

2.6 IMPLEMENTACIÓN DE SERVICIOS HTTP

SECCIÓN 1

Install httpd

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player
Install 1 Package (+4 Dependent packages)

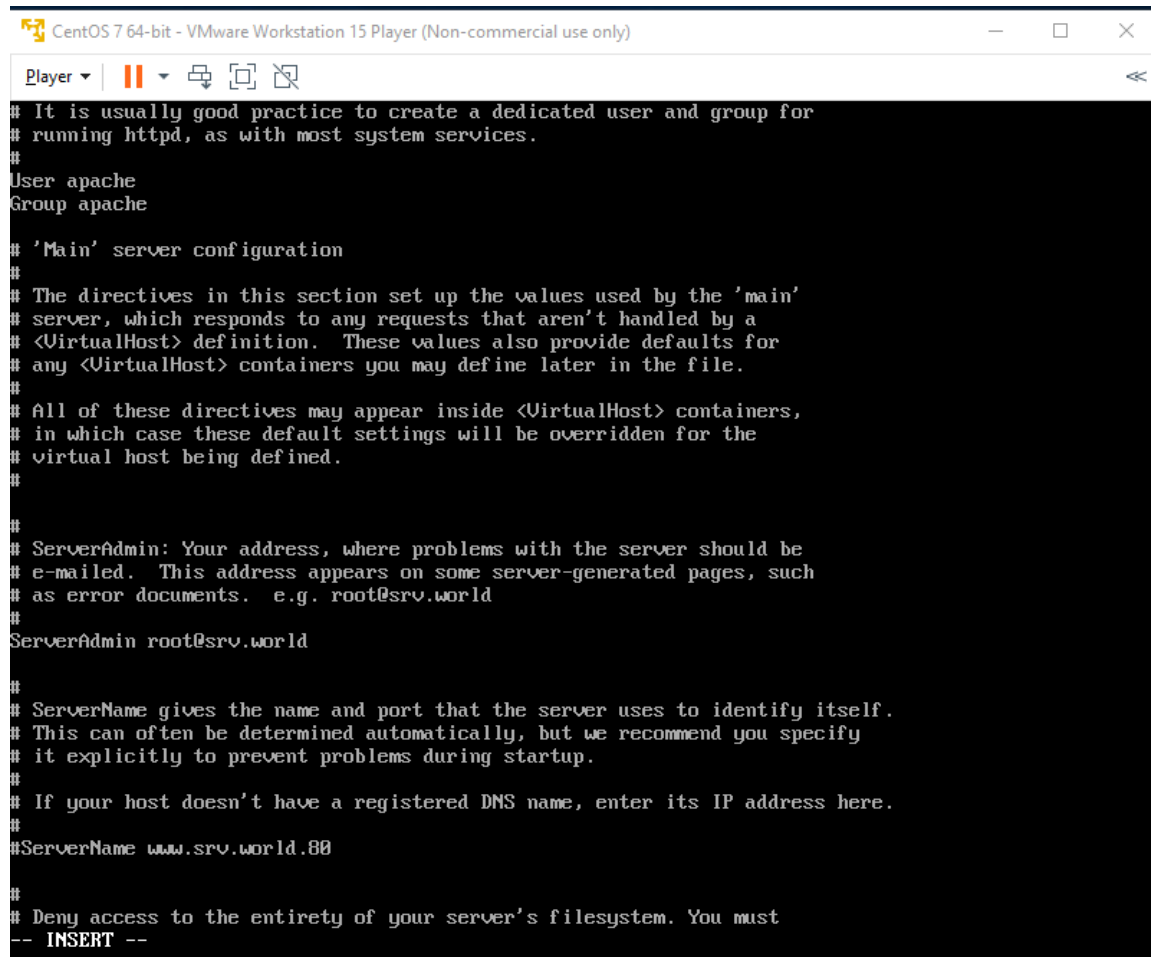
Total download size: 3.0 M
Installed size: 10 M
Downloading packages:
(1/5): apr-1.4.8-3.el7_4.1.x86_64.rpm           | 103 kB  00:00:01
(2/5): apr-util-1.5.2-6.el7.x86_64.rpm         |  92 kB  00:00:01
(3/5): mailcap-2.1.41-2.el7.noarch.rpm         |  31 kB  00:00:01
(4/5): httpd-tools-2.4.6-88.el7.centos.x86_64.rpm |  90 kB  00:00:01
(5/5): httpd-2.4.6-88.el7.centos.x86_64.rpm    | 2.7 MB  00:01:34
-----
Total                                          33 kB/s | 3.0 MB  00:01:34
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.4.8-3.el7_4.1.x86_64                1/5
  Installing : apr-util-1.5.2-6.el7.x86_64              2/5
  Installing : httpd-tools-2.4.6-88.el7.centos.x86_64   3/5
  Installing : mailcap-2.1.41-2.el7.noarch              4/5
  Installing : httpd-2.4.6-88.el7.centos.x86_64        5/5
  Verifying  : httpd-tools-2.4.6-88.el7.centos.x86_64   1/5
  Verifying  : apr-1.4.8-3.el7_4.1.x86_64              2/5
  Verifying  : mailcap-2.1.41-2.el7.noarch             3/5
  Verifying  : httpd-2.4.6-88.el7.centos.x86_64       4/5
  Verifying  : apr-util-1.5.2-6.el7.x86_64            5/5

Installed:
  httpd.x86_64 0:2.4.6-88.el7.centos

Dependency Installed:
  apr.x86_64 0:1.4.8-3.el7_4.1          apr-util.x86_64 0:1.5.2-6.el7
  httpd-tools.x86_64 0:2.4.6-88.el7.centos mailcap.noarch 0:2.1.41-2.el7

Complete!
[root@localhost ~]# rm -f /etc/httpd/config.d/welcome.config
[root@localhost ~]# _
```

Configure httpd



```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player ▾ | [Icons]
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache

# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. root@srv.world
#
ServerAdmin root@srv.world

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.srv.world.88

#
# Deny access to the entirety of your server's filesystem. You must
-- INSERT --
```

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)

Player ▾ | [Icons]

# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride ALL

#
# Controls who can get stuff from this server.
#
Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html index.cgi index.php
    ServerTokens Prod
    KeepAlive On
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
-- INSERT --
```

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player
</IfModule>

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

"/etc/httpd/conf/httpd.conf" 357L, 11804C written
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]#
```

Firewall is Running

```
"/etc/httpd/conf/httpd.conf" 357L, 11804C written
[root@localhost ~]# systemctl start httpd
[root@localhost ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@localhost ~]# firewall-cmd --add-service=http --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# _
```

Create HTML

[illegible]

SECCIÓN 2

Install php

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player | || | |
(8/9): php-5.4.16-46.el7.x86_64.rpm | 1.4 MB 00:00:12
(9/9): php-cli-5.4.16-46.el7.x86_64.rpm | 2.7 MB 00:01:15
-----
Total | 81 kB/s | 6.0 MB 00:01:15
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libzip-0.10.1-8.el7.x86_64 | 1/9
  Installing : php-common-5.4.16-46.el7.x86_64 | 2/9
  Installing : php-cli-5.4.16-46.el7.x86_64 | 3/9
  Installing : php-process-5.4.16-46.el7.x86_64 | 4/9
  Installing : libxslt-1.1.28-5.el7.x86_64 | 5/9
  Installing : php-xml-5.4.16-46.el7.x86_64 | 6/9
  Installing : 1:php-pear-1.9.4-21.el7.noarch | 7/9
  Installing : php-5.4.16-46.el7.x86_64 | 8/9
  Installing : php-mbstring-5.4.16-46.el7.x86_64 | 9/9
  Verifying : libxslt-1.1.28-5.el7.x86_64 | 1/9
  Verifying : php-mbstring-5.4.16-46.el7.x86_64 | 2/9
  Verifying : php-process-5.4.16-46.el7.x86_64 | 3/9
  Verifying : php-cli-5.4.16-46.el7.x86_64 | 4/9
  Verifying : libzip-0.10.1-8.el7.x86_64 | 5/9
  Verifying : php-5.4.16-46.el7.x86_64 | 6/9
  Verifying : php-common-5.4.16-46.el7.x86_64 | 7/9
  Verifying : php-xml-5.4.16-46.el7.x86_64 | 8/9
  Verifying : 1:php-pear-1.9.4-21.el7.noarch | 9/9

Installed:
  php.x86_64 0:5.4.16-46.el7  php-mbstring.x86_64 0:5.4.16-46.el7  php-pear.noarch 1:1.9.4-21.el7

Dependency Installed:
  libxslt.x86_64 0:1.1.28-5.el7 | libzip.x86_64 0:0.10.1-8.el7
  php-cli.x86_64 0:5.4.16-46.el7 | php-common.x86_64 0:5.4.16-46.el7
  php-process.x86_64 0:5.4.16-46.el7 | php-xml.x86_64 0:5.4.16-46.el7

Complete!
[root@localhost ~]#
```

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player
[CLI Server]
; Whether the CLI web server uses ANSI color coding in its terminal output.
cli_server.color = On

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
;date.timezone = "Asia/Tokyo"

; http://php.net/date.default-latitude
;date.default_latitude = 31.7667

; http://php.net/date.default-longitude
;date.default_longitude = 35.2333

; http://php.net/date.sunrise-zenith
;date.sunrise_zenith = 90.583333

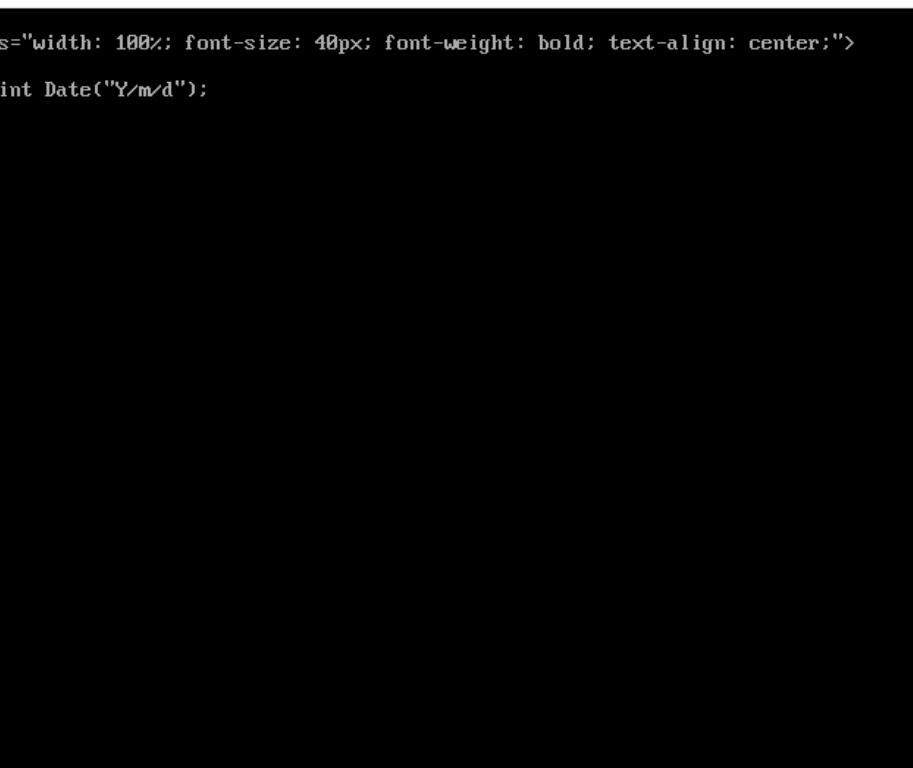
; http://php.net/date.sunset-zenith
;date.sunset_zenith = 90.583333

[filter]
; http://php.net/filter.default
;filter.default = unsafe_raw

; http://php.net/filter.default-flags
;filter.default_flags =

[iconv]
;iconv.input_encoding = ISO-8859-1
"/etc/php.ini" 1797L, 64958C written
[root@localhost ~]# systemctl restart httpd
[root@localhost ~]#
```

Create a php



The screenshot shows a terminal window within a VMware Workstation 15 Player. The terminal displays the following PHP code and its output:

```
<body>
<div style="width: 100%; font-size: 40px; font-weight: bold; text-align: center;">
<?php
    print Date("Y/m/d");
?>
</div>
</body>
</html>
```

The output of the script is:

```
2020/07/22
```

At the bottom of the terminal, the following command and output are visible:

```
"/var/www/html/index.php" [New] 10L, 154C written
[root@localhost ~]#
```


SECCIÓN 30

Install mod security

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player | || | | |
Loading mirror speeds from cached hostfile
* base: mirror.us-midwest-1.nexcess.net
* extras: mirrors.xmission.com
* updates: centos.mirror.lstn.net
Resolving Dependencies
--> Running transaction check
---> Package mod_security.x86_64 0:2.9.2-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version           Repository        Size
=====
Installing:
mod_security            x86_64        2.9.2-1.el7       base              249 k
=====

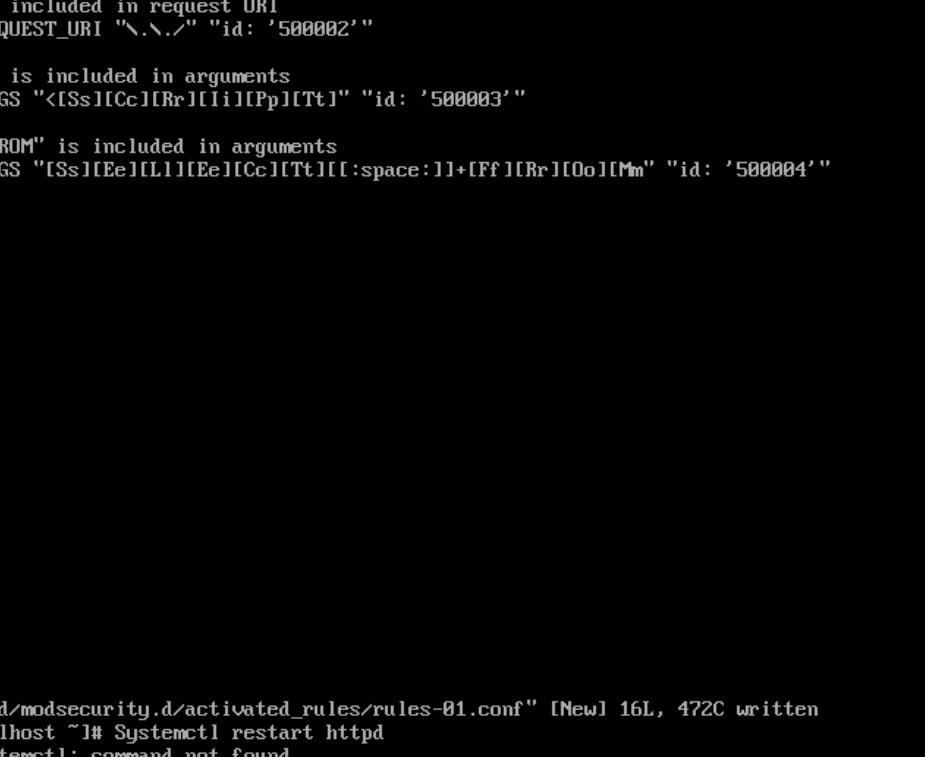
Transaction Summary
=====
Install 1 Package

Total download size: 249 k
Installed size: 980 k
Downloading packages:
mod_security-2.9.2-1.el7.x86_64.rpm                | 249 kB  00:00:03
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : mod_security-2.9.2-1.el7.x86_64      1/1
  Verifying  : mod_security-2.9.2-1.el7.x86_64      1/1

Installed:
  mod_security.x86_64 0:2.9.2-1.el7

Complete!
[root@localhost ~]# _
```

For example



```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player | [Icons]
# "../" is included in request URI
SecRule REQUEST_URI "\.\/" "id: '500002'"

#"<SCRIPT" is included in arguments
SecRule ARGS "<[Ss][Cc][Rr][Ii][Pp][Tt]" "id: '500003'"

#"SELECT FROM" is included in arguments
SecRule ARGS "[Ss][Ee][Ll][Ee][Cc][Tt][:space:]+[Ff][Rr][Oo][Mm]" "id: '500004'"

...

/etc/httpd/modsecurity.d/activated_rules/rules-01.conf" [New] 16L, 472C written
[root@localhost ~]# Systemctl restart httpd
-bash: Systemctl: command not found
[root@localhost ~]# systemctl restart httpd
Job for httpd.service failed because the control process exited with error code. See "systemctl stat
us httpd.service" and "journalctl -xe" for details.
[root@localhost ~]#
```

General rules

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Loading mirror speeds from cached hostfile
* base: mirror.us-midwest-1.nexcess.net
* extras: mirrors.xmission.com
* updates: centos.mirror.lstn.net
Resolving Dependencies
--> Running transaction check
---> Package mod_security_crs.noarch 0:2.2.9-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                        Arch          Version        Repository      Size
=====
Installing:
mod_security_crs              noarch        2.2.9-1.el7    base            91 k
=====

Transaction Summary
=====
Install 1 Package

Total download size: 91 k
Installed size: 375 k
Downloading packages:
mod_security_crs-2.2.9-1.el7.noarch.rpm | 91 kB 00:00:23
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : mod_security_crs-2.2.9-1.el7.noarch | 1/1
  Verifying  : mod_security_crs-2.2.9-1.el7.noarch | 1/1

Installed:
  mod_security_crs.noarch 0:2.2.9-1.el7

Complete!
[root@localhost ~]#
```

```
CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player ▾ || ▾ □ □ □
Downloading packages:
mod_security_crs-2.2.9-1.el7.noarch.rpm | 91 kB 00:00:23
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : mod_security_crs-2.2.9-1.el7.noarch 1/1
  Verifying : mod_security_crs-2.2.9-1.el7.noarch 1/1

Installed:
  mod_security_crs.noarch 0:2.2.9-1.el7

Complete!
[root@localhost ~]# ll /usr/lib/modsecurity.d/base_rules
total 336
-rw-r--r--. 1 root root 1969 Nov 5 2016 modsecurity_35_bad_robots.data
-rw-r--r--. 1 root root 386 Nov 5 2016 modsecurity_35_scanners.data
-rw-r--r--. 1 root root 3928 Nov 5 2016 modsecurity_40_generic_attacks.data
-rw-r--r--. 1 root root 2224 Nov 5 2016 modsecurity_50_outbound.data
-rw-r--r--. 1 root root 56714 Nov 5 2016 modsecurity_50_outbound_malware.data
-rw-r--r--. 1 root root 22924 Nov 5 2016 modsecurity_crs_20_protocol_violations.conf
-rw-r--r--. 1 root root 6914 Nov 5 2016 modsecurity_crs_21_protocol_anomalies.conf
-rw-r--r--. 1 root root 3792 Nov 5 2016 modsecurity_crs_23_request_limits.conf
-rw-r--r--. 1 root root 6933 Nov 5 2016 modsecurity_crs_30_http_policy.conf
-rw-r--r--. 1 root root 5410 Nov 5 2016 modsecurity_crs_35_bad_robots.conf
-rw-r--r--. 1 root root 20469 Nov 5 2016 modsecurity_crs_40_generic_attacks.conf
-rw-r--r--. 1 root root 43654 Nov 5 2016 modsecurity_crs_41_sql_injection_attacks.conf
-rw-r--r--. 1 root root 96711 Nov 5 2016 modsecurity_crs_41_xss_attacks.conf
-rw-r--r--. 1 root root 1795 Nov 5 2016 modsecurity_crs_42_tight_security.conf
-rw-r--r--. 1 root root 3660 Nov 5 2016 modsecurity_crs_45_trojans.conf
-rw-r--r--. 1 root root 2247 Nov 5 2016 modsecurity_crs_47_common_exceptions.conf
-rw-r--r--. 1 root root 2787 Nov 5 2016 modsecurity_crs_48_local_exceptions.conf.example
-rw-r--r--. 1 root root 1838 Nov 5 2016 modsecurity_crs_49_inbound_blocking.conf
-rw-r--r--. 1 root root 22336 Nov 5 2016 modsecurity_crs_50_outbound.conf
-rw-r--r--. 1 root root 1448 Nov 5 2016 modsecurity_crs_59_outbound_blocking.conf
-rw-r--r--. 1 root root 2674 Nov 5 2016 modsecurity_crs_60_correlation.conf
[root@localhost ~]#
```