

Proyecto Módulo 2

Manual de Usuario


Cabrera Balderas Carlos Eduardo
Gonzalez Vargas Andrea Itzel

Índice

1. Login	2
2. Dashboard	2
3. Sección de monitoreo de usuarios	3
4. Sección de monitoreo de procesos	3
5. Sección de monitoreo de red	4
6. Sección de monitoreo de autenticación	4
7. Sección de monitoreo de almacenamiento	5
8. Sección de monitoreo de archivos y sockets	5
9. Sección de monitoreo de servidor web	6
10.Secciones personalizadas	9
11.Archivo de configuración	9
12.Administrar cuentas de usuario	10

1. Login

Para iniciar sesión se tiene que contar con credenciales válidas, se ingresan y le da en *Iniciar Sesión* para iniciar sesión con su usuario.



The logo for UNAM CERT is centered at the top. It features a blue shield with a white keyhole in the center, containing a red dot. Above the shield are two blue horse heads facing each other. Below the shield, the text "UNAM" is stacked above "CERT" in a blue, serif font.

Below the logo is a login form with two input fields and a button:

- The first input field has a small person icon on the left.
- The second input field has a small lock icon on the right.
- Below the input fields is a blue button with the text "INICIAR SESIÓN" in white, uppercase letters.

2. Dashboard

Es la ventana principal, por lo tanto, es lo que primero verá el usuario al acceder a su cuenta, contando con características como la distribución, arquitectura y nombre del equipo, dominio y las tareas de cron que existen en el sistema.

Podemos acceder a las demás secciones dando click en la parte superior izquierda en el menú y eligiendo la sección deseada.

Dashboard

Distribución: Ubuntu 16.04.3 LTS
 Arquitectura: x86_64
 Nombre de equipo: chepe
 Nombre de dominio: (none)

Tareas de cron:

Sistema:
 SHELL=/bin/sh
 PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
 17 * * * * root cd / && run-parts --report /etc/cron.hourly
 25 6 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily)
 47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly)
 52 6 1 * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly)
 Usuario chepe:
 0 5 * * 1 ls

3. Sección de monitoreo de usuarios

Es la primera sección y, en esta, se muestran todos los usuarios del sistema con sus respectivos grupos, así como los usuarios activos y bloqueados.

Monitoreo de usuarios

USUARIOS Y GRUPOS

USUARIOS ACTIVOS

Usuario: Grupos
 root: root
 daemon: daemon
 bin: bin
 sys: sys
 sync: nogroup
 games: games
 man: man
 lp: lp
 mail: mail
 news: news
 uucp: uucp
 proxy: proxy
 www-data: www-data
 backup: backup
 list: list
 irc: irc
 gnats: gnats
 nobody: nogroup
 systemd-timesync: systemd-timesync
 systemd-network: systemd-network
 systemd-resolve: systemd-resolve
 systemd-bus-proxy: systemd-bus-proxy
 syslog: syslog adm
 apt: nogroup
 messagebus: messagebus
 uidd: uidd
 lightdm: lightdm
 whoopsie: whoopsie
 avahi-autoipd: avahi-autoipd
 avahi: avahi
 dnsmasq: nogroup

Usuarios bloqueados
 daemon
 bin
 sys
 sync
 games
 man
 lp
 mail
 news
 uucp
 proxy
 www-data
 backup
 list
 irc
 gnats
 nobody
 systemd-timesync
 systemd-network
 systemd-resolve
 systemd-bus-proxy
 syslog
 _apt
 messagebus
 uidd
 lightdm
 whoopsie
 avahi-autoipd
 avahi
 dnsmasq
 colord
 speech-dispatcher

4. Sección de monitoreo de procesos

En dicha sección se podrán visualizar los procesos actuales del sistema con características como el PID, usuario, CPU, uso de memoria por proceso y el nombre del proceso.

Se puede hacer búsqueda textual o por expresión regular para filtrar la información y tener algo más específico a lo que se requiere.

Monitoreo de procesos

Búsqueda textual

Búsqueda por expresión regular

FILTRAR

PID	UID	USER	%CPU	%MEM	CMD
1	0	root	0.0	0.0	/sbin/init splash
2	0	root	0.0	0.0	[kthreadd]
3	0	root	0.0	0.0	[ksoftirqd/0]
5	0	root	0.0	0.0	[kworker/0:0H]
7	0	root	0.1	0.0	[rcu_sched]
8	0	root	0.0	0.0	[rcu_bh]
9	0	root	0.0	0.0	[migration/0]
10	0	root	0.0	0.0	[watchdog/0]
11	0	root	0.0	0.0	[watchdog/1]
12	0	root	0.0	0.0	[migration/1]
13	0	root	0.0	0.0	[ksoftirqd/1]
15	0	root	0.0	0.0	[kworker/1:0H]
16	0	root	0.0	0.0	[watchdog/2]
17	0	root	0.0	0.0	[migration/2]
18	0	root	0.0	0.0	[ksoftirqd/2]
20	0	root	0.0	0.0	[kworker/2:0H]
21	0	root	0.0	0.0	[watchdog/3]
22	0	root	0.0	0.0	[migration/3]
23	0	root	0.0	0.0	[ksoftirqd/3]
25	0	root	0.0	0.0	[kworker/3:0H]
26	0	root	0.0	0.0	[watchdog/4]
27	0	root	0.0	0.0	[migration/4]
28	0	root	0.0	0.0	[ksoftirqd/4]
30	0	root	0.0	0.0	[kworker/4:0H]
31	0	root	0.0	0.0	[watchdog/5]
32	0	root	0.0	0.0	[migration/5]
33	0	root	0.0	0.0	[ksoftirqd/5]
35	0	root	0.0	0.0	[kworker/5:0H]
36	0	root	0.0	0.0	[watchdog/6]
37	0	root	0.0	0.0	[migration/6]
38	0	root	0.0	0.0	[ksoftirqd/6]
40	0	root	0.0	0.0	[kworker/6:0H]

5. Sección de monitoreo de red

Aquí se puede encontrar información de la red como la ip, el gateway, los puertos escucha en TCP/UDP, las conexiones, estadísticas y las reglas de iptables entre otros.

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

UNAM CERT

Monitoreo de red

INTERFACES Y PUERTOS

CONEXIONES

IPTABLES

ESTADÍSTICAS

Interfaz IP/Máscara Gateway

wlp3s0 192.168.100.23/24 192.168.100.1

wlp3s0 192.168.100.23/24 0.0.0.0

wlp3s0 192.168.100.23/24 0.0.0.0

vmnet1 172.16.163.1/24 0.0.0.0

vmnet2 192.168.1.1/24 0.0.0.0

vmnet8 192.168.42.1/24 0.0.0.0

virbr0 192.168.122.1/24 0.0.0.0

Puertos en escucha

tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	5083/cupsd
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	2529/master
tcp	0	0	127.0.0.1:9050	0.0.0.0:*	LISTEN	1197/tor
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	2093/vmware-hostd
tcp	0	0	0.0.0.0:17500	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	127.0.0.1:8000	0.0.0.0:*	LISTEN	8033/python3
tcp	0	0	127.0.0.1:17600	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	127.0.0.1:17603	0.0.0.0:*	LISTEN	3394/dropbox
tcp	0	0	0.0.0.0:389	0.0.0.0:*	LISTEN	1399/slapd
tcp	0	0	0.0.0.0:902	0.0.0.0:*	LISTEN	1696/vmware-authdla
tcp	0	0	127.0.0.1:11211	0.0.0.0:*	LISTEN	1140/memcached
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	LISTEN	1142/ssh
tcp	0	0	0.0.0.0:7890	0.0.0.0:*	LISTEN	3053/goaccess
tcp	0	0	127.0.0.1:8307	0.0.0.0:*	LISTEN	2093/vmware-hostd
tcp	0	0	127.0.1.1:53	0.0.0.0:*	LISTEN	2757/dnsmasq
tcp	0	0	192.168.122.1:53	0.0.0.0:*	LISTEN	2292/dnsmasq
tcp6	0	0	:::1:631	:::*	LISTEN	5083/cupsd
tcp6	0	0	:::25	:::*	LISTEN	2529/master
tcp6	0	0	:::443	:::*	LISTEN	2093/vmware-hostd
tcp6	0	0	:::17500	:::*	LISTEN	3394/dropbox
tcp6	0	0	:::389	:::*	LISTEN	1399/slapd

6. Sección de monitoreo de autenticación

En esta sección se podrá ver la bitácora de auth.log de manera *cruda* pero permitiendo búsquedas específicas para depurar la información que queremos obtener del archivo.

EDITAR DATOS

ADMINISTRAR USUARIOS

ADMINISTRAR SECCIONES

Bitácora auth.log

Ubicación: /var/log/auth.log

Número máximo de líneas

Búsqueda textual

Búsqueda por expresión regular

FILTRAR

```
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u rtkit -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u saned -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u usbmux -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u chepe -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u sshd -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u postgres -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u memcache -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u guest-4wksfp -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u mysql -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u guest-ux0cqm -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u libvirt-qemu -l
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 31 21:54:20 chepe sudo: pam_unix(sudo:session): session closed for user root
Mar 31 21:54:20 chepe sudo: superuser : TTY=unknown ; PWD=/home/superuser ; USER=root ; COMMAND=/usr/bin/crontab -u libvirt-dnsmasq -l
```

7. Sección de monitoreo de almacenamiento

Sección que nos da una vista de las particiones actuales del disco, su capacidad usado y libre, así como la visualización de la memoria RAM y del CPU con los mismos fines.

Monitoreo de almacenamiento

Particiones						
Filesystem	Size	Used	Avail	Use%	Mounted on	
udev	3.9G	0	3.9G	0%	/dev	
tmpfs	787M	18M	770M	3%	/run	
/dev/sda5	994G	182G	677G	22%	/	
tmpfs	3.9G	65M	3.8G	2%	/dev/shm	
tmpfs	5.0M	4.0K	5.0M	1%	/run/lock	
tmpfs	3.9G	0	3.9G	0%	/sys/fs/cgroup	
/dev/sda1	1.2G	4.5M	1.2G	1%	/boot/efi	
cgfs	100K	0	100K	0%	/run/cgmanager/fs	
tmpfs	787M	64K	787M	1%	/run/user/1000	

Memoria RAM						
Mem:	total	used	free	shared	buff/cache	available
	7.7G	2.7G	2.1G	561M	2.9G	4.1G
Swap:	11G	0B	11G			

CPU												
Linux 4.4.0-116-generic (chepe) 23/03/18 _x86_64_ (8 CPU)												
10:10:14	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle	
10:10:14	all	1.86	0.03	0.70	0.00	0.00	0.00	0.00	0.00	0.00	96.61	
Total usado: 3.39%												
Total libre: 96.61%												

8. Sección de monitoreo de archivos y sockets

La sección nos mostrará los archivos abiertos, con todos sus campos de información como su proceso asociado y el usuario que los está ejecutando.

A la vez, nos da una manera de filtrar esta información para la comodidad del usuario.

Monitoreo de archivos y sockets

Numero máximo de líneas			Búsqueda textual			Búsqueda por expresión regular			FILTRAR
COMMAND	PID	TID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE NAME	
systemd	1		root	cwd	DIR	8,5	4096	2 /	
systemd	1		root	rtld	DIR	8,5	4096	2 /	
systemd	1		root	txt	REG	8,5	1577232	4719006 /lib/systemd/systemd	
systemd	1		root	mem	REG	8,5	18976	4725289 /lib/x86_64-linux-gnu/libuuid.so.1.3.0	
systemd	1		root	mem	REG	8,5	262408	4723515 /lib/x86_64-linux-gnu/libblkid.so.1.1.0	
systemd	1		root	mem	REG	8,5	14608	4728155 /lib/x86_64-linux-gnu/libdl-2.23.so	
systemd	1		root	mem	REG	8,5	456632	4723461 /lib/x86_64-linux-gnu/libpcrc.so.3.13.2	
systemd	1		root	mem	REG	8,5	1868984	4728153 /lib/x86_64-linux-gnu/libc-2.23.so	
systemd	1		root	mem	REG	8,5	138696	4728152 /lib/x86_64-linux-gnu/libpthread-2.23.so	
systemd	1		root	mem	REG	8,5	286824	4718619 /lib/x86_64-linux-gnu/libmount.so.1.1.0	
systemd	1		root	mem	REG	8,5	64144	4718812 /lib/x86_64-linux-gnu/libapparmor.so.1.4.0	
systemd	1		root	mem	REG	8,5	92864	4719904 /lib/x86_64-linux-gnu/libmod.so.2.3.0	
systemd	1		root	mem	REG	8,5	117288	4723322 /lib/x86_64-linux-gnu/libaudit.so.1.0.0	
systemd	1		root	mem	REG	8,5	55904	4723448 /lib/x86_64-linux-gnu/libpam.so.0.83.1	
systemd	1		root	mem	REG	8,5	280848	4718638 /lib/x86_64-linux-gnu/libseccomp.so.2.3.1	
systemd	1		root	mem	REG	8,5	31712	4728171 /lib/x86_64-linux-gnu/librt-2.23.so	
systemd	1		root	mem	REG	8,5	23128	4723335 /lib/x86_64-linux-gnu/libcap.so.2.24	
systemd	1		root	mem	REG	8,5	138224	4723490 /lib/x86_64-linux-gnu/libselinux.so.1	
systemd	1		root	mem	REG	8,5	162632	4728151 /lib/x86_64-linux-gnu/libd-2.23.so	
systemd	1		root	0u	CHR	1,3	010	6 /dev/null	
systemd	1		root	1u	CHR	1,3	010	6 /dev/null	
systemd	1		root	2u	CHR	1,3	010	6 /dev/null	
systemd	1		root	3u	CHR	1,11	010	12 /dev/kmsg	
systemd	1		root	4u	a_inode	0,11	0	8064 [eventpoll]	
systemd	1		root	5u	a_inode	0,11	0	8064 [signalfd]	
systemd	1		root	6r	DIR	0,23	0	1 /sys/fs/cgroup/systemd	
systemd	1		root	7u	a_inode	0,11	0	8064 [timerfd]	
systemd	1		root	8u	netlink		010	11565 KOBJECT_UEVENT	
systemd	1		root	9u	a_inode	0,11	0	8064 [eventpoll]	
systemd	1		root	10r	REG	0,4	0	11566 /proc/1/mountinfo	
systemd	1		root	11r	a_inode	0,11	0	8064 inotify	
systemd	1		root	12r	REG	0,4	0	4026532036 /proc/swaps	
systemd	1		root	13u	unix	0xfffff88021f9dc00	010	12411 /run/systemd/notify type=DGRAM	

9. Sección de monitoreo de servidor web

Finalmente, en esta sección podemos obtener los módulos y VirtualHost de Apache habilitados.

The screenshot shows a web interface titled 'Monitoreo del servidor web'. At the top, there is a navigation bar with a hamburger menu icon on the left and three links: 'EDITAR DATOS', 'ADMINISTRAR USUARIOS', and 'ADMINISTRAR SECCIONES'. On the far right of the navigation bar is a logo for 'UNAM CERT'. Below the navigation bar, the main content area has a title 'Monitoreo del servidor web' and two tabs: 'GRÁFICAS Y ESTADÍSTICAS' (which is active and highlighted in blue) and 'BITÁCORAS'. Under the 'GRÁFICAS Y ESTADÍSTICAS' tab, there are two sub-sections: 'MÓDULOS Y VIRTUALHOSTS' and 'BITÁCORAS'. The 'MÓDULOS Y VIRTUALHOSTS' section displays a list of loaded modules, including 'core_module (static)', 'so_module (static)', 'watchdog_module (static)', 'http_module (static)', 'log_config_module (static)', 'logio_module (static)', 'version_module (static)', 'unixd_module (static)', 'access_compat_module (shared)', 'actions_module (shared)', 'alias_module (shared)', 'auth_basic_module (shared)', 'auth_digest_module (shared)', 'authn_core_module (shared)', 'authn_file_module (shared)', 'authnz_ldap_module (shared)', 'authz_core_module (shared)', 'authz_host_module (shared)', 'authz_user_module (shared)', 'autoindex_module (shared)', 'cgi_module (shared)', 'cgid_module (shared)', 'deflate_module (shared)', 'dir_module (shared)', 'env_module (shared)', 'filter_module (shared)', 'headers_module (shared)', 'info_module (shared)', 'ldap_module (shared)', 'mime_module (shared)', and 'mpm_prefork_module (shared)'. The 'VIRTUALHOST configuration:' section shows three entries: '*:6888' for '127.0.1.1 (/etc/apache2/sites-enabled/web-ip.conf:1)', '*:80' for 'becarios.cert.unam.mx (/etc/apache2/sites-enabled/wordpress.conf:1)', and '*:443' for 'becarios.cert.unam.mx (/etc/apache2/sites-enabled/wordpress.conf:21)'.

Además, de que contará con una pestaña llamada *Bitácoras* donde podremos elegir entre las bitácoras de Apache y otras, desplegando así una lista de los logs que se pueden mostrar, tales como: Messages, Syslog, PostgreSQL, MySQL, y ModSecurity.

Para cada bitácora de Apache se muestra el sitio al que le pertenece, junto con su ubicación.

EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONESUNAM CERT

Monitoreo del servidor web

GRÁFICAS Y ESTADÍSTICAS

MÓDULOS Y VIRTUALHOSTSBITÁCORAS

ACCESO DE APACHE
General: /var/log/apache2/access.log
other-vhosts-access-log.conf: /var/log/apache2/other_vhosts_access.log
proyecto.conf: /var/log/apache2/acceso_proyecto.log

ERROR DE APACHE
General: /var/log/apache2/error.log
proyecto.conf: /var/log/apache2/error_proyecto.log

APACHE MOD SECURITY
Mod Security

OTRAS
Syslog
Messages
PostgreSQL
MySQL

En las bitácoras de acceso de Apache se tiene la opción de mostrar con un formato definido la salida presentada, lo cual se hace por medio de una entrada en el campo **Formato** que debe tener la forma **[hlutrsbRU]+**.

EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONESUNAM CERT

Bitácora de acceso de Apache

Ubicación: /var/log/apache2/access.log

Número máximo de líneas

Búsqueda textual

Búsqueda por expresión regular

Formato

?

FILTRAR

127.0.0.1 - - [15/Mar/2018:08:14:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:19:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:24:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:29:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:34:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:39:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:44:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:49:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:54:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:08:59:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:04:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:09:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:14:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:19:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:24:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:29:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:34:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:39:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:44:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:49:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:54:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:09:59:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:04:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:09:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:14:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:19:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:24:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:29:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:34:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:39:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:44:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:49:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"
127.0.0.1 - - [15/Mar/2018:10:54:44 -0600] "GET / HTTP/1.1" 200 11666 "-" "check_http/v2.1.2 (monitoring-plugins 2.1.2)"

Cada letra del formato representa un campo de la bitácora de acceso, de manera que se muestran estos en el orden indicado.

10. Secciones personalizadas



En esta sección se muestran las bitácoras que se especificaron en el archivo de configuración para alguna sección personalizada.

11. Archivo de configuración

En el archivo de configuración se debe especificar las rutas de las bitácoras para las secciones que lo requieran. El formato del archivo es el siguiente:

```
[seccion]
```

```
archivo = /ruta/del/archivo
```

```
[seccion_2]
```

```
archivo_2 = /otra/ruta
```

Las secciones que requieren rutas para sus bitácoras son **web**, **autenticacion** y las secciones personalizadas, de manera que para estas últimas, el nombre de la sección que será especificada en el archivo de configuración será el **Nombre de configuración** que tenga asociado cada una, es decir, si se creó la sección que tiene por título “Sección de prueba 1”, con **Nombre de configuración** **seccion_1**, entonces en el archivo de configuración se debe de especificar como:

```
[seccion_1]
```

```
archivo1=/ruta/del/archivo
```

```
...
```

La sección de monitoreo de autenticación debe de especificar la ruta de su bitácora de la siguiente manera:

```
[autenticacion]
```

```
auth = /var/log/auth.log
```

Y las bitácoras de la sección de monitoreo web deben de ser especificadas como se indica:

```
[web]
```

```
mod_sec = /var/log/apache2/modsec_audit.log
syslog = /var/log/syslog
messages = /var/log/messages
postgres = /var/log/postgresql/postgresql-9.6-main.log
mysql = /var/log/mysql/error.log
```

Sólo en el caso de las secciones personalizadas es irrelevante el nombre de las variables de cada archivo, sin embargo, en las otras secciones (**web** y **autenticacion**), es importante que se utilicen los nombres definidos.

Un ejemplo completo de un archivo de configuración es el siguiente:

```
[autenticacion]
```

```
auth = /var/log/auth.log
```

```
[web]
```

```
mod_sec = /var/log/apache2/modsec_audit.log
syslog = /var/log/syslog
messages = /var/log/messages
postgres = /var/log/postgresql/postgresql-9.6-main.log
mysql = /var/log/mysql/error.log
```

```
[seccion_1]
```

```
archivo1 = /var/log/auth.log
archivo2 = /var/log/bootstrap.log
```

12. Administrar cuentas de usuario

En la barra superior en la parte derecha tendremos la opción de administrar las cuentas a manera de poder crear o eliminar a nuestro gusto.

Editar datos

Nombre de usuario	<input type="text" value="admin"/>
Nombre	<input type="text" value="Admin"/>
Apellido	<input type="text"/>
Dirección de correo electrónico	<input type="text" value="admin@localhost"/>

[Cambiar contraseña](#)

ACEPTAR

En esta sección podemos obtener los módulos y VirtualHost de Apache habilitados. Además, de que contiene la pestaña llamada bitácoras donde podremos elegir entre las bitácoras de Apache y otras, desplegando así una lista de los logs que se pueden mostrar, tales como: Messages, Syslog, POstgreSQL, MySQL y ModSecurity.




Usuarios





ADMIN
 Nombre: Admin
 Correo: admin@localhost
 Fecha de registro: 16 de Marzo de 2018 a las 19:11
 Último inicio de sesión: 23 de Marzo de 2018 a las 10:08


En la barra superior derecha tenemos también la opción de administrar las cuentas de los usuarios, se listarán con la opción de administrar las cuentas de los usuarios, se listarán con la opción de eliminar la cuenta justo debajo de cada una.

Hasta arriba de las cuentas se podrán agregar más dando click en el +, donde tenemos que llenar el nombre de usuario, el nombre y apellido, correo, contraseña y una confirmación de la misma.



EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONES



Secciones personalizadas




SECCIÓN 1



Nombre de configuración: seccion_1

Fecha de creación: 17 de Marzo de 2018 a las 19:01



En esta opción podemos ver la secciones que hemos creado con su respectivo nombre, nombre de configuración y fecha de creación, teniendo las mismas opciones de agregar, eliminar y editar a cada una de ellas.



EDITAR DATOSADMINISTRAR USUARIOSADMINISTRAR SECCIONES

Nueva sección

Título

Nombre de configuración

CREAR SECCIÓN

En caso de querer agregar una nueva sección se deberá especificar el título, nombre de configuración y dar click en el botón de crear sección.