Guía de instalación de MISP

Pasos a Seguir

Los siguientes pasos describen la instalación de la herramienta MISP para un ambiente productivo.

1. Instalación de MISP y sus dependencias principales.

Existen varias formas de instalar MISP. En su documentación oficial dentro de su github ofrece guías de instalación para diversos sistemas operativos. En ellas se detallan todas las dependencias y cómo instalarlas y configurarlas.

También posee un script donde se instalan y configuran todas las dependencias de forma automática.

Para instalar desde el script se debe descargar. Ejecutar comando:

```
$ wget -O /tmp/INSTALL.sh
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

Una vez descargado el script se debe ejecutar con las opciones que se crean necesarias en cada caso. Si se ejecuta sin opciones entonces se mostrará la lista de opciones de instalación. Comando y respuesta:

```
misp3@testmisptres:~$ bash /tmp/INSTALL.sh
…
/tmp/INSTALL.sh -c | Install ONLY MISP Core
          -M | MISP modules
          -m | Mail 2 MISP
          -S | Experimental ssdeep correlations
          -A | Install all of the above
----------------------------------------------------------------------------------------------------------------------------------
          -C | Only do pre-install checks and exit
----------------------------------------------------------------------------------------------------------------------------------
          -u | Do an unattended Install, no questions asked
     -U | Attempt and upgrade of selected item
     -N | Nuke this MISP Instance
     -f | Force test install on current Ubuntu LTS schim, add -B for 18.04 -> 18.10, or -BB 18.10 -> 19.10)

Options can be combined: /tmp/INSTALL.sh -c -D $ Will install Core+Dashboard
----------------------------------------------------------------------------------------------------------------------------------
Recommended is either a barebone MISP install (ideal for syncing from other instances) or
MISP + modules - /tmp/INSTALL.sh -c -M
```

```
Interesting environment variables that get considered are:

MISP_USER/MISP_PASSWORD $ Local username on machine, default: misp/opensslGeneratedPassword

PATH_TO_MISP $ Where MISP will be installed, default: /var/www/MISP (recommended)

DBHOST/DBNAME $ database hostname, MISP database name, default: localhost/misp
DBUSER_ADMIN/DBPASSWORD_ADMIN $ MySQL admin user, default: root/opensslGeneratedPassword
DBUSER_MISP/DBPASSWORD_MISP $ MISP database user, default: misp/opensslGeneratedPassword

You need to export the variable(s) to be taken into account. (or specified in-line when invoking
INSTALL.sh)
----------------------------------------------------------------------------------------------------------------------------------
```

En nuestro caso realizamos la instalación con la opción -c para instalar sólo el core de MISP. Comando:

```
$ wget -O /tmp/INSTALL.sh -c
```

Este comando puede tardar mucho tiempo en terminar de ejecutarse, y al finalizar se detallarán usuarios y contraseñas que se han generado en la instalación. Estos se deben copiar y guardar de forma segura hasta que se cambien, de otra manera se perderá el acceso.

Adicionalmente, al finalizar aclara las configuraciones necesarias para postfix en caso de querer enviar mails.

```
-------------------------------------------------------------------------
Admin (root) DB Password: 446fcaxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxadc111
User  (misp) DB Password: 9281f4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx1fa80b
Authkey: o3PKFxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxnx738
--------------------------------------------------------------------------
MISP Installed, access here:

User: admin@admin.test
Password: admin
--------------------------------------------------------------------------
The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
Contents:
cat: /home/misp/mysql.txt: Permission denied
/home/misp/MISP-authkey.txt
Contents:
cat: /home/misp/MISP-authkey.txt: Permission denied
--------------------------------------------------------------------------
The LOCAL system credentials:
User: misp
```

```
Password: e071dxxxxxxxxxxxxxxxxxxxxxxx361a1d $ Or the password you used of your custom user
---------------------------------------------------------------------------
GnuPG Passphrase is: 3ad9e88534xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4d61f0a9d5
---------------------------------------------------------------------------
To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:

sudo postconf -e 'relayhost = example.com'
sudo postfix reload
---------------------------------------------------------------------------
Enjoy using MISP. For any issues see here: https://github.com/MISP/MISP/issues
---------------------------------------------------------------------------
```

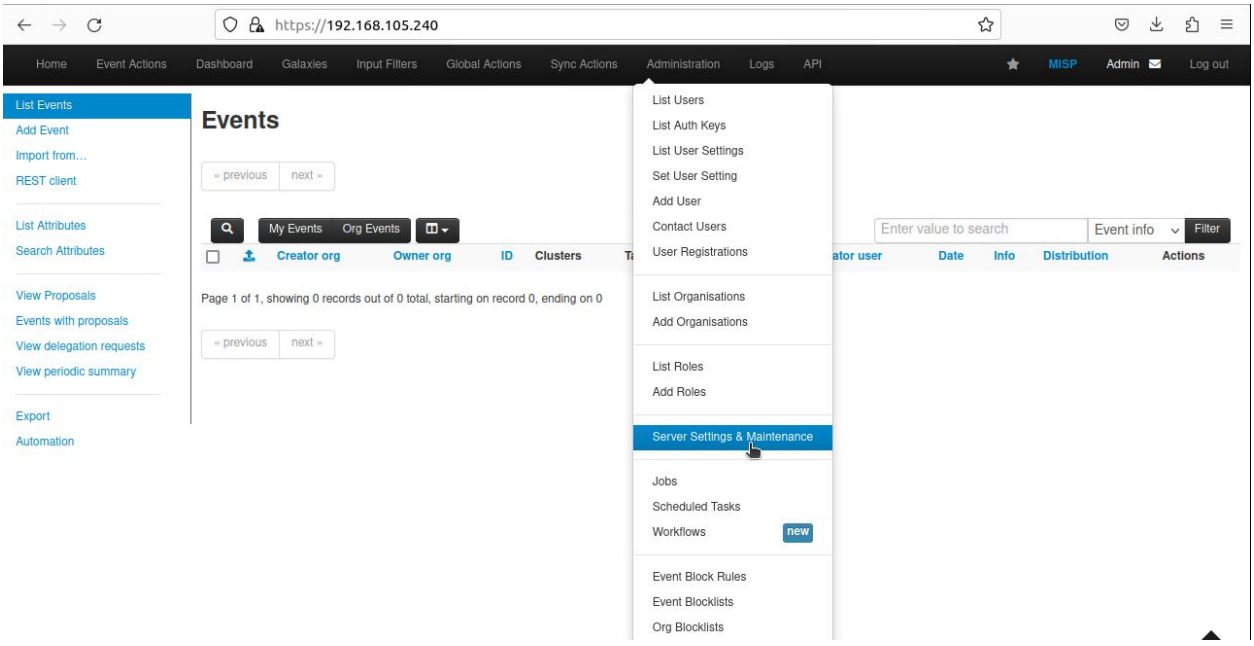
Al finalizar ya se puede acceder a MISP desde la IP del host configurado y cambiar el correo electrónico, la contraseña y la clave de autenticación después de la instalación. Las credenciales iniciales son:

User: admin@admin.test

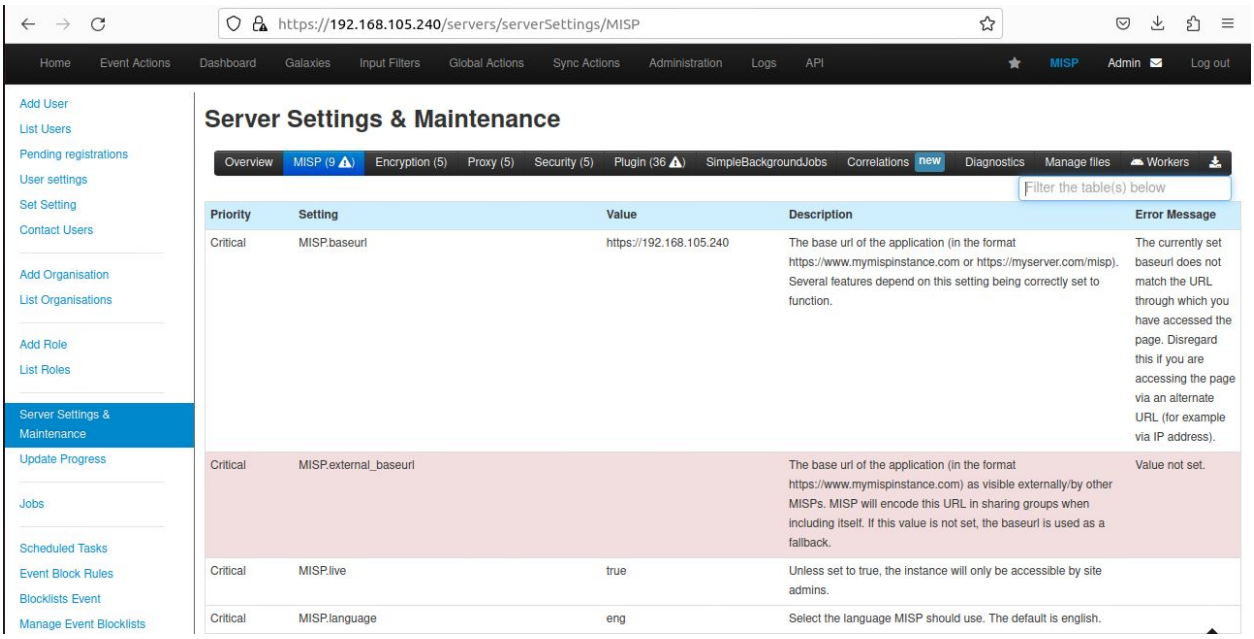
Password: admin

2) Configuración de MISP

Una vez instalado y con usuario y claves cambiadas se debe seleccionar la opción Administración del menú superior y elegir Server Settings & Maintenance.



En esta pantalla se solicitará atención a algunas configuraciones. Se podrán resolver tanto en el panel visual como por consola.



A continuación se detalla la configuración recomendada para realizar si decide utilizar consola. También será útil para tener un ejemplo de cada campo si se está configurando de manera visual.

2. 1. Definir la URL de MSIP. Si la configuración actual de baseurl figura como https://<tu IP> es correcto dejarlo de esa forma.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
MISP.baseurl https://<tu FQDN>

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.external_baseurl" https://<tu FQDN>
```

Para averiguar su FQDN, también conocido como Nombre de Dominio Completo, ingrese el siguiente comando:

```
$ hostname --fqdn
```

2. 2. Habilitar la organización predeterminada y configurar algunas variables.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.host_org_id" 1

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.email" "<tu_email>"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.disable_emailing" true
```

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.contact" "<tu_email>"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.disablerestalert" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.showCorrelationsOnIndex" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.default_event_tag_collection" 0
```

2. 3. Configuar plugins

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_services_enable" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_services_url" "http://127.0.0.1"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_services_port" 9000

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_timeout" 120

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_authkey" "" --force

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_ssl_verify_peer" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_ssl_verify_host" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Cortex_ssl_allow_self_signed" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Sightings_policy" 0

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Sightings_anonymise" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Sightings_range" 365

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.Sightings_sighting_db_enable" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.CustomAuth_disable_logout" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_policy" "DROP"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
```

```
"Plugin.RPZ_walled_garden" "127.0.0.1"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_serial" "\$date00"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_refresh" "2h"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_retry" "30m"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_expiry" "30d"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_minimum_ttl" "1h"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_ttl" "1w"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_ns" "localhost."
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_ns_alt" "" --force
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Plugin.RPZ_email" "root.localhost"
```

2. 4. Configurar Redis.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.redis_host" "127.0.0.1"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.redis_port" 6379
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.redis_database" 13
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.redis_password" ""
```

2. 5. Configurar opciones por defecto.

2. 5. 1. Forzar valores predeterminados para reducir los problemas "Críticos" (red) de la configuración del servidor MISP.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.language" "eng"
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.proposals_block_attributes" false
```

2. 5. 2. Forzar valores predeterminados para reducir las configuraciones "recomendadas" (yellow) en el servidor MISP.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.ssdeep_correlation_threshold" 40

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.extended_alert_subject" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.default_event_threat_level" 4

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.newUserText" "Estimado nuevo usuario de MISP,\\n\\nPor la pesrente nos
agrada darle la bienvenida a la comunidad \$org MISP.\\n\\n Utilice las
siguientes credenciales para iniciar sesión en MISP en \$misp, donde se le
pedirá que cambie manualmente su contraseña a algo de su propia elección.\\
n\\nUsuario: \$username\\nContraseña: \$password\\n\\nSi tiene alguna
pregunta, no dude en ponerse en contacto con nosotros: \$contact.\\n\\
nSaludos cordiales,\\nEquipo de soporte de \$org MISP"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.passwordResetText" "Estimado usuario de MISP,\\n\\nSe ha activado un
restablecimiento de contraseña para su cuenta. Utilice la contraseña temporal
proporcionada a continuación para iniciar sesión en MISP en \$misp, donde se
le pedirá que cambie manualmente su contraseña a algo de su propia
elección.\\n\\nUsuario: \$username\\nContraseña temporal: \$password\\n\\nSi
tiene alguna pregunta, no dude en ponerse en contacto con nosotros: \
$contact.\\n\\nSaludos cordiales,\\nEquipo de soporte de \$org MISP"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.enableEventBlocklisting" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.enableOrgBlocklisting" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.disableUserSelfManagement" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.block_event_alert" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.block_event_alert_tag" "no-alerts=\"true\"" --force

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.block_old_event_alert" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.block_old_event_alert_age" ""

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.block_old_event_alert_by_date" ""

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
```

```
"MISP.incoming_tags_disabled_by_default" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.maintenance_message" "¡Grandes cosas están sucediendo! MISP está en
mantenimiento, pero regresará en breve. Puede ponerse en contacto con la
administración mediante el correo \$email."

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.attachments_dir" "/var/www/MISP/app/files"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.download_attachments_on_load" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.title_text" "MISP"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.terms_download" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.showorgalternate" false

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.event_view_filter_fields" "id, uuid, value, comment, type, category,
Tag.name"
```

2. 5. 3. Forzar valores predeterminados para reducir las configuraciones "opcionales" (green) en el servidor MISP.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Security.password_policy_length" 12

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Security.password_policy_complexity" '/^((?=.*\d)|(?=.*\W+))(?![\n])(?=.*[A-
Z])(?=.*[a-z]).*$|.{16,}/'

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"Security.self_registration_message" "Si desea enviarnos una solicitud de
registro, por favor complete el siguiente formulario. Asegúrese de completar
la mayor cantidad de información posible para facilitar la tarea de los
administradores."
```

2. 6. Agregar la dirección IP en los registros.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.log_client_ip" true

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.log_auth" true
```

2. 7. Personalizar MISP.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.footermidleft" ""

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.footermidright" "Operated by <SU_ORG>"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.welcome_text_top" "<SU_ORG>"

$ sudo -u www-data /var/www/MISP/app/Console/cake admin setSetting
"MISP.welcome_text_bottom" ""
```

2. 8. Actualizar galaxias, taxonomías entre otros objetos: Estas actualizaciones demoran unos minutos.

```
$ sudo -u www-data /var/www/MISP/app/Console/cake admin updateGalaxies

$ sudo -u www-data /var/www/MISP/app/Console/cake admin updateTaxonomies

$ sudo -u www-data /var/www/MISP/app/Console/cake admin updateWarningLists

$ sudo -u www-data /var/www/MISP/app/Console/cake admin updateNoticeLists

$ sudo -u www-data /var/www/MISP/app/Console/cake admin updateObjectTemplates
"1337"
```