

She쥼포s' 이야기

- [홈](#)
- [태그](#)
- [미디어로그](#)
- [위치로그](#)
- [방명록](#)

Apache + SSL on Windows 관련 URL

[Unix/Linux](#) 2007/11/15 15:55

Windows용 Apache에 SSL 설정하기

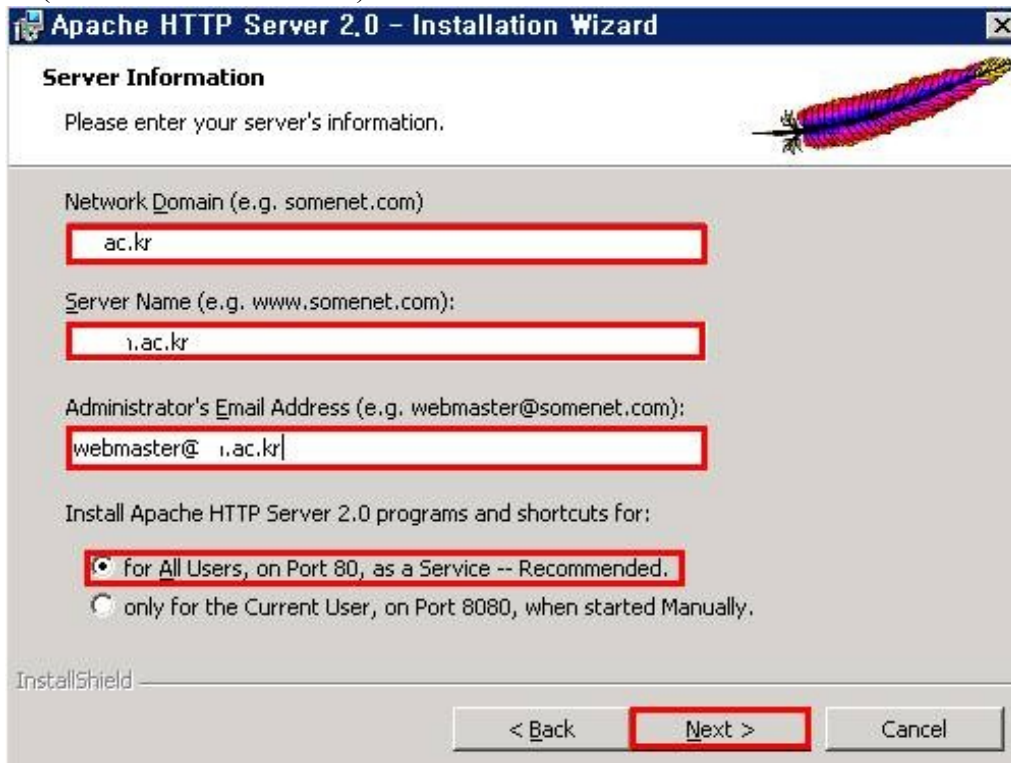
o 패키지 다운로드

- <http://www.apache.org> 또는
- <http://mirror.apache-kr.org> 에 접속하여 SSL을 지원하는 바이너리 파일 선택

※ 현재 최신 안정버전(2.0대)은 apache_2.0.61-win32-x86-openssl-0.9.7m.msi 임(x86용)

o 패키지 설치

- 설치과정 생략(일반 패키지 설치와 비슷)



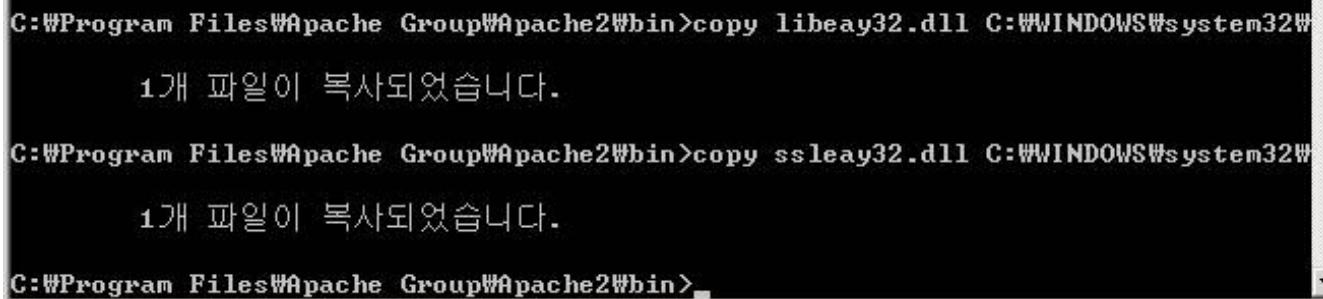
기본설정

※ 설치디렉토리는 기본적으로 "C:\Program Files\Apache Group\Apache2"이다.

- o bin 디렉토리로 이동("C:\Program Files\Apache Group\Apache2\bin")하여 설치디렉토리 밑의 bin 디렉토리에 있는 ssleay32.dll, libeay32.dll 파일을 시스템디렉토리, (Windows 2000의 경우 C:\WINNT, Windows XP, 2003등은 C:\Windows)아래 system32 디렉토리로 복사한다.

```
PROMPT> copy ssleay32.dll C:\WINDOWS\system32\
```

```
PROMPT> copy libeay32.dll C:\WINDOWS\system32\
```



```
C:\Program Files\Apache Group\Apache2\bin>copy libeay32.dll C:\WINDOWS\system32\
1개 파일이 복사되었습니다.

C:\Program Files\Apache Group\Apache2\bin>copy ssleay32.dll C:\WINDOWS\system32\
1개 파일이 복사되었습니다.

C:\Program Files\Apache Group\Apache2\bin>
```

- o openssl.conf 파일 편집

- 인증서를 위한 csr 파일을 만들때 입력하는 부분을 지정
- _default로 된 값을 설정하면 추가 입력이 필요없다.
- openssl.conf 파일은 conf 디렉토리 밑에 있다.(위치는 지정하면 되므로 상관없다)

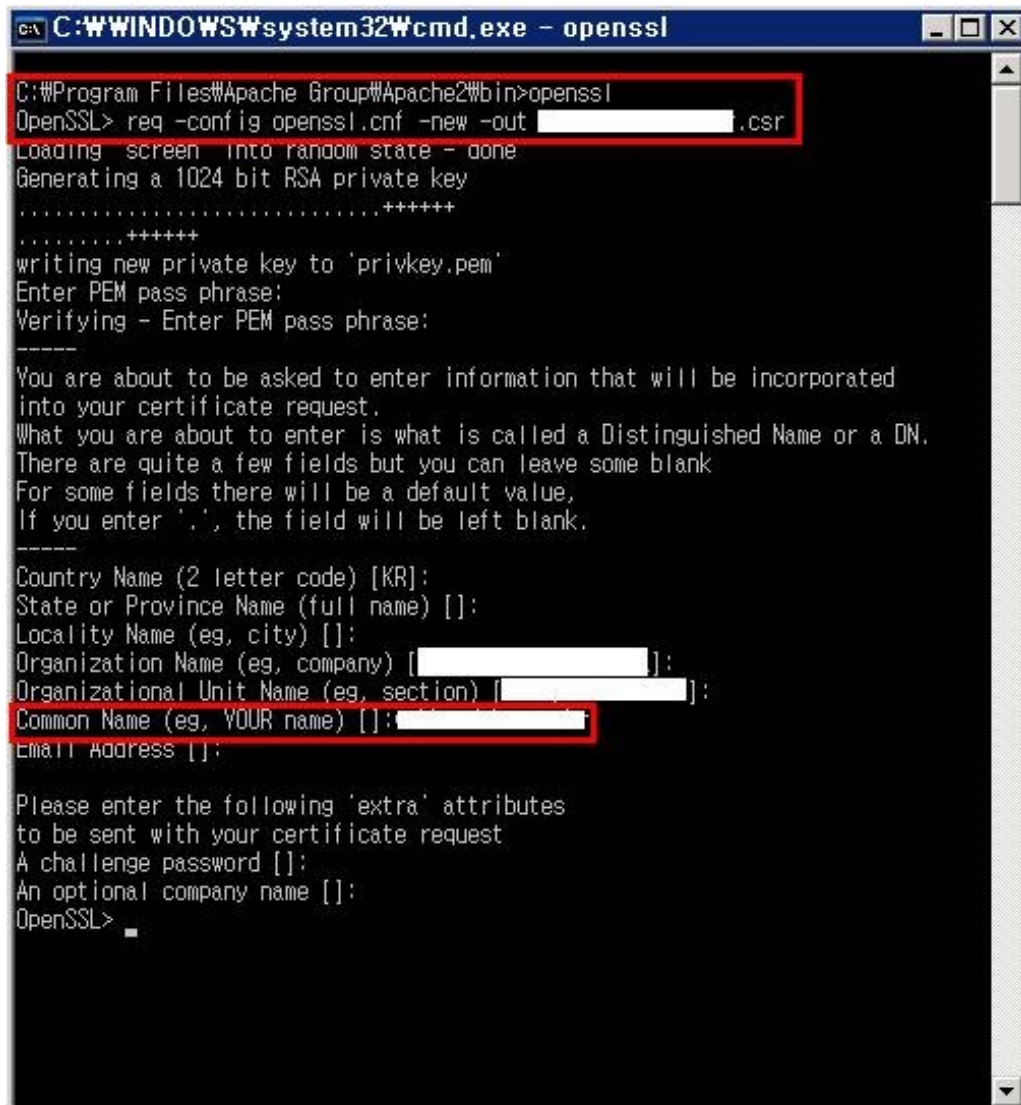
```
openssl.cnf
118 # so use this option with caution!
119 string_mask = nombstr
120
121 # req_extensions = v3_req # The extensions to add to a certificate request
122
123 [ req_distinguished_name ]
124 countryName = Country Name (2 letter code)
125 countryName_default = AU
126 countryName_min = 2
127 countryName_max = 2
128
129 stateOrProvinceName = State or Province Name (full name)
130 stateOrProvinceName_default = Some-State
131
132 localityName = Locality Name (eg, city)
133
134 O.organizationName = Organization Name (eg, company)
135 O.organizationName_default = Internet Widgits Pty Ltd
136
137 # we can do this but it is not needed normally :-)
138 #1.organizationName = Second Organization Name (eg, company)
139 #1.organizationName_default = World Wide Web Pty Ltd
140
141 organizationalUnitName = Organizational Unit Name (eg, section)
142 #organizationalUnitName_default =
143
144 commonName = Common Name (eg, YOUR name)
145 commonName_max = 64
146
147 emailAddress = Email Address
148 emailAddress_max = 64
149
150 # SET-ex3 = SET extension number 3
151
152 [ req_attributes ]
```

openssl.conf 파일 편집

o CSR 생성(이과정을 마치면 privkey.pem, www.my-server.csr 파일이 생성됨)

PROMPT> openssl req -config openssl.cnf -new -out [www.my-server.csr](#)

※ "Common Name" 부분에 웹서버의 정확한 이름(FQDN)을 입력하지 않으면 접속시 인증서의 이름과 다르다는 내용이 나온다.



```
C:\WINDOWS\system32\cmd.exe - openssl
C:\Program Files\Apache Group\Apache2\bin>openssl
OpenSSL> req -config openssl.cnf -new -out [redacted].csr
Loading screen into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [KR]:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) [redacted]:
Organizational Unit Name (eg, section) [redacted]:
Common Name (eg, YOUR name) []: [redacted]
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL>
```

- o privkey.pem 파일에서 passphrase를 제거
 - 이과정은 private key에서 passphrase를 제거하는 과정이다.
 - key값은 아파치 서버와 관리자만 읽을 수 있어야 한다.

```
C:\WINDOWS\system32\cmd.exe - openssl

C:\Program Files\Apache Group\Apache2\bin>openssl
OpenSSL> rsa -in privkey.pem -out [redacted].key
Enter pass phrase for privkey.pem:
writing RSA key
OpenSSL>
```

- .rnd 파일이 생성되는데 이 파일에는 키생성을 위한 entropy 정보를 담고 있고 private key에 대한 암호학적 공격에 사용될 수 있기 때문에 .rnd 파일을 삭제한다.

```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\Apache Group\Apache2\bin>dir *.*
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: E4D0-E4DA

C:\Program Files\Apache Group\Apache2\bin 디렉터리

2007-11-13 오전 11:14 <DIR>
2007-11-13 오전 11:14 <DIR>
2007-11-13 오전 11:13 1,024 .rnd
1개 파일 1,024 바이트
2개 디렉터리 1,378,758,656 바이트 남음

C:\Program Files\Apache Group\Apache2\bin>del .rnd
C:\Program Files\Apache Group\Apache2\bin>
```

o Self Sign

- 이 과정은 CA로부터 실제 인증서를 받기 전까지 사용할 수 있는 self-signed 인증서를 생성하는 과정이다. 이 인증서는 1년 후에 expire된다. -days 옵션을 통해 날짜를 증가시킬 수 있다.

PROMPT> openssl x509 -in [www.my-server.csr](#) -out [www.my-server.cert](#) -req -signkey [www.my-server.csr.key](#) -days 365

```
C:\WINDOWS\system32\cmd.exe - openssl

C:\Program Files\Apache Group\Apache2\bin>openssl
OpenSSL> x509 -in [redacted].csr -out [redacted].cert -req -signkey
[redacted].kr.key -days 365
Loading screen into random state - done
Signature ok
subject=/C=KR/O=[redacted]/OU=[redacted]/CN=[redacted]
Getting Private key
OpenSSL>
```

- o 아파치 설치 디렉토리의 conf 디렉토리 아래에 ssl 디렉토리를 만든다.


```
PROMPT> cd "C:\Program Files\Apache Group\Apache2\conf"
PROMPT> mkdir ssl
```

- o 인증서 파일(www.my-server.cert)과 키(www.my-server.key) 파일을 지정한 디렉토리로 옮긴다.

```
PROMPT> cd "C:\Program Files\Apache Group\Apache2\bin"
PROMPT> move www.my-server.cert ..\conf\ssl\
PROMPT> move www.my-server.key ..\conf\ssl\
```

- o httpd.conf 수정(mod_ssl 사용하도록)

```
#
<IfModule mod_ssl.c>
    Include conf/ssl.conf
</IfModule>

LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule ssl_module modules/mod_ssl.so
```

- o ssl.conf 수정

```
#<IfDefine SSL>
#
# Note: This must come before the <IfDefine SSL> container to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random 512
#       to use and second the expiring timeout (in seconds).
SSLSessionCache             none
#SSLSessionCache             shmmt:logs/ssl_scache(512000)
#SSLSessionCache             shmcb:logs/ssl_scache(512000)
#SSLSessionCache             dbm:logs/ssl_scache
#SSLSessionCacheTimeout     300
#
# Semaphore:
# Configure the path to the mutual exclusion semaphore the
# SSL engine uses internally for inter-process synchronization.
SSLMutex default
```

```
<VirtualHost _default_:443>
#   General setup for the virtual host
DocumentRoot " "
ServerName :443
ServerAdmin 
ErrorLog logs/error_log
TransferLog logs/access_log

<Directory " ">
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   SSL Cipher Suite:
```

```
#   ciphers, etc.)
SSLCertificateFile conf/ssl/ .cer
#SSLCertificateFile conf/ssl.crt/server.crt
#SSLCertificateFile conf/ssl.crt/server-dsa.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file. Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile conf/ssl/ .key
#SSLCertificateKeyFile conf/ssl.key/server.key
#SSLCertificateKeyFile conf/ssl.key/server-dsa.key
#SSLCertificateKeyFile conf/ssl.key/server-ecdsa.key
#SSLCertificateKeyFile conf/ssl.key/server-gss.conf
#SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire
<FilesMatch "%.(cgi|shtml|phtml|php|html|php3?)$" >
    SSLOptions +StdEnvVars
</FilesMatch>

CustomLog logs/ssl_request_log %
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x W"%rW" %b"

</VirtualHost>
#</IfDefine>
```

o 설정파일 문법 검사 및 아파치 시작

```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\Apache Group\Apache2\bin>apache -t
Syntax OK

C:\Program Files\Apache Group\Apache2\bin>apache -k restart_
```

o 네트워크 open port 확인

```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\Apache Group\Apache2\bin>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP    0.0.0.0:80              0.0.0.0:0               LISTENING
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING
TCP    0.0.0.0:443             0.0.0.0:0               LISTENING
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1025            0.0.0.0:0               LISTENING
TCP    0.0.0.0:1028            0.0.0.0:0               LISTENING
```

o 서비스 접속 확인

주의:Internet Explorer 보안 강화 구성 설정 안 됨

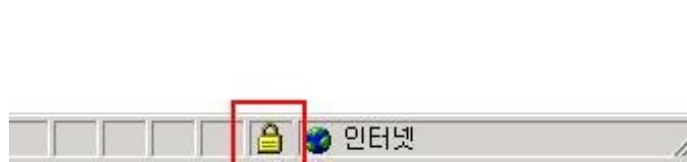
Internet Explorer 보안 강화 구성은 Windows Server 2003 운영 체제에서 제공하는 선택 사항으로, 자에 대해 Internet Explorer 보안 설정을 강화하는 데 사용될 수 있습니다.

이 사이트와 교환한 정보는 다른 사람이 보거나 변경할 수 없습니다. 그러나 사이트 보안 인증서에 문제가 있습니다.

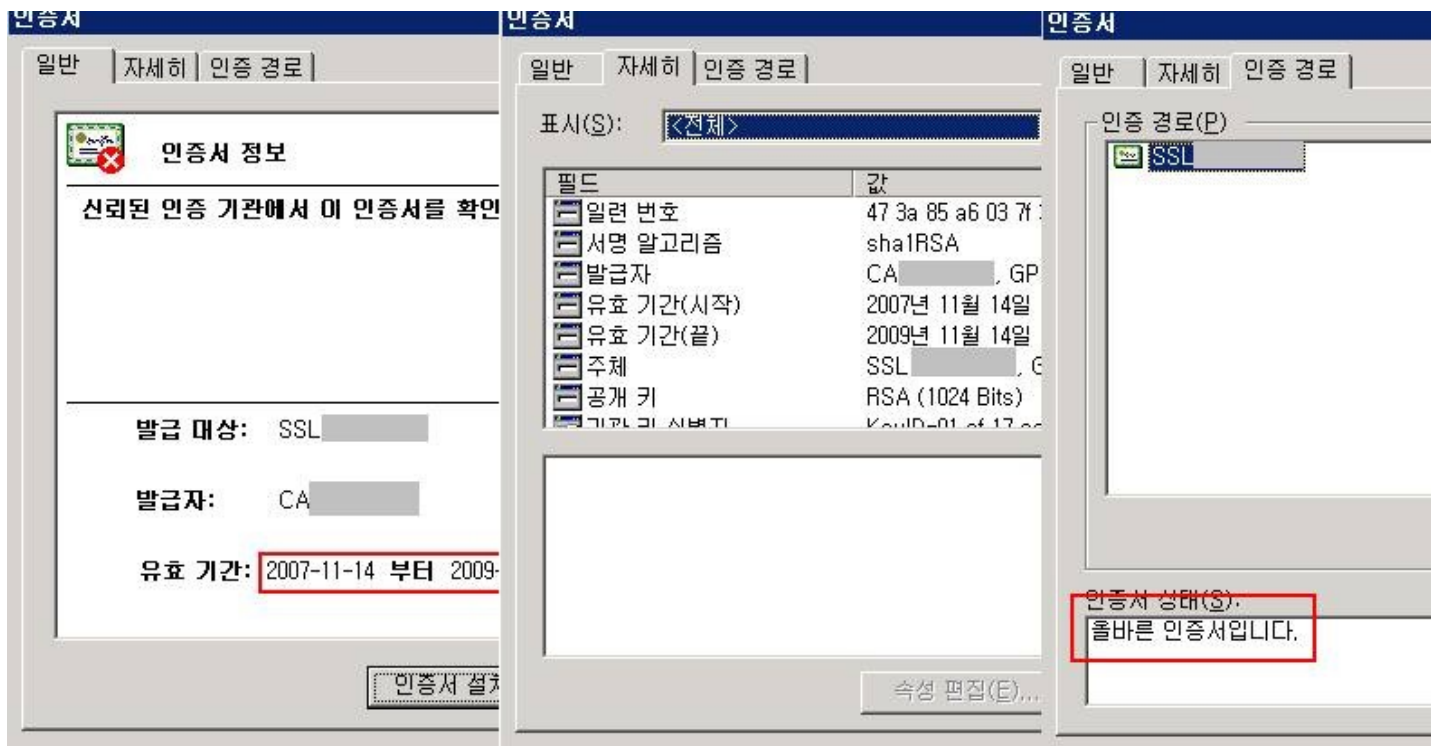
- 신뢰 여부를 결정한 적이 없는 회사에서 발급한 보안 인증서입니다. 인증 기관의 신뢰 여부를 결정하려면 인증서를 확인하십시오.
- 보안 인증서 날짜가 유효합니다.
- 보안 인증서의 이름이 올바르지 않거나 사이트 이름과 일치하지 않습니다.

계속하시겠습니까?

예(Y) 아니오(N) 인증서 보기(V)



o 인증서 정보 확인



o 참고 URL

http://www.modssl.org/docs/2.8/ssl_faq.html

○ apache+ssl

<http://www.thompsonbd.com/tutorials/apachessl.php>

 마이피플  트위터  페이스북 [더보기 ▾](#)



Posted by She쥬포s

TAG [apache](#), [apache+ssl+windows](#), [linux](#), [self-singed CA](#), [SSL](#), [UNIX](#), [보안](#), [인증서](#)
[트랙백 0개](#), [댓글 0개가 달렸습니다](#).

[이전 1](#) ... [226](#) [227](#) [228](#) [229](#) [230](#) [231](#) [232](#) [233](#) [234](#) ... [327](#) [다음](#)



by She쥬포s
[별아가면서 지켜야..](#)

- [23/3923](#)
- [\[읽어주세요\]내용상..](#)
- [안녕하세요?](#)

•

 관리자

 글쓰기

검색

카테고리

-  분류 전체보기 (327)
-  살다보면 (71)
-  RedHat (2)
-  Network (2)
-  Unix (150)
-  Windows (16)
-  보안 (20)
-  음악 (20)
-  System HW (4)
-  Utility (11)
-  기타내용 (9)
-  피닉스 (4)
-  DataBase (12)
-  뉴스따라잡기 (2)
-  IT관련정리 (1)
-  MCTS (1)

태그목록

- [GMP](#)
- [Absolute](#)
- [dd](#)
- [Solaris](#)
- [jar](#)
- [라스베가스](#)
- [감정 다스리기](#)
- [relative](#)
- [xargs](#)
- [rsync](#)
- [Zip](#)
- [linux](#)
- [tutorial](#)
- [HP-UX](#)
- [RT](#)
- [tar](#)
- [0403-027 The parameter list is too long](#)
- [영어문장](#)
- [UNIX](#)
- [wakeonlan](#)
- [java](#)
- [queryformat](#)

- [Oracle](#)
- [RPM](#)
- [PAX](#)
- [지침서](#)
- [sysrq](#)
- [lvm](#)
- [설치](#)
- [online JFS](#)

최근에 올라온 글

- [내자가추\(來者可追\).](#)
- [오늘 하루는..?](#)
- [많은 파일 다루기\(D...](#)
- [블로그 블라인드??](#)
- [\[영어문장\]2012-03-02.](#)

최근에 달린 댓글

- [안녕하세요. 혹시...](#) 도움이 필요합니다. 05/25
- [ㅎㅎㅎ 왜 안되지?...](#) She쥐포s 2010
- [꼭 좋으네요 즐감^^](#) 고리 2010
- [음 옛날에 번역해...](#) She쥐포s 2009
- [한글자료 구하든 나...](#) Goodez 2009

최근에 받은 트랙백

글 보관함

- [2012/06](#)(1)
- [2012/04](#)(2)
- [2012/03](#)(2)
- [2012/01](#)(2)
- [2011/11](#)(1)

달력

« 2012/06 »

일	월	화	수	목	금	토
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

링크

- [나의 실크로드를 찾...](#)
- [OKJSP tistory.](#)

Total
69,010
Today
11
Yesterday
91



[티스토리 가입하기!](#)



[지역로그](#) : [태그로그](#) : [미디어로그](#) : [방명록](#) : [관리자](#) : [글쓰기](#)
[She쥬포s's Blog](#) is powered by [Daum](#) / Designed by [Tistory](#)

