

# Basic G-Cloud Security Guide on Linux server (CentOS)



คมกริช คำสวัสดิ์

วิศวกรความมั่นคงปลอดภัยสารสนเทศอาวุโส  
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)



# Basic G-Cloud Security Guide

---

## Linux server (CentOS)

- Change root password
- Clock sync with NTP server
- Update patch
- Local Firewall (IPTABLES)
- SSH
- MySQL server
- Secure FTP server (vsftpd) / SFTP by OpenSSH
- Apache server

# เปลี่ยนรหัสผ่านของ Root

```
[root@Server ~]# passwd root
```

```
Changing password for user root.
```

```
New password: <NEW PASSWORD>
```

```
Retype new password: <NEW PASSWORD>
```

```
passwd: all authentication tokens updated successfully.
```

# BAD PASSWORD!

---

```
[root@Server ~]# passwd root
```

```
Changing password for user root.
```

```
New password: <Password>
```

```
BAD PASSWORD: it is based on a dictionary word
```

```
Retype new password: <Password>
```

```
passwd: all authentication tokens updated successfully.
```

# BAD PASSWORD!

---

BAD PASSWORD: it is based on a dictionary word (e.g. P@\$\$w0rd)

BAD PASSWORD: it does not contain enough DIFFERENT characters

BAD PASSWORD: is too simple

BAD PASSWORD: it is too short

BAD PASSWORD: it is too simplistic/systematic (e.g. 123456)

BAD PASSWORD: it is WAY too short

BAD PASSWORD: is a palindrome



# การตั้งนาฬิกาของเครื่องกับ NTP server

---

```
[root@Server ~]# ntpdate time.ega.or.th
```

```
14 Mar 17:40:09 ntpdate[1225]: step time server  
164.115.2.132 offset -25199.971278 sec
```

# การตั้งนาฬิกาของเครื่องกับ NTP server

---

```
[root@Server ~]# ntpdate time.ega.or.th
```

```
-bash: ntpdate: command not found
```

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

```
...
```

```
Installed:
```

```
ntpdate.x86_64 0:4.2.6p5-2.e16.centos
```

```
Complete!
```

# การตั้งค่าฬิกาของเครื่องกับ NTP server

```
### ติดตั้ง ntpd
```

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

```
...
```

```
...
```

```
Installed:
```

```
ntp.x86_64 0:4.2.6p5-2.el6.centos
```

```
Dependency Installed:
```

```
libedit.x86_64 0:2.11-4.20080712cvs.1.el6
```

```
Complete!
```



# การตั้งค่าพิกษาของเครื่องกับ NTP server

### แก้ไขไฟล์ Configuration ของ ntpd ที่ **/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
```

# การตั้งค่าฬิกาของเครื่องกับ NTP server

### ทำการ Start ntpd

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

Starting ntpd:

[ OK ]

### กำหนดให้ ntpd ทำงานทุกครั้งที restart เครื่อง

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

# การตั้งนาฬิกาของเครื่องกับ NTP server

### ตรวจสอบการทำงานของ 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	63	64	1	2.687	1.532	2.017
+113.53.247.3	.PPS.	1	u	60	64	3	4.963	1.854	1.137
*203.185.69.60	.PPS.	1	u	33	64	3	4.008	2.189	1.216
+203.185.69.59	.PPS.	1	u	32	64	7	4.012	1.410	1.344

# การตั้งค่าฬิกาของเครื่องกับ NTP server

---

### ทำการเพิ่มไฟล์ `/etc/cron.d/ntpdate`

```
55 * * * * root /usr/sbin/ntpdate -s -u time.ega.or.th time.navy.mi.th
```

# Update/Upgrade/Patch

```
[root@Server ~]# yum upgrade
```

```
Loaded plugins: fastestmirror
```

```
Setting up Upgrade Process
```

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

```
...
```

```
=====
```

```
Install          1 Package(s)
```

```
Upgrade         37 Package(s)
```

```
Total download size: 77 M
```

```
Is this ok [y/N]: y
```

```
Downloading Packages:
```



# Update/Upgrade/Patch

## Updated:

```
busybox.x86_64 1:1.15.1-21.el6_6
cyrus-sasl-lib.x86_64 0:2.1.23-15.el6_6.1
dhclient.x86_64 12:4.1.1-43.P1.el6.centos.1
dracut-kernel.noarch 0:004-356.el6_6.1
initscripts.x86_64 0:9.03.46-1.el6.centos.1
kpartx.x86_64 0:0.4.9-80.el6_6.3
libxml2.x86_64 0:2.7.6-17.el6_6.1
nss-softokn.x86_64 0:3.14.3-22.el6_6
nss-tools.x86_64 0:3.16.2.3-3.el6_6
openssh-server.x86_64 0:5.3p1-104.el6_6.1
rpm.x86_64 0:4.8.0-38.el6_6
rsyslog.x86_64 0:5.8.10-10.el6_6
tzdata.noarch 0:2015a-1.el6

curl.x86_64 0:7.19.7-40.el6_6.4
device-mapper.x86_64 0:1.02.90-2.el6_6.1
dhcp-common.x86_64 12:4.1.1-43.P1.el6.centos.1
glibc.x86_64 0:2.12-1.149.el6_6.5
iproute.x86_64 0:2.6.32-33.el6_6
libcurl.x86_64 0:7.19.7-40.el6_6.4
mdadm.x86_64 0:3.3-6.el6_6.1
nss-softokn-freebl.x86_64 0:3.14.3-22.el6_6
nss-util.x86_64 0:3.16.2.3-2.el6_6
openssl.x86_64 0:1.0.1e-30.el6_6.5
rpm-libs.x86_64 0:4.8.0-38.el6_6
selinux-policy.noarch 0:3.7.19-260.el6_6.2

cyrus-sasl.x86_64 0:2.1.23-15.el6_6.1
device-mapper-libs.x86_64 0:1.02.90-2.el6_6.1
dracut.noarch 0:004-356.el6_6.1
glibc-common.x86_64 0:2.12-1.149.el6_6.5
kernel-firmware.noarch 0:2.6.32-504.12.2.el6
libssh2.x86_64 0:1.4.2-1.el6_6.1
nss.x86_64 0:3.16.2.3-3.el6_6
nss-sysinit.x86_64 0:3.16.2.3-3.el6_6
openssh.x86_64 0:5.3p1-104.el6_6.1
policycoreutils.x86_64 0:2.0.83-19.47.el6_6.1
rpm-python.x86_64 0:4.8.0-38.el6_6
selinux-policy-targeted.noarch 0:3.7.19-260.el6_6.2
```

Complete!

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

```
Broadcast message from root@Server
(/dev/pts/0) at 17:58 ...
```

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

# Linux Firewall (iptables)

! การกำหนดให้ iptables ทำงานทุกครั้งที่มีการ reboot เครื่อง

**chkconfig iptables on**

! การ start/stop/restart iptables

**service iptables start|stop|restart**

# Linux Firewall (iptables)

! การกำหนด Policy ของ iptables เบื้องต้น

! แก้ไขไฟล์ `"/etc/sysconfig/iptables"`

```
*filter
:INPUT ACCEPT [90:6544]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [49:6392]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state ESTABLISH,RELATED -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -s 172.17.12.0/24 -p tcp --dport 22 -j ACCEPT
-A INPUT -j DROP
COMMIT
```



# Linux Firewall (iptables)

! การตรวจสอบ policy ของ iptables

## iptables -nvL

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
67	4828	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
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	--	*	*	172.17.12.0/24	0.0.0.0/0	state NEW tcp dpt:22
5	338	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

Chain OUTPUT (policy ACCEPT 37 packets, 5180 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------



# Secure Shell (SSH)

! SSH Login Banner

! สร้างไฟล์สำหรับใส่ข้อความ Banner เช่น /etc/ssh/banner

```
* * * * * W A R N I N G * * * * *  
Unauthorized access to this system is forbidden  
and will be prosecuted by law. By accessing this system,  
you agree that your actions may be monitored  
if unauthorized usage is suspected.  
* * * * *
```

! แก้ไขไฟล์ /etc/ssh/sshd\_config

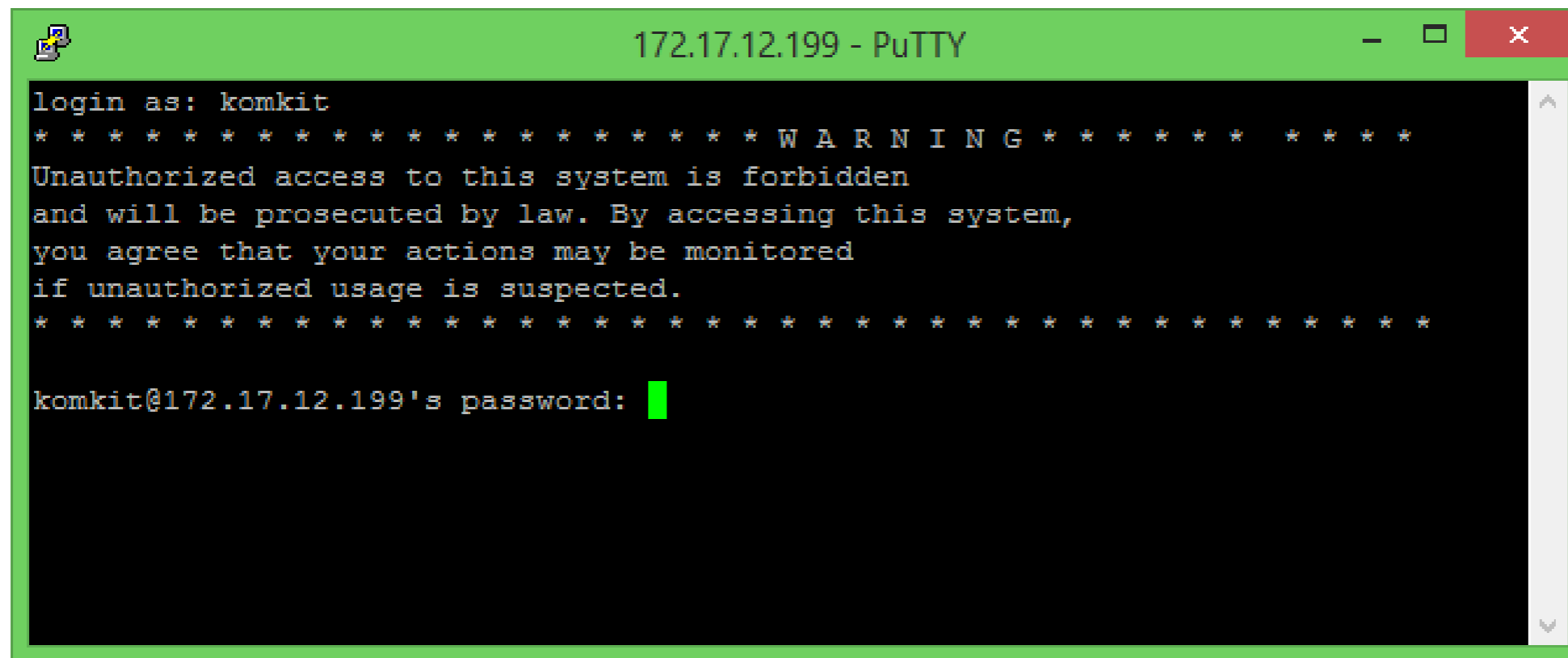
```
Banner /etc/ssh/banner
```

จากนั้นทำการ restart sshd service



# Secure Shell (SSH)

! SSH Login Banner



```
172.17.12.199 - PuTTY
login as: komkit
***** WARNING *****
Unauthorized access to this system is forbidden
and will be prosecuted by law. By accessing this system,
you agree that your actions may be monitored
if unauthorized usage is suspected.
*****
komkit@172.17.12.199's password: █
```

# 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)

# MySQL server

### แก้ไข LISTEN address หากไม่มีการติดต่อมาจากเครื่องอื่น (e.g. LAMP)

```
[root@Server ~]# netstat -ant
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	LISTEN

### แก้ไขไฟล์ /etc/my.cnf

```
[mysqld]
```

```
bind-address=127.0.0.1 <---- เพิ่มบรรทัดนี้
```



# MySQL server

### ทำการ restart mysqld

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

```
Stopping mysqld:           [ OK ]
```

```
Starting mysqld:           [ OK ]
```

### ตรวจสอบ MySQL LISTEN address

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN

# FTP server by vsftpd

! แก้ไข vsftpd banner

Default banner ของ vsftpd

```
X:\>ftp 172.17.12.199
Connected to 172.17.12.199.
220 (vsFTPd 2.2.2)
User (172.17.12.199:(none)):
```

# FTP server by vsftpd

! แก้ไขไฟล์ `/etc/vsftpd/vsftpd.conf`

`ftpd_banner=Authorized person only!`

จากนั้นทำการ `restart vsftpd service`.

```
X:\>ftp 172.17.12.199
Connected to 172.17.12.199.
220 Authorized person only!
User (172.17.12.199:(none)):
```

# 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
```



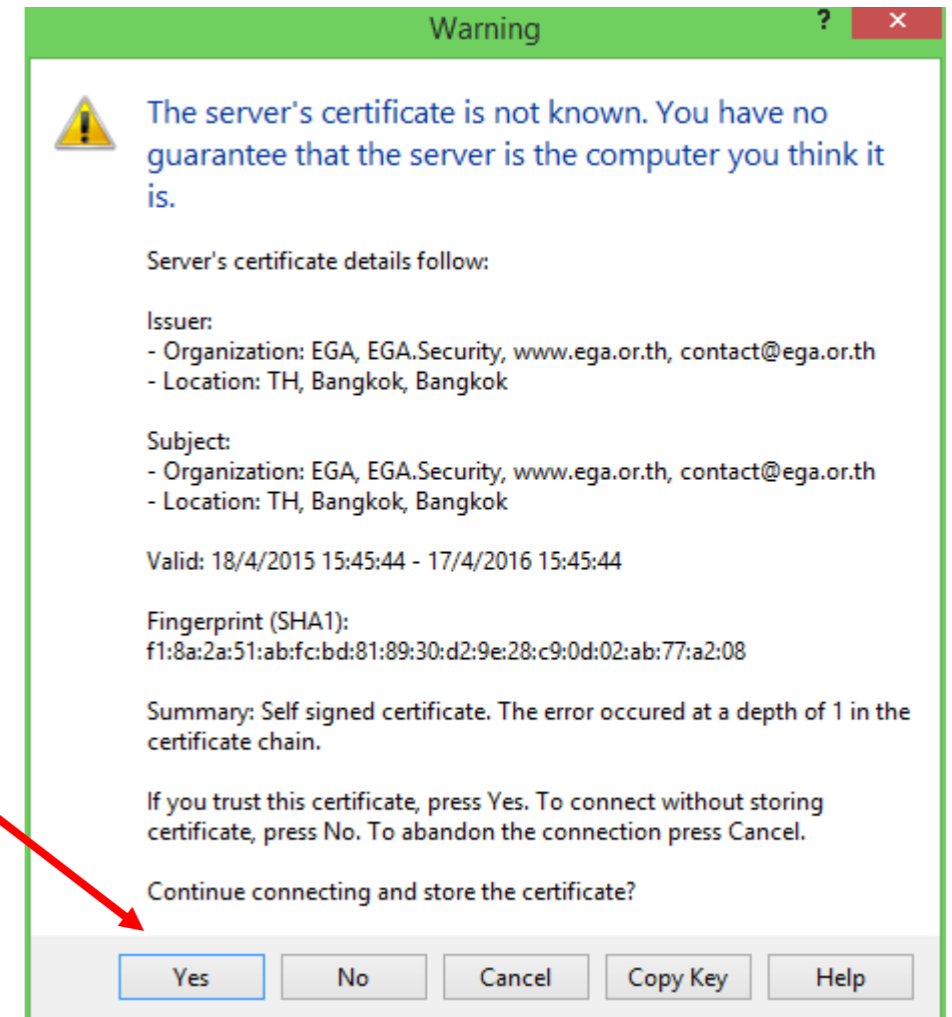
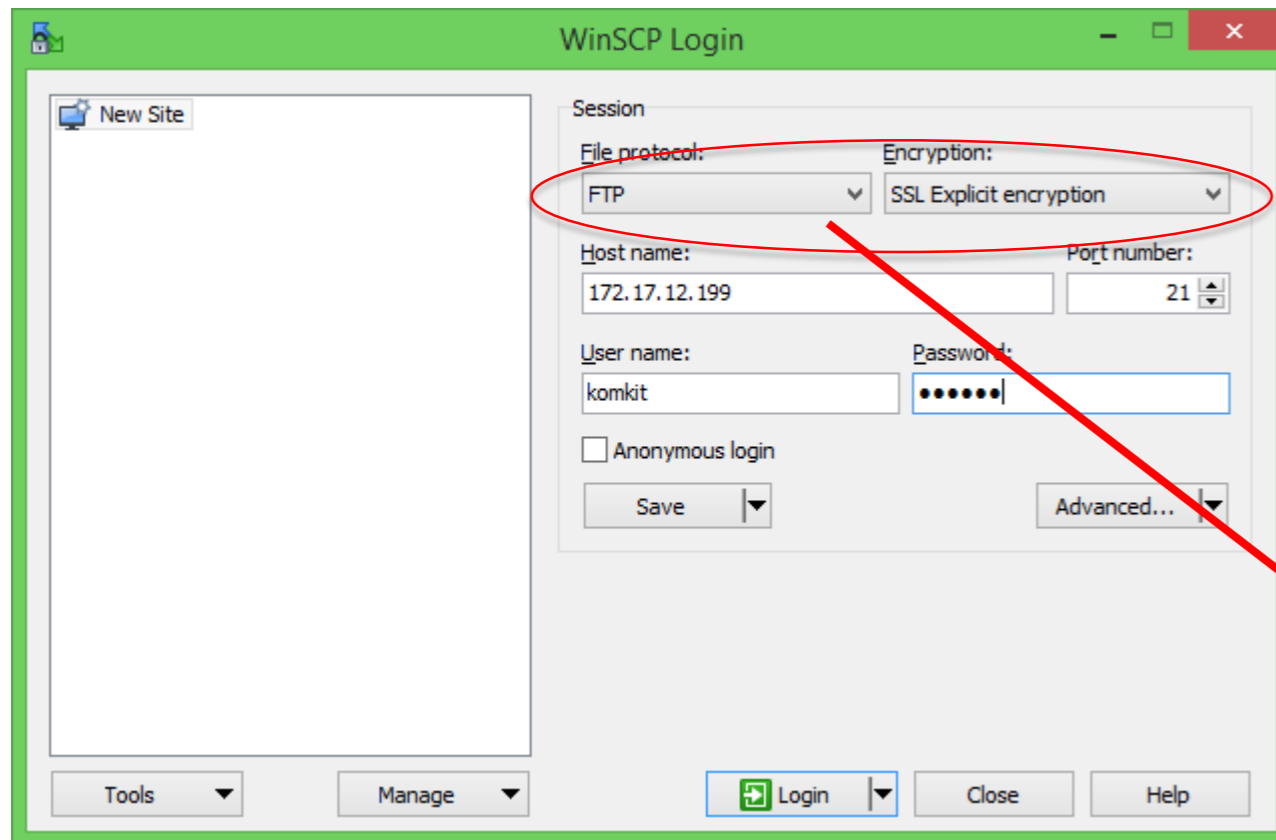
# vsftpd with SSL

! 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
```

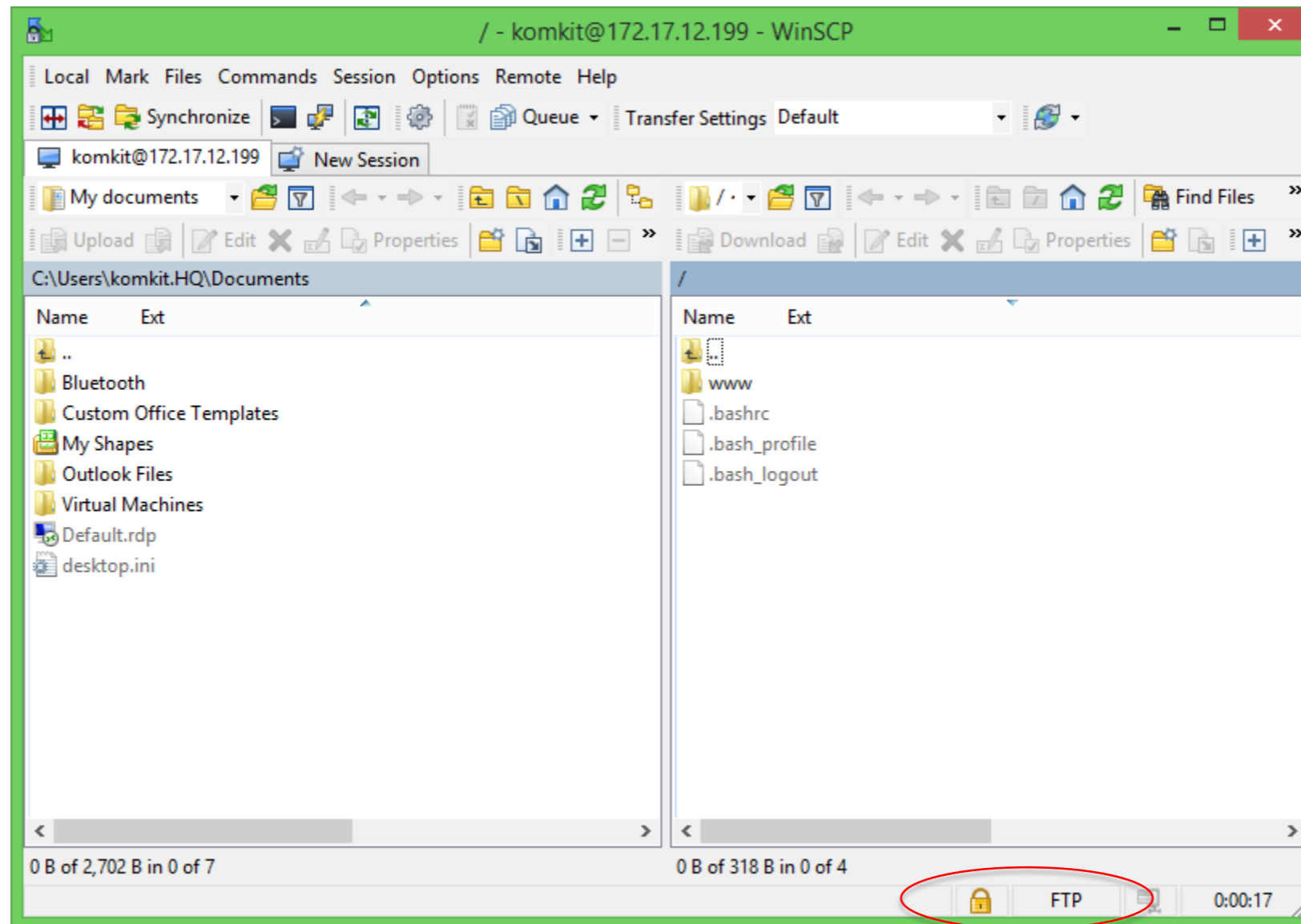
# vsftpd with SSL

! ทดสอบการใช้งานผ่าน SSL



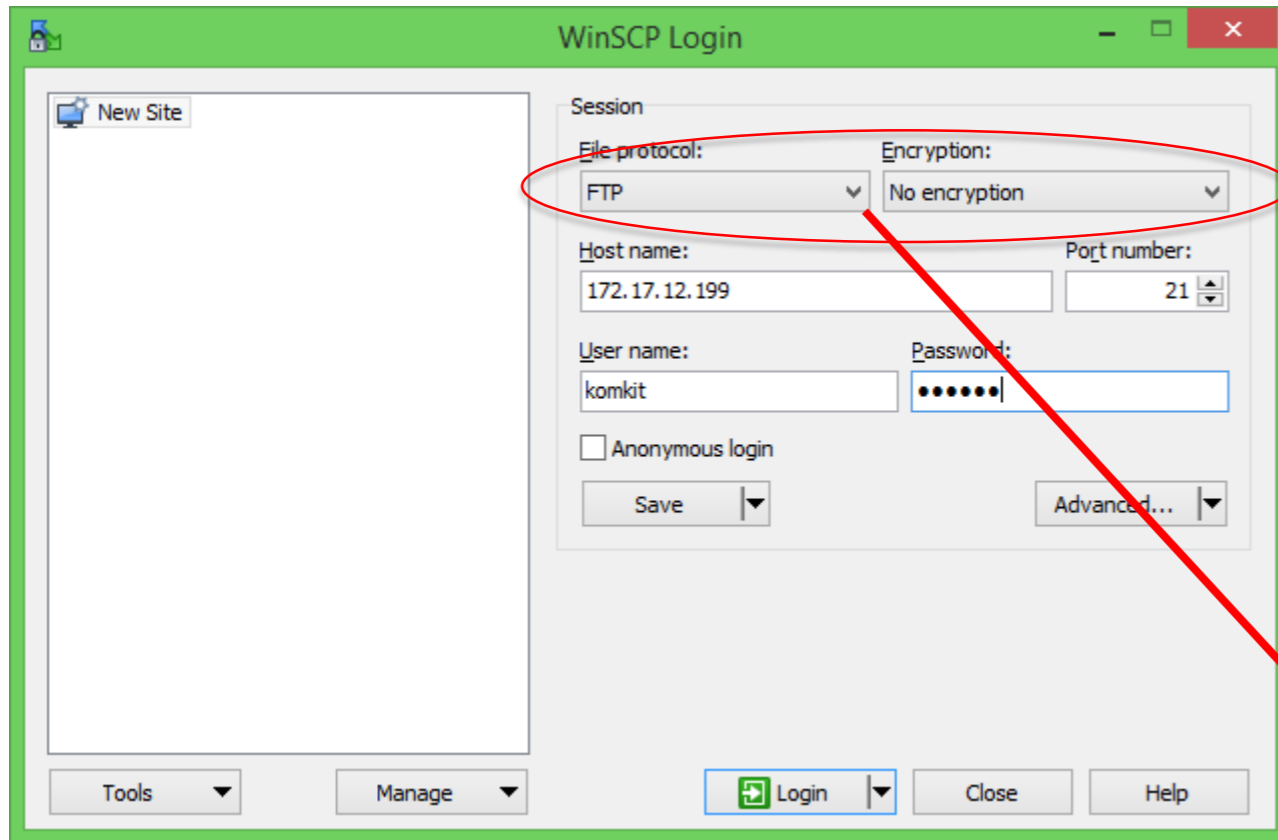
# vsftpd with SSL

! ทดสอบการใช้งานผ่าน SSL

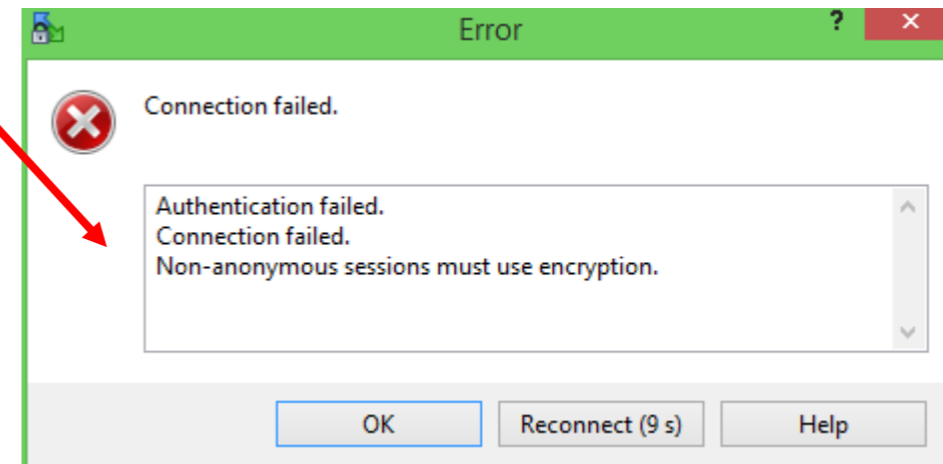


# vsftpd with SSL

! ทดสอบใช้งานแบบไม่ผ่าน SSL

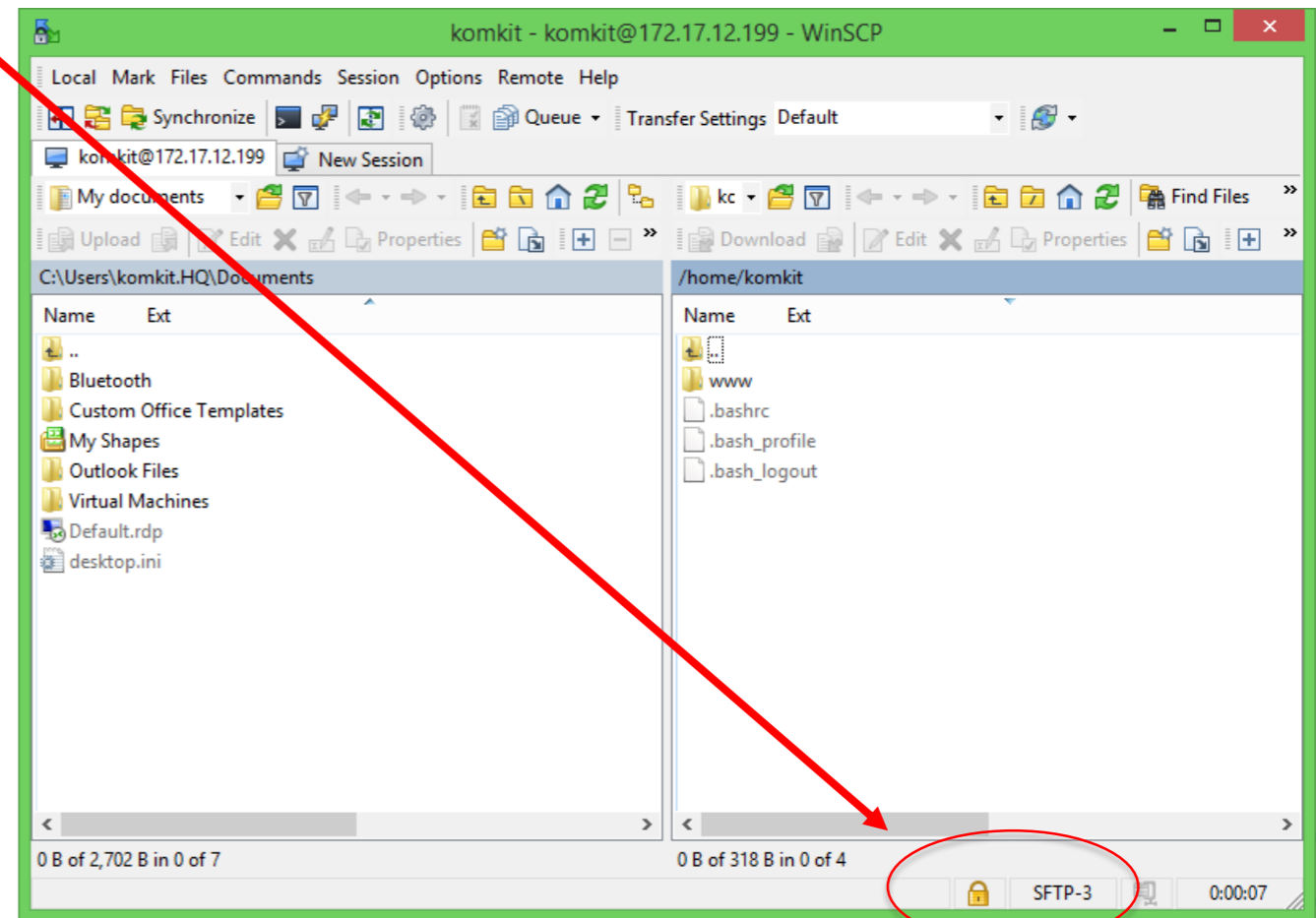
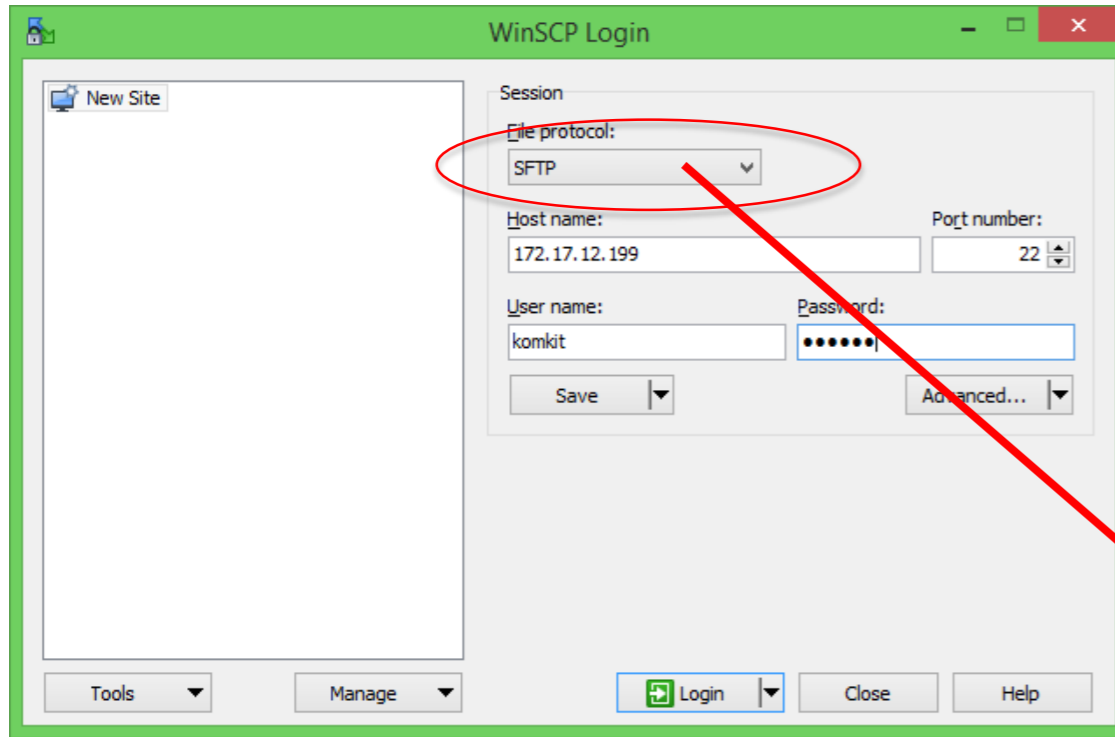


```
X:\>ftp 172.17.12.199
Connected to 172.17.12.199.
220 Authorized person only!
User (172.17.12.199:(none)): komkit
530 Non-anonymous sessions must use encryption.
Login failed.
ftp>
```





# SFTP by OpenSSH



# Apache: enable HTTPS

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

จากนั้นทำการ restart httpd

```
[root@www conf.d]# service httpd restart
```

ตรวจสอบว่า HTTPS ถูกเปิดแล้ว

```
[root@www conf.d]# netstat -antup
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	:::443	:::*	LISTEN	2412/httpd

# Apache: enable HTTPS

Apache HTTP Server Test Page ... x +

https://172.17.12.199

You are connected to **172.17.12.199**

You have added a security exception for this site.

The connection to this website is secure.

More Information...

## Apache 2 Test Page

powered by **CentOS**

The Apache HTTP server after it has been installed. If you can read this page it means that it is working properly.

**If you are a member of the general public:**

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.



If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to "webmaster@example.com".

**If you are the website administrator:**

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!

**Powered by**  **CentOS** 

**About CentOS:**

**The Community ENTERprise Operating System** (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux. The CentOS Project is the organization that builds CentOS. We mainly change packages to remove upstream vendor branding and artwork.

For information on CentOS please visit the [CentOS website](http://www.centos.org).

**Note:**

CentOS is an Operating System and it is used to power this website; however, the webserver is owned by the domain owner and not the CentOS Project. **If you have issues with the content of this site, contact the owner of the domain, not the CentOS Project.**

Unless this server is on the CentOS.org domain, the CentOS Project doesn't have anything to do with the content on this webserver or any e-mails that directed you to this site.

For example, if this website is `www.example.com`, you would find the owner of the `example.com` domain at the following WHOIS server:

<http://www.internic.net/whois.html>

# Apache: Redirect Users to HTTPS

! แก้ไข `/etc/httpd/conf/httpd.conf`

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

```
...
```

```
    AllowOverride All
```

! จากนั้นทำการ `restart httpd service`

# 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]
```

