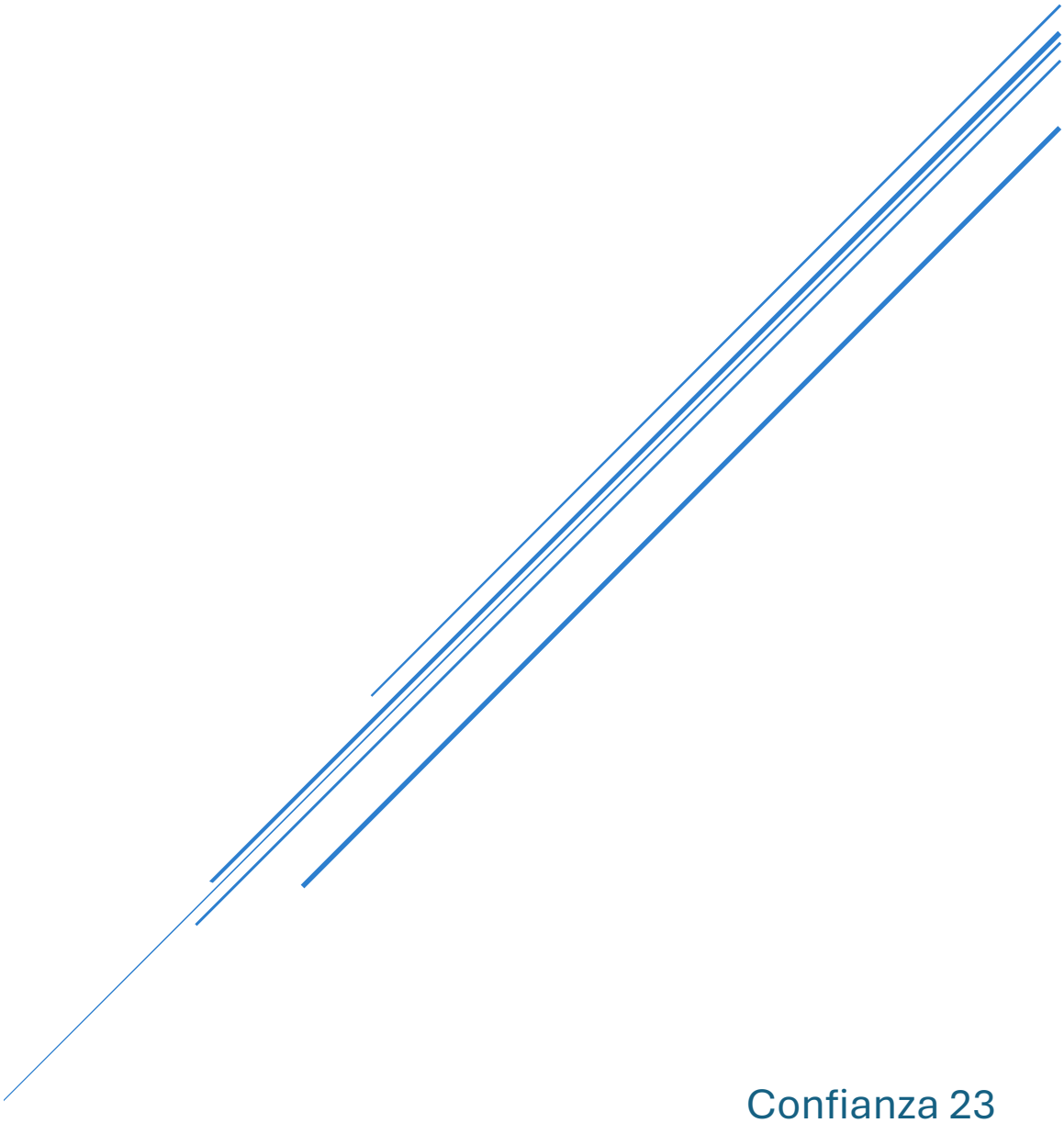
INSTALACIÓN MISP

Ubuntu 24.04.02



Confianza 23
Practicas

Contenidos

¿Qué es MISP?

MISP (Malware Information Sharing Platform) es una plataforma de código abierto diseñada para la gestión, almacenamiento y distribución de indicadores de compromiso (IoCs) y amenazas cibernéticas. Tiene como propósito facilitar el intercambio de inteligencia de amenazas entre organizaciones, equipos de seguridad y centros de respuesta a incidentes (SOC/CSIRT).

Principales Características

- **Gestión de IoCs**: Permite almacenar, correlacionar y compartir indicadores de amenazas como direcciones IP, hashes de archivos maliciosos y dominios sospechosos.
- **Automatización**: Soporta integraciones con herramientas de seguridad mediante API REST y PyMISP (Python).
- **Colaboración**: Facilita la cooperación entre equipos de seguridad, gobiernos y empresas privadas.
- **Compatibilidad con STIX/TAXII**: Utiliza estándares para compartir inteligencia con otras plataformas.
- **Integración con herramientas industriales**: Puede conectarse con SIEMs, honeypots y firewalls para mejorar la detección y respuesta.

Algunos casos de Ciberseguridad Industrial:

- **Monitoreo de amenazas en infraestructuras críticas (SCADA/ICS):** Detectar ataques dirigidos a sistemas industriales.
- **Detección de malware especializado**: Ransomware como Industroyer o TRITON.
- **Automatización de inteligencia de amenazas**: Correlación de IoCs con logs de seguridad para prevenir ataques.

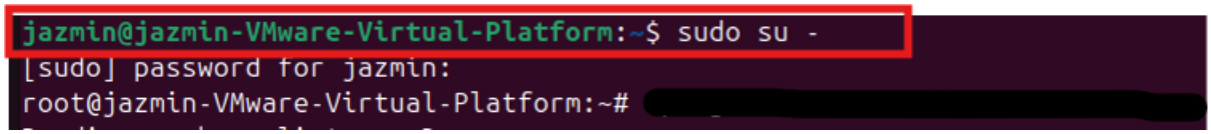
Requisitos

- Ubuntu 20.04 o superior
- Virtual box (en caso de ser necesario)
- Opcional Docker

Proceso de Instalación

Una vez instalado Ubuntu, correr la terminal y cambiar el usuario a root con el comando:

Sudo su –

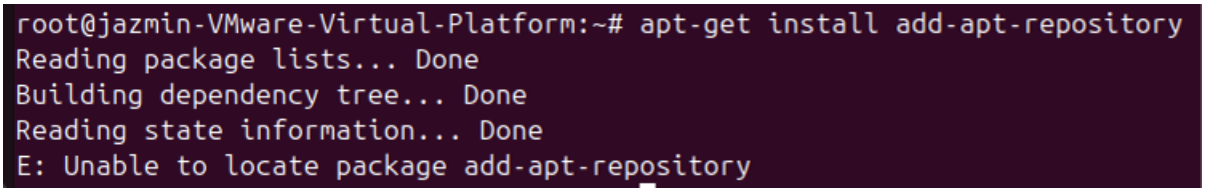


Lo siguiente en el proceso es utilizar los siguientes comandos por orden:

1.Instalar ese repositorio

apt-get install add-apt-repository

Este comando instala el paquete **add-apt-repository**, herramienta que permite añadir repositorios adicionales a la lista de fuentes de software de Ubuntu. Facilita la gestión de repositorios y la instalación de software desde fuentes externas.



***Nota*,** *solución:*

- Verificar el Estado del Gestor de Paquetes

  ps aux | grep apt

- Desbloquear el Sistema de Paquetes

  sudo rm /var/lib/dpkg/lock-frontend

  sudo rm /var/lib/dpkg/lock

  sudo rm /var/cache/apt/archives/lock

- Reconfigurar el Gestor de Paquetes

  sudo dpkg --configure -a

- Instalar software-properties-common

  sudo apt update

  sudo apt install software-properties-common

- Reintentar la Instalación

  sudo add-apt-repository

```
root@jazmin-VMware-Virtual-Platform:~# ps aux | grep apt
root        5813  0.0  0.0  17812  2372 pts/1    S+   00:57   0:00 grep --color=auto apt
root@jazmin-VMware-Virtual-Platform:~# sudo rm /var/lib/dpkg/lock-frontend
root@jazmin-VMware-Virtual-Platform:~# sudo rm /var/lib/dpkg/lock
root@jazmin-VMware-Virtual-Platform:~# sudo rm /var/cache/apt/archives/lock
root@jazmin-VMware-Virtual-Platform:~# sudo dpkg --configure -a
root@jazmin-VMware-Virtual-Platform:~# sudo apt update
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [961 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [213 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [13.5 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,043 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [263 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [364 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [25.9 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:15 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,088 B]
```

```
Get:24 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.0 kB]
Get:25 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [17.0 kB]
Get:26 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 4,361 kB in 7s (614 kB/s)
sudo apt install sofware-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
76 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Agregar el repositorio:

add-apt-repository

```
root@jazmin-VMware-Virtual-Platform:~# sudo add-apt-repository
Error: no actions requested.
usage: add-apt-repository [-h] [-d] [-r] [-s] [-c COMPONENT] [-p POCKET] [-y] [-n] [-l] [--dry-run] [-L] [-P PPA]
                          [-C CLOUD] [-U URI] [-S SOURCESLIST [SOURCESLIST ...]]
                          [line ...]

Only ONE of -P, -C, -U, -S, or old-style 'line' can be specified

positional arguments:
  line                  sources.list line to add (deprecated)

options:
  -h, --help            show this help message and exit
  -d, --debug           Print debug
  -r, --remove          Disable repository
  -s, --enable-source   Allow downloading of the source packages from the repository
  -c COMPONENT, --component COMPONENT
                        Components to use with the repository
  -p POCKET, --pocket POCKET
                        Add entry for this pocket
  -y, --yes             Assume yes to all queries
  -n, --no-update       Do not update package cache after adding
  -l, --login           Login to Launchpad.
```

```
  --dry-run             Don't actually make any changes.
  -L, --list            List currently configured repositories
  -P PPA, --ppa PPA     PPA to add
  -C CLOUD, --cloud CLOUD
                        Cloud Archive to add
  -U URI, --uri URI     Archive URI to add
  -S SOURCESLIST [SOURCESLIST ...], --sourceslist SOURCESLIST [SOURCESLIST ...]
                        Full sources.list entry line to add
```

2. Eliminar paquetes:

apt-get clean

Este comando elimina los paquetes descargados que ya han sido instalados. Limpia el caché de paquetes. Libera espacio en disco al eliminar archivos temporales que ya no son necesarios.

```
root@jazmin-VMware-Virtual-Platform:~# apt-get clean
```

3. Agrega un PPA

sudo add-apt-repository ppa:ondrej/php

Agrega un PPA (Personal Package Archive) llamado ondrej/php, que es un repositorio que contiene versiones más recientes de PHP y sus extensiones. Permite acceder a versiones de PHP que no están disponibles en los repositorios estándar de Ubuntu.

```
root@jazmin-VMware-Virtual-Platform:~# sudo add-apt-repository ppa:ondej/php
ERROR: ppa 'ondej/php' not found (use --login if private)
```

***Nota*,** *solución:*

```
root@jazmin-VMware-Virtual-Platform:~# apt-get install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 76 not upgraded.
```

```
root@jazmin-VMware-Virtual-Platform:~# sudo add-apt-repository ppa:ondrej/php
PPA publishes dbgsym, you may need to include 'main/debug' component
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/ondrej/php/ubuntu/
Suites: noble
Components: main
'
Description:
Co-installable PHP versions: PHP 5.6, PHP 7.x, PHP 8.x and most requested extensions are included. Only Supported Ubuntu
 Releases (https://wiki.ubuntu.com/Releases) are provided.

Debian oldstable and stable packages are provided as well: https://deb.sury.org/#debian-dpa

You can get more information about the packages at https://deb.sury.org
```

```
BUGS&FEATURES: This PPA now has a issue tracker:
https://deb.sury.org/#bug-reporting

CAVEATS:
1. If you are using php-gearman, you need to add ppa:ondrej/pkg-gearman
2. If you are using apache2, you are advised to add ppa:ondrej/apache2
3. If you are using nginx, you are advised to add ppa:ondrej/nginx-mainline
   or ppa:ondrej/nginx

PLEASE READ: If you like my work and want to give me a little motivation, please consider donating regularly: https://do
nate.sury.org/

WARNING: add-apt-repository is broken with non-UTF-8 locales, see
https://github.com/oerdnj/deb.sury.org/issues/56 for workaround:

# LC_ALL=C.UTF-8 add-apt-repository ppa:ondrej/php
More info: https://launchpad.net/~ondrej/+archive/ubuntu/php
Adding repository.
Press [ENTER] to continue or Ctrl-c to cancel.
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble InRelease [24.4 kB]
Get:6 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 Packages [129 kB]
Get:7 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main Translation-en [39.8 kB]
Fetched 193 kB in 7s (26.5 kB/s)
Reading package lists... Done
```

4. Actualizar paquetes

apt-get update

Actualiza la lista de paquetes y sus versiones disponibles desde todos los repositorios configurados. Asegura que el sistema tenga información actualizada sobre los paquetes disponibles, lo que es necesario antes de instalar nuevos paquetes.

```
root@jazmin-VMware-Virtual-Platform:~# apt-get update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble InRelease
Reading package lists... Done
```

5. Instalar PHP 8.3

sudo apt install php8.3 php8.3-cli php8.3-{bz2,curl,mbstring,intl}

Instala PHP 8.3 y sus extensiones: **cli** (interfaz de línea de comandos), **bz2** (compresión bzip2), **curl** (transferencias de URL), **mbstring** (manipulación de cadenas multibyte) e **intl** (funciones de internacionalización). Proporciona las herramientas necesarias para ejecutar aplicaciones PHP y permite el uso de funciones esenciales y populares dentro de PHP.

```
root@jazmin-VMware-Virtual-Platform:~# sudo apt install php8.3-cli php8.3-{bz2,curl,mnstring,intl}
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package php8.3-mnstring
E: Couldn't find any package by glob 'php8.3-mnstring'
```

***Nota*,** *solución:*

El error que estás viendo se debe a que el sistema no puede encontrar el paquete **php8.3-mnstring** o cualquier variante de él.

- Verificar la Disponibilidad del Paquete

apt search php8.3

```
root@jazmin-VMware-Virtual-Platform:~# apt search php.3
Sorting... Done
Full Text Search... Done
php-symfony-polyfill-php73/noble 1.28.0-1 all
  Symfony polyfill backporting some PHP 7.3+ features to lower PHP versions

php-symfony-polyfill-php83/noble 1.28.0-1 all
  Symfony polyfill backporting some PHP 8.3+ features to lower PHP versions
```

- Actualizar Repositorios

sudo apt-get update

```
root@jazmin-VMware-Virtual-Platform:~# sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
```

```
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Hit:5 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble InRelease
Reading package lists... Done
E: Release file for http://security.ubuntu.com/ubuntu/dists/noble-security/InRelease is not valid yet (invalid for anoth
er 7h 11min 29s). Updates for this repository will not be applied.
E: Release file for http://archive.ubuntu.com/ubuntu/dists/noble-updates/InRelease is not valid yet (invalid for another
 10h 32min 20s). Updates for this repository will not be applied.
E: Release file for http://archive.ubuntu.com/ubuntu/dists/noble-backports/InRelease is not valid yet (invalid for anoth
er 7h 13min 17s). Updates for this repository will not be applied.
```

- Instalar PHP y sus Extensiones

sudo apt install php8.3 php8.3-cli php8.3-curl php8.3-intl

```
root@jazmin-VMware-Virtual-Platform:~# sudo apt install php8.3 php8.3-cli php8.3-curl php8.3-intl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64 libsodium23 php-common php8.3-common php8.3-opcache php8.3-readline
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php8.3 libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64 libsodium23 php-common php8.3 php8.3-cli php8.3-common php8.3-curl php8.3-intl
  php8.3-opcache php8.3-readline
0 upgraded, 18 newly installed, 0 to remove and 77 not upgraded.
Need to get 7,235 kB of archives.
After this operation, 31.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Get:2 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php-common all 2:95+ubuntu24.04.1+deb.sury.org
+2 [13.2 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
```

```
Unpacking apache2-utils (2.4.58-1ubuntu8.5) ...
Selecting previously unselected package apache2.
Preparing to unpack .../07-apache2_2.4.58-1ubuntu8.5_amd64.deb ...
Unpacking apache2 (2.4.58-1ubuntu8.5) ...
Selecting previously unselected package php-common.
Preparing to unpack .../08-php-common_2%3a95+ubuntu24.04.1+deb.sury.org+2_all.deb ...
Unpacking php-common (2:95+ubuntu24.04.1+deb.sury.org+2) ...
Selecting previously unselected package php8.3-common.
Preparing to unpack .../09-php8.3-common_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-common (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3-opcache.
Preparing to unpack .../10-php8.3-opcache_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-opcache (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3-readline.
Preparing to unpack .../11-php8.3-readline_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-readline (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package libsodium23:amd64.
Preparing to unpack .../12-libsodium23_1.0.18-1build3_amd64.deb ...
Unpacking libsodium23:amd64 (1.0.18-1build3) ...
Selecting previously unselected package php8.3-cli.
Preparing to unpack .../13-php8.3-cli_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-cli (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package libapache2-mod-php8.3.
Preparing to unpack .../14-libapache2-mod-php8.3_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking libapache2-mod-php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3.
Preparing to unpack .../15-php8.3_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_all.deb ...
Unpacking php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3-curl.
Preparing to unpack .../16-php8.3-curl_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-curl (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3-intl.
```

```
Selecting previously unselected package php8.3-curl.
Preparing to unpack .../16-php8.3-curl_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-curl (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Selecting previously unselected package php8.3-intl.
Preparing to unpack .../17-php8.3-intl_8.3.19-1+ubuntu24.04.1+deb.sury.org+1_amd64.deb ...
Unpacking php8.3-intl (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Setting up php-common (2:95+ubuntu24.04.1+deb.sury.org+2) ...
Created symlink /etc/systemd/system/timers.target.wants/phpsessionclean.timer → /usr/lib/systemd/system/phpsessionclean.
timer.
Setting up libsodium23:amd64 (1.0.18-1build3) ...
Setting up php8.3-common (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...

Creating config file /etc/php/8.3/mods-available/calendar.ini with new version

Creating config file /etc/php/8.3/mods-available/ctype.ini with new version

Creating config file /etc/php/8.3/mods-available/exif.ini with new version

Creating config file /etc/php/8.3/mods-available/fileinfo.ini with new version

Creating config file /etc/php/8.3/mods-available/ffi.ini with new version

Creating config file /etc/php/8.3/mods-available/ftp.ini with new version

Creating config file /etc/php/8.3/mods-available/gettext.ini with new version

Creating config file /etc/php/8.3/mods-available/iconv.ini with new version

Creating config file /etc/php/8.3/mods-available/pdo.ini with new version

Creating config file /etc/php/8.3/mods-available/phar.ini with new version
```

```
Creating config file /etc/php/8.3/mods-available/sysvsem.ini with new version

Creating config file /etc/php/8.3/mods-available/sysvshm.ini with new version

Creating config file /etc/php/8.3/mods-available/tokenizer.ini with new version
Setting up php8.3-readline (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...

Creating config file /etc/php/8.3/mods-available/readline.ini with new version
Setting up libapr1t64:amd64 (1.7.2-3.1ubuntu0.1) ...
Setting up apache2-data (2.4.58-1ubuntu8.5) ...
Setting up php8.3-opcache (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...

Creating config file /etc/php/8.3/mods-available/opcache.ini with new version
Setting up libaprutil1t64:amd64 (1.6.3-1.1ubuntu7) ...
Setting up php8.3-curl (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...

Creating config file /etc/php/8.3/mods-available/curl.ini with new version
Setting up php8.3-intl (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...

Creating config file /etc/php/8.3/mods-available/intl.ini with new version
Setting up libaprutil1-ldap:amd64 (1.6.3-1.1ubuntu7) ...
Setting up php8.3-cli (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
update-alternatives: using /usr/bin/php8.3 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar8.3 to provide /usr/bin/phar (phar) in auto mode
update-alternatives: using /usr/bin/phar.phar8.3 to provide /usr/bin/phar.phar (phar.phar) in auto mode

Creating config file /etc/php/8.3/cli/php.ini with new version
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.1ubuntu7) ...
Setting up apache2-utils (2.4.58-1ubuntu8.5) ...
Setting up apache2-bin (2.4.58-1ubuntu8.5) ...
Setting up libapache2-mod-php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Package apache2 is not configured yet. Will defer actions by package libapache2-mod-php8.3.
```

```
Creating config file /etc/php/8.3/apache2/php.ini with new version
No module matches
Setting up apache2 (2.4.58-1ubuntu8.5) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
info: Switch to mpm prefork for package libapache2-mod-php8.3
Module mpm_event disabled.
Enabling module mpm_prefork.
```

```
Enabling module php8.3.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache
-htcacheclean.service.
Setting up php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Processing triggers for php8.3-cli (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Processing triggers for libapache2-mod-php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
```

6. MISP Instalación

wget --no-cache -O /tmp/INSTALL.sh
https://raw.githubusercontent.com/MISP/MISP/refs/heads/2.5/INSTALL/INSTALL.ubuntu244.sh bash /tmp/INSTALL.sh

```
root@jazmin-VMware-Virtual-Platform:~# wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/re
fs/heads/2.5/INSTALL/INSTALL.ubuntu2404.sh
bash /tmp/INSTALL.sh
--2025-03-27 01:14:09--  https://raw.githubusercontent.com/MISP/MISP/refs/heads/2.5/INSTALL/INSTALL.ubuntu2404.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ..
.
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34604 (34K) [text/plain]
Saving to: '/tmp/INSTALL.sh'

/tmp/INSTALL.sh              100%[=============================================>]  33.79K  --.-KB/s    in 0.03s

2025-03-27 01:14:09 (1.22 MB/s) - '/tmp/INSTALL.sh' saved [34604/34604]

 _____ _____ _____ _____
|     |     |   __|  _  |
| | | |-   -|__   |   __|
|_|_|_|_____|_____|__|
v2.5 Setup on Ubuntu 24.04 LTS
```

```
v2.5 Setup on Ubuntu 24.04 LTS
[STATUS] Updating base system...

[OK] Base system update successfully completed.
[STATUS] Installing apt packages (git curl python3 python3-pip python3-virtualenv apache2 zip gcc sudo binutils openssl
supervisor)...
[OK] git installation successfully completed.
[OK] curl installation successfully completed.
[OK] python3 installation successfully completed.
[OK] python3-pip installation successfully completed.
[OK] python3-virtualenv installation successfully completed.
[OK] apache2 installation successfully completed.
[OK] zip installation successfully completed.
[OK] gcc installation successfully completed.
[OK] sudo installation successfully completed.
[OK] binutils installation successfully completed.
[OK] openssl installation successfully completed.
[OK] supervisor installation successfully completed.
[OK] Basic dependencies installation successfully completed.
[STATUS] Installing MariaDB...
[OK] mariadb-server installation successfully completed.
[OK] mariadb-client installation successfully completed.
[OK] MariaDB installation successfully completed.
[STATUS] Installing PHP and the list of required extensions...
[OK] redis-server installation successfully completed.
[OK] php8.3 installation successfully completed.
[OK] php8.3-cli installation successfully completed.
[OK] php8.3-dev installation successfully completed.
[OK] php8.3-xml installation successfully completed.
[OK] php8.3-mysql installation successfully completed.
[OK] php8.3-opcache installation successfully completed.
[OK] php8.3-readline installation successfully completed.
[OK] php8.3-mbstring installation successfully completed.
```

```
[STATUS] Installing PHP and the list of required extensions...
[OK] redis-server installation successfully completed.
[OK] php8.3 installation successfully completed.
[OK] php8.3-cli installation successfully completed.
[OK] php8.3-dev installation successfully completed.
[OK] php8.3-xml installation successfully completed.
[OK] php8.3-mysql installation successfully completed.
[OK] php8.3-opcache installation successfully completed.
[OK] php8.3-readline installation successfully completed.
[OK] php8.3-mbstring installation successfully completed.
[OK] php8.3-zip installation successfully completed.
[OK] php8.3-intl installation successfully completed.
[OK] php8.3-bcmath installation successfully completed.
[OK] php8.3-gd installation successfully completed.
[OK] php8.3-redis installation successfully completed.
[OK] php8.3-gnupg installation successfully completed.
[OK] php8.3-apcu installation successfully completed.
[OK] libapache2-mod-php8.3 installation successfully completed.
[OK] php8.3-curl installation successfully completed.
[OK] PHP and required extensions installation. successfully completed.
[STATUS] Installing composer...
[OK] Composer installation successfully completed.
[STATUS] Configuring php and MySQL configs...
[OK] Apache restart successfully completed.
[OK] MySQL restart successfully completed.
[OK] PHP and MySQL configured...
```

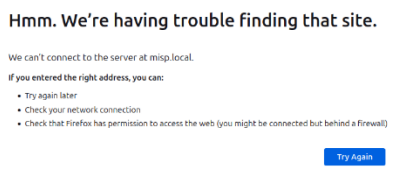
```
[STATUS] Installing PECL extensions...
[OK] PECL brotli extension installation successfully completed.
[OK] PECL simdjson extension installation successfully completed.
[OK] PECL zstd extension installation successfully completed.
[STATUS] Cloning MISP
[OK] MISP cloning successfully completed.
[OK] Fetching 2.5 branch successfully completed.
[OK] Checking out 2.5 branch successfully completed.
[STATUS] Cloning MISP submodules...

[OK] MISP submodules cloning successfully completed.
[OK] MISP's submodules cloned.
[STATUS] Installing MISP composer dependencies...
[OK] MISP composer dependencies installation successfully completed.
[STATUS] Create DB and user for MISP as well as importing the basic MISP schema...
[OK] MISP database schema import successfully completed.
[STATUS] Moving and configuring MISP php config files..
[OK] MISP php config files moved and configured.
[NOTICE] Generating self-signed SSL certificate.
[OK] Self-signed SSL certificate generation successfully completed.
[STATUS] Creating Apache configuration file for MISP...
[STATUS] Running MISP updates
[OK] MISP updated.
[STATUS] Generating PGP key
[OK] PGP key generation successfully completed.
[OK] PGP key export successfully completed.
[STATUS] Setting up Python environment for MISP
[OK] Python virtualenv creation successfully completed.
[OK] Python virtualenv activation successfully completed.
[OK] Python dependencies installation successfully completed.
```

```
[STATUS] Setting up background workers
[OK] Background workers setup successfully completed.
[OK] Settings configured.
[STATUS] Ingesting JSON structures


[OK] JSON structures ingestion successfully completed.
[OK] Apache restart successfully completed.
[OK] Settings configured.
[STATUS] Finalising MISP setup...
[NOTICE] Settings saved to /var/log/misp_settings.txt
[NOTICE] You can now access your MISP instance at https://misp.local
[NOTICE] The default admin credentials are:
[NOTICE] Username: admin@admin.test
[NOTICE] Password: LT0yUvxApG2G9qLtZ3dGqKMu7r30INgr
[NOTICE] MISP setup complete. Thank you, and have a very safe, and productive day.
```

Abrir https://misp.local



***Nota*,** *solución:*

- Verificar la Instalación de MISP

```
root@jazmin-VMware-Virtual-Platform:~# wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/refs/heads/2.5/INSTALL/INSTALL.ubuntu2404.sh
--2025-03-27 15:04:21--  https://raw.githubusercontent.com/MISP/MISP/refs/heads/2.5/INSTALL/INSTALL.ubuntu2404.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34604 (34K) [text/plain]
Saving to: '/tmp/INSTALL.sh'

/tmp/INSTALL.sh              100%[=================================================>]  33.79K  --.-KB/s    in 0.006s

2025-03-27 15:04:22 (5.62 MB/s) - '/tmp/INSTALL.sh' saved [34604/34604]
```

- Verificar el Archivo Hosts

sudo nano /etc/hosts

```
root@jazmin-VMware-Virtual-Platform:~# sudo nano /etc/hosts
```

- Verificar que este y sino agregar

127.0.0.1 misp.local

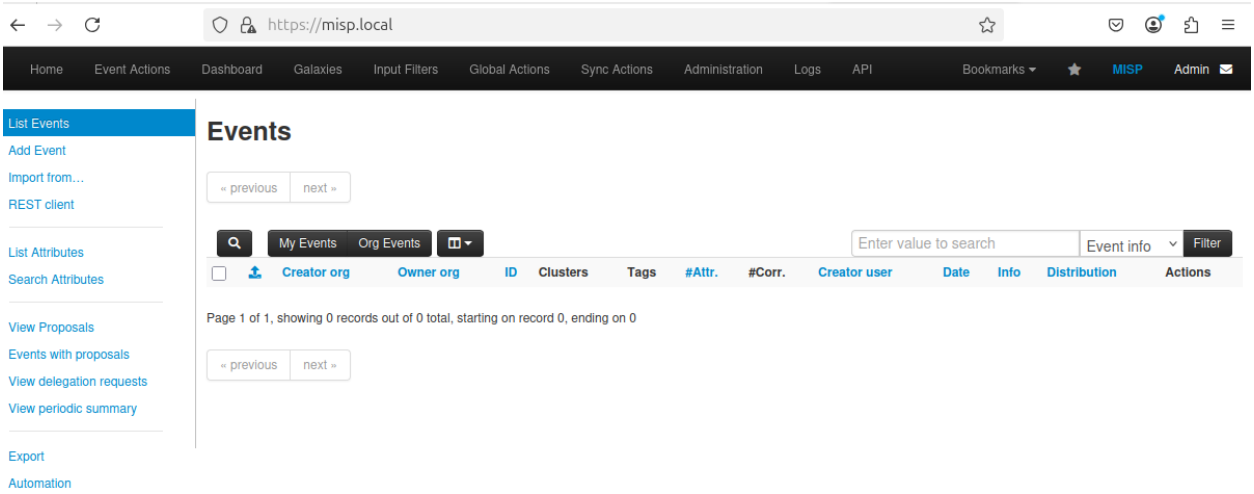
```
 GNU nano 7.2                        /etc/hosts
127.0.0.1 localhost
127.0.1.1 jazmin-VMware-Virtual-Platform
127.0.0.1 misp.local

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- Reiniciar el Servidor Web

sudo systemctl restart apache2

Abrir nuevamente https://misp.local


https://misp.local
Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Logs
API
Bookmarks
MISP
Admin
List Events
Add Event
Import from…
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
View periodic summary
Export
Automation
Events
« previous
next »
My Events
Org Events
Enter value to search
Event info
Filter
Creator org
Owner org
ID
Clusters
Tags
#Attr.
#Corr.
Creator user
Date
Info
Distribution
Actions
Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0
« previous
next »

Notas Finales

- Asegúrate de actualizar MISP regularmente para obtener las últimas funcionalidades y parches de seguridad.
- Consulta la documentación oficial de MISP para más detalles y soporte.

Recursos

- Osepov, B. (2024) 'Installing MISP 2.5 and basic API usage - Boris Osepov - medium,' *Medium*, 3 December. https://medium.com/@boristheblade1/installing-misp-2-5-and-basic-api-usage-ccfbee4177a9
- Misp (no date) *GitHub - MISP/MISP: MISP (core software) - Open-Source Threat Intelligence and Sharing Platform*. https://github.com/MISP/MISP
- Misp (no date a) *Download*. https://www.misp-project.org/download/