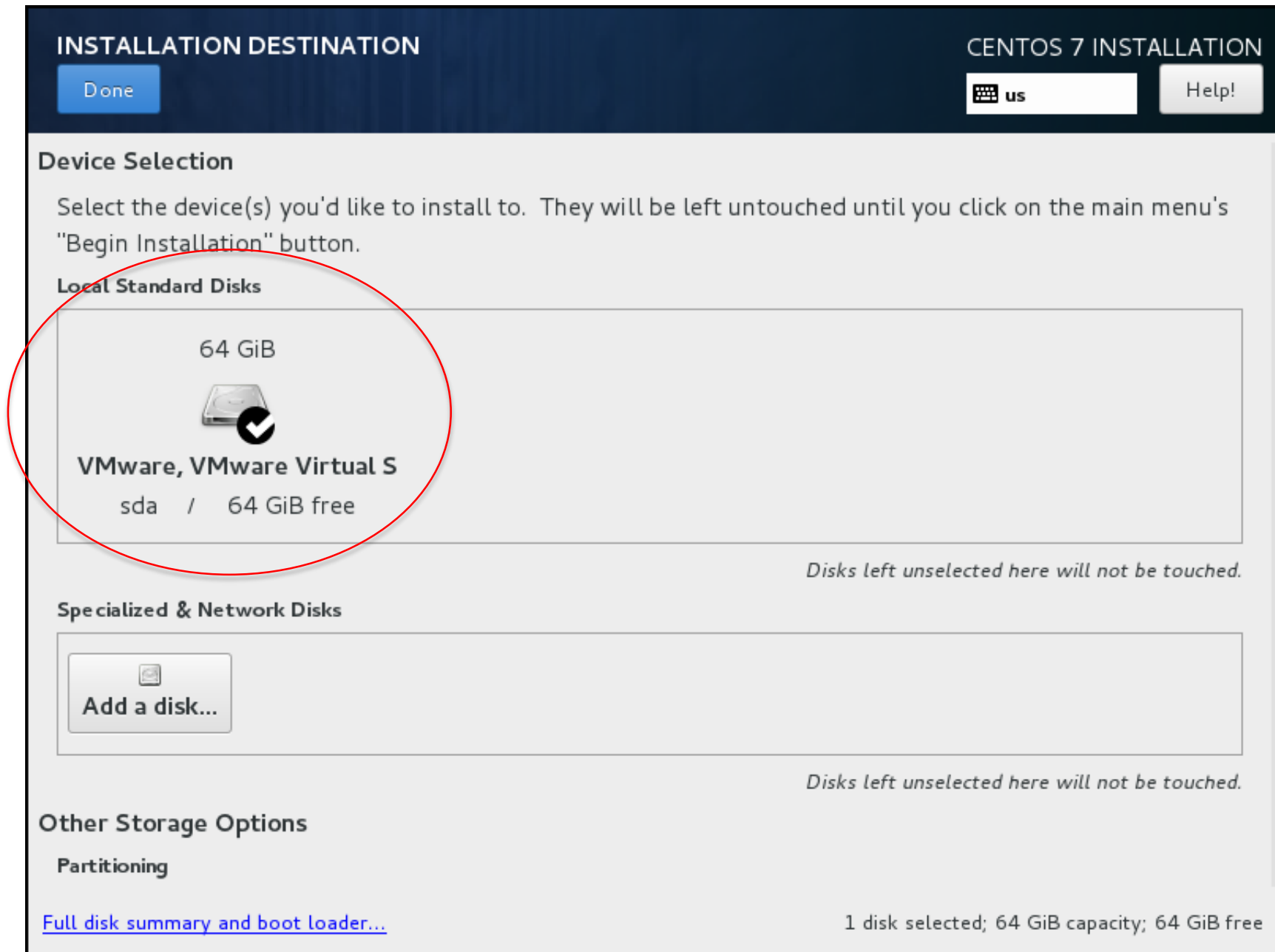
การติดตั้ง CentOS 7 : Network



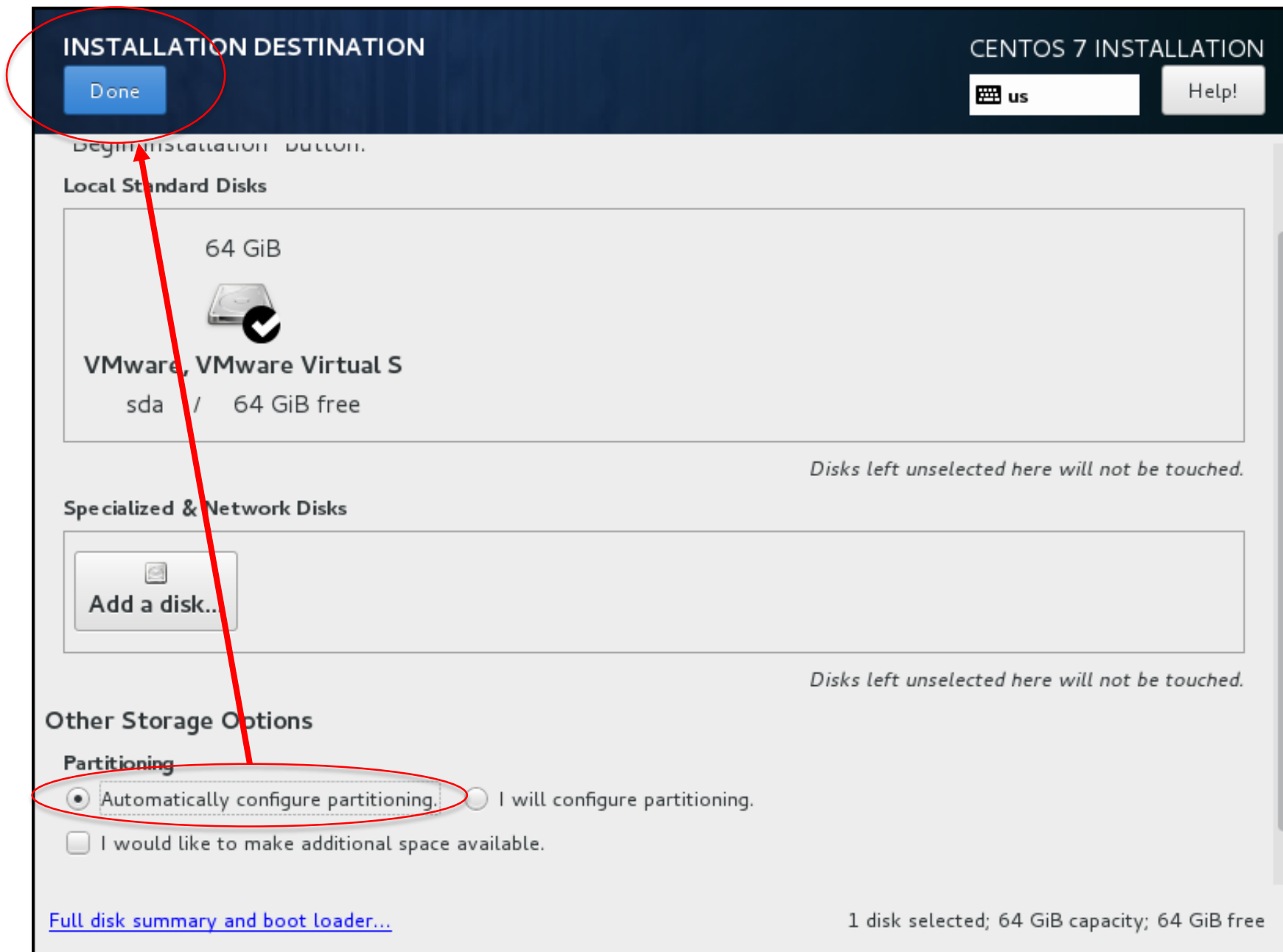
การติดตั้ง CentOS 7 : Disk Partition (Auto partition)



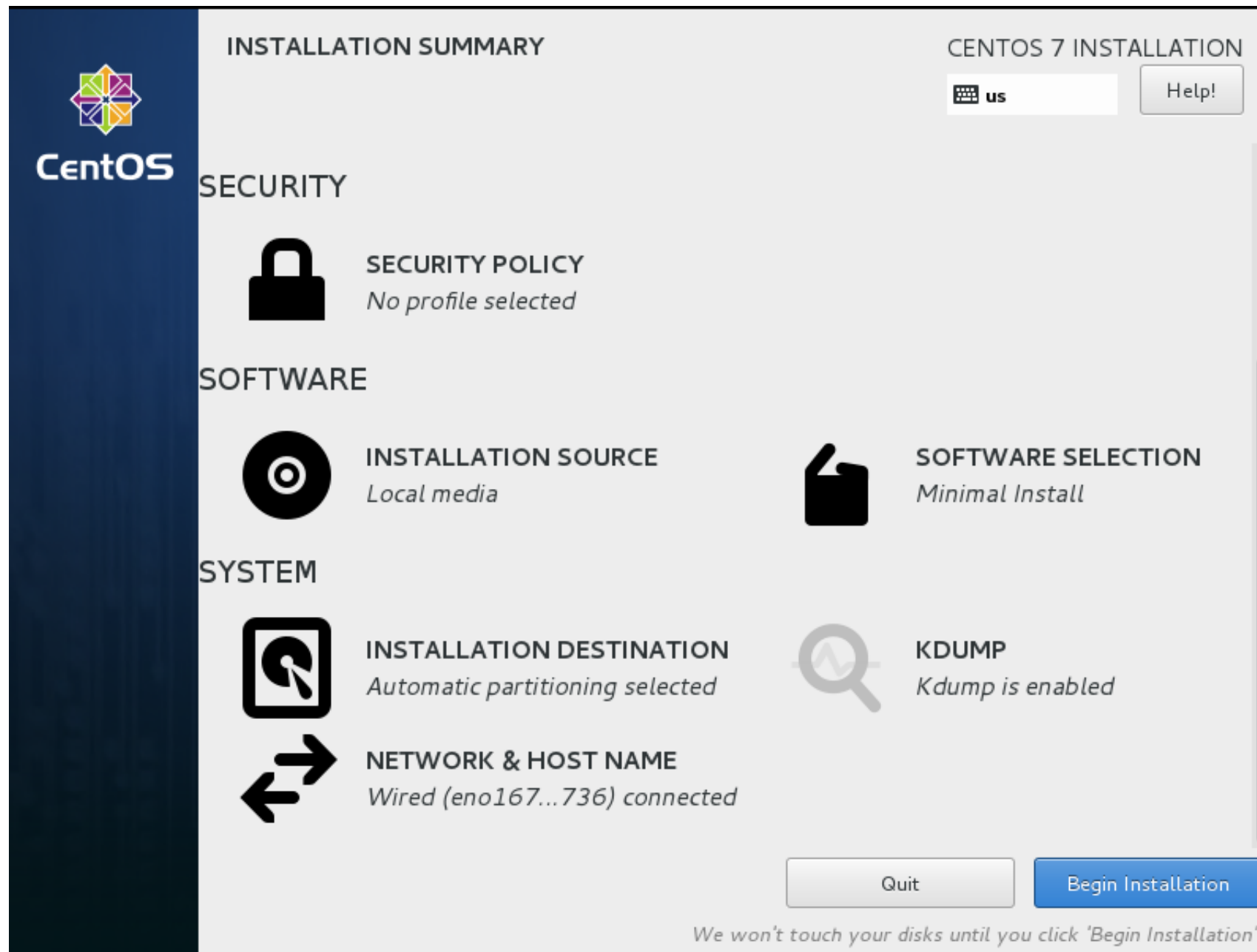
การติดตั้ง CentOS 7 : Disk Partition (Auto partition)



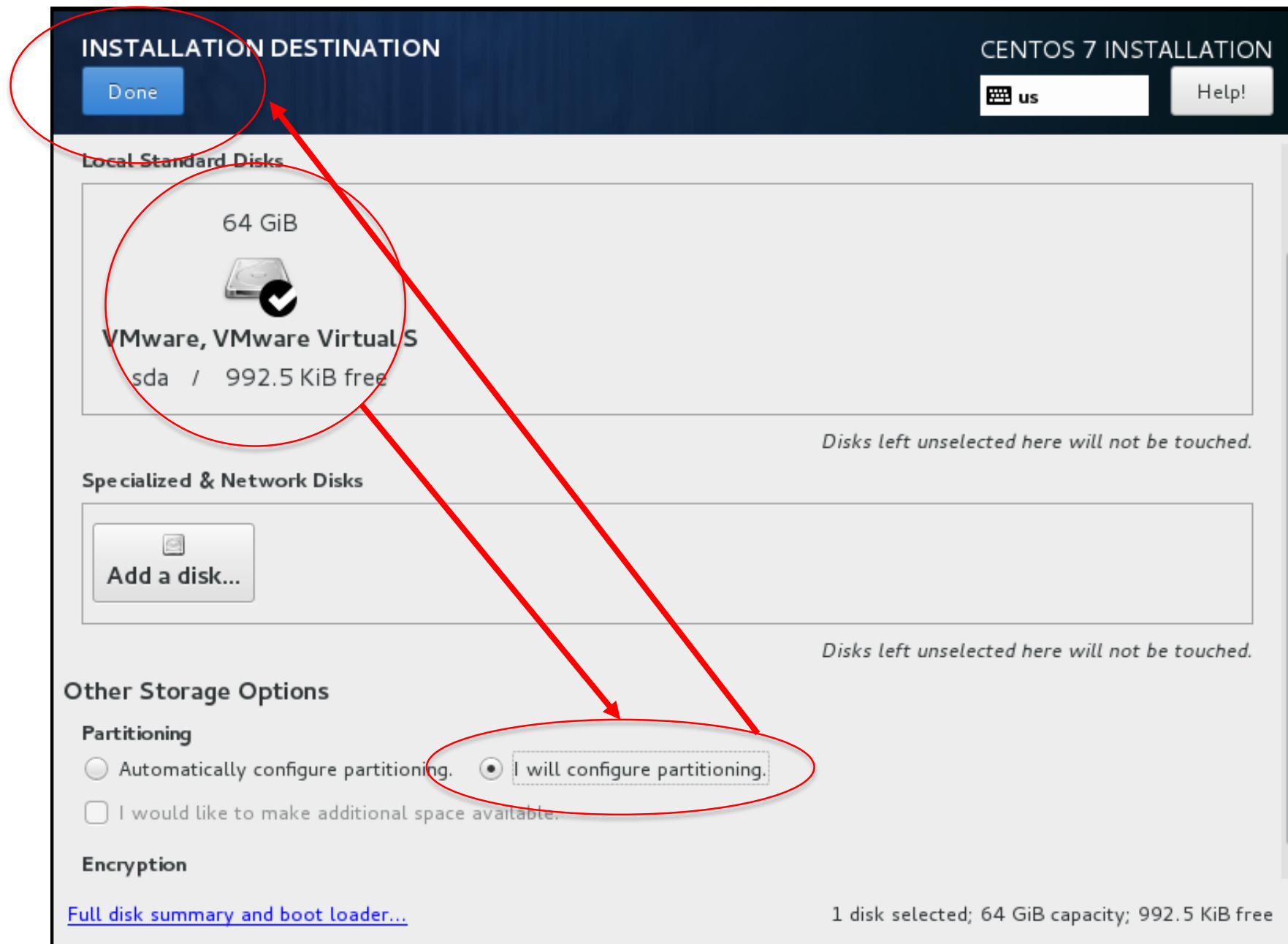
การติดตั้ง CentOS 7 : Disk Partition (Auto partition)



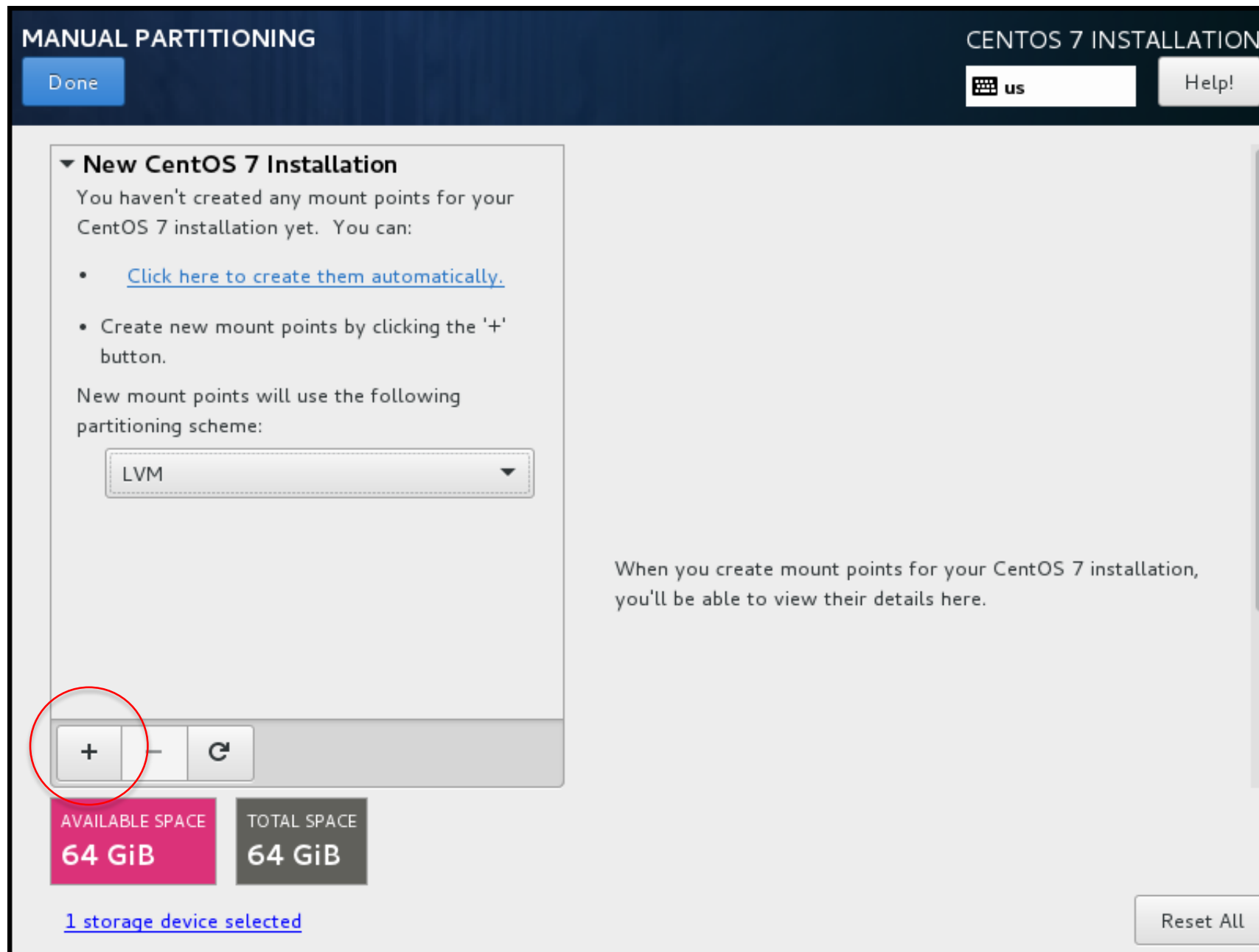
การติดตั้ง CentOS 7 : Disk Partition (Auto partition)



การติดตั้ง CentOS 7 : Disk Partition (Manual partition)



การติดตั้ง CentOS 7 : Disk Partition (Manual partition)



การติดตั้ง CentOS 7 : Disk Partition (Manual partition)

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

Mount Point:

Desired Capacity:

MANUAL PARTITIONING CENTOS 7 INSTALLATION

us

▼ New CentOS 7 Installation

SYSTEM

/boot	512 MiB	>
sda1		

sda1

Mount Point:

Desired Capacity:

Device Type: ☐ Encrypt

File System: ☒ Reformat

Label:

Name:

AVAILABLE SPACE: **63.5 GiB**

TOTAL SPACE: **64 GiB**

[1 storage device selected](#)

การติดตั้ง CentOS 7 : Disk Partition (Manual partition)

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

Mount Point:

Desired Capacity:

MANUAL PARTITIONING CENTOS 7 INSTALLATION

us

▼ New CentOS 7 Installation

SYSTEM	
/boot sda1	512 MiB
swap sda2	4096 MiB >

AVAILABLE SPACE
59.5 GiB

TOTAL SPACE
64 GiB

[1 storage device selected](#)

sda2

Mount Point:

Desired Capacity:

Device Type: ☐ Encrypt

File System: ☒ Reformat

Label:

Name:

การติดตั้ง CentOS 7 : Disk Partition (Manual partition)

ADD A NEW MOUNT POINT

More customization options are available after creating the mount point below.

Mount Point:

Desired Capacity:

MANUAL PARTITIONING CENTOS 7 INSTALLATION

us

▼ New CentOS 7 Installation

SYSTEM	
/boot sda1	512 MiB
/ sda3	59.5 GiB >
swap sda2	4096 MiB

AVAILABLE SPACE **992.5 KiB** TOTAL SPACE **64 GiB**

[1 storage device selected](#)

sda3

Mount Point: Device(s): VMware, VMware Virtual S (sda)

Desired Capacity:

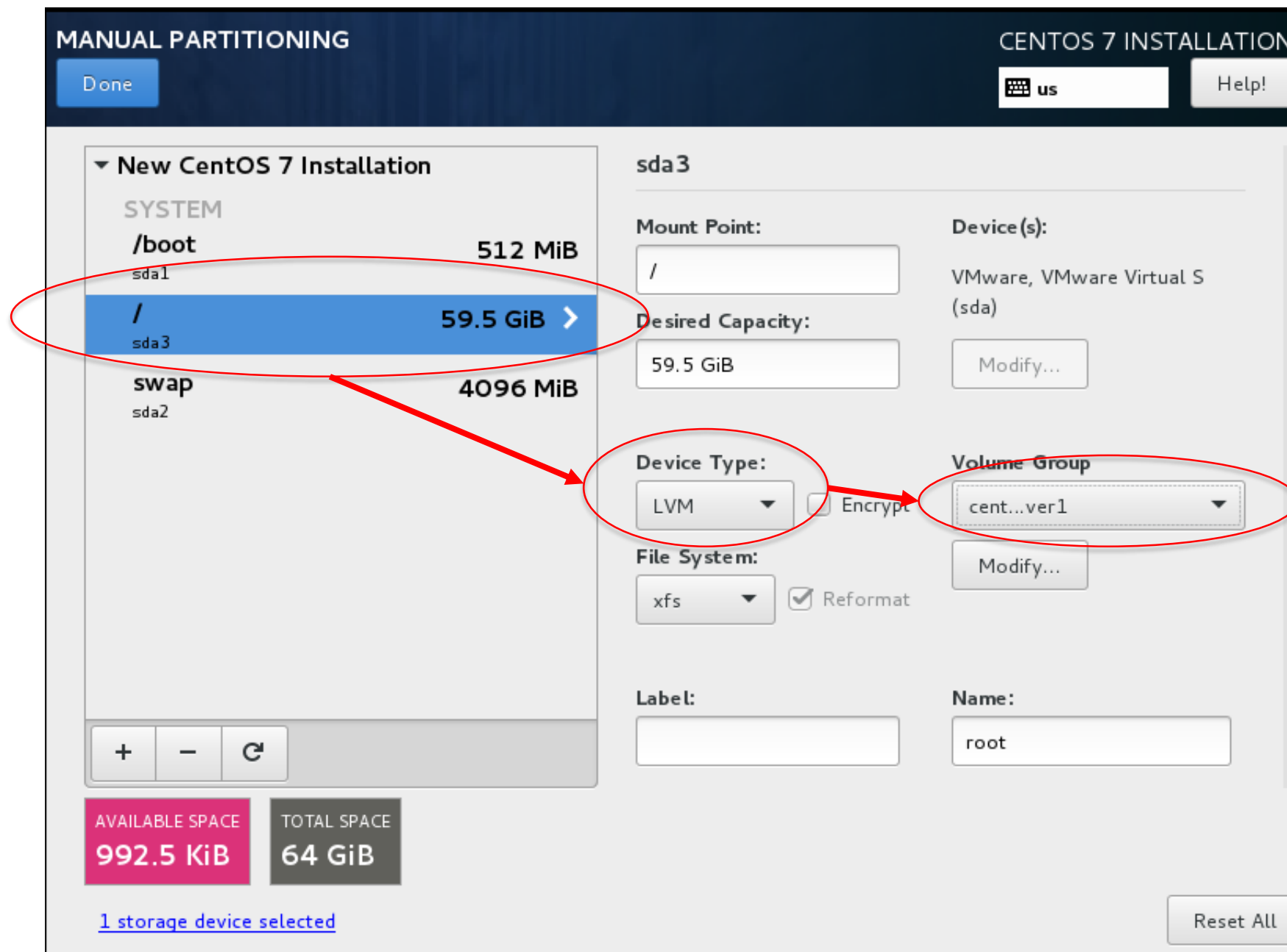
Device Type: ☐ Encrypt

File System: ☒ Reformat

Label: Name:



การติดตั้ง CentOS 7 : Disk Partition (Manual partition)



การติดตั้ง CentOS 7 : Disk Partition (Manual partition)

CONFIGURE VOLUME GROUP

Please create a name for this volume group and select at least one disk below.

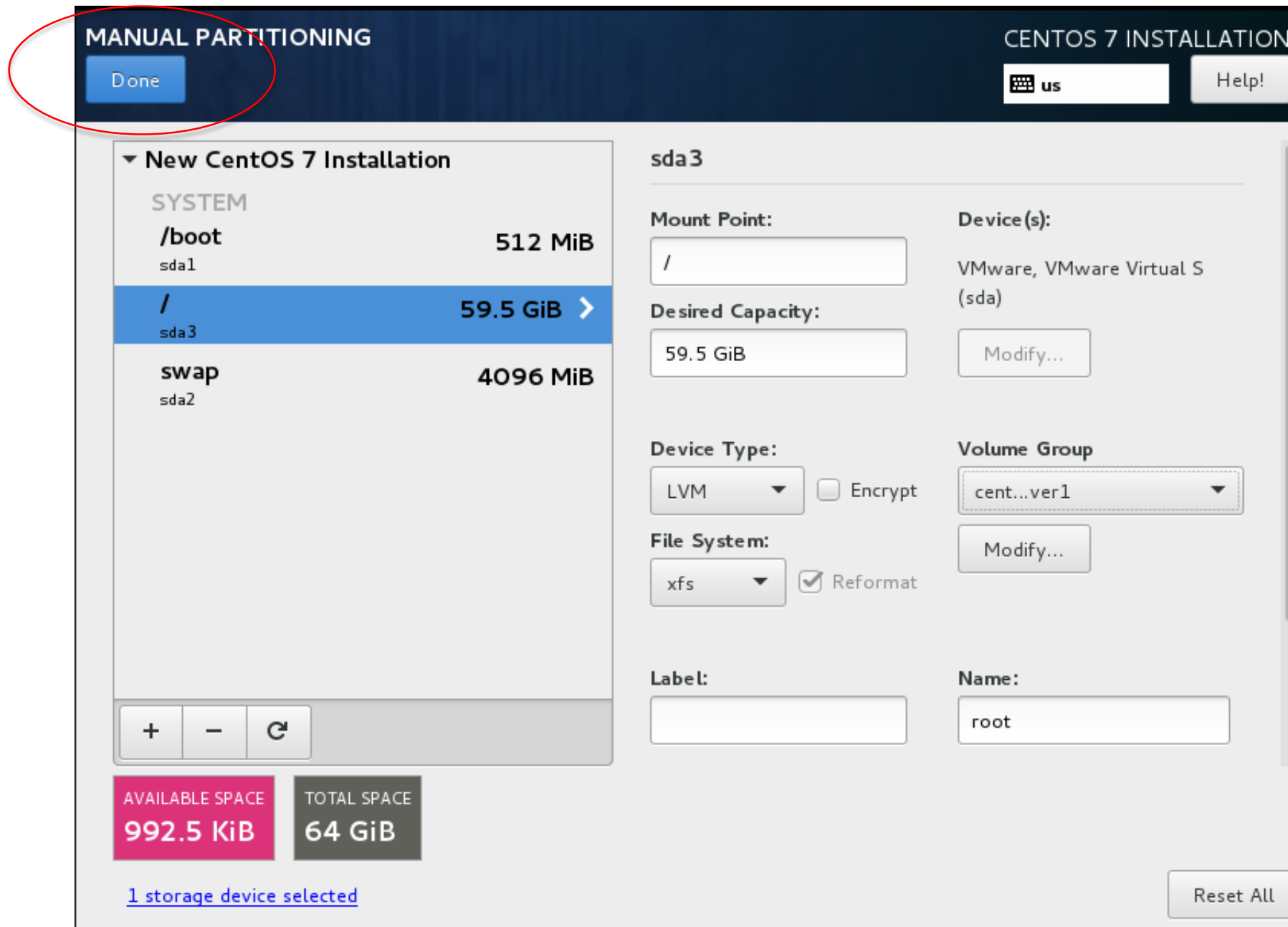
Name:

Disk	Capacity	Free	ID
VMware, VMware Virtual S	64 GiB	992.5 KiB	

RAID Level: ☐ Encrypt

Size policy:

การติดตั้ง CentOS 7 : Disk Partition (Manual partition)



The screenshot shows the 'MANUAL PARTITIONING' window in the CentOS 7 installer. The window title is 'CENTOS 7 INSTALLATION'. In the top-left corner, the 'MANUAL PARTITIONING' text is circled in red, and a 'Done' button is located directly below it. The main area is divided into two panels. The left panel, titled 'New CentOS 7 Installation', shows a list of partitions under the 'SYSTEM' heading: '/boot' (sda1, 512 MiB), '/' (sda3, 59.5 GiB, highlighted with a blue bar and a right arrow), and 'swap' (sda2, 4096 MiB). Below this list are three buttons: '+', '-', and a circular arrow icon. At the bottom of the left panel, a pink box displays 'AVAILABLE SPACE 992.5 KiB' and a grey box displays 'TOTAL SPACE 64 GiB'. A link at the bottom left of the left panel reads '1 storage device selected'. The right panel is for configuring the selected partition 'sda3'. It includes fields for 'Mount Point:' (set to '/'), 'Desired Capacity:' (set to '59.5 GiB'), 'Device Type:' (set to 'LVM'), 'File System:' (set to 'xfs'), 'Label:', and 'Name:' (set to 'root'). There are also checkboxes for 'Encrypt' (unchecked) and 'Reformat' (checked). A 'Volume Group' dropdown is set to 'cent...ver1'. 'Modify...' buttons are present for the capacity and volume group. A 'Reset All' button is in the bottom right corner. The top right of the window shows a keyboard layout selector set to 'us' and a 'Help!' button.

MANUAL PARTITIONING CENTOS 7 INSTALLATION

[Done](#)

▼ New CentOS 7 Installation

SYSTEM

Partition	Device	Size
/boot	sda1	512 MiB
/	sda3	59.5 GiB
swap	sda2	4096 MiB

+ - ↻

AVAILABLE SPACE
992.5 KiB

TOTAL SPACE
64 GiB

[1 storage device selected](#)

sda3

Mount Point:
/

Desired Capacity:
59.5 GiB

Device Type:
LVM ☐ Encrypt

File System:
xfs ☒ Reformat

Volume Group
cent...ver1

Label:

Name:
root

[Modify...](#) [Modify...](#)

[Reset All](#)

การติดตั้ง CentOS 7 : Disk Partition

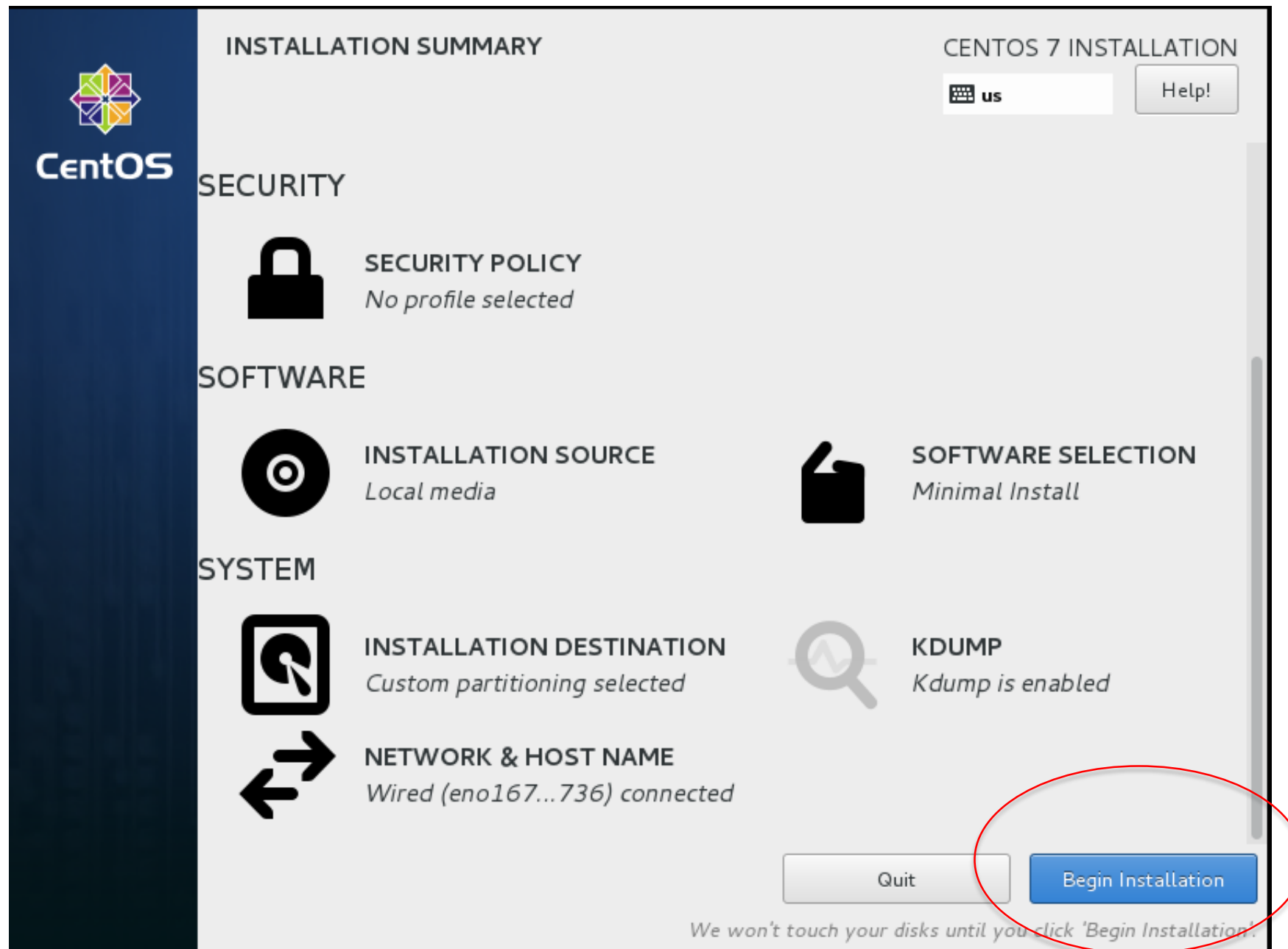
SUMMARY OF CHANGES

Your customizations will result in the following changes taking effect after you return to the main menu and begin installation:

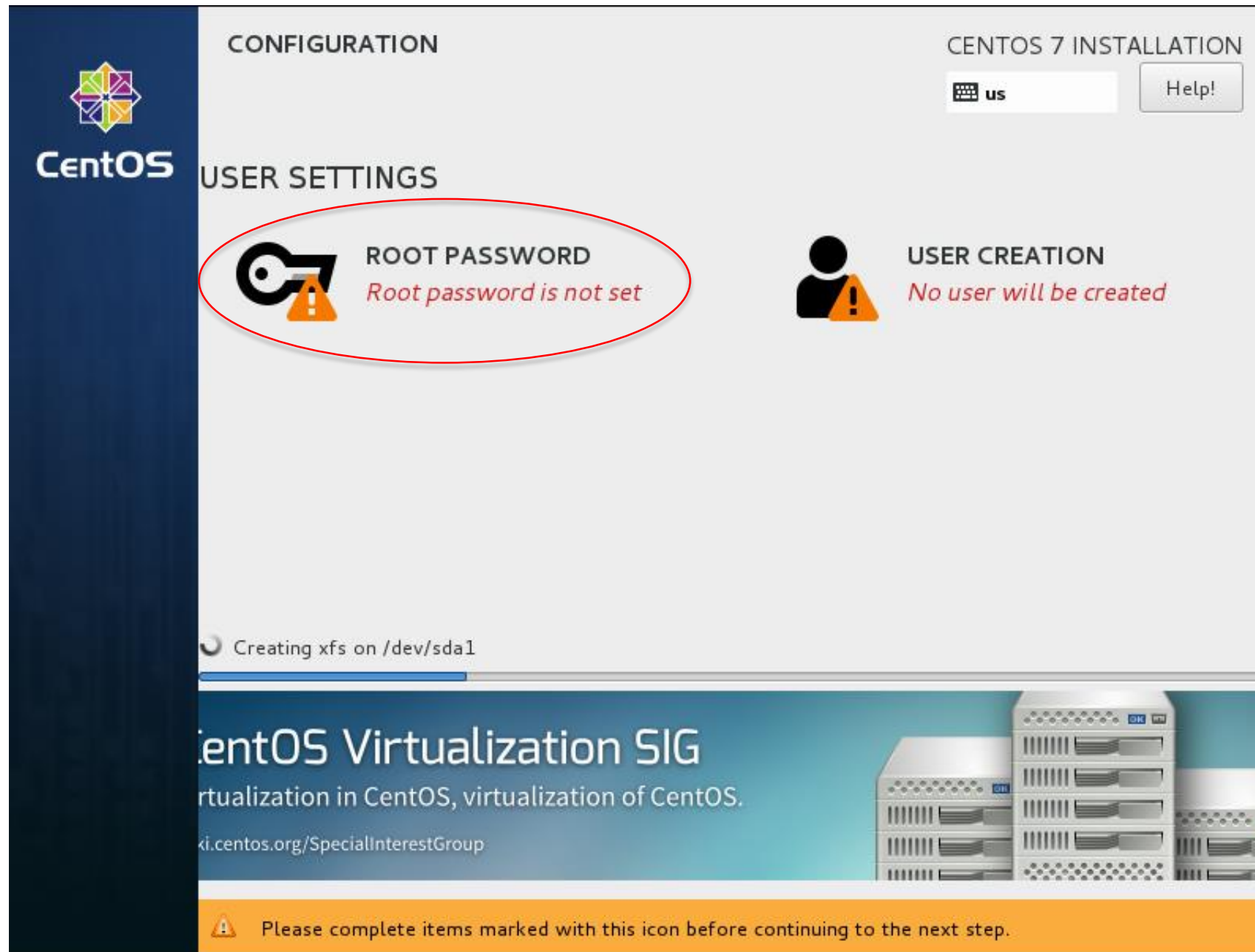
Order	Action	Type	Device Name	Mount point
1	Destroy Format	Unknown	sda	
2	Create Format	partition table (MSDOS)	sda	
3	Create Device	partition	sda1	
4	Create Device	partition	sda2	
5	Create Device	partition	sda3	
6	Create Format	physical volume (LVM)	sda3	
7	Create Device	lvmvg	centos_server1	
8	Create Device	lvmlv	centos_server1-root	
9	Create Format	xf	centos_server1-root /	
10	Create Format	swap	sda2	
11	Create Format	xf	sda1	/boot

Cancel & Return to Custom Partitioning Accept Changes

การติดตั้ง CentOS 7



การติดตั้ง CentOS 7 : Username/Password



การติดตั้ง CentOS 7 : Username/Password

ROOT PASSWORD

CENTOS 7 INSTALLATION

Done

us

Help!

The root account is used for administering the system. Enter a password for the root user.

Root Password:

Strong

Confirm:

การติดตั้ง CentOS 7 : Username/Password



The screenshot shows the 'ROOT PASSWORD' screen during 'CENTOS 7 INSTALLATION'. The 'Done' button is circled in red. The password field shows a strength indicator labeled 'Weak'. A large red arrow points from the 'Weak' label to a warning message at the bottom.

ROOT PASSWORD CENTOS 7 INSTALLATION

Done us Help!

The root account is used for administering the system. Enter a password for the root user.

Root Password:

Weak

Confirm:

Weak Password Warning!

 The password you have provided is weak: The password fails the dictionary check - it is based on a dictionary word. You will have to press Done twice to confirm it.

การติดตั้ง CentOS 7 : Username/Password

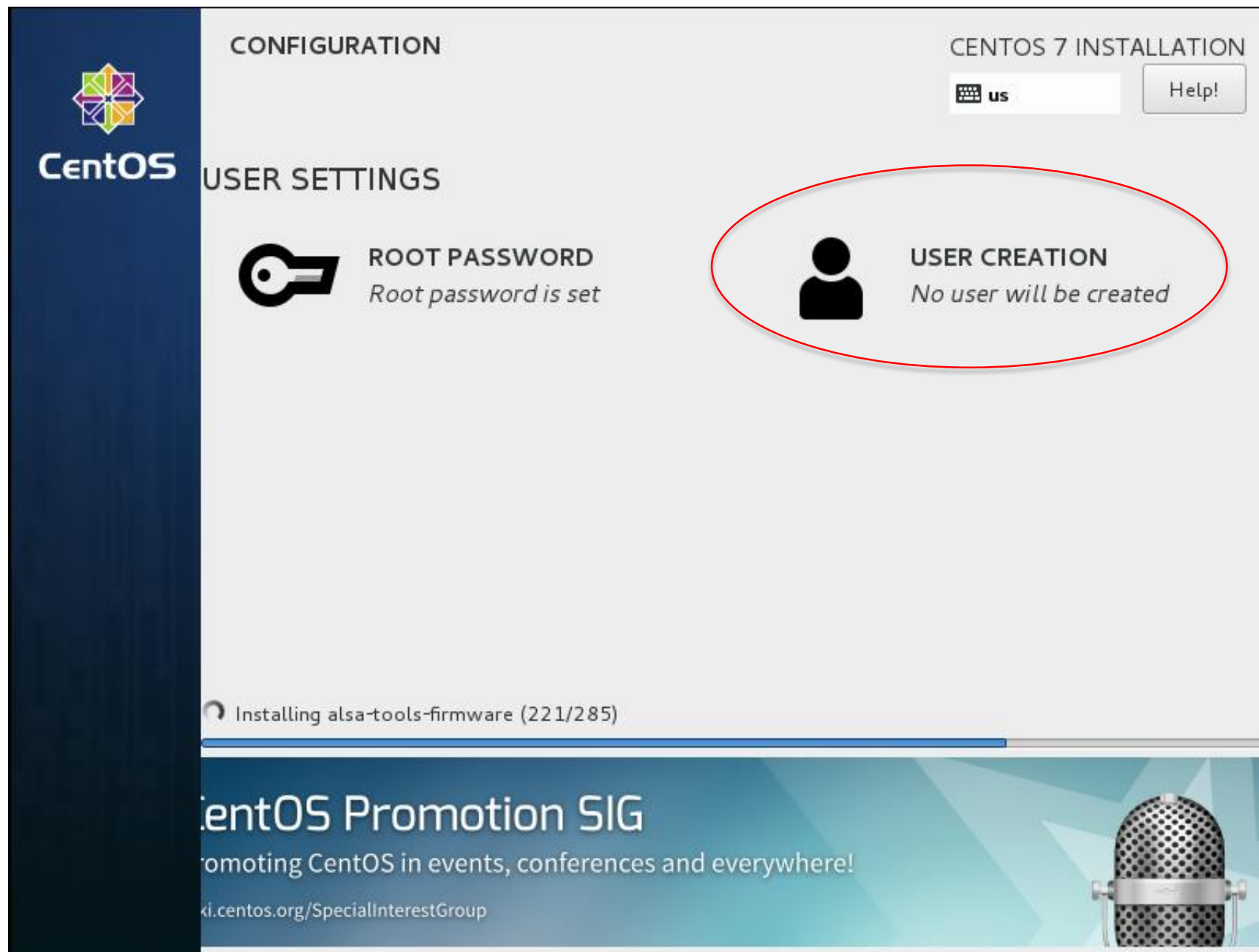


The screenshot shows the 'ROOT PASSWORD' screen during CentOS 7 installation. The title bar includes 'ROOT PASSWORD' and 'CENTOS 7 INSTALLATION'. A 'Done' button is circled in red. The main text states: 'The root account is used for administering the system. Enter a password for the root user.' Below this are two password input fields. The first field, labeled 'Root Password:', contains a password represented by dots. A strength indicator bar below it is mostly red and labeled 'Weak'. The second field, labeled 'Confirm:', also contains a password represented by dots. A large red arrow points from the 'Weak' label to a warning message at the bottom. The warning message, on an orange background, reads: 'You have provided a weak password: The password fails the dictionary check - it is based on a dictionary word. Press Done again to use anyway.'

Weak Password Warning!

You have provided a weak password: The password fails the dictionary check - it is based on a dictionary word. Press Done again to use anyway.

การติดตั้ง CentOS 7 : Username/Password



การติดตั้ง CentOS 7 : Username/Password

CREATE USER

Done

CENTOS 7 INSTALLATION

us

Help!

Full name

Trojan Horse

User name

horse

Tip: Keep your user name shorter than 32 characters and do not use spaces.

☒ Make this user administrator

☒ Require a password to use this account

Password

••••••••

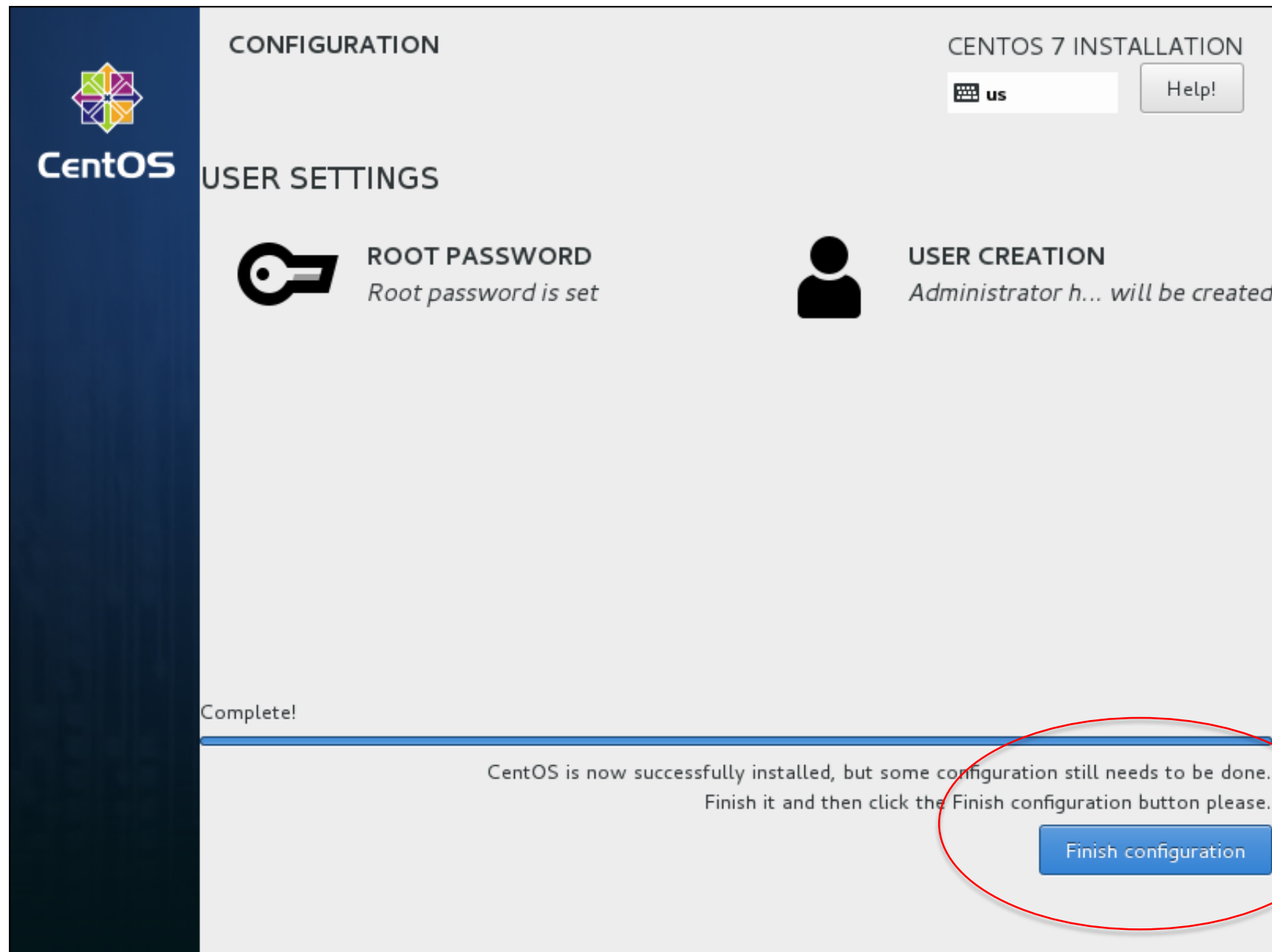
Fair

Confirm password

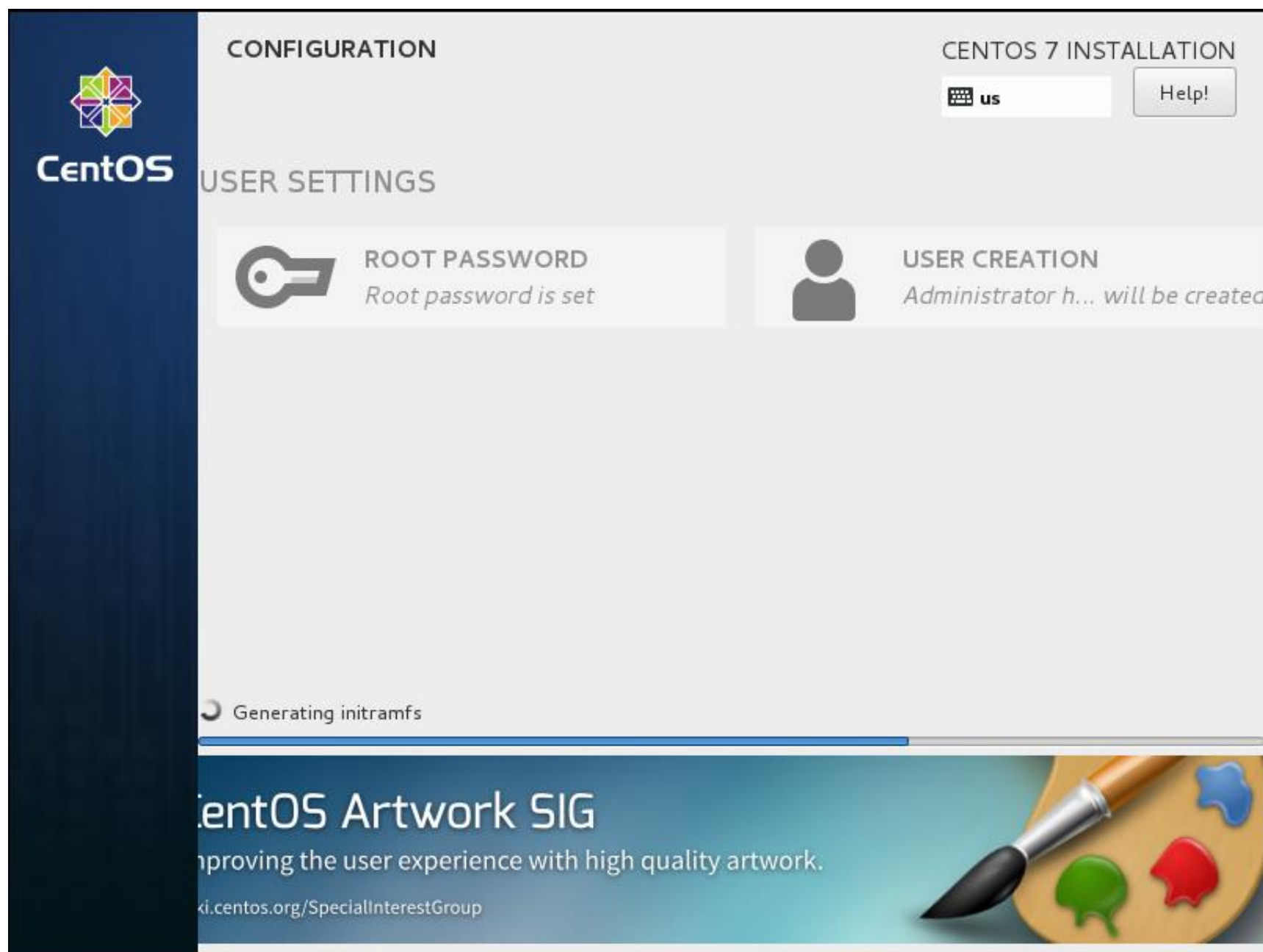
••••••••

Advanced...

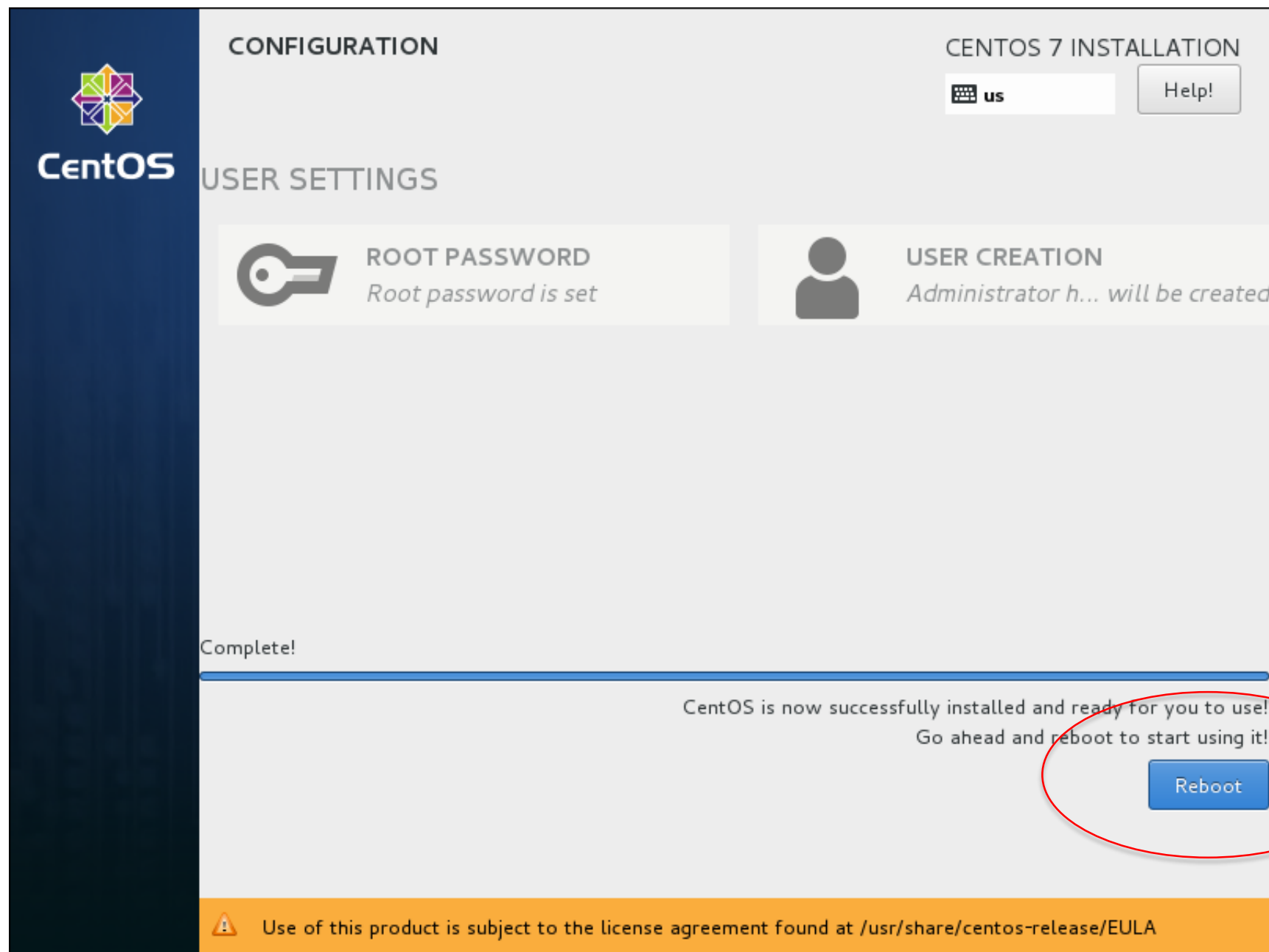
การติดตั้ง CentOS 7 : Username/Password



การติดตั้ง CentOS 7



การติดตั้ง CentOS 7



การติดตั้ง CentOS 7 : พร้อมใช้งาน

```
CentOS Linux 7 (Core)  
Kernel 3.10.0-327.el7.x86_64 on an x86_64  
  
server1 login:
```



```
CentOS Linux 7 (Core)  
Kernel 3.10.0-327.el7.x86_64 on an x86_64  
  
server1 login: root  
Password:  
Last login: Tue Jul 26 19:03:48 on tty2  
[root@server1 ~]#  
[root@server1 ~]#
```

ข้อยกเว้นสำหรับเอกสารนี้ !!!!!!!

เพื่อให้่ายในการทดสอบปฏิบัติใน Class นี้ จึงขอให้ทำการ Disable SELINUX ดังนี้

- ทำการแก้ไขไฟล์ /etc/selinux/config ดังนี้

SELINUX=disabled

- ทำการแก้ไขโหมดการทำงานของ SELINUX เป็น Permissive

```
[root@server1 ~]# setenforce 0
```

- ตรวจสอบการทำงานของ SELINUX

```
[root@server1 ~]# getenforce
```

Permissive

การเทียบเวลาเครื่องกับ Time server

```
[root@server1 ~]# yum -y install ntpdate
```

```
[root@server1 ~]# ntpdate time.navy.mi.th
```

```
26 Jul 11:29:06 ntpdate[2399]: step time server 113.53.247.3 offset -28788.342002  
sec
```

```
[root@server1 ~]# date
```

```
Tue Jul 26 11:29:16 ICT 2016
```

แนะนำให้ติดตั้งเพิ่ม !!!

```
[root@server1 ~]# yum -y install wget net-tools epel-release
```

หมายเหตุ

wget ใช้สำหรับ Download ไฟล์จาก Network

net-tools เป็นชุดคำสั่งเกี่ยวกับการจัดการเครือข่าย เช่น ifconfig , netstat เป็นต้น

epel-release เป็น repo สำหรับการติดตั้ง Software package บางตัว

การ Update/Upgrade ระบบ

```
[root@server1 ~]# yum -y upgrade
```

```
Loaded plugins: fastestmirror
```

```
Loading mirror speeds from cached hostfile
```

```
* base: mirror1.ku.ac.th
```

```
* extras: mirror1.ku.ac.th
```

```
* updates: mirror1.ku.ac.th
```

```
Resolving Dependencies
```

```
.....
```

```
.....
```

```
.....
```

```
Complete!
```

```
[root@server1 ~]# reboot
```

Local Firewall by iptables

ติดตั้ง iptables-services

```
[root@server1 ~]# yum -y install iptables-service
```

กำหนดให้ iptables ทำงานทุกครั้งเมื่อมีการ reboot เครื่อง

```
[root@server1 ~]# systemctl enable iptables
```

เปิดการทำงานของ iptables

```
[root@server1 ~]# systemctl start iptables
```

iptables

ตรวจสอบการทำงานของ iptables

```
root@server1 ~]# iptables -nvL
```

```
[root@server1 ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
  203 14596 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
    1   104 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 125 packets, 14680 bytes)
 pkts bytes target    prot opt in     out     source            destination
```

iptables

แก้ไข Rules ของ iptables โดยการแก้ไขไฟล์ /etc/sysconfig/iptables

```
*filter
```

```
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
```

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A INPUT -p icmp -j ACCEPT
```

```
-A INPUT -i lo -j ACCEPT
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

```
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

```
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
```

```
COMMIT
```

iptables

ตัวอย่างการเพิ่ม Rules ของ iptables

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT  
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT  
-A INPUT -p tcp -m state --state NEW -m tcp --dport 3306 -j ACCEPT
```

เมื่อแก้ไขเสร็จแล้ว ทำการ restart iptables

```
[root@server1 ~]# systemctl restart iptables
```

iptables

ตรวจสอบการทำงานของ iptables

```
[root@server1 ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
  37  2712 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 ACCEPT    tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         state NEW tcp dpt:80
   0     0 ACCEPT    tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         state NEW tcp dpt:443
   0     0 ACCEPT    tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         state NEW tcp dpt:3306
   7   546 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 23 packets, 2332 bytes)
 pkts bytes target    prot opt in     out     source            destination
```

หมายเหตุ สำหรับ IPv6 ให้เปลี่ยน command จาก iptables เป็น ip6tables

SSH basic Hardening

- Disable Root Login

แก้ไขไฟล์ `/etc/ssh/sshd_config`

จากเดิม

```
#PermitRootLogin yes
```

แก้เป็น

```
PermitRootLogin no
```

แล้วทำการ restart SSH service

```
[root@server1 ~]# systemctl restart sshd
```

SSH basic Hardening

- อนุญาตเฉพาะบาง Users หรือ บาง Groups เท่านั้นที่สามารถ Login ได้
- แก้ไขไฟล์ `/etc/ssh/sshd_config` โดยเพิ่ม Configuration ต่อไปนี้

กรณีอนุญาต Users

```
AllowUsers user1 user2 user3
```

กรณีอนุญาต Groups

```
AllowGroups group1 group2 group3
```

แล้วทำการ restart SSH service

```
[root@server1 ~]# systemctl restart sshd
```

SSH basic Hardening

- ไม่อนุญาตเฉพาะบาง Users หรือ บาง Groups ให้สามารถ Login ได้

แก้ไขไฟล์ `/etc/ssh/sshd_config` โดยเพิ่ม Configuration ต่อไปนี้

กรณีไม่อนุญาต Users

```
DenyUsers user1 user2 user3
```

กรณีไม่อนุญาต Groups

```
DenyGroups group1 group2 group3
```

แล้วทำการ restart SSH service

```
[root@server1 ~]# systemctl restart sshd
```

SSH basic Hardening

ตัวอย่าง Log ของ SSH (/var/log/secure)

Aug 7 17:20:22 server1 sshd[4284]: User webadmin from 192.168.146.1 **not allowed because none of user's groups are listed in AllowGroups**

Aug 7 17:23:47 server1 sshd[4304]: User webadmin from 192.168.146.1 **not allowed because a group is listed in DenyGroups**

Aug 7 17:25:31 server1 sshd[4307]: Failed password for root from 192.168.146.1 port 62404 ssh2

Aug 7 17:26:32 server1 sshd[4320]: Accepted password for webadmin from 192.168.146.1 port 62412 ssh2

Aug 7 17:26:32 server1 sshd[4320]: pam_unix(sshd:session): session opened for user webadmin by (uid=0)

Aug 7 17:26:34 server1 sshd[4320]: pam_unix(sshd:session): session closed for user webadmin

การส่ง System Log ไปเก็บที่ Syslog server

แก้ไขไฟล์ `/etc/rsyslog.conf`

กรณีส่งแบบ UDP

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

กรณีส่งเป็น TCP

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

จากนั้นทำการ restart syslog service

```
[root@server1 ~]# systemctl restart rsyslog
```

การติดตั้ง NTP service

```
[root@server1 ~]# yum -y install ntp
```

```
[root@server1 ~]# systemctl enable ntpd
```

Created symlink from /etc/systemd/system/multi-user.target.wants/ntpd.service to /usr/lib/systemd/system/ntpd.service.

```
[root@server1 ~]# systemctl start ntpd
```

- ntpd.service - Network Time Service

Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)

Active: **active (running)** since Wed 2016-07-27 21:45:35 ICT; 7h left

Main PID: 2496 (ntpd)

CGroup: /system.slice/ntpd.service

└─2496 /usr/sbin/ntpd -u ntp:ntp -g

การติดตั้ง NTP service

- แก้ไข Time server โดยการแก้ไขไฟล์ `/etc/ntp.conf`

```
server time.ega.or.th iburst
```

```
server time.navy.mi.th iburst
```

```
server time1.nimt.or.th iburst
```

```
server time2.nimt.or.th iburst
```

จากนั้นทำการ restart service

```
[root@server1 ~]# systemctl restart ntpd
```

การติดตั้ง NTP service

ทำการตรวจสอบการทำงานผ่าน ntpq

```
[root@server1 ~]# ntpq -pn
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
=====									
*164.115.18.123	.PPS.	1	u	15	64	1	1.553	28.889	17.840
113.53.247.3	.PPS.	1	u	26	64	0	0.000	0.000	0.000
203.185.69.60	.IRIG.	1	u	26	64	0	0.000	0.000	0.000
203.185.69.59	.GPS.	1	u	26	64	0	0.000	0.000	0.000

```
[root@server1 ~]# timedatectl
```

Local time: Wed 2016-07-27 13:56:20 ICT

Universal time: Wed 2016-07-27 06:56:20 UTC

RTC time: Wed 2016-07-27 06:56:19

Time zone: Asia/Bangkok (ICT, +0700)

NTP enabled: yes

NTP synchronized: yes

RTC in local TZ: no

DST active: n/a

MariaDB

<https://mariadb.org/about/>

About MariaDB

MariaDB is one of the most popular database servers in the world. It's made by the original developers of MySQL and guaranteed to stay open source. Notable users include Wikipedia, Facebook and Google.

MariaDB turns data into structured information in a wide array of applications, ranging from banking to websites. It is an enhanced, drop-in replacement for MySQL. MariaDB is used because it is fast, scalable and robust, with a rich ecosystem of storage engines, plugins and many other tools make it very versatile for a wide variety of use cases.

MariaDB is developed as open source software and as a relational database it provides an SQL interface for accessing data. The latest versions of MariaDB also include GIS and JSON features.

More information can be found in the MariaDB Knowledge Base, for example:

- › [MariaDB vs. MySQL – Features](#)
- › [MariaDB vs. MySQL – Compatibility](#)
- › [MariaDB Success Stories](#)

There is also a good Wikipedia article about MariaDB and the MySQL history.

MariaDB

ติดตั้ง MariaDB server

```
[root@server1 ~]# yum -y install mariadb-server
```

กำหนดให้ MariaDB ทำงานทุกครั้งเมื่อมีการ reboot เครื่อง

```
[root@server1 ~]# systemctl enable mariadb
```

สั่งให้ MariaDB service ทำงาน

```
[root@server1 ~]# systemctl start mariadb
```

MariaDB

ตรวจสอบสถานะของ MariaDB service

```
[root@server1 ~]# systemctl status mariadb
```

- mariadb.service - MariaDB database server

Loaded: loaded (/usr/lib/systemd/system/mariadb.service; **enabled**; vendor preset: disabled)

Active: active (running) since Sat 2016-08-06 18:15:59 ICT; 23s ago

Process: 10138 ExecStartPost=/usr/libexec/mariadb-wait-ready \$MAINPID (code=exited, status=0/SUCCESS)

Process: 10058 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)

Main PID: 10137 (mysqld_safe)

CGroup: /system.slice/mariadb.service

└─10137 /bin/sh /usr/bin/mysqld_safe --basedir=/usr

└─10295 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql/plugin --log-error=/var/log/mariadb/mariadb.log --pid-file=/var/r...

MariaDB

ตรวจสอบสถานะของ MariaDB service

```
[root@server1 ~]# 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	10295/mysqld

MariaDB : mysql_secure_installation

การกำหนด Password ให้ Root ของ MariaDB

```
[root@server1 ~]# mysql_secure_installation
```

...

Enter current password for root (enter for none): <ENTER>

OK, successfully used password, moving on...

MariaDB : mysql_secure_installation

Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation.

Set root password? [Y/n] <ENTER>

New password: <New Password>

Re-enter new password: <New Password>

Password updated successfully!

Reloading privilege tables..

... Success!

MariaDB : mysql_secure_installation

By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.

Remove anonymous users? [Y/n] <ENTER>

... Success!

MariaDB : mysql_secure_installation

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] <ENTER>

... Success!

By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? [Y/n] <ENTER>

- Dropping test database...

... Success!

- Removing privileges on test database...

... Success!



MariaDB : mysql_secure_installation

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? [Y/n] <ENTER>

... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB installation should now be secure.

Thanks for using MariaDB!

MariaDB

ทดสอบการเข้าใช้งาน MariaDB

```
[root@server1 ~]# mysql -u root -p
```

```
[root@server1 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 5.5.47-MariaDB MariaDB Server

Copyright (c) 2000, 2015, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
MariaDB [(none)]> show databases;
+-----+
| Database                |
+-----+
| information_schema       |
| mysql                    |
| performance_schema       |
+-----+
3 rows in set (0.00 sec)
```

MariaDB

การกำหนดให้ MariaDB สามารถเข้าใช้งานได้จาก Localhost เท่านั้น (ซึ่งเหมาะสมในกรณีที่ Application และ Database อยู่บนเครื่องเดียวกัน)

โดยให้ทำการแก้ไขไฟล์ชื่อ `/etc/my.cnf` แล้วใส่ค่า Configuration ดังนี้

```
[mysqld]
```

```
bind-address=127.0.0.1
```

จากนั้นทำการ restart mariadb

```
[root@server1 ~]# systemctl restart mariadb
```

MariaDB

ตรวจสอบสถานะของ MariaDB service

```
[root@server1 ~]# netstat -antp
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	10649/mysqld

MariaDB

การเปลี่ยน User Root ของ Database

Login เข้า MariaDB โดย root

```
[root@server1 etc]# mysql -u root -p
```

Enter password: <password>

ทำการแก้ไข Username ด้วยคำสั่ง

```
MariaDB [(none)]> use mysql;
```

```
MariaDB [mysql]> update user set user="zeus" where user="root";
```

```
MariaDB [mysql]> flush privileges;
```

MariaDB

การเปลี่ยน User Root ของ Database

- ก่อนเปลี่ยน

```
MariaDB [mysql]> select user,password,host from user;
```

user	password	host
root	*8061C323A725701555411A7E18421F077A840CD7	localhost
root	*8061C323A725701555411A7E18421F077A840CD7	127.0.0.1
root	*8061C323A725701555411A7E18421F077A840CD7	:::1

3 rows in set (0.01 sec)

- หลังเปลี่ยน

```
MariaDB [mysql]> select user,password,host from user;
```

user	password	host
zeus	*8061C323A725701555411A7E18421F077A840CD7	localhost
zeus	*8061C323A725701555411A7E18421F077A840CD7	127.0.0.1
zeus	*8061C323A725701555411A7E18421F077A840CD7	:::1

3 rows in set (0.01 sec)

MariaDB

การเปลี่ยน User Root ของ Database

```
[root@server1 ~]# mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
```

```
[root@server1 ~]# mysql -u zeus -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19
Server version: 5.5.47-MariaDB MariaDB Server

Copyright (c) 2000, 2015, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

MariaDB

ลบ MySQL History file

โดยปกติ MariaDB หรือ MySQL จะเก็บประวัติการใช้คำสั่ง SQL ไว้ที่ ~/.mysql_history เช่น /root/.mysql_history หรือที่ /home/<username>/.mysql_history

การแก้ไขสามารถทำได้โดยลบไฟล์นั้นทิ้งได้โดยตรง และสร้าง Shortcut ไปที่ /dev/null เพื่อป้องกันการเขียนประวัติในอนาคต ดังนี้

```
[root@server1 ~]# ls -la /root/.mysql_history
```

```
-rw----- 1 root root 662 Aug  6 23:46 /root/.mysql_history
```

```
[root@server1 ~]# rm /root/.mysql_history
```

```
rm: remove regular file '/root/.mysql_history'? y
```

MariaDB

ลบ MySQL History file

ทำการสร้าง Shortcut ไปยัง /dev/null

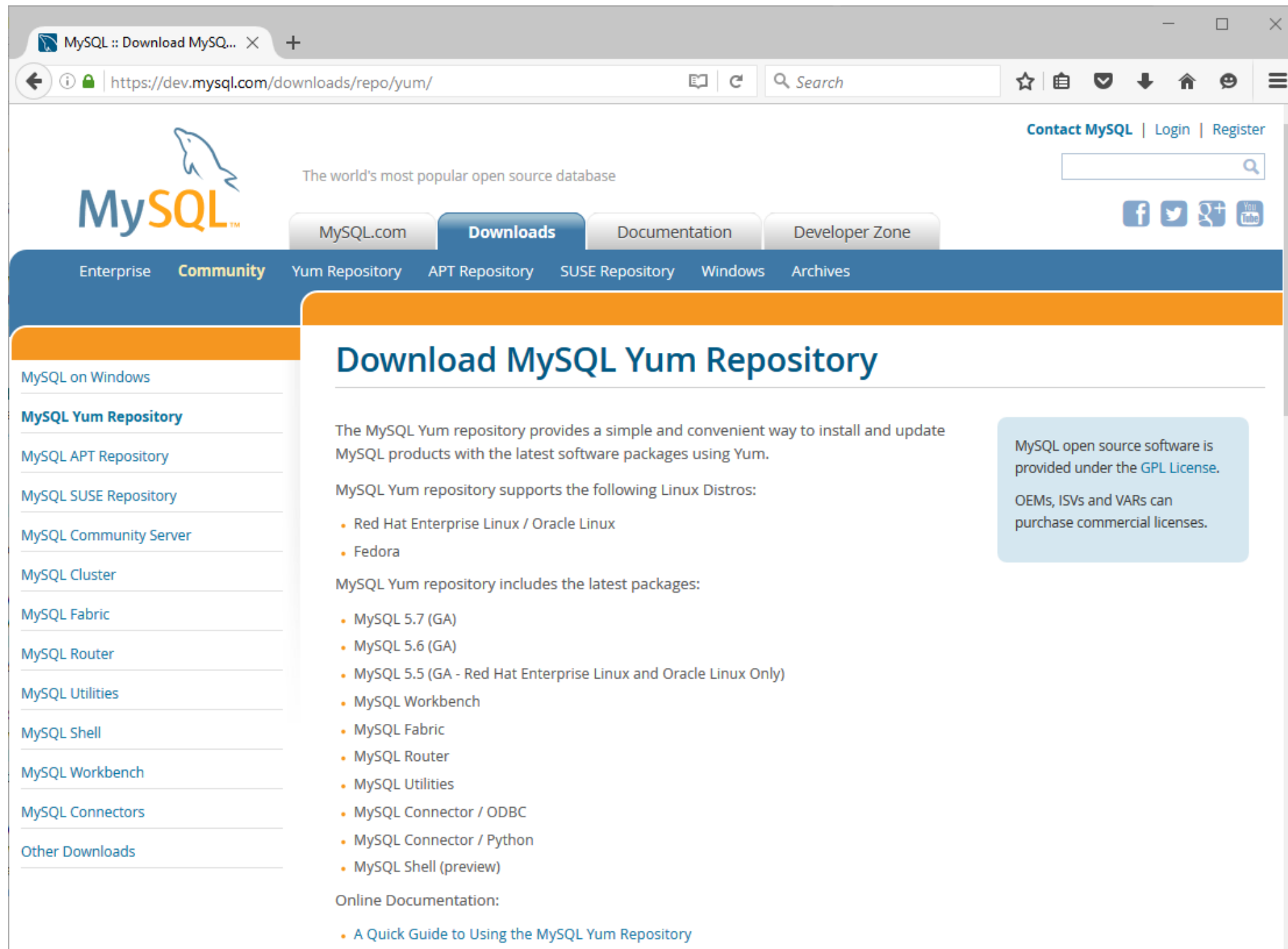
```
[root@server1 ~]# ln -s /dev/null /root/.mysql_history
```

ตรวจสอบโดย

```
[root@server1 ~]# ls -la /root/.mysql_history
```

```
lrwxrwxrwx 1 root root 9 Aug  6 23:55 /root/.mysql_history -> /dev/null
```

MySQL



The screenshot shows a web browser window with the URL <https://dev.mysql.com/downloads/repo/yum/>. The page features the MySQL logo and tagline "The world's most popular open source database". The navigation bar includes links for MySQL.com, Downloads (active), Documentation, and Developer Zone. A secondary navigation bar lists Enterprise, Community (active), Yum Repository, APT Repository, SUSE Repository, Windows, and Archives. The left sidebar contains a list of links: MySQL on Windows, MySQL Yum Repository (active), MySQL APT Repository, MySQL SUSE Repository, MySQL Community Server, MySQL Cluster, MySQL Fabric, MySQL Router, MySQL Utilities, MySQL Shell, MySQL Workbench, MySQL Connectors, and Other Downloads. The main content area is titled "Download MySQL Yum Repository" and explains that the repository provides a simple way to install and update MySQL products. It lists supported Linux distributions: Red Hat Enterprise Linux / Oracle Linux and Fedora. A list of available packages is provided, including MySQL 5.7 (GA), MySQL 5.6 (GA), MySQL 5.5 (GA - Red Hat Enterprise Linux and Oracle Linux Only), MySQL Workbench, MySQL Fabric, MySQL Router, MySQL Utilities, MySQL Connector / ODBC, MySQL Connector / Python, and MySQL Shell (preview). A link to "A Quick Guide to Using the MySQL Yum Repository" is also present. A right-hand sidebar contains information about the GPL license and commercial licenses for OEMs, ISVs, and VARs.

MySQL :: Download MySQL... X +

https://dev.mysql.com/downloads/repo/yum/ Search

Contact MySQL | Login | Register

MySQL.com Downloads Documentation Developer Zone

Enterprise Community Yum Repository APT Repository SUSE Repository Windows Archives

Download MySQL Yum Repository

The MySQL Yum repository provides a simple and convenient way to install and update MySQL products with the latest software packages using Yum.

MySQL Yum repository supports the following Linux Distro:

- Red Hat Enterprise Linux / Oracle Linux
- Fedora

MySQL Yum repository includes the latest packages:

- MySQL 5.7 (GA)
- MySQL 5.6 (GA)
- MySQL 5.5 (GA - Red Hat Enterprise Linux and Oracle Linux Only)
- MySQL Workbench
- MySQL Fabric
- MySQL Router
- MySQL Utilities
- MySQL Connector / ODBC
- MySQL Connector / Python
- MySQL Shell (preview)

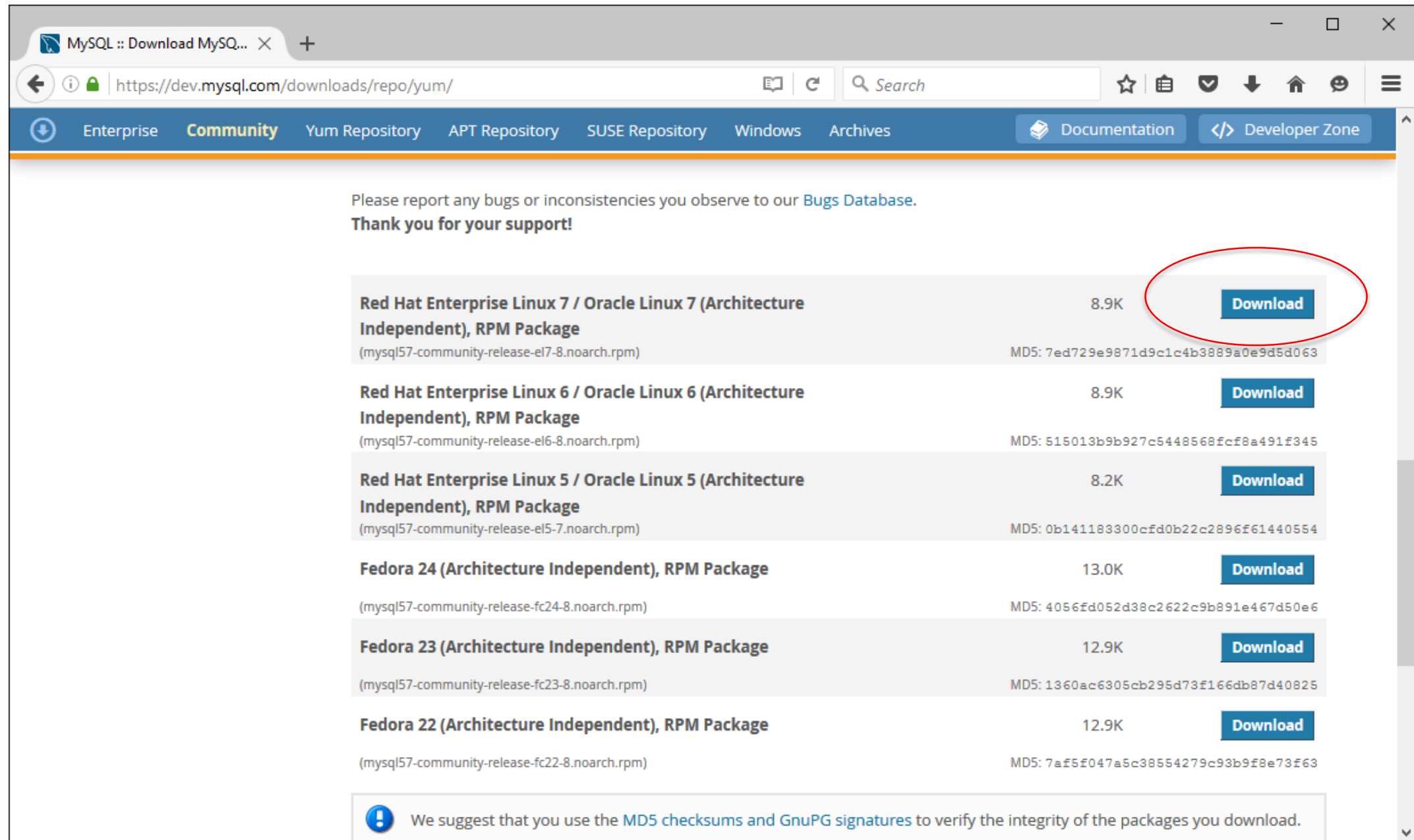
Online Documentation:

- [A Quick Guide to Using the MySQL Yum Repository](#)

MySQL open source software is provided under the [GPL License](#).

OEMs, ISVs and VARs can purchase commercial licenses.

MySQL



MySQL :: Download MySQL... X

https://dev.mysql.com/downloads/repo/yum/

Enterprise **Community** Yum Repository APT Repository SUSE Repository Windows Archives Documentation Developer Zone

Please report any bugs or inconsistencies you observe to our [Bugs Database](#).
Thank you for your support!

Red Hat Enterprise Linux 7 / Oracle Linux 7 (Architecture Independent), RPM Package (mysql57-community-release-el7-8.noarch.rpm)	8.9K	Download
MD5: 7ed729e9871d9c1c4b3889a0e9d5d063		
Red Hat Enterprise Linux 6 / Oracle Linux 6 (Architecture Independent), RPM Package (mysql57-community-release-el6-8.noarch.rpm)	8.9K	Download
MD5: 515013b9b927c5448568fcf8a491f345		
Red Hat Enterprise Linux 5 / Oracle Linux 5 (Architecture Independent), RPM Package (mysql57-community-release-el5-7.noarch.rpm)	8.2K	Download
MD5: 0b141183300cfd0b22c2896f61440554		
Fedora 24 (Architecture Independent), RPM Package (mysql57-community-release-fc24-8.noarch.rpm)	13.0K	Download
MD5: 4056fd052d38c2622c9b891e467d50e6		
Fedora 23 (Architecture Independent), RPM Package (mysql57-community-release-fc23-8.noarch.rpm)	12.9K	Download
MD5: 1360ac6305cb295d73f166db87d40825		
Fedora 22 (Architecture Independent), RPM Package (mysql57-community-release-fc22-8.noarch.rpm)	12.9K	Download
MD5: 7af5f047a5c38554279c93b9f8e73f63		

 We suggest that you use the [MD5 checksums](#) and [GnuPG signatures](#) to verify the integrity of the packages you download.

MySQL

MySQL :: Begin Your Dow... x +

https://dev.mysql.com/downloads/file/?id=462554

MySQL The world's most popular open source database

MySQL.com Downloads Documentation Developer Zone

Enterprise Community Yum Repository APT Repository SUSE Repository Windows Archives

Begin Your Download - mysql57-community-release-el7-8.noarch.rpm

Login Now or Sign Up for a free account.

An Oracle Web Account provides you with the following advantages:

- Fast access to MySQL software downloads
- Download technical White Papers and Presentations
- Post messages in the MySQL Discussion Forums
- Report and track bugs in the MySQL bug system
- Comment in the MySQL Documentation

Login »
using my Oracle Web account

Sign Up »
for an Oracle Web account

MySQL.com is using Oracle SSO for authentication. If you already have an Oracle Web account, click the Login link. Otherwise, you can signup for a free account by clicking the Sign Up link and following the instructions.

No thanks, just start my download.

CONTACT SALES PRODUCTS DOWNLOADS DOCUMENTATION

MySQL

การติดตั้ง MySQL server

```
[root@server1 ~]# rpm -ivh https://dev.mysql.com/get/mysql57-community-release-el7-8.noarch.rpm
```

warning: /var/tmp/rpm-tmp.XPAw1n: Header V3 DSA/SHA1 Signature, key ID 5072e1f5: NOKEY

Preparing... ##### [100%]

Updating / installing...

1:mysql57-community-release-el7-8 ##### [100%]

MySQL

ติดตั้ง MySQL server

```
[root@server1 ~]# yum -y install mysql-server
```

กำหนดให้ MySQL ทำงานทุกครั้งเมื่อมีการ reboot เครื่อง

```
[root@server1 ~]# systemctl enable mysqld
```

สั่งให้ MySQL service ทำงาน

```
[root@server1 ~]# systemctl start mysqld
```

HTTPD (Apache)

ติดตั้ง Web server (httpd)

```
[root@server1 ~]# yum -y install httpd
```

กำหนดให้ HTTPD ทำงานทุกครั้งที่มีการ Reboot เครื่อง

```
[root@server1 ~]# systemctl enable httpd
```

ทำการเปิดใช้งาน HTTPD

```
[root@server1 ~]# systemctl start httpd
```

HTTPD (Apache)

ตรวจสอบสถานะของ HTTPD

```
[root@server1 ~]# systemctl status httpd
```

```
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2016-08-07 00:09:35 ICT; 1min 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 4434 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─4434 /usr/sbin/httpd -DFOREGROUND
              └─4435 /usr/sbin/httpd -DFOREGROUND
                └─4436 /usr/sbin/httpd -DFOREGROUND
                  └─4437 /usr/sbin/httpd -DFOREGROUND
                    └─4438 /usr/sbin/httpd -DFOREGROUND
                      └─4439 /usr/sbin/httpd -DFOREGROUND
```

```
Aug 07 00:09:29 server1 systemd[1]: Starting The Apache HTTP Server...
```

```
Aug 07 00:09:35 server1 httpd[4434]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::20c:29ff:fe01:41be. Set the...
```

```
Aug 07 00:09:35 server1 systemd[1]: Started The Apache HTTP Server.
```

```
Hint: Some lines were ellipsized, use -l to show in full.
```

HTTPD (Apache)

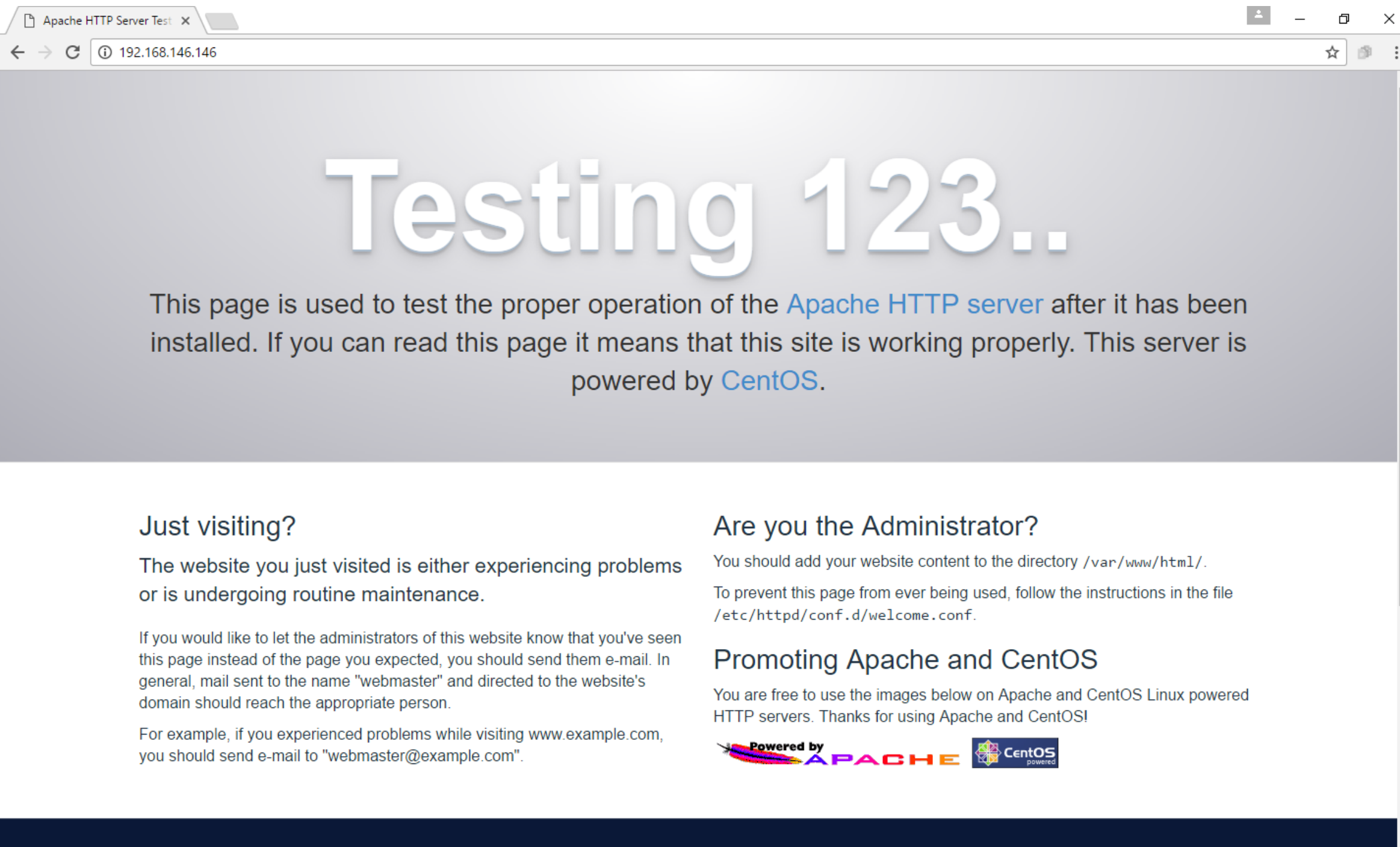
ตรวจสอบสถานะของ HTTPD

```
[root@server1 ~]# netstat -antp
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6      0      0 :::80                  :::*                    LISTEN      4434/httpd
```

HTTPD (Apache)

ทดสอบใช้งานผ่าน Web browser



HTTPD (Apache) + PHP

ทำการติดตั้ง PHP

```
[root@server1 ~]# yum -y install php
```

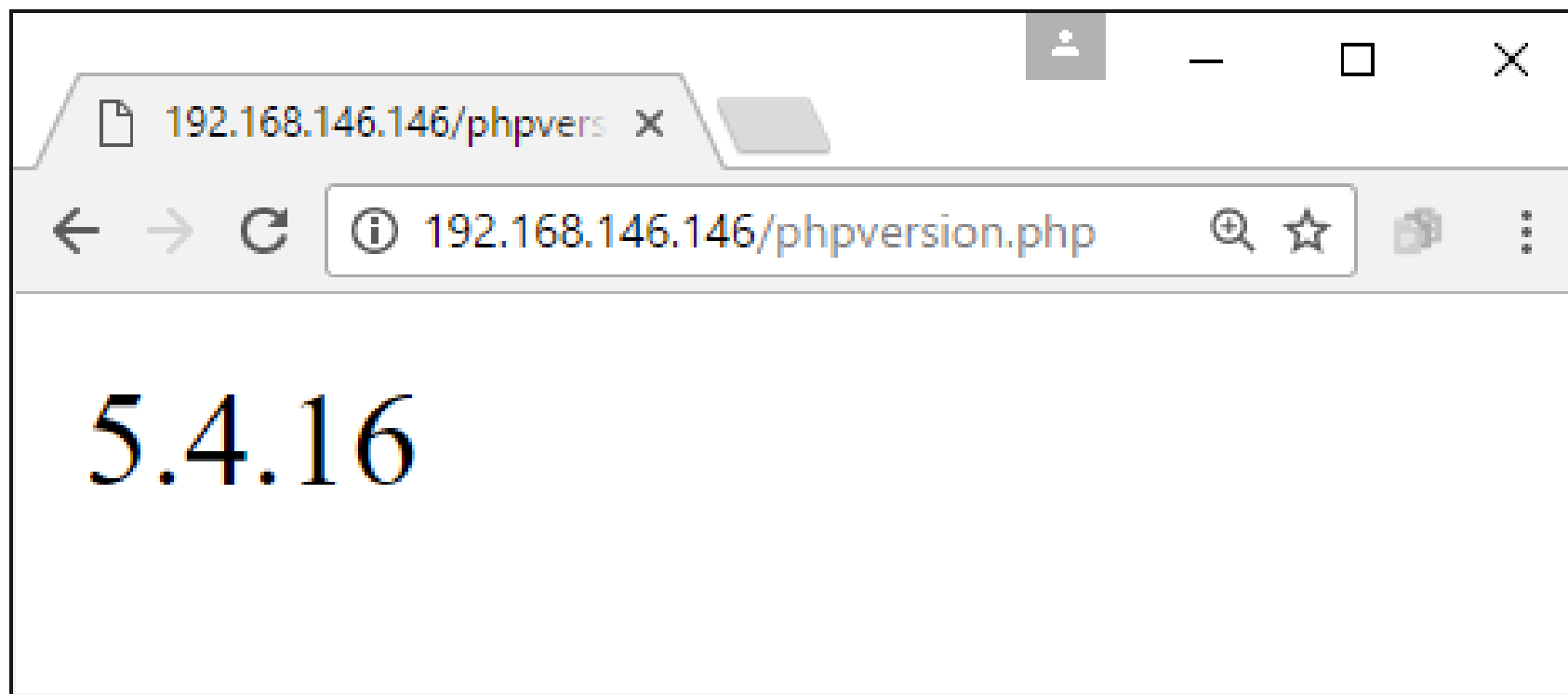
จากนั้นทำการ restart HTTPD

```
[root@server1 ~]# systemctl restart httpd
```

HTTPD (Apache)

ทดสอบ PHP

```
[root@server1 ~]# echo "<?php echo PHP_VERSION; ?>" > /var/www/html/phpversion.php
```



HTTPD (Apache) + PHP + MariaDB

การทำให้ HTTPD Connect Database ด้วย PHP

```
[root@server1 ~]# yum -y install php-mysql
```

```
[root@server1 ~]# systemctl restart httpd
```

HTTPD (Apache) + PHP + MariaDB

ทดสอบโดยสร้างไฟล์ต่อไปนี้

ไฟล์ /var/www/html/dbuser.php

```
<?php
    $dbserver = "localhost";
    $dbuser = "wwwuser";
    $dbpassword = "AbCpassWoRD";
    $conn = mysql_connect($dbserver,$dbuser,$dbpassword);
?>
```

HTTPD (Apache) + PHP + MariaDB

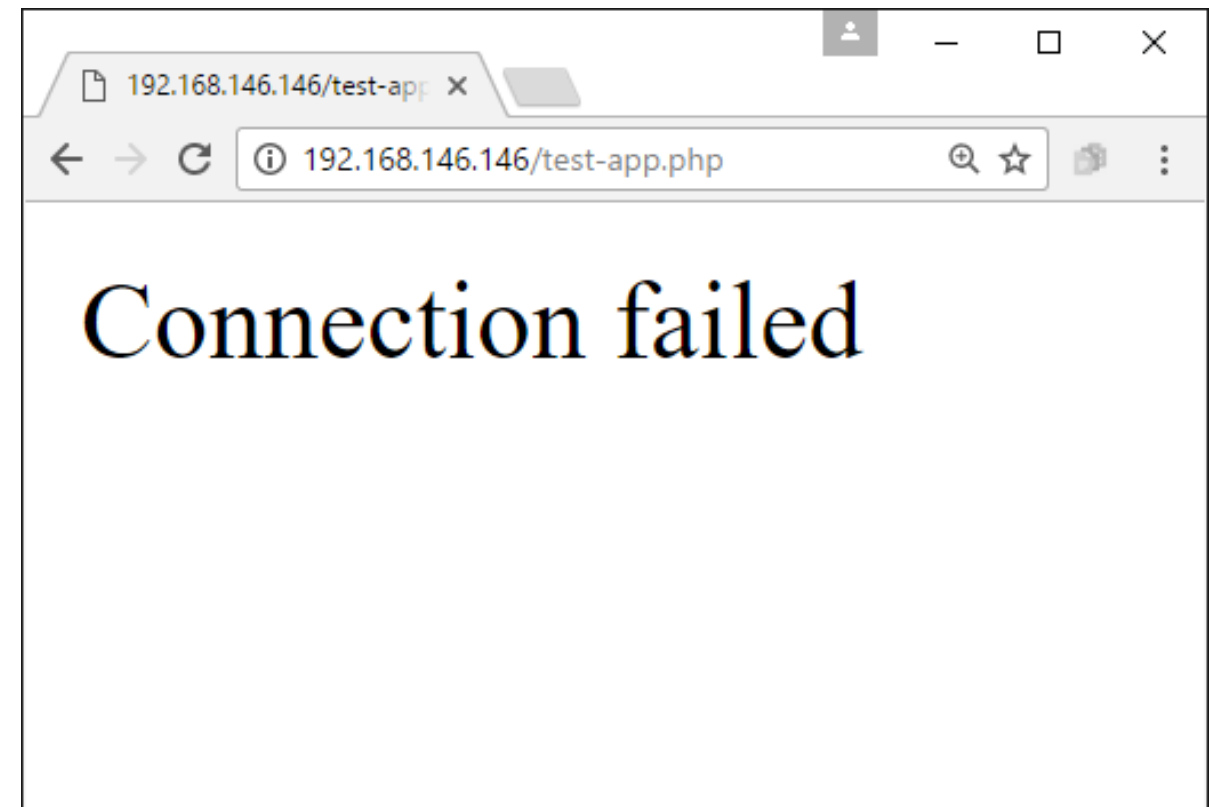
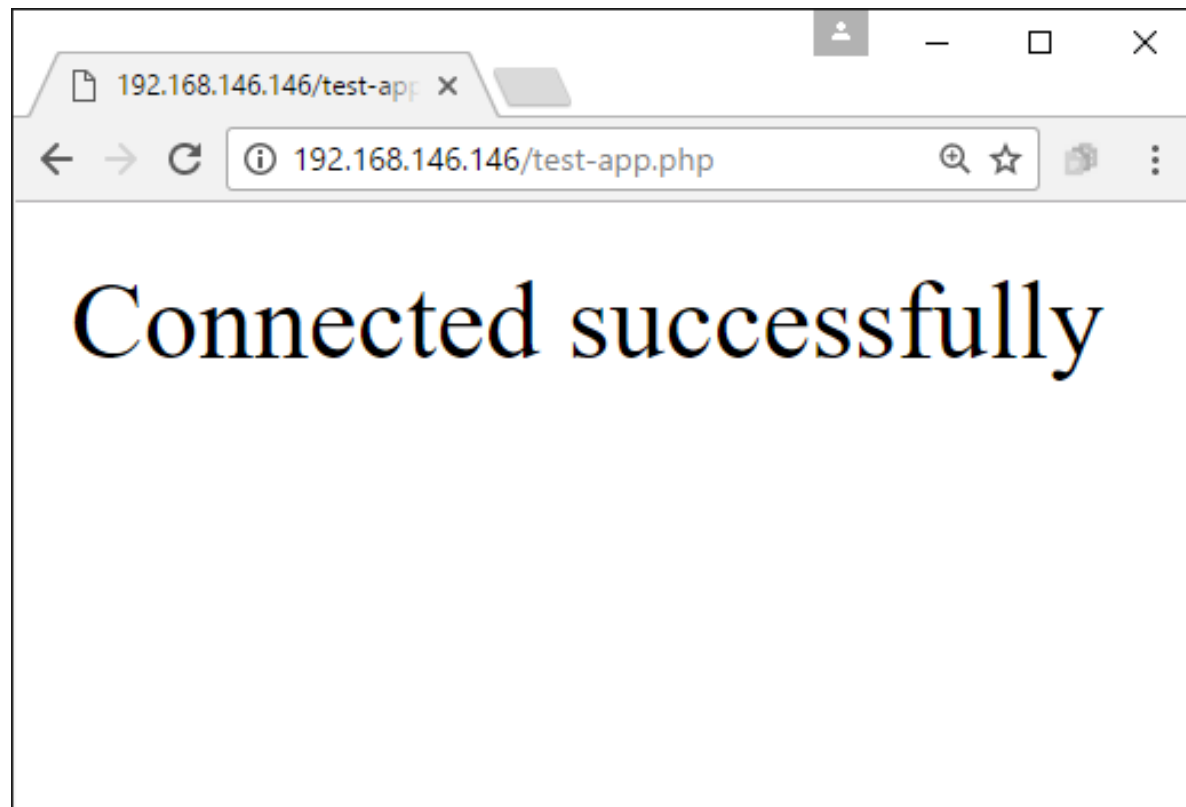
ทดสอบโดยสร้างไฟล์ต่อไปนี้

ไฟล์ /var/www/html/test-app.php

```
<?php  
  
include 'dbuser.php';  
  
if($conn)  
    { echo "Connected successfully"; }  
  
else  
    { echo "Connection failed"; }  
  
mysql_close($conn);  
  
?>
```

HTTPD (Apache) + PHP + MariaDB

ทดสอบการใช้งานผ่าน Web browser



HTTPD : Basic Hardening

ปิดการแสดงหมายเลขรุ่นของ Apache และระบบปฏิบัติการ ดังตัวอย่าง

```
[root@server1 html]# telnet 192.168.146.146 80
Trying 192.168.146.146...
Connected to 192.168.146.146.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
HTTP/1.1 403 Forbidden
Date: Sun, 07 Aug 2016 05:48:51 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
ETag: "1321-5058a1e728280"
Accept-Ranges: bytes
Content-Length: 4897
Connection: close
Content-Type: text/html; charset=UTF-8

Connection closed by foreign host.
```

HTTPD : Basic Hardening

ปิดการแสดงผลหมายเลขรุ่นของ Apache และระบบปฏิบัติการ

ให้ทำการแก้ไขไฟล์ `/etc/httpd/conf/httpd.conf` แล้วเพิ่ม Configure ต่อไปนี้เข้าไป

```
ServerTokens Prod
```

จากนั้นให้ restart httpd

```
[root@server1 conf]# systemctl restart httpd
```

HTTPD : Basic Hardening

ผลการทดสอบ

```
[root@server1 conf]# telnet 192.168.146.146 80
Trying 192.168.146.146...
Connected to 192.168.146.146.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
HTTP/1.1 403 Forbidden
Date: Sun, 07 Aug 2016 05:56:15 GMT
Server: Apache
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
ETag: "1321-5058a1e728280"
Accept-Ranges: bytes
Content-Length: 4897
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
Connection closed by foreign host.
```

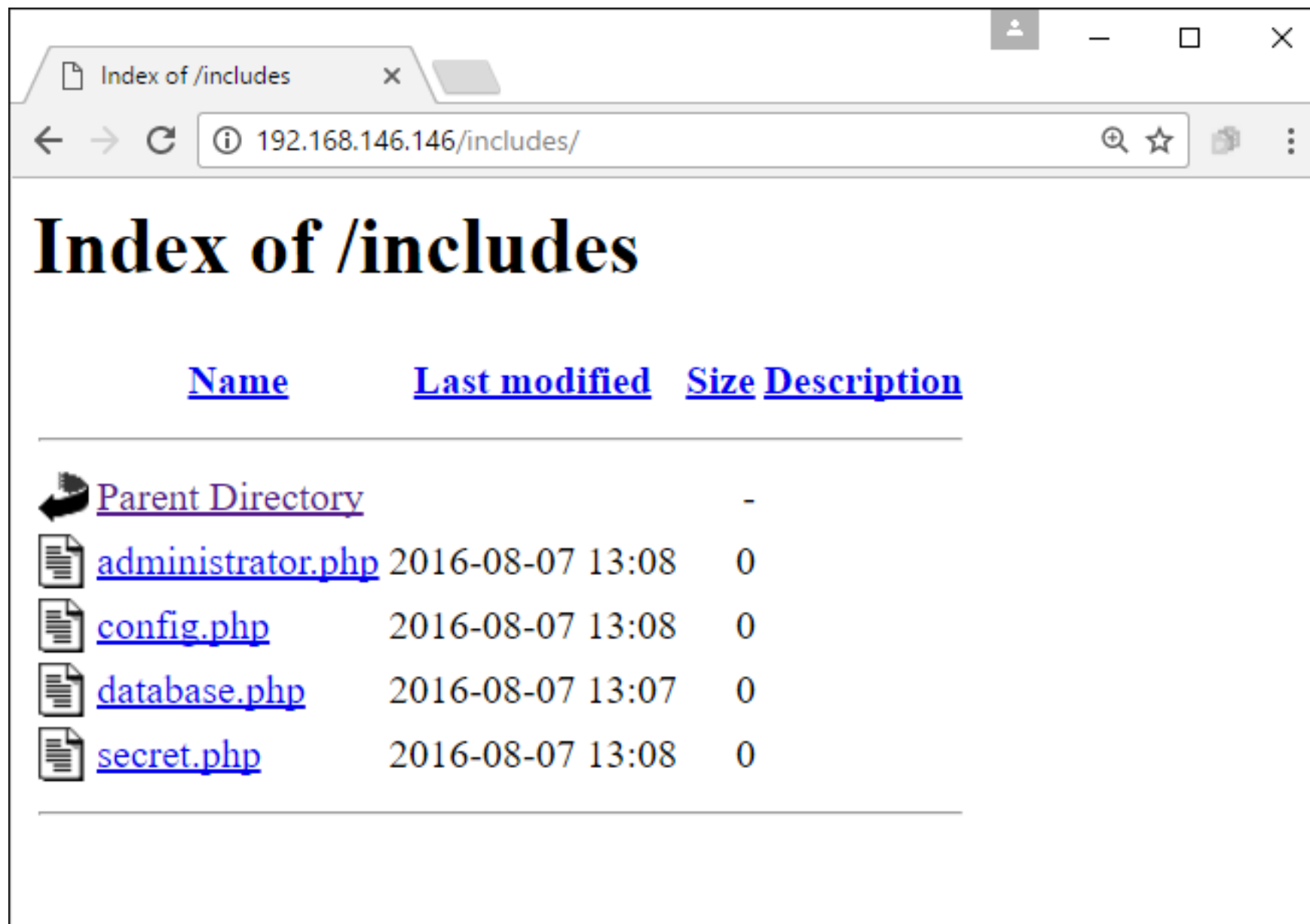
HTTPD : Basic Hardening

ServerTokens แบบต่างๆ

ServerTokens Full	--> Server: Apache/2.4.6 (CentOS) PHP/5.4.16
ServerTokens OS	--> Server: Apache/2.4.6 (CentOS)
ServerTokens Min	--> Server: Apache/2.4.6
ServerTokens Minor	--> Server: Apache/2.4
ServerTokens Major	--> Server: Apache/2
ServerTokens Prod	--> Server: Apache

HTTPD : Basic Hardening

ปิดการใช้งาน Directory Listing



HTTPD : Basic Hardening

ปิดการใช้งาน Directory Listing

ให้ทำการแก้ไขไฟล์ `/etc/httpd/conf/httpd.conf` โดยให้แก้ดังนี้

`<Directory "/var/www/html">`

`Options Indexes FollowSymLinks`

แก้เป็น

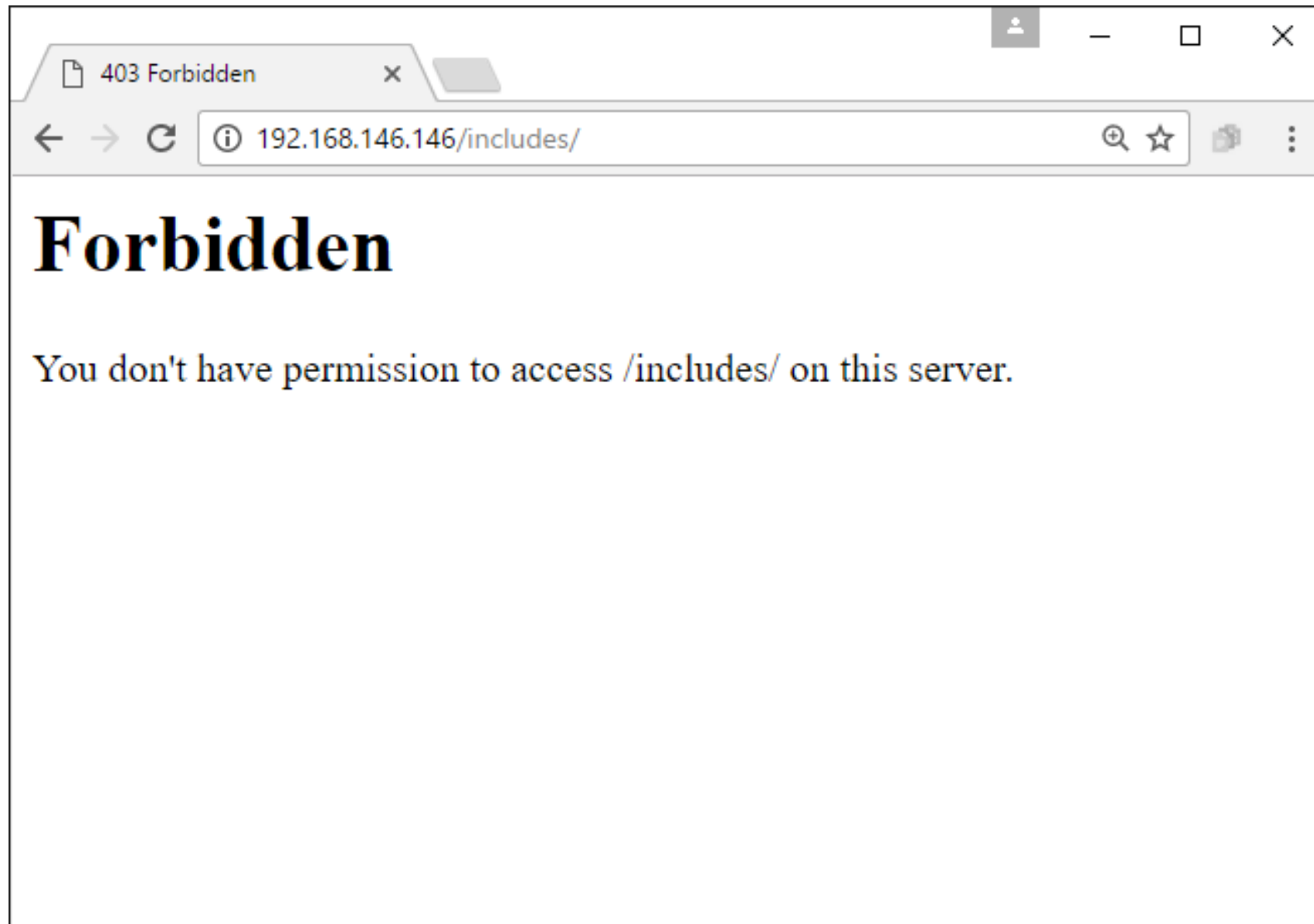
`<Directory "/var/www/html">`

`Options FollowSymLinks`

HTTPD : Basic Hardening

จากนั้นทำการ restart httpd

```
[root@server1 includes]# systemctl restart httpd
```



HTTPD : Basic Hardening

การจำกัดให้เฉพาะบาง IP เข้าถึง Directory สำคัญโดย .htaccess

- เปิดการใช้งาน .htaccess โดยแก้ไข `/etc/httpd/conf/httpd.conf`

ค่าเดิม

```
<Directory "/var/www/html">  
    AllowOverride None
```

แก้เป็น

```
<Directory "/var/www/html">  
    AllowOverride All
```

จากนั้นทำการ restart httpd

```
[root@server1 includes]# systemctl restart httpd
```

HTTPD : Basic Hardening

ทำการสร้างไฟล์ .htaccess ใน Directory ที่ต้องการ เช่น ถ้าต้องการให้เฉพาะ IP ชุด 192.168.145.0/24 สามารถเข้าถึง <http://IP.or.Domain/administrator/> ดังตัวอย่าง

สร้างไฟล์ /var/www/html/administrator/.htaccess

```
order deny,allow
```

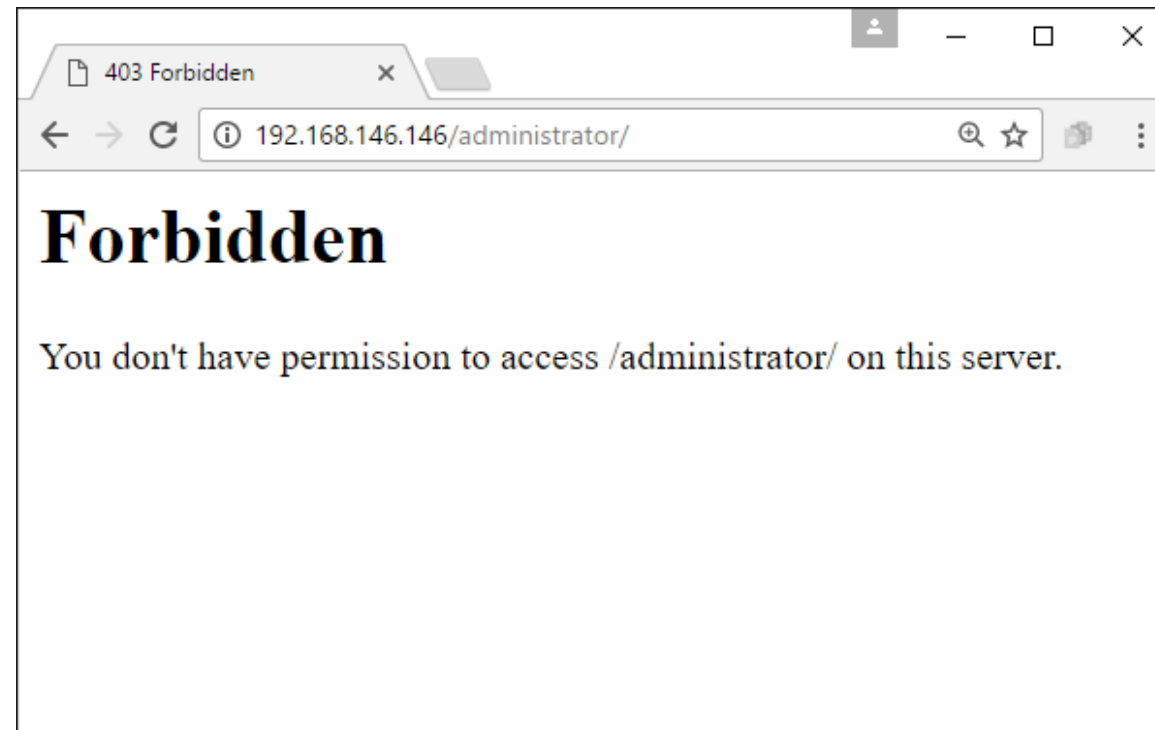
```
deny from all
```

```
allow from 192.168.145.0/24
```

HTTPD : Basic Hardening

ซึ่งถ้า User มาจากชุด IP ที่เรากำหนดไว้ จะเข้าใช้งานได้ปกติ

แต่ถ้า User มาจาก IP อื่นที่ไม่ได้อนุญาตไว้ ก็จะไม่สามารถเข้าใช้งานได้ ดังตัวอย่าง



และจะมี Log เกิดขึ้นที่ /var/log/httpd/error_log ดังนี้

```
[Sun Aug 07 13:35:28.186225 2016] [access_compat:error] [pid 2786] [client 192.168.146.1:59488] AH01797: client denied by server configuration: /var/www/html/administrator/
```

HTTPD : เปิดการใช้งาน HTTPS

เปิดการใช้งาน HTTPS

```
[root@server1 administrator]# yum -y install mod_ssl
```

```
[root@server1 administrator]# systemctl restart httpd
```

ตรวจสอบการทำงาน

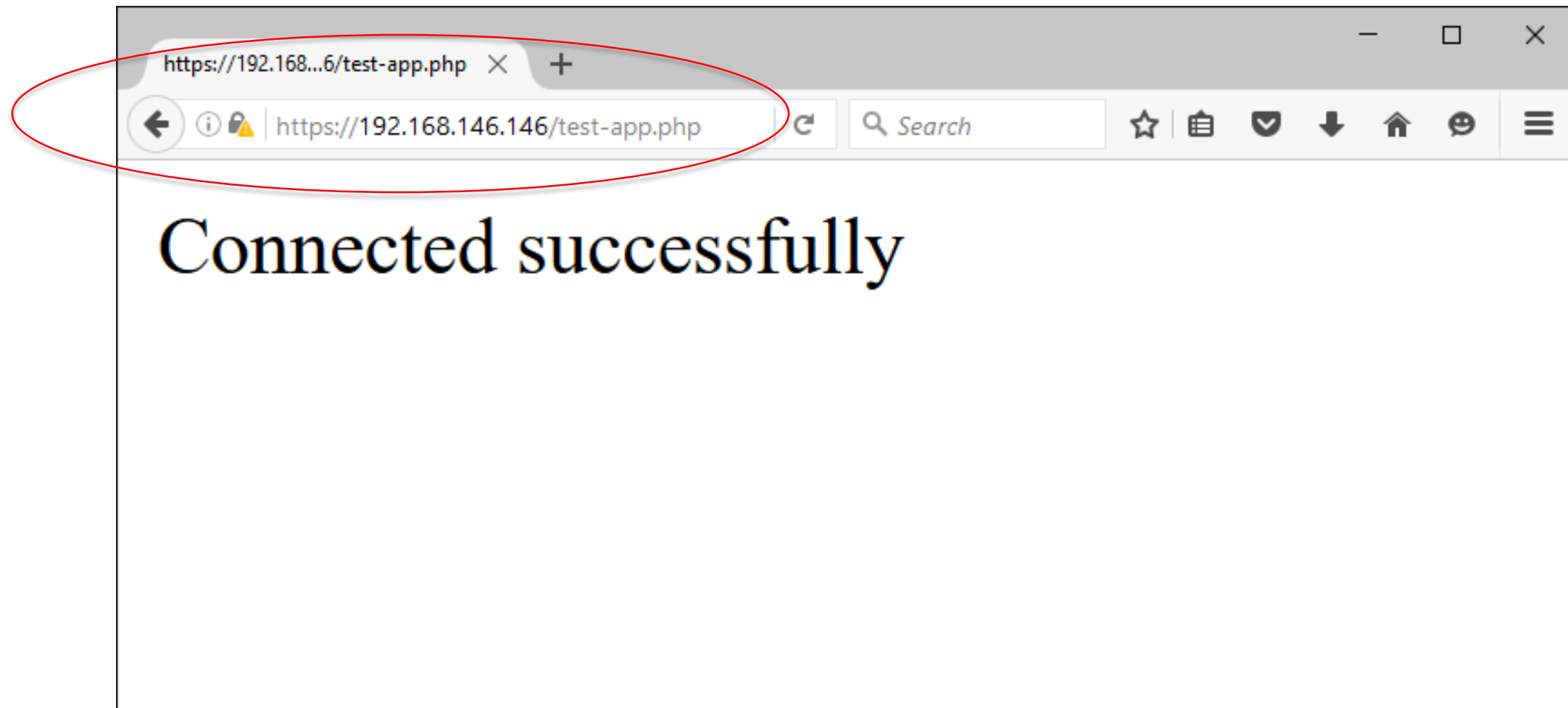
```
[root@server1 administrator]# netstat -ant
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp6	0	0	:::80	:::*	LISTEN
tcp6	0	0	:::443	:::*	LISTEN

HTTPD : Basic Hardening

ทดสอบใช้งานผ่าน Web browser



HTTPD : Redirect Users to HTTPS

สร้างไฟล์ .htaccess ในตำแหน่ง Directory ที่ต้องการให้ Redirect ไป HTTPS โดยในตัวอย่างนี้จะทำการ Redirect ทุกหน้าไปที่ HTTPS จึงจะทำการสร้างไฟล์ที่ Root ของเว็บ ที่ /var/www/html/.htaccess

```
RewriteEngine On
```

```
RewriteCond %{HTTPS} !on
```

```
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

จากนั้นทำการทดสอบการใช้งาน

FTP server

ติดตั้ง FTP service โดย vsftpd

```
[root@server1 html]# yum -y install vsftpd
```

กำหนดให้ VSFTPD ทำงานทุกครั้งที่ Reboot

```
[root@server1 html]# systemctl enable vsftpd
```

เปิดการใช้งาน VSFTPD

```
[root@server1 html]# systemctl start vsftpd
```

FTP server

ตรวจสอบการทำงานของ VSFTPD

```
[root@server1 html]# systemctl status vsftpd
```

● vsftpd.service - Vsftpd ftp daemon

Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)

Active: active (running) since Sun 2016-08-07 14:19:57 ICT; 1min 8s ago

Process: 3208 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)

Main PID: 3209 (vsftpd)

CGroup: /system.slice/vsftpd.service

└─3209 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Aug 07 14:19:57 server1 systemd[1]: Starting Vsftpd ftp daemon...

Aug 07 14:19:57 server1 systemd[1]: Started Vsftpd ftp daemon.

```
[root@server1 html]# netstat -antp
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp6	0	0	:::21	:::*	LISTEN	3209/vsftpd

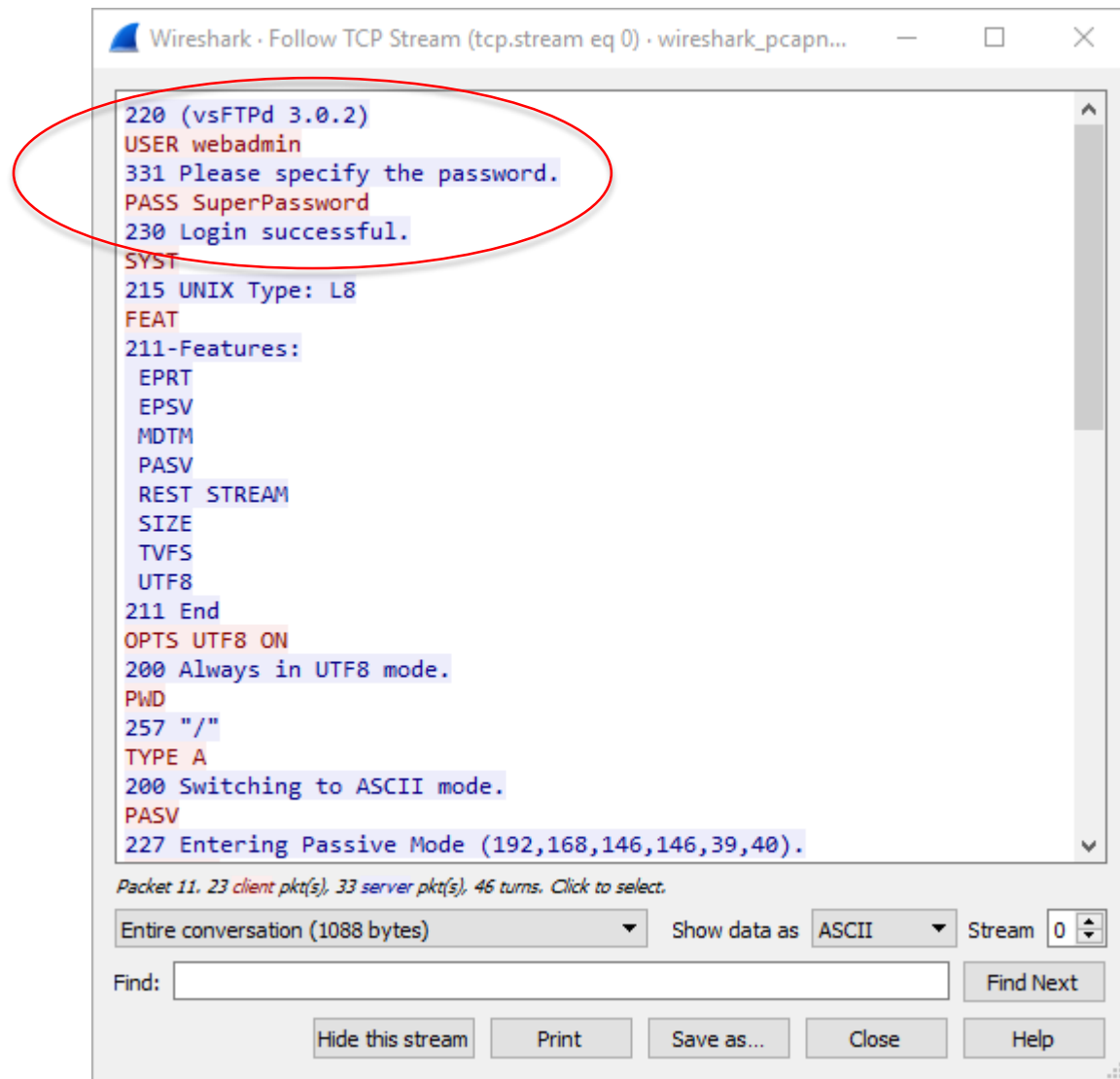
FTP server: Basic Hardening

แก้ไขไฟล์ `/etc/vsftpd/vsftpd.conf` ดังตัวอย่าง

```
anonymous_enable=NO  
chroot_local_user=YES  
allow_writeable_chroot=YES  
pasv_enable=YES  
port_enable=YES  
pasv_max_port=10029  
pasv_min_port=10020
```

FTP server with SSL

ตัวอย่าง FTP ที่ไม่มี SSL



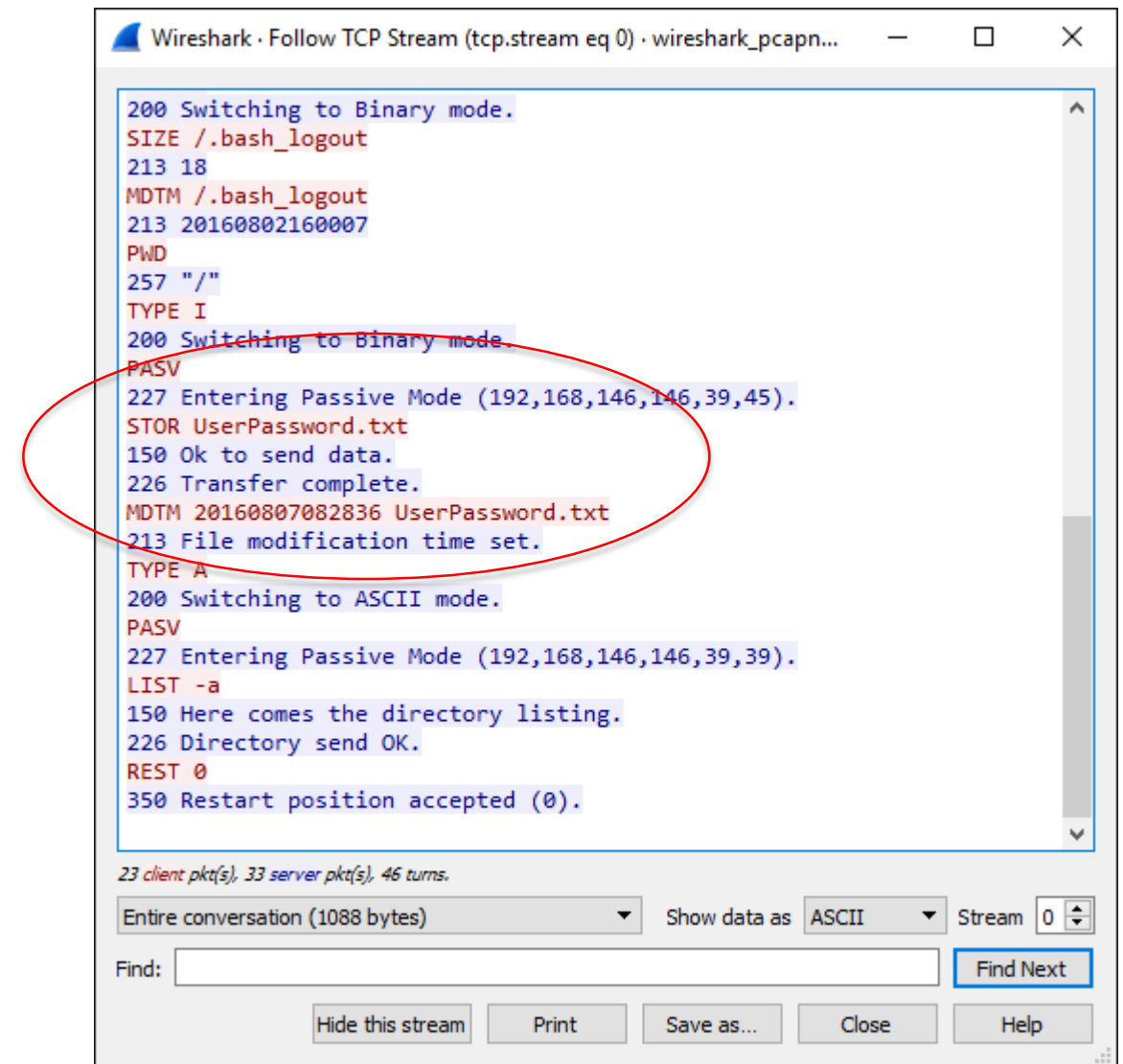
```
220 (vsFTPD 3.0.2)
USER webadmin
331 Please specify the password.
PASS SuperPassword
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
  EPRT
  EPSV
  MDTM
  PASV
  REST STREAM
  SIZE
  TVFS
  UTF8
211 End
OPTS UTF8 ON
200 Always in UTF8 mode.
PWD
257 "/"
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (192,168,146,146,39,40).
```

Packet 11, 23 client pkt(s), 33 server pkt(s), 46 turns. Click to select.

Entire conversation (1088 bytes) Show data as ASCII Stream 0

Find: Find Next

Hide this stream Print Save as... Close Help



```
200 Switching to Binary mode.
SIZE /.bash_logout
213 18
MDTM /.bash_logout
213 20160802160007
PWD
257 "/"
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (192,168,146,146,39,45).
STOR UserPassword.txt
150 Ok to send data.
226 Transfer complete.
MDTM 20160807082836 UserPassword.txt
213 File modification time set.
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (192,168,146,146,39,39).
LIST -a
150 Here comes the directory listing.
226 Directory send OK.
REST 0
350 Restart position accepted (0).
```

23 client pkt(s), 33 server pkt(s), 46 turns.

Entire conversation (1088 bytes) Show data as ASCII Stream 0

Find: Find Next

Hide this stream Print Save as... Close Help

FTP server with SSL

เริ่มด้วยการสร้าง Server Key และ Server Certificate (ในกรณีที่ยังไม่มี)

```
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) []:Security

Common Name (eg, your name or your server's hostname) []:Server1

Email Address []:contact@ega.or.th



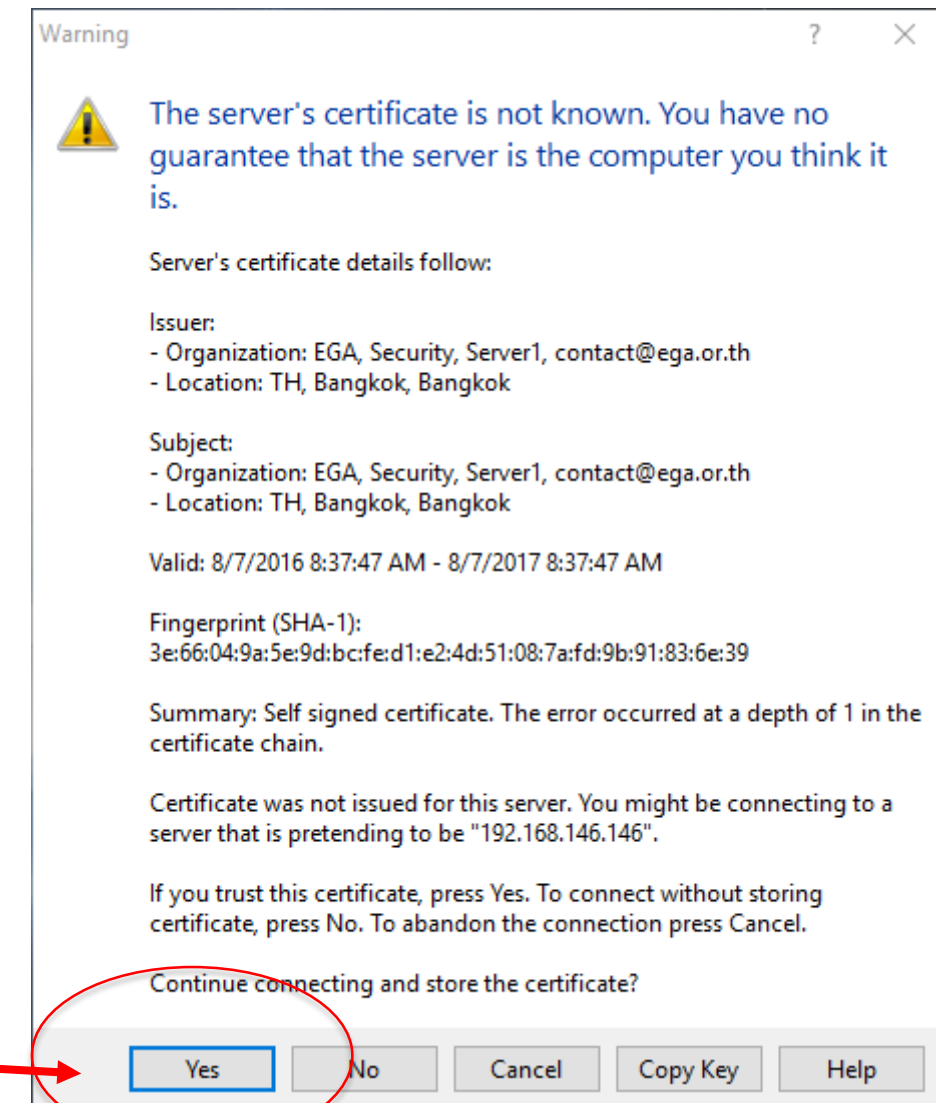
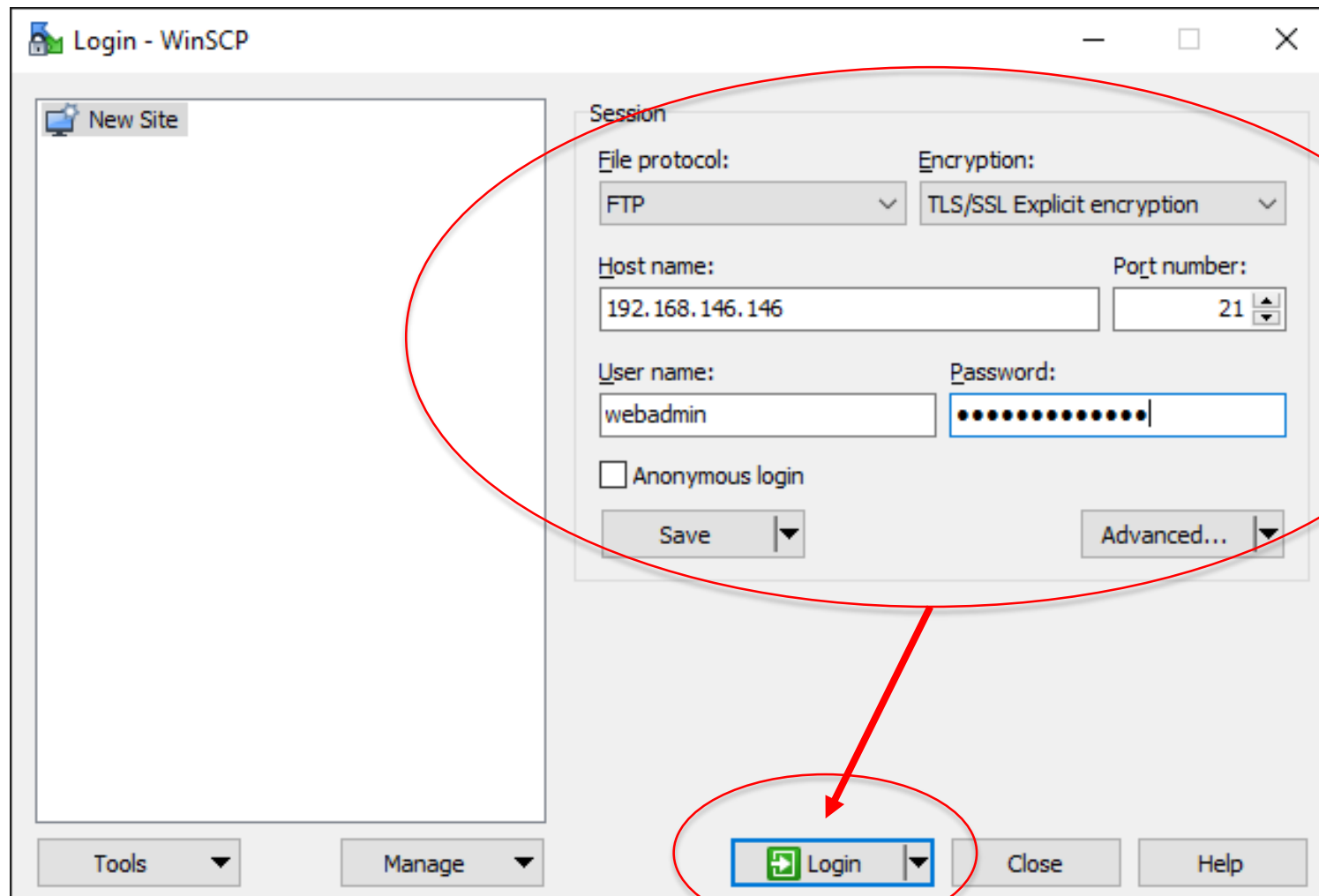
FTP server with SSL

แก้ไขไฟล์ /etc/vsftpd/vsftpd.conf โดยเพิ่ม Configuration ต่อไปนี้

```
ssl_enable=YES  
  
rsa_cert_file=/etc/vsftpd/vsftpd.pem  
  
rsa_private_key_file=/etc/vsftpd/vsftpd.pem  
  
allow_anon_ssl=NO  
  
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
```

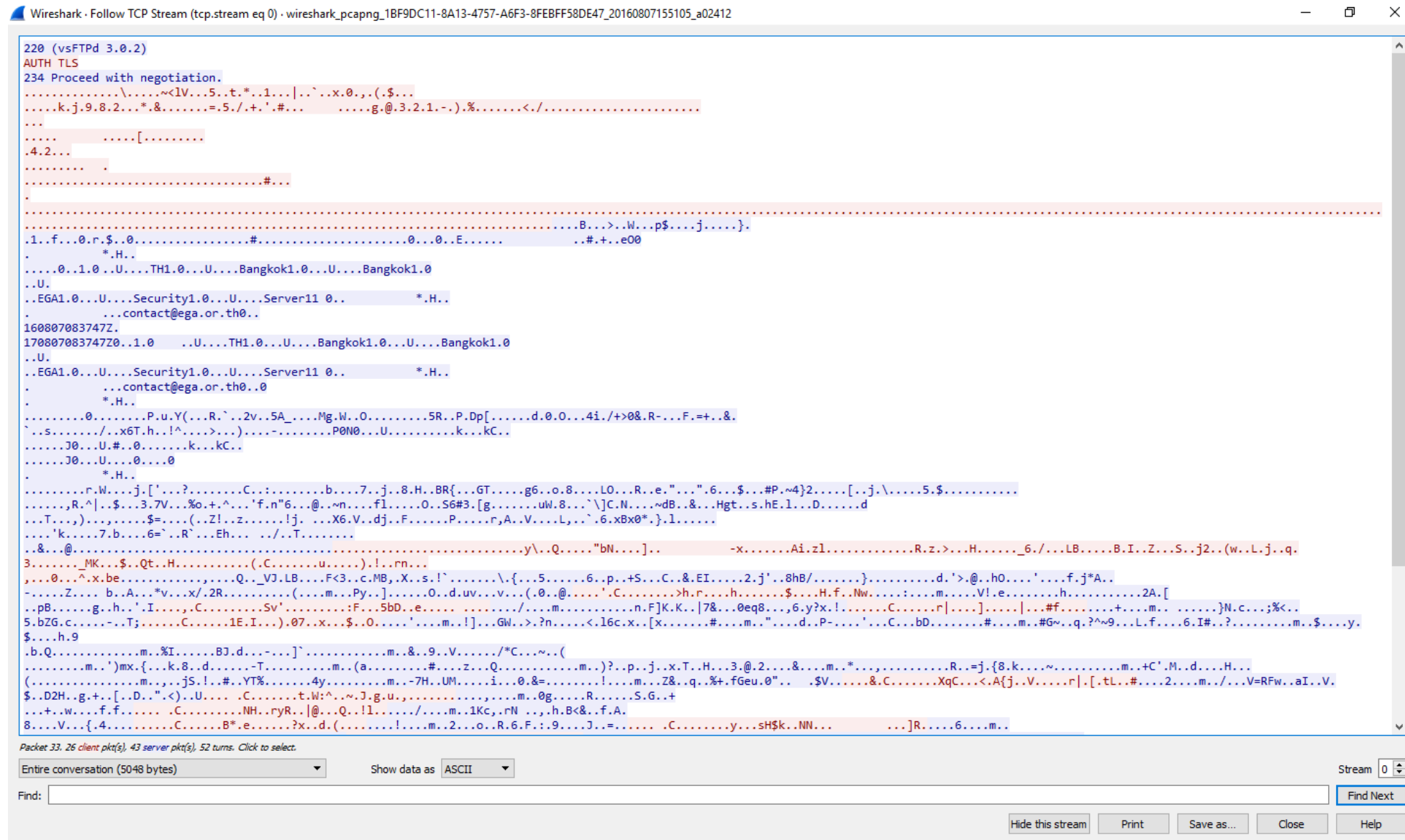
FTP server with SSL

ทดสอบใช้งาน FTP ผ่าน SSL



FTP server with SSL

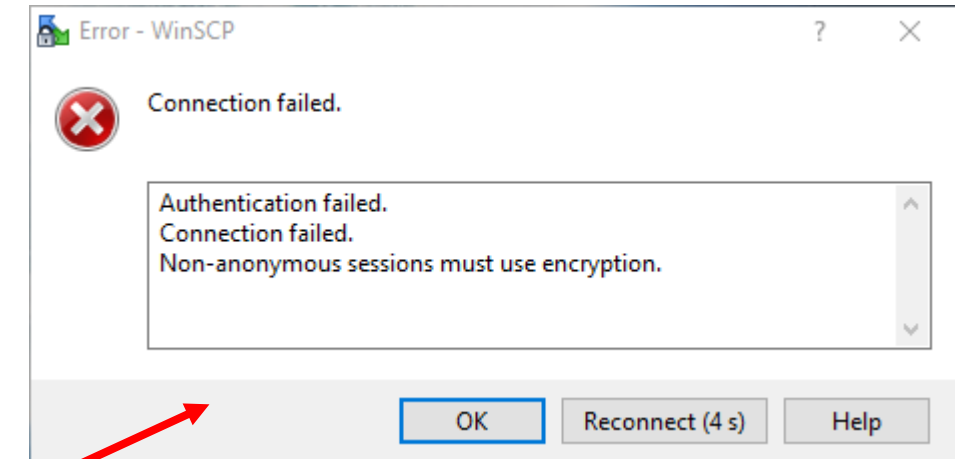
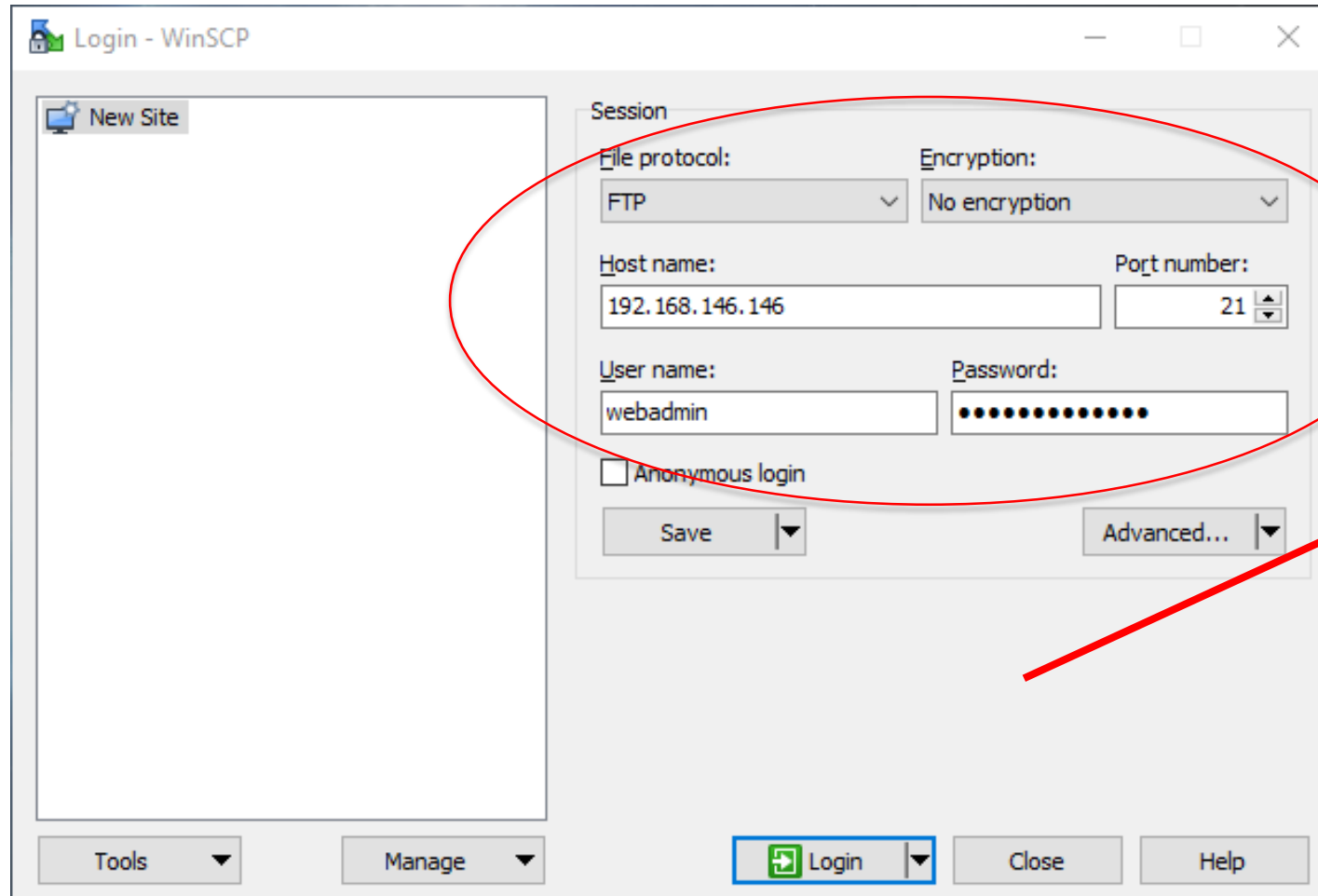
ทดสอบโดยการดัก traffic FTP



```
220 (vsFTPD 3.0.2)
AUTH TLS
234 Proceed with negotiation.
.....~<lv...S...t...1...|...x...0...(. $...
.....k.j.9.8.2...*.&.....=5./+.'.#... ..g.@.3.2.1.-.)%.<./.....
.....[.....
.4.2...
.....#...
.....
.....B...>..W...p$...j....}.
.1..f...0..r...$...0.....#.....0...0..E..... ..#..+...e00
.....*..H...
.....0...1.0...U...TH1.0...U...Bangkok1.0...U...Bangkok1.0
..U.
..EGA1.0...U...Security1.0...U...Server11 0.. ..*..H...
.....contact@ega.or.th0..
160807083747Z.
170807083747Z0..1.0 ...U...TH1.0...U...Bangkok1.0...U...Bangkok1.0
..U.
..EGA1.0...U...Security1.0...U...Server11 0.. ..*..H...
.....contact@ega.or.th0..
.....*..H...
.....0.....P.u.Y(...R...2v...5A...Mg..W...0.....5R...P.Dp[.....d.0.O...4i./+>0&R...F.=+...&.
`s.s.../..x6T.h...!^...>...).....P0N0...U.....k...kC..
.....J0...U..#...0.....k...kC..
.....J0...U...0.....0
.....*..H...
.....r..W...j..['...?.....C.....b...7..j...8.H...BR[...GT.....g6...o.8...LO...R...e...".6...$.#P...~4}2.....[...j...5.$.....
.....R..^]..$.3.7V...%o.+...^...'f.n"6...@...~n...f1...O..S6#3.[g.....uW.8...`]\C.N...~dB...&...Hgt...s.hE.l...D.....d
.....T...j...$=....(..Z!..z.....!j... ..X6.V..dj...F.....P.....r,A..V...L...`6.xBx0*...}.1.....
.....'k...7.b...6="R`...Eh... ../.T.....
..&...@.....y\..Q....."bN...]. ..-x.....Ai.z1.....R.z.>...H....._6./...LB.....B.I..Z...S..j2..(w..L..j..q.
3....._MK...$.Qt..H.....(C.....u.....).!..rn...
.....0...^..x.be.....Q..._VJ.LB...F<3..c.MB...X..s..!`.....\..{...5.....6...p...+S...C...&EI.....2.j'..8hB/.....}......d.'>..@..h0...'.f.j*A..
.....Z....b..A...*v...x/.2R.....(.....m...Py...]......O..d.uv...v...(.0...@.....'C.....>h.r...h.....$...H.f.Nw.....:.....m...V!e.....h.....2A.[
.....pB...g..h...'I.....C.....Sv'..:F...5bD..e...../.....n.F]K.K..|7&...0eq8...6.y?x!.....C.....r|.....]......|...#f.....+.....m...}N.c...;%<..
5.bZG.c.....T;.....C.....1E.I...).07..x...$.O.....'.....m..!]...GW...>?n.....<.l6c.x.[x.....#.....m...".d..P-.....'...C...bD.....#.....m...#G~..q.?^~9...L.f...6.I#...?.....m...$.y.
$.h.9
.b.Q.....m...%I.....BJ.d...-...]'.....m...&..9..V...../*C...~..(
.....m...')mx...{...k.8..d...-T.....m... (a.....#.....z...Q.....m...)?..p..j..x..T..H...3..@..2...&.....m...*.....R...=j..{8.k...~.....m...+C'.M..d...H...
.....m...jS...!..#..YT%.....4y.....m...-7H..UM.....i...0..&=.....!.....m...Z&..q...%+..fGeu..0"... ..$V.....&C.....XqC...<..A{j..V.....r|..[.tL..#.....2.....m.../...V=RFw...aI..V.
$.D2H..g...+..[.D...".<)...U... ..C.....t.W:^^..~J.g.u... ..m...0g.....R.....S.G..+
.....+..w...f..f.....C.....NH...ryR...|@...Q...!l.../.....m...1Kc...rN ...h.B<&..f.A.
8...V...{.4.....C.....B*.e.....?x..d.(.....!.....m...2...o..R.6.F...9...J...=.....C.....y...SH$k..NN... ..]R.....6.....m...
```

FTP server with SSL

ทดสอบ Login FTP โดยไม่ผ่าน SSL



Questions?